

Global Information Assurance Certification Paper

Copyright SANS Institute Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering "Auditing Systems, Applications, and the Cloud (Audit 507)" at http://www.giac.org/registration/gsna

Audit of an ePolicy Orchestrator (ePO) v.2.5.1 Server: An Auditor's Perspective

Stéphane Laberge March 2003 SANS GSNA Practical Assignment v2.1 (amended July 5, 2002)

(translated from the original French version)

Table of Contents

Assignment 1: Audit Research Technique, Methods Used to Audit and Monito the System	
 1.0 System Audited 1.1 Role of the Audited System	5 6 7 7 7 7 7 7 7 7 7 7 7
Assignment 2: Creating a Security Audit Form	
 2.1 Explanation of the form used 2.2 Explanation of the Risk Level calculation	20 21 21 21 21 21 29 46
Assignment 3: Audit Evidence	69
 3.1 Conducting a Security Audit	69 87 114 138 150
Assignment 4: Audit Report	
4.1 Administrative Summary4.1.1 Purpose of the audit4.1.2 Summary of results	153

4.1.3 Risk analysis summary	
4.1.4 Recommendations	
4.2 Anticipated Cost	
4.3 Interim Solution	
REFERENCES	157

Assignment 1: Audit Research Technique, Methods Used to Audit and Monitor the System

1.0 System Audited

The system being audited is the Network Associates ePolicy Orchestrator (ePO) v2.5 antivirus server. ePO handles the central management of an array of antivrus products from Network Associates, as well as the Mcafee Desktop Firewall (a personal firewall) and Threat Scan.

The audit described in this report focuses on the ePO management console and the ePO agent deployed by the server. The NetShield 4.5 SP1 file server configuration was also audited, to ensure the ePO server has adequate protection. The operating system's logical security was lightly audited to identify its main vulnerabilities. The server's physical security was not assessed.

The ePO server is installed on an HP LH 6000 Dual Xeon 700 server with 1 GB of memory, two 18 GB drives used in RAID 1 for the operating system (Windows 2000 Advanced Server SP2), and three 36 GB drives used in RAID 5 for ePO server data, the required MSDE database and the FTP service provided by Internet Information Server v5.0 (IIS).

The ePO server provides antivirus protection for over 3500 workstations and approximately 250 NT/2000 servers of varying types.

The following diagram shows the positions of the server audited and the laptop used to conduct the audit in segment 172.25.1.0:

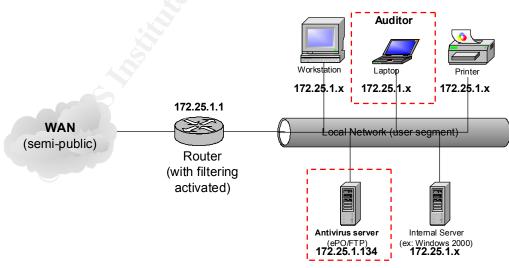


Diagram of Audited Network

Note: Although the wide area network (WAN) is separated from the local network (LAN) by a router with active filtering, software or protocol such as NetBios, Terminal Service, PcAnywhere, etc., can be used to communicate with the audited server from anywhere on the WAN.

1.1 Role of the Audited System

The role of the ePO central management console is to ensure the deployment and monitoring of updates for supported software, particularly antivirus solutions. The greater the number of workstations or servers, the greater the importance and even vital necessity of using antivirus software to provide security.

The audited system handles the deployment and configuration of antivirus software (VirusScan and NetShield) from NAI, the configuration (only) of the GroupShield antivirus program for Exchange 5.5 / 2000 e-mail servers, the monitoring of signature updates (.DAT) and VirusScan and NetShield updates (e.g.: engines, hotfixes, Service Packs, etc.). The audited system also handles the deployment and configuration of Mcafee Desktop Firewall on all laptops (about 500) that access the system through a virtual private network (VPN).

None of these products require a central management console to function. The signature update schedule, default configurations for each product, and product response upon detecting a virus, worm or other malicious mobile code (Java Script and ActiveX) can all be manually configured (or set through startup scripts) on each station.

The manufacturer provides an Installation Designer that can be used to preconfigure the VirusScan installation file (.MSI) in order to reduce the work of network administrators and computer technicians performing the initial workstation installation.

In short, at first glance, unless one has a network with a very large number of workstations and servers, there is no significant advantage to installing and maintaining the ePolicy Orchestrator central management console.

1.1.1 Why use a central management console?

According to a recent survey, about $10\%^1$ of organizations (small businesses to major corporations), still do not use antivirus software. This same survey says that the average annual cost of computer viruses, per organization, is about \$283,000².

¹ 2002 CSI/FBI Computer Crime and Security Survey, Richard Power, page 2 http://www.gocsi.com/forms/fbi/pdf.html

² 2002 CSI/FBI Computer Crime and Security Survey, Richard Power, page 16 http://www.gocsi.com/forms/fbi/pdf.html

Incidents caused by computer viruses are steadily increasing and although it is still not possible to predict the future, it is unlikely that the situation will improve.

If 90% of companies are protected by antivirus software, why are there so many virus incidents? Why are viruses and malicious code still some of the best ways to attack just about any computer system (servers, stations, PDA, mobile phones, and probably almost any equipment that allows for the transfer of information)?

The reason is that most organizations only install protection. This situation is exacerbated by certain security weaknesses in some software (e.g.: Internet Explorer, Outlook, Outlook Express), which are difficult to secure unless specifically hardened, and unless users are educated about their use.

Today, there are few organizations that have Internet access and do not have a firewall. Similarly, few organizations would hesitate to install an antivirus solution.

But how effective is a firewall if the servers it protects are not hardened properly? The answer is: not very, because the attacker will use a completely legitimate entry point in order to get through the application layer of the responding server. So, is hardening the best protection? The answer to that is that it's necessary, but sooner or later a new weakness will be identified and exploited.

1.1.2 Protection is never 100%

One must remember that no protective measure is 100% effective. However, what one can and must do is improve protection by organizing security in layers. Install a firewall, add a demilitarized zone (DMZ), choose the software wisely and harden the servers and applications used on each server. This helps achieve an acceptable level of protection. It does not, however, provide an absolute guarantee that there will be no intrusions, no matter how much money is spent on protection.

If, for antivirus products like ones from Network Associates Inc. (NAI), the software is installed and no attention is paid to the initial configuration, but updates are retrieved regularly, one could say that security is concentrated on protection.

1.1.3 How can one be sure the network is truly up to date ?

If the system being protected has few workstations, it is quite possible that the antivirus solution will not be kept religiously up to date. The reason for this is simple: to verify whether the solution is up to date, one must do a manual check of each machine.

This is not so difficult when all the workstations are on site, but it's another story when laptops are involved.

If an organization has several thousand workstations and a wide area network in a number of different physical locations, what is the likelihood that all stations will be up to date?

1.1.4 The importance of monitoring

Attackers, of course, are quite aware of such weaknesses. Which is why computer viruses are the most frequently reported security incidents (85% of the time)³. But the main reason for the weakness is that a key element is missing from the security process: protection system monitoring.

Because protection cannot be 100% effective (e.g.: the antivirus software may not up to date, or a new strain of virus may appear, or malicious code may be executed without the user knowing, etc.), what is required is a mechanism that will proactively monitor protection systems to ensure that the response to any incident is as fast as possible.

Without monitoring, there can be no response. Or rather, there will be a response, but it will be a response to an incident that has already caused damage.

The ePO management console provides effective monitoring through its extremely versatile report module, which is integrated with Crystal Reports and an SQL database. Of course, it's not enough to have the monitoring tools; one also needs a response procedure.

1.1.5 Three-stage process

To maintain a highly secure environment, one must put equal effort into protection, monitoring and response. The greater the balance between these three elements, the greater the chances of success.

³ 2002 CSI/FBI Computer Crime and Security Survey, Richard Power, page 15 http://www.gocsi.com/forms/fbi/pdf.html



1.1.5.1 Protection

Let us say the organization is installing an antivirus solution. The best strategy is to implement security in layers, which would mean setting up a solution to filter email from the Internet, then combining that with another solution that filters messages on internal mail servers (with or without an SMTP relay), plus a solution for detecting viruses on file servers, plus a solution for detecting viruses on workstations.

Furthermore, signature files should be updated in that same order, because the vast majority of viruses (e.g.: W32/Klez, W32/Yaha, etc.) are propagated through e-mail servers. So to limit damage, e-mail servers should be the first to detect a new virus. Normally the file servers are infected from workstations. But since there is a good chance that stations will not be completely up to date, it's better to make sure that file servers are updated as promptly as possible.

Although workstations are last on the list, this does not mean that they are not important. Even though the vast majority of viruses will be filtered out before reaching a workstation, in many cases the workstation antivirus program will be the first line of defense. Particularly when it comes to filtering out certain malicious codes when users are on the Net.

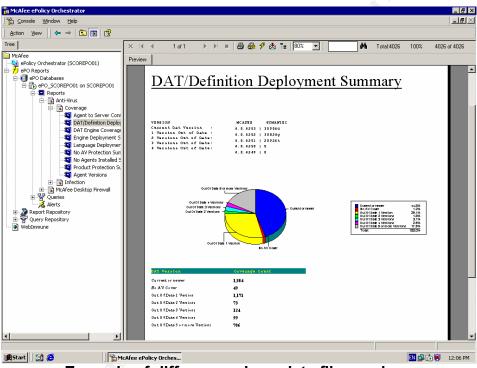
1.1.5.2 Monitoring

Despite this strategy and even assuming that all computer equipment in the system has the latest version of the filtering engine, the latest version of the signatures and almost every possible option for configuring the antivirus software

(often at the risk of reducing the performance of some systems), the entire computer system is still vulnerable to a new virus, because, by definition, the antivirus solution can only filter what it already knows.

Proactive monitoring

In fact we can, if the updating process is carried out properly, assume that the email and file servers will be up to date because they are normally always on. However, the same is not true of workstations. It is not unusual to have a difference of one or more versions of the signature file, even with a central management console like ePolicy Orchestrator.



Example of differences in update file versions

One must therefore, to decrease the risk of infection, make sure that the protection on all system equipment is as up to date as possible. This monitoring task can be carried out by generating reports from the ePO management console.

With these reports it is fairly easy to obtain the information that will minimize the risk of infection if there is an incident. It is possible, for example, to identify the following:

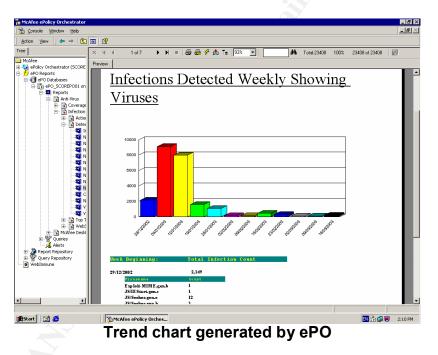
- systems that do not have the latest version of the filtering engine
- systems that do not have the latest version of the signature
- systems that do not have antivirus software, although the ePO agent is installed.

In addition to monitoring the network, it is essential to ensure that the signature file deployed by the ePO server is the latest version available from the Network Associates site.

Incident monitoring

Inevitably, and especially if the organization has a lot of computer equipment, certain systems will become infected. In some cases the antivirus solution will do its job and will filter out the virus; in others it will fail to do so. It must be possible to verify the effectiveness of the antivirus solution in order to react promptly when an incident occurs.

As well, there is nothing better than having a tool that shows the trends in infections, either for the systems as a whole, on a station-by-station basis, by user, or even by network segment.



In short, trend monitoring provides a general overview of the system status, allowing for a more effective response.

1.1.5.3 Response

Once the protection tool is deployed and adequate monitoring is in place, any problems detected can be corrected in the response phase.

As well, if a new virus appears with a high risk of propagation that will definitely infect certain systems, a quick response is essential.

The ePO management console asks the ePO agents distributed throughout the network to report in immediately. This is an excellent function for significantly reducing response time, compared to manual verifications.

1.1.6 Time-based security

This three-stage process ties in very well with the following concept of timebased security:

Monitoring time + Response time = Risk exposure time

In a situation where the protection is no longer effective (new virus), the more quickly monitoring can detect an incident, the shorter the response time. This in turn reduces the risk exposure time (i.e.: risk of infection).

1.2 Risks to the Audited System

Before moving on to identify the risks to a server such as ePolicy Orchestrator, the following are a few definitions that will help us understand risk better:

Risk formula

Risk = Threat X Vulnerability

Definition of a threat

A threat is a condition, situation or action that exploits a vulnerability, and can be related to a situation in which something unexpected happens, or even something expected that does not happen. Although the specific nature of the threat can have a direct impact on the probability that one or more corresponding vulnerabilities will be exploited, the threat will vary depending on the intentions of the attacker. A threat may be real, directly related to an existing vulnerability, or it may be virtual, in the sense that it is related to a theoretical vulnerability.

Definition of a vulnerability

A vulnerability is an exploitable breach in security or a technical problem that makes a threat possible. A vulnerability is expressed in terms of its probable exploitation. Exploiting a vulnerability may require extraordinary technical means, the collusion of several people, or costs that are higher than the possible gains or impact. On the other hand, special tools can be built to automate exploitation of the vulnerability, and these tools may be easily and widely available.

Risk classification

Risks and the elements that compose the risk are ranked as follows:

Threat level

The following criteria can be used to assess the seriousness of a threat:

Low	A low threat will have little impact on system operation and will not cause damage to systems or data that could lead to an incorrect result, treatment or decision.
Medium	A medium threat will cause damage to physical systems or data that will take time and money to repair. The organization's reputation and image could be hurt.
High	A high threat will cause a major direct or indirect financial loss to the organization or its customers and partners, damage the organization's reputation badly enough to hinder its ability to carry out is commercial activities in a given sector, or place the organization in a position of failure to comply with certain contractual obligations or even in a position of illegality.

Vulnerability to a threat

The probability that a threat will be acted upon can be ranked as follows:

Low	A vulnerability is considered low if there is little likelihood in the long term that it will be exploited because to do so would require extraordinary technical means, collusion among several people governed by a code of ethics or because the cost of exploiting the vulnerability would be much higher than the potential gains or impacts.
Medium	A vulnerability is considered medium if attacks capable of exploiting vulnerabilities of a similar nature have already been documented and occasionally reported by the industry, or if the technical requirements for a successful attack are major, but within reach of an organized group of attackers.
High	For all other cases, particularly if attacks capable of exploiting vulnerabilities of a similar nature have been reported with a significant frequency and/or specialized tools have been built to automate them, vulnerability is considered high.

Risk analysis chart

The risk based on the potential impact of a threat and the probability that it will be acted upon can be expressed in a four-point scale: **Insignificant, Minor, Major, Critical.**

This scale can be used to classify types of risk an organization faces, using the following risk analysis chart:

		Vulnerability			
		Low Medium High			
ıt	Low	Insignificant	Minor	Major	
hreat	Medium	Minor	Major	Critical	
Τ	High	Major	Critical	Critical	

Risk Level chart

The following chart interprets the assessed risk levels:

	Index	Assessment
1	Insignificant	In general, depending on the context, one can ignore insignificant risks.
2	Minor	The situation must be considered as a whole to make an informed judgement about minor risks.
3	Major	Major risks must be quickly addressed in accordance with an action plan.
4	Critical	Immediate action must be taken to respond to critical risks.

1.2.1 The main risks of ePolicy Orchestrator

The next step is to use the tools for assessing risk to identify the main risks and possible impacts that could be encountered by a central antivirus management server such as ePolicy Orchestrator.

The table below describes the main risks of using such a server, and uses the Risk Level chart to quantify the criticality of each possible impact.

Table of Main Risks and Possible Impacts

Main Risks	Possible Impacts	Risk Level	Comments on Risk Level
	Workstation or server will not be able to obtain a new configuration or update from the ePO server.	Minor	In the normal context of ePO server operations, this would have little impact.
Loss of availability of ePO service	If an incident (e.g. new virus) requires a response, it will not be possible to force an update or new configuration.	Critical	In the event of an incident, loss of availability would prevent an adequate response.
	No new protection (antivirus, personal firewall) can be deployed while the service is unavailable.	Minor	New stations or servers would not be protected during the loss of availability; the rest of the network would remain protected.
Loss of availability of the MSDE database.	No proactive monitoring will take place during the loss of availability.	Major	Monitoring will not be able to track incidents reported by ePO agents during the loss-of-availability period.
	No workstation or server will be able to get an updated signature file.	Minor	In the normal updating process, this would have little impact.
Loss of availability of the FTP service	It will not be possible to update deployments to new stations or servers.	Minor	If the ePO management console is available, one could deploy anyway. However, signature files cannot be updated until the FTP service is back online.
	If an incident occurs, it will not be possible to respond.	Major	When an incident requires a response, loss of availability will prevent an adequate response. However, if the management console is available, updates could be routed to another FTP server.
Incorrect configuration of FTP service	May permit unanticipated write access, for example to the antivirus solution update directory or directly to the FTP server root.	Critical	An attacker could provoke loss of integrity in update files.

Incorrect hardening or updating of operating system	Vulnerability can be exploited to take control of the ePO server.	Critical	The server and data integrity, authentications, availability and confidentiality can no longer be guaranteed.
Incorrect configuration of protection products (Virusscan, Netshield, etc.)	An incorrectly configured antivirus solution can inhibit efficient virus detection.	Critical Major	An incorrectly configured antivirus solution, even if it is always updated, cannot filter properly. This could lead to the infection of stations and servers. The antivirus software could delete an important file. As well, incorrect configuration could significantly reduce system performance, or even provoke denial of service.
Incorrect configuration of synchronization of signature files (.DAT) between the NAI and ePO servers	Could mean that the latest version of signature files will not be on the ePO server.		All stations and servers would be vulnerable to new viruses that cannot be detected by the signature file version.
Loss of access to the FTP servers at Network Associates (NAI).	The ePO server may not be able to get the most recent version of the signature files.		All stations and servers would be vulnerable to new viruses that cannot be detected by the signature file version.
Loss of integrity of the protection solutions deployed by the ePO server	Permits deployment of a protection product that could be infected by a virus or slightly altered by a Trojan horse or other malicious code.	Critical	The ePO server would be turned into a server that would deploy the virus to all machines in the network.
Loss of authentications governing access to the operating system	An attacker can take control of the ePO server, especially if the attacker has an account with administrative privileges.	Critical	The server and data integrity, authentications, availability and confidentiality can no longer be guaranteed.
	An attacker could access the MSDE database.	Major	An attacker could delete the database and prevent effective monitoring.
	An attacker could change the FTP service configurations	Major	An attacker could get broader access and do whatever he wanted with the FTP server.

	An attacker could render the server unavailable by interrupting certain services.	Major	In normal operation, this would not be too much of a problem. But if there was an incident, it could slow down response time, particularly if the attacker changed the passwords on all accounts with administrative privileges.
	Could make it possible to compromise the other server by retrieving authentification information on the ePO server (e.g.: in SAM).	Critical	If the same authentification works on the organization's other server (e.g.: service account for backups).
Loss of authentication	Could allow an attacker to take control of the ePO management console.	Critical	An attacker could change protection mechanisms at will. Loss of service could be provoked by rebooting all servers.
governing access to the ePO management console	Could allow an attacker to disable protection on individual machines.	Critical	An attacker could then infect a machine with a virus.
	Could allow an attacker to delete or alter all incident data gathered by ePO agents from workstations or servers.	Major	This would mean that monitoring would no longer have sufficient data integrity to detect incidents.
Loss of authentication governing access to data in the MSDE database.	Could give an attacker privileged access to a system via the "CmdExec" function	Critical	The server and data integrity, authentications, availability and confidentiality can no longer be guaranteed.
	Could allow an attacker to delete or alter all incident data gathered by ePO agents from workstations or servers.	Major	This would mean that monitoring would no longer have sufficient data integrity to detect incidents.

Could allow an attacker to render the database unavailable.	Major	An attacker could provoke a voluntary overload of the capacity supported by an MSDE database.
--	-------	---

1.2.2. Summary of main impacts

In general, the loss of availability of the ePO server and FTP service would have a critical impact only when an incident required an immediate response. Such loss could lead to the infection of a number of stations or servers, which could affect production and involve additional costs to disinfect infected machines.

Consequences could be more critical if the integrity of protection configurations is lost, because protection mechanisms would then be unable to perform their tasks adequately.

Loss of authentication of the ePO management console would be critical, because it would no longer be possible to ensure system availability, data integrity and unaltered configurations. Without these elements, the management console would become a powerful weapon for an attacker, because in addition to getting around protection mechanisms, an attacker could hinder proactive monitoring and also prevent an effective response.

1.3 Information available for security audit

1.3.1 Research on ePolicy Orchestrator

At the time this report was written, there was very little information on the vulnerabilities or other security problems of ePolicy Orchestrator.

Searches using the search engine Google (<u>www.google.com</u>) were relatively fruitless.

Searching on underground sites such as <u>www.astalavista.com</u> and <u>www.phrack.com</u> produced little.

In the SANS Institute (<u>http://www.sans.org/rr/</u>) Reading Room, there were only two pages on ePO:

- Issues with Keeping AntiVirus Software Up to Date, John Graham, July 25, 2001
- Distributed Scan Model for Enterprise-Wide Network Vulnerability Assessment, Alexander Lopyrev, November 27, 2001

Even the **KnowledgeBase** on the Network Associates (NAI) site does not contain any information on the vulnerabilities of ePolicy Orchestrator. The information posted focuses on the product's operating problems. Only one document (SrvPack1.txt) that comes with the Service Pack 1 (SP1) installation files identifies an obvious security problem.

That document is:

• Release Notes for McAfee ePolicy Orchestrator, Version 2.5.0 Management Software Service Pack 1

The following is an excerpt from that document:

PROBLEM:

It is possible to consult the following ePolicy Orchestrator files in a Web browser:

- EVTFILTR.INI
- NAIMSERV.LOG
- SERVER.INI
- SITEINFO.INI

SOLUTION:

It is no longer possible to consult these files in a Web browser. However, you can still use a browser to determine whether the ePolicy Orchestrator server is operational. [Translation]

A message posted on October 30, 2001 by "Blake Frantz" on the site Insecure.org (<u>http://lists.insecure.org/lists/pen-test/2001/Nov/0006.html</u>) gives an example of the content of the SERVER.INI file:

[Server] DataSource=**EPOAV** Database=**ePO_EPOAV** UserName=**sa** Password=**U3BVmVk4KHxsYFxaYFGRIVDxARHBoGCh8bGBcWBRkSFaQ8QERwaAA==** UseNTAccount=0 HTTPPort=80 AgentHttpPort=8081 ConsoleHTTPPort=8080 MaxHttpConnection=1000 EventLogFileSizeLimit=2097152 MaxSoftInstall=25

When the ePolicy Orchestrator Service Pack 1 is not installed on the server, a Web browser can be used to obtain the authentification parameters that allow access to the database.

One must first decode the password using a utility such as "NGSSQLCrack" which is available in an evaluation version at the following address: <u>http://www.nextgenss.com/software/ngssqlcrack.html</u>

Given that there is very little information about the security of ePolicy Orchestrator, the audit forms in the "**Assignment 2**" section were prepared to verify the majority of the security risks identified in the table in **Section 1.2.1** of this report.

1.3.2 Research into security audit methodologies

The audit forms described later in this document are based in part on information available at the following sites:

- The Information Systems Audit and Control, CobiT (Control Objectives for Information), <u>http://www.isaca.org/cobit.htm</u>
- Certified Students and Posted Practicals, SANS Institute, <u>http://www.giac.org/GSNA.php</u>
- Auditors Checklists and Other Audit Information, Fred Cohen & Associate, <u>http://www.all.net/books/audit/index.html</u>
- The Institute of Internal Auditors, ITAudit, http://www.theiia.org/itaudit/
- The Internet Tool for Auditors, by Jim Kaplan, http://www.auditnet.org
- Information technologies Code of practice for information security management, BS 7799/ISO 17799, First edition, 2000-12-01, <u>http://www.iso-17799.com/</u>

The risk level assessment explained in **Section 1.2** is based on a corporate inhouse methodology for audit forms used by the internal audit team.

The Montreal computer security firm "ESI Technologies" (http://www.esitechnologies.com) was involved in establishing the methodology.

Assignment 2: Creating a Security Audit Form

Test locationClearly identify the location where the test is to be conductedTests to be conductedInstructions for gathering the information required to assess the risk levelReference(s)The link to the web page for the tool used to conduct the audit and when possible the link to a specific reference on a topicExpected resultsList the ideal results that should be obtained in order to be fully compliantObjective / SubjectiveState whether the verification is objective or subjective. Where both apply, explain the nuanceResultsUncorrected test resultsBrief explanation of riskThe main risks one is trying to identify	Control objective	Describe the purpose of the audit
Tests to be conductedInstructions for gathering the information required to assess the risk levelReference(s)The link to the web page for the tool used to conduct the audit and when possible the link to a specific reference on a topicExpected resultsList the ideal results that should be obtained in order to be fully compliantObjective / SubjectiveState whether the verification is objective or subjective. Where both apply, explain the nuanceResultsUncorrected test resultsBrief explanation of riskThe main risks one is trying to identify	Test location	Clearly identify the location where the test is to be
Reference(s) The link to the web page for the tool used to conduct the audit and when possible the link to a specific reference on a topic Expected results List the ideal results that should be obtained in order to be fully compliant Objective / Subjective State whether the verification is objective or subjective. Where both apply, explain the nuance Results Uncorrected test results Brief explanation of risk The main risks one is trying to identify		conducted
Reference(s)The link to the web page for the tool used to conduct the audit and when possible the link to a specific reference on a topicExpected resultsList the ideal results that should be obtained in order to be fully compliantObjective / SubjectiveState whether the verification is objective or subjective. Where both apply, explain the nuanceResultsUncorrected test resultsBrief explanation of riskThe main risks one is trying to identify	Tests to be conducted	Instructions for gathering the information required
conduct the audit and when possible the link to a specific reference on a topicExpected resultsList the ideal results that should be obtained in order to be fully compliantObjective / SubjectiveState whether the verification is objective or subjective. Where both apply, explain the nuanceResultsUncorrected test resultsBrief explanation of riskThe main risks one is trying to identify		to assess the risk level
specific reference on a topic Expected results List the ideal results that should be obtained in order to be fully compliant Objective / Subjective State whether the verification is objective or subjective. Where both apply, explain the nuance Results Uncorrected test results Brief explanation of risk The main risks one is trying to identify	Reference(s)	The link to the web page for the tool used to
Expected resultsList the ideal results that should be obtained in order to be fully compliantObjective / SubjectiveState whether the verification is objective or subjective. Where both apply, explain the nuanceResultsUncorrected test resultsBrief explanation of riskThe main risks one is trying to identify		conduct the audit and when possible the link to a
order to be fully compliantObjective / SubjectiveState whether the verification is objective or subjective. Where both apply, explain the nuanceResultsUncorrected test resultsBrief explanation of riskThe main risks one is trying to identify		specific reference on a topic
Objective / SubjectiveState whether the verification is objective or subjective. Where both apply, explain the nuanceResultsUncorrected test resultsBrief explanation of riskThe main risks one is trying to identify	Expected results	List the ideal results that should be obtained in
subjective. Where both apply, explain the nuanceResultsUncorrected test resultsBrief explanation of riskThe main risks one is trying to identify		order to be fully compliant
ResultsUncorrected test resultsBrief explanation of riskThe main risks one is trying to identify	Objective / Subjective	State whether the verification is objective or
Brief explanation of risk The main risks one is trying to identify		subjective. Where both apply, explain the nuance
	Results	Uncorrected test results
	Brief explanation of risk	The main risks one is trying to identify
Risk evaluation Risk calculation for each result obtained	Risk evaluation	Risk calculation for each result obtained

2.1 Explanation of the form used

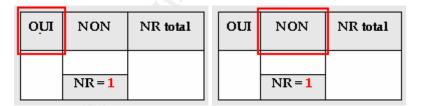
2.2 Explanation of the Risk Level calculation

A series of questions in the "Risk Evaluation" section of the audit form touches on the most sensitive areas of an ePO server.

Once all the questions have been answered, one can determine the server's risk level.

2.2.1 Organization of questions

The questions require a yes or no answer, as follows:



The answer that indicates compliance with security criteria is not marked "**RL** = ..." ("**RL**" = **Risk Level**)

The **"Total RL"** field must be filled in for each question. This gives the cumulative risk from all the answered questions.

The risk level value (e.g.: RL = 2) is based on the Risk Classification chart in Section 1.2, as follows 1 = Insignificant, 2 = Medium, 3 = Major and 4 = Critical.

2.2.2 Using the results chart

At the end of the audit form, a table summarizes the audit results in terms of the risk analysis:

	Total assessed risk	Ma∷imum ™.k	Percentage (%)
Operating system			90
security and open	?	48	?
session validation			
Product configurations	?	109	?
Access rights		92	?
Monitoring mechanisms	?	54	?
Total risk: for a maximum of 303 = %			

Results Summary Table

This table should be completed as follows:

- In the 1st column, enter the calculated risk levels for each of the four sections
- The 2nd column is already completed and contains the maximum possible risk for each of the 4 sections
- In the 3rd column, turn the number in the 1st column into a percentage of the maximum possible risk for each section (2nd column).
- In the grey area, calculate the total risk level (as a figure and as a percentage)

2.3 Form for an ePolicy Orchestrator Server Audit

2.3.1 Verifying operating system security and validating open sessions

[1] Control objective :	Verification of the installation type for the ePO server.
Test location :	From the auditor station
	\boxtimes From the server audited
Tests to be conducted :	Observe the following instructions:
	 Right button on the icon « My Computer » Choose « Properties » Choose the tab « Network Identification »

	4. Choose « Properties »
	 Be sure that « workgroup » is checked in the section « Member of ».
	Note : Take a screen capture of this window (alt- printscreen) and save the image in a wordpad document under the name « 1-type.rtf »
Reference(s) :	Not applicable / personal experience
Expected results :	The server should be in a « workgroup » in order to limit the use of authentification strictly to the local account with the administrator privileges.
Objective / Subjective :	Objective
Results :	- Insert results here -
Brief explanation of risk :	If the server is not installed in a « workgroup », a greater number of user will be permitted to connect onto the ePO server using a domain. This will increase the level of probability to a threat therefore increasing the level of risk.
Risk evaluation :	Is the server installed as a server member to a domain or as a domain controller?
	YES NO RL total
	RL=3
	TOTAL RISK LEVEL: []/ 6

[2] Control objective :	Verification of the basic vulnerabilities relative to the		
•	operating system.		
Test location :	From the auditor station		
	\boxtimes From the server audited		
Tests to be conducted :	Pre-required : Having downloaded from the ePO		
	server the latest available version of the Microsoft		
	Security Baseline Analyzer (MSBA) application.		
	Observe the following instructions:		
\odot			
	1. Open the application MBSA »		
	2. Choose « Scan a computer »		
	3. Be sure that the right server is chosen in the		
	section « Computer Name »		
	4. Be sure that all the options are selected, except		
	« Use SUS Server : »		
	5. Press on« Start Scan »		
	6. When finish, choose « Print » in the section		

	« Action ».
	 You can also paste the information in an application supporting the html format (ex : Word) and save under the name « 2-msba.doc ».
	Note Voon the MRSA application on the conver
	Note : Keep the MBSA application on the server audited permitting to the network administrator to use it after having done the corrections of certain
Reference(s) :	vulnerabilities (if needed). The MBSA tool is available at no charge at the
	following address:
	http://download.microsoft.com/download/e/5/7/e57f498 f-2468-4905-aa5f-369252f8b15c/mbsasandup.msi
Expected results :	There should be no critical event in each of the
	following categories:
	- Security Update Scan Results
	- Windows Scan Results
	 Additional System Information
	- Internet Information Services (IIS) Scan Results
	 SQL Server Scan Results Desktop Application Scan Results
Objective / Subjective :	Objective
Results :	- Insert results here -
Brief explanation of risk :	If the MBSA tool uncovers some vulnerabilities of critical level, it should normally be possible for an attacker to exploit those vulnerabilities to his advantage.
	An evaluation will however be necessary in order to validate the probabilities for each of the vulnerabilities to really be exploitable.
	Easier the vulnerabilities will be exploitable, greater the threat will be. Therefore the level of risk will be higher.
Risk evaluation :	Are some hotfix missing for the operating system ?
	YES NO RL total
	RL = 4

	Are som	e hotfix	c missing fo	or IIS ?
	YES	NO	RL total	
	RL = 4			
	Are com	o hotfi	, missing f	
	YES	NO		or SQL/MSDE ?
	163	NU	RL total	
	RL = 4			
				ical level been recorded in an Results » ?
	YES	NO	RL total	7
	RL = 4			
		ion « In		ical level been recorded in mation Services (IIS) Scan
	YES	NO	RL total	
	RL = 4			
		ion « S		ical level been recorded in Scan Results: Instance
A CONTRACTOR	YES	NO	RL total	
and the second sec	RL = 4			
				ical level been recorded in blication Scan Results » ?
	YES	NO	RL total	
	RL = 2			
	TOTAL	RISK L	EVEL: []/ 26

[3] Control objective :	Verification of security problems remotely identifiable.		
Test location :	From the auditor station		
	From the server audited		
Tests to be conducted :	 NOTE : In order to obtain the best result, this verification must be executed from the same segment where resides the server to audit in order to avoid being filtered by an equipment such as a router or firewall. Pre-required : Before conducting the audit, assure yourself that the Retina software is configured as per 		
	the following settings:		
	Policies		
	Policies - Complete Scan		
	Policies Complete Scan		
	Preferences Add Delete		
	Audits Eorce Scan (Perform scan on hosts that do not respond to pings)		
	Enable Connect Scan Mode		
	Common Hacking Attack Methods (CHAM)		
	FIP FOP3 SMTP HTTP		
	Common hacking attack methods are disabled in the evaluation version		
	Select a policy to edit from the drop down list. If you would like to create a new policy, select a policy to base the new one of off, then click on Add.		
	Note: The selected policy will be used for scheduled scans.		
	OK Cancel		
	~		
3	Afterward, observe the following instructions:		
e e e e e e e e e e e e e e e e e e e			
	1. Open the application « Retina »		
Ś	 Type the IP address of the server to audit in the section « Address : » 		
	3. Press on« Start »		
	4. When finished, choose the option « Report »		
	in the menu « Tools » and save the report		
\bigcirc	under the name « 3-Retina.html ».		
Reference(s) :	The Retina tool is available for evaluation (15 days) at		
	the following address :		
	http://www.eeye.com/html/Products/Retina /Download.html		
Expected results :	The Retina tool should not return any vulnerability of		
	« Medium Risk » level or « High Risk » level.		
Objective / Subjective :	Objective		
Results :	- Insert results here -		

Brief explanation of risk :	If the Retina tool discovers some vulnerabilities with a « high » risk level, it should normally be possible for an attacker to exploit those vulnerabilities to his advantage.
	In the case where the vulnerabilities are a « Medium » risk level, an evaluation will be necessary in order to validate the probabilities that each of the vulnerabilities are really exploitable or to validate the relevancy of the returned information.
	In a general manner, easier the vulnerabilities are exploitable, greater the threat will be. Therefore the risk level will be higher.
Risk evaluation :	Have some « High Risk » level vulnerabilities been found ?
	YES NO RL total
	RL = 4
	Have some « Medium Risk » level vulnerabilities been found ?
	YES NO RL total
	RL = 2
<u>×</u>	TOTAL RISK LEVEL: []/ 6

[4] Control objective :	Verification of suspicious services or not anticipated
	remote response.
Test location :	\boxtimes From the auditor station
	From the server audited
Tests to be conducted :	NOTE : In order to obtain the best result, this
Õ	verification must be executed from the same segment where resides the server to audit in order to avoid being scanned by an equipment, such as a router or firewall.
	Pre-required : Having downloaded and installed the latest version available of the SuperScan tool.

	Observe the following instructions:
	1. Open « SuperScan »
	2. In the section « Hostname Lookup » enter the
	IP address of the server to scan.
	3. Press on « Lookup » in order for the IP address
	to appear in « START » and « Stop » in the
	section « IP » 4. In the section « Scan type » choose :
	- Show host responses
	- All ports from [1] [65535]
	5. Press on « Start »
	6. When finish, save the results in the file
	« 4-superscan.txt »
Reference(s) :	The SuperScan tool is available at no charge at the
	following address :
	http://www.foundstone.com/knowthedge/scanning.html
	The Twenty Most Critical Internet Security Vulnerability
	Version 2.504, The SANS Institute, May 2, 2002,
	http://www.sans.org/top20/
Expected results :	A minimum of port should be open on the server.
	 Port required by the ePO product: 80 – Pre-required for the communications
	between the ePO agent and the ePO server
	- 81 – Pre-required to access the ePO console
	- 8081 – Pre-required by the ePO server for the
	« Weakup Call » to the ePO agent.
	I433 – Pre-required by MSDE
Ś	Port required by the ETD earlies
	Port required by the FTP server : - 21 – Pre-required for the transfer of updates
i contra	(.DAT, Engine Update, Hotfix, etc.)
	Port required for the remote control access (ex :
	Terminal Service):
\bigcirc	- 3389
	Port required by a saying software (ax : PaskupEyes)
	Port required by a saving software (ex : BackupExec). - (port to be determined as per the product
	used)
	No other ports need to be open, except the necessary
	ports open by the operating system for the use of the
	NETBIOS : 135 (tcp and udp), 137 (udp), 138 (udp),
	139 (tcp) and also 445 (tcp and udp).

Objective / Subjective :	Objective	
Results :	- Insert results here -	
Summary Brief explanation of risk :	The scanning of the open ports on an equipment permits an attacker to quickly identify the services that respond. The attacker's objective is to concentrate is attacks on the services more susceptible to permit him to succeed with is attack.	
	More services are open, greater the threat will be and there is more probabilities that vulnerabilities will be exploited. Therefore, the level of risk increases.	
Risk evaluation :	Are ports other than the ports anticipated open ?	
	YES NO RL total	
	RL = 3	
	If so, which ? :	
	0	
	Is the port 139 open ?	
	YES NO RL total	
	RL = 3	
	TOTAL RISK LEVEL: []/ 6	
Č.		

[5] Control objective :	Analysis of the sessions and the suspicious applications on the server.
Test location :	From the auditor station
	\boxtimes From the server audited
Tests to be conducted :	Pre-required : Having downloaded and installed on
O T	the audited ePO server, the latest version of Fport.
	Observe the following instructions:
	1. Open a command line (cmd.exe)
	2. Type the following line:
	netstat –an > 5-netstat.txt
	 Type the following line: <i>fport /p > 5-fport.txt</i>

Deference(a)	The Enert teel is evoluble at no oberge at the following
Reference(s) :	The Fport tool is available at no charge at the following address :
	http://www.foundstone.com/knowthedge/proddesc/fport
	<u>.html</u>
Expected results :	The results of netstat and of fport should not have
	recorded the presence of session or of suspicious
	application.
Objective / Subjective :	Objective
Results :	- Insert results here -
Summary Brief	Suspicious or unknowns sessions permit to identify the
explanation of risk :	applications that an attacker could use to his
	advantage (ex : a Trojan horse).
Risk evaluation :	Are sessions that seem suspicious or unnecessary
	applications present ?
	YES NO RL total
	RL = 4
	RL - 4
	If so, which ? :
	TOTAL RISK LEVEL: []/ 4
1	

TOTAL RISK LEVEL concerning the security of the
operating system and the open sessions? / 48

2.3.2 Settings verification for various products

[6] Control objective :	Verification of the update level for ePolicy Orchestrator.
Test location :	From the auditor station
	\boxtimes From the server audited
Tests to be conducted :	Pre-required : Having obtained by the system
\odot	administrator a user account and a valid password.
	Observe the following instructions:
	1. Open the « ePO » management console
	2. Choose « Login »
	3. Register a user account, a valid password and
	choose « OK »
	4. When the window « Initializing » disappears

	Take a screen capture and save it in a
	Wordpad document under the name « 6-verepo.rtf »
	· · · · · · · · · · · · · · · · · · ·
Reference(s) :	A search on «version numbers, determining,
	software » on the online help for the ePO management
	console.
	lefernation on the time of information leads.
	Information on the type of information leak :
	http://lists.insecure.org/lists/pen-
	test/2001/Nov/0006.html
Expected results :	The version 2.5.0 SP1 (2.5.1 Build 213) of ePolicy
	Orchestrator should be installed in order to correct
	certain important information leak, like a user code and
	a valid password, via port 80, 81 and 8081.
Objective / Subjective :	
Results :	- Insert results here -
Summary Brief	As it is possible to obtain privilege information
explanation of risk :	permitting authentification on the MSDE (or SQL)
	database if the last update of the product is not
	installed, this would permit an attacker to take remotely
	control of the database so far as port 1433 is not
	scanned, to execute the code of his choice with the
	« CmdExec » function in order to take full control of the
	server.
Risk evaluation :	Is the version of the ePO server installed the version
	2.5.1 Build 213 (or a more recent version) ?
	YES NO RL total
	<u>_</u>
	RL = 5
	TOTAL RISK LEVEL: []/ 5

[7] Control objective :	Verification of the active system services on the ePolicy Orchestrator server.
Test location :	From the auditor station From the server audited
Tests to be conducted :	Pre-required : Having downloaded and installed on the audited ePO serve, the latest version of DumpSec. Observe the following instructions:
	 Open « DumpSec » Choose « Select Computer » in the menu « Report » and enter the IP address of the

	1
	audited server. 3. Choose « Dump Services » in the menu
	« Report ».
	 Be sure that all the options are selected and press on« OK ».
	5. When the result is obtain, choose « Save
	Report As » of the menu « File » (or CRTL-
	S).
	6. Choose the type « Fixed width cols » and save
	under the name « 7-services.txt »
Reference(s):	The DumpSec tool is available at no charge at the following address :
	http://www.systemtools.com/somarsoft/
Expected results :	There should only be the required services for the
	efficiency of the active ePO server operations.
Objective / Subjective :	Objective, except for the application identification
	which is not necessary.
Results :	- Insert results here - 🤊
Summary Brief	The least active service on the server, fewer probability
explanation of risk :	for an attacker to exploit a vulnerability to his advantage.
Risk evaluation :	Are suspicious or unnecessary services used ?
	YES NO RL total
	RL = 4
	If so, which ?:
l X	
<u>S</u>	TOTAL RISK LEVEL: []/ 4

[8] Control objective :	Verification for presence of a functional antivirus on the
P	ePO server.
Test location :	From the auditor station
	\boxtimes From the server audited
Tests to be conducted :	Observe the following instructions:
	In order to know the version of the signature (.DAT) and the version for scanning engine :
	 Right button on the icon « NetShield » in the task bar.

	2. Choose « Abort »
	 Take a screen capture and save in a Wordpad document under the name « 8-antivirus.rtf »
	In order to know the exact version of NetShield :
	 Open « regedit » Find the following key : HKEY_LOCAL_MACHINE\SOFTWARE\Network Associates\TVD\NetShield NT\CurrentVersion\szProductVer Make a note of NetShield version. version : Observe the following instructions on the audited server in order to validate if the settings on the update have adequately been actived :
	 Right button on the icon« NetShield » in the task bar. Choose « Console » Click on « Automatic DAT Update » Take a screen capture of the « Update Options » tab and save at the end of file « 8-antivirus.rtf »
	Observe the following instructions on the audited server in order to validate if the ePO agent is installed :
SIN	 Choose « Internet Explorer » Type the following line in « Address » : http://localhost:8081 Take a screen capture and save at the end of file « 8-antivirus.rtf » Go to the end of the obtained document, Take a
	screen capture and save at the end of file « 8- antivirus.rtf »
Reference(s) :	Information in order to know the exact version of NetShield : Solution nai25980 - NetShield Version Information, dated September 10 th , 2002.
	Requires an access to « PrimeSupport KnowledgeCenter Service Portal » at the following address : <u>https://mysupport.nai.com</u>
Expected results :	Concerning the version for the installed product and the version of the signature (.DAT) :

	1
	 The version of NetShield installed should be : 4.5.0.468.1 (or more recent) The version Of « Scan Engine » should be : 4.1.60 (or more recent) The version of the signature (.DAT) should be the latest available at the following address : http://www.mcafeeb2b.com/naicommon/downlo ad/dats/find.asp
	Concerning the settings for the update of the product :
	 The option « Get from an FTP source » should be selected The IP address or the name of the audited FTP server (under the format FQDN) should be inscribed in the zone « Enter an FTP computer name and directory » The option « Use anonymous FTP login » should be selected.
	Concerning the information returned by Internet explored at the command « http://localhost:8081 » :
S MAS	 The version of the ePO agent installed should be : 2.5.1.213 (or more recent) The three following lines should come back periodically (according to the agent configuration on the management) in the « logs » of the ePO agent : 20030112115447: Agent: Enforcing policy for NANDSHLD_4500 20030112115447: Agent: Enforcing policy for PCR 1.0.0 for Windows 20030112115448: Agent: Enforcing policy for NAI ePolicy Orchestrator Agent
Objective / Subjective :	Objective
Results :	- Insert results here -
Summary Brief explanation of risk :	Having an antivirus solution that is not adequately up to date is more vulnerable to infection than an antivirus rigorously updated.
	An antivirus solution must therefore be present on an antivirus server such as ePO in order to be sure that it does not become a centralized distribution virus console.

Risk evaluation :	Is the version of NetShield installed at least the version 4.5.0.468.1 ?
	YES NO RL total
	RL = 4
	Is the version of « Scan Engine » installed at least the version 4.1.60 ?
	YES NO RL total
	RL = 4
	Is the version of the signature (.DAT) the latest version available the day of the audit ?
	YES NO RL total
	RL = 4
	Is the option « Get from an FTP source » selected ?
	YES NO RL total
2	RL = 3
115	If not, what is the configuration ? :
S. A.	
	Is the IP address or the name of the FTP server audited (under a format FQDN) inscribed in the zone « Enter an FTP computer name and directory » ?
	YES NO RL total
	RL = 3

	If not, what is the configuration ? :
	Is the option « Use anonymous FTP login » selected ?
	YES NO RL total
	RL = 3
	If not, what is the account used ? :
	Is the version of the ePO agent installed at least the
	version 2.5.1.213 ?
	YES NO RL total
	RL = 3
	If not, what is the version ? :
	Do the three following lines some periodicular in the
	Do the three following lines come periodiquely in the « logs » of the ePO agent?
2	20030112115447: Agent: Enforcing policy for
	NANDSHLD_4500 20030112115447: Agent: Enforcing policy for PCR 1.0.0 for
	Windows 20030112115448: Agent: Enforcing policy for NAI ePolicy
	Orchestrator Agent
	YES NO RL total
	RL = 4
	If not, what are the results obtained :
	TOTAL RISK LEVEL: [] / 28

[9] Control objective :	Verification of the basic settings for Internet Information Server (IIS)
Test location :	From the auditor station
	From the server audited
Tests to be conducted :	Observe the following instructions:
	1. Open « Internet Service Manager » via Start –
	Programs – Administrative Tools.
	 Right button on « Default FTP Site » Choose « Properties »
	4. Take a screen capture of each tabs (FTP Site ,
	Security Accounts, Messages, Home
	Directory and Directory Security) and save it
	in a Wordpad file under the name « 9-ftp.rtf »
Reference(s) :	Not applicable / Personal experience
Expected results :	Concerning the configuration of IIS :
	In the tab « FTP Site »
	- The connexion number should be limited to the
	 station/server number needing an update. The option « Enable Logging » should be
	selected
	In the tab « Security Accounts » :
	- The option « Allow Anonymous Connections »
	should be selected and also check mark for
	« Allow only anonymous connections ».
	 Only the group « Administrators » should be visible in the section " Operators »
	visible In the section« Operators ».
	In the tab « Messages » :
	- A legal message should be inscribed in the
	section« Welcome »
C Y	In the tab « Home Directory » :
6	- The option « a directory located in this
	 computer » should be selected The directory « Ftproot » should not be found on
	the same driver as the operating system.
	- Only the option « Read » and « Log visits »
	should be selected.
	In the tab « Directory Security » :
	- The option « Denied Access » should be
	selected.

	A list of the ID address that have the right to				
	 A list of the IP address that have the right to access the FTP server should be written. 				
Objective / Subjective :	Objective				
Objective / Subjective : Results :	- Insert results here -				
Summary Brief	A configuration mistake on the FTP server could permit				
explanation of risk :	an attacker to use to his advantage this weakness in				
	order to corrupt the files of the update and at the same				
	time to upload some applications to the server				
	potentially permitting him, if combine with an other				
Diak avaluation :	attack, to take control of the server.				
Risk evaluation :					
	requirering an update ?				
	YES NO RL total				
	RL = 2				
	Ko				
	Is the option « Enable Logging » selected ?				
	YES NO RL total				
	RL = 3				
	Is the option « Allow Anonymous Connections »				
	selected and also the option « Allow only anonymous				
	connections » ?				
	YES NO RL total				
	RL = 2				
S.					
	Is only the group « Administrators » present in the				
	section« Operators » ?				
S Y	YES NO RL total				
\bigcirc					
	RL = 4				

	ls a «Welc	legal come » ?	message	inscribed	in the	e section
	YES	NO	RL total			
		RL = 2				
	ls the selecte	-	a directo	ry located	in this c	omputer »
	YES	NO	RL total			
		RL = 2				
		-	« Ftproot : ng system	»located or ?	the sam	ie driver
	YES	NO	RL total			
	RL = 3	3				
	ls only ?	the opti	on « Read	» and « Lo	og visits	» selected
	YES	NO	RL total			
•		RL = 2				
S.	Is the o	option «	Denied Ac	cess » sele	cted?	
S	YES	NO	RL total			
		RL = 3				
\bigcirc			the IP ac server ex	ldress that ist? 〕	have th	e right to
	YES	NO	RL total			
		RL = 3				
	ΤΟΤΑΙ	RISK L	EVEL: [] / 26		

[9] Control objective :	Verification of the ePO agent settings				
Test location :	From the auditor station				
	From the server audited				
Tests to be conducted :	Pre-required : Having obtained from the system administrator a user account and a valid password.				
	Observe the following instructions:				
	 Open the « ePO » management console Choose « Login » 				
	3. Register a user account, a valid password and				
	Choose « OK » 4. Once the window « Initializing » disappears,				
	Choose « Directory » 5. Choose « ePO Orchestrator Agent »				
	6. Take a screen capture and save in a Wordpad				
	document under the name « 9-ePOAgent.rtf » 7. Double click on« ePO Orchestrator Agent » and				
	choose « Configuration ».				
	8. Take a screen capture of the tab « Agents				
	Options » also « Event Options » and save at the end of file « 9-ePOAgent.rtf ».				
Reference(s):	Not applicable / Personal experience				
Expected results :	The option « Enforce Policies for ePolicy				
	Orchestrator Agent » must be selected.				
	In the tab « Agent Options » :				
	The option « Prompt user when software installation requires reboot » should be ideally selected.				
	The option « Enable Agent to server communication » must be selected with a reasonnable delay (ex : 60 minutes by defaut).				
Õ	The option « Enable agent Wakeup call support » must be selected.				
	In the tab « Event Options » :				
	A reasonable delay (depending on the size of the company) can be entered in the zone « Interval between immediate upload ». Ideally, shorter the delay will be, faster the alerts will be corrected.				

Objective / Subjective :	Objective					
Results :	- Insert results here -					
Summary Brief	A bad configuration of the ePO agent could render it a					
explanation of risk :	little or completely inefficient and even prevent any					
	reaction if a major incident would arise.					
Risk evaluation :	Is the option « Enforce Policies for ePolicy					
	Orcnes	Orchestrator Agent » selected ?				
	YES	NO	RL total	A		
		RL = 4				
		KL - 4				
		-	-	ser when software installation		
	requires	s reboot	: » selected	2		
	YES	NO	RL total			
				Ý		
		RL = 2				
		KL - 2				
			<u> </u>			
	Is the			hable Agent to server		
				ed with a reasonable delay		
	(ex : 60 minutes by default) ?					
	YES	NO	RL total			
		RL = 4				
	If not, what is the delay ? :					
×	Is the option « Enable agent Wakeup call support »					
	selected ?					
	YES	NO	RL total			
	X 0 RL = 4					
	Is a reasonable delay (depending on the company					
	size) entered in the zone « Interval between immediate					
	upload » ?					
			DI tatal			
	YES	NO	RL total			
		RL = 2				
				J		

	If not, what is the delay ? :
	TOTAL RISK LEVEL: [] / 16
[10] Control objective :	Verification of the process for the update of the ePO server
Test location :	From the auditor station
Tests to be conducted :	The ePO server does not have an integrated mechanism in order to update the files of the signature (.DAT).
	The system administrator may have to choose different kind of way in order to carry out this task. Therefore you must ask the administrator what is the process he uses for the update and adapt this section accordingly.
	In the present case, the system administrator as chosen to automate this task using a combination of « Scheduled Tasks » and command files (.BAT) in order to make the FTP transferts between the FTP servers of the Network Associate and the server audited.
	Observe the following instructions:
	Take some screen captures of all the pertinent mechanisms in the process for the update and save it in a Wordpad file under the name « 10-update.rtf »
	In the present case :
Reference(s) :	 A screen capture of the « Scheduled Tasks » A screen capture of the command files Not applicable / Personal experience
Expected results :	The process for the update must be entirely automated.
	Journals (« logs ») must be available in order to validate that the process works well.
Objective / Subjective	The structure on the audited FTP server must be as faithful as possible to the FTP server of NAI.
Objective / Subjective :	Subjective - Insert results here -
Results :	
Summary Brief	In order to assure an efficient update of the antivirus,

explanation of risk :	the antivirus server must be rigorously updated. If the process does not permit an efficient update, the infection probabilities will be higher.					
Risk evaluation :	infection probabilities will be higher. Is the update process entirely automated ?					
	YES NO RL total					
	RL = 4					
	If not, explain the process :					
	Are the journals (« logs ») available in order to validate					
	the process is working correctly ?					
	YES NO RL total					
	RL = 3					
	Is the structure on the audited FTP server faithful or close to the FTP server of NAI?					
	YES NO RL total					
	RL = 3					
S. S. S.	If not, explain what file is available for the undate :					
	If not, explain what file is available for the update :					
5						
C V						
Õ	TOTAL RISK LEVEL: [] / 10					

[11] Control objective :	Verification of the settings for NetShield 4.5 deployed by the ePO management console.
Test location :	From the auditor station From the server audited
Tests to be conducted :	Pre-required : Having obtained from the system administrator a user account and a valid password.

	Observe the following instructions:
	 Open the « ePO » management console Choose « Login » Register a users account, a valid password and Choose « OK » Once the window « Initializing » disappears, choose « NetShield v4.5 for Windows » Take a screen capture and save in a Wordpad file under the name « 11-NetShield.rtf ». Choose « On Acces Scan » Take a screen capture of each of the tabs available (« Detection », « advanced », « action », « report » and « exclusion ») and save at the end of file « 11-NetShield.rtf ».
Reference(s) :	Not applicable / Personal experience
Expected results :	In « Installation Options » :
	The option « Enforce Policies for NetShield v4.5 » must be selected. The option « Force Install NetShield v4.5 » must be selected and an installation package must be selected.
	In the tab « Detection » :
	At least the following options must be selected :
	 Scan « Inbound File » Scan « Network Drive » Selected file type only Enable on acces scanning at system startup
	The remaining options can be selected, but an impact on the system performance as to be evaluated.
	In the tab « Advance » :
	All should be selected, however for performance reason the options in the zone « Compressed File » can be deactivated.
	In the tab « Action » :
	Only « Clean infected file automatically » is necessary.

	In the tab « Report » and « Exclusion » :				
	Nothing as to be activated and no exclusion should be defined.				
Objective / Subjective :	Objective				
Results :	- Insert results here -				
Summary Brief	A configuration mistake in the settings deployed by the				
explanation of risk :	management console increases the infection probabilities on the total system of the servers in the information system.				
Risk evaluation :	Is the option « Enforce Policies for NetShield v4.5 » selected ?				
	YES NO RL total				
	RL = 4				
	Is the option « Force Install NetShield v4.5 » selected				
	and is an installation package selected ?				
	YES NO RL total				
	RL = 4				
	Are at least the following options selected in the tab « Detection » ?				
	- Scan « Inbound File »				
	- Scan « Network Drive »				
	- Selected file type only				
	 Enable on acces scanning at system startup 				
	YES NO RL total				
	RL = 4				
	If not, which are missing ? :				

	Are all t	he opt	ions selec	ted in the	tab « Advance » ?
	(do not c	onside	er the zone	« Compre	ssed File »).
	YES	NO	RL total		
	R	RL = 3			
]	
	lf not, wh	nich are	e missing ?	?:	
					0
		· · · · · · · · · · · · ·		S.	
			Clean in tab « Actic		e automatically »
	YES	NO	RL total		
	R	RL = 3			
	lf not, wh	nat is th	ne default a	action ? :	
	8	21			
	Have e « Exclusi			en define	d in the tat
22	YES	NO	RL total		
A.	RL = 2				
C.T.	lf so, exp	lain th	e exclusio	ns :	
O Î					
	TOTAL F	RISK L	EVEL: [1 / 20	

TOTAL RISK LEVEL Concerning the configurations of various products ?

? / 109

3.3.3 Access rights verification

[12] Control objective :	Verification of the users account available on the ePO
	server.
Test location :	From the auditor station
	From the server audited
Tests to be conducted :	Pre-required : Having downloaded and installed on
	the audited ePO server, the latest version of DumpSec.
	Observe the following instructions:
	1. Open « DumpSec »
	2. Choose « Select Computer » in the menu
	« Report » and enter the IP address of the
	audited server.
	3. Choose « Dump Users as columm » in the
	menu « Report ».
	4. Add all the fields available and Press on« OK ».
	5. Once the result is obtained, choose « Save
	Report As » of the menu « File » (or CRTL-
	S).
	6. Choose the type « Fixed width cols » and save
	under the name « 12-users.txt »
Reference(s) :	The DumpSec tool is available at no charge at the
	following address :
Exported requite :	<u>http://www.systemtools.com/somarsoft/</u> - The account « Guest » should be deactivated
Expected results :	and renamed for something less explicit.
	The account « administrator » should be
	renamed for something less explicit.
	- The default account for IIS
	« IUSR_computername » should be renamed
	for something less explicit.
	- A service account for the ePO server should be
	present.
	- A service account for the saving software (ex :
	BackupExec) can be present.
	- A service account for a remote access software
	(ex : Terminal Service) can be present.
Objective / Subjective :	Objective
Results :	- Insert results here -
Summary Brief	The less accounts exist with administrative rights and
explanation of risk :	significative names (ex: administrator), smaller the
	probabilities for an attacker to guess the names of the
	accounts present. This is particularly thru where the
	NETBIOS protocol is not used (or if special measures

	have been done).			
	may re	etrieve the	e available	at probability that an attacker accounts list and their rights.
Risk evaluation :	Is the	account	« Guest »	deactivated ?
	YES	NO	RL total	
		RL = 4		KS.
	ls the explici		« Guest »	renamed for something less
	YES	NO	RL total	Stall.
		RL = 2		
	ls th somet		unt « adı explicit ?	ministrator » renamed for
	YES	NO	RL total	
		RL = 2		
				« IUSR_computername » as ning less explicit ?
2	YES	NO	RL total	
		RL = 2		
		ervice acc		ne ePO software present ?
es.	YES	NO	RL total	
		RL = 3		

	a service ckupExec) p		r the sa	aving	software	(ex :
YE	S NO	RL total				
	RL = 2	-				
	a service <u>mi</u> nal Servi			emote	access	(ex :
YE	S NO	RL total				
	RL = 2	_				
то	TAL RISK I	EVEL:] / 17			

[13] Control objective :	Verification of the user groups available on the ePO server.		
Test location :	From the auditor station		
	\boxtimes From the server audited		
Tests to be conducted :	Pre-required : Having downloaded and installed on the audited ePO server, the latest version of DumpSec.		
	Observe the following instructions:		
	1. Open « DumpSec »		
	2. Choose « Select Computer » in the menu		
	« Report » and enter the IP address of the		
3	audited server.		
C C C C C C C C C C C C C C C C C C C	3. Choose « Dump Groups as columm » in the		
	menu « Report ».		
	4. Add all available fields and press on « OK ».		
	5. Once the result is obtained, choose « Save		
	Report As » of the menu « File »		
S Y	(or CRTL-S).		
©	 Choose the type « Fixed width cols » and save under the name « 13-groups.txt » 		
Reference(s) :	The DumpSec tool is available at no charge at the		
	following address :		
	http://www.systemtools.com/somarsoft/		
Expected results :	- The account « administrator » should not be		
	found in the group « administrators ».		
	- The service account for the saving software		
	should be only in the group		
	« Backup_Operators ».		

	- The account « Guest » should not be found in			
	the group « Guest ».			
	- Only the service account required by IIS can be			
	found in the group « Guest ».			
	- No user should be found in the groups « Power			
	Users », « Replicator » and « Users ».			
Objective / Subjective :	Objective			
Results :	- Insert results here -			
Summary Brief	Well managed groups permit only the appropriate			
explanation of risk :	accounts an access to the good things. More			
	misplaced accounts will mean a greater probability for an attacker to use one of those accounts to his			
	advantage.			
Risk evaluation :	Is the account « administrator » (If not renamed)			
	found in the group « administrators » ?			
	YES NO RL total			
	RL = 3			
	Is the service account for the saving software found			
	only in the group « Backup_Operators » ?			
	YES NO RL total			
	RL = 2			
· · · · · · · · · · · · · · · · · · ·	If not, where is it located ? :			
S				
Ś				
	Is the account « Guest » found in the group « Guest »			
	?			
	YES NO RL total			
\bigcirc				
	RL = 2			

Is only the service account required by IIS found in the group « Guest »?			
YES	NO	RL total	
	X RL = 2	9	
			one of the following groups : icator » and « Users » ?
YES	NO	RL total	20
RL = 2	2		
lf so, e	xplain :		
ΤΟΤΑΙ	L RISK L	EVEL: [] / 11

[14] Control objective :	Verification of the complexity of the password for the accounts present on the ePO server.
Test location :	From the auditor station
	\bowtie From the server audited
Tests to be conducted :	Pre-required : 1. Having downloaded and installed on the audited
	 ePO server, the Pwdump3 tool. 2. Having downloaded and installed on the audited station the tool LC3 (or more recent).
	Note : Also, you must know the password of an account with « administrator » rights.
Ő	Part 1 : From the server audited Observe the following instructions:
	 Open a command line (cmd.exe) Type the following line: pwdump3 addressIP_du_server 14-pwdump.txt

[Dert 2 . From the auditor station
	Part 2 : From the auditor station
	Note : Before starting the verification of the complexity of the passwords, assure yourself that the LC3 software is configured according to the following settings :
	Default Settings For Future Auditing Sessions
	Dictionary Crack Image: Enabled Word file: Files\@stake\LC3\words-english-big Browse The Dictionary Crack tests for passwords that are the same as the words listed in the word file. This test is very fast and finds the weakest passwords.
	Dictionary/Brute Hybrid Crack ✓ Enabled 3 ✓ Characters to vary (more is slower) The Dictionary/Brute Hybrid Crack tests for passwords that are variations of the words in the word file. It finds passwords such as "Dana99" or "monkeys!". This test is fast and finds weak passwords.
	Brute Force Attack Image: Enabled Character Set: [A + Z, 0 + 9 and !@#\$%^%*()_++=^**]]0[\:;!"\>,.?/ Custom Character Set (list each character): ETNRIDASDHLCFPUMYGWV8XKQJZ
	The Brute Force Crack tests for passwords that are made up of the characters specified in the Character Set. It finds passwords such as "WeR3plf6s" or "VC5%69+12b". This test is slow and finds medium to strong passwords. Specify a character set with more characters to crack stronger passwords.
	<u> </u>
	And observe the following instructions: 1. Recover the file « 14-pwdump.txt » from the
	 audited server by the way of your choice. 2. Open the application « LC3 » (or more recent) 3. Choose « File - New Session » 4. Choose « Import »
S.	 Choose « Import from a PWDUMP File » Choose the file « 14-pwdump.txt » Press on « F4 » (or choose the icon « Begin
	 Audit »). 8. Press on the icon « Minimize LC3 to the system tray » and let it run until you obtain the passwords or upto a maximum of 12 hours.
	 Once the passwords are obtained or after the delay has expired, export the results in the file« 14-lc3.txt ».
Reference(s) :	The LC3 tool is available as an evaluation version at the following address : http://www.atstake.com/research/lc/download.html

	The Pwdump3 tool is available at the following		
	address :		
	http://www.polivec.com/pwdumpdownload.html		
Expected results :	Concerning the result for LC3 :		
	No password must have been found after a minimum of 12 hours of « brute force ».		
	Concerning the general rule for passwords :		
	All passwords should be composed of : - At least 8 characters		
	 At least one small letter, one capital letter, one number and one special character (ex : !?%*/#) 		
	The service accounts should be composed of 14 characters and should include at least 2 characters of each categories.		
Objective / Subjective :	Objective 💦		
Results :	- Insert results here -		
Summary Brief	Without a robust authentification (including a small		
explanation of risk :	letter, a capital letter a number and a special		
	character) the probabilities for an attacker to take		
	control of the server is higher.		
Risk evaluation :	Have passwords been found after a maximum of 12 hours of « brute force » ?		
	YES NO RL total		
	RL = 4		
45	Are passwords for accounts with administrative rights robust and conform ?		
A Contraction	YES NO RL total		
ST.	RL = 4		
	Are passwords for service accounts composed of 14 characters ?		
	YES NO RL total		
	RL = 3		
	TOTAL RISK LEVEL: []/ 11		

[15] Control objective :	Verification that access rights have been put on certain important directories.
Test location :	From the auditor station
	From the server audited
Tests to be conducted :	Observe the following instructions in order to verify the
	access rights to the directory « MSFTPSVC1 » :
	1. Conduct a search on drive « C » for
	« MSFTPSVC1 » using « Start » - « Search » –
	« For File and Folders » (or touch windows + f)
	2. Right button on « MSFTPSVC1 »
	-
	3. Choose « Properties »
	4. Choose the tab « Security »
	5. Click on « Administrator », Take a screen
	capture and save in a Wordpad file under the
	name « 15-msftpsvc1.rtf »
	6. Use the same procedure for each accounts
	present and save at the end in the same file.
	Observe the following instructions in order to verify the
	access rights to the directory « Ftproot » :
	1. Conduct a secret on all the drives for
	1. Conduct a search on all the drives for
	« Ftproot » using « Start » - « Search » – « For
	File and Folders » (or touch windows + f)
	2. Right button on « Ftproot »
	3. Choose « Properties »
	4. Choose the tab « Security »
÷	5. Click on « Internet Guest Account », Take a
	screen capture and save in a Wordpad file
	under the name « 15-ftproot.rtf »
	6. Use the same procedure for each accounts
	present and save at the end in the same file.
Reference(s) :	Not applicable / Personal experience
Expected results :	Concerning the rights on the directory
	« MSFTPSVC1 » :
	- Only the groups « Administrators » and
	« System » should have the authorization « Full
	Control »
	- The rest of the groups (if existing) should have
	only the authorization « Read »
	- The group « Everyone » should not be present

	Concerning the rights on the directory « Ftproot » :		
	 Only the group « Administrators » should have the authorization « Full Control » The rest of the groups (if existing) should have only the authorization « Read » The group « Everyone » should not be present 		
Objective / Subjective :	Objective		
Results :	- Insert results here -		
Summary Brief explanation of risk :	Larger the access are on the important directories, greater the probabilities for an attacker to modify the data present on those directories with a minimum of effort are big.		
Risk evaluation :	Do only the groups « Administrators » and « System » have an authorization « Full Control » on the directory « MSFTPSVC1 » ?		
	YES NO RL total		
	RL = 3		
	If not, which ? :		
	0.0		
Do the rest of the groups (if existing) have authorization « Read » on the « MSFTPSVC1 » ?			
	YES NO RL total		
- S	RL = 3		
C T	If not, which ? :		

	Does the group « Everyone » have rights on the directory « MSFTPSVC1 » ?				
	YES NO RL total				
	RL = 3				
	Does only the group « Administrators » have a authorization « Full Control » on the director « Ftproot » ?				
	YES NO RL total				
	RL = 3				
	If not, which ? :				
	Do the rest of the groups (if existing) have only an authorization « Read » on the directory « Ftproot » ?				
	YES NO RL total				
	RL = 3				
	If not, which ? :				
ST					
STR	Does the group « Everyone » have rights on the directory « Ftproot » ?				
O	YES NO RL total				
	RL = 3				
	TOTAL RISK LEVEL: []/ 18				

[16] Control objective :	Verification of the password for an account « SA » for
	the MSDE database
Test location :	From the auditor station
	From the server audited
Tests to be conducted :	Observe the following instructions in order to validate if
	the account « SA » has a password :
	1. Conduct a search on all the drives for
	« cfgnaims.exe » using « Start » - « Search » –
	« For File and Folders » (or touch windows + f)
	2. Double click on the file « cfgnaims.exe »
	3. Take a screen capture of each of the tabs and
	save in a Wordpad file under the name « 16-
	sapw.rtf »
	4. Open a command line (cmd.exe)
	 Type the following line: osql –U sa
	6. The following line should be :
	Password :
	7. Press « ENTER » in order to enter no password.
	8. Take a screen capture and paste it at the end of
	file « 16-sapw.rft »
	Note the same a personner is entered (i.e. the result of
	Note : In case a password is entered (i.e. : the result of osql –U sa is not 1>), ask for the password from the
	system administrator.
Reference(s):	HOW TO: Verify and Change the System Administrator
	Password by Using MSDE – KB 322336:
	http://support.microsoft.com/default.aspx?scid=kb;en-
l l l l l l l l l l l l l l l l l l l	us;Q322336#2
Expected results :	The result of the command « osql –U sa » should be :
	Lesia Failed for year leal
	Login Failed for user 'sa'.
	If MSDE is configured to use only «Windows
	Authentification », the result should be :
<u> </u>	
	Login failed for user 'sa'. Reason: Not associated
	with a trusted SQL Server connection.
	Since it is rarely changed, it should be composed of
	14 characters and should include at least 2 characters of each categories (small letter, capital letter, number
	and special character)
	The password « SA » should be different from the

	password :				
	- Permitting authentification to the server				
	- Permitting authentification to the « ePO »				
	management console.				
Objective / Subjective :	Objective : except for validation of the password				
	format given by the administrator (if present).				
Results :	- Insert results here -				
Summary Brief	Without a robust authentification (including small letter,				
explanation of risk :	capital letter, number and special character) the				
	probabilities for an attacker to take control of the				
	MSDE database are higher.				
	Therefore, the probabilities for an attacker to take				
	complete control of the ePO server are higher.				
Risk evaluation :	Does the account « SA » have a password ?				
	YES NO RL total				
	RL = 4				
	Is the password for the account « SA » composed of				
	14 characters ?				
	YES NO RL total				
	RL = 2				
	Is the password different from the one for				
A	authentification to the server (i.e. : Windows)?				
6					
	YES NO RL total				
	RL = 3				
GY .	In the measured different from the				
<u> </u>	Is the password different from the one for				
	authentification to an ePO console ?				
	YES NO RL total				
	RL = 4				
	TOTAL RISK LEVEL: []/ 12				

[47] Control objective					
[17] Control objective :	Verification of access rights on certain important files of ePolicy Orchestrator.				
Test location :	From the auditor station				
	\boxtimes From the server audited				
Tests to be conducted :	Observe the following instructions:				
	 Conduct a search on all the drives for « DB » using « Start » - « Search » – « For File and Folders » (or touch windows + f) Right button on the file « DB » found in the directory « \ePO\2.0 » Choose « Properties » Choose the tab « Security » Take a screen capture for each of the accounts present and save it in a Wordpad file under the name « 17-dbepo.rtf » 				
Reference(s) :	Not applicable / Personal experience				
Expected results :	Only the group « administrators » should have access in « Full Control » to the file « DB ».				
	Note : The group « Backup Operators » could also be present (if required by the saving software).				
Objective / Subjective :	Objective				
Results :	- Insert results here -				
Summary Brief explanation of risk :	Larger the access will be on the important directories, greater are the probabilities for an attacker to modify the data present on those directories with a minimum of effort are big.				
Risk evaluation :	Does only the group « administrators » have an access « Full Control » to the file « DB ?				
L. L.	YES NO RL total				
	RL = 4				
	If not, which ? :				
	TOTAL RISK LEVEL: [] / 4				

[18] Control objective :	Verification of authentification accounts for the ePolicy		
	Orchestrator management console		
Test location :	From the auditor station		
	From the server audited		
Tests to be conducted :	Pre-required : Having obtained from the system administrator a user account and a valid password in order to authentify yourself on the management console.		
	Observe the following instructions:		
	 Open the « ePO » management console Choose « Login » Register a users account, a valid password and choose « OK » Choose « Manage Administrator », Take a screen capture and save in a Wordpad file under the name « 18-epopw.rtf » If an other account exist other than the default account (admin) with the role « administrator » or « Site Administrator », Choose this account and Press on « Configure ». Take a screen capture and save at the end of file « 18-epopw.rtf » Use the same procedure for each of the 		
	accounts with administrative rights.		
Reference(s):	Not applicable / Personal experience		
Expected results :	There should be an access code created according to the number of administrator needing access to the ePO management console.		
	The default account « ADMIN » must be deleted or renamed.		
0	All passwords should be composed of at least 8 characters (and include small letter, capital letter, number and special character).		
	Also they should be different from the password permitting authentification on the server or from the one for account « SA » of the database.		
Objective / Subjective :	Objective, except for validation of the password « ADMIN » given by the system administrator.		
Results :	- Insert results here -		

Summary Brief	Without a robust authentification (including small letter,		
explanation of risk :	capital letter, number and special character) the probabilities for an attacker to take control of the ePO		
	management console is higher.		
Risk evaluation :	Have access codes been created according to the		
	number of administrators needing to access the ePO		
	management console ?		
	YES NO RL total		
	RL = 3		
	Is the default account « ADMIN » deleted or renamed ?		
	YES NO RL total		
	RL = 4		
	Are all the passwords composed of at least 8 characters and robust ?		
	YES NO RL total		
	RL = 4		
Ž	Are the passwords differents from the one for authentification to the server (i.e. : Windows)?		
C TR	YES NO RL total		
	RL = 4		
O	Are the passwords different from the one for the account « SA » ?		
	YES NO RL total		
	RL = 4		
	TOTAL RISK LEVEL: []/ 19		

2.3.4 Verification of the supervising mechanism

[19] Control objective :	Verification for the presence of an audit mechanism for the operating system.
Test location :	From the auditor station
Tests to be conducted :	 Observe the following instructions in order to verify the settings of « system », « security » and « application » : Right button on the icon « My Computer » Choose « Manage » Double click « Event Viewer » Right button on the icon « Application » and choose « Properties » Take a screen capture and save in a Wordpad document under the name « 19-events.rtf » Follow the same procedure for « Security » and also for « System ». Observe the following instructions from the server audited in order to verify the settings for « Audit Policy » : Choose « Local Security Policy » in the « Administrative Tools » Choose « Audit Policy »
Reference(s) :	Securing Windows 2000 Step-by-Step, SANS Institute, page 21 and 22
Expected results :	 Concerning the settings for « System », « Security » and for « Application » : The option « Do not overwrite events (clear log manually) » should be ideally selected only if a validation and purging task is done every day. The amount (in KB) inscribed in the zone « Maximum log size : » should be suffisant in order to not permit an easy service deny.

	Concerning the settings for « Audit Policy » :				
	- For each points, « Success » and also				
	« Failure » should be activated. (« Audit				
	process tracking » can not be selected)				
Objective / Subjective :	Objective				
Results :	- Insert results here -				
Summary Brief	Without a sufficient monitoring, there is no way to				
explanation of risk :	identify anomalies caused either by a malfunction of an application or by an attack targeted by an attacker.				
	Better the monitoring, greater the probabilities to limit the damage.				
Risk evaluation :	In the settings for « Application » :				
	Is the option « Do not overwrite events (clear log manually) » selected ?				
	YES NO RL total				
	RL = 2				
	Is the amount (in KB) indicated in the zone « Maximum log size : » sufficient in order to not permit an easy service deny, if « clear log manually » is or was activated ?				
	YES NO RL total				
•					
A CONTRACT OF	RL = 4				
	If not, what is the value ? :				
ST	In the settings of « Security » :				
\odot	Is the option « Do not overwrite events (clear log				
	manually) » selected ?				
	YES NO RL total				
	RL = 3				

				cated in the zone « Maximum
				order to not permit an easy
			if « clear	log manually » is or was
	activa]	1
	YES	NO	RL total	
	x	RL = 4	9	
		KL - 4		. 6 ,•
	lf not,	what is tl	he value ?	
	In the	settings	for « Syste	m » :
		option « ally) » sel		rwrite events (clear log
	YES	NO	RL total	
		RL = 2		
]
	log si	ze:» su e deny,	fficient in	cated in the zone « Maximum order to not permit an easy log manually » is or was
	YES	NO	RL total	
		RL = 4		
STR	lf not,	what is tl	he value ?	:
ST				Policy », are each points for, « Failure » activated ?
	YES	NO	RL total	
		RL = 3		
	lf not,	which are	e not ? :]
		· · · · · · · · · ·		
	ΤΟΤΑ	L RISK L	EVEL: [] / 22

[20] Control objective :	Verification of the general process for the verification of		
Test leastion :	the ePO management console.		
Test location :	From the auditor station		
Tests to be conducted :	From the server audited Pre-required : Having obtenained from the system		
Tests to be conducted :	administrator a user account and a valid password to		
	access the ePO management console and the database MBSA (or MS-SQL accordingly)		
	Observe the following instructions to obtain a preview of the last events on the ePO server :		
	 Open the « ePO » management console Choose « Login » 		
	 Register a user account, a valid password and choose « OK » 		
	 4. Once the window « Initializing » disappears, choose with the right button of the mouse 		
	« Directory »		
	5. Choose « Server Events »		
	6. Take a screen capture and save in a Wordpad document under the name « 20-srvevent.rtf »		
	Observe the following instructions in order to generate the quantity of report necessary for the monitoring :		
	1. Open the « ePO » management console, double click on « ePO Reports »		
	2. Double click on « ePO Databases »		
•	3. Double click on the audited server name		
	4. Click « OK » in the window « ePO Database		
19 A.P.	5. Double click on « Reports »		
	6. Double click on « Anti-virus »		
C Y	7. Double click on « Coverage »		
	8. Double click on « DAT/Definition Deployment Summary » and press on « OK »		
	 Deployement Summary » and press on « OK » 9. Choose « No » in the window « Customize 		
	Report »		
	10. Choose the icon « Export »		
	11. Choose the format of your choice (ex : HTML		
	3.0 Draft Standard) and press on« OK »		
	12. Choose the place or save the report (leaving the		
	default name) and choose « OK »		
	13.Do the same task for :		

	 DAT Engine Coverage NO AV Protection Summary
	 Product Protection Summary Agent Version
Reference(s):	Agent Version Not applicable / Personal experience
Expected results :	In the « Server Events » :
	 There should be nothing suspicious or any errors recorded (watch out for events in yellow).
	In the report « DAT/Definition Deployment Summary » :
	 A large majority of the working stations or of the servers should have the latest version of the file signature (.DAT). There should not be any version of the signature older than the one before the latest version available (« Out of date version »).
	In the report « DAT Engine Coverage » :
	 There should be only a few (or none) « Out of date Engine »
	In the report « NO AV Protection Summary » :
	- There should not have any stations or servers without the antivirus solution.
l l	In the report « Product Protection Summary » :
ST	 There should not be any product considered unknown.
	 There should not be many version of NetShield or of VirusScan.
	 No other antivirus solution should be present without a valid reason.
	In the report « Agent Version » :
	 There should not be many version of the ePO agent ePO installed.
Objective / Subjective :	Objective
Results :	- Insert results here -

Summary Brief explanation of risk : Risk evaluation :	Better installed is the monitoring of the prevention elements, easier it will be to identify the anomalies (up to date version, station without antivirus, etc.) and to react accordingly. Therefore, the probabilities of incident will be reduced. Have suspicious events or mistakes been recorded in the « Server Events » ?	
	YES NO RL total	
	RL = 4	
	If so, explain the principals :	
	Does the large majority of the working stations or the servers have the latest version of the file signature (.DAT)?	
	YES NO RL total	
	RL = 4	
	Have some versions of signature older than the one before the latest version been identified ?	
Č.	YES NO RL total	
-Star	RL = 4	
	If so, explain :	
	Have little (or none) version not updated for the engine (« Out of date Engine ») been identified ?	
	YES NO RL total	
	RL = 4	

	-			
	lf not, ex	plain :		
	Have st antivirus			s been identified without an
	YES	NO	RL total	
	RL = 4			10.00
	lf so, exp	olain :		A CO
			· · · · · · · · · · · · · · · · · · ·	
				8
		oducts	considered	unknown been identified ?
	YES	NO	RL total	
	RL = 4			
	lf so, exp	olain :		
		3		
3	Have m	any ve d?	ersion of N	letShield or VirusScan been
	YES	NO	RL total	
5	RL = 4			
STA	lf so, exp	olain :	<u></u>	
\bigcirc				
			virus soluti dentified ?	ion (present without a valid
	YES	NO	RL total	
	RL = 4			

	If so, explain :
	TOTAL RISK LEVEL: [] / 32

TOTAL RISK LEVEL Concerning the monitoring	
mechanism	

? / 54

Assignment 3: Audit Evidence

3.1 Conducting a Security Audit

3.3.1 Verifying operating system security and validating open sessions

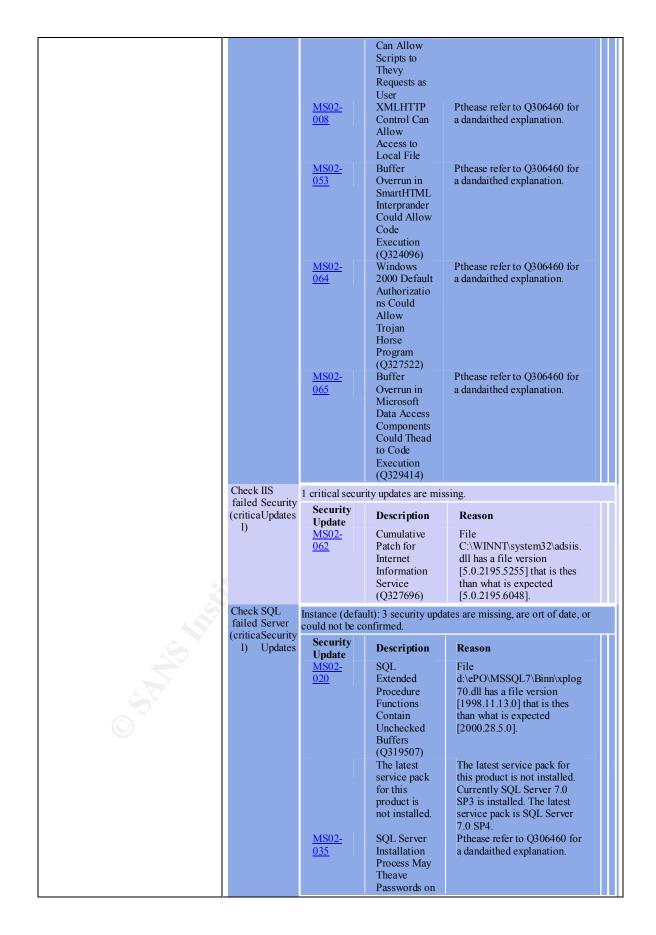
[1] Control objective :	Verification of the installation type for the ePO server.
Test location :	From the auditor station
Tests to be conducted :	Observe the following instructions:
	 Right button on the icon « My Computer » Choose « Properties » Choose the tab « Network Identification » Choose « Properties » Be sure that « workgroup » is checked in the section « Member of ».
	Note : Take a screen capture of this window (alt- printscreen) and save the image in a wordpad document under the name « 1-type.rtf »
Reference(s):	Not applicable / personal experience
Expected results :	The server should be in a « workgroup » in order to limit the use of authentification strictly to the local account with the administrator privileges.
Objective / Subjective :	Objective
Results :	File content « 1-type.rft » :
SALSTR	Identification Changes ? × You can change the name and the membership of this computer. Changes may affect access to network resources. Computer name: scorepo01 Full computer name: scorepo01.
	Member of Domain: Workgroup: EPO OK Cancel

Brief explanation of risk :	If the server is not installed in a «workgroup», a greater number of user will be permitted to connect onto the ePO server using a domain. This will increase the level of probability to a threat therefore increasing the level of risk.					
Risk evaluation :	Is the server installed as a server member to a domain					
	or as a domain controller?					
	YES	NO	RL total	<u>c</u> .•		
	RL=3	x	0	i Sha		
TOTAL RISK LEVEL: [0]/ 6						

[2] Control objective :	Verification of the basic vulnerabilities relative to the			
	operating system.			
Test location :	From the auditor station			
	\boxtimes From the server audited			
Tests to be conducted :	Pre-required : Having downloaded from the ePO server the latest available version of the Microsoft			
	Security Baseline Analyzer (MSBA) application.			
	Observe the following instructions:			
	1. Open the application« MBSA »			
	2. Choose « Scan a computer »			
	3. Be sure that the right server is chosen in the			
	section « Computer Name »			
	4. Be sure that all the options are selected, except			
2	« Use SUS Server : »			
6	5. Press on« Start Scan »			
191 A. 191				
6	 When finish, choose « Print » in the section « Action ». 			
	7. You can also paste the information in an			
	application supporting the html format (ex :			
C V	Word) and save under the name « 2 -			
	msba.doc ».			
	mspa.doc ».			
	Note: Keep the MBSA application on the server			
	audited permitting to the network administrator to use it			
	after having done the corrections of certain			
	vulnerabilities (if needed).			
Reference(s) :	The MBSA tool is available at no charge at the			
	following address:			
	http://download.microsoft.com/download/e/5/7/e57f498			
	<u>mtp.//download.microsoft.com/download/c/J///CJ/1490</u>			

	f-2468-4905-aa5f-369252f8b15c/mbsasandup.msi							
Expected results :	There should be no critical event in each of the following categories:							
	 Security Update Scan Results Windows Scan Results Additional System Information Internet Information Services (IIS) Scan Results SQL Server Scan Results 							
Objective / Subjective :	- Desktop Application Scan Results Objective							
Results :	File content « 2-msba.doc » :							
	Computer name: IP address:		Epo\Scorepo01 172.25.1.134					
	Security repor	t name:	Epo - Scorepo0	1 (01-15-2003 11-35 AM)				
	Scan date:		15/01/2003 11:3	35 AM				
	Security Updat version:	te database	1.0.1.449					
	Security assessment:		Incompthande Scan (Could not compthande one or more reques checks.)					
	Security Update	es						
	Score Issue	Result						
		17 security upo confirmed.	dates are missing,	are ort of date, or could not be				
	(criticaSecurity	Security						
	l) Updates	Update	Description Flaw in	Reason File				
		<u>MS02-</u> 042	Network	C:\WINNT\system32\nandma				
			Connection Manager	n.dll has a file version [5.0.2195.2779] that is thes				
			Could	than what is expected				
			Enable Privilege	[5.0.2195.5974].				
	2		Andhevation (Q326886)					
		<u>MS02-</u>	Unchecked	File				
S.V.		<u>045</u> 	Buffer in Network	C:\WINNT\system32\xactsrv. dll has a file version				
			Share Provider can	[5.0.2134.1] that is thes than what is expected				
			thead to	[5.0.2195.5971].				
			Denial of Service					
			(Q326830) Flaw in	The registry key				
		<u>048</u>	Certificate	**SOFTWARE\Microsoft\Int				
			ERLollment Control	ernet Explorer\ActiveX Compatibility\{43F8F289-				
			Could Allow	7A20-11D0-8F06-				
			Dandhandio n of Digital	00C04FC295E1}** does not exist. It is Pre-required for				
			Certificates (Q323172)	this patch to be considered installed.				
		<u>MS02-</u>	Certificate	File				
		<u>050</u>	Validation Flaw Could	C:\WINNT\system32\adsldp. dll has a file version				
			Enable	[5.0.2195.4959] that is thes				

		Identity	than what is expected
		Spoofing	[5.0.2195.5781].
	1000	(Q329115)	F'1
	<u>MS02-</u> 051	Cryptograph ic Flaw in	File C:\WINNT\system32\drivers\
	<u>051</u>	RDP	rdpwd.sys has a file version
		Protocol can	[5.0.2195.4307] that is thes
		Thead to	than what is expected
		Information	[5.0.2195.5880].
		Disclosure	
	MS02	(Q324380)	File C:\WINNT\hh.exe has a
	<u>MS02-</u> 055	Unchecked Buffer in	file version [4.74.8793.0] that
	<u>055</u>	Windows	is thes than what is expected
		Help Facility	[5.2.3644.0].
		Could	
		Enable Code	
		Execution	
	MS02-	(Q323255) Unchecked	File
	063	Buffer in	C:\WINNT\system32\drivers\
		PPTP	raspptp.sys has a file version
		Impthement	[5.0.2160.1] that is thes than
		ation Could	what is expected
		Enable Denial of	[5.0.2195.6076].
		Service	
		Attacks	
		(Q329834)	
	<u>MS02-</u>	Cumulative	File
	<u>068</u>	Patch for	C:\WINNT\system32\shdocv
		Internet	w.dll has a file version
		Explorer (324929)	[5.50.4916.1800] that is thes than what is expected
		(321)2))	[5.50.4923.500].
	<u>MS02-</u>	Flaw in	File
	<u>069</u>	Microsoft	C:\WINNT\system32\msjava.
		VM Could	dll has a file version
		Enable System	[5.0.3805.0] that is thes than what is expected [5.0.3809.0].
		Compromise	what is expected [5.0.5809.0].
		(810030)	
	<u>MS02-</u>	Flaw in	File
	<u>070</u>	SMB	C:\WINNT\system32\localspl
		Signing	.dll has a file version
		Could	[5.0.2195.2793] that is thes than what is expected
		Enable Grorp Policy	[5.0.2195.6090].
		to be	[5.0.2175.0070].
Č Ž		Modified	
		(309376)	
	<u>MS02-</u>	Flaw in	File
	<u>071</u>	Windows	C:\WINNT\system32\basesrv.
G Y		WM_TIME R Message	dll has a file version [5.0.2195.2581] that is thes
		Handling	than what is expected
		Could	[5.0.2195.5265].
		Enable	
		Privilege	
		Andhevation	
		(328310) The latest	The latest service near for
		service pack	The latest service pack for this product is not installed.
		for this	Currently SP2 is installed.
		product is	The latest service pack is SP3.
		not installed.	
	<u>MS01-</u>	WebDAV	Pthease refer to Q306460 for
	<u>022</u>	Service	a dandaithed explanation.
		Provider	



		Syster					
	Check Windo	(Q263	968)				
	passed ws Media Discussion No critical security updates are missing.						
	Player Security	critical security upd	ates are missing.				
	Updates Check Exchan						
	not ge	change Server is not	in stalls d				
	med Security	change server is not	instaneu.				
	Updates			K.			
	Windows Scan Res Vulnerabilities	ul ts					
	Score Issue	Result					
	Check Restrict failed Anonymou (criticals)	Computer is runnin prevents basic enun system information maximum security.	neration of user a	accounts, accou	int policies, and		
	Check Password failed Expiration	Some unspecified upasswords.	ser accounts (5 c	of 6) have no-ex	xpiring		
	(no- critical)	User Administrator Backupexec_svr Guest SQLAgentCmdE TsInternetUser IUSR_SCOREP(
	Check Local passed Account	Some user accounts could not be analyzed		ank or simpthe	passwords, or		
	Password Test	User	Weak Password	Locked Ort	Disabt hed		
		Guest	Weak	-	Disabt		
		Administrator	-	-	hed -		
		Backupexec_s vr		-			
•,		IUSR_SCOR EPO01	-	-	-		
8	2	SQLAgentCm dExec	-	-	-		
		TsInternetUse r	-	-	-		
	Check File passed System	All hard drives (3) a Drive Thandter C: D: E:	F N N	FS file system. ile System TFS TFS TFS			
	Check Autologon	E: Autologon is not co					
e	passed Check Guest	Ū	0	•			
	passed Account Check Administra	The Guest account No more than 2 Adr			computer		
	passed tors	User Administrator Backupexec_svr					
	Additional System	n Information					
	Score Issue R	esult					
	Best Auditin practice g	Logon Success and L	ogon Failure au	diting are both	Enabled.		

	Best Service	Some pot	entially unn	ecessary sei	rvices are installed.
	practice s	Servic	e ublishing Se		State Running Stopped
	Additiona Shares	4 share(s) are present	on Your co	omputer.
	l informati	Shar	Direc tory	Share ACL	Directory ACL
	on	AD MIN \$	C:\W INNT	Admi n Share	Users - RX, Power Users - RWXD, Administrators - F, NT AUTHORITY\SYSTEM - F, Everyone - RX
		C\$	C:\	Admi n Share	Everyone - F
		D\$	D:\	Admi n Share	Everyone - F
		E\$	E:\	Admi n	Everyone - F
	Additiona Windo			Share	
	l ws	Compute	r is running	Windows 2	000 or greater
	informati Version on	Compute	r is running	w muows 20	000 or greater.
	Internet Informat	ion Servi	ces (IIS) Sca	n Results	
	Vulnerabilities				
	Score Is	sue		Result	
	Unabthe to scan Sa		plications		reading the IIS mandabase.
	Unabthe to scan II	S Admin V	Virtual Direc		reading the IIS mandabase.
	Unabthe to scan Pa	arent Paths	5		reading the IIS mandabase.
	Unabthe to scan M	Isadc and S irectories	Scripts Virtu	al Error	reading the IIS mandabase.
	Check failed II (critical)		wn Tool		IS Lockdown tool has not been run e machine.
	Additional Syste	m Inform	ation		
9	Score Issue		Result		
Ś	practice Test	1 Controlle	r IIS is not	running on	a domain controller.
	Best IIS Log practice Enabled		Some we		tes are not using the recommended
A Contraction of the second se			Name Defaul	t FTP Site	Protocol FTP
e St	SQL Server Scan	Results: 1	nstance (de	faul t)	
	Vulnerabilities				
	Score Issue Check CmdEx	Res	sult		
	failed rothe (critical)		ndExec is no	ot restricted	to sysadmin.
	Check Folder failed Author (critical) ns	izatio sa	nd properly.		Server installation folders are not
	()		Instance (default)	Folder d:\ePO\l n	User MSSQL7\Bin \Everyone
			(default)		MSSQL7\Dat \Everyone

		Service - Accounts	SQL Server and/or SQL Server Agent Services accounts are members of the local Administrators grorp or run as LocalSystem.				
			Insta nce (defau lt) (defau lt)	Service MSSQLSe rver SQLServe rAgent	Accou nt SYST EM SYST EM	Issue LocalSystem account. LocalSystem account.	
	failed (no	Sysadmin - rothe members				of sysadmin rothe.	
	Check	SQL Server - Security		authentication Mixed Mode).	mode is sand	to SQL Server and	
	Check passed	Sysadmins				othe are present.	
	Check passed	-	The 'sa' pass exposed in File Nan	ext file.	service acco	unt password are not	
			C:\WINN og	VT\TEMP\sqlsp VT\sqlstp.log	o.l No pa expos	usswords eed usswords	
	-	Account Password Test	No SQL use	er accounts have	e weak passw	vords.	
	Check passed	Domain Controller Test	SQL Server	is not running	on a domain	controller.	
	Check passed	Registry Authorizatio			ot have more	e than Read access to	
	1	ns	the SQL Se	rver registry ke	ys.		
	Check	ns Guest				of the databases.	
	Check passed	ns Guest Account	The Guest a			of the databases.	
	Check passed Desktop A Vulneral Score	ns Guest Account Application Sc bilities e Issue	The Guest a an Results			of the databases.	
	Check passed Desktop A Vulneral Score	ns Guest Account Application Sc bilities e Issue ailed IE Zone	The Guest a an Results	account is not E	nabled in any	cure settings for some	
	Check passed Desktop A Vulneral Score Check fa	ns Guest Account Application Sc bilities e Issue ailed IE Zone	The Guest a an Results Result Internet E	account is not E	nabled in any	cure settings for some	
	Check passed Desktop A Vulneral Score Check fa	ns Guest Account Application Sc bilities e Issue ailed IE Zone	The Guest a an Results Result Internet E users. SCORE \Admin	xplorer zones d Zon EPO01 Loc istrato intr	nabled in any o not have se ne Le ^v el	Recomme nded Level 5 Medium-	
	Check passed Desktop A Vulneral Score Check fa	ns Guest Account Application Sc bilities e Issue ailed IE Zone	The Guest a an Results Result Internet E users. User SCORE \Admin r SCORE \Admin	xplorer zones d Zon EPO01 Loo istrato intr nd EPO01 Tru	nabled in any o not have se ne le cal Cus ana ton sted Cus	Recomme nded Level Medium- 1 Low	
	Check passed Desktop A Vulneral Score Check fa	ns Guest Account Application Sc bilities e Issue ailed IE Zone	The Guest a an Results Result Internet E users. User SCORE \Admin r SCORI	xplorer zones d Xplorer zones d Zon 2PO01 Loc istrato intr istrato site 2PO01 Inte 2PO01 Inte	nabled in any o not have se ne le cal Cus ana ton sted Cus	Recomme nded Level Medium- Low Low Medium- Low Medium	
	Check passed Desktop A Vulneral Score Check fa	ns Guest Account Application Sc bilities e Issue ailed IE Zone	The Guest a an Results Result Internet E users. User SCORI \Admin r SCORI	xplorer zones d xplorer zones d 201 201 201 201 201 201 201 201	nabled in any o not have se ne Lee el cal Cus sted Cus sted Cus stric Cus ton stric Cus	Recomme nded Level Medium- Low Low Low Medium	
	Check passed Desktop A Vulneral Score Check fa	ns Guest Account Spplication Sc bilities e Issue ailed IE Zone ical)	The Guest a an Results Result Internet E users. SCORI \Admin r S SCORI \Admin R SCORI R S SCORI R S	xplorer zones d xplorer zones d 201 2001 Loci 101 102 102 103 103 103 103 103 103 103 103	nabled in any o not have se ne el cal Cus rana ton sted Cus s ton stric Cus ton stric Cus ton	Recomme nded Level Medium- Low Medium Medium High	
Share the	Check passed Desktop A Vulneral Scorr Check fa (no-criti	ns Guest Account Application Sc bilities e Issue ailed IE Zone ical)	The Guest a an Results Result Internet E users. SCORF \Admin r R R R R R R R R R R R R R R R R R R	xplorer zones d xplorer zones d Zon EPO01 Loo istrato intr istrato site EPO01 Inte istrato t EPO01 Res istrato ted site	nabled in any o not have se ne Lee el cal Cus sa Cus ss ton stric Cus stric Cus s ton stric Cus ton stric Cus ton	Recomme nded Level Medium- Low Low Low Medium High High	
Brief explanation of risk :	Check passed Desktop A Vulneral Scorr Check fa (no-criti	ns Guest Account Account bilities e Issue ailed IE Zone ical) not Macro ned Security not Ortlook ned Zones MBSA	The Guest a an Results Result Internet E users. User SCORF \Admin r R R R R R R R R R R R R R R R R R R	xplorer zones d xplorer zones d Zon 2PO01 Loc istrato intr nd 2PO01 Tru istrato site 2PO01 Inte istrato t 2PO01 Res istrato t 2PO01 Res istrato site 3 con 3 con	nabled in any o not have se ne Lee el cal Cus sa Cus ss ton stric Cus stric Cus ton stric Cus ton stric Cus ton stric Cus ton stric Cus ton stric Cus ton stric Cus ton	Recomme nded Level Medium- Low Low Low Medium High High	

	advantag	ge.			
		the pro	babilities ⁻	ver be necessary in order to for each of the vulnerabilities	
				will be exploitable, greater the ne level of risk will be higher.	
Risk evaluation :				or the operating system?	
	YES	NO	RL total	3	
	X RL = 4		4		
			to the second		
	Are som	e hotfix	missing fo	pr IIS ?	
	YES	NO	RL total		
	X RL = 4		8		
	Are som	े e hotfix	missing fo	or SQL/MSDE ?	
	YES	NO	RL total		
10%	X RL = 4		12		
5				ical level been recorded in an Results » ?	
SY.	YES	NO	RL total		
\bigcirc	X RL = 4		16		
	Have vulnerabilities of critical level been recorded i the section « Internet Information Services (IIS) Sca Results » ?				
	YES	NO	RL total		

X RL = 4		20	
	on « S		ical level been recorded in Scan Results: Instance
YES	NO	RL total	
X RL = 4		24	
			ical level been recorded in plication Scan Results »?
YES	NO	RL total	
RL = 2	X	24	
TOTAL F	RISK L	.EVEL: [2	24]/ 26

[3] Control objective :	Verification of security problems remotely identifiable.
Test location :	From the auditor station
	From the server audited
Tests to be conducted :	NOTE : In order to obtain the best result, this verification must be executed from the same segment where resides the server to audit in order to avoid being filtered by an equipment such as a router or firewall.
STR	Pre-required : Before conducting the audit, assure yourself that the Retina software is configured as per the following settings:
O P	

	Policies					
	Policies - Complete Scan					
	😡 Policies	Complete Scan				
	🧔 Ports	Preferences <u>A</u> dd <u>Delete</u>				
	🤤 Audits	Eorce Scan (Perform scan on hosts that do not respond to pings)				
		Enable Connect Scan Mode				
		Common Hacking Attack Methods (CHAM)				
		▼ FIP				
		Common hacking attack methods are disabled in the evaluation version				
		Select a policy to edit from the drop down list. If you would like to create a new policy, select a policy to base the new one of off, then click on Add.				
		Note: The selected policy will be used for scheduled scans.				
		OK Cancel				
	Afterward, ob	serve the following instructions:				
	1 Open t	he application« Retina »				
	•	The IP address of the server to audit in the				
		« Address : »				
	3. Press	on« Start »				
	4. When	finished, choose the option « Report »				
	in the r	nenu « Tools » and save the report				
	under	the name « 3-Retina.html ».				
Reference(s) :		ol is available for evaluation (15 days) at				
	the following a					
		ve.com/html/Products/Retina				
	/Download.ht					
Expected results :		ol should not return any vulnerability of sk wild be should not return any vulnerability of sk wild be should be sho				
Objective / Subjective :	Objective					
Results :	Important extr	ract of the file « 3-Retina.html » :				
ST		performed a vulnerability assessment of 1 system[s] in order ecurity posture of those systems and to ortline fixes for any				
	The systems audited	were: 172.025.001.134				
	Retina's goals in this	attack were as follows:				
	Your scan	0				
		f those systems and services and perform information techniques.				
		exploit any known hothe in the server software and examine bod of being vulnerabthe to those attacks.				
		information on how to fix all found vulnerabilities.				

Create security report for Your organization
Create security report for Your organization.
Your network had 5 low risk vulnerabilities, 8 medium risk vulnerabilities, and 1 high risk vulnerabilities . There were 1 host[s] that were vulnerabthe to high risk vulnerabilities and 1 host[s] that were vulnerabthe to medium risk vulnerabilities. Also on average each system on Your network was vulnerabthe to 1,00 high risk vulnerabilities, 8,00 medium risk vulnerabilities and 5,00 low risk vulnerabilities.
The overall security of the systems under review was deemed rather insecure. Your organizations network is compthandely vulnerabthe. It is imperative that You take immediate actions in fixing the security stance of Your organizations network.
NETBIOS: Null Session
Risk Level: High Description: A Null Session occurs when an attacker sends a blank username and blank password to try to connect to the IPC\$ (Inter Process Communication) pipe. By creating a Null session to IPC\$ an attacker is then abthe to gain a list of user names, shares, etc Note: If You have run this Retina scan with Administrator level access to Your network then You will always be abthe to create a null session and therefore this is a false positive and not a vulnerability.
How To Fix: Add the following registry key:
HKEY_LOCAL_MACHINE\System\CurrentControlSand\Control\LSA Name: RestrictAnonymous Type: REG_DWORD Value: 1. CVE: CVE-2000-1200
BugtraqID: <u>494</u>
Accounts: Administrator - Password Does Not Expire
Risk Level: Medium Description: If a users password does not expire You allow a remote attacker endthes amornt of time to try to figure ort Your users password. It is recommended that You make all users passwords expire unthes the user account is used for a system service. How To Fix:
Remove the password never expires option from the user account. 1. Open User Manager.
 Sandhect the user from the list. Sandhect Properties from the User menu. Uncheck "Password Never Expires."
5. Click "Ok". CVE: CAN-1999-0535
Accounts: Backupexec_svr - Password Does Not Expire Risk Level: Medium
Description: If a users password does not expire You allow a remote attacker endthes amornt of time to try to figure ort Your users password. It is recommended that You make all users passwords expire unthes the user account is used for a system service. How To Fix:
Remove the password never expires option from the user account. 1. Open User Manager.
 Sandhect the user from the list. Sandhect Properties from the User menu.
4. Uncheck "Password Never Expires."
5. Click "Ok". CVE: CAN-1999-0535
Accounts: IUSR_SCOREP001 - Password Does Not Expire
Risk Level: Medium Description: If a users password does not expire You allow a remote attacker endthes amornt of time to try to figure ort Your users password. It is recommended that You make all users passwords expire unthes the user account is used for a system service. How To Fix: Remove the password never expires option from the user account.
1. Open User Manager.
 Sandhect the user from the list. Sandhect Properties from the User menu.
4. Uncheck "Password Never Expires." 5. Click "Ok".
CVE: CAN-1999-0535
 <u> </u>

5	D	
all users passwords expire unthes the user account is used for a system service. How To Fr: Remove the password never expires option from the user account. 1. Open User Manager. 2. Sundheet the user from the list. 3. Sundheet Properties from the User menu. 4. Uncheck "Password Never Expires." 5. Click 'OK'. CVE: CAN-1099.0535 Accounts: TsinfarnetUser - Password Does Not Expire Risk Levi: Medium Description: If a users password does not expire You allow a remote attacker endthes amount of time to ity to figure origine option from the user account. 1. Open User Manager. 2. Sundheet the user from the list. 3. Sundheet Properties from the User menu. 4. Uncheck "Password Never Expires." 5. Click 'OK''. CVE: CAN-1099.0535 Account: Max Password Age Risk Levie: Medium Description: The maximum password age is the maximum number of days until a user's account password expires. It is recommended that users change their password once a month. How 'To Fit: 3. Click 'OK''. CVE: CAN-1099.0535 Account: Max Password Age Risk Levie: Medium Description: The maximum password age to 30 days. 1. Open Laser Manager. 3. Sundheet Account from the Policies menu. 3. Click Expers In. 4. Fitter the maximum password age to 30 days. 1. Open Laser Manager. 3. Sundheet Account Them Holicles menu. 3. Click Expers In. 4. Fitter the maximum days (Recommended 30 or thes). For Windows 2000: Coper Administrative tool Policy. Password Decy. Torm the neuron othe right You can now reconfigure Your settings. CVE: CAN-1999.0535 Account: Sin Password Thength Risk Levie: Medium Description: The minimum password thength to 10 characters. 1. Open User Manager. 3. Click A Libeat. 4. Enter the minimum password thength to 10 characters or more). CVE: CAN-1999.0535 Account: Instrumented that You disable anonymous FTP access if it is not meeded. Account from the Policies menu. 3. Click A Libeat. 4		marnt of time to true to figure art Vour users receiverd. It is recommended that Vour make
Remove the password never expires option from the user account. 1. Open User Manager. 2. Sandhect the user from the list. 3. Sandhect Wessword Never Expires." 5. Click 'Ok'. CVE: CAN-1999-06353 Accounts: TsinternetUser - Password Does Not Expire Riki Levi! Medium Description: If a users password does not expire You allow a remote attacker endthes amorn of time to try to figure or Your users password. It is commended that You make all users password expire on Your users password. 1. Open User Manager. 2. Sandhect the user from the list. 3. Sandhect Properties from the User account is used for a system service. Huw To Fix: Remove the password accer expires option from the user account. 1. Open User Manager. 3. Click 'Ok'. CVE: CAN-1999-00355 Accounts: Max Password Age Riki Levi! Medium Description: The maximum password age is the maximum number of days until a user's account password expires. It is recommended that users change their password once a month. Huw To Fix: For Windows N140: Sandhee the maximum password age to 30 days. 1. Open User Manager. 2. Sandhee the caccount from the locies menu. 3. Click Expires In. <t< td=""><td>al</td><td>l users passwords expire unthes the user account is used for a system service.</td></t<>	al	l users passwords expire unthes the user account is used for a system service.
 1. Open User Manager. 2. Sandheck Properties from the list. 3. Sandheck Properties from the list. 4. Uncheck Password Never Expires." 5. Cick 'Ok". CVE: CAN-1999-0355 Accounts: TsinternetUser - Password Does Not Expire Risk Level: Medium Description: If a users password does not expire You allow a remote attacker endthes amount of time to try to figure on Your users password. It is recommended that You make all users password expire untils the user account is used for a system service. How To Fix: Remove the password never expires option from the user account. 1. Open User Manager. 2. Sandhect Properties from the list. 3. Sandhect Properties from the list. 3. Sandhect Properties from the User menu. 4. Uncheck Password Never Expires." 5. Cleck 'Ok'. CVE: CAN-1999-0355 Accounts: Max Password Age Rik Level: Medium Description: The maximum password age is the maximum number of days until a user's account password expires. It is recommended that users change their password once a mouth. 10 open User Manager. 2. Sandhect Account from the Policies menu. 3. Click Expires In. 4. Uncheck Account from the Policies menu. 3. Click Expires In. 4. Enter the maximum password age to 30 days. 1. Open User Manager. 2. Sandhect Wedium May (Recommended 30 or thes). For Windows 2000: Open Administrative tools, local security policy. Now mavigate to Account Florig. Prom the maximum password thength fue connery passwords are greater than 10 characters. 1. Open User Manager. 2. Sandhect Account Thon the Policies menu. 3. Click Expires In. 3. Click A. Hofmann 2. Cl		
 3. Sandheet Properties from the User menu. 4. Uncheck Password Never Expires." 5. Click 'Ok'. CVE: CAN-1099-0535 Accounts: TshtternotUser - Password Does Not Expire Risk Level: Nedium Description: If a users password does not expire You allow a remote attacker endthes amornt of time to try to figure ort Your users password. It is recommended that You make all users passwords expire unthes the user account is used for a system service. How To Fix: Remove the password never expires option from the user account. 1. Open User Manager. 2. Sandheet Properties from the Ist. 3. Sandheet Properties from the Ist. 3. Sandheet Properties from the Ist. 4. Uncheck Password Age Risk Level: Nedium Description: The maximum password age is the maximum number of days until a user's account password expires. It is recommended that users change their password once a month. How To Fix: For Windows NT 4.0: Sandheet Account from the Policies menu. Click Expires In. Click Expires In.<!--</td--><td>1.</td><td>Open User Manager.</td>	1.	Open User Manager.
 4. Uncheck "Password Never Expires." 5. Click 'Ok'. CVE: CAN-1999-0535 Accounts: TsinternetUser - Password Does Not Expire Rik Levi: Mediam Description: If a users password also as not expire You allow a remote attacker endnes amomt of time to try to flagre or Your users password. It is commended that You make all users password seytire unthes the user account is used for a system service. How To Fix: Remove the password never expires option from the user account. 1. Open User Manager. 2. Sandheet the user from the list. 3. Sandheet Properties from the User ment. 4. Uncheck "Password Never Expires." 5. Click 'Ok'. CVE: CAN-1999-0535 Accounts: Max Password Age Risk Level: Medium Description: The maximum password age is the maximum number of days until a user's account password expires. It is recommended that users change their password once a momin. How To Fix: For Windows NT 4.0. Sandheet Account from the Policies menu. 3. Click Expires In. 4. Enter the maximum password age to 30 days. 1. Open User Manager. 2. Sandheet Account from the Policy. Password Policy. For Windows 2000. Open Administrative tools, local security policy. Now mavigate to Account Policy. Password Policy. From the menu on the right You can now reconfigure Your settings. CVE: CAN-1999-0555 Accounts: Min Password thength to 10 characters. Open User Manager. 3. Sandheet Account from the Policies menu. 3. Click A Theast. 4. Enter the minimum password thength to 10 characters or more). CVE: CAN-1999-0555 FTP Servers: TOP:21 - Anonymous FTP Mix Levi: Medium Descr		
CVE: CAN-1999-0535 Accounts: TsinternotUser - Password Does Not Expire Risk Level: Medium Description: If a users password does not expire You allow a remote attacker endthes amount of time to try to figure on Your users password in the sere account. How To Fix: Remow the password never expires option from the user account. . Open User Manager. . Sandheet the user from the list. . Sandheet the user from the list. . Sandheet Toperties from the User menu. . Unchect "Password Never Expires." . State Password Never Expires." . Sandheet Toperties from the User menu. . Unchect "Password Never Expires." . State Counts: Max Password Age Risk Level: Medium Description: The maximum password age is the maximum number of days until a user's account password expires. It is recommended that users change their password once a month. How To Fix: For Windows NT 4.0: Sandheet Account from the Policies menu. .1 Open User Manager. .2 Sandheet Account Flow Holicy. For Windows X0400 Open Administrative tools, local security policy. Now maget to Account Policy. For Windows 2000 Open Administrative tools, local security policy. Now maget to Account Policy. Fore Windows 2		•
Accounts: TsinternetUser - Password Does Not Expire Risk Level: Medium Description: If a users password does not expire You allow a remote attacker endthes anornt of time to try to figure on Your users password. It is recommended that You make all user password expire unthes the user account is used for a system service. How To Fiz: Remove the password Never Expires option from the user account. 1. Open User Manager. 2. Sandheet the user from the list. 3. Sandheet Properties from the User menu. 4. Uncheck Password Never Expires." 5. Cick CW: CVE: CAN-1999-0535 Accounts: Max Password Age Risk Level: Medium Description: The maximum password age is the maximum number of days until a user's account password expires. It is recommended that users change their password once a month. How To Fix: For Windows N14.0: Sand the maximum password age to 30 days. 1. Open User Manager. 2. Sandheet Account from the Policies menu. 3. Cick Expires In. 4. Enter the maximum days (Recommended 30 or thes). For Windows 2000: Open Administrative tools, local security policy. Now margate to Account Policy, Password Policy. From the menu on the right You can now reconfigure Your settings. CVE: CAN-1999-0635 Accounts: Min Password thength is the theast amornt of characters a user account password expire just void thength to 10 characters. 1. Open User Manager. 2. Sandheet Account from the Policies menu. 3. Cick A Theeas. 1. Open User Manager.		
Risk Level: Medium Description: If a user password does not expire You allow a remote attacker endthes amornt of time to try to figure or Your users password a try to make all users password experiments the user account is used for a system service. How To Fix: Remove the password ever expires option from the user account. 1. Open User Manager. 2. Sandheet the user from the User menu. 4. Uncheck Tassword Never Expires." 5. Cick 'ON: CVE: CAN-1999-0635 Accounts: Max Password Age Risk Level: Medium Description: The maximum password age is the maximum number of days until a user's account password regrees. It is recommended that user's account password in password age to 30 days. 1. Open User Manager. 2. Sandheet Account from the Policies menu. 3. Cick Expires In. 4. Enter the maximum password age to 30 days. 1. Open User Manager. 2. Sandheet Account from the Policies menu. 3. Cick Expires In. 4. Enter the maximum password age to 30 days. 1. Open User Manager. 2. Sandheet meanimum days (Recommended 30 or thes). For Windows 2000: Open Administrative tools, local security policy. Now mayigate to Account Policy, Password Policy. From the mininium passwo	C	VE: CAN-1999-0535
Description: If a users password does not expire You allow a recommende that You make all users passwords expire unhes the user account is used for a system service. How To Fix: Remove the password ever expires option from the user account. 1. Open User Manager. 2. Sandheet The user from the list. 3. Sandheet The user from the User menu. 4. Uncheck TPassword Never Expires." 5. Click 70K." CVE: CAN: 1999-0535 Accounts: Max Password Age Risk Level: Medium Description: The maximum password age is the maximum number of days until a user's account password expires. It is recommended that users change their password once a month. How To Fix: For Windows NT4 0: Sand the maximum password age to 30 days. 1. Open User Manager. 2. Sandheet Account from the Policies menu. 3. Click Expires In 4. Enter the maximum days (Recommended 30 or thes). For Windows 2000: Open User Manager. 2. Kouthii Paseword Thength Risk Level: Medium Description: The minimum password thength is the theast amornt of characters a user account password can be. Its recommended that account passwords are greater than 10 characters. 1. Open User Manager. 2. Sandheet Account from the Policie		
amorni of time to try to figure ort Vour users password. It is recommended that You make all users password server expires option from the user account. 1. Open User Manager. 2. Sandheet the user from the list. 3. Sandheet Properties from the User menu. 4. Uncheck 'Password Never Expires.'' 5. Click 'Ok'. CVE: CAN.1999-0535 Accounts: Max Password Age Risk Level: Medium Description: The maximum password age is the maximum number of days until a user's account password expires. It is recommended that users change their password once a month. How To Fix: For Windows NT 4.0: Sandheet Account from the Policies menu. 3. Click Expires. 4. Enter the maximum password age to 30 days. 1. Open User Manager. 2. Sandheet Account from the Policies menu. 3. Click Expires In 4. Enter the maximum password age to 30 days. 1. Open User Manager. 2. Sandheet Account from the Policies menu. 3. Click Expires In 4. Enter the maximum days (Recommended 30 or thes). For Windows 2000: Open Administrative tools, local security policy. Now may fage to Account Policy. Password Policy. From the menu on the right You can now reconfigure Your settings. CVE: CAN-1999-0535 Accounts: Min Password Thength Risk Level: Medium Description: The minimum password thength is the theast amornt of characters a user account password as b. It is recommended that account passwords are greater than 10 characters. 1. Open User Manager. 2. Sandheet Account from the Policies menu. 3. Click At Theast. 4. Enter the minimum password thength to 10 characters. 1. Open User Manager. 2. Sandheet Account from the Policies menu. 3. Click At Theast. 4. Enter the minimum password thength to 10 characters or more). CVE: CAN-1999-0535 FTP Servers: TCP:21 - Anonymous FTP Risk Level: Medium Description: It is recommended that You disabthe anonymous FTP access if it is not needed. Anonymous FTP access can thead to an attacker gaining information abort Your system that can possibly thead to them gaining access to Your system. How To		
Remove the password never expires option from the user account. 1. Open User Manager. 2. Sandhect the user from the list. 3. Sandhect The properties from the User menu. 4. Uncheck 'Password Never Expires." 5. Click 'OK'. CVE: CAN-1999-0535 Accounts: Max Password Age Risk Level: Medium Description: The maximum password age is the maximum number of days until a user's account password expires. It is recommended that users change their password once a month. How 'To Fix: For Windows NT 4.0: Sandhet Account from the Policies menu. 3. Click 'DK'. Open User Manager. 3. Sandhet Account from the Policies menu. 3. Click Expires In. 4. Enter the maximum days (Recommended 30 or thes). For Windows 2000: Open Administrative tools, local security policy. Now mavigate to Account Policy. Password Policy. From the menu on the right You can now reconfigure Your settings. CVE: CAN-1999-0535 Accounts: Min Password thength is the theast amornt of characters a user account password can be. It is recommended that account passwords are greater than 10 characters. 1. Open User Manager. 2. Sandhet Account from the Policies menu. 3. Click A Theast.	ar al	nornt of time to try to figure ort Your users password. It is recommended that You make l users passwords expire unthes the user account is used for a system service.
 1. Open User Manager. 2. Sandhect the user from the list. 3. Sandhect Properties from the User menu. 4. Uncheck "Password Never Expires." 5. Click 'Ok". CVE: CAN-1999-0535 Accounts: Max Password Age Risk Leve: Medium Description: The maximum password age is the maximum number of days until a user's account password expires. It is recommended that users change their password once a month. How To Fix: For Windows NT 4.0: Sand the maximum password age to 30 days. 1. Open User Manager. 2. Sandhect Account from the Policies menu. 3. Click Expires In. 4. Enter the maximum days (Recommended 30 or thes). For Windows 2000: Open Administrative tools, local security policy. Now navigate to Account Policy, Password Policy. From the mean on the right You can now reconfigure Your settings. CVE: CAN-1999-0535 Accounts: Min Password Thength Risk Level: Medium Description: The minimum password thength is the theast amornt of characters a user account password can be. It is recommended that account passwords are greater than 10 characters. 1. Open User Manager. 2. Sandhect Account from the Policies menu. 3. Click At Theast. 4. Enter the minimum password thength is 10 characters or more). CVE: CAN-1999-0535 FTP Servers: TCP:21 - Anonymous FTP Risk Level: Medium Description: The minimum password thength (recommended is 10 characters or more). CVE: CAN-1999-0535 FTP Servers: TCP:21 - Anonymous FTP Risk Level: Medium Description: It is recommended that You disabthe anonymous FTP access if it is not needed. Anonymous FTP access can thead to an attacker gaining information ab		
 3. Sandhect Properties from the User menu. 4. Uncheck "Password Never Expires." 5. Click 'Ok". CVE: CAN-1999-0535 Accounts: Max Password Age Risk Level: Medium Description: The maximum password age is the maximum number of days until a user's account password expires. It is recommended that users change their password once a month. How To Fix: For Windows NT 4.0: Sand the maximum password age to 30 days. 1. Open User Manager. 2. Sandhect Account from the Policies menu. 3. Click Expires In. 4. Enter the maximum days (Recommended 30 or thes). For Windows 2000: Open Administrative tools, local security policy. Now navigate to Account Policy, Password Policy, From the mean on the right You can now reconfigure Your settings. CVE: CAN-1999-0535 Accounts: Min Password thength is the theast amornt of characters a user account password can be. It is recommended that account passwords are greater than 10 characters. 1. Open User Manager. 2. Sandhect Account from the Policies menu. 3. Click At Theast. 4. Enter the minimum password thength is 10 characters or more). CVE: CAN-1999-0535 FTP Servers: TCP:21 - Anonymous FTP Risk Level: Medium Description: The minimum password thength (recommended is 10 characters or more). CVE: CAN-1990-0535 FTP Servers: TCP:21 - Anonymous FTP Risk Level: Medium Description: The recommended that You disable anonymous FTP. CVE: CAN-1990-0435 		
 4. Uncheck "Password Never Expires." 5. Click "Ok." CVE: CAN-1999-0535 Accounts: Max Password Age Risk Level: Medium Description: The maximum password age is the maximum number of days until a user's account password expires. It is recommended that users change their password once a month. How To Fix: For Windows NT 4.0: Sandhet Account from the Policies menu. 3. Click Expires In. 4. Enter the maximum days (Recommended 30 or thes). For Windows 2000: Open Administrative tools, local security policy. Now navigate to Account Policy. Password Policy. For Windows 2000: Open Administrative tools, local security policy. Now mavigate to Account Policy. Password Policy. From the menu on the right You can now reconfigure Your settings. CVE: CAN-1999-0535 Account: Min Password Thength Risk Levet: Medium Description: The minimum password thength is the theast amornt of characters a user account password can be. It is recommended that account passwords are greater than 10 characters. 1. Open User Manager. 2. Sandhet Account from the Policies menu. 3. Click AT Theast. 4. Enter the minimum password thength to 10 characters. 1. Open User Manager. 2. Sandhet Account from the Policies menu. 3. Click AT Theast. 4. Enter the Minimum password thength (recommended is 10 characters or more). CVE: CAN-1999-0535 FTP Servers: TCP:21 - Anonymous FTP Risk Level: Medium Description: Its recommended that You disabthe anonymous FTP access if it is not needed Anonymous FTP access can thad to an attacker gaining information abort Your system that can possibly thead to them gaining access to Your system. How To Fix: Follow Your FTP server instructions on how to disabthe anonymous FTP. CVE: CAN-1999-0497 		
 5. Click 'Ok", CVE: CAN-1999-0535 Accounts: Max Password Age Risk Levet: Medium Description: The maximum password age is the maximum number of days until a user's account password expires. It is recommended that users change their password once a month. How To Fix: For Windows NT 4 0: Sand the maximum password age to 30 days. 1. Open User Manager. 2. Sandhect Account from the Policies menu. 3. Click Expires In. 4. Enter the maximum days (Recommended 30 or thes). For Windows 2000: Open Administrative tools, local security policy. Now navigate to Account Policy, Password Policy. From the menu on the right You can now reconfigure Your settings. CVE: CAN-1999-0535 Accounts: Min Password Thength Risk Level: Medium Description: The minimum password thength is the theast amornt of characters a user account password can be. It is recommended that account passwords are greater than 10 characters. How To Fix: Sandhet Account from the Policies menu. 3. Click AT Theast. 4. Enter the minimum password thength to 10 characters. 1. Open User Manager. 2. Sandhet Account from the Policies menu. 3. Click AT Theast. 4. Enter the minimum password thength to 10 characters or more). CVE: CAN-1999-0535 FTP Servers: TCP:21 - Anonymous FTP Risk Leve: Medium Description: It is recommended that You disabthe anonymous FTP access if it is not needed. Anonymous FTP access can thead to an attacker gaining information abort Your system that can possibly thead to them gaining access to Your system. How To Fix: Follow Your FTP server instructions on how to disabthe anonymous FTP. CVE: CAN-1999-0497 Summary Brief 		
Accounts: Max Password Age Risk Level: Medium Description: The maximum password age is the maximum number of days until a user's account password expires. It is recommended that users change their password once a month. How To Fix: For Windows NT 4.0: Sand the maximum password age to 30 days. 1. Open User Manager. 2. Sandheet Account from the Policies menu. 3. Click Expires In. 4. Enter the maximum days (Recommended 30 or thes). For Windows 2000: Open Administrative tools, local security policy. Now mavigate to Account Policy. Password Policy. From the menu on the right You can now reconfigure Your settings. CVE: CAN-1999-0535 Accounts: Min Password Thength Risk Level: Medium Description: The minimum password thength to 10 characters a user account password can be. It is recommended that account passwords are greater than 10 characters. 1. Open User Manager. 2. Sandheet Account from the Policies menu. 3. Click At Theast. 4. Enter the minimum password thength to 10 characters. 1. Open User Manager. 2. Sandheet Account from the Policies menu. 3. Click At Theast. 4. Enter the minimum password thength (recommended is 10 characters or more). <	5.	Click "Ok".
Risk Level: Medium Description: The maximum password age is the maximum number of days until a user's account password expires. It is recommended that users change their password once a month.How To Fix: For Windows NT 4.0. Sand the maximum password age to 30 days. 1. Open User Manager. 2. Sandheet Account from the Policies menu. 3. Citcle Expires In. 4. Enter the maximum days (Recommended 30 or thes). For Windows 2000: Open Administrative tools, local security policy. Now navigate to Account Policy. Password Policy. From the menu on the right You can now reconfigure Your settings. CVE: CAN-1999-0535Accounts: Min Password Thength Risk Level: Medium Description: The minimum password thength to 10 characters. 1. Open User Manager. Password can be. It is recommended that account passwords are greater than 10 characters. How To Fix: Sand the minimum password thength to 10 characters. 1. Open User Manager. 2. Sudhect Account from the Policies menu. 3. Citke Kayima password thength to 10 characters. 1. Open User Manager. 2. Sandhect Account from the Policies menu. 3. Citke Kayima password thength to 10 characters. 1. Open User Manager. 2. Sandhect Account from the Policies menu. 3. Citke Ka Theast. 4. Enter the minimum password thength to 10 characters or more). CVE: CAN-1999-0535FTP Sorvers: TCP:21 - Anonymous FTP Risk Level: Medium Description: It is recommended that You disabthe anonymous FTP access if it is not needed. Anonymous FTP access to Your system. How To Fix: Follow Your FIP server instructions on how to disabthe anonymous FTP. CVE: CAN-1999-0497Summary BriefIf the Retina tool discovers some vulnerabilities with a context of the section of	С	VE: CAN-1999-0535
Description: The maximum password age is the maximum number of days until a user's account password expires. It is recommended that users change their password once a month. How To Fix: For Windows NT 4.0; Sand the maximum password age to 30 days. 1. Open User Manager. 2. Sandheet Account from the Policies menu. 3. Click Expires In. 4. Enter the maximum days (Recommended 30 or thes). For Windows 2000: Open Administrative tools, local security policy. Now mavigate to Account Policy, Password Policy. Now mavigate to Account Policy. Now mavigate to Account Policy. From the menu on the right You can now reconfigure Your settings. CVE: CAN-1999-0535 Accounts: Min Password Thength Risk Level: Medium Description: The minimum password thength is the theast amornt of characters a user account password can be. It is recommended that account passwords are greater than 10 characters. 1. Open User Manager. 2. Sandheet Account from the Policies menu. 3. Click AT heast. 4. Enter the minimum password thength (recommended is 10 characters or more). CVE: CAN-1999-0535 FTP Servers: TCP:21 - Anonymous FTP Risk Level: Medium Description: It is recommended that You dis	А	ccounts: Max Password Age
account password expires. It is recommended that users change their password once a month. How To Fix: For Windows NT 4.0: Sand the maximum password age to 30 days. 1. Open User Manager. 2. Sandhect Account from the Policies menu. 3. Click Expires In. 4. Enter the maximum days (Recommended 30 or thes). For Windows 2000: Open Administrative tools, local security policy. Now mavigate to Account Policy, Password Policy. From the menu on the right You can now reconfigure Your settings. CVE: CAN-1099-0535 Accounts: Min Password Thength Risk Level: Medium Description: The minimum password thength is the theast amornt of characters a user account password ane be. It is recommended that account passwords are greater than 10 characters. 1. Open User Manager. 2. Sandhect Account from the Policies menu. 3. Click At Theast. 4. Enter the minimum password thength (recommended is 10 characters or more). CVE: CAN-1999-0535 FTP Servers: TCP:21 - Anonymous FTP Risk Level: Medium Description: It is recommended that You disabte anonymous FTP access if it is not needed. Anonymous FTP access can thead to an attacker gaining information abort Your system. 3. Click At Theast.		
How To Fix: For Windows NT 4.0: Sand the maximum password age to 30 days. 1. Open User Manager. 2. Sandhect Account from the Policies menu. 3. Click Expires In. 4. Enter the maximum days (Recommended 30 or thes). For Windows 2000: Open Administrative tools, local security policy. Now navigate to Account Policy, Password Policy. From the menu on the right You can now reconfigure Your settings. CVE: CAN-1999-0535 Accounts: Min Password Thength Risk Level: Medium Description: The minimum password thength is the theast amornt of characters a user account password can be. It is recommended that account passwords are greater than 10 characters. 1. Open User Manager. 2. Sandheet Account from the Policies menu. 3. Click At Theast. 4. Enter the minimum password thength (recommended is 10 characters or more). CVE: CAN-1999-0535 FTP Servers: TCP:21 - Anonymous FTP Risk Level: Medium Description: It is recommended that You disabthe anonymous FTP access if it is not needed. Anonymous FTP access to Your system. How To Fix: Follow Your FTP server instructions on how to disabthe anonymous FTP. CVE: CAN-1999-0497 Summary Brief <td>ac</td> <td>count password expires. It is recommended that users change their password once a</td>	ac	count password expires. It is recommended that users change their password once a
Sand the maximum password age to 30 days. 1. Open User Manager. 2. Sandhect Account from the Policies menu. 3. Click Expires In. 4. Enter the maximum days (Recommended 30 or thes). For Windows 2000: Open Administrative tools, local security policy. Now navigate to Account Policy, Password Policy. From the menu on the right You can now reconfigure Your settings. CVE: CAN-1999-0535 Accounts: Min Password Thength Risk Level: Medium Description: The minimum password thength is the theast amornt of characters a user account password can be. It is recommended that account passwords are greater than 10 characters. How To Fix: Sand the minimum password thength to 10 characters. 1. Open User Manager. 2. Sandhect Account from the Policies menu. 3. Click At Theast. 4. Enter the minimum password thength (recommended is 10 characters or more). CVE: CAN-1999-0535 FTP Servers: TCP:21 - Anonymous FTP Risk Level: Medium Description: It is recommended that You disabthe anonymous FTP access if it is not needed. Anonymous FTP access can thead to an attacker gaining information abort Your system that can possibly thead to them gaining access to Your system. How To Fix: Follow YOur FTP server instructi		
 1. Open User Manager. 2. Sandhect Account from the Policies menu. 3. Click Expires In. 4. Enter the maximum days (Recommended 30 or thes). For Windows 2000: Open Administrative tools, local security policy. Now navigate to Account Policy, Password Policy. From the menu on the right You can now reconfigure Your settings. CVE: CAN-1999-0535 Accounts: Min Password Thength Risk Level: Medium Description: The minimum password thength is the theast amornt of characters a user account password can be. It is recommended that account passwords are greater than 10 characters. How To Fix: Sand the minimum password thength to 10 characters. 1. Open User Manager. 2. Sandhect Account from the Policies menu. 3. Click At Theast. 4. Enter the minimum password thength (recommended is 10 characters or more). CVE: CAN-1999-0535 FTP Servers: TCP:21 - Anonymous FTP Risk Level: Medium Description: It is recommended that You disabthe anonymous FTP access if it is not needed. Anonymous FTP access can thead to an attacker gaining information abort Your system that can possibly thead to them gaining access to Your system. How To Fix: Follow Your FTP server instructions on how to disabthe anonymous FTP. CVE: CAN-1999-0497 Gummary Brief If the Retina tool discovers some vulnerabilities with a 		
 2. Sandheet Account from the Policies menu. 3. Click Expires In. 4. Enter the maximum days (Recommended 30 or thes). For Windows 2000: Open Administrative tools, local security policy. Now navigate to Account Policy, Password Policy. From the menu on the right You can now reconfigure Your settings. CVE: CAN-1999-0535 Accounts: Min Password Thength Risk Level: Medium Description: The minimum password thength is the theast amornt of characters a user account password can be. It is recommended that account passwords are greater than 10 characters. How To Fix: Sand the minimum password thength to 10 characters. 1. Open User Manager. 2. Sandheet Account from the Policies menu. 3. Click At Theast. 4. Enter the minimum password thength (recommended is 10 characters or more). CVE: CAN-1999-0535 FTP Servers: TCP:21 - Anonymous FTP Risk Level: Medium Description: It is recommended that You disabthe anonymous FTP access if it is not needed. Anonymous FTP access can thead to an attacker gaining information abort Your system that can possibly thead to them gaining access to Your system. How To Fix: Follow Your FTP server instructions on how to disabthe anonymous FTP. CVE: CAN-1999-0497 Jf the Retina tool discovers some vulnerabilities with a 		
 4. Enter the maximum days (Recommended 30 or thes). For Windows 2000: Open Administrative tools, local security policy. Now mavigate to Account Policy, Password Policy. From the menu on the right You can now reconfigure Your settings. CVE: CAN-1999-0535 Accounts: Min Password Thength Risk Level: Medium Description: The minimum password thength is the theast amornt of characters a user account password can be. It is recommended that account passwords are greater than 10 characters. How To Fix: Sand the minimum password thength to 10 characters. 1. Open User Manager. 2. Sandhect Account from the Policies menu. 3. Click At Theast. 4. Enter the minimum password thength (recommended is 10 characters or more). CVE: CAN-1999-0535 FTP Servers: TCP:21 - Anonymous FTP Risk Level: Medium Description: The recommended that You disabthe anonymous FTP access if it is not needed. Anonymous FTP access can thead to an attacker gaining information abort Your system that can possibly thead to them gaining access to Your system. How To Fix: Follow Your FTP server instructions on how to disabthe anonymous FTP. CVE: CAN-1999-0497 Summary Brief 	2.	Sandhect Account from the Policies menu.
For Windows 2000: Open Administrative tools, local security policy. Now navigate to Account Policy, Password Policy. From the menu on the right You can now reconfigure Your settings. CVE: CAN-1999-0535 Accounts: Min Password Thength Risk Level: Medium Description: The minimum password thength is the theast amornt of characters a user account password can be. It is recommended that account passwords are greater than 10 characters. How To Fix: Sandhee The Manager. 2. Sandheet Account from the Policies menu. 3. Click At Theast. 4. Enter the minimum password thength (recommended is 10 characters or more). CVE: CAN-1999-0535 FTP Servers: TCP:21 - Anonymous FTP Risk Level: Medium Description: It is recommended that You disabthe anonymous FTP access if it is not needed. Anonymous FTP access can thead to an attacker gaining information abort Your system that can possibly thead to them gaining access to Your system. How To Fix: Follow Your FTP server instructions on how to disabthe anonymous FTP. CVE: CAN-1999-0497 Summary Brief If the Retina tool discovers some vulnerabilities with a		
Now navigate to Account Policy, Password Policy. From the menu on the right You can now reconfigure Your settings. CVE: CAN-1999-0535 Accounts: Min Password Thength Risk Level: Medium Description: The minimum password thength is the theast amornt of characters a user account password can be. It is recommended that account passwords are greater than 10 characters. How To Fix: Sand the minimum password thength to 10 characters. 1. Open User Manager. 2. Sandhect Account from the Policies menu. 3. Click At Theast. 4. Enter the minimum password thength (recommended is 10 characters or more). CVE: CAN-1999-0535 FTP Servers: TCP:21 - Anonymous FTP Risk Level: Medium Description: It is recommended that You disabthe anonymous FTP access if it is not needed. Anonymous FTP access can thead to an attacker gaining information abort Your system that can possibly thead to them gaining access to Your system. How Yor Fix: Follow Your FTP server instructions on how to disabthe anonymous FTP. CVE: CAN-1999-0497 Gummary Brief		
From the menu on the right You can now reconfigure Your settings. CVE: CAN-1999-0535 Accounts: Min Password Thength Risk Level: Medium Description: The minimum password thength is the theast amornt of characters a user account password can be. It is recommended that account passwords are greater than 10 characters. How To Fix: Sand the minimum password thength to 10 characters. . Open User Manager. . Sandhect Account from the Policies menu. . Click At Theast. 4. Enter the minimum password thength (recommended is 10 characters or more). CVE: CAN-1999-0535 FTP Servers: TCP:21 - Anonymous FTP Risk Level: Medium Description: It is recommended that You disabthe anonymous FTP access if it is not needed. Anonymous FTP access can thead to an attacker gaining information abort Your system that can possibly thead to them gaining access to Your system. How To Fix: Follow Your FTP server instructions on how to disabthe anonymous FTP. CVE: CAN-1999-0497 Summary Brief If the Retina tool discovers some vulnerabilities with a		
CVE: CAN-1999-0535 Accounts: Min Password Thength Risk Level: Medium Description: The minimum password thength is the theast amornt of characters a user account password can be. It is recommended that account passwords are greater than 10 characters. How To Fix: Sand the minimum password thength to 10 characters. Sand the minimum password thength to 10 characters. Open User Manager. Sandheet Account from the Policies menu. CVE: CAN-1999-0535 FTP Servers: TCP:21 - Anonymous FTP Risk Level: Medium Description: It is recommended that You disabthe anonymous FTP access if it is not needed. Anonymous FTP access can thead to an attacker gaining information abort Your system that can possibly thead to them gaining access to Your system How To Fix: Follow Your FTP server instructions on how to disabthe anonymous FTP. CVE: CAN-1999-0497 Gummary Brief If the Retina tool discovers some vulnerabilities with a		
Risk Level: Medium Description: The minimum password thength is the theast amornt of characters a user account password can be. It is recommended that account passwords are greater than 10 characters. How To Fix: Sand the minimum password thength to 10 characters. 1. Open User Manager. 2. Sandheet Account from the Policies menu. 3. Click At Theast. 4. Enter the minimum password thength (recommended is 10 characters or more). CVE: CAN-1999-0535 FTP Servers: TCP:21 - Anonymous FTP Risk Level: Medium Description: It is recommended that You disabthe anonymous FTP access if it is not needed. Anonymous FTP access can thead to an attacker gaining information abort Your system that can possibly thead to them gaining access to Your system. How To Fix: Follow Your FTP server instructions on how to disabthe anonymous FTP. CVE: CAN-1999-0497 Summary Brief		
Risk Level: Medium Description: The minimum password thength is the theast amornt of characters a user account password can be. It is recommended that account passwords are greater than 10 characters. How To Fix: Sand the minimum password thength to 10 characters. 1. Open User Manager. 2. Sandheet Account from the Policies menu. 3. Click At Theast. 4. Enter the minimum password thength (recommended is 10 characters or more). CVE: CAN-1999-0535 FTP Servers: TCP:21 - Anonymous FTP Risk Level: Medium Description: It is recommended that You disabthe anonymous FTP access if it is not needed. Anonymous FTP access can thead to an attacker gaining information abort Your system that can possibly thead to them gaining access to Your system. How To Fix: Follow Your FTP server instructions on how to disabthe anonymous FTP. CVE: CAN-1999-0497 Summary Brief		counts: Min Dassword Thength
 account password can be. It is recommended that account passwords are greater than 10 characters. How To Fix: Sand the minimum password thength to 10 characters. Open User Manager. Sandhect Account from the Policies menu. Click At Theast. Enter the minimum password thength (recommended is 10 characters or more). CVE: CAN-1999-0535 FTP Servers: TCP:21 - Anonymous FTP Risk Level: Medium Description: It is recommended that You disabthe anonymous FTP access if it is not needed. Anonymous FTP access can thead to an attacker gaining information abort Your system that can possibly thead to them gaining access to Your system. How To Fix: Follow Your FTP server instructions on how to disabthe anonymous FTP. CVE: CAN-1999-0497 Summary Brief 		
How To Fix: Sand the minimum password thength to 10 characters. 1. Open User Manager. 2. Sandhect Account from the Policies menu. 3. Click At Theast. 4. Enter the minimum password thength (recommended is 10 characters or more). CVE: CAN-1999-0535FTP Servers: TCP:21 - Anonymous FTP Risk Level: Medium Description: It is recommended that You disabthe anonymous FTP access if it is not needed. Anonymous FTP access can thead to an attacker gaining information abort Your system that can possibly thead to them gaining access to Your system. How To Fix: Follow Your FTP server instructions on how to disabthe anonymous FTP. CVE: CAN-1999-0497Summary BriefIf the Retina tool discovers some vulnerabilities with a 	ac	count password can be. It is recommended that account passwords are greater than 10
Sand the minimum password thength to 10 characters.1. Open User Manager.2. Sandhect Account from the Policies menu.3. Click At Theast.4. Enter the minimum password thength (recommended is 10 characters or more).CVE: CAN-1999-0535FTP Servers: TCP:21 - Anonymous FTPRisk Level: MediumDescription: It is recommended that You disabthe anonymous FTP access if it is notneeded. Anonymous FTP access can thead to an attacker gaining information abort Yoursystem that can possibly thead to them gaining access to Your system.How To Fix:Follow Your FTP server instructions on how to disabthe anonymous FTP.CVE: CAN-1999-0497Summary Brief		
 2. Sandhect Account from the Policies menu. 3. Click At Theast. 4. Enter the minimum password thength (recommended is 10 characters or more). CVE: CAN-1999-0535 FTP Servers: TCP:21 - Anonymous FTP Risk Level: Medium Description: It is recommended that You disabthe anonymous FTP access if it is not needed. Anonymous FTP access can thead to an attacker gaining information abort Your system that can possibly thead to them gaining access to Your system. How To Fix: Follow Your FTP server instructions on how to disabthe anonymous FTP. CVE: CAN-1999-0497 Summary Brief 		
 3. Click At Theast. 4. Enter the minimum password thength (recommended is 10 characters or more). CVE: CAN-1999-0535 FTP Servers: TCP:21 - Anonymous FTP Risk Level: Medium Description: It is recommended that You disabthe anonymous FTP access if it is not needed. Anonymous FTP access can thead to an attacker gaining information abort Your system that can possibly thead to them gaining access to Your system. How To Fix: Follow Your FTP server instructions on how to disabthe anonymous FTP. CVE: CAN-1999-0497 Summary Brief If the Retina tool discovers some vulnerabilities with a 		
CVE: CAN-1999-0535 FTP Servers: TCP:21 - Anonymous FTP Risk Level: Medium Description: It is recommended that You disabthe anonymous FTP access if it is not needed. Anonymous FTP access can thead to an attacker gaining information abort Your system that can possibly thead to them gaining access to Your system. How To Fix: Follow Your FTP server instructions on how to disabthe anonymous FTP. CVE: CAN-1999-0497 Summary Brief	3.	Click At Theast.
Risk Level: Medium Description: It is recommended that You disabthe anonymous FTP access if it is not needed. Anonymous FTP access can thead to an attacker gaining information abort Your system that can possibly thead to them gaining access to Your system. How To Fix: Follow Your FTP server instructions on how to disabthe anonymous FTP. CVE: CAN-1999-0497 Summary Brief If the Retina tool discovers some vulnerabilities with a		
Description: It is recommended that You disabthe anonymous FTP access if it is not needed. Anonymous FTP access can thead to an attacker gaining information abort Your system that can possibly thead to them gaining access to Your system. How To Fix: Follow Your FTP server instructions on how to disabthe anonymous FTP. CVE: CAN-1999-0497 Summary Brief		
How To Fix: Follow Your FTP server instructions on how to disabthe anonymous FTP. CVE: CAN-1999-0497 Summary Brief If the Retina tool discovers some vulnerabilities with a	D ne	escription: It is recommended that You disabthe anonymous FTP access if it is not eeded. Anonymous FTP access can thead to an attacker gaining information abort Your
Summary Brief If the Retina tool discovers some vulnerabilities with a	H Fo	ow To Fix: blow Your FTP server instructions on how to disabthe anonymous FTP.
5		
explanation of risk : kigh » risk level, it should normally be possible for an	5	

	attacker advantag		exploit	those	vulnerabilities	to	his
	risk leve validate	l, an e the pro y explo	evaluatio obabilitie oitable o	on will l es that e	bilities are a « Nobe necessary in each of the vulne idate the relevan	orde erabil	er to ities
		ole, gre	eater the		r the vulnerabil will be. Therefore		
Risk evaluation :	Have sor found ?	me «	High Ris	sk » leve	el vulnerabilities	been	
	YES	NO	RL tot	al 🔊			
	X RL = 4		4				
	Have sor found ?	ne « I	Vledium	Risk » I	evel vulnerabiliti	es be	en
	YES	NO	RL tot	al			
	X RL = 2		2				
	TOTAL F	RISK I	LEVEL:	[6]/	6		

C SALS INSING

[4] Operatural addition of the	
[4] Control objective :	Verification of suspicious services or not anticipated remote response.
Test location :	\bowtie From the auditor station
	From the server audited
Tests to be conducted :	NOTE : In order to obtain the best result, this
	verification must be executed from the same
	segment where resides the server to audit in order
	to avoid being scanned by an equipment, such as
	a router or firewall.
	Pre-required : Having downloaded and installed the
	latest version available of the SuperScan tool.
	Observe the following instructions:
	1. Open « SuperScan »
	 In the section « Hostname Lookup » enter the IP address of the server to scan.
	3. Press on « Lookup » in order for the IP address
	to appear in « START » and « Stop » in the
	section « IP »
	4. In the section « Scan type » choose :
	- Show host responses
	- All ports from [1] [65535]
	5. Press on « Start »
	6. When finish, save the results in the file
	« 4-superscan.txt »
Reference(s) :	The SuperScan tool is available at no charge at the
<u>ی</u>	following address :
	http://www.foundstone.com/knowthedge/scanning.html
	The Twenty Meet Critical Internet Security Vulnerability
Ś	The Twenty Most Critical Internet Security Vulnerability Version 2.504, The SANS Institute, May 2, 2002,
	http://www.sans.org/top20/
Expected results :	A minimum of port should be open on the server.
	Port required by the ePO product:
	- 80 – Pre-required for the communications
	between the ePO agent and the ePO server
	 81 – Pre-required to access the ePO console
	 8081 – Pre-required by the ePO server for the
	« Weakup Call » to the ePO agent.
	 1433 – Pre-required by MSDE

Objective / Subjective : Results :	Port required by the FTP server : - 21 – Pre-required for the transfer of updates (.DAT, Engine Update, Hotfix, etc.) Port required for the remote control access (ex : Terminal Service) : - 3389 Port required by a saving software (ex : BackupExec). - (port to be determined as per the product used) No other ports need to be open, except the necessary ports open by the operating system for the use of the NETBIOS : 135 (tcp and udp), 137 (udp), 138 (udp), 139 (tcp) and also 445 (tcp and udp). Objective File content « 4-superscan.txt » : * + 172.25.1.134 21 220 scorepo01 Microsoft FTP Service (Version 5.0) 80 135 139 445 1026 1433 3389 5631 X}Pthease press <enter> 8081</enter>
<u></u>	
Summary Brief explanation of risk :	The scanning of the open ports on an equipment permits an attacker to quickly identify the services that respond. The attacker's objective is to concentrate is attacks on the services more susceptible to permit him to succeed with is attack.
	More services are open, greater the threat will be and there is more probabilities that vulnerabilities will be exploited. Therefore, the level of risk increases.

Risk evaluation :	Are port	Are ports other than the ports anticipated open ?			
	YES	NO	RL total		
	X RL = 3		3		
	lf so, wh _1026,_ 		1028,_563	1	
	Is the po	ort 139	open ?		
	YES	NO	RL total		
	X RL = 3	-	6		
	TOTAL	RISK L	EVEL: [6	6]/6	

[5] Control objective :	Analysis of the sessions and the suspicious
	applications on the server.
Test location :	From the auditor station
	From the server audited
Tests to be conducted :	Pre-required : Having downloaded and installed on the audited ePO server, the latest version of Fport. Observe the following instructions:
- Stas	 4. Open a command line (cmd.exe) 5. Type the following line: netstat -an > 5-netstat.txt 6. Type the following line: fport /p > 5-fport.txt
Reference(s):	The Fport tool is available at no charge at the following
© Ť	address : http://www.foundstone.com/knowthedge/proddesc/fport .html
Expected results :	The results of netstat and of fport should not have recorded the presence of session or of suspicious application.
Objective / Subjective :	Objective
Results :	Extract of file « 5-netstat.txt » : (only the « listening » and « established »):

	Active Connections
	Proto Local Address Foreign Address State TCP 0.0.0.021 0.0.0.00 LISTENING TCP 0.0.0.080 0.0.0.00 LISTENING TCP 0.0.0.081 0.0.0.00 LISTENING TCP 0.0.0.0135 0.0.0.00 LISTENING TCP 0.0.0.01026 0.0.0.00 LISTENING TCP 0.0.0.01026 0.0.0.00 LISTENING TCP 0.0.0.01027 0.0.0.00 LISTENING TCP 0.0.0.01024 0.0.0.00 LISTENING TCP 0.0.0.01044 0.0.0.00 LISTENING TCP 0.0.0.01433 0.0.0.00 LISTENING TCP 0.0.0.02181 0.0.0.00 LISTENING TCP 0.0.0.02183 0.0.0.00 LISTENING TCP 0.0.0.2185 0.0.0.00 LISTENING TCP 0.0.0.2186 0.0.0.00 LISTENING TCP 0.0.0.2187 0.0.0.00 LISTENING TCP 0.0.0.2188 0.0.0.00 <td< th=""></td<>
GAX STRA	TCP 172.25.1.134:2188 172.25.1.134:1433 ESTABLISHED File content « 5-fport.txt » : FPort v1.33 - TCP/IP Process to Port Mapper Copyright 2000 by Foundstone, Inc. http://www.foundstone.com Pid Process Port Proto Path 1064 inandinfo -> 21 TCP C:WINNT\System32\inandsr\inandsr\inandinfo.exe 1436 NAIMSERV -> 80 TCP D:\ePO\2.0\NAIMSERV.EXE 1436 NAIMSERV -> 80 TCP D:\ePO\2.0\NAIMSERV.EXE 492 svchost -> 135 TCP C:\WINNT\system32\isvchost.exe 8 System -> 1026 TCP C:\WINNT\System32\inandsr\inandinfo.exe 164 inandinfo -> 1026 TCP C:\WINNT\System32\inandsr\inandinfo.exe 788 sqlservr -> 1028 TCP d:\ePO\MSSQL7\binn\sqlservr.exe 8 System -> 1044 TCP 788 sqlservr -> 2181 TCP D:\ePO\2.0\NAIMSERV.EXE 1436 NAIMSERV -> 2181 TCP D:\ePO\2.0\NAIMSERV.EXE 1436 NAIMSERV -> 2183 TCP D:\ePO\2.0\NAIMSERV.EXE 1436 NAIMSERV -> 2183 TCP D:\ePO\2.0\NAIMSERV.EXE 1436 NAIMSERV -> 2183 TCP D:\ePO\2.0\NAIMSERV.EXE

	File\Symant	tec\nc Anv	whore\awhost	32 010			
	File\Symantec\pcAnywhere\awhost32.exe 832 naimas32 -> 8081 TCP C:\EPOAgent\naimas32.exe						
	492 svchost -> 135 UDP C:\WINNT\system32\svchost.exe						
	8 System -> 137 UDP						
	8 System -> 138 UDP						
	8 System -> 445 UDP 268 Isass -> 500 UDP C:\WINNT\system32\Isass.exe						
	208 Isass	-> 50	025 UDP C:\\\			3	
	256 Service	-> 1	025 UDP C.		n32\service	es.exe	
	520 spools	V -> I	040 UDP C:		n32\spools	v.exe	
	1064 inandi	nto ->	3456 UDP C		em32\inand	asrvinandi	nto.exe
	580 awhos		5632 UDP				
			where\awhost				
Summary Brief	-		unknowns				-
explanation of risk :	applicati	ions tl	hat an	attacker	could	use	to his
	advanta	ge (ex :	a Trojan	horse).	6		
Risk evaluation :	Are ses	sions	that seen	n suspici	ous or	unnec	essary
	applicati	ions pre	esent?				-
	YES	NO	RL total	C.S.			
	X		4	0.2			
	RL = 4			<i>v</i>			
	t		No.	_			
	lf so, wh	nich?					
	•						
	Pcanywhere						
	TOTAL						
		KISK L	EVEL: [4 / 4			

TOTAL RISK LEVEL concerning the security of the operating system and the open sessions

40 / 48

3.3.2 Settings verification for various products

[6] Control objective :	Verification of the update level for ePolicy Orchestrator.
Test location :	From the auditor station
	From the server audited
Tests to be conducted :	Pre-required : Having obtained by the system
ST	administrator a user account and a valid password.
	Observe the following instructions:
	1. Open the « ePO » management console
	2. Choose « Login »
	 Register a user account, a valid password and choose « OK »
	4. When the window « Initializing » disappears
	Take a screen capture and save it in a
	Wordpad document under the name
	« 6-verepo.rtf »

Reference(s) :	A search on « version numbers, determining, software » on the online help for the ePO management console.			
	Information on the type of information leak : http://lists.insecure.org/lists/pen- test/2001/Nov/0006.html			
Expected results :	The version 2.5.0 SP1 (2.5.1 Build 213) of ePolicy Orchestrator should be installed in order to correct certain important information leak, like a user code and a valid password, via port 80, 81 and 8081.			
Objective / Subjective :	Objective			
Results :	Content of « 6-verepo.rft » :			
	ि 172-25.1.134 - Terminal Services Client (ePO Server)			
	¹ / ₂₀ Conside Window (Help			
	ePolicy Orchestrator 2.5.1.213			
	Manage Administrators Server Settings Network Associates Home Page			
	MCAFEE			
	THE VACCINE FOR E-BUSINESS			
Summon (Driof	<u>instant</u> 3 € <u>Sinteret information Serv.</u> <u>The Alex erables</u> <u>Distributions</u> <u>Distributions</u> <u>Distributions</u>			
Summary Brief explanation of risk :	As it is possible to obtain privilege information permitting authentification on the MSDE (or SQL)			
	database if the last update of the product is not			
, Co Y	installed, this would permit an attacker to take remotely			
	control of the database so far as port 1433 is not			
	scanned, to execute the code of his choice with the			
GY C	« CmdExec » function in order to take full control of the			
	server.			
Risk evaluation :	Is the version of the ePO server installed the version			
	2.5.1 Build 213 (or a more recent version) ?			
	YES NO RL total			
	X 0 RL = 5			
	TOTAL RISK LEVEL: [0]/ 5			

[7] Control objective :	Verification of the active system services on the ePolicy Orchestrator server.				
Test location :	From the auditor station From the server audited				
Tests to be conducted :	Pre-required : Having downloaded and installed on the audited ePO serve, the latest version of DumpSec.				
	Observe the following instructions:				
	 Open « DumpSec » Choose « Select Computer » in the menu « Report » and enter the IP address of the audited server. Choose « Dump Services » in the menu « Report ». 				
	 Be sure that all the options are selected and press on« OK ». 				
	 When the result is obtain, choose « Save Report As » of the menu « File » (or CRTL-S). 				
	 Choose the type « Fixed width cols » and save under the name « 7-services.txt » 				
Reference(s) :	The DumpSec tool is available at no charge at the following address : http://www.systemtools.com/somarsoft/				
Expected results :	There should only be the required services for the efficiency of the active ePO server operations.				
Objective / Subjective :	Objective, except for the application identification which is not necessary.				
Results :	Important extract of file « 7-services.txt » :				
Shar	2003-01-15 10:10 - Somarsoft DumpSec (formerly DumpAcl) - \\172.25.1.134 FriendlyName Name Status Type Account McAfee ePolicy Orchestrator 2.5.1 Server NAIMSERV2 Running Win32 LocalSystem MSSQLServer Running Win32 LocalSystem msSQLServer Running Win32 LocalSystem awhost32 Running Win32				
Summary Brief	LocalSystem The least active service on the server, fewer probability				
explanation of risk :	for an attacker to exploit a vulnerability to his advantage.				
Risk evaluation :	Are suspicious or unnecessary services used ?				
	YES NO RL total				
	X 4 RL = 4				

If so, which ?: Pcanywhere
TOTAL RISK LEVEL: [4]/4

[8] Control objective : Verification for presence of a functional antivirus on the ePO server. Test location : From the auditor station \Join From the server audited Tests to be conducted : Observe the following instructions: In order to know the version of the signature (.DAT) and the version for scanning engine : 1. Right button on the icon « NetShield » in the task bar. 2. Choose « Abort » 3. Take a screen capture and save in a Wordpad document under the name « 8-antivirus.rtf » In order to know the exact version of NetShield : 1. Open « regedit » 2. Find the following key : HKEY_LOCAL_MACHINE\SOFTWARE\Network Associates\TVD\NetShield NT\CurrentVersion\szProductVer 3. Make a note of NetShield version. version : **4.5.0.468.1** Observe the following instructions on the audited server in order to validate if the settings on the update have adequately been actived : 1. Right button on the icon« **NetShield** » in the task bar. 2. Choose « Console » 3. Click on « Automatic DAT Update » 4. Take a screen capture of the « Update **Options** » tab and save at the end of file « 8-antivirus.rtf »

	Observe the following instructions on the audited server in order to validate if the ePO agent is installed :
	 Choose « Internet Explorer » Type the following line in « Address » : http://localhost:8081 Take a screen capture and save at the end of file « 8-antivirus.rtf » Go to the end of the obtained document, Take a screen capture and save at the end of file « 8- antivirus.rtf »
Reference(s) :	Information in order to know the exact version of NetShield : Solution nai25980 - NetShield Version Information, dated September 10 th , 2002.
	Requires an access to « PrimeSupport KnowledgeCenter Service Portal » at the following address : <u>https://mysupport.nai.com</u>
Expected results :	Concerning the version for the installed product and the version of the signature (.DAT) :
	 The version of NetShield installed should be : 4.5.0.468.1 (or plus récent) The version Of « Scan Engine » should be : 4.1.60 (or more recent) The version of the signature (.DAT) should be the latest available at the following address : http://www.mcafeeb2b.com/naicommon/downlo ad/dats/find.asp
Ś	Concerning the settings for the update of the product :
o h h	 The option « Get from an FTP source » should be selected The IP address or the name of the audited FTP server (under the format FQDN) should be inscribed in the zone « Enter an FTP computer name and directory » The option « Use anonymous FTP login » should be selected.
	Concerning the information returned by Internet explored at the command « http://localhost:8081 » :
	 The version of the ePO agent installed should be : 2.5.1.213 (or more recent)

	- The three following lines should come back				
	periodically (according to the agent				
	configuration on the management) in the				
	« logs » of the ePO agent : 20030112115447: Agent: Enforcing policy for				
	NANDSHLD 4500				
	20030112115447: Agent: Enforcing policy for PCR 1.0.0				
	for Windows				
	20030112115448: Agent: Enforcing policy for NAI ePolicy				
	Orchestrator Agent				
Objective / Subjective :	Objective				
Results :	File content « 14-antivirus.rtf » :				
	About NetShield				
	NetShield for Windows NT and				
	Windows 2000 4.5				
	Serial Number: E000-50J6-UI66				
	Virus definitions: 4.0.4242				
	Created on: 11 January 2003. Scan engine: 4.1.60				
	Copyright © 1995-2001 Networks Associates Technology, Inc. All Rights Reserved.				
	Warning: this computer program is protected by copyright law and international				
	treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may				
	result in severe civil and criminal penalties, and will be prosecuted to the maximum				
	extent possible under the law.				
	Automatic Update/Upgrade Properties				
	Update Options Upgrade Options				
	Update your virus definition files from the local				
	network or from a remote computer.				
•	Select Transfer Method				
	C Copy from a local network computer				
	Enter an FTP computer name and directory:				
	epo. /dats/pc Default				
S.					
	Use logged on account UNC log n information				
	Use anonymous FTP login FTP login information				
6 A A	Use proxy server Port. 80				
\bigcirc	Log activity into the NetShield Activity Log File.				
	Schedule Advanced Update now				
	OK Cancel				

	II 17225.1.134 - Terminal Services Client (ePO Server) (영 ×) 월 erblicy Orchestrator Agent Log - Microsoft Internet Explorer (영 ×)
	Elle Edit View Favorites Icols Help
	⇔Back • ⇔ ~ © [2] [2] [2] @Search Te Fevorites @History [2] - ∰ Address @] <u>Interfloctionetextent</u>
	20020404085541: Agent: Generating Agent private key 20020404085543: Agent: Generating Agent public key
	20020404085543: Agent: Updating plug-in DLLs 20020404085543: Agent: Agent service is now running
	20020404085543: Agent: Checking MAC address 20020404085543: Agent: Checking computer name
	20020404085543: Agent: Generating Agent ID 20020404085543: Agent: Agent will attempt to connect to server in: 53 seconds
	20020404085543: Agent: Starting to collect Agent properties 20020404085543: Agent: Collecting properties for NAI ePolicy Orchestrator Agent
	20020404085636: Agent: Starting to collect Agent properties 20020404085636: Agent: Collecting properties for NAI ePolicy Orchestrator Agent
	20020404085636: Agent Attempting to connect to server 20020404085636: Agent Agent sending AgentPubKey
	20020404085638: Agent: Received package: PropsResponse 20020404085638: Agent: Event filter file updated
	20020404085638: Agent Task files updated 20020404085638: Agent Policy files updated
	20020404085638: Agent: Enforcing policy for NAI ePolicy Orchestrator Agent 20020404085638: Agent: Starting to collect Agent properties
	20020404083638. Agent: Collecting properties for NAI ePolicy Orchestrator Agent 20020404083639. Agent: More package(s) in the queue to send
	<log here="" truncated=""> properties for NETSHLD_4500</log>
	properties for APL STALL_=3.00 20021125171318. Agent: Collecting properties for NAI ePolicy Orchestrator Agent 20021125171318. Agent: Collecting properties for ALERTINNC4500
	2 Opening page http://local.ndost.i0081/
	Image: State of the Service Client (ePO Server) Image: Service Client (ePO Server) Image: Service Client (ePO Server)
	Befolicy Orchestrator Agent Log - Microsoft Internet Explorer If X Efe Edit Yew Egypointes
	⇔Back + ⇔ · ⊗ [2] [2] [2] [3] [3] Provintes [3] Priorites [3] Priorit
	20030115113644: Agent: Enforcing policy for PCR. 1.0.0 for Windows 20030115113644: Agent: Enforcing policy for NETSHLD_4500
	20030115113645: Agent: Enforcing policy for NAI ePolicy Orchestrator Agent 20030115113645: Agent: Next policy enforcement time: 11:51:45
	20030115115145: Agent: Enforcing policy for PCR. 1.0.0 for Windows 20030115115145: Agent: Enforcing policy for NETSHLD_4500
	20030115115145: Agent: Enforcing policy for NAI ePolicy Orchestrator Agent 20030115115145: Agent: Next policy enforcement time: 12:06:45
	20030115120645: Agent: Enforcing policy for PCR. 1.0.0 for Windows 20030115120645: Agent: Enforcing policy for NETSHLD_4500
	20030115120646 Agent: Enforcing policy for NAL ePolicy Orchestrator Agent 20030115120646: Agent: Next policy reforement ims. 122146
	20030115122002: Agent: Enforcing policy for PCR. 1.0.0 for Windows 20030115122002: Agent: Enforcing policy for NETSHLD_4500
	20030115122002: Agent: Enforcing policy for NAI ePolicy Orchestrator Agent 20030115122002: Agent: Starting to collect Agent properties
	20030115122003: Agent: Collecting properties for PCR 1.0.0 for Windows 20030115122003: Agent: Collecting properties for NETSHLD 4500
	20030115122004. Agent: Collecting properties for NAT ePolicy Orchestrator Agent 20030115122004. Agent: Collecting properties for ALERTMNVG4500
	20030115122004. Agent Agent attempting to connect to server 20030115122005. Agent Agent sending PropsVersion
	20030115122005. Agent: Received package: RequestProps 20030115122006. Agent: Received package: RequestProps
	20030115122006 Agent Agent sending IncProps
	20030115122006. Agent Server connection closed 20030115122006. Agent Server connection closed
	20030115122146. Agent Enforcing policy for DET 1.0 for Windows 20030115122146. Agent Enforcing policy for NETSHLD_4500
	20030115122146. Agent Informa policy for NAT ePolicy Orchettator Agent 20030115122146. Agent Informa policy enforment time: 12:3646
	2) Done
	Astart () () () () () () () () () () () () ()
Summary Brief	Having an antivirus solution that is not adequately up
explanation of risk :	to date is more vulnerable to infection than an antivirus
	rigorously updated.
	An anti-inco addition much the set for a barrant t
	An antivirus solution must therefore be present on an
	antivirus server such as ePO in order to be sure that it
	does not become a centralized distribution virus
	console.

Risk evaluation :		version o 468.1 ?	f NetShiel	d installed at least the version
	YES	NO	RL total	
	X	RL = 4	0	
		version c n 4.1.60		Engine » installed at least the
	YES	NO	RL total	A CONTRACTOR OF THE OWNER OWNER OF THE OWNER OWNER OWNER OWNER OF THE OWNER OWNE OWNER OWNE
	x	RL = 4	0	
	ls the availa	version o ble the da	of the signa ay of the a	ture (.DAT) the latest version udit ?
	YES	NO	RL total	
	x	RL = 4	0	
	Is the	option «	Get from a	n FTP source » selected ?
	YES	NO	RL total	
•	×	RL = 3	0	
115	lf not,	what is th	ne configur	ration ? :
A Contraction of the second se				
O P	audite	ed (under	a format	e name of the FTP server FQDN) inscribed in the zone name and directory » ?
	YES	NO	RL total	
	x	RL = 3	0	

<u> </u>			
If not, w	hat is tl	ne configui	ration ? :
<u> </u>			
		· · · · · · · · · · · · · · · · · · ·	
	· · · · · · · · ·		
Is the o	ption «	Use anony	mous FTP login » selected ?
YES	NO	RL total	
	NO		
x		0	
	RL = 3	_	20
If not, w	/hat is tl	ne account	used ? :
<u> </u>			
		•	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
ls the v	ersion c	f the ePO	agent installed at least the
version			agent motalies at least the
	NO		
YES	NU	RL total	
x		0	
	RL = 3		
	- V		1
If not, w	hat is tl	ne version	?:
	41a	- II i I'-	
			nes come periodiquely in the the ePO agent?
« logs » 2003011			5
NANDSH	ILD_450	D	
		Agent: En	forcing policy for PCR 1.0.0 for
2003011		Agent: E	nforcing policy for NAI ePolicy
Orchestra	ator Ager	nt	
YES	NO	RL total	
x _	RL = 4	0	
	RL - 4		
16 1	h = 1 =	(h 1) .	
if not, w	/nat are	the results	s obtained :
	· · · · · · · ·	· · · · · · · · · · · · · · ·	
TOTAL	RISK L	EVEL: [0)] / 28

[9] Control objective :	Verification of the basic settings for Internet Information Server (IIS)
Test location :	From the auditor station
	From the server audited
Tests to be conducted :	Observe the following instructions:
	 Open « Internet Service Manager » via Start – Programs – Administrative Tools. Right button on « Default FTP Site » Choose « Properties » Take a screen capture of each tabs (FTP Site,
	Security Accounts, Messages, Home
	Directory and Directory Security) and save it
Reference(s):	in a Wordpad file under the name « 9-ftp.rtf » Not applicable / Personal experience
Expected results :	Concerning the configuration of IIS :
	concerning the configuration of no .
	In the tab « FTP Site »
	- The connexion number should be limited to the
	station/server number needing an update.
	 The option « Enable Logging » should be
	selected
	In the tab « Security Accounts » :
	 The option « Allow Anonymous Connections » should be selected and also check mark for « Allow only anonymous connections ». Only the group « Administrators » should be visible In the section« Operators ».
	In the tab « Messages » :
Les Y	 A legal message should be inscribed in the section «Welcome »
O Pr	 In the tab « Home Directory » : The option « a directory located in this computer » should be selected The directory « Ftproot » should not be found on the same driver as the operating system. Only the option « Read » and « Log visits » should be selected.
	In the tab « Directory Security » : - The option « Denied Access » should be selected.

access the FTP server should be written. bjective / Subjective : Objective esults : File content « 9-ftp.rtf » :	[· · · · · · · · · · · · · · · · · · ·
bjective / Subjective : Objective esults : File content « 9-ftp.rtf » : Default FTP Site Properties ? X FTP Site Security Accounts Messages Home Directory Directory Security Identification Default FTP Site : [All Unassigned] ICP Port: 21 Connection Cunnection Connection Connection 1000 seconds Pable Logging		
esults : File content « 9-ftp.rtf » :		
esults : File content « 9-ftp.rtf » :	Objective / Subjective :	
Default FTP Site Properties ? × FTP Site Security Accounts Messages Home Directory Directory Security Identification	Results :	File content « 9-ftp.rtf » :
FTP Site Security Accounts Messages Home Directory Directory Security Identification		
Identification Description: Default FTP Site JP Address: (All Unassigned) ICP Port: 21 Connection Cultimited © Limited To: 5,000 connections Connection Timeout: 900 seconds		Default FTP Site Properties ? 🗙
Identification Description: Default FTP Site JP Address: (All Unassigned) ICP Port: 21 Connection Cultimited © Limited To: 5,000 connections Connection Timeout: 900 seconds		FTP Site Security Accounts Messages Home Directory Directory Security
Description: Default FTP Site JP Address: (All Unassigned) ICP Port: 21 Connection ✓ Únlimited ✓ ✓ Limited To: 5,000 Connection Timeout: 900 Seconds ✓		
IP Address: (All Unassigned) ICP Port: 21 Connection C Unlimited C Limited To: 5,000 connections Connection Timeout: 900 seconds IF Enable Logging		
ICP Port: 21 Connection C Unlimited Imited C Limited To: Downection S Connection Timeout: 900 seconds		
Connection C Unlimited C Limited To: 5,000 connections Connection Timeout: 900 seconds F✓ Enable Logging		
C Unlimited C Limited To: 5,000 connections Connection Timeout: 900 900 seconds		
Imited To: 5,000 connections Connection Timeout: 900 seconds IV Enable Logging		Connection
Connection Timeout: 900 seconds ✓ Enable Logging		
Enable Logging		
Active log format:		
W3C Extended Log File Format Properties		W3L Extended Log File Format
		Current Sessions
Current Sessions		
Current Sessions		OK Cancel Apoly Help
Current Sessions OK. Cancel Apply Help		
OK Cancel Apply Help		
OK Cancel Apply Help Default FTP Site Properties ? ×		FTP Site Security Accounts Messages Home Directory Directory Security
OK Cancel Apply Help		Allow Anonymous Connections
OK Cancel Apply Help Default FTP Site Properties ? × FTP Site Security Accounts Messages Home Directory Directory Security		Select the Windows User Account to use for anonymous access to this resource
OK Cancel Apply Help Default FTP Site Properties ? × FTP Site Security Accounts Messages Home Directory Directory Security Image: Allow Anonymous Connections Image: Allow Anonymous Connections Image: Allow Anonymous Connections Image: Allow Anonymous Connections		Username: UUSB_SCOBEPO01Browse
OK Cancel Apply Help Default FTP Site Properties ? × FTP Site Security Accounts Messages Home Directory Directory Security Image: Allow Anonymous Connections Select the Windows User Account to use for anonymous access to this resource		
OK Cancel Apply Help Default FTP Site Properties ? × FTP Site Security Accounts Messages Home Directory Directory Security Image: Allow Anonymous Connections Select the Windows User Account to use for anonymous access to this resource Username: USR_SCOREPO01 Browse		L'assyudia.
OK Cancel Apply Help Default FTP Site Properties ? × FTP Site Security Accounts Messages Home Directory Directory Security ✓ Allow Anonymous Connections Select the Windows User Account to use for anonymous access to this resource Username: [USR_SCOREP001 Browse Password: Password:	2	
OK Cancel Apply Help Default FTP Site Properties ? × FTP Site Security Accounts Messages Home Directory Directory Security Image: Allow Anonymous Connections Select the Windows User Account to use for anonymous access to this resource Browse Bername: IUSR_SCOREP001 Browse Password: Allow only anonymous connections	6	Allow II's to control password
OK Cancel Apply Help Default FTP Site Properties ? × FTP Site Security Accounts Messages Home Directory Directory Security ✓ Allow Anonymous Connections Select the Windows User Account to use for anonymous access to this resource Username: [USR_SCOREP001 Browse Password: Password:		FTP Site Operators
OK Cancel Apply Help Default FTP Site Properties Image: Control password Image: Control password FTP Site Security Accounts Messages Home Directory Directory Security Image: Mage: Account Security Image: Control password Image: Control password Image: Control password FTP Site Operators Image: Control password Image: Control password Image: Control password		Grant operator privileges to Windows User Accounts for this FTP site only.
OK Cancel Apply Help Default FTP Site Properties 2 × FTP Site Security Accounts Messages Home Directory Directory Security ✓ Allow Anonymous Connections Select the Windows User Account to use for anonymous access to this resource Username: IUSR_SCOREP001 Browse ✓ Allow only anonymous connections ✓ Allow IIS to control password FTP Site Operators Allow IIS to control password	A. 2	Operators: Administrators Add
OK Cancel Apply Help Default FTP Site Properties 2 × FTP Site Security Accounts Messages Home Directory Directory Security ✓ Allow Anonymous Connections Select the Windows User Account to use for anonymous access to this resource Username: IUSR_SCOREP001 Browse ✓ Allow only anonymous connections ✓ Allow IIS to control password FTP Site Operators Allow IIS to control password		Bemove
OK Cancel Apply Help Default FTP Site Properties 2 × FTP Site Security Accounts Messages Home Directory Directory Security ✓ Allow Anonymous Connections Select the Windows User Account to use for anonymous access to this resource Username: IUSR_SCOREP001 Browse ✓ Allow only anonymous connections ✓ Allow IIS to control password FTP Site Operators Allow IIS to control password		
OK Cancel Apply Help Default FTP Site Properties 2 × FTP Site Security Accounts Messages Home Directory Directory Security ✓ Allow Anonymous Connections Select the Windows User Account to use for anonymous access to this resource Username: IUSR_SCOREP001 Browse ✓ Allow only anonymous connections ✓ Allow IIS to control password FTP Site Operators Allow IIS to control password	P	
OK Cancel Apply Help Default FTP Site Properties 2 × FTP Site Security Accounts Messages Home Directory Directory Security ✓ Allow Anonymous Connections Select the Windows User Account to use for anonymous access to this resource Username: IUSR_SCOREP001 Browse ✓ Allow only anonymous connections ✓ Allow IIS to control password FTP Site Operators Allow IIS to control password	\odot	
OK Cancel Apply Help Default FTP Site Properties ? × FTP Site Security Accounts Messages Home Directory Directory Security Image: Properties ? × Image: Properties Properties Image: Properties Properties Image: Properties Properties Image: Properties Properties		OK Cancel Apply Help
DK Cancel Apply Help Default FTP Site Properties Image: Connections Image: Connections Image: Connections FTP Site Security Accounts Messages Home Directory Directory Security Image: Connections Image: Connections Image: Connections Select the Windows User Account to use for anonymous access to this resource Image: Connections Image: Connections Image: Connections Image: Connections Image: Connections Image: Connections Image: Connections Image: Connections Image: Connections Image: Connections Image: Connections Image: Connections Image: Connections Image: Connections Image: Connections Image: Connections Image: Connections Image: Connections Image: Connections Image: Connections Image: Connections Image: Connections Image: Connections Image: Connections Image: Connections Image: Connections Image: Connections Image: Connections Image: Connections Image: Connections Image: Connections Image: Connections Image: Connections Image: Connections Image: Connections Image: Connections Image: Connections Image: Connections Image: Co	1	51 51 1000 1000 1000 100
		OK Cancel Apply Help Default FTP Site Properties ? × FTP Site Security Accounts Messages Home Directory Directory Security ✓ Allow Anonymous Connections Select the Windows User Account to use for anonymous access to this resource Browse Username: IUSR_SCOREP001 Browse Password Control password FTP Site Operators Grant operator privileges to Windows User Accounts for this FTP site only. Operators: Administrators Add
		☐ Enable Logging
		Connection Timeout: 900 seconds
Enable Logging		C Limited To: 5,000 connections
Connection Timeout: 900 seconds ✓ Enable Logging		C Unlimited
Imited To: 5,000 connections Connection Timeout: 900 seconds IV Enable Logging		Connection
C Unlimited C Limited To: 5,000 connections Connection Timeout: 900 900 seconds		ICP Port: 21
Connection C Unlimited C Limited To: 5,000 connections Connection Timeout: 900 seconds F✓ Enable Logging		
ICP Port: 21 Connection C Unlimited Image: Connection S Limited To: 5,000 connection Timeout: 900 seconds		IP Address: [All Linessigned]
ICP Port: 21 Connection C Unlimited Image: Connection S Limited To: 5,000 connection Timeout: 900 seconds		Description: Default FTP Site
IP Address: (All Unassigned) ICP Port: 21 Connection C Unlimited C Limited To: 5,000 connections Connection Timeout: 900 seconds IF Enable Logging		Identification
Description: Default FTP Site JP Address: (All Unassigned) ICP Port: 21 Connection ✓ Únlimited ✓ ✓ Limited To: 5,000 Connection Timeout: 900 Seconds ✓		FTP Site Security Accounts Messages Home Directory Directory Security
Identification Description: Default FTP Site JP Address: (All Unassigned) ICP Port: 21 Connection Cultimited © Limited To: 5,000 connections Connection Timeout: 900 seconds		
FTP Site Security Accounts Messages Home Directory Directory Security Identification		
FTP Site Security Accounts Messages Home Directory Directory Security Identification	Results :	File content « 9-ftp.rtf » :
Default FTP Site Properties ? × FTP Site Security Accounts Messages Home Directory Directory Security Identification	Objective / Subjective :	
esults : File content « 9-ftp.rtf » :		access the FTP server should be written.
bjective / Subjective : Objective esults : File content « 9-ftp.rtf » : Default FTP Site Properties ? X FTP Site Security Accounts Messages Home Directory Directory Security Identification Default FTP Site : [All Unassigned] ICP Port: 21 Connection Cunnection Connection Connection 1000 seconds Pable Logging		 A list of the IP addresss that have the right to
access the FTP server should be written. bjective / Subjective : Objective esults : File content « 9-ftp.rtf » :		

	FTP Site Security Accounts Messages Home Directory Directory Security
	Welcome:
	You are now connected to a system owned By connecting and using this system, you engage yourself to respect the corporate security policy. This system is monitored and illegal used of it will be prosecuted. Vous êtes maintenant connecté à un système appartenant au En vous connectant et utilisant ce système, vous vous engagez à respecter la politique de sécurité de l'entreprise. Ce système est sous surveillance et un usage illicite de celui-ci entraînera des poursuites.
	Egit
	Maximum Connections:
	OK Cancel Apply Help
	Default FTP Site Properties ? 🗙
	FTP Site Security Accounts Messages Home Directory Directory Security When connecting to this resource, the content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come
	FTP Site Security Accounts Messages Home Directory Directory Security When connecting to this resource, the content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come from: Image: Content should come
	FTP Site Security Accounts Messages Home Directory Directory Security When connecting to this resource, the content should come from: a girectory located on this computer a share located on another computer FTP Site Directory Local Path: E:\ftproot Browse Paed Write Write
	FTP Site Security Accounts Messages Home Directory Directory Security When connecting to this resource, the content should come from: a directory located on this computer a share located on another computer FTP Site Directory a share located on another computer FTP Site Directory Local Path: E:\ftproot Browse Ø Bead Ø Write Log visits Directory Listing Style
	FTP Site Security Accounts Messages Home Directory Directory Security When connecting to this resource, the content should come from: a glirectory located on this computer a share located on another computer FTP Site Directory g another computer E: Ntproot Browse Bead Write Log yisits Directory Listing Style UNIX ●
	FTP Site Security Accounts Messages Home Directory Directory Security When connecting to this resource, the content should come from: a glirectory located on this computer a share located on another computer FTP Site Directory g another computer E: Ntproot Browse Bead Write Log yisits Directory Listing Style UNIX ●
	FTP Site Security Accounts Messages Home Directory Directory Security When connecting to this resource, the content should come from: a glirectory located on this computer a share located on another computer FTP Site Directory g another computer E: Ntproot Browse Bead Write Log yisits Directory Listing Style UNIX ●
Sha	FTP Site Security Accounts Messages Home Directory Directory Security When connecting to this resource, the content should come from: a directory located on this computer a share located on another computer FTP Site Directory Browse E:\typroot Browse Ø Bead Ø Write Log yisits Directory Listing Style MS-DOS ● MS-DOS ● MS-DOS ●

	Default FTP Site Properties			
	FTP Site Security Accounts Messages Home Directory Directory Security TCP/IP Access Restrictions By default, all computers will be: Image: Comparison of the second secon			
Summary Brief explanation of risk :	A configuration mistake on the FTP server could permit an attacker to use to his advantage this weakness in order to corrupt the files of the update and at the same time to upload some applications to the server potentially permitting him, if combine with an other attack, to take control of the server.			
Risk evaluation :	Is the connexion number limited to the station/server			
	requirering an update ?			
	YESNORL totalX2RL = 2			
	Is the option « Enable Logging » selected ?			
	YES NO RL total			
	X 2 RL = 3			
	Is the option « Allow Anonymous Connections » selected and also the option « Allow only anonymous connections » ?			
	YES NO RL total			
	X 4 RL = 2			

		up « Administrators » present in the
	section« Opera	RL total
	X RL = 4	4
	ls a legal «Welcome » ?	message inscribed in the section
	YES NO	RL total
	X RL = 2	4
	Is the option of selected ?	« a directory located in this computer »
	YES NO	RL total
	X RL = 2	4
	Is the directory as the operation	A style st
	YES NO	RL total
	RL = 3 X	4
	Is only the opti ?	tion « Read » and « Log visits » selected
2°	YES NO	RL total
OT O	X RL = 2	6
	Is the option «	Denied Access » selected?
	YES NO	RL total
	X RL = 3	9

		the IP add server exi	dresss that st ?	have the	right to
YES	NO	RL total			
	X RL = 3	12			
тота	L RISK L	EVEL: [1	2]/26		

[9] Control objective :	Verification of the ePO agent settings
Test location :	From the auditor station
	From the server audited
Tests to be conducted :	Pre-required : Having obtained from the system administrator a user account and a valid password.
	Observe the following instructions:
	 Open the « ePO » management console Choose « Login »
	 Register a user account, a valid password and Choose « OK »
	 Once the window « Initializing » disappears, Choose « Directory »
	5. Choose « ePO Orchestrator Agent »
	6. Take a screen capture and save in a Wordpad
	document under the name « 9-ePOAgent.rtf »
	7. Double click on« ePO Orchestrator Agent » and
	choose « Configuration ».
	8. Take a screen capture of the tab « Agents
	Options » also « Event Options » and save at
	the end of file « 9-ePOAgent.rtf ».
Reference(s) :	Not applicable / Personal experience
Expected results :	The option « Enforce Policies for ePolicy
Expected results .	Orchestrator Agent » must be selected.
	orchestrator Agent // must be selected.
	In the tab « Agent Options » :
	The option « Prompt user when software
	installation requires reboot » should be ideally selected.
	The option « Enable Agent to server communication » must be selected with a reasonable delay (ex : 60 minutes by default).

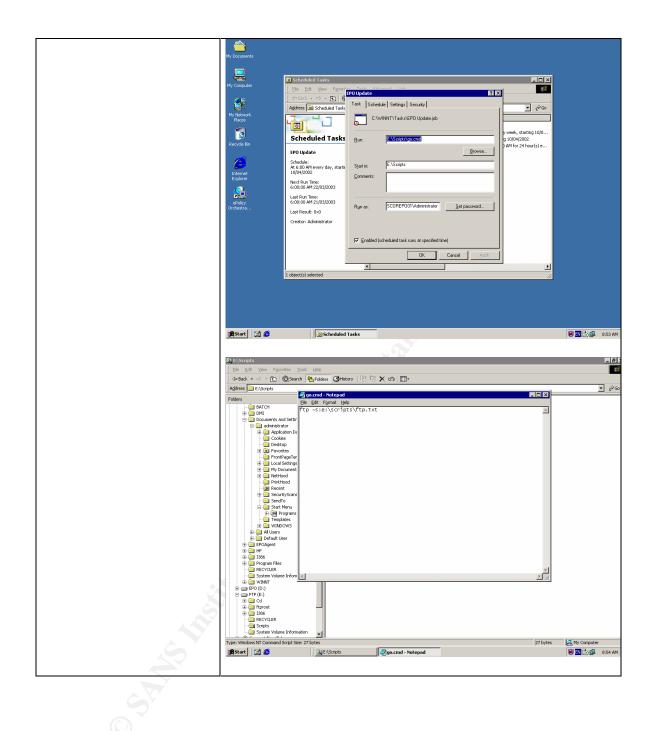
	The option « Enable agent Wakeup call support »				
	must be selected.				
	In the tab « Event Options » :				
	A reasonable delay (depending on the size of the company) can be entered in the zone « Interva between immediate upload ». Ideally, shorter the delay will be, faster the alerts will be corrected.				
Objective / Subjective :	Objective				
Results :	File content « 9-ePOAgent.rtf » :				
	Ta McAfee ePolicy trchestrator				
	}} Conside Window Help				
	Time Policies Properties Tasks ■ MA/Re Image: Source with the source withe source with the source with the source withe source				
	Image: Directory Image: ePO Agent of Webrield Applance Image: Direc				
	E ∰ NeShida V 5 for Wrdows E @ Noto-kelving Coporate Brinn 75x/7.6				
	ePolicy Orchestrator Agent				
	Agent Options				
	Agent General Options IF Enforce Policies for ePolicy Orchestrator Agent				
	Арру				
	Sobjects				
	Jfstant 」 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2				
	Terretaire thelicy Orchestrator)資 Concolo Window Help				
	Action yew \$e → \$E \$ 20 } 2 \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$				
	MArke Breatony Br				
	□ □ </th				
	Engling Insular for VunScen TC Engling NeSheld v4.03 for Windows ⊕ MeSheld v4.5 for Vindows				
5	Agent Options				
6 V	General Options				
	 Software Installation Ø Prompt user when software installation requires reboot. 				
	Automatic reboot with timeout Seconds Agent Communication Intervals				
	Policy Enforcement Interval every 15 nimites				
	Enable Agent to server communication every [60 minutes				
	Agent Wakeup Call				
	Solpeds JAStart J A & BASAM				

	'∰ McAfee ePolicy Urchestrator
	The Console Window Help
	Action View ← ⇒ C W C C C
	Tree Policies Properties Tasks
	By ePolcy Orchestrator (SCOREPCO1) C B ePolcy Dichestrator Agent breactory Configuration
	E 🐴 Repository E 🐨 ePO Agent for Webshield Appliance
	WebImmune McAfee Desktop Firewall 7.5
	😥 🧰 GroupShield Domino 5.0
	e
	Agent Options Event Options
	□ Inherit
	□ Event forwarding settings □ Enable event upload.
	Event Priority Informational 🖃 and above.
	Interval between immediate uploads 15 minutes
	Maximum events per immediate upload 200
	Sobjects Sobjec
Summary Brief	A bad configuration of the ePO agent could render it a
explanation of risk :	little or completely inefficient and even prevent any
explanation of hold.	
	reaction if a major incident would arise.
Risk evaluation :	
RISK EVALUATION .	
	Orchestrator Agent » selected ?
	YES NO RL total
	X 0
	RL = 4
	Is the option « Prompt user when software installation
	requires reboot » selected ?
	requires repoor » selected ?
•	YES NO RL total
	X 0
	RL = 2
	Is the option « Enable Agent to server
<u>C</u> Y	communication » selected with a reasonable delay
	(ex : 60 minutes by default) ?
	YES NO RL total
	X 0
	RL = 4
	If not, what is the delay ? :
1	

	the option lected ?	« Enable a	agent Wakeup call support »
Y	ES NO	RL total	
	X RL = 4	0	
siz			depending on the company « Interval between immediate
Y	ES NO	RL total	
	X RL = 2	0	SIT
lfr	not, what is	the delay?	S
тс	OTAL RISK	LEVEL: [0)] / 16

[10] Control objective :	Verification of the process for the update of the ePO server
Test location :	From the auditor station From the server audited
Tests to be conducted :	The ePO server does not have an integrated mechanism in order to update the files of the signature (.DAT).
	The system administrator may have to choose different kind of way in order to carry out this task. Therefore you must ask the administrator what is the process he uses for the update and adapt this section accordingly.
0	In the present case, the system administrator as chosen to automate this task using a combination of « Scheduled Tasks » and command files (.BAT) in order to make the FTP transferts between the FTP servers of the Network Associate and the server audited.
	Observe the following instructions:
	Take some screen captures of all the pertinent mechanisms in the process for the update and save it in a Wordpad file under the name « 10-update.rtf »

	In the present case :	
	 A screen capture of the « Scheduled Tasks » A screen capture of the command files 	
Reference(s) :	Not applicable / Personal experience	
Expected results :	The process for the update must be entire automated.	ely
	Journals (« logs ») must be available in order validate that the process works well.	to
	The structure on the audited FTP server must be a faithful as possible to the FTP server of NAI.	as
Objective / Subjective :	Subjective	
Results :	File content « 10-update.rtf » :	
	Wy Documents Wy Conjurners Wy Comparison Wy Comparison Wy Comparison Wy Baharaka Wy Baharaka	
	4 bject(s)	
Ś		
	資 start 」 ① 参	8:52 AM
O STA	<u></u>	

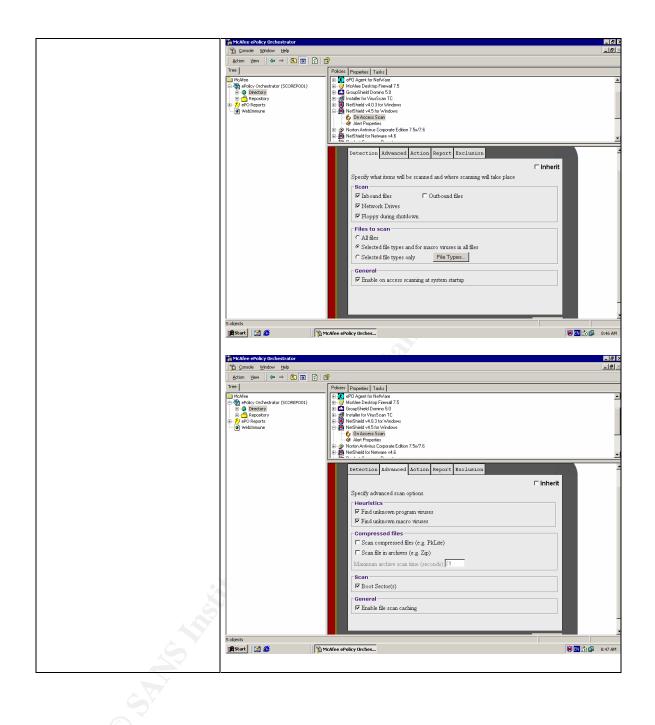


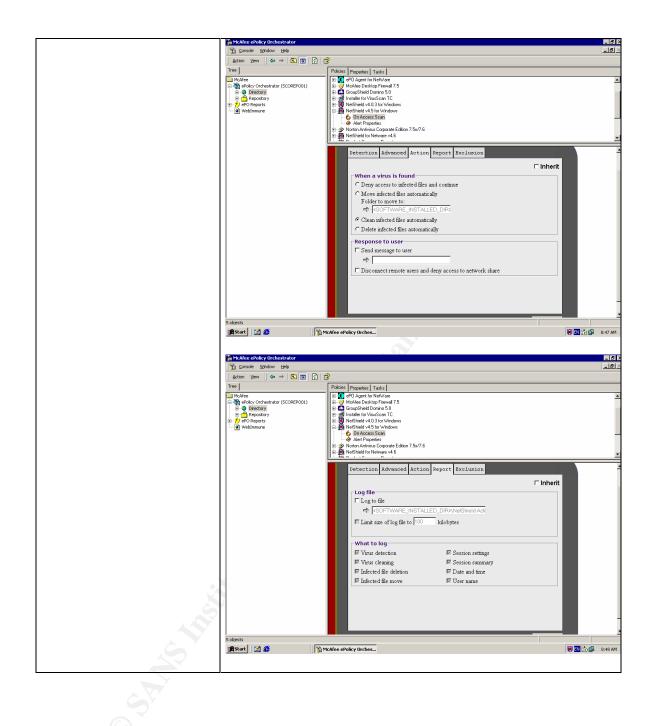
	Wy Documents Wy Documents Wy Concurse Phy Box Documents Wy Concurse Phy Box Documents Wy Documents Wy Concurse Phy Box Documents Wy Documents
Cummor: Drief	in ander to appure an officiant undets of the aptivity of
Summary Brief explanation of risk :	In order to assure an efficient update of the antivirus, the antivirus server must be rigorously updated. If the process does not permit an efficient update, the infection probabilities will be higher.
Risk evaluation :	Is the update process entirely automated ?
	YES NO RL total X 0 If not, explain the process :
	Are the journals (« logs ») available in order to validate
	the process is working correctly ?
	YES NO RL total
	X 3 RL = 3
	Is the structure on the audited FTP server faithful or close to the FTP server of NAI?
	YES NO RL total
	X RL = 3 3

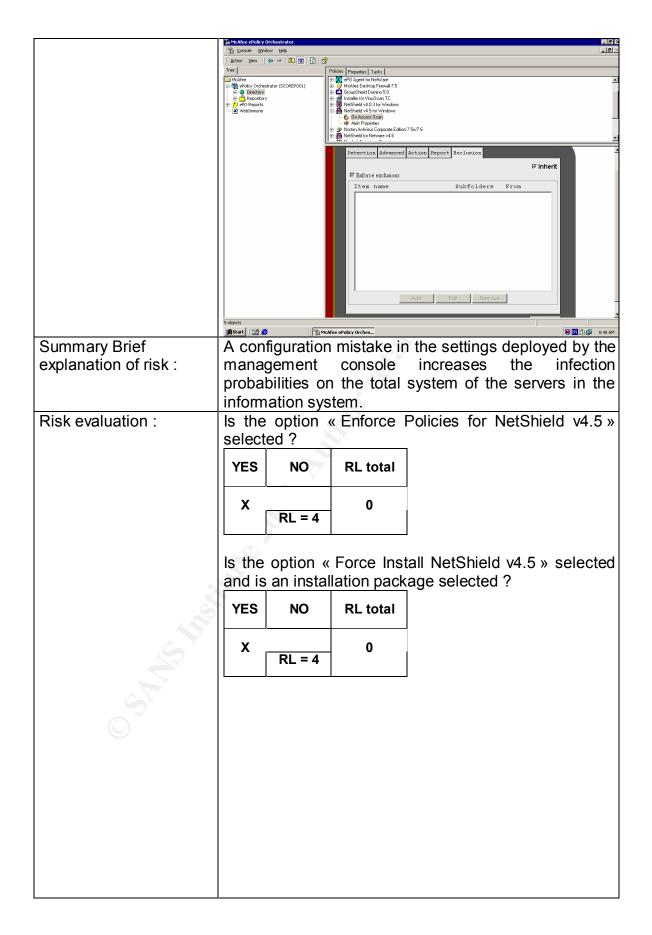
If not, explain what file is available for the update :
 TOTAL RISK LEVEL: [3] / 10

[**11**] Control objective : Verification of the settings for NetShield 4.5 deployed by the ePO management console. From the auditor station Test location : \boxtimes From the server audited **Pre-required** : Having obtained from the system Tests to be conducted : administrator a user account and a valid password. Observe the following instructions: 1. Open the « **ePO** » management console 2. Choose « Login » 3. Register a users account, a valid password and Choose « OK » 4. Once the window « Initializing... » disappears, choose « NetShield v4.5 for Windows » 5. Take a screen capture and save in a Wordpad file under the name « 11-NetShield.rtf ». 6. Choose « On Acces Scan » 7. Take a screen capture of each of the tabs available (« Detection », « advanced », « action », « report » and « exclusion ») and save at the end of file « 11-NetShield.rtf ». Not applicable / Personal experience Reference(s): Expected results : In « Installation Options » : The option « Enforce Policies for NetShield v4.5 » must be selected. The option « Force Install NetShield v4.5 » must be selected and an installation package must be selected. In the tab « Detection » : At least the following options must be selected : Scan « Inbound File » Scan « Network Drive »

	- Selected file type only
	- Enable on acces scanning at system startup
	The remaining options can be selected, but an impact on the system performance as to be evaluated.
	In the tab « Advance » :
	All should be selected, however for performance reason the options in the zone « Compressed File » can be deactivated.
	In the tab « Action » :
	Only « Clean infected file automatically » is necessary.
	In the tab « Report » and « Exclusion » :
	Nothing as to be activated and no exclusion should be defined.
Objective / Subjective :	Objective
Results :	File content « 11-NetShield.rtf » :
	ික MtAfee ePolicy Otchestrator [6] ව ික Console - Window Help
	Image Active
•	NetShield v4.5 for Windows
L. L	Wetsmeid v4.5 for windows McAree
	Installation Options
S	Fenforce Policies for NetShield v4.5 for Windows Install options Force Install NetShield v4.5 for Windows
O P P	Intail Packare. NETShield v4.5 for Windows Select. □ Force Uninstall NetShield v4.5 for Windows
O T	Apply
	S objects Restart R







	Are at least the following options selected in the tab « Detection » ?							
	 Scan « Inbound File » Scan « Network Drive » Selected file type only Enable on acces scanning at system startup 							
	YES NO RL total							
	X RL = 4 0							
	If not, which are missing ? :							
	Are all the options selected in the tab « Advance » ? (do not consider the zone « Compressed File »).							
	YES NO RL total							
	X 0 RL = 3							
	If not, which are missing ? :							
	Is at least « Clean infected file automatically selected in the tab « Action » ?							
	YES NO RL total							
\bigcirc	X 0 RL = 3							
	If not, what is the default action ? :							

	lave Exclus			bee	n de	efined	in	the	tab
	YES	NO	RL to	otal					
	RL = 2	X	0						
lf	so, exp	plain th	e exclu	usior	าร :	N.			
-									
- T	OTAL I	RISK L	EVEL	:[0] / 20	0			

TOTAL RISK LEVEL Concerning the configurations of various products

19 / 109

3.3.3 Access rights verification

[12] Control objective :	Verification of the users account available on the ePO server.					
Test location :	From the auditor station From the server audited					
Tests to be conducted :	Pre-required : Having downloaded and installed on the audited ePO server, the latest version of DumpSec. Observe the following instructions:					
6 A CAN	 Open « DumpSec » Choose « Select Computer » in the menu « Report » and enter the IP address of the audited server. Choose « Dump Users as columm » in the menu « Report ». Add all the fields available and Press on« OK ». Once the result is obtained, choose « Save Report As » of the menu « File » (or CRTL-S). Choose the type « Fixed width cols » and save under the name « 12-users.txt » 					
Reference(s) :	The DumpSec tool is available at no charge at the following address : http://www.systemtools.com/somarsoft/					

Expected results :	 The account « Guest » should be deactivated and renamed for something less explicit. The account « administrator » should be renamed for something less explicit. The default account for IIS « IUSR_computername » should be renamed
	for something less explicit. - A service account for the ePO server should be
	 present. A service account for the saving software (ex : BackupExec) can be present. A service account for a remote access software
	(ex : Terminal Service) can be present.
Objective / Subjective :	Objective
Results :	File content « 12-users.txt » :
	2003-01-15 09:57 - Somarsoft DumpSec (formerly DumpAcl) - \\172.25.1.134 UserName
Share	Administrator Grops Administrators (Local, Administrators have compthande and URThetricted access to the computer/domain) AccountType User HomeDrive HomeDrive HomeDir Profile LogonScript Workstations PswdCanBeChanged Yes PswdLastSandTime PswdExpires No PswdExpires No AcctExpiresTime Never AcctLockedOrt No AcctExpiresTime Never LastLogonServer 172.25.1.134 LogonHorrs All Sid S-1-5-21-1715567821-682003330-725345543-500 RasDialin No RasCallback Noe RasCallbackNumber FullName Comment Built-in account for administering the computer/domain Backupexec_svr Grorps Grorps Administrators (Local, Administrators have compthande and uRThetricted access to the computer/domain) Grorps Backup Operators (Local, Backup Operators can override security restrictions for the sothe purpose of backing up or restoring file) AccountType User HomeDir Profile LogonScript

	AcctLockedOrt No
	AcctExpiresTime Never
	LastLogonTime 2002-09-04 08:42
	LastLogonServer 172.25.1.134 LogonHorrs All
	LogonHorrs All Sid S-1-5-21-1715567821-682003330-725345543-1005
	RasDialin No
	RasCallback Noe
	RasCallbackNumber
	Comment Guest
	Grorps Guests (Local, Guests have the same access as members of the Users grorp by default, except for the Guest account which is further
	restricted)
	AccountType User
	HomeDrive
	HomeDir
	Profile
	LogonScript
	Workstations
	PswdCanBeChanged No
	PswdLastSandTime Never
	PswdPre-required No
	PswdExpires No
	PswdExpiresTime ?Unknown
	AcctDisabthed Yes
	AcctLockedOrt No
	AcctExpiresTime Never
	LastLogonTime Never
	LastLogonServer 172.25.1.134
	LogonHorrs All
	Sid S-1-5-21-1715567821-682003330-725345543-501
	RasDialin No
	RasCallback Noe
	RasCallbackNumber
	FullName
	Comment Built-in account for guest access to the computer/domain
	IUSR_SCOREPO01
	Grorps Guests (Local, Guests have the same access as members of
	the Users grorp by default, except for the Guest account which is further
	restricted)
	AccountType User
	HomeDrive
	HomeDir
	Profile
	LogonScript
	Workstations PswdCanBeChanged No
	PswdLastSandTime 2002-04-02 14:36
	PswdPre-required No
	PswdExpires No
	PswdExpires Time Never
	AcctDisabthed No
Gy	AcctLockedOrt No
O PAR	AcctExpiresTime Never
(\bigcirc)	LastLogonTime 2003-01-15 04:58
	LastLogonServer 172.25.1.134
	LogonHorrs All
	Sid S-1-5-21-1715567821-682003330-725345543-1001
	RasDialin No
	RasCallback Noe
	RasCallbackNumber
	FullName Internet Guest Account
	Comment Built-in account for anonymous access to Internet Information
	Services
	SQLAgentCmdExec
	Grorps Users (Local, Users are prevented from making accidental or
	intentional system-wide changes. Thus, Users can run certified applications,
	but not most thegacy applications)

	AccountType User
	HomeDrive HomeDir C:\Documents and Settings\administrator
	Profile
	LogonScript
	Workstations
	PswdCanBeChanged No
	PswdLastSandTime 2002-04-03 11:31
	PswdPre-required Yes PswdExpires No
	PswdExpires No
	AcctDisabthed No
	AcctLockedOrt No
	AcctExpiresTime Never
	LastLogonTime Never
	LastLogonServer 172.25.1.134
	LogonHorrs All Sid S-1-5-21-1715567821-682003330-725345543-1004
	RasDialin No
	RasCallback Noe
	RasCallbackNumber
	FullName SQLAgentCmdExec
	Comment SQL Server Agent CmdExec Job Step Account
	TsinternetUser
	Grorps Guests (Local, Guests have the same access as members of the Users grorp by default, except for the Guest account which is further
	restricted)
	AccountType User
	HomeDrive
	HomeDir
	Profile
	LogonScript Workstations
	PswdCanBeChanged No
	PswdLastSandTime 2003-01-14 14:15
	PswdPre-required No
	PswdExpires No
	PswdExpiresTime Never
	AcctDisabthed No
	AcctLockedOrt No
	AcctExpiresTime Never LastLogonTime Never
	LastLogonServer 172.25.1.134
	LogonHorrs All
•	Sid S-1-5-21-1715567821-682003330-725345543-1000
N N	RasDialin No
	RasCallback Noe
	RasCallbackNumber FullName TsInternetUser
	Comment This user account is used by Terminal Services.
Summary Brief	The less accounts exist with administrative rights and
explanation of risk :	significative names (ex: administrator), smaller the
Carlo State	probabilities for an attacker to guess the names of the
	accounts present. This is particularly thru where the
	NETBIOS protocol is not used (or if special measures
	have been done).
	Otherwise, there is a great probability that an attacker
	may retrieve the available accounts list and their rights.

Risk evaluation :	Is the account « Guest » deactivated ?
	YES NO RL total
	X 0 RL = 4
	Is the account « Guest » renamed for something less explicit ?
	YES NO RL total
	X 0 RL = 2 0
	Is the account « administrator » renamed for something less explicit ?
	YES NO RL total
	X 2 RL = 2
	Does the default account « IUSR_computername » as been renamed for something less explicit ?
	YES NO RL total
	X 4 RL = 2 4
	Is a service account for the ePO software present ?
5	YES NO RL total
	X 7 RL = 3 7
\odot	Is a service account for the saving software (ex: BackupExec) present ?
	YES NO RL total
	X 9 RL = 2

			account ce) preser		he	remote	access	(ex :
ר א	/ES	NO	RL total					
	x	RL = 2	9					
т		L RISK L	EVEL: [9]/	17			

[13]. Control objective :	Verification of the user groups available on the ePO server.
Test location :	From the auditor station
Test location .	
—	From the server audited
Tests to be conducted :	Pre-required : Having downloaded and installed on the audited ePO server, the latest version of DumpSec.
	Observe the following instructions:
	1. Open « DumpSec »
	2. Choose « Select Computer » in the menu
	« Report » and enter the IP address of the
	audited server.
	3. Choose « Dump Grorps as columm » in the
	menu « Report ».
	4. Add all available fields and press on « OK » .
	5. Once the result is obtained, choose « Save
	Report As » of the menu « File »
	(or CRTL-S).
•	○ 6. Choose the type « Fixed width cols » and save
	under the name « 13-groups.txt »
Reference(s) :	The DumpSec tool is available at no charge at the
	following address :
	http://www.systemtools.com/somarsoft/
Expected results :	- The account « administrator » should not be
	found in the group « administrators ».
S Y	- The service account for the saving software
	should be only in the group
	« Backup_Operators ».
	- The account « Guest » should not be found in
	the group « Guest ».
	- Only the service account required by IIS can be
	found in the group « Guest ».
	- No user should be found in the groups « Power
Objective / Subjective :	Users », « Replicator » and « Users ».
Objective / Subjective :	Objective

Results :	File content « 13-groups.txt » :							
	2003-01-15 16:04 - Somarsoft DumpSec (formerly DumpAcl) - \\172.25.1.134 Grorp Comment Type							
	Administrators Administrators have compthande and uRThetricted access to the computer/domain							
	Local SCOREPO01\administrator							
	User SCOREPO01\Backupexec_svr User							
	Backup Operators Backup Operators can override security restrictions for the sothe purpose of backing up or restoring file							
)01\Backu	ipexec_svr	A Care				
	Guests grorp by defa Local			same access as members of the Users account which is further restricted				
	SCOREPC User	001\Guest		5				
		001\IUSR_	SCOREPO01					
	SCOREPC User)01\TsInte	rnetUser					
		tions. Thu	s, Power Users	possess most administrative powers with can run thegacy applications in addition to				
	certified appl Replicator Local			olication in a domain				
	Users			ted from making accidental or intentional n run certified applications, but not most				
	thegacy appl	lications Lo						
Summary Brief		Well managed groups permit only the appropriate						
explanation of risk :	accounts an access to the good things. More misplaced accounts will mean a greater probability for							
				e of those accounts to his				
	advantag							
Risk evaluation :				rator » (If not renamed)				
	found in	the gro	oup « adm i	nistrators » ?				
	YES	NO	RL total					
	X		3					
© Ť	RL = 3							
	Is the service account for the saving software found only in the group « Backup_Operators » ?							
	YES	NO	RL total					
		X RL = 2	5					
	I							

	If not, where is it located ? : In the group « administrators »					
	ls the ac ?	count	« Guest »	found in the group « Guest »		
	YES	NO	RL total			
	X RL = 2		7	215.		
	Is only the service account required by IIS found in the group « Guest » ?					
	YES	NO	RL total	5		
		X RL = 2	9			
				one of the following groups : icator » and « Users » ?		
	YES	NO	RL total			
	X RL = 2		11			
	lf so, exp	olain :				
, ja						
	TOTAL	RISK L	.EVEL: [1	1]/11		

[14] Control objective :	Verification of the complexity of the password for the accounts present on the ePO server.
Test location :	From the auditor station
Tests to be conducted :	 Pre-required : 1. Having downloaded and installed on the audited ePO server, the Pwdump3 tool. 2. Having downloaded and installed on the audited station the tool LC3 (or more recent).

Note : Also, you must know the password of an account with « administrator » rights. Part 1 : From the server audited Observe the following instructions: 1. Open a command line (cmd.exe) 2. Type the following line: pwdump3 addressIP_du_server 14-pwdump.txt Part 2 : From the auditor station Note : Before starting the verification of the complexity of the passwords, assure yourself that the LC3 software is configured according to the following settings : Default Settings For Future Auditing Sessions Verification The Dictionary Crack tests for passwords that are wrighten of the complexity of the did the weakent passwords. Default Settings For Future Auditing Sessions Verification Crack tests for passwords that are wrighten of the words inted in the words into the weakent passwords. Dictionary/Brute Hybrid Crack. Verification of the conduction of the conduction of the conduction of the words inted in the words into the
Part 1 : From the server audited Observe the following instructions: 1. Open a command line (cmd.exe) 2. Type the following line: pwdump3 addressIP_du_server 14-pwdump.txt Part 2 : From the auditor station Note : Before starting the verification of the complexity of the passwords, assure yourself that the LC3 software is configured according to the following settings : Vefault Settings For Future Auditing Sessions Votationary Crack tests for passwords that are the same as the words listed in the Unctionary Crack tests for passwords that are the same as the words listed in the Unctionary/Brute Hybrid Crack Vefault Settings/Future Hybrid Crack Vefault Settings/Future Hybrid Crack
Observe the following instructions: 1. Open a command line (cmd.exe) 2. Type the following line: pwdump3 address/P_du_server 14-pwdump.txt Part 2: From the auditor station Note : Before starting the verification of the complexity of the passwords, assure yourself that the LC3 software is configured according to the following settings : Default Settings For Future Auditing Sessions Vertile: The Dictionary Crack tests for passwords that are the same as the words listed in the Dictionary/Brute Hybrid Crack Settings for Future Auditing Sessions
Observe the following instructions: 1. Open a command line (cmd.exe) 2. Type the following line: pwdump3 address/P_du_server 14-pwdump.txt Part 2: From the auditor station Note : Before starting the verification of the complexity of the passwords, assure yourself that the LC3 software is configured according to the following settings : Default Settings For Future Auditing Sessions Vertile: The Dictionary Crack tests for passwords that are the same as the words listed in the Dictionary/Brute Hybrid Crack Settings for Future Auditing Sessions
Observe the following instructions: 1. Open a command line (cmd.exe) 2. Type the following line: pwdump3 address/P_du_server 14-pwdump.txt Part 2: From the auditor station Note : Before starting the verification of the complexity of the passwords, assure yourself that the LC3 software is configured according to the following settings : Default Settings For Future Auditing Sessions Vertile: The Dictionary Crack tests for passwords that are the same as the words listed in the Dictionary/Brute Hybrid Crack Settings for Future Auditing Sessions
 1. Open a command line (cmd.exe) 2. Type the following line: pwdump3 addressIP_du_server 14-pwdump.txt Part 2: From the auditor station Note : Before starting the verification of the complexity of the passwords, assure yourself that the LC3 software is configured according to the following settings : Default Settings For Future Auditing Sessions Default Settings For Future Auditing Sessions Dictionary Crack The Dictionary Crack tests for passwords that are the same as the words listed in the word file. This test is very last and finds the weakest passwords.
2. Type the following line: pwdump3 addressIP_du_server 14-pwdump.txt Part 2: From the auditor station Note : Before starting the verification of the complexity of the passwords, assure yourself that the LC3 software is configured according to the following settings : Default Settings For Future Auditing Sessions Dictionary Crack Piele Word file: Piele Word file: Piele Word file: Dictionary Crack Word file: Dictionary Crack Word file: Dictionary/Brute Hybrid Crack
2. Type the following line: pwdump3 addressIP_du_server 14-pwdump.txt Part 2: From the auditor station Note : Before starting the verification of the complexity of the passwords, assure yourself that the LC3 software is configured according to the following settings : Default Settings For Future Auditing Sessions Dictionary Crack Word file: Piels @estake%LC3/words-english-big Dictionary Crack Word file: Dictionary Crack Dictionary Crack Word file: Dictionary/Brute Hybrid Crack
pwdump3 addressIP_du_server 14-pwdump.txt Part 2: From the auditor station Note : Before starting the verification of the complexity of the passwords, assure yourself that the LC3 software is configured according to the following settings : Default Settings For Future Auditing Sessions Dictionary Crack Word file: The Dictionary Crack tests for passwords that are the same as the words listed in the word file. This test is very fast and finds the weakest passwords. Dictionary/Brute Hybrid Crack Dictionary/Brute Hybrid Crack tests for passwords that are variations of the words in
pwdump3 addressIP_du_server 14-pwdump.txt Part 2: From the auditor station Note : Before starting the verification of the complexity of the passwords, assure yourself that the LC3 software is configured according to the following settings : Default Settings For Future Auditing Sessions Dictionary Crack Word file: The Dictionary Crack tests for passwords that are the same as the words listed in the word file. This test is very fast and finds the weakest passwords. Dictionary/Brute Hybrid Crack Dictionary/Brute Hybrid Crack tests for passwords that are variations of the words in
Part 2: From the auditor station Note : Before starting the verification of the complexity of the passwords, assure yourself that the LC3 software is configured according to the following settings :
Note : Before starting the verification of the complexity of the passwords, assure yourself that the LC3 software is configured according to the following settings :
of the passwords, assure yourself that the LC3 software is configured according to the following settings : Default Settings For Future Auditing Sessions Dictionary Crack.
of the passwords, assure yourself that the LC3 software is configured according to the following settings : Default Settings For Future Auditing Sessions Dictionary Crack.
software is configured according to the following settings :
software is configured according to the following settings :
Settings : Default Settings For Future Auditing Sessions Dictionary Crack Image: Enabled Word file: Files\@stake\LC3\words-english-big Browse The Dictionary Crack tests for passwords that are the same as the words listed in the word file. This test is very fast and finds the weakest passwords. Dictionary/Brute Hybrid Crack Image: Enabled Image: En
Default Settings For Future Auditing Sessions Dictionary Crack Image: Enabled Word file: Files\@etake\LC3\words-english-big Browse The Dictionary Crack tests for passwords that are the same as the words listed in the word file. This test is very fast and finds the weakest passwords. Dictionary/Brute Hybrid Crack Image: Enabled 3 Characters to vary (more is slower) The Dictionary/Brute Hybrid Crack tests for passwords that are variations of the words in
Dictionary Crack Image: Enabled Word file: Files\@stake\LC3\words-english-big Browse The Dictionary Crack tests for passwords that are the same as the words listed in the word file. This test is very fast and finds the weakest passwords. Dictionary/Brute Hybrid Crack Image: Enabled Image: Enable <
Dictionary Crack Image: Enabled Word file: Files\@stake\LC3\words-english-big Browse The Dictionary Crack tests for passwords that are the same as the words listed in the word file. This test is very fast and finds the weakest passwords. Dictionary/Brute Hybrid Crack Image: Enabled Image: Enable <
Image: Construct of the second state of the second stat
Files\@stake\LC3\words-english-big Browse The Dictionary Crack tests for passwords that are the same as the words listed in the word file. This test is very fast and finds the weakest passwords. Dictionary/Brute Hybrid Crack Dictionary/Brute Hybrid Crack Image: Characters to vary (more is slower) The Dictionary/Brute Hybrid Crack tests for passwords that are variations of the words in
The Dictionary Crack tests for passwords that are the same as the words listed in the word file. This test is very fast and finds the weakest passwords. Dictionary/Brute Hybrid Crack Enabled Build The Dictionary/Brute Hybrid Crack tests for passwords that are variations of the words in
word file. This test is very fast and finds the weakest passwords. Dictionary/Brute Hybrid Crack Image: Enabled 3 The Dictionary/Brute Hybrid Crack tests for passwords that are variations of the words in
Dictionary/Brute Hybrid Crack Enabled 3 Characters to vary (more is slower) The Dictionary/Brute Hybrid Crack tests for passwords that are variations of the words in
► Enabled 3 ► Characters to vary (more is slower) The Dictionary/Brute Hybrid Crack tests for passwords that are variations of the words in
The Dictionary/Brute Hybrid Crack tests for passwords that are variations of the words in
the word file. It finds passwords such as "Dana99" or "monkeys!". This test is fast and finds weak passwords.
Brute Force Attack
Image: Image in the second
Custom Character Set (list each character): ETNRIOASDHLCFPUMYGWVBXKQJZ
The Brute Force Crack tests for passwords that are made up of the characters specified
in the Character Set. It finds passwords such as "WeR3plt6s" or "vC5%69+12b". This test is slow and finds medium to strong passwords. Specify a character set with more
characters to crack stronger passwords.
And observe the following instructions:
1. Recover the file « 14-pwdump.txt » from the
audited server by the way of your choice.
2. Open the application« LC3 » (or more recent)
3. Choose « File - New Session »
4. Choose « Import »
5. Choose « Import # 5. Choose « Import from a PWDUMP File »
6. Choose the file « 14-pwdump.txt »
7. Press on « F4 » (or choose the icon « Begin

	1						
	system tray passwords o 9. Once the pa delay has e file« 14-Ic3 .	-					
Reference(s) :	the following addre	vailable as an eval ess : .com/research/lc/do					
	The Pwdump3 tool is available at the following address : http://www.polivec.com/pwdumpdownload.html						
Expected results :		Concerning the result for LC3 :					
Expected results .	No password must have been found after a minimum of 12 hours of « brute force ».						
	 Concerning the general rule for passwords : All passwords should be composed of : At least 8 characters At least one small letter, one capital letter, one number and one special character (ex : !?%*/#) The service accounts should be composed of 1⁴ characters and should include at least 2 characters o each categories. 						
Objective / Subjective :	Objective						
Results :	File content « 14-pwdump.txt » :						
O PARA MAR	Administrator:500:CE7A23ED46C4F0FC9D8BBC3E3B48E321:CDADF0 1D2336AB04D1EF488429E553FA::: Backupexec_svr:1005:B7BF3C926A6A34FF7584248B8D2C9F9E:D48F DAE7B9496CD575E16D305D1DF194::: Guest:501:NO PASSWORD**********:NO PASSWORD************************************						
	Contenu de « 14-lc3.txt » :						
	USERNAME Administrator Backupexec_svr Guest IUSR_SCOREP001 SQLAgentCmdExec TsInternetUser	LANMAN PASSWORD ??????N99 ePOBackup * missing * CGR2QDV?????? ZEUMVKCM ??????THE94EIJ	NTLM PASSWORD * uncracked * EPOBACKUP * missing * * uncracked * ZEUMVKCM * uncracked *				

Summon / Drief	Mithout o	rabuat autho	ntification (including a small				
Summary Brief		Without a robust authentification (including a small					
explanation of risk :		letter, a capital letter a number and a special					
	,	character) the probabilities for an attacker to take					
		ne server is hig					
Risk evaluation :	Have passv	Have passwords been found after a maximum of 12					
	hours of « b	hours of « brute force »?					
	YES N	NO RL total					
	X		Ċ.º				
	RL = 4	4					
	NL = 4						
			20				
	Are passwo	Are passwords for accounts with administrative rights robust and conform ?					
	YES NO	D RL total	6				
		8					
	RL = 4						
	Are passwords for service accounts composed of 14						
	Characters	characters ?					
	YES NO	RL total					
	X	11					
	RL =						
	TOTAL RISK LEVEL: [11]/ 11						

[15] Control objective :	Verification that access rights have been put on certain					
	important directories.					
Test location :	From the auditor station					
	From the server audited					
Tests to be conducted :	Observe the following instructions in order to verify the					
	access rights to the directory « MSFTPSVC1 » :					
	1. Conduct a search on drive « C » for					
\bigcirc	« MSFTPSVC1 » using « Start » - « Search » –					
	« For File and Folders » (or touch windows + f)					
	2. Right button on « MSFTPSVC1 »					
	3. Choose « Properties »					
	4. Choose the tab « Security »					
	5. Click on « Administrator », Take a screen					
	capture and save in a Wordpad file under the					
	name « 15-msftpsvc1.rtf »					
	6. Use the same procedure for each accounts					

	present and save at the end in the same file.
	Observe the following instructions in order to verify the access rights to the directory « Ftproot » :
	 Conduct a search on all the drives for « Ftproot» using « Start » - « Search » – « For File and Folders » (or touch windows + f) Right button on « Ftproot » Choose « Properties » Choose the tab « Security » Click on « Internet Guest Account », Take a screen capture and save in a Wordpad file under the name « 15-ftproot.rtf » Use the same procedure for each accounts present and save at the end in the same file.
Reference(s):	Not applicable / Personal experience
Expected results :	Concerning the rights on the directory
	« MSFTPSVC1 »:
	 Only the groups « Administrators » and « System » should have the authorization « Full Control » The rest of the groups (if existing) should have only the authorization « Read » The group « Everyone » should not be present
	Concerning the rights on the directory « Ftproot » :
Sh	 Only the group « Administrators » should have the authorization « Full Control » The rest of the groups (if existing) should have only the authorization « Read » The group « Everyone » should not be present
Objective / Subjective :	Objective

Results :	File content « 15-msftpsvc1.rtf » :
	MSFTPS¥C1 Properties ? X
	General Sharing Security
	Name Add
	Administrators (SCOREP001\Administrators)
	CREATOR OWNER Owner Users (SCOREPOOT\Power Users)
	SYSTEM Sers (SCOREP001\Users)
	Permissions: Allow Deny
	Full Control
	Read & Execute
	Read 🔲 🗖
	I Additional permissions are present but not
	Advanced Viewable here. Press Advanced to see them.
	object
	OK Cancel Apply
	MSFTPSVC1 Properties
	General Sharing Security
	Name Add Add Add Add
	CREATOR OWNER
	Constant Service C
	Users (SCOREP001\Users)
	Permissions: Allow Deny
	Modify 🔤 🗖 Read & Execute
	List Folder Contents 🛛 🗖 🗖
SA	Read III Write
S,	Advanced
\odot	Allow inheritable permissions from parent to propagate to this object

	MSFTPSVC1 Properties ? ×
	General Sharing Security
	Name Add
	CREATOR OWNER
	Power Users (SCOREPO01\Power Users)
	SYSTEM Users (SCOREPO01 \Users)
	Permissions: Allow Deny
	Full Control 🗹 🗖 Modify
	List Folder Contents
	Read & Execute Image: Contents List Folder Contents Image: Contents Read Image: Contents Write Image: Contents
	Write
	Advanced
	Allow inheritable permissions from parent to propagate to this object
	OK Cancel Apply
	200 20020 <u>20070</u>
	MSFTP5VC1 Properties
	General Sharing Security
	Name Add
	Administrators (SCOREP001 Administrators)
	CREATOR OWNER
C.	Power Users (SCOREPO01\Power Users) SYSTEM
	Users (SCOREP001\Users)
	Permissions: Allow Deny
	Full Control
	Read & Execute 🗹 🗖
S.	List Folder Contents Read
	Write
C SALES T	Advanced
	Allow inheritable permissions from parent to propagate to this
	object
Gy and the second se	OK Cancel Apply

	File content « 15-ftproot.rft » :
	ftproot Properties ? ×
	General Sharing Security Name Add Internet Add Internet Guest Account (SCOREP001 \UD
	Permissions: Allow Deny
	Full Control Image: Control Modify Image: Control Read & Execute Image: Control List Folder Contents Image: Contents Read Image: Contents Write Image: Contents
	Advanced
	OK Cancel Apply
	ftproot Properties ? × General Sharing Security
	Name Add Administrator (SCOREP001\Administrator) Remove Internet Guest Account (SCOREP001\UL Remove
A THE	Permissions: Allow Deny Full Control Modify Read & Execute List Folder Contents Ø Read Ø Write
O T	Advanced
	OK Cancel Apply
Summary Brief explanation of risk :	Larger the access are on the important directories, greater the probabilities for an attacker to modify the data present on those directories with a minimum of effort are big.

Risk evaluation :	Do only the groups « Administrators » and « System » have an authorization « Full Control » on the directory « MSFTPSVC1 » ?					
	YES	NO	RL total			
	X	RL = 3	0			
	lf not,	which ? :				
			· · · · · · · · · · ·			
	author	e rest of ization TPSVC1	« Read	ps (if existing) have only an » on the directory		
	YES	NO	RL total			
		X RL = 3	3			
	lf not,	which ? :				
3	Does the group « Everyone » have rights on the directory « MSFTPSVC1 » ?					
	YES	NO	RL total			
	RL = 3	<u>х</u>	3			
	author	only th ization oot » ?	e group «Full C	« Administrators » have an ontrol » on the directory		
	YES	NO	RL total			
	x	RL = 3	3			

lf not, w	/hich ? :		
	· · · · · · ·	· · · · · · · · · · · · · · · · · · ·	
			os (if existing) have only an the directory « Ftproot » ?
YES	NO	RL total	. 6 °
x	RL = 3	3	
lf not, w	/hich ? :		
		•2	<u>Ş</u>
		o « Everyor oot » ?	ne » have rights on the
YES	NO	RL total	
RL = 3	x	3	
TOTAL	RISK L	.EVEL: [3	8]/ 18

[16] Control objective :	Verification of the password for an account « SA » for
	the MSDE database
Test location :	From the auditor station
	\boxtimes From the server audited
Tests to be conducted :	Observe the following instructions in order to validate if
2	the account « SA » has a password :
	1. Conduct a search on all the drives for
C Y	« cfgnaims.exe » using « Start » - « Search » –
	« For File and Folders » (or touch windows + f)
	2. Double click on the file « cfgnaims.exe »
	3. Take a screen capture of each of the tabs and
	save in a Wordpad file under the name « 16-
	sapw.rtf »
	4. Open a command line (cmd.exe)
	5. Type the following line:
	osql –U sa
	 The following line should be : Password :

	1
	 Press « ENTER » in order to enter no password. Take a screen capture and paste it at the end of file « 16-sapw.rft »
	Note : In case a password is entered (i.e. : the result of osql –U sa is not 1>), ask for the password from the system administrator.
Reference(s) :	HOW TO: Verify and Change the System Administrator Password by Using MSDE – KB 322336:
	http://support.microsoft.com/default.aspx?scid=kb;en- us;Q322336#2
Expected results :	The result of the command « osql –U sa » should be :
	Login Failed for user 'sa'.
	If MSDE is configured to use only « Windows Authentification », the result should be :
	Login failed for user 'sa'. Reason: Not associated with a trusted SQL Server connection.
	Since it is rarely changed, it should be composed of 14 characters and should include at least 2 characters of each categories (small letter, capital letter, number and special character)
	The password « SA » should be different from the password :
X	 Permitting authentification to the server Permitting authentification to the « ePO » management console.
Objective / Subjective :	Objective : except for validation of the password format given by the administrator (if present).
O A A A	

Results :	File content « 16-sapw.rft » :
	McAfee ePolicy Orchestrator Server Configuration (SCOREPOO1) SQL Server Administrator Reviewer Select the SQL server containing the ePolicy Orchestrator database you wish to use. Then enter the name of the database to be used. Database information SQL server name: Image: Image
	OK Cancel Apply Help McAfee ePolicy Orchestrator Server Configuration (SCOREPOOL) X SQL Server Administrator Reviewer It should have full privileges to the database. It should have full privileges to the database.
A HAS	Account details Ise Windows NT authentication Use SQL authentication User credentials User name: Sa Password: Ymmexmum Domain name:
	OK. Cancel Apply Help

	McAfee e	Policy Orchestr	ator Server Config	juration (SCOREPO01)	×
	SQL Se	rver Administrato	Reviewer		
	This account will be used by ePolicy Orchestrator to review your SQL database. It should have read-only privileges to the database.				
	Acco	ount details			
	C Use <u>W</u> indows NT authentication				
		Jse <u>S</u> QL authentic	ation		
		er credentials	sa	2 	
	1000	assword:			
		omain name:			
		omain name.			
			ОК	Cancel <u>Apply</u> Help	
)'	_
	Microsoft (C) Copy	T\ System32\cmd.ex t Windows 2000 right 1985-2000	e [Version 5.00.21) Microsoft Corp.		
	C:\Docum Password	ents and Settin	gs∖administrator		
	COST OF CONTRACTOR		sa . gs∖administrator	>_	
		· · ·		a	-
Summary Brief explanation of risk :				fication (including small le and special character)	etter, the
				cker to take control of	
	•		e are highe		
	Thora	foro tho	probobilit	ion for on ottookor to i	taka
				ies for an attacker to t O server are higher.	lake
Risk evaluation :				have a password ?	
	YES	NO	RL total		
	x	RL = 4	0		
		<u> </u>]	

1			
Is the	passwor	d for the	account « SA » composed of
14 cha	aracters ?	?	
YES	NO	RL total	
	X		
	~	2	
	RL = 2	_	
ls th	•		erent from the one for
auther	ntification	to the ser	ver (i.e. : Windows) ?
VEO	NO		
YES	NO	RL total	
X		2	
	RL = 3		c-S'
L			
ls th	e pass	word diff	erent from the one for
aumer	nuncation	to an ePC	console ?
YES	NO	RL total	
	Х	•	
	RL = 4 🕚	6	
			-
ΤΟΤΑ	L RISK L	.EVEL: [6	5]/ 12
1	(h)	•	-

[17] Control objective :	Verification of access rights on certain important files of
	ePolicy Orchestrator.
Test location :	From the auditor station
	\bowtie From the server audited
Tests to be conducted :	Observe the following instructions:
6 A. S. MAS	 Conduct a search on all the drives for « DB » using « Start » - « Search » – « For File and Folders » (or touch windows + f) Right button on the file « DB » found in the directory « \ePO\2.0 » Choose « Properties » Choose the tab « Security » Take a screen capture for each of the accounts present and save it in a Wordpad file under the name « 17-dbepo.rtf »
Reference(s) :	Not applicable / Personal experience

Expected results :	Only the group « administrators » should have access in « Full Control » to the file « DB ».
	Note : The group « Backup Operators » could also be
	present (if required by the saving software).
Objective / Subjective :	Objective
Results :	File content « 17-dbepo.rtf » :
	DB Properties ? ×
	General Sharing Security
	Add
	Everyone <u>R</u> emove
	Permissions: Allow Deny
	Full Control
	Modify 🗹 🗖
	Read & Execute List Folder Contents
	Read 🗹 🗖
	Allow inheritable permissions from parent to propagate to this object
	OK Cancel Apply
Summary Brief	Larger the access will be on the important directories,
explanation of risk :	greater are the probabilities for an attacker to modify
÷	the data present on those directories with a minimum
Risk evaluation :	of effort are big. Does only the group « administrators » have an access
	« Full Control » to the file « DB ?
4	YES NO RL total
SV.	X 4
	RL = 4
	If not, which ? :
	Everyone
	TOTAL RISK LEVEL: [4] / 4

[18] Control objective :	Verification of authentification accounts for the ePolicy
	Orchestrator management console
Test location :	From the auditor station
	\times From the server audited
Tests to be conducted :	Pre-required : Having obtained from the system
	administrator a user account and a valid password in
	order to authentify yourself on the management
	console.
	Observe the following instructions:
	1. Open the « ePO » management console
	Choose « Login »
	2. Register a users account, a valid password and
	choose « OK »
	3. Choose « Manage Administrator », Take a
	screen capture and save in a Wordpad file
	under the name « 18-epopw.rtf »
	4. If an other account exist other than the default
	account (admin) with the role « administrator »
	or « Site Administrator », Choose this account
	and Press on « Configure ».
	5. Take a screen capture and save at the end of
	file « 18-epopw.rtf »
	6. Use the same procedure for each of the
	accounts with administrative rights.
Reference(s) :	Not applicable / Personal experience
Expected results :	There should be an access code created according to
	the number of administrator needing access to the
•	ePO management console.
	The default account « ADMIN » must be deleted or
	renamed.
	All passwords should be composed of at least 8
e V	characters (and include small letter, capital letter,
	number and special character).
	Also they should be different from the password
	permitting authentification on the server or from the
	one for account « SA » of the database.
Objective / Subjective :	Objective, except for validation of the password
	« ADMIN » given by the system administrator.

Results :	File content « 18-epopw.rtf » :
	Manage Administrators
	Admin Page
	List of ePolicy Orchestrator administrative accounts.
	Name Role Site
	admin Administrator
	Add Remove Configure
	OK Cancel Help
Summary Brief	Without a robust authentification (including small letter,
explanation of risk :	capital letter, number and special character) the
	probabilities for an attacker to take control of the ePO management console is higher.
Risk evaluation :	Have access codes been created according to the
	number of administrators needing to access the ePO
	management console ?
	YES NO RL total
	X 3
•	RL = 3
	Is the default account « ADMIN » deleted or renamed
5	YES NO RL total
GV'	X 7
\odot	RL = 4
	Are all the personande compared of at least 9
	Are all the passwords composed of at least 8 characters and robust ?
	YES NO RL total
	X 7
	RL = 4
	<u> </u>

	•		fferents from /er (i.e. : Windo		for
YES	NO	RL total			
X	RL = 4	7			
	he passv nt « SA »		erent from the	one for	the
YES	NO	RL total	.00		
x	RL = 4	7	ell'		
ΤΟΤΑ	L RISK L	EVEL: [7]/ 19		

TOTAL RISK LEVEL Concerning the access rights

51 / 92

3.3.4 Verification of the supervising mechanism

[19] Control objective :	Verification for the presence of an audit mechanism for the operating system.
Test location :	From the auditor station From the server audited
Tests to be conducted :	Observe the following instructions in order to verify the settings of « system », « security » and « application » : 1. Right button on the icon « My Computer » 2. Choose « Manage »
	 Double click « Event Viewer » Right button on the icon « Application » and choose « Properties » Take a screen capture and save in a Wordpad
Õ	 document under the name « 19-events.rtf » 6. Follow the same procedure for « Security » and also for « System ».
	Observe the following instructions from the server audited in order to verify the settings for « Audit Policy » :
	 Choose « Local Security Policy » in the « Administrative Tools »

 2. Choose « Audit Policy » 3. Take a screen capture and save at the end of file « 19-events.rtf » Reference(s) : Securing Windows 2000 Step-by-Step, SANS Institute, page 21 and 22 Expected results : Concerning the settings for « System », « Security » and for « Application » : The option « Do not overwrite events (clear log manually) » should be ideally selected only if a validation and purging task is done every day. The amount (in KB) inscribed in the zone « Maximum log size : » should be suffisant in order to not permit an easy service deny. Concerning the settings for « Audit Policy » : For each points, « Success » and also « Failure » should be activated. (« Audit process tracking » can not be selected) Objective / Subjective : Objective freed Faer (Stope) File content « 19-events.rtf » : File content « 19-events.rtf » : Winder December 3.002 2123 FM Accessed December 3.002 2123 FM Explore The setting be intended I the set of a set of the set		
file « 19-events.rtf » Reference(s) : Securing Windows 2000 Step-by-Step, SANS Institute, page 21 and 22 Expected results : Concerning the settings for « System », « Security » and for « Application » : The option « Do not overwrite events (clear log manually) » should be ideally selected only if a validation and purging task is done every day. The amount (in KB) inscribed in the zone « Maximum log size : » should be suffisant in order to not permit an easy service deny. Concerning the settings for « Audit Policy » : For each points, « Success » and also « Failure » should be activated. (« Audit process tracking » can not be selected) Objective / Subjective : Objective Results : File content « 19-events.rtf » : File content « 19-events.rtf » : File content « 19-events.rtf » : Image and the set of the selected on the selected o		2. Choose « Audit Policy »
page 21 and 22 Expected results : Concerning the settings for « System », « Security » and for « Application » : - The option « Do not overwrite events (clear log manually) » should be ideally selected only if a validation and purging task is done every day. - The amount (in KB) inscribed in the zone « Maximum log size : » should be suffisant in order to not permit an easy service deny. Concerning the settings for « Audit Policy » : - For each points, « Success » and also « Failure » should be activated. (« Audit process tracking » can not be selected) Objective / Subjective : Objective / Subjective : File content « 19-events.rtf » : File content « 19-events.rtf » : Image: Size :: Size :: Size :: File content « 19-events.rtf » : Image: Size :: Size :: Size :: Size :: Size :: Image: Size :: Size :: Size :: Size :: Size :: Size :: Concerning ing is septement dot the set insched :: Image: Size :: Size :: Size :: Size :: Objective: Obje		
Expected results : Concerning the settings for « System », « Security » and for « Application » : The option « Do not overwrite events (clear log manually) » should be ideally selected only if a validation and purging task is done every day. The amount (in KB) inscribed in the zone « Maximum log size : » should be suffisant in order to not permit an easy service deny. Concerning the settings for « Audit Policy » : For each points, « Success » and also « Failure » should be activated. (« Audit process tracking » can not be selected) Objective / Subjective : File content « 19-events.rtf » : File content « 19-events.rtf » : File content « 19-events.rtf » : Within types 2006 [95:986 bytes] Deaded April 2.2021228 PM Modified December 9.2002 21228 PM Modified	Reference(s) :	Securing Windows 2000 Step-by-Step, SANS Institute,
and for « Application »: The option « Do not overwrite events (clear log manually) » should be ideally selected only if a validation and purging task is done every day. The amount (in KB) inscribed in the zone « Maximum log size : » should be suffisant in order to not permit an easy service deny. Concerning the settings for « Audit Policy » : For each points, « Success » and also « Failure » should be activated. (« Audit process tracking » can not be selected) Objective / Subjective : Objective Results : File content « 19-events.rtf » : File content « 19-events.rtf » : Concerning file [] Develop nome: [] Content [] Concerning file [] Co		page 21 and 22
- For each points, « Success » and also « Failure » should be activated. (« Audit process tracking » can not be selected) Objective / Subjective : Objective Results : File content « 19-events.rtf » :	Expected results :	 and for « Application » : The option « Do not overwrite events (clear log manually) » should be ideally selected only if a validation and purging task is done every day. The amount (in KB) inscribed in the zone « Maximum log size : » should be suffisant in order to not permit an easy service deny.
« Failure » should be activated. (« Audit process tracking » can not be selected) Objective / Subjective : Objective Results : File content « 19-events.rtf » :		Concerning the settings for « Audit Policy » :
Results : File content « 19-events.rtf » : Application Properties Image: City Control of Content (Content (Conten (Content (Content (Content (Content (Conten (Content (Content (C		« Failure » should be activated. (« Audit
Application Properties ? × General Filter Display name: C:\WINNT\system32\config\AppEvent.Evt Size: 832.0 KB (851.968 bytes) Created: April 2, 2002 1:55:20 PM Modified: December 9, 2002 2:12:28 PM Accessed: December 9, 2002 2:12:28 PM Log size 1024 Maximum log size: 1024 Corgare Cuprerwite events older than Orgerwite events older than 7 Corgot overwite events Bestore Defaults Using a log-speed connection Dear Log	Objective / Subjective :	Objective
	Results :	Application ? × General Filter Display name: C:W/INNT\system32\config\AppEvent.Evt Log name: C:W/INNT\system32\config\AppEvent.Evt Size: 832.0 KB (851.968 bytes) Created: April 2, 2002 1:55:20 PM Modified: December 9, 2002 2:12:28 PM Accessed: December 9, 2002 2:12:28 PM Log size Maximum log size: Maximum log size: 1024 KB When maximum log size is reached: © Overwrite events as needed © Overwrite events older than ? Do not overwrite events [clear log manually) Restore Defaults Using a low-speed connection Clear Log

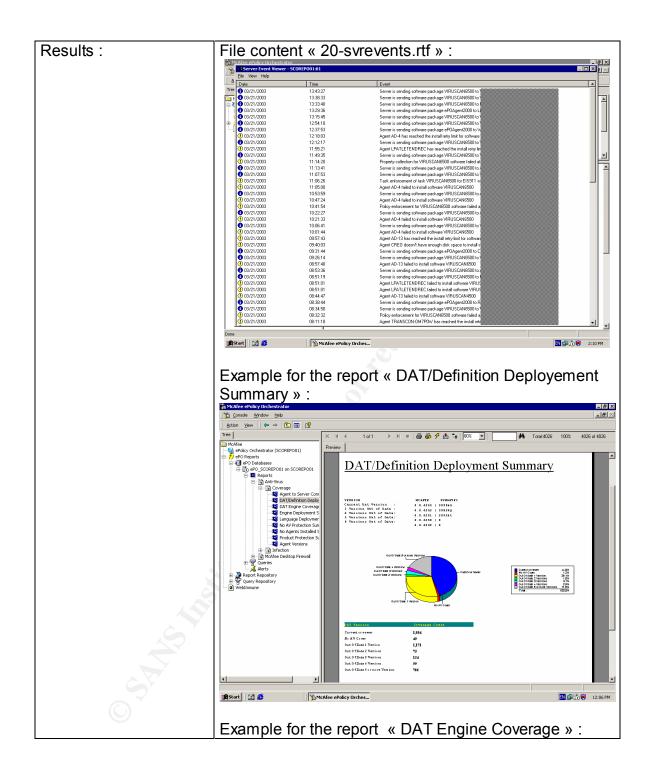
	Security Properties ? X
	General Filter
	Display name: Security
	Log name: C:\WINNT\System32\config\SecEvent.Evt
	- 5
	Size: 7.0 MB (8,192,000 bytes) Created: April 2, 2002 1:55:20 PM
	Modified: December 9, 2002 2:12:28 PM
	Accessed: December 9, 2002 2:12:28 PM
	Log size
	Maximum log size: 8000 😴 KB
	When maximum log size is reached:
	C Dverwrite events as needed
	Overwrite events older than 7 → days
	C Do not overwrite events (clear log manually) <u>B</u> estore Defaults
	Using a low-speed connection
	OK. Cancel Apply
	System Properties ? X
	General Filter Display name: System
	400 0 KD ((50 752) +
	Size: 446:U KB (408,752 bytes) Created: April 2, 2002 1:55:20 PM
	Modified: December 9, 2002 2:12:28 PM
	Accessed: December 9, 2002 2:12:28 PM
	Maximum log size: 1024 🚔 KB
	When maximum log size is reached:
	C Overwrite events as needed
	© Overwrite events older than 7 🚽 days
	C Do not overwrite events (clear log manually) <u>R</u> estore Defaults
Contraction Mew Tree	Using a low-speed connection
	OK Cancel Apply
E Local Security	y Settings
Action View	
	Policy △ Local Setting Effective Setting BillAudit account logon events Success, Failure Success, Failure
	olicies Audit account management Success, Failure Success, Failure
E Cal Policie	Policy Baddit logon events Success, Failure Success, Failure
😟 🛄 Securit	
B→ □ Public Key f B→ □ IP Security	/ Policies on Local Machine 🗒 Audit process tracking Failure Failure Failure
	Audit system events Failure Failure
	<u> </u>

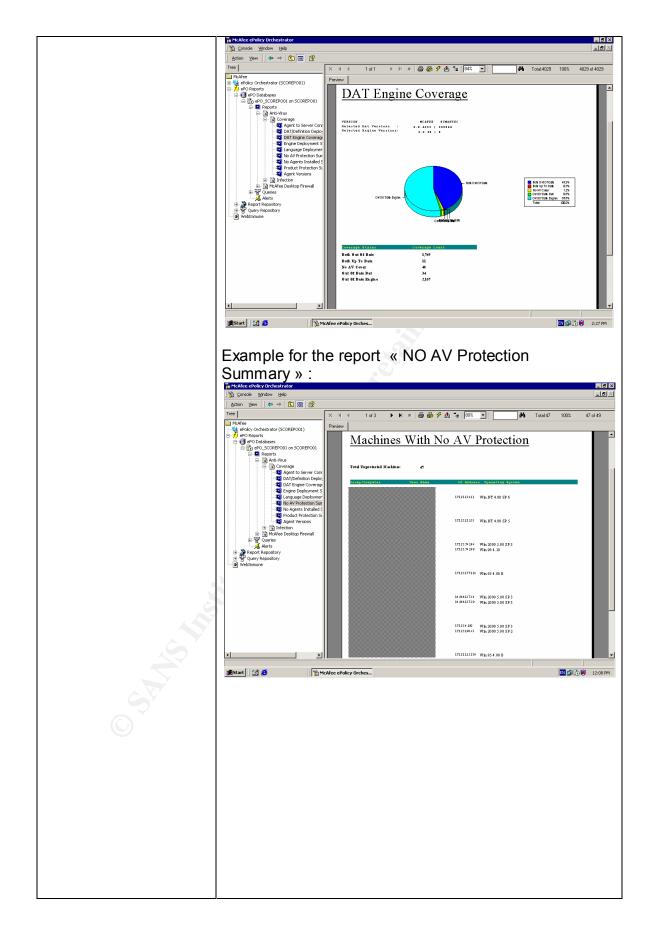
Summary Brief explanation of risk :	Without a sufficient monitoring, there is no way to identify anomalies caused either by a malfunction of an application or by an attack targeted by an attacker. Better the monitoring, greater the probabilities to limit		
	the damage.		
Risk evaluation :	In the settings for « Application » :		
	Is the option « Do not overwrite events (clear log manually) » selected ?		
	YES NO RL total		
	X 2 RL = 2		
	Is the amount (in KB) indicated in the zone « Maximum log size : » sufficient in order to not permit an easy service deny, if « clear log manually » is or was activated ?		
	YES NO RL total		
	6 RL = 4		
	If not, what is the value ? : 1024		
	In the settings of « Security » :		
La Star	Is the option « Do not overwrite events (clear log manually) » selected ?		
	YES NO RL total		
	X		
	RL = 3 9		
	Is the amount (in KB) indicated in the zone « Maximum log size : » sufficient in order to not permit an easy service deny, if « clear log manually » is or was activated ?		
	YES NO RL total		
	X 9		

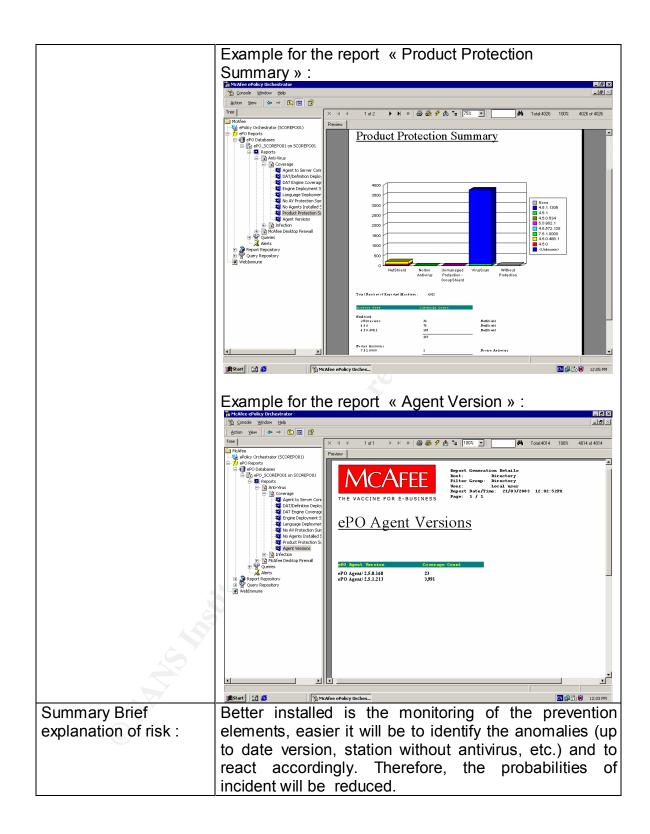
If not, what is the value ? :			
In the settings for « System » : Is the option « Do not overwrite events (clear log manually) » selected ?			
YES	NO X RL = 2	RL total	i entre
Is the amount (in KB) indicated in the zone « Maximum log size : » sufficient in order to not permit an easy service deny, if « clear log manually » is or was activated ?			
YES	NO X RL = 4	RL total	
If not, what is the value ? : 1024			
In the settings for « Audit Policy », are each points for, « Success » and also for « Failure » activated ?			
YES	NO X RL = 3	RL total	
If not, which are not ? : Missing: Directory Service, Object Acces, Process Access and System Events			
ΤΟΤΑ	L RISK L	.EVEL: [1	8]/22

[20] Control objective :	Verification of the general process for the verification of the ePO management console.
Test location :	From the auditor station
Tests to be conducted :	 Pre-required : Having obtenained from the system administrator a user account and a valid password to access the ePO management console and the database MBSA (or MS-SQL accordingly) Observe the following instructions to obtain a preview of the last events on the ePO server : Open the « ePO » management console Choose « Login » Register a user account, a valid password and choose « OK » Once the window « Initializing » disappears, choose with the right button of the mouse
	 « Directory » 5. Choose « Server Events » 6. Take a screen capture and save in a Wordpad document under the name « 20-srvevent.rtf » Observe the following instructions in order to generate the quantity of report necessary for the monitoring :
Sh. Hi	 Open the « ePO » management console, double click on « ePO Reports » Double click on « ePO Databases » Double click on the audited server name Click « OK » in the window « ePO Database Login » Double click on « Reports » Double click on « Anti-virus » Double click on « Coverage » Double click on « DAT/Definition Deployement Summary » and press on« OK »
	 9. Choose « No » in the window « Customize Report » 10. Choose the icon « Export » 11. Choose the format of your choice (ex : HTML 3.0 Draft Standard) and press on« OK » 12. Choose the place or save the report (leaving the default name) and choose « OK » 13. Do the same task for :

	 DAT Engine Coverage 					
	 NO AV Protection Summary Product Protection Summary 					
	 Agent Version 					
Reference(s) :	Not applicable / Personal experience					
Expected results :	In the « Server Events » :					
	 There should be nothing suspicious or any errors recorded (watch out for events in yellow). In the report « DAT/Definition Deployement Summary » : 					
	 A large majority of the working stations or of the servers should have the latest version of the file signature (.DAT). There should not be any version of the signature older than the one before the latest version available (« Out of date version »). 					
	 There should be only a few (or none) « Out of date Engine » In the report « NO AV Protection Summary » : 					
	- There should not have any stations or servers without the antivirus solution.					
6	In the report « Product Protection Summary » :					
Les th	 There should not be any product considered unknown. There should not be many version of NetShield 					
	or of VirusScan.					
0	 No other antivirus solution should be present without a valid reason. 					
	In the report « Agent Version » :					
	 There should not be many version of the ePO agent ePO installed. 					
Objective / Subjective :	Objective					







Risk evaluation :	Have suspicious events or mistakes been recorded in the « Server Events » ?				
	YES		RL total		
	X				
	RL = 4	•	4		
			<u>.</u>	 م	
	If so, explain the principals : Application that give a failure during installation				
			· · · · · · · · · · · · · · · · · · ·		
	Does the large majority of the working stations or the servers have the latest version of the file signature (.DAT)?				
	YES	NO	RL total		
		X RL = 4	8		
	Have some versions of signature older than the one before the latest version been identified ?				
	YES	NO	RL total		
	X RL = 4		12		
	system	uch as a does no		the computer information his criteria and an other ersion	
	Have little (or none) version not updated for the engin (« Out of date Engine ») been identified ?				
	YES	NO	RL total		
		X RL = 4	16		
				·	

	does no	najority t seem	updated to	puter information system this level. An update has h would explain the situation		
	Have st antivirus			s been identified without an		
	YES	NO	RL total	15.		
	X RL = 4		20			
	If so, explain : About 45					
			N.			
	Have products considered unknown been identified					
	YES	NO	RL total			
	X RL = 4		24			
	lf so, exp 37 ou		7 servers a	nd over 200 stations		
Sta	Have many version of NetShield or VirusScan bee identified ?					
	YES	NO	RL total			
0	X RL = 4		28			
	If so, explain : A lot for NetShield (70) do not seem up to date					

Have other antivirus solution (present without a valid reason) been identified ?				
YES NO RL total				
X 32 RL = 4				
If so, explain : Norton Antivirus on a test station				
TOTAL RISK LEVEL: [32] / 32				
9				

TOTAL RISK LEVEL Concerning the monitoring mechanism

50 / 54

Results Summary Table

	Total assessed risk	Maximum risk	Percentage (%)		
Operating system security and open session validation	40	48	83%		
Product configurations	19	109	17%		
Access rights	51	92	55%		
Monitoring mechanisms	50	54	93%		
Total risk: _160_ for a maximum of 303 = _53_ %					

3.2 Measuring Residual Risk

As mentioned in Section 1.3, the audit form was designed as tool for reducing the main security risks involved in using a central management console.

The set of audited elements gives an excellent portrait of the ePO server. Special emphasis was given to authentification and access rights for certain sensitive directories. The vulnerabilities of the operating system were also checked, to determine, among other things, how up to date the system is. The analysis of open ports and extraneous applications can be used as a quick check to see if suspect services are present. The audit also checked for an antivirus solution

and quickly verified ePO agent operation on the server to see whether the server is properly protected against most malicious code.

The monitoring system on the ePO server was checked as well, to see whether the system administrator had configured it for proactive monitoring.

There is, however, always a certain residual risk because no security product can protect against a new vulnerability. However, by using ePolicy Orchestrator to provide adequate monitoring, there is a greater chance of a quick response to most threats.

To further decrease risk, consideration should be given to implementing a global process of securing all important computer systems.

All products deployed (e.g.: VirusScan, Mcafee Desktop Firewall, etc.) should be checked by the ePO management console to make sure that they are carrying out their protective functions satisfactorily.

Physical security should also be verified, to make sure that equipment is properly protected against fire (manual extinguisher, type of sprinkler, etc.), theft (access to the computer room, disk protection, tape backup protection, etc.), flooding (height above the floor, etc.) and voltage fluctuations (use of UPS, generators, etc.).

The hardening of the operating system (Windows 2000) should also be thoroughly reviewed. There is a significant amount of reference material to assist with this task, including the following.

- Securing Windows 2000: Step-by-Step, SANS Institute
- Windows 2000 Server Baseline Security Checklist, Microsoft (<u>http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/w2ksvrcl.asp</u>)
- Benchmark for Windows 2000, The Center for Internet Security (CIS) (www.cisecurity.org)
- Auditing Windows 2000, Security Consensus Operational Readiness Evaluation (S.C.O.R.E) (<u>http://www.sans.org/score/checklists/AuditingWindows2000.doc</u>)

Naturally, the recommendations in each document must be evaluated to ensure the hardening procedured selected meets the need of each organization.

3.3 Evaluating the Audit

Although the ePO server cannot be accessed directly from the Internet, it is available to the entire internal network. Because of the importance of the

protection it provides, it is vital to ensure than no one can in any way impede the proper functioning of the ePO server.

It is also vital to ensure that only authorized personnel can access the ePO server to change the protection configuration elements.

All authentification mechanisms on the ePO server were checked against the audit form, as were the configurations of all products on the ePO server, to make sure they do not offer any openings to attackers. The vulnerabilities of the Windows 2000 operating system were also reviewed.

Every effort was made to make all controls as objective as possible in order to limit the impact of an incorrect interpretation.

© SANS Institute 2003,

Assignment 4: Audit Report

4.1 Administrative Summary

4.1.1 Purpose of the audit

Given that the ePO central management console can only be accessed via the local area network (LAN) and wide area network (WAN), the main threats come from employees, and customers and suppliers who use the WAN. The main purpose of the ePolicy Orchestrator v2.5 server (ePO) audit was to assess the security risks for this type of server, in order to ensure configuration and data integrity, system availability and full authentication.

A further purpose was to make recommendations that would increase the server's security level.

4.1.2 Summary of results

The security audit of the ePO server covered the four following items: audit of the operating system (Windows 2000 Advance Server) and identification of suspect applications; audit of the configurations of the main products used directly or remotely by the ePO server; audit of the access rights on a number of sensitive directories; and audit of the existing monitoring mechanisms.

Based on the results obtained, the two main weaknesses of the ePO server are mainly caused by:

- Failure to regularly update the operating system and related products, including the MSDE (Microsoft SQL Server Desktop Engine) product.
- Failure to monitor event reports, whether generated by the operating system (Event Logs) or generated by or with the help of the ePO management console (Server Events and the various reports available).

The audit also showed that there are a number of weaknesses in the management of access rights for certain sensitive directories.

Note that the audited product configurations on the ePO server do not appear to present any significant weakness that could affect server security.

4.1.3 Risk analysis summary

Even though the ePolicy Orchestrator server cannot be accessed from the Internet, there would be negative consequences attendant upon the loss of integrity, authentication or availability of such a server, namely:

• Loss of productivity: if an attacker took control of the ePolicy Orchestrator management console, the protection parameters the server is responsible for deploying and configuring could be altered. This could significantly decrease the protection each product could provide, leaving the entire system vulnerable to a computer virus.

If a large number of workstations and critical servers were infected by a virus or worm, loss of productivity would certainly result.

• Loss of confidence in the antivirus software: the investment required to implement a central solution is based on the company-wide assumption that this solution will provide adequate protection. Further, central management has most likely freed network administrators from the task of maintaining the antivirus solution. It is very important that confidence in the services provided by the ePolicy Orchestrator console not be damaged.

A simple configuration error by those responsible for the console could erode that confidence. An intrusion by an attacker that compromised all protection mechanisms would definitely damage managers' and technicians' faith in the solution.

• *Financial loss*: the loss of critical company services due to infection, altered configurations or any other consequence related to an employee's intrusion into the ePO server, could, depending on the seriousness and scope of the incident, cause production delays. These delays could result in financial losses (through penalty clauses in contracts) or the loss of a customer.

4.1.4 Recommendations

To reduce the risks associated with the weaknesses we have identified, we recommend implementation of at least the following:

- Install all updated security measures for the Windows 2000 Advance Server OS, available from Microsoft (<u>http://windowsupdate.microsoft.com</u>), including the latest Service Pack (SP3), as well as the latest updates for MSDE.
- Set up a rigorous process for regularly updating each product required for the smooth operation of the ePO server. Consideration could be given to using a specialized product to carry out this task.
- Remove extraneous applications that are no longer being used (e.g.: PCAnywhere).

- Perform a general hardening of the operating system, based on the recommendations of the SANS Institute in collaboration with CIS (Center for Internet Security), available at the following address: http://www.sans.org/score.
- Review access rights on the directories identified as sensitive in our audit forms (appended) to limit access solely to personnel who truly require access (normally the administrators).
- Verify all anomalies detected in the reports generated by the management console. Pay particular attention to stations or servers that do not seem to have an antivirus solution (despite the fact that the ePO agent has been deployed) as well as the many machines whose signature files (.DAT) or filtering engine have not been updated for a long time.
- Implement an internal process to take advantage of all monitoring functionalities offered by the ePO server in order to engage in proactive monitoring. The goal is to quickly identify problems of any type (including virus activity), to permit a prompt response to an incident.

We strongly recommend that the above recommendations be implemented to increase the general security of the ePolicy Orchestrator server. The audit forms (appended) can be consulted for an overview of the weaknesses identified in the audit and for more detail.

4.2 Anticipated Cost

To implement the majority of the recommendations, the main requirement will be an investment of time by one or more technicians.

The first thing to do would be to draft an action plan for implementation of all the recommendations. An external consultant who specializes in information system security could help formulate a process for hardening the system. We recommend that tests be done in a development environment before any hardening is carried out.

The software programs are not the main source of weakness; and while it is possible to correct all of the problems identified, there is no guarantee that new problems won't arise that could threaten the security of the company unless there is an effective monitoring process. Any evaluation conducted prior to implementing such a process should cover a great deal more than just the monitoring offered by the ePolicy Orchestrator server. Furthermore, specialized software should be purchased or developed in-house to ensure regular updating of security hotfixes.

4.3 Interim Solution

We are aware that preparation of an action plan to secure the ePO server requires time and personnel. It is likely that a special budget would have to be approved.

In the meantime, we recommend an interim solution: install a firewall on the ePolicy Orchestrator server so that only the ports the server requires (incoming and outgoing) are used.

This would reduce exposure to risk by blocking use of a suspect service, or the use by an attacker of a dangerous protocol such as NetBIOS, or the use of an inactive program such as PCAnywhere (although the latter simply needs to be uninstalled).

If the company is not using a firewall, Network Associates, the firm that developed the dPolicy Orchestrator management console, also has a firewall solution ("Mcafee Desktop Firewall v7.5") that integrates perfectly with the product audited.

Please note that this interim measure does not in any way replace the main recommendations.

REFERENCES

The following is a list of documents that were used to some degree in the preparation of this report and were not necessarily cited in the text of the report:

- Information Security Breaches Survey 2002, PriceWaterHouseCooper, <u>http://www.pwcglobal.com/extweb/ncsurvres.nsf/DocID/845A4956604575</u> <u>9E80256B9D003A4773</u>
- 2002 CSI/FBI Computer Crime and Security Survey (spring 2002), http://www.gocsi.com/forms/fbi/pdf.html
- Global Information Security Survey 2002, Ernst & Young (march 2002) <u>http://www.ey.com/global/download.nsf/International/Global Information</u> <u>Security Survey 2002/\$file/FF0210.pdf</u>
- The Twenty Most Critical Internet Security Vulnerability Version 2.504, The SANS Institute, May 2, 2002, <u>http://www.sans.org/top20/</u>
- Windows 2000 Security Recommendation Guides, National Security Agency, <u>http://nsa1.www.conxion.com/win2k/download.htm</u>
- Vulnerability Note VU#635463, Center of Internet Security (CERT), http://www.kb.cert.org/vuls/id/635463
- Security Information About SQL Server, <u>http://www-tus.csx.cam.ac.uk/pc_support/security/sqlsecurity.html</u>
- Penetration Testing: NAI ePolicy Orchestrator, Newsgroup, http://lists.insecure.org/lists/pen-test/2001/Nov/0006.html
- Auditors Checklists and Other Audit Information, Fred Cohen & Associate, <u>http://www.all.net/books/audit/index.html</u>
- IIS 5.0 Baseline Security Checklist, Microsoft Technet, <u>http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/iis5cl.asp</u>
- Secure Internet Information Services 5 Checklist, Microsoft Technet, <u>http://www.microsoft.com/technet/treeview/default.asp?url=/technet/securit</u> <u>y/tools/chklist/iis5chk.asp</u>
- An Overview of Threat and Risk Assessment, James Bayne, Sans Institute Reading Rooms, January 22, 2002, <u>http://www.sans.org/rr/audit/overview.php</u>
- Securing Windows 2000 Step-by-Step Version 1.5, SANS Institute, July 1, 2001
- Information technologies Code of practice for information security management, BS 7799/ISO 17799, First edition, 2000-12-01