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 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:

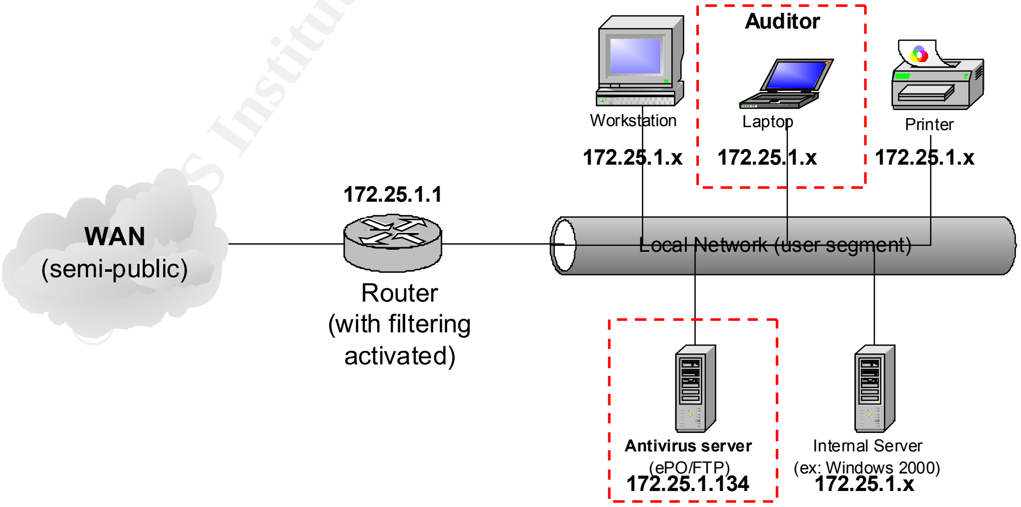


Diagram of Audited Network

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 $283,000[2].

[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.

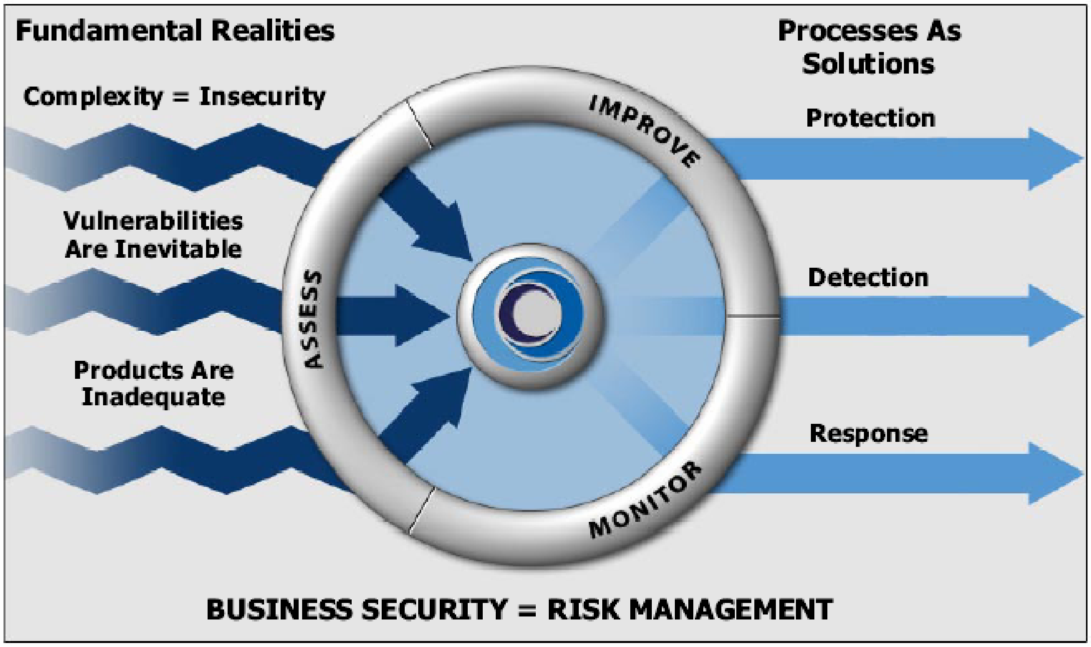
Without monitoring, there can be no response. Or rather, there will be a response, but it will be a response to an incident that has already caused damage.

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



source: http://www.counterpane.com/presentation2.pdf (page 6)

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 e-mail 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.

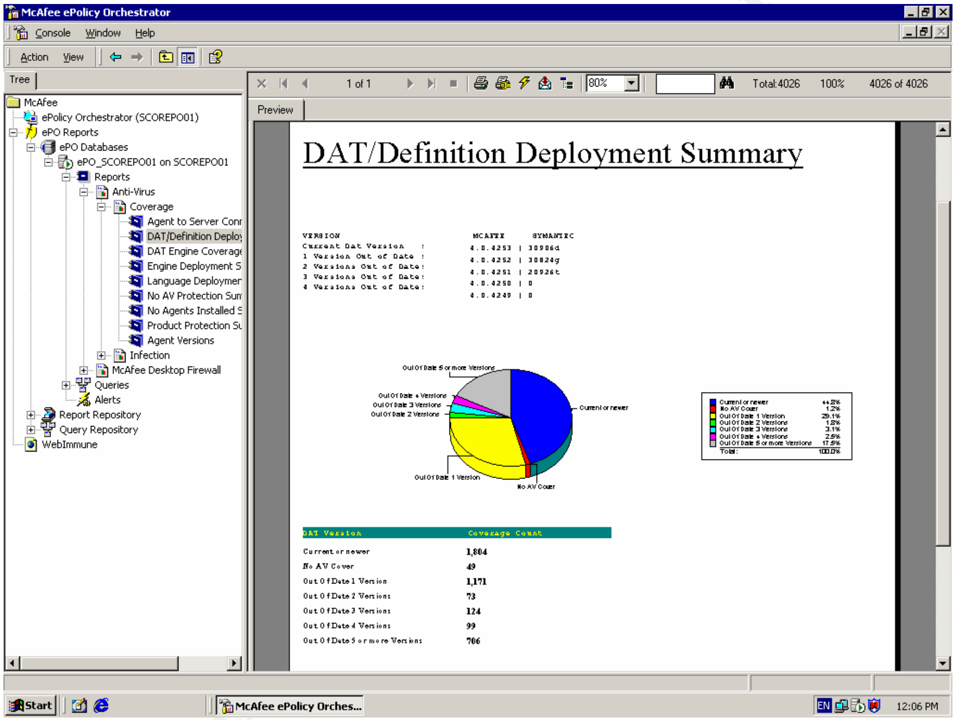
Although workstations are last on the list, this does not mean that they are not important. Even though the vast majority of viruses will be filtered out before reaching a workstation, in many cases the workstation antivirus program will be the first line of defense. Particularly when it comes to filtering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



DAT/Definition Deployment Summary

```
VERSION                                MCAFEE      SYMANTEC
Current Dat Version    :              4.0.4253 | 30906d
1 Version Out of Date  :              4.0.4252 | 30824g
2 Versions Out of Date:               4.0.4251 | 20926t
3 Versions Out of Date:               4.0.4250 | 0
4 Versions Out of Date:               4.0.4249 | 0
```

🟦	Current or newer	44.8%
🟥	No AV Cover	1.2%
🟨	Out Of Date 1 Version	29.1%
🟩	Out Of Date 2 Versions	1.8%
▨	Out Of Date 3 Versions	3.1%
🟪	Out Of Date 4 Versions	2.5%
⬜	Out Of Date 5 or more Versions	17.5%
	Total:	100.0%

DAT Version	Coverage Count
Current or newer	1,804
No AV Cover	49
Out Of Date 1 Version	1,171
Out Of Date 2 Versions	73
Out Of Date 3 Versions	124
Out Of Date 4 Versions	99
Out Of Date 5 or more Versions	706

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:

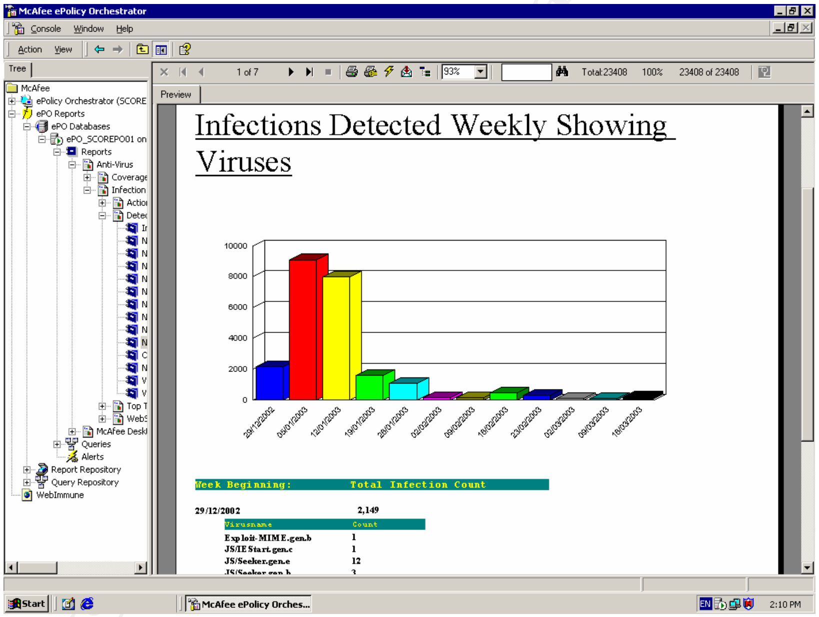
- systems that do not have the latest version of the filtering engine
- systems that do not have the latest version of the signature
- systems that do not have antivirus software, although the ePO agent is installed.

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.



Infections Detected Weekly Showing Viruses

Week Beginning:	Total Infection Count
29/12/2002	2,149

Virusname	Count
Exploit-MIME.gen.b	1
JS/IEStart.gen.c	1
JS/Seeker.gen.e	12
JS/Seeker.gen.b	3

Trend chart generated by ePO

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 time-based 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**
Threat	**Low**	Insignificant	Minor	Major
	Medium	Minor	Major	Critical
	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
Loss of availability of ePO service	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.
	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.
Loss of availability of the FTP service	No workstation or server will be able to get an updated signature file.	Minor	In the normal updating process, this would have little impact.
	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	An incorrectly configured antivirus solution, even if it is always updated, cannot filter properly. This could lead to the infection of stations and servers.
	Incorrect configuration of the response to virus detection can lead to loss of availability.	Major	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.	Critical	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.	Critical	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 governing access to the ePO management console	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.
	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 (www.google.com) were relatively fruitless.

Searching on underground sites such as www.astalavista.com and www.phrack.com produced little.

In the SANS Institute (http://www.sans.org/rr/) 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 (http://lists.insecure.org/lists/pen-test/2001/Nov/0006.html) 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:
http://www.nextgenss.com/software/ngssqlcrack.html

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), http://www.isaca.org/cobit.htm

- Certified Students and Posted Practicals, SANS Institute, http://www.giac.org/GSNA.php

- Auditors Checklists and Other Audit Information, Fred Cohen & Associate, http://www.all.net/books/audit/index.html

- 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, http://www.iso-17799.com/

The risk level assessment explained in **Section 1.2** is based on a corporate in-house 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

2.1 Explanation of the form used

Control objective	Describe the purpose of the audit
Test location	Clearly identify the location where the test is to be conducted
Tests to be conducted	Instructions for gathering the information required to assess the risk level
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
Risk evaluation	Risk calculation for each result obtained

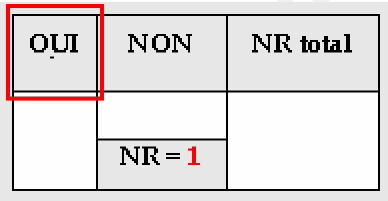
2.2 Explanation of the Risk Level calculation

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

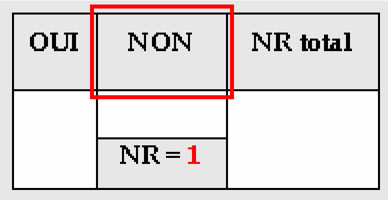
Once all the questions have been answered, one can determine the server's risk level.

2.2.1 Organization of questions

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



OUI	NON	NR total
	NR = 1	



OUI	NON	NR total
	NR = 1	

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:

Results Summary Table

	Total assessed risk	**Maximum risk**	**Percentage (%)**
Operating system security and open session validation	**?**	**48**	**?**
Product configurations	**?**	**109**	**?**
Access rights	**?**	**92**	**?**
Monitoring mechanisms	**?**	**54**	**?**
Total risk: ____ for a maximum of 303 = ____ %			

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 ☒ From the server audited
Tests to be conducted :	Observe the following instructions: 1. Right button on the icon « **My Computer** » 2. Choose « **Properties** » 3. Choose the tab « **Network Identification** »

<table>
<tr><td></td><td>4. Choose « <b>Properties</b> »
5. Be sure that « <b>workgroup</b> » is checked in the section « <b>Member of</b> ».

<b>Note :</b> Take a screen capture of this window (alt-printscreen) and save the image in a wordpad document under the name « <b>1-type.rtf</b> »</td></tr>
<tr><td>Reference(s) :</td><td>Not applicable / personal experience</td></tr>
<tr><td>Expected results :</td><td>The server should be in a « workgroup » in order to limit the use of authentification strictly to the local account with the administrator privileges.</td></tr>
<tr><td>Objective / Subjective :</td><td>Objective</td></tr>
<tr><td>Results :</td><td><i>- Insert results here -</i></td></tr>
<tr><td>Brief explanation of risk :</td><td>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.</td></tr>
<tr><td>Risk evaluation :</td><td>Is the server installed as a server member to a domain or as a domain controller?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td>RL=3</td><td></td><td></td></tr>
</table>
<b>TOTAL RISK LEVEL: [ ] / 6</b></td></tr>
</table>

[**2**] Control objective :	Verification of the basic vulnerabilities relative to the operating system.
Test location :	☐ From the auditor station ☒ 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 « **Use SUS Server :** » 5. Press on« **Start Scan** » 6. When finish, choose « **Print** » in the section

<table>
<tr><td></td><td>« <b>Action</b> ».
7. You can also paste the information in an application supporting the html format (ex : Word) and save under the name « <b>2-msba.doc</b> ».

<b>Note :</b> 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).</td></tr>
<tr><td>Reference(s) :</td><td>The MBSA tool is available at no charge at the following address: http://download.microsoft.com/download/e/5/7/e57f498f-2468-4905-aa5f-369252f8b15c/mbsasandup.msi</td></tr>
<tr><td>Expected results :</td><td>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</td></tr>
<tr><td>Objective / Subjective :</td><td>Objective</td></tr>
<tr><td>Results :</td><td><i>- Insert results here -</i></td></tr>
<tr><td>Brief explanation of risk :</td><td>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.</td></tr>
<tr><td>Risk evaluation :</td><td>Are some hotfix missing for the operating system ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td>RL = 4</td><td></td><td></td></tr>
</table>
</td></tr>
</table>

Are some hotfix missing for IIS ?

YES	NO	RL total
RL = 4		

Are some hotfix missing for SQL/MSDE ?

YES	NO	RL total
RL = 4		

Have vulnerabilities of critical level been recorded in the section « Windows Scan Results » ?

YES	NO	RL total
RL = 4		

Have vulnerabilities of critical level been recorded in the section « Internet Information Services (IIS) Scan Results » ?

YES	NO	RL total
RL = 4		

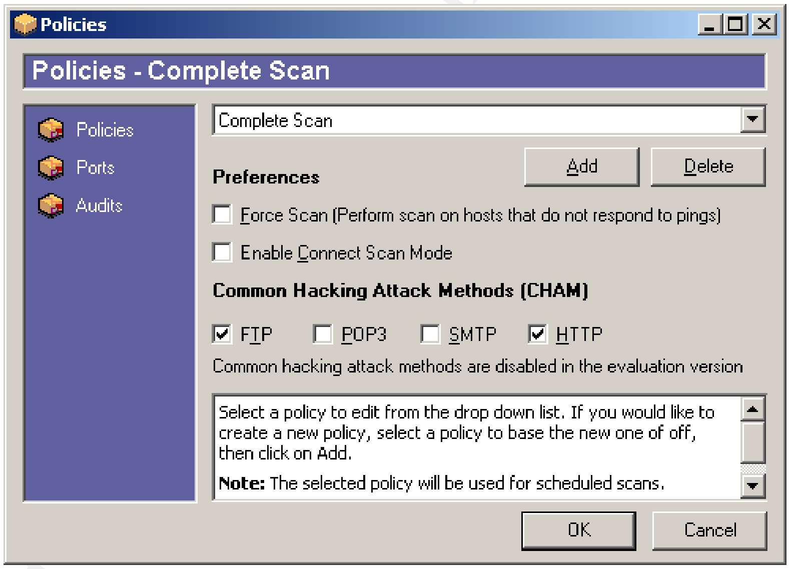
Have vulnerabilities of critical level been recorded in the section « SQL Server Scan Results: Instance (default) » ?

YES	NO	RL total
RL = 4		

Have vulnerabilities of critical level been recorded in the section « Desktop Application Scan Results » ?

YES	NO	RL total
RL = 2		

TOTAL RISK LEVEL: [ ] / 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 Ports Audits Add Delete OK Cancel Complete Scan **Preferences** ☐ Force Scan (Perform scan on hosts that do not respond to pings) ☐ Enable Connect Scan Mode **Common Hacking Attack Methods (CHAM)** ☑ FTP ☐ POP3 ☐ 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. Afterward, observe the following instructions: 1. Open the application« **Retina** » 2. 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 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 -*

<table>
<tr><td>Brief explanation of risk :</td><td>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.</td></tr>
<tr><td>Risk evaluation :</td><td>Have some « High Risk » level vulnerabilities been found ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td>RL = 4</td><td></td><td></td></tr>
</table>
Have some « Medium Risk » level vulnerabilities been found ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td>RL = 2</td><td></td><td></td></tr>
</table>
<b>TOTAL RISK LEVEL: [ ] / 6</b></td></tr>
</table>

[**4**] Control objective :	Verification of suspicious services or not anticipated remote response.
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 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. - **1433** – Pre-required by MSDE 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).

<table>
<tr><td>Objective / Subjective :</td><td>Objective</td></tr>
<tr><td>Results :</td><td><i>- Insert results here -</i></td></tr>
<tr><td>Summary Brief explanation of risk :</td><td>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.</td></tr>
<tr><td>Risk evaluation :</td><td>Are ports other than the ports anticipated open ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td><b>RL = 3</b></td><td></td><td></td></tr>
</table>

If so, which ? :
____
____
____

Is the port 139 open ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td><b>RL = 3</b></td><td></td><td></td></tr>
</table>

<b>TOTAL RISK LEVEL: [ ] / 6</b></td></tr>
</table>

<table>
<tr><td>[<b>5</b>] Control objective :</td><td>Analysis of the sessions and the suspicious applications on the server.</td></tr>
<tr><td>Test location :</td><td>□ From the auditor station
☒ From the server audited</td></tr>
<tr><td>Tests to be conducted :</td><td><b>Pre-required :</b> Having downloaded and installed on 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:
<i>netstat –an > 5-netstat.txt</i>
3. Type the following line:
<i>fport /p > 5-fport.txt</i></td></tr>
</table>

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

<b>TOTAL RISK LEVEL: [ ] / 4</b></td></tr>
</table>

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 ☒ From the server audited
Tests to be conducted :	**Pre-required :** Having obtained by the system 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

<table>
<tr><td></td><td>Take a screen capture and save it in a Wordpad document under the name « <b>6-verepo.rtf</b> »</td></tr>
<tr><td>Reference(s) :</td><td>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</td></tr>
<tr><td>Expected results :</td><td>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.</td></tr>
<tr><td>Objective / Subjective :</td><td>Objective</td></tr>
<tr><td>Results :</td><td><i>- Insert results here -</i></td></tr>
<tr><td>Summary Brief explanation of risk :</td><td>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 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.</td></tr>
<tr><td>Risk evaluation :</td><td>Is the version of the ePO server installed the version 2.5.1 Build 213 (or a more recent version) ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td></td><td>RL = 5</td><td></td></tr>
</table>
<b>TOTAL RISK LEVEL: [ ] / 5</b></td></tr>
</table>

[**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: 1. Open « **DumpSec** » 2. Choose « **Select Computer** » in the menu « **Report** » and enter the IP address of the

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

<b>TOTAL RISK LEVEL: [ ] / 4</b></td></tr>
</table>

[**8**] Control objective :	Verification for presence of a functional antivirus on the ePO server.
Test location :	□ From the auditor station ☒ 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 : _____________ 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 : 1. Choose « **Internet Explorer** » 2. Type the following line in « **Address** » : http://localhost:8081 3. Take a screen capture and save at the end of file « **8-antivirus.rtf** » 4. 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 10th, 2002. Requires an access to « PrimeSupport KnowledgeCenter Service Portal » at the following address : https://mysupport.nai.com
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 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/download/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 » : - 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
	RL = 3	

If not, what is the configuration ? :

____
____
____

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 come periodiquely 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...

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. 2. Right button on « **Default FTP Site** » 3. 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 ». In the tab « **Messages** » : - A legal message should be inscribed in the section« Welcome » 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.

<table>
<tr><td></td><td>- A list of the IP address that have the right to access the FTP server should be written.</td></tr>
<tr><td>Objective / Subjective :</td><td>Objective</td></tr>
<tr><td>Results :</td><td><i>- Insert results here -</i></td></tr>
<tr><td>Summary Brief explanation of risk :</td><td>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.</td></tr>
<tr><td>Risk evaluation :</td><td>Is the connexion number limited to the station/server requirering an update ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td></td><td><b>RL = 2</b></td><td></td></tr>
</table>
Is the option « Enable Logging » selected ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td></td><td><b>RL = 3</b></td><td></td></tr>
</table>
Is the option « Allow Anonymous Connections » selected and also the option « Allow only anonymous connections » ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td></td><td><b>RL = 2</b></td><td></td></tr>
</table>
Is only the group « Administrators » present in the section« Operators » ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td></td><td><b>RL = 4</b></td><td></td></tr>
</table>
</td></tr>
</table>

Is a legal message inscribed in the section « Welcome » ?

YES	NO	RL total
	RL = 2	

Is the option « a directory located in this computer » selected ?

YES	NO	RL total
	RL = 2	

Is the directory « Ftproot »located on the same driver as the operating system ?

YES	NO	RL total
RL = 3		

Is only the option « Read » and « Log visits » selected ?

YES	NO	RL total
	RL = 2	

Is the option « Denied Access » selected?

YES	NO	RL total
	RL = 3	

Does a list of the IP address that have the right to access the FTP server exist ?

YES	NO	RL total
	RL = 3	

TOTAL RISK LEVEL: [ ] / 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: 1. Open the « **ePO** » management console 2. 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). 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.

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

	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 ☒ 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. 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 entirely automated. Journals (« logs ») must be available in order to validate that the process works well. The structure on the audited FTP server must be as faithful as possible to the FTP server of NAI.
Objective / Subjective :	Subjective
Results :	*- Insert results here -*
Summary Brief	In order to assure an efficient update of the antivirus,

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

[**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: 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** ».
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.

<table>
<tr><td></td><td>In the tab « <b>Report</b> » and « <b>Exclusion</b> » :

Nothing as to be activated and no exclusion should be defined.</td></tr>
<tr><td>Objective / Subjective :</td><td>Objective</td></tr>
<tr><td>Results :</td><td><i>- Insert results here -</i></td></tr>
<tr><td>Summary Brief explanation of risk :</td><td>A configuration mistake in the settings deployed by the management console increases the infection probabilities on the total system of the servers in the information system.</td></tr>
<tr><td>Risk evaluation :</td><td>Is the option « Enforce Policies for NetShield v4.5 » selected ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td></td><td>RL = 4</td><td></td></tr>
</table>

Is the option « Force Install NetShield v4.5 » selected and is an installation package selected ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td></td><td>RL = 4</td><td></td></tr>
</table>

Are at least the following options selected in the tab « Detection » ?
<ul>
<li>Scan « <b>Inbound File</b> »</li>
<li>Scan « <b>Network Drive</b> »</li>
<li><b>Selected file type only</b></li>
<li><b>Enable on acces scanning at system startup</b></li>
</ul>
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td></td><td>RL = 4</td><td></td></tr>
</table>

If not, which are missing ? :
____
____
____
____</td></tr>
</table>

Are all the options selected in the tab « Advance » ? (do not consider the zone « **Compressed File** »).

YES	NO	RL total
	RL = 3	

If not, which are missing ? :

____

____

____

____

Is at least « **Clean infected file automatically** » selected in the tab « Action » ?

YES	NO	RL total
	RL = 3	

If not, what is the default action ? :

____

____

Have exclusions been defined in the tab « Exclusion » ?.

YES	NO	RL total
RL = 2		

If so, explain the exclusions :

____

____

____

____

TOTAL RISK LEVEL: [ ] / 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 : 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 :	*- Insert results here -*
Summary Brief explanation of risk :	The less accounts exist with administrative rights and 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

<table>
<tr><td></td><td>have been done).

Otherwise, there is a great probability that an attacker may retrieve the available accounts list and their rights.</td></tr>
<tr><td>Risk evaluation :</td><td>Is the account « <b>Guest</b> » deactivated ?
<table><tr><th>YES</th><th>NO</th><th>RL total</th></tr><tr><td></td><td><b>RL = 4</b></td><td></td></tr></table>
Is the account « <b>Guest</b> » renamed for something less explicit ?
<table><tr><th>YES</th><th>NO</th><th>RL total</th></tr><tr><td></td><td><b>RL = 2</b></td><td></td></tr></table>
Is the account « <b>administrator</b> » renamed for something less explicit ?
<table><tr><th>YES</th><th>NO</th><th>RL total</th></tr><tr><td></td><td><b>RL = 2</b></td><td></td></tr></table>
Does the default account « <b>IUSR_computername</b> » as been renamed for something less explicit ?
<table><tr><th>YES</th><th>NO</th><th>RL total</th></tr><tr><td></td><td><b>RL = 2</b></td><td></td></tr></table>
Is a service account for the ePO software present ?
<table><tr><th>YES</th><th>NO</th><th>RL total</th></tr><tr><td></td><td><b>RL = 3</b></td><td></td></tr></table>
</td></tr>
</table>

Is a service account for the saving software (ex : BackupExec) present ?

YES	NO	RL total
	RL = 2	

Is a service account for the remote access (ex : Terminal Service) present ?

YES	NO	RL total
	RL = 2	

TOTAL RISK LEVEL: [ ] / 17

[**13**] Control objective :	Verification of the user groups 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 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** » (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** ». - The service account for the saving software should be only in the group « **Backup_Operators** ».

<table>
<tr><td></td><td>- The account « <b>Guest</b> » should not be found in the group « Guest ».
- Only the service account required by IIS can be found in the group « <b>Guest</b> ».
- No user should be found in the groups « <b>Power Users</b> », « <b>Replicator</b> » and « <b>Users</b> ».</td></tr>
<tr><td>Objective / Subjective :</td><td>Objective</td></tr>
<tr><td>Results :</td><td><i>- Insert results here -</i></td></tr>
<tr><td>Summary Brief explanation of risk :</td><td>Well managed groups permit only the appropriate 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.</td></tr>
<tr><td>Risk evaluation :</td><td>Is the account « <b>administrator</b> » (If not renamed) found in the group « <b>administrators</b> » ?
<table><tr><th>YES</th><th>NO</th><th>RL total</th></tr><tr><td><b>RL = 3</b></td><td></td><td></td></tr></table>
Is the service account for the saving software found only in the group « <b>Backup_Operators</b> » ?
<table><tr><th>YES</th><th>NO</th><th>RL total</th></tr><tr><td></td><td><b>RL = 2</b></td><td></td></tr></table>
If not, where is it located ? :
____
____
Is the account « <b>Guest</b> » found in the group « <b>Guest</b> » ?
<table><tr><th>YES</th><th>NO</th><th>RL total</th></tr><tr><td><b>RL = 2</b></td><td></td><td></td></tr></table></td></tr>
</table>

Is only the service account required by IIS found in the group « **Guest** » ?

YES	NO	RL total
	X	9
	RL = 2	

Are accounts found in one of the following groups : « **Power Users** », « **Replicator** » and « **Users** » ?

YES	NO	RL total
RL = 2		

If so, explain :

____

____

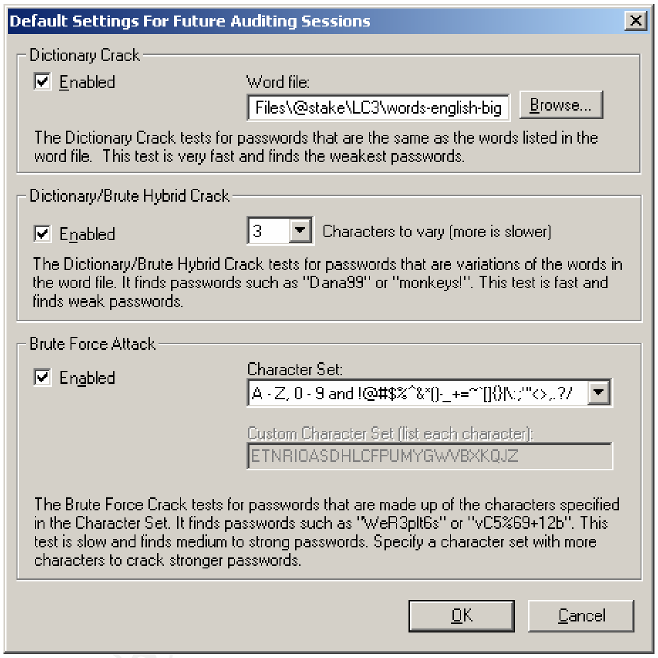
____

TOTAL RISK LEVEL: [ ] / 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 ☒ 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. **<u>Part 1</u> :** 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

Dictionary Crack

☑ Enabled

Word file: Files\@stake\LC3\words-english-big

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

☑ Enabled

Character Set: A - Z, 0 - 9 and !@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/

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 "WeR3pl6s" 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 from a PWDUMP File…** »
6. Choose the file « **14-pwdump.txt** »
7. 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.
9. 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

<table>
<tr><td></td><td>The Pwdump3 tool is available at the following address :
http://www.polivec.com/pwdumpdownload.html</td></tr>
<tr><td>Expected results :</td><td>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.</td></tr>
<tr><td>Objective / Subjective :</td><td>Objective</td></tr>
<tr><td>Results :</td><td><i>- Insert results here -</i></td></tr>
<tr><td>Summary Brief explanation of risk :</td><td>Without a robust authentification (including a small letter, a capital letter a number and a special character) the probabilities for an attacker to take control of the server is higher.</td></tr>
<tr><td>Risk evaluation :</td><td>Have passwords been found after a maximum of 12 hours of « brute force » ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td><b>RL = 4</b></td><td></td><td></td></tr>
</table>
Are passwords for accounts with administrative rights robust and conform ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td></td><td><b>RL = 4</b></td><td></td></tr>
</table>
Are passwords for service accounts composed of 14 characters ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td></td><td><b>RL = 3</b></td><td></td></tr>
</table>
<b>TOTAL RISK LEVEL: [ ] / 11</b></td></tr>
</table>

[**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 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

<table>
<tr><td></td><td>Concerning the rights on the directory « <b>Ftproot</b> » :

- 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</td></tr>
<tr><td>Objective / Subjective :</td><td>Objective</td></tr>
<tr><td>Results :</td><td><i>- Insert results here -</i></td></tr>
<tr><td>Summary Brief explanation of risk :</td><td>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.</td></tr>
<tr><td>Risk evaluation :</td><td>Do only the groups « Administrators » and « System » have an authorization « Full Control » on the directory « <b>MSFTPSVC1 »</b> ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td></td><td><b>RL = 3</b></td><td></td></tr>
</table>
If not, which ? :
____
____
____

Do the rest of the groups (if existing) have only an authorization « Read » on the directory « <b>MSFTPSVC1</b> » ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td></td><td><b>RL = 3</b></td><td></td></tr>
</table>
If not, which ? :
____
____
____</td></tr>
</table>

Does the group « Everyone » have rights on the directory « **MSFTPSVC1 »** ?

YES	NO	RL total
RL = 3		

Does only the group « Administrators » have an authorization « Full Control » on the directory « **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 ? :

____

____

____

Does the group « Everyone » have rights on the directory « **Ftproot »** ?

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) 5. 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 :** 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

<table>
<tr><td></td><td>password :
- Permitting authentification to the server
- Permitting authentification to the « ePO » management console.</td></tr>
<tr><td>Objective / Subjective :</td><td>Objective : except for validation of the password format given by the administrator (if present).</td></tr>
<tr><td>Results :</td><td><i>- Insert results here -</i></td></tr>
<tr><td>Summary Brief explanation of risk :</td><td>Without a robust authentification (including small letter, 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.</td></tr>
<tr><td>Risk evaluation :</td><td>Does the account « SA » have a password ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td></td><td><b>RL = 4</b></td><td></td></tr>
</table>
Is the password for the account « SA » composed of 14 characters ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td></td><td><b>RL = 2</b></td><td></td></tr>
</table>
Is the password different from the one for authentification to the server (i.e. : Windows) ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td></td><td><b>RL = 3</b></td><td></td></tr>
</table>
Is the password different from the one for authentification to an ePO console ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td></td><td><b>RL = 4</b></td><td></td></tr>
</table>
<b>TOTAL RISK LEVEL: [ ] / 12</b></td></tr>
</table>

<table>
<tr><td>[<b>17</b>] Control objective :</td><td>Verification of access rights on certain important files of ePolicy Orchestrator.</td></tr>
<tr><td>Test location :</td><td>□ From the auditor station
☒ From the server audited</td></tr>
<tr><td>Tests to be conducted :</td><td>Observe the following instructions:

1. Conduct a search on all the drives for « <b>DB</b> » using « Start » - « Search » – « For File and Folders » (or touch windows + f)
2. Right button on the file « <b>DB</b> » found in the directory « <b>\ePO\2.0</b> »
3. Choose « <b>Properties</b> »
4. Choose the tab « <b>Security</b> »
5. Take a screen capture for each of the accounts present and save it in a Wordpad file under the name « <b>17-dbepo.rtf</b> »</td></tr>
<tr><td>Reference(s) :</td><td>Not applicable / Personal experience</td></tr>
<tr><td>Expected results :</td><td>Only the group « <b>administrators</b> » should have access in « <b>Full Control</b> » to the file « <b>DB</b> ».

<b>Note :</b> The group « <b>Backup Operators</b> » could also be present (if required by the saving software).</td></tr>
<tr><td>Objective / Subjective :</td><td>Objective</td></tr>
<tr><td>Results :</td><td><i>- Insert results here -</i></td></tr>
<tr><td>Summary Brief explanation of risk :</td><td>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.</td></tr>
<tr><td>Risk evaluation :</td><td>Does only the group « administrators » have an access « Full Control » to the file « DB ?
<table><tr><th>YES</th><th>NO</th><th>RL total</th></tr><tr><td rowspan="2"></td><td></td><td rowspan="2"></td></tr><tr><td><b>RL = 4</b></td></tr></table>
If not, which ? :
____
____
____

<b>TOTAL RISK LEVEL: [ ] / 4</b></td></tr>
</table>

[**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: 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 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 -*

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

TOTAL RISK LEVEL Concerning the access rights	**? / 92**

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 ☒ 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** » 3. Double click « **Event Viewer** » 4. Right button on the icon « **Application** » and choose « **Properties** » 5. Take a screen capture and save in a Wordpad 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** » : 1. 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.

<table>
<tr><td></td><td>Concerning the settings for « Audit Policy » :

- For each points, « <b>Success</b> » and also « <b>Failure</b> » should be activated. (« Audit process tracking » can not be selected)</td></tr>
<tr><td>Objective / Subjective :</td><td>Objective</td></tr>
<tr><td>Results :</td><td><i>- Insert results here -</i></td></tr>
<tr><td>Summary Brief explanation of risk :</td><td>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.</td></tr>
<tr><td>Risk evaluation :</td><td>In the settings for « Application » :

Is the option « Do not overwrite events (clear log manually) » selected ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td><b>RL = 2</b></td><td></td></tr>
</table>

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 ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td><b>RL = 4</b></td><td></td></tr>
</table>

If not, what is the value ? :
____

In the settings of « Security » :

Is the option « Do not overwrite events (clear log manually) » selected ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td><b>RL = 3</b></td><td></td></tr>
</table>
</td></tr>
</table>

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
	RL = 4	

If not, what is the value ? :

____

In the settings for « System » :

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
	RL = 4	

If not, what is the value ? :

____

In the settings for « Audit Policy », are each points for, « **Success** » and also for « **Failure** » activated ?

YES	NO	RL total
	RL = 3	

If not, which are not ? :

____

____

TOTAL RISK LEVEL: [ ] / 22

[**20**] Control objective :	Verification of the general process for the verification of the ePO management console.
Test location :	□ From the auditor station ☒ From the server audited
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 : 1. Open the « **ePO** » management console 2. Choose « **Login** » 3. 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 Login** » 5. Double click on « **Reports** » 6. Double click on « **Anti-virus** » 7. Double click on « **Coverage** » 8. 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 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. In the report « **Product Protection Summary** » : - 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 -*

<table>
<tr><td>Summary Brief explanation of risk :</td><td>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.</td></tr>
<tr><td>Risk evaluation :</td><td>Have suspicious events or mistakes been recorded in the « Server Events » ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td>RL = 4</td><td></td><td></td></tr>
</table>
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) ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td></td><td>RL = 4</td><td></td></tr>
</table>
Have some versions of signature older than the one before the latest version been identified ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td>RL = 4</td><td></td><td></td></tr>
</table>
If so, explain :
____
____
Have little (or none) version not updated for the engine (« <b>Out of date Engine</b> ») been identified ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td></td><td>RL = 4</td><td></td></tr>
</table>
</td></tr>
</table>

If not, explain :

____

____

Have stations or servers been identified without an antivirus solution ?

YES	NO	RL total
RL = 4		

If so, explain :

____

____

____

Have products considered unknown been identified ?

YES	NO	RL total
RL = 4		

If so, explain :

____

____

____

Have many version of NetShield or VirusScan been identified ?

YES	NO	RL total
RL = 4		

If so, explain :

____

____

____

Have other antivirus solution (present without a valid reason) been identified ?

YES	NO	RL total
RL = 4		

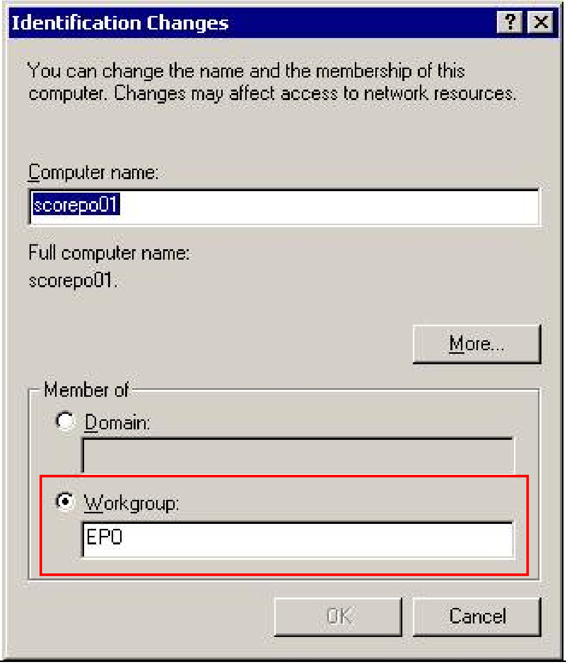
	If so, explain : ____ ____ ____ **TOTAL RISK LEVEL: [ ] / 32**

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 ☒ From the server audited
Tests to be conducted :	Observe the following instructions: 1. Right button on the icon « **My Computer** » 2. Choose « **Properties** » 3. Choose the tab « **Network Identification** » 4. Choose « **Properties** » 5. 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 » :  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

<table>
<tr><td>Brief explanation of risk :</td><td>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.</td></tr>
<tr><td>Risk evaluation :</td><td>Is the server installed as a server member to a domain or as a domain controller?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td>
RL=3</td><td>X</td><td>0</td></tr>
</table>
<b>TOTAL RISK LEVEL: [0] / 6</b></td></tr>
</table>

[**2**] Control objective :	Verification of the basic vulnerabilities relative to the operating system.
Test location :	□ From the auditor station ☒ 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 « **Use SUS Server :** » 5. Press on« **Start Scan** » 6. When finish, choose « **Print** » in the section « **Action** ». 7. You can also paste the information in an application supporting the html format (ex : Word) and save under the name « **2-msba.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

	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 :	File content « 2-msba.doc » :

Computer name:	Epo\Scorepo01
IP address:	172.25.1.134
Security report name:	Epo - Scorepo01 (01-15-2003 11-35 AM)
Scan date:	15/01/2003 11:35 AM
Security Update database version:	1.0.1.449
Security assessment:	Incompthande Scan (Could not compthande one or more requested checks.)

Security Updates

Score	Issue	Result
Check failed (critical)	Windows Security Updates	17 security updates are missing, are ort of date, or could not be confirmed.

Security Update	**Description**	**Reason**
MS02-042	Flaw in Network Connection Manager Could Enable Privilege Andhevation (Q326886)	File C:\WINNT\system32\nandman.dll has a file version [5.0.2195.2779] that is thes than what is expected [5.0.2195.5974].
MS02-045	Unchecked Buffer in Network Share Provider can thead to Denial of Service (Q326830)	File C:\WINNT\system32\xactsrv.dll has a file version [5.0.2134.1] that is thes than what is expected [5.0.2195.5971].
MS02-048	Flaw in Certificate ERLollment Control Could Allow Dandhandion of Digital Certificates (Q323172)	The registry key **SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\{43F8F289-7A20-11D0-8F06-00C04FC295E1}** does not exist. It is Pre-required for this patch to be considered installed.
MS02-050	Certificate Validation Flaw Could Enable	File C:\WINNT\system32\adsldp.dll has a file version [5.0.2195.4959] that is thes

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

				Can Allow Scripts to Thevy Requests as User	
			MS02-008	XMLHTTP Control Can Allow Access to Local File	Pthease refer to Q306460 for a dandaithed explanation.
			MS02-053	Buffer Overrun in SmartHTML Interprander Could Allow Code Execution (Q324096)	Pthease refer to Q306460 for a dandaithed explanation.
			MS02-064	Windows 2000 Default Authorizations Could Allow Trojan Horse Program (Q327522)	Pthease refer to Q306460 for a dandaithed explanation.
			MS02-065	Buffer Overrun in Microsoft Data Access Components Could Thead to Code Execution (Q329414)	Pthease refer to Q306460 for a dandaithed explanation.
	Check failed (critical)	IIS Security Updates	1 critical security updates are missing.		
			Security Update	**Description**	**Reason**
			MS02-062	Cumulative Patch for Internet Information Service (Q327696)	File C:\WINNT\system32\adsiis.dll has a file version [5.0.2195.5255] that is thes than what is expected [5.0.2195.6048].
	Check failed (critical)	SQL Server Security Updates	Instance (default): 3 security updates are missing, are ort of date, or could not be confirmed.		
			Security Update	**Description**	**Reason**
			MS02-020	SQL Extended Procedure Functions Contain Unchecked Buffers (Q319507)	File d:\ePO\MSSQL7\Binn\xplog70.dll has a file version [1998.11.13.0] that is thes than what is expected [2000.28.5.0].
				The latest service pack for this product is not installed.	The latest service pack for this product is not installed. Currently SQL Server 7.0 SP3 is installed. The latest service pack is SQL Server 7.0 SP4.
			MS02-035	SQL Server Installation Process May Theave Passwords on	Pthease refer to Q306460 for a dandaithed explanation.

<table>
<tr><td></td><td></td><td>System (Q263968)</td></tr>
<tr><td>Check passed</td><td>Windows Media Player Security Updates</td><td>No critical security updates are missing.</td></tr>
<tr><td>Check not performed</td><td>Exchange Server Security Updates</td><td>Exchange Server is not installed.</td></tr>
</table>

Windows Scan Results

Vulnerabilities

<table>
<tr><th>Score</th><th>Issue</th><th>Result</th></tr>
<tr><td>Check failed (criticals)</td><td>Restrict Anonymous</td><td>Computer is running with RestrictAnonymous = 0. This level prevents basic enumeration of user accounts, account policies, and system information. Sand RestrictAnonymous = 2 to ensure maximum security.</td></tr>
<tr><td>Check failed (no-critical)</td><td>Password Expiration</td><td>Some unspecified user accounts (5 of 6) have no-expiring passwords.
<table>
<tr><th>User</th></tr>
<tr><td>Administrator</td></tr>
<tr><td>Backupexec_svr</td></tr>
<tr><td>Guest</td></tr>
<tr><td>SQLAgentCmdExec</td></tr>
<tr><td>TsInternetUser</td></tr>
<tr><td>IUSR_SCOREPO01</td></tr>
</table></td></tr>
<tr><td>Check passed</td><td>Local Account Password Test</td><td>Some user accounts (1 of 6) have blank or simpthe passwords, or could not be analyzed.
<table>
<tr><th>User</th><th>Weak Password</th><th>Locked Ort</th><th>Disabthed</th></tr>
<tr><td>Guest</td><td>Weak</td><td>-</td><td>Disabthed</td></tr>
<tr><td>Administrator</td><td>-</td><td>-</td><td>-</td></tr>
<tr><td>Backupexec_svr</td><td>-</td><td>-</td><td>-</td></tr>
<tr><td>IUSR_SCOREPO01</td><td>-</td><td>-</td><td>-</td></tr>
<tr><td>SQLAgentCmdExec</td><td>-</td><td>-</td><td>-</td></tr>
<tr><td>TsInternetUser</td><td>-</td><td>-</td><td>-</td></tr>
</table></td></tr>
<tr><td>Check passed</td><td>File System</td><td>All hard drives (3) are using the NTFS file system.
<table>
<tr><th>Drive Thandter</th><th>File System</th></tr>
<tr><td>C:</td><td>NTFS</td></tr>
<tr><td>D:</td><td>NTFS</td></tr>
<tr><td>E:</td><td>NTFS</td></tr>
</table></td></tr>
<tr><td>Check passed</td><td>Autologon</td><td>Autologon is not configured on this computer.</td></tr>
<tr><td>Check passed</td><td>Guest Account</td><td>The Guest account is disabthed on this computer.</td></tr>
<tr><td>Check passed</td><td>Administrators</td><td>No more than 2 Administrators were found on this computer.
<table>
<tr><th>User</th></tr>
<tr><td>Administrator</td></tr>
<tr><td>Backupexec_svr</td></tr>
</table></td></tr>
</table>

Additional System Information

Score	Issue	Result
Best practice	Auditing	Logon Success and Logon Failure auditing are both Enabled.

<table>
<tr><td>Best practice</td><td>Services</td><td>Some potentially unnecessary services are installed.<table><tr><th>Service</th><th>State</th></tr><tr><td>FTP Publishing Service</td><td>Running</td></tr><tr><td>Telnand</td><td>Stopped</td></tr></table></td></tr>
<tr><td>Additional information</td><td>Shares</td><td>4 share(s) are present on Your computer.<table><tr><th>Share</th><th>Directory</th><th>Share ACL</th><th>Directory ACL</th></tr><tr><td>ADMIN$</td><td>C:\WINNT</td><td>Admin Share</td><td>Users - RX, Power Users - RWXD, Administrators - F, NT AUTHORITY\SYSTEM - F, Everyone - RX</td></tr><tr><td>C$</td><td>C:\</td><td>Admin Share</td><td>Everyone - F</td></tr><tr><td>D$</td><td>D:\</td><td>Admin Share</td><td>Everyone - F</td></tr><tr><td>E$</td><td>E:\</td><td>Admin Share</td><td>Everyone - F</td></tr></table></td></tr>
<tr><td>Additional information</td><td>Windows Version</td><td>Computer is running Windows 2000 or greater.</td></tr>
</table>

Internet Information Services (IIS) Scan Results

Vulnerabilities

Score	Issue	Result
Unabthe to scan	Sampthe Applications	Error reading the IIS mandabase.
Unabthe to scan	IIS Admin Virtual Directory	Error reading the IIS mandabase.
Unabthe to scan	Parent Paths	Error reading the IIS mandabase.
Unabthe to scan	Msadc and Scripts Virtual Directories	Error reading the IIS mandabase.
Check failed (critical)	IIS Lockdown Tool	The IIS Lockdown tool has not been run on the machine.

Additional System Information

<table>
<tr><th>Score</th><th>Issue</th><th>Result</th></tr>
<tr><td>Best practice</td><td>Domain Controller Test</td><td>IIS is not running on a domain controller.</td></tr>
<tr><td>Best practice</td><td>IIS Logging Enabled</td><td>Some web or FTP sites are not using the recommended logging options.<table><tr><th>Name</th><th>Protocol</th></tr><tr><td>Default FTP Site</td><td>FTP</td></tr></table></td></tr>
</table>

SQL Server Scan Results: Instance (default)

Vulnerabilities

<table>
<tr><th>Score</th><th>Issue</th><th>Result</th></tr>
<tr><td>Check failed (critical)</td><td>CmdExec rothe</td><td>CmdExec is not restricted to sysadmin.</td></tr>
<tr><td>Check failed (critical)</td><td>Folder Authorizations</td><td>Authorizations on the SQL Server installation folders are not sand properly.<table><tr><th>Instance</th><th>Folder</th><th>User</th></tr><tr><td>(default)</td><td>d:\ePO\MSSQL7\Binn</td><td>\Everyone</td></tr><tr><td>(default)</td><td>d:\ePO\MSSQL7\Data</td><td>\Everyone</td></tr></table></td></tr>
</table>

<table>
<tr><td>Check failed (no-critical)</td><td>Service Accounts</td><td>SQL Server and/or SQL Server Agent Services accounts are members of the local Administrators grorp or run as LocalSystem.<table><tr><th>Instance</th><th>Service</th><th>Account</th><th>Issue</th></tr><tr><td>(default)</td><td>MSSQLServer</td><td>SYSTEM</td><td>LocalSystem account.</td></tr><tr><td>(default)</td><td>SQLServerAgent</td><td>SYSTEM</td><td>LocalSystem account.</td></tr></table></td></tr>
<tr><td>Check failed (no-critical)</td><td>Sysadmin rothe members</td><td>BUILTIN\Administrators grorp is part of sysadmin rothe.</td></tr>
<tr><td>Check failed (no-critical)</td><td>SQL Server Security Mode</td><td>SQL Server authentication mode is sand to SQL Server and Windows (Mixed Mode).</td></tr>
<tr><td>Check passed</td><td>Sysadmins</td><td>No more than 2 members of sysadmin rothe are present.</td></tr>
<tr><td>Check passed</td><td>Exposed SQL Password</td><td>The 'sa' password and SQL service account password are not exposed in text file.<table><tr><th>File Name</th><th>Status</th></tr><tr><td>C:\WINNT\TEMP\sqlsp.log</td><td>No passwords exposed</td></tr><tr><td>C:\WINNT\sqlstp.log</td><td>No passwords exposed</td></tr></table></td></tr>
<tr><td>Check passed</td><td>SQL Account Password Test</td><td>No SQL user accounts have weak passwords.</td></tr>
<tr><td>Check passed</td><td>Domain Controller Test</td><td>SQL Server is not running on a domain controller.</td></tr>
<tr><td>Check passed</td><td>Registry Authorizations</td><td>The Everyone grorp does not have more than Read access to the SQL Server registry keys.</td></tr>
<tr><td>Check passed</td><td>Guest Account</td><td>The Guest account is not Enabled in any of the databases.</td></tr>
</table>

Desktop Application Scan Results

Vulnerabilities

<table>
<tr><th>Score</th><th>Issue</th><th>Result</th></tr>
<tr><td>Check failed (no-critical)</td><td>IE Zones</td><td>Internet Explorer zones do not have secure settings for some users.<table><tr><th>User</th><th>Zone</th><th>Level</th><th>Recommended Level</th></tr><tr><td>SCOREPO01\Administrator</td><td>Local intranand</td><td>Custom</td><td>Medium-Low</td></tr><tr><td>SCOREPO01\Administrator</td><td>Trusted sites</td><td>Custom</td><td>Low</td></tr><tr><td>SCOREPO01\Administrator</td><td>Internet</td><td>Custom</td><td>Medium</td></tr><tr><td>SCOREPO01\Administrator</td><td>Restricted sites</td><td>Custom</td><td>High</td></tr></table></td></tr>
<tr><td>Check not performed</td><td>Macro Security</td><td>No Microsoft Office products are installed</td></tr>
<tr><td>Check not performed</td><td>Ortlook Zones</td><td>No Microsoft Office products are installed</td></tr>
</table>

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

<table>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Risk evaluation :</td>
<td>Are some hotfix missing for the operating system ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td>X</td><td rowspan="2"></td><td rowspan="2">4</td></tr>
<tr><td>RL = 4</td></tr>
</table>
Are some hotfix missing for IIS ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td>X</td><td rowspan="2"></td><td rowspan="2">8</td></tr>
<tr><td>RL = 4</td></tr>
</table>
Are some hotfix missing for SQL/MSDE ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td>X</td><td rowspan="2"></td><td rowspan="2">12</td></tr>
<tr><td>RL = 4</td></tr>
</table>
Have vulnerabilities of critical level been recorded in the section « Windows Scan Results » ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td>X</td><td rowspan="2"></td><td rowspan="2">16</td></tr>
<tr><td>RL = 4</td></tr>
</table>
Have vulnerabilities of critical level been recorded in the section « Internet Information Services (IIS) Scan Results » ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
</table>
</td>
</tr>
</table>

X **RL = 4**		**20**

Have vulnerabilities of critical level been recorded in the section « SQL Server Scan Results: Instance (default) » ?

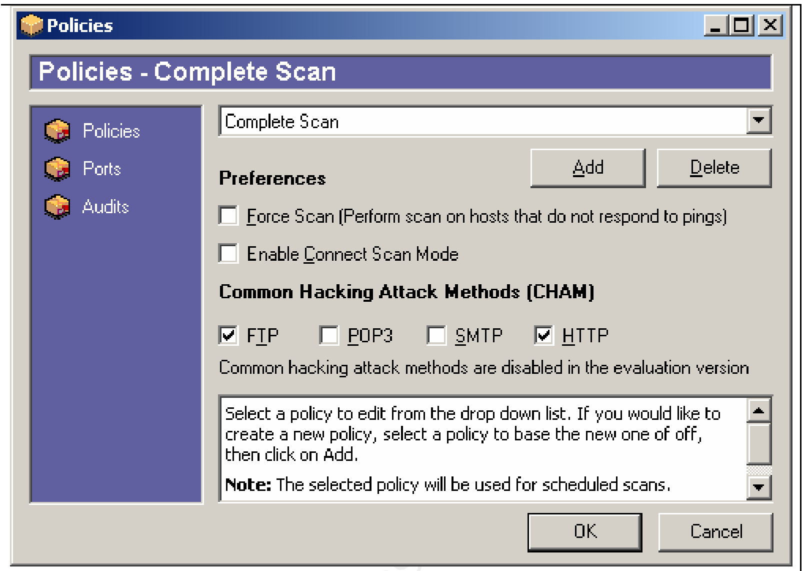
YES	**NO**	**RL total**
X **RL = 4**		**24**

Have vulnerabilities of critical level been recorded in the section « Desktop Application Scan Results » ?

YES	**NO**	**RL total**
RL = 2	**X**	**24**

TOTAL RISK LEVEL: [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.** **Pre-required :** Before conducting the audit, assure yourself that the Retina software is configured as per the following settings:

	 Policies Policies - Complete Scan Policies Ports Audits Add Delete OK Cancel Complete Scan **Preferences** ☐ Force Scan (Perform scan on hosts that do not respond to pings) ☐ Enable Connect Scan Mode **Common Hacking Attack Methods (CHAM)** ☑ FTP ☐ POP3 ☐ 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. Afterward, observe the following instructions: 1. Open the application« **Retina** » 2. 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 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 :	Important extract of the file « 3-Retina.html » : On 13:38:12 Retina performed a vulnerability assessment of 1 system[s] in order to dandermine the security posture of those systems and to ortline fixes for any found vulnerabilities. The systems audited were: 172.025.001.134 Retina's goals in this attack were as follows: • Perform network scan to dandermine all systems and services within Your scan range. • Analysis of those systems and services and perform information gathering techniques. • Attack and exploit any known hothe in the server software and examine the likelihood of being vulnerabthe to those attacks. • Generate information on how to fix all found vulnerabilities.

- 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: 494

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.
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: 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.
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: IUSR_SCOREPO01 - 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.
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: SQLAgentCmdExec - 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. 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: TsInternetUser - 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. 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 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 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
Summary Brief explanation of risk :	If the Retina tool discovers some vulnerabilities with a « high » risk level, it should normally be possible for an

<table>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Risk evaluation :</td>
<td>Have some « High Risk » level vulnerabilities been found ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td>X</td><td rowspan="2"></td><td rowspan="2">4</td></tr>
<tr><td>RL = 4</td></tr>
</table>

Have some « Medium Risk » level vulnerabilities been found ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td>X</td><td rowspan="2"></td><td rowspan="2">2</td></tr>
<tr><td>RL = 2</td></tr>
</table>

<b>TOTAL RISK LEVEL: [6] / 6</b></td>
</tr>
</table>

[**4**] Control objective :	Verification of suspicious services or not anticipated remote response.
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 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. - **1433** – Pre-required by MSDE

	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 / Subjective :	Objective
Results :	File content « 4-superscan.txt » : * **+ 172.25.1.134** |___ 21 |___ 220 scorepo01 Microsoft FTP Service (Version 5.0)... |___ 80 |___ 81 |___ 135 |___ **139** |___ 445 |___ **1026** |___ **1027** |___ **1028** |___ 1433 |___ 3389 |___ **5631** |___ .X..}......Pthease press <Enter>..... |___ 8081
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.

<table>
<tr><td>Risk evaluation :</td><td>Are ports other than the ports anticipated open ?
<table><tr><th>YES</th><th>NO</th><th>RL total</th></tr><tr><td>X</td><td></td><td>3</td></tr><tr><td>RL = 3</td><td></td><td></td></tr></table>
If so, which ? :
_1026,_1027,_1028,_5631______________________
____
____

Is the port 139 open ?
<table><tr><th>YES</th><th>NO</th><th>RL total</th></tr><tr><td>X</td><td></td><td>6</td></tr><tr><td>RL = 3</td><td></td><td></td></tr></table>
<b>TOTAL RISK LEVEL: [6] / 6</b></td></tr>
</table>

[**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: 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 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    0.0.0.0:21             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:81             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1027           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1028           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1044           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1433           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2181           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2182           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2183           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2184           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2185           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2186           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2187           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2188           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5631           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:8081           0.0.0.0:0              LISTENING
  TCP    172.25.1.134:1433      172.25.1.134:2181      ESTABLISHED
  TCP    172.25.1.134:1433      172.25.1.134:2182      ESTABLISHED
  TCP    172.25.1.134:1433      172.25.1.134:2183      ESTABLISHED
  TCP    172.25.1.134:1433      172.25.1.134:2184      ESTABLISHED
  TCP    172.25.1.134:1433      172.25.1.134:2185      ESTABLISHED
  TCP    172.25.1.134:1433      172.25.1.134:2186      ESTABLISHED
  TCP    172.25.1.134:1433      172.25.1.134:2187      ESTABLISHED
  TCP    172.25.1.134:1433      172.25.1.134:2188      ESTABLISHED
  TCP    172.25.1.134:2181      172.25.1.134:1433      ESTABLISHED
  TCP    172.25.1.134:2182      172.25.1.134:1433      ESTABLISHED
  TCP    172.25.1.134:2183      172.25.1.134:1433      ESTABLISHED
  TCP    172.25.1.134:2184      172.25.1.134:1433      ESTABLISHED
  TCP    172.25.1.134:2185      172.25.1.134:1433      ESTABLISHED
  TCP    172.25.1.134:2186      172.25.1.134:1433      ESTABLISHED
  TCP    172.25.1.134:2187      172.25.1.134:1433      ESTABLISHED
  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\inandsrv\inandinfo.exe
1436  NAIMSERV       ->  80    TCP   D:\ePO\2.0\NAIMSERV.EXE
1436  NAIMSERV       ->  81    TCP   D:\ePO\2.0\NAIMSERV.EXE
492   svchost        ->  135   TCP   C:\WINNT\system32\svchost.exe
8     System         ->  139   TCP
8     System         ->  445   TCP
904   MSTask         ->  1026  TCP   C:\WINNT\system32\MSTask.exe
1064  inandinfo      ->  1027  TCP   C:\WINNT\System32\inandsrv\inandinfo.exe
788   sqlservr       ->  1028  TCP   d:\ePO\MSSQL7\binn\sqlservr.exe
8     System         ->  1044  TCP
788   sqlservr       ->  1433  TCP   d:\ePO\MSSQL7\binn\sqlservr.exe
1436  NAIMSERV       ->  2181  TCP   D:\ePO\2.0\NAIMSERV.EXE
1436  NAIMSERV       ->  2182  TCP   D:\ePO\2.0\NAIMSERV.EXE
1436  NAIMSERV       ->  2183  TCP   D:\ePO\2.0\NAIMSERV.EXE
1436  NAIMSERV       ->  2184  TCP   D:\ePO\2.0\NAIMSERV.EXE
1436  NAIMSERV       ->  2185  TCP   D:\ePO\2.0\NAIMSERV.EXE
1436  NAIMSERV       ->  2186  TCP   D:\ePO\2.0\NAIMSERV.EXE
1436  NAIMSERV       ->  2187  TCP   D:\ePO\2.0\NAIMSERV.EXE
1436  NAIMSERV       ->  2188  TCP   D:\ePO\2.0\NAIMSERV.EXE
384   termsrv        ->  3389  TCP   C:\WINNT\System32\termsrv.exe
580   awhost32       ->  5631  TCP   C:\Program
```

<table>
<tr><td></td><td><b>File\Symantec\pcAnywhere\awhost32.exe</b>
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   lsass   -> 500   UDP   C:\WINNT\system32\lsass.exe
256   services   -> 1025 UDP   C:\WINNT\system32\services.exe
520   spoolsv   -> 1040 UDP   C:\WINNT\system32\spoolsv.exe
1064 inandinfo   -> 3456 UDP   C:\WINNT\System32\inandsrv\inandinfo.exe
<b>580   awhost32   -> 5632 UDP   C:\Program File\Symantec\pcAnywhere\awhost32.exe</b></td></tr>
<tr><td>Summary Brief explanation of risk :</td><td>Suspicious or unknowns sessions permit to identify the applications that an attacker could use to his advantage (ex : a Trojan horse).</td></tr>
<tr><td>Risk evaluation :</td><td>Are sessions that seem suspicious or unnecessary applications present ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td><b>X</b></td><td rowspan="2"></td><td rowspan="2"><b>4</b></td></tr>
<tr><td><b>RL = 4</b></td></tr>
</table>
If so, which ? :
__Pcanywhere______________________________
____
____

<b>TOTAL RISK LEVEL: [4] / 4</b></td></tr>
</table>

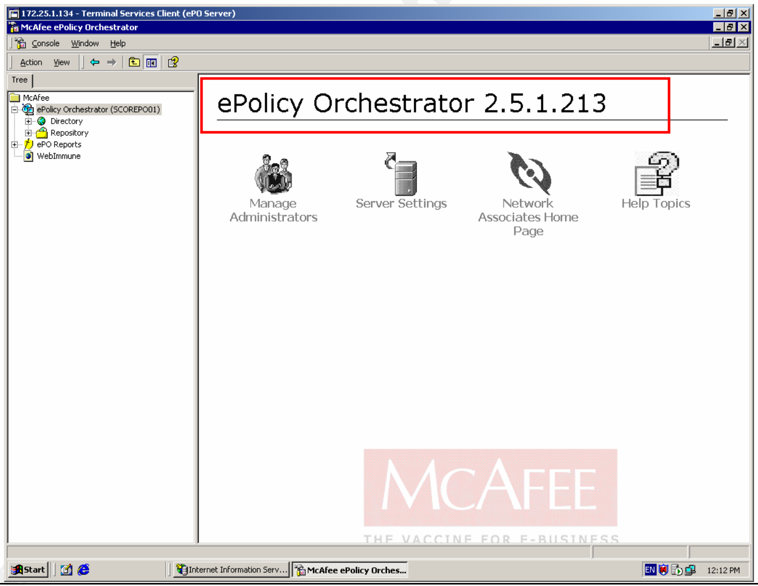
TOTAL RISK LEVEL concerning the security of the operating system and the open sessions	**40 / 48**

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 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** »

<table>
<tr><td>Reference(s) :</td><td>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</td></tr>
<tr><td>Expected results :</td><td>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.</td></tr>
<tr><td>Objective / Subjective :</td><td>Objective</td></tr>
<tr><td>Results :</td><td>Content of « 6-verepo.rft » :


172.25.1.134 - Terminal Services Client (ePO Server)
McAfee ePolicy Orchestrator
Console Window Help
Action View
Tree
McAfee
ePolicy Orchestrator (SCOREPO01)
Directory
Repository
ePO Reports
WebImmune
ePolicy Orchestrator 2.5.1.213
Manage Administrators
Server Settings
Network Associates Home Page
Help Topics
MCAFEE
THE VACCINE FOR E-BUSINESS
Start
Internet Information Serv...
McAfee ePolicy Orches...
12:12 PM
</td></tr>
<tr><td>Summary Brief explanation of risk :</td><td>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 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.</td></tr>
<tr><td>Risk evaluation :</td><td>Is the version of the ePO server installed the version 2.5.1 Build 213 (or a more recent version) ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td>X</td><td>RL = 5</td><td>0</td></tr>
</table>

<b>TOTAL RISK LEVEL: [0] / 5</b></td></tr>
</table>

<table>
<tr><td>[<b>7</b>] Control objective :</td><td>Verification of the active system services on the ePolicy Orchestrator server.</td></tr>
<tr><td>Test location :</td><td>☐ From the auditor station
☒ From the server audited</td></tr>
<tr><td>Tests to be conducted :</td><td><b>Pre-required :</b> Having downloaded and installed on the audited ePO serve, the latest version of DumpSec.

Observe the following instructions:

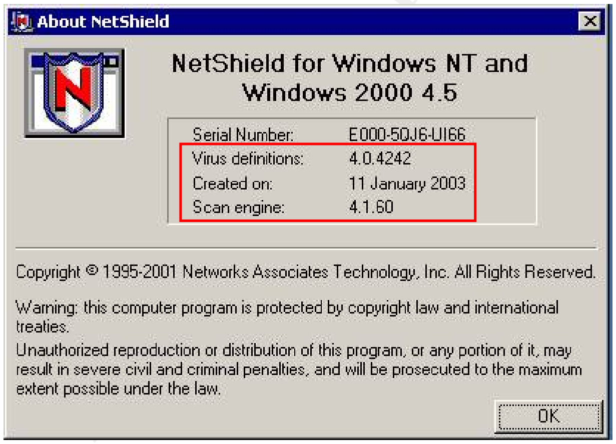
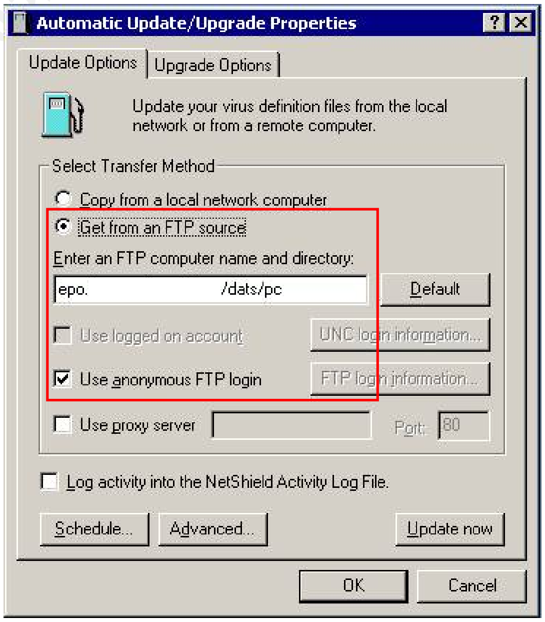
1. Open « <b>DumpSec</b> »
2. Choose « <b>Select Computer</b> » in the menu « <b>Report</b> » and enter the IP address of the audited server.
3. Choose « <b>Dump Services…</b> » in the menu « <b>Report</b> ».
4. Be sure that all the options are selected and press on« <b>OK</b> ».
5. When the result is obtain, choose « <b>Save Report As…</b> » of the menu « <b>File</b> » (or CRTL-S).
6. Choose the type « <b>Fixed width cols</b> » and save under the name « <b>7-services.txt</b> »</td></tr>
<tr><td>Reference(s) :</td><td>The DumpSec tool is available at no charge at the following address :
http://www.systemtools.com/somarsoft/</td></tr>
<tr><td>Expected results :</td><td>There should only be the required services for the efficiency of the active ePO server operations.</td></tr>
<tr><td>Objective / Subjective :</td><td>Objective, except for the application identification which is not necessary.</td></tr>
<tr><td>Results :</td><td>Important extract of file « 7-services.txt » :

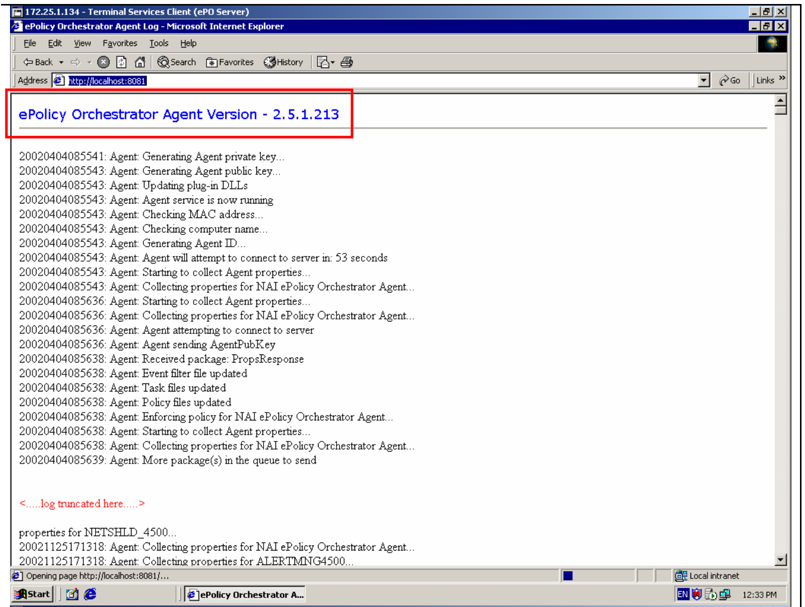
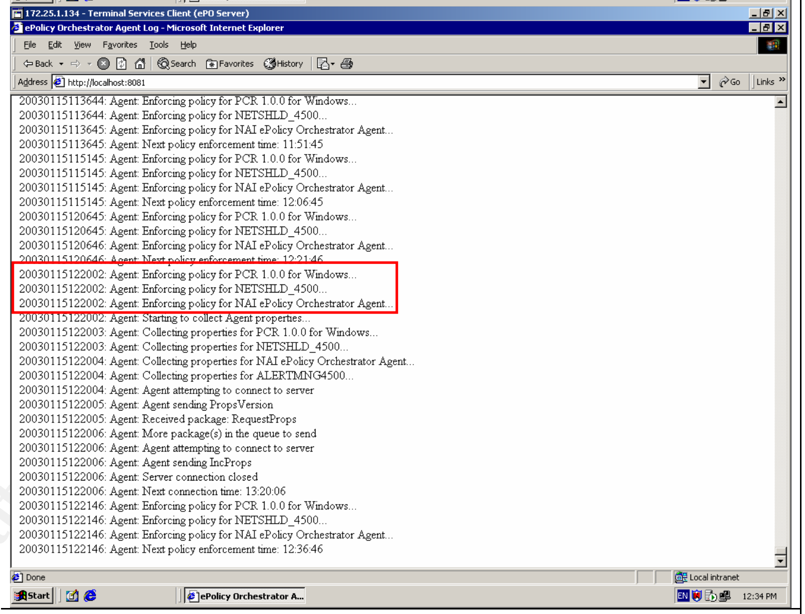
2003-01-15 10:10 - Somarsoft DumpSec (formerly DumpAcl) - \\172.25.1.134
FriendlyName   Name   Status Type   Account
McAfee ePolicy Orchestrator 2.5.1 Server   NAIMSERV2   Running
Win32 LocalSystem
MSSQLServer   MSSQLServer   Running Win32
LocalSystem
<b>pcAnywhere Host Service   awhost32   Running Win32
LocalSystem</b></td></tr>
<tr><td>Summary Brief explanation of risk :</td><td>The least active service on the server, fewer probability for an attacker to exploit a vulnerability to his advantage.</td></tr>
<tr><td>Risk evaluation :</td><td>Are suspicious or unnecessary services used ?
<table><tr><th>YES</th><th>NO</th><th>RL total</th></tr><tr><td><b>X</b></td><td rowspan="2"></td><td rowspan="2"><b>4</b></td></tr><tr><td><b>RL = 4</b></td></tr></table></td></tr>
</table>

	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 ☒ 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 : 1. Choose « **Internet Explorer** » 2. Type the following line in « **Address** » : http://localhost:8081 3. Take a screen capture and save at the end of file « **8-antivirus.rtf** » 4. 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 10th, 2002. Requires an access to « PrimeSupport KnowledgeCenter Service Portal » at the following address : https://mysupport.nai.com
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/download/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 » : - 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: E000-5QJ6-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. OK  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 ○ Copy from a local network computer ● Get from an FTP source Enter an FTP computer name and directory: epo. /dats/pc Default □ Use logged on account UNC login information... ☑ Use anonymous FTP login FTP login information... □ Use proxy server Port: 80 □ Log activity into the NetShield Activity Log File. Schedule... Advanced... Update now OK Cancel

	 
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.

172.25.1.134 - Terminal Services Client (ePO Server)
ePolicy Orchestrator Agent Log - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://localhost:8081
Go Links
Opening page http://localhost:8081/...
Local intranet
Start
ePolicy Orchestrator A...
EN
12:33 PM

ePolicy Orchestrator Agent Version - 2.5.1.213

```
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: 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...
20020404085638: Agent: Collecting properties for NAI ePolicy Orchestrator Agent...
20020404085639: Agent: More package(s) in the queue to send


<.....log truncated here.....>

properties for NETSHLD_4500...
20021125171318: Agent: Collecting properties for NAI ePolicy Orchestrator Agent...
20021125171318: Agent: Collecting properties for ALERTMNG4500...
```

172.25.1.134 - Terminal Services Client (ePO Server)
ePolicy Orchestrator Agent Log - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://localhost:8081
Go Links
Done
Local intranet
Start
ePolicy Orchestrator A...
EN
12:34 PM

```
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 NAI ePolicy Orchestrator Agent...
20030115120646: Agent: Next policy enforcement time: 12:21:46
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 NAI ePolicy Orchestrator Agent...
20030115122004: Agent: Collecting properties for ALERTMNG4500...
20030115122004: Agent: Agent attempting to connect to server
20030115122005: Agent: Agent sending PropsVersion
20030115122005: Agent: Received package: RequestProps
20030115122006: Agent: More package(s) in the queue to send
20030115122006: Agent: Agent attempting to connect to server
20030115122006: Agent: Agent sending IncProps
20030115122006: Agent: Server connection closed
20030115122006: Agent: Next connection time: 13:20:06
20030115122146: Agent: Enforcing policy for PCR 1.0.0 for Windows...
20030115122146: Agent: Enforcing policy for NETSHLD_4500...
20030115122146: Agent: Enforcing policy for NAI ePolicy Orchestrator Agent...
20030115122146: Agent: Next policy enforcement time: 12:36:46
```

Risk evaluation :

Is the version of NetShield installed at least the version **4.5.0.468.1** ?

YES	NO	RL total
X	RL = 4	0

Is the version of « Scan Engine » installed at least the version **4.1.60** ?

YES	NO	RL total
X	RL = 4	0

Is the version of the signature (.DAT) the latest version available the day of the **audit** ?

YES	NO	RL total
X	RL = 4	0

Is the option « Get from an FTP source » selected ?

YES	NO	RL total
X	RL = 3	0

If not, what is the configuration ? :

____

____

____

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
X	RL = 3	0

If not, what is the configuration ? :

____

____

____

Is the option « Use anonymous FTP login » selected ?

YES	**NO**	**RL total**
X	**RL = 3**	**0**

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**
X	**RL = 3**	**0**

If not, what is the version ? :

____

Do the three following lines come periodiquely 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...
```

YES	**NO**	**RL total**
X	**RL = 4**	**0**

If not, what are the results obtained :

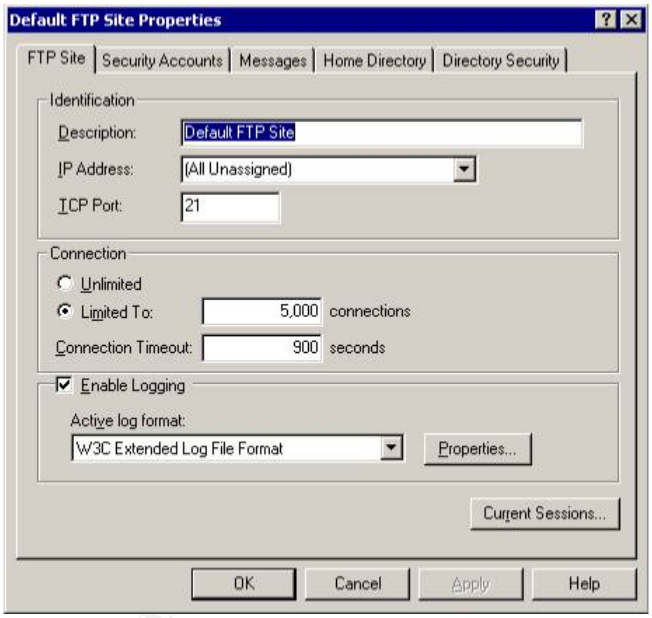
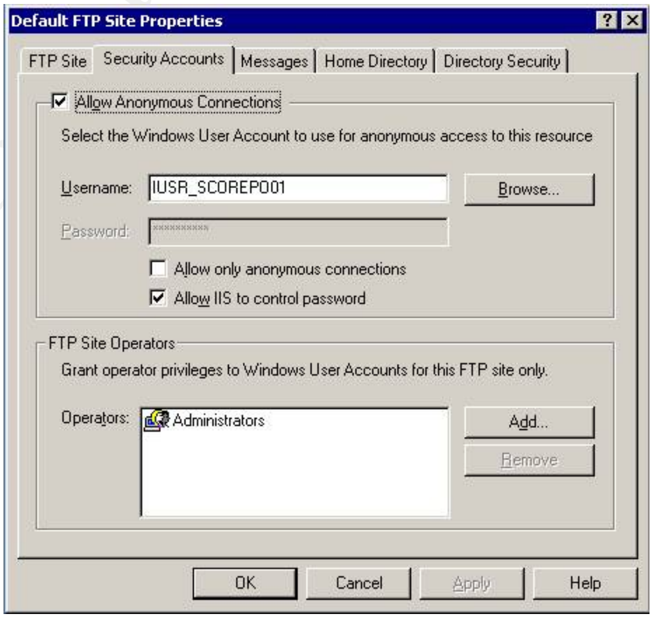
____

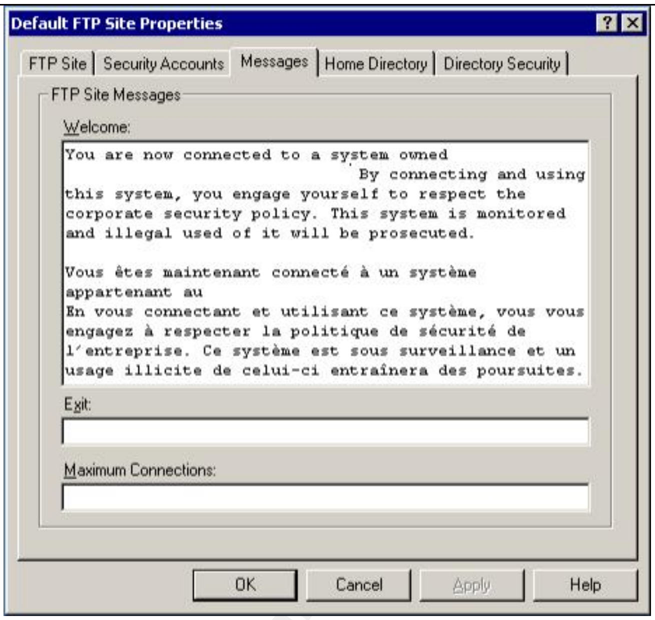
____

____

TOTAL RISK LEVEL: [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: 1. Open « **Internet Service Manager** » via Start – Programs – Administrative Tools. 2. Right button on « **Default FTP Site** » 3. 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 ». In the tab « **Messages** » : - A legal message should be inscribed in the section« Welcome » 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.

	- A list of the IP addresss that have the right to access the FTP server should be written.
Objective / Subjective :	Objective
Results :	File content « 9-ftp.rtf » :  Default FTP Site Properties FTP Site | Security Accounts | Messages | Home Directory | Directory Security Identification Description: Default FTP Site IP Address: (All Unassigned) TCP Port: 21 Connection ○ Unlimited ● Limited To: 5,000 connections Connection Timeout: 900 seconds ☑ Enable Logging Active log format: W3C Extended Log File Format Properties... Current Sessions... 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: IUSR_SCOREPO01 Password: ********** ☐ Allow only anonymous connections ☑ Allow IIS to control password FTP Site Operators Grant operator privileges to Windows User Accounts for this FTP site only. Operators: Administrators Browse... Add... Remove OK Cancel Apply Help



FTP Site Messages

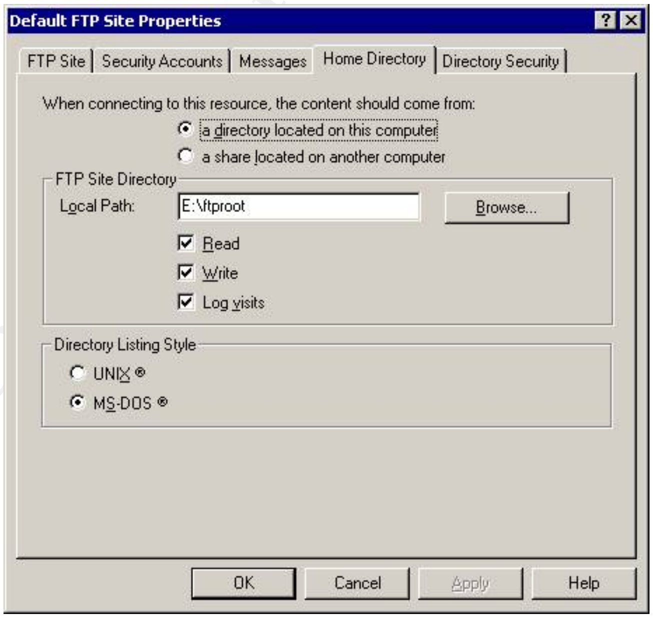
Welcome:

```
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.
```

Exit:

Maximum Connections:



When connecting to this resource, the content should come from:

● a directory located on this computer
○ a share located on another computer

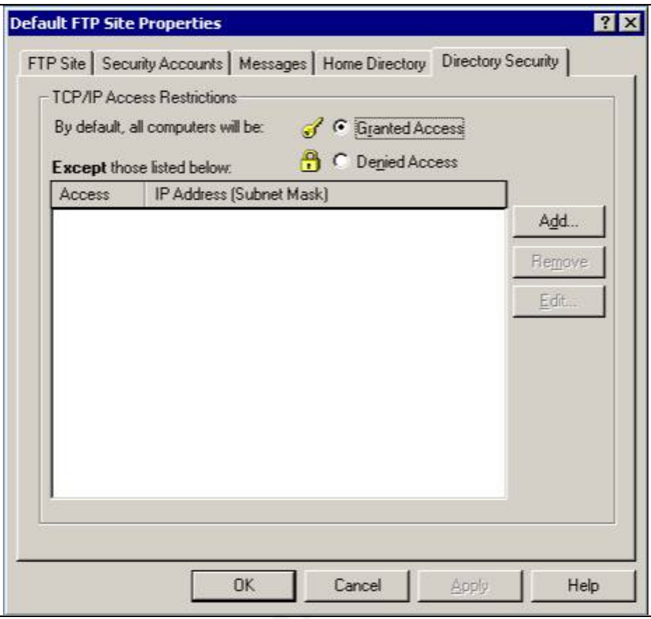
FTP Site Directory

Local Path: E:\ftproot

☑ Read
☑ Write
☑ Log visits

Directory Listing Style

○ UNIX ®
● MS-DOS ®

<table>
<tr><td></td><td>

TCP/IP Access Restrictions
By default, all computers will be: ● Granted Access ○ Denied Access
Except those listed below:
Access | IP Address (Subnet Mask)</td></tr>
<tr><td>Summary Brief explanation of risk :</td><td>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.</td></tr>
<tr><td>Risk evaluation :</td><td>Is the connexion number limited to the station/server requirering an update ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td></td><td><b>X</b>
<b>RL = 2</b></td><td><b>2</b></td></tr>
</table>
Is the option « Enable Logging » selected ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td><b>X</b></td><td><b>RL = 3</b></td><td><b>2</b></td></tr>
</table>
Is the option « Allow Anonymous Connections » selected and also the option « Allow only anonymous connections » ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td></td><td><b>X</b>
<b>RL = 2</b></td><td><b>4</b></td></tr>
</table></td></tr>
</table>

Is only the group « Administrators » present in the section« Operators » ?

YES	NO	RL total
X		4
	RL = 4	

Is a legal message inscribed in the section « Welcome » ?

YES	NO	RL total
X		4
	RL = 2	

Is the option « a directory located in this computer » selected ?

YES	NO	RL total
X		4
	RL = 2	

Is the directory « Ftproot »located on the same driver as the operating system ?

YES	NO	RL total
	X	4
RL = 3		

Is only the option « Read » and « Log visits » selected ?

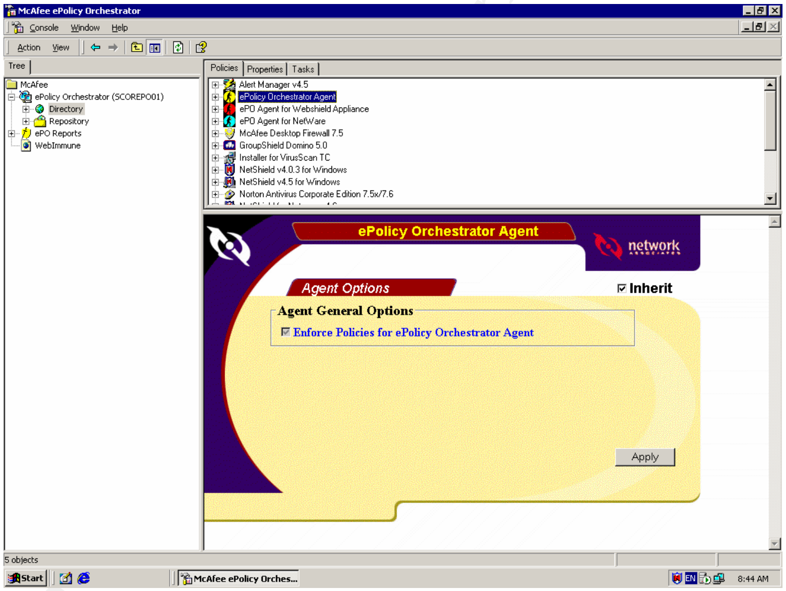
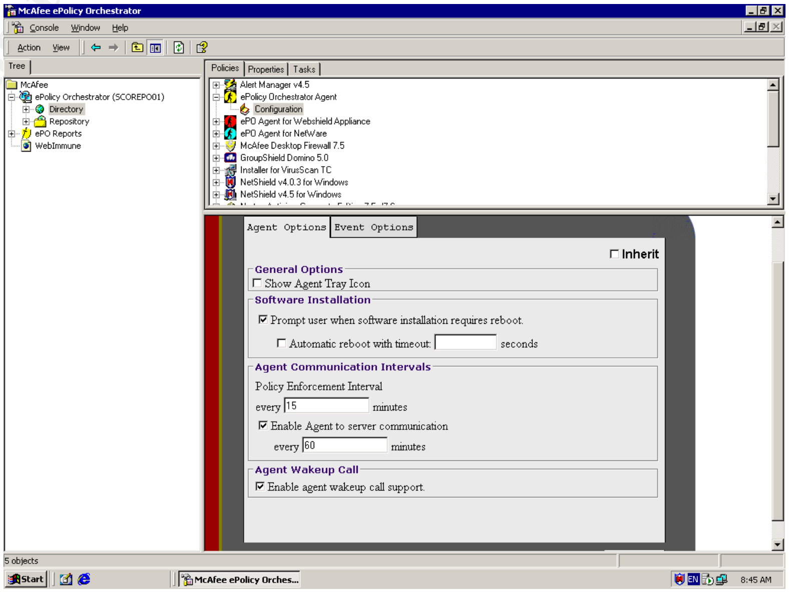
YES	NO	RL total
	X	6
	RL = 2	

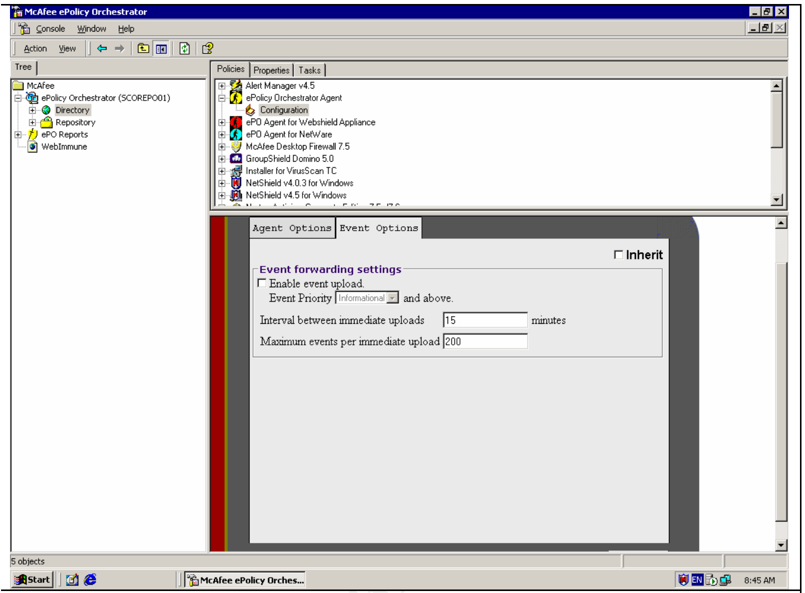
Is the option « Denied Access » selected?

YES	NO	RL total
	X	9
	RL = 3	

<table>
<tr><td></td><td>Does a list of the IP addresss that have the right to access the FTP server exist ?
<table><tr><th>YES</th><th>NO</th><th>RL total</th></tr><tr><td></td><td>X
RL = 3</td><td>12</td></tr></table>
<b>TOTAL RISK LEVEL: [12] / 26</b></td></tr>
</table>

[**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: 1. Open the « **ePO** » management console 2. 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 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 « **Interval between immediate upload** ». Ideally, shorter the delay will be, faster the alerts will be corrected.
Objective / Subjective :	Objective
Results :	File content « 9-ePOAgent.rtf » :  McAfee ePolicy Orchestrator Console Window Help Action View Tree McAfee ePolicy Orchestrator (SCOREPO01) Directory Repository ePO Reports WebImmune Policies Properties Tasks Alert Manager v4.5 ePolicy Orchestrator Agent ePO Agent for Webshield Appliance ePO Agent for NetWare McAfee Desktop Firewall 7.5 GroupShield Domino 5.0 Installer for VirusScan TC NetShield v4.0.3 for Windows NetShield v4.5 for Windows Norton Antivirus Corporate Edition 7.5x/7.6 ePolicy Orchestrator Agent network Agent Options Apply 5 objects Start McAfee ePolicy Orches... 8:44 AM ☑ Inherit Agent General Options ☑ Enforce Policies for ePolicy Orchestrator Agent  McAfee ePolicy Orchestrator Console Window Help Action View Tree McAfee ePolicy Orchestrator (SCOREPO01) Directory Repository ePO Reports WebImmune Policies Properties Tasks Alert Manager v4.5 ePolicy Orchestrator Agent Configuration ePO Agent for Webshield Appliance ePO Agent for NetWare McAfee Desktop Firewall 7.5 GroupShield Domino 5.0 Installer for VirusScan TC NetShield v4.0.3 for Windows NetShield v4.5 for Windows Agent Options Event Options 5 objects Start McAfee ePolicy Orches... 8:45 AM ☐ Inherit General Options ☐ Show Agent Tray Icon Software Installation ☑ Prompt user when software installation requires reboot. ☐ Automatic reboot with timeout: ____ seconds Agent Communication Intervals Policy Enforcement Interval every 15 minutes ☑ Enable Agent to server communication every 60 minutes Agent Wakeup Call ☑ Enable agent wakeup call support.

<table>
<tr><td></td><td>

McAfee ePolicy Orchestrator
Console Window Help
Action View
Tree
McAfee
ePolicy Orchestrator (SCOREPO01)
Directory
Repository
ePO Reports
WebImmune
Policies Properties Tasks
Alert Manager v4.5
ePolicy Orchestrator Agent
Configuration
ePO Agent for Webshield Appliance
ePO Agent for NetWare
McAfee Desktop Firewall 7.5
GroupShield Domino 5.0
Installer for VirusScan TC
NetShield v4.0.3 for Windows
NetShield v4.5 for Windows
Agent Options
Event Options
5 objects
Start
McAfee ePolicy Orches...
8:45 AM

□ Inherit
Event forwarding settings
□ Enable event upload.
Event Priority Informational and above.
Interval between immediate uploads 15 minutes
Maximum events per immediate upload 200</td></tr>
<tr><td>Summary Brief explanation of risk :</td><td>A bad configuration of the ePO agent could render it a little or completely inefficient and even prevent any reaction if a major incident would arise.</td></tr>
<tr><td>Risk evaluation :</td><td>Is the option « Enforce Policies for ePolicy Orchestrator Agent » selected ?
<table><tr><th>YES</th><th>NO</th><th>RL total</th></tr><tr><td>X</td><td>RL = 4</td><td>0</td></tr></table>
Is the option « Prompt user when software installation requires reboot » selected ?
<table><tr><th>YES</th><th>NO</th><th>RL total</th></tr><tr><td>X</td><td>RL = 2</td><td>0</td></tr></table>
Is the option « Enable Agent to server communication » selected with a reasonable delay (ex : 60 minutes by default) ?
<table><tr><th>YES</th><th>NO</th><th>RL total</th></tr><tr><td>X</td><td>RL = 4</td><td>0</td></tr></table>
If not, what is the delay ? : ______________________</td></tr>
</table>

<table>
<tr><td></td><td>Is the option « Enable agent Wakeup call support » selected ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td>X</td><td>
RL = 4</td><td>0</td></tr>
</table>
Is a reasonable delay (depending on the company size) entered in the zone « Interval between immediate upload » ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td>X</td><td>
RL = 2</td><td>0</td></tr>
</table>
If not, what is the delay ? : _______________________

<b>TOTAL RISK LEVEL: [0] / 16</b></td></tr>
</table>

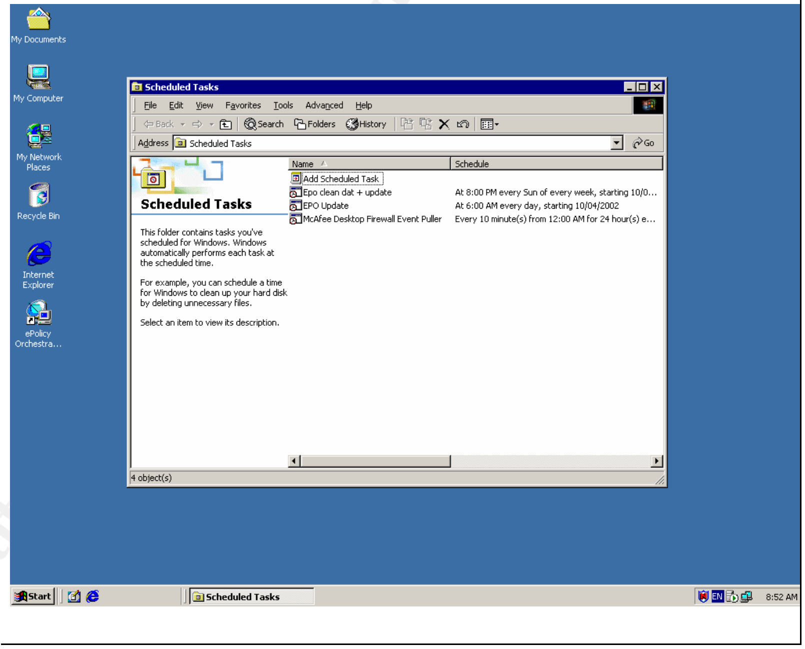
<table>
<tr><td>[<b>10</b>] Control objective :</td><td>Verification of the process for the update of the ePO server</td></tr>
<tr><td>Test location :</td><td>☐ From the auditor station
☒ From the server audited</td></tr>
<tr><td>Tests to be conducted :</td><td>The ePO server does not have an integrated mechanism in order to update the files of the signature (.DAT).

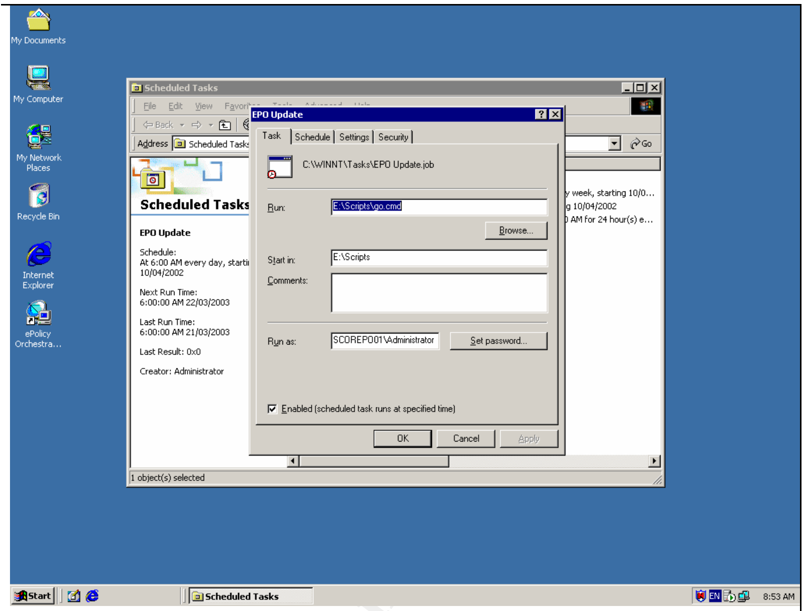
The system administrator may have to choose different kind of way in order to carry out this task. Therefore you must ask the administrator what is the process he uses for the update and adapt this section accordingly.

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 « <b>10-update.rtf</b> »</td></tr>
</table>

	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 entirely automated. Journals (« logs ») must be available in order to validate that the process works well. The structure on the audited FTP server must be as faithful as possible to the FTP server of NAI.
Objective / Subjective :	Subjective
Results :	File content « 10-update.rtf » :  My Documents My Computer My Network Places Recycle Bin Internet Explorer ePolicy Orchestra... Scheduled Tasks File Edit View Favorites Tools Advanced Help Back Search Folders History Address Scheduled Tasks Go Start Scheduled Tasks EN 8:52 AM 4 object(s) Scheduled Tasks This folder contains tasks you've scheduled for Windows. Windows automatically performs each task at the scheduled time. For example, you can schedule a time for Windows to clean up your hard disk by deleting unnecessary files. Select an item to view its description. Name – Schedule Add Scheduled Task Epo clean dat + update – At 8:00 PM every Sun of every week, starting 10/0... EPO Update – At 6:00 AM every day, starting 10/04/2002 McAfee Desktop Firewall Event Puller – Every 10 minute(s) from 12:00 AM for 24 hour(s) e...



EPO Update

Task

C:\WINNT\Tasks\EPO Update.job

Run: E:\Scripts\go.cmd

Start in: E:\Scripts

Comments:

Run as: SCOREPO01\Administrator

☑ Enabled (scheduled task runs at specified time)

Scheduled Tasks

EPO Update

Schedule:
At 6:00 AM every day, starti
10/04/2002

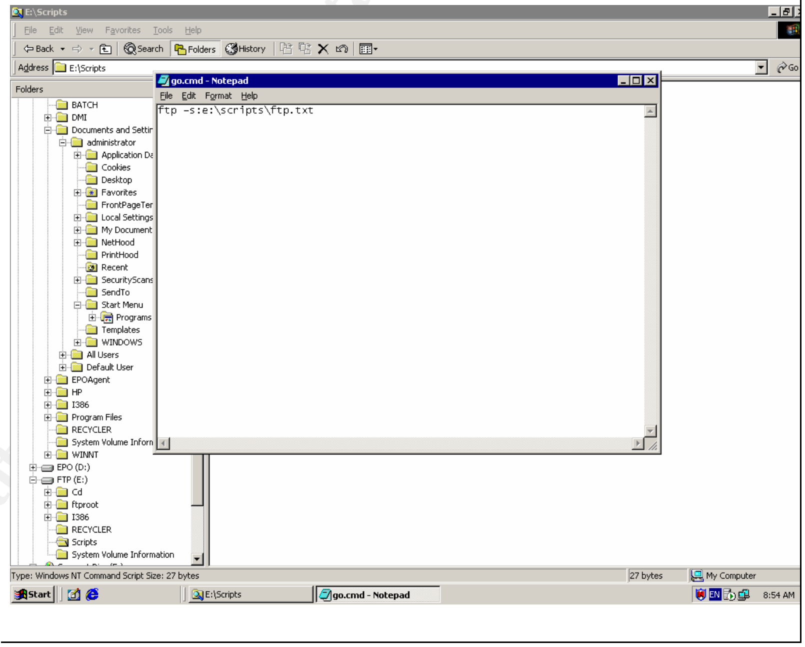
Next Run Time:
6:00:00 AM 22/03/2003

Last Run Time:
6:00:00 AM 21/03/2003

Last Result: 0x0

Creator: Administrator

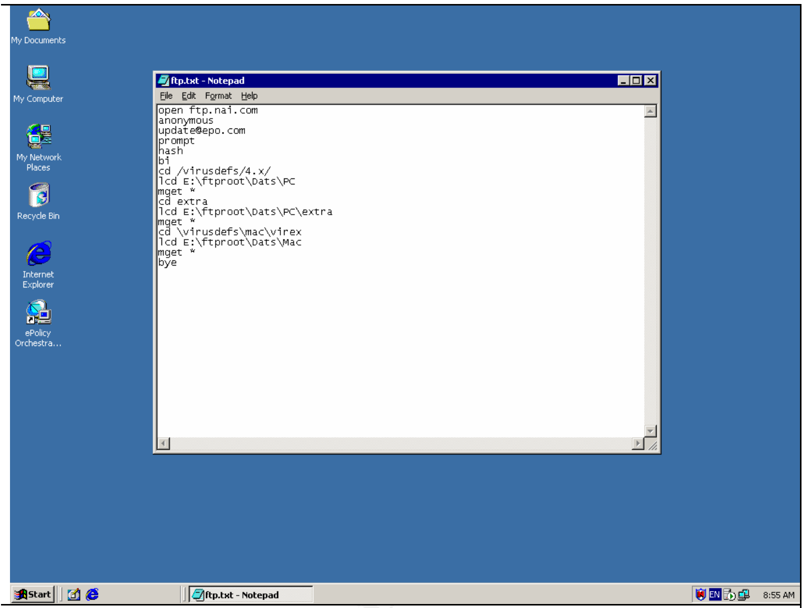
1 object(s) selected



go.cmd - Notepad

```
ftp -s:e:\scripts\ftp.txt
```

Type: Windows NT Command Script Size: 27 bytes



```
open ftp.nai.com
anonymous
update@epo.com
prompt
hash
bi
cd /virusdefs/4.x/
lcd E:\ftproot\Dats\PC
mget *
cd extra
lcd E:\ftproot\Dats\PC\extra
mget *
cd \virusdefs\mac\virex
lcd E:\ftproot\Dats\Mac
mget *
bye
```

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	RL = 4	0

If not, explain the process :

____

____

____

Are the journals (« logs ») available in order to validate the process is working correctly ?

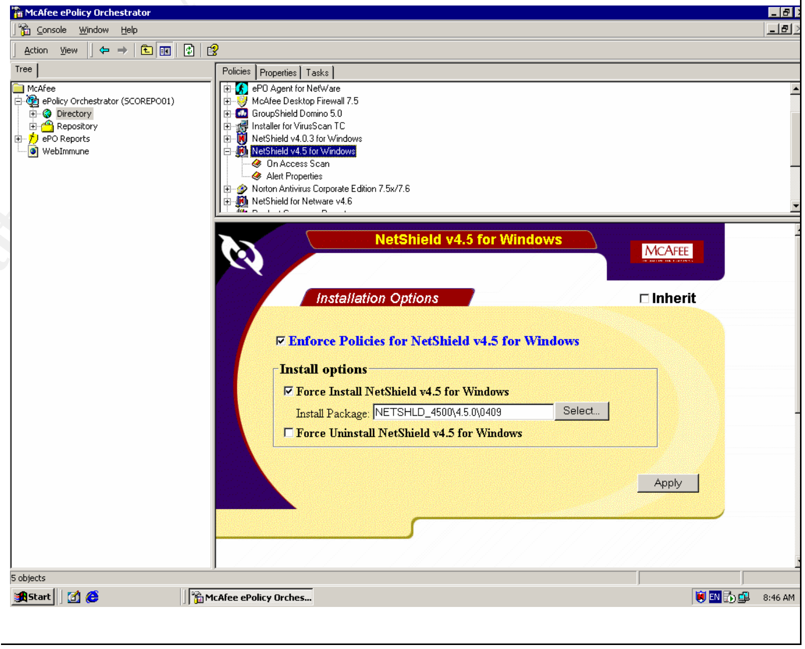
YES	NO	RL total
	X RL = 3	3

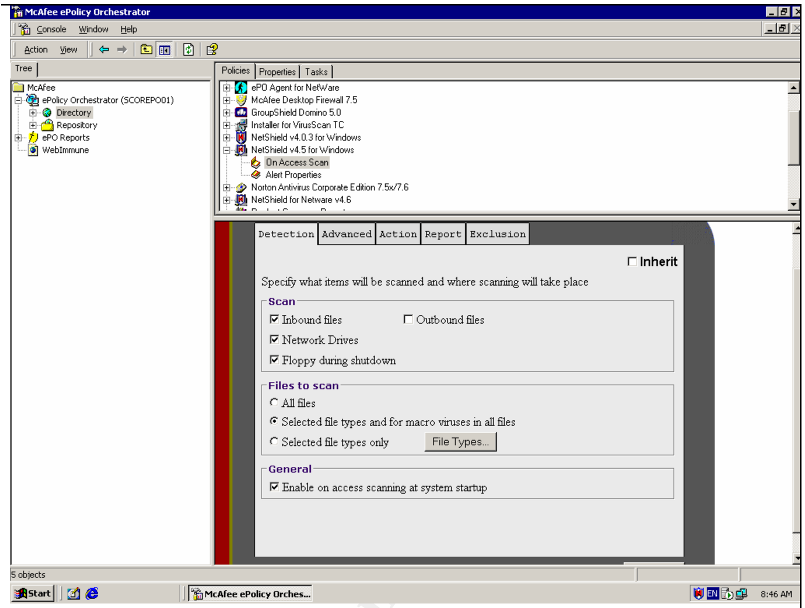
Is the structure on the audited FTP server faithful or close to the FTP server of NAI ?

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.
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: 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** ».
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 :	File content « 11-NetShield.rtf » :  McAfee ePolicy Orchestrator Console Window Help Action View Tree McAfee ePolicy Orchestrator (SCOREPO01) Directory Repository ePO Reports WebImmune Policies Properties Tasks ePO Agent for NetWare McAfee Desktop Firewall 7.5 GroupShield Domino 5.0 Installer for VirusScan TC NetShield v4.0.3 for Windows NetShield v4.5 for Windows On Access Scan Alert Properties Norton Antivirus Corporate Edition 7.5x/7.6 NetShield for Netware v4.6 MCAFEE Select... Apply 5 objects Start McAfee ePolicy Orches... EN 8:46 AM NetShield v4.5 for Windows Installation Options □ Inherit ☑ Enforce Policies for NetShield v4.5 for Windows Install options ☑ Force Install NetShield v4.5 for Windows Install Package: NETSHLD_4500\4.5.0\0409 □ Force Uninstall NetShield v4.5 for Windows


McAfee ePolicy Orchestrator
Console Window Help
Action View
Tree
McAfee
ePolicy Orchestrator (SCOREPO01)
Directory
Repository
ePO Reports
WebImmune
Policies Properties Tasks
ePO Agent for NetWare
McAfee Desktop Firewall 7.5
GroupShield Domino 5.0
Installer for VirusScan TC
NetShield v4.0.3 for Windows
NetShield v4.5 for Windows
On Access Scan
Alert Properties
Norton Antivirus Corporate Edition 7.5x/7.6
NetShield for Netware v4.6
Detection Advanced Action Report Exclusion
5 objects
Start
McAfee ePolicy Orches...
EN
8:46 AM

☐ Inherit

Specify what items will be scanned and where scanning will take place

Scan

☑ Inbound files ☐ Outbound files

☑ Network Drives

☑ Floppy during shutdown

Files to scan

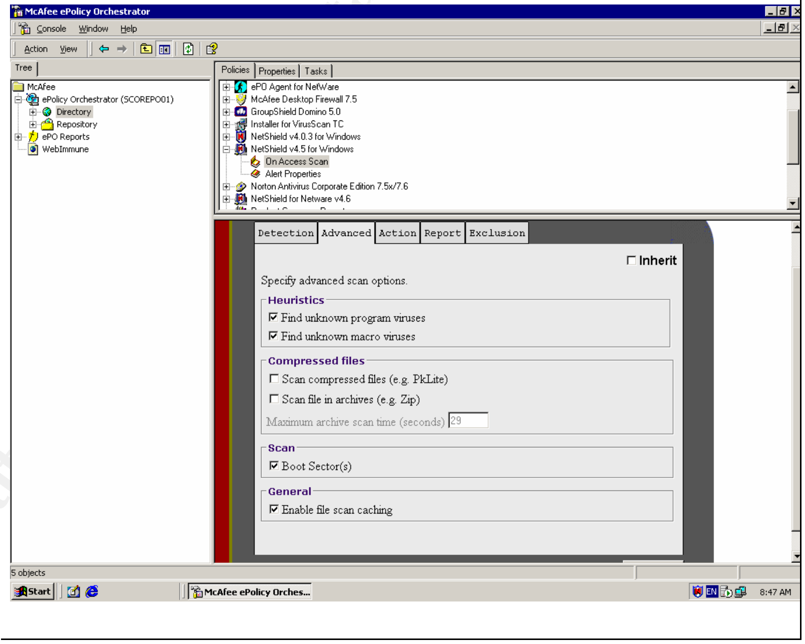
○ All files

● Selected file types and for macro viruses in all files

○ Selected file types only [File Types...]

General

☑ Enable on access scanning at system startup


McAfee ePolicy Orchestrator
Console Window Help
Action View
Tree
McAfee
ePolicy Orchestrator (SCOREPO01)
Directory
Repository
ePO Reports
WebImmune
Policies Properties Tasks
ePO Agent for NetWare
McAfee Desktop Firewall 7.5
GroupShield Domino 5.0
Installer for VirusScan TC
NetShield v4.0.3 for Windows
NetShield v4.5 for Windows
On Access Scan
Alert Properties
Norton Antivirus Corporate Edition 7.5x/7.6
NetShield for Netware v4.6
Detection Advanced Action Report Exclusion
5 objects
Start
McAfee ePolicy Orches...
EN
8:47 AM

☐ Inherit

Specify advanced scan options.

Heuristics

☑ Find unknown program viruses

☑ Find unknown macro viruses

Compressed files

☐ Scan compressed files (e.g. PkLite)

☐ Scan file in archives (e.g. Zip)

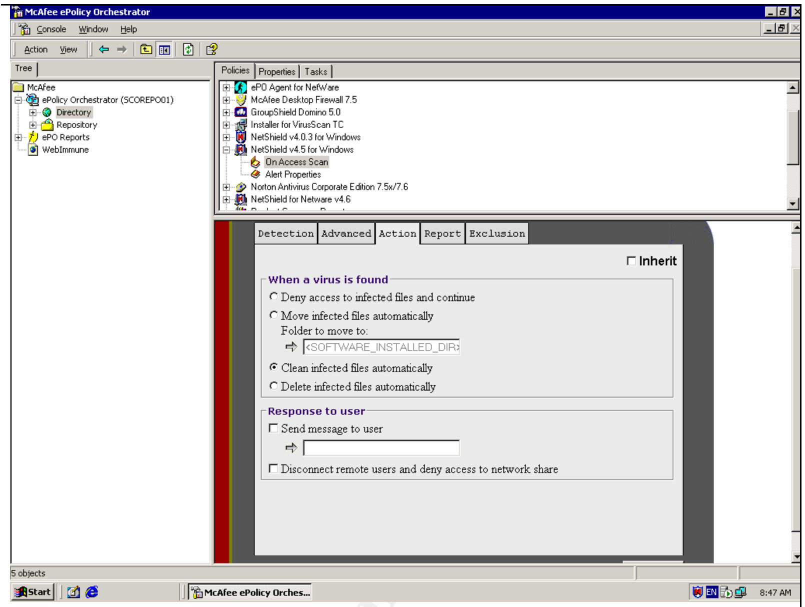
Maximum archive scan time (seconds) 29

Scan

☑ Boot Sector(s)

General

☑ Enable file scan caching


McAfee ePolicy Orchestrator
Console Window Help
Action View
Tree
McAfee
ePolicy Orchestrator (SCOREPO01)
Directory
Repository
ePO Reports
WebImmune
Policies Properties Tasks
ePO Agent for NetWare
McAfee Desktop Firewall 7.5
GroupShield Domino 5.0
Installer for VirusScan TC
NetShield v4.0.3 for Windows
NetShield v4.5 for Windows
On Access Scan
Alert Properties
Norton Antivirus Corporate Edition 7.5x/7.6
NetShield for Netware v4.6
Detection Advanced Action Report Exclusion
5 objects
Start
McAfee ePolicy Orches...
8:47 AM

☐ Inherit

When a virus is found

○ Deny access to infected files and continue

○ Move infected files automatically

Folder to move to:

<SOFTWARE_INSTALLED_DIR>

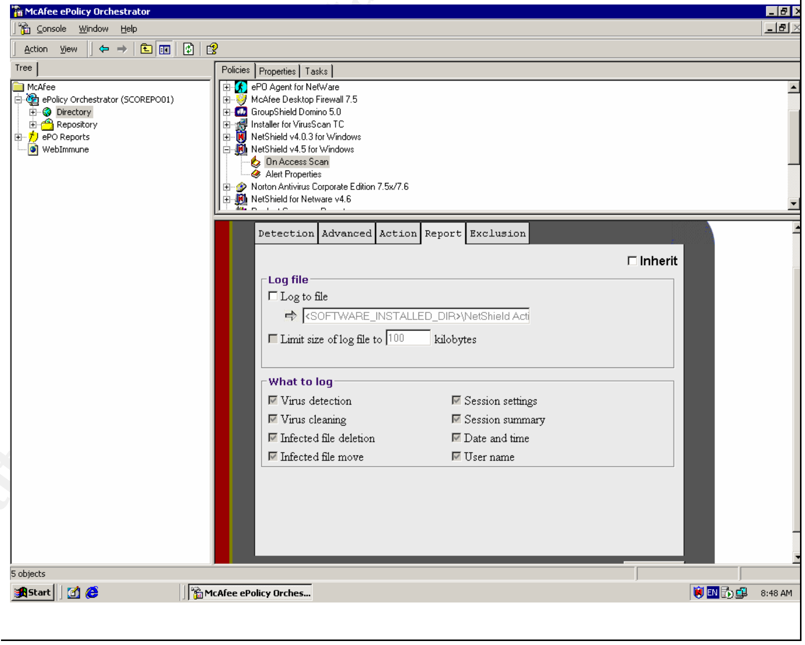
● Clean infected files automatically

○ Delete infected files automatically

Response to user

☐ Send message to user

☐ Disconnect remote users and deny access to network share


McAfee ePolicy Orchestrator
Console Window Help
Action View
Tree
McAfee
ePolicy Orchestrator (SCOREPO01)
Directory
Repository
ePO Reports
WebImmune
Policies Properties Tasks
ePO Agent for NetWare
McAfee Desktop Firewall 7.5
GroupShield Domino 5.0
Installer for VirusScan TC
NetShield v4.0.3 for Windows
NetShield v4.5 for Windows
On Access Scan
Alert Properties
Norton Antivirus Corporate Edition 7.5x/7.6
NetShield for Netware v4.6
Detection Advanced Action Report Exclusion
5 objects
Start
McAfee ePolicy Orches...
8:48 AM

☐ Inherit

Log file

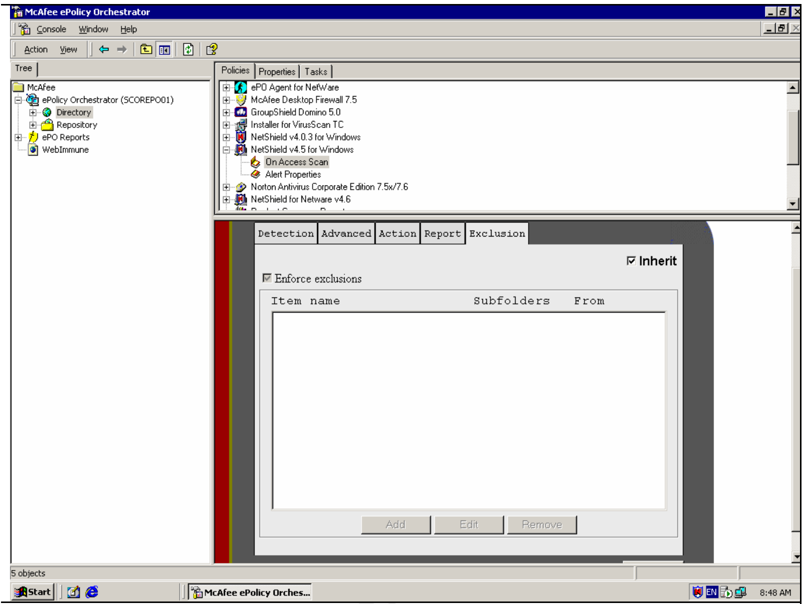
☐ Log to file

<SOFTWARE_INSTALLED_DIR>\NetShield Acti

☐ Limit size of log file to 100 kilobytes

What to log

☑ Virus detection	☑ Session settings
☑ Virus cleaning	☑ Session summary
☑ Infected file deletion	☑ Date and time
☑ Infected file move	☑ User name

<table>
<tr><td></td><td>
McAfee ePolicy Orchestrator
Console Window Help
Action View
Tree
McAfee
ePolicy Orchestrator (SCOREPO01)
Directory
Repository
ePO Reports
WebImmune
Policies Properties Tasks
ePO Agent for NetWare
McAfee Desktop Firewall 7.5
GroupShield Domino 5.0
Installer for VirusScan TC
NetShield v4.0.3 for Windows
NetShield v4.5 for Windows
On Access Scan
Alert Properties
Norton Antivirus Corporate Edition 7.5x/7.6
NetShield for Netware v4.6
Detection Advanced Action Report Exclusion
Item name Subfolders From
Add Edit Remove
5 objects
Start
McAfee ePolicy Orches...
EN
8:48 AM
☑ Inherit
☑ Enforce exclusions</td></tr>
<tr><td>Summary Brief explanation of risk :</td><td>A configuration mistake in the settings deployed by the management console increases the infection probabilities on the total system of the servers in the information system.</td></tr>
<tr><td>Risk evaluation :</td><td>Is the option « Enforce Policies for NetShield v4.5 » selected ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td>X</td><td>RL = 4</td><td>0</td></tr>
</table>
Is the option « Force Install NetShield v4.5 » selected and is an installation package selected ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td>X</td><td>RL = 4</td><td>0</td></tr>
</table></td></tr>
</table>

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	RL = 3	0

If not, which are missing ? :

____

____

____

____

Is at least « **Clean infected file automatically** » selected in the tab « Action » ?

YES	NO	RL total
X	RL = 3	0

If not, what is the default action ? :

____

____

<table>
<tr><td></td><td>Have exclusions been defined in the tab « Exclusion » ?.
<table><tr><th>YES</th><th>NO</th><th>RL total</th></tr><tr><td>RL = 2</td><td>X</td><td>0</td></tr></table>
If so, explain the exclusions :
____
____
____
____
<b>TOTAL RISK LEVEL: [0] / 20</b></td></tr>
</table>

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: 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 : 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

Administrator
   Grorps          Administrators (Local, Administrators have compthande and
uRThetricted access to the computer/domain)
   AccountType       User
   HomeDrive
   HomeDir
   Profile
   LogonScript
   Workstations
   PswdCanBeChanged  Yes
   PswdLastSandTime   2002-04-02 14:13
   PswdPre-required      Yes
   PswdExpires       No
   PswdExpiresTime   Never
   AcctDisabthed       No
   AcctLockedOrt      No
   AcctExpiresTime   Never
   LastLogonTime     2003-01-15 09:50
   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          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
   HomeDrive
   HomeDir
   Profile
   LogonScript
   Workstations
   PswdCanBeChanged  Yes
   PswdLastSandTime   2002-08-26 16:38
   PswdPre-required      Yes
   PswdExpires       No
   PswdExpiresTime   Never
   AcctDisabthed       No
```

	AcctLockedOrt No AcctExpiresTime Never LastLogonTime 2002-09-04 08:42 LastLogonServer 172.25.1.134 LogonHorrs All Sid S-1-5-21-1715567821-682003330-725345543-1005 RasDialin No RasCallback Noe RasCallbackNumber FullName Backupexec_svr 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 PswdExpiresTime Never AcctDisabthed No AcctLockedOrt No AcctExpiresTime Never 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 PswdExpiresTime Never AcctDisabthed No AcctLockedOrt No AcctExpiresTime Never LastLogonTime Never LastLogonServer 172.25.1.134 LogonHorrs All Sid S-1-5-21-1715567821-682003330-725345543-1004 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 RasDialin No RasCallback Noe RasCallbackNumber FullName TsInternetUser Comment This user account is used by Terminal Services.
Summary Brief explanation of risk :	The less accounts exist with administrative rights and 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). 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	RL = 4	0

Is the account « **Guest** » renamed for something less explicit ?

YES	NO	RL total
X	RL = 2	0

Is the account « **administrator** » renamed for something less explicit ?

YES	NO	RL total
	X RL = 2	2

Does the default account « **IUSR_computername** » as been renamed for something less explicit ?

YES	NO	RL total
	X RL = 2	4

Is a service account for the ePO software present ?

YES	NO	RL total
	X RL = 3	7

Is a service account for the saving software (ex : BackupExec) present ?

YES	NO	RL total
	X RL = 2	9

	Is a service account for the remote access (ex : Terminal Service) present ?

YES	NO	RL total
X	RL = 2	9

TOTAL RISK LEVEL: [9] / 17

[**13**]. Control objective :	Verification of the user groups 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 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** ». - 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

<table>
<tr><td>Results :</td><td>File content « 13-groups.txt » :

2003-01-15 16:04 - Somarsoft DumpSec (formerly DumpAcl) - \\172.25.1.134
Grorp   Comment
Type

<b>Administrators</b>   Administrators have compthande and uRThetricted access to the computer/domain
Local
  <b>SCOREPO01\administrator</b>
User
  <b>SCOREPO01\Backupexec_svr</b>
User
<b>Backup Operators</b>   Backup Operators can override security restrictions for the sothe purpose of backing up or restoring file
Local
  <b>SCOREPO01\Backupexec_svr</b>
User
<b>Guests</b>   Guests have the same access as members of the Users grorp by default, except for the Guest account which is further restricted
Local
  <b>SCOREPO01\Guest</b>
User
  <b>SCOREPO01\IUSR_SCOREPO01</b>
User
  <b>SCOREPO01\TsInternetUser</b>
User
<b>Power Users</b>   Power Users possess most administrative powers with some restrictions. Thus, Power Users can run thegacy applications in addition to certified applications Local
<b>Replicator</b>   Supports file replication in a domain
Local
<b>Users</b>   Users are prevented from making accidental or intentional system-wide changes. Thus, Users can run certified applications, but not most thegacy applications Local
  <b>SCOREPO01\SQLAgentCmdExec</b>
User</td></tr>
<tr><td>Summary Brief explanation of risk :</td><td>Well managed groups permit only the appropriate 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.</td></tr>
<tr><td>Risk evaluation :</td><td>Is the account « <b>administrator</b> » (If not renamed) found in the group « <b>administrators</b> » ?

<table><tr><th>YES</th><th>NO</th><th>RL total</th></tr><tr><td>X</td><td rowspan="2"></td><td rowspan="2">3</td></tr><tr><td>RL = 3</td></tr></table>
Is the service account for the saving software found only in the group « <b>Backup_Operators</b> » ?
<table><tr><th>YES</th><th>NO</th><th>RL total</th></tr><tr><td rowspan="2"></td><td>X</td><td rowspan="2">5</td></tr><tr><td>RL = 2</td></tr></table></td></tr>
</table>

If not, where is it located ? :
__In the group « administrators »_______________
____

Is the account « **Guest** » found in the group « **Guest** » ?

YES	NO	RL total
X		7
RL = 2		

Is only the service account required by IIS found in the group « **Guest** » ?

YES	NO	RL total
	X	9
	RL = 2	

Are accounts found in one of the following groups : « **Power Users** », « **Replicator** » and « **Users** » ?

YES	NO	RL total
X		11
RL = 2		

If so, explain :
____
____
____

TOTAL RISK LEVEL: [11] / 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 ☒ 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).

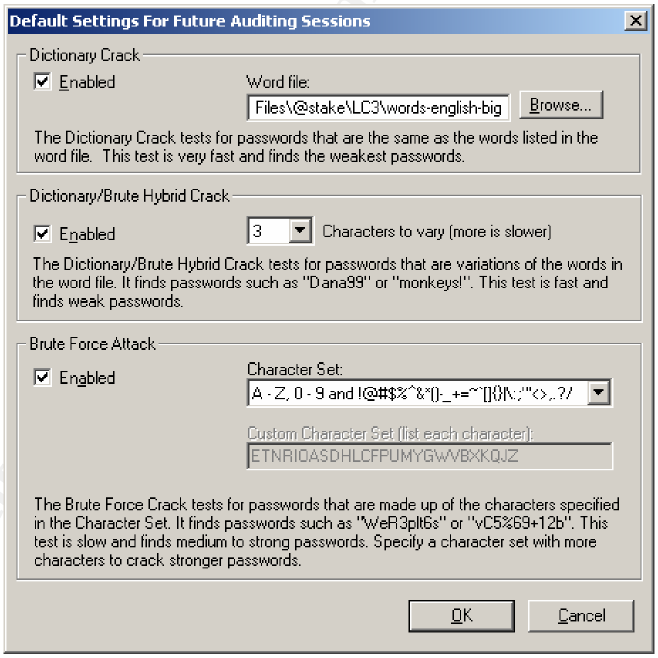
Note : Also, you must know the password of an account with « administrator » rights.

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

Dictionary Crack

☑ Enabled

Word file: Files\@stake\LC3\words-english-big

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

☑ Enabled

Character Set: A - Z, 0 - 9 and !@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/

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 "WeR3pl6s" 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:

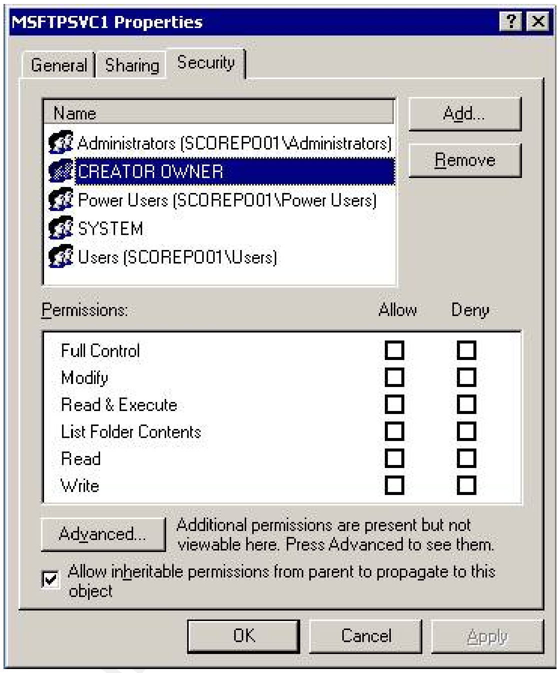
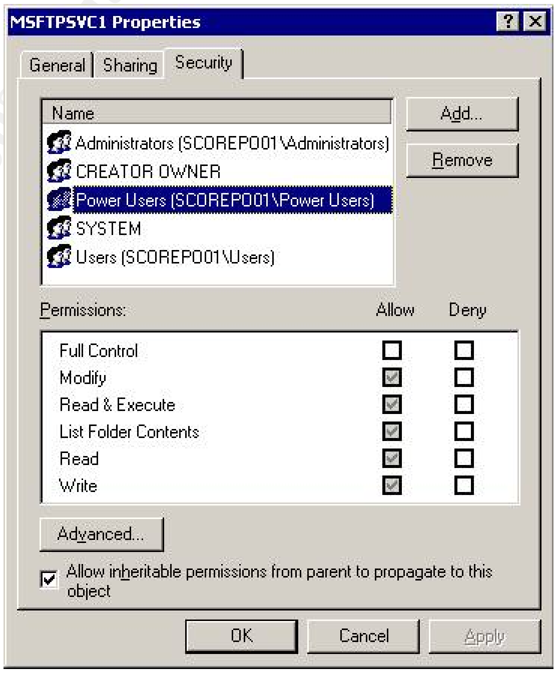
1. Recover the file « **14-pwdump.txt** » from the audited server by the way of your choice.
2. Open the application« **LC3** » (or more recent)
3. Choose « **File - New Session…** »
4. Choose « **Import** »
5. Choose « **Import from a PWDUMP File…** »
6. Choose the file « **14-pwdump.txt** »
7. Press on« **F4** » (or choose the icon « Begin Audit »).

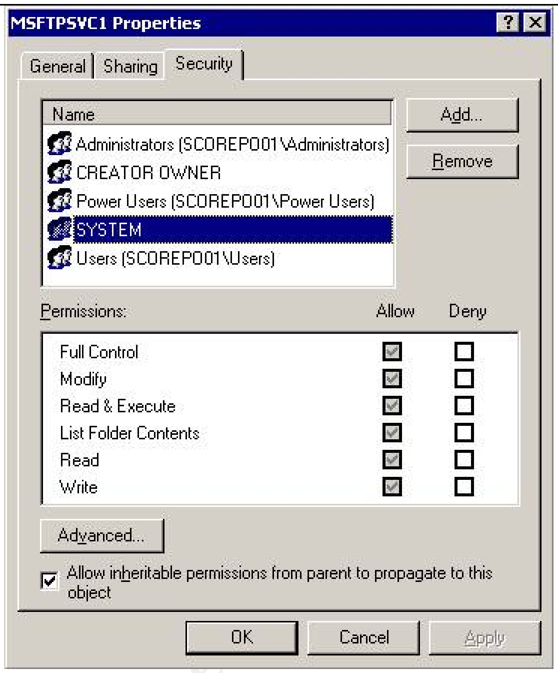
	8. Press on the icon « **Minimize LC3 to the system tray** » and let it run until you obtain the passwords or upto a maximum of 12 hours. 9. Once the passwords are obtained or after the delay has expired, export the results in the file« **14-lc3.txt** ».
Reference(s) :	The LC3 tool is available as an 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 :	File content « 14-pwdump.txt » : **Administrator**:500:CE7A23ED46C4F0FC9D8BBC3E3B48E321:CDADF01D2336AB04D1EF488429E553FA::: **Backupexec_svr**:1005:B7BF3C926A6A34FF7584248B8D2C9F9E:D48FDAE7B9496CD575E16D305D1DF194::: **Guest**:501:NO PASSWORD*********************:NO PASSWORD*********************::: **IUSR_SCOREPO01**:1001:4AC018FBC87DE18C6647BD48BAB3C431:305349374C9BB8D73D4C8DCD9B1667FA::: **SQLAgentCmdExec**:1004:14AC06232C3171941486235A2333E4D2:E29526B19D19B6EAE96A24D0B39E85DA::: **TsInternetUser**:1000:165F364381FE397ED10C5288A0723450:EBB9A3BBAA10E33A974EE84FBABEFFAC::: Contenu de « 14-lc3.txt » : **USERNAME** **LANMAN PASSWORD** **NTLM PASSWORD** Administrator ???????N99 * uncracked * Backupexec_svr ePOBackup EPOBACKUP Guest * missing * * missing * IUSR_SCOREPO01 CGR2QDV??????? * uncracked * SQLAgentCmdExec ZEUMVKCM ZEUMVKCM TsInternetUser ???????THE94EIJ * uncracked *

<table>
<tr><td>Summary Brief explanation of risk :</td><td>Without a robust authentification (including a small letter, a capital letter a number and a special character) the probabilities for an attacker to take control of the server is higher.</td></tr>
<tr><td>Risk evaluation :</td><td>Have passwords been found after a maximum of 12 hours of « brute force » ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td>X</td><td></td><td>4</td></tr>
<tr><td>RL = 4</td><td></td><td></td></tr>
</table>
Are passwords for accounts with administrative rights robust and conform ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td></td><td>X</td><td>8</td></tr>
<tr><td></td><td>RL = 4</td><td></td></tr>
</table>
Are passwords for service accounts composed of 14 characters ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td></td><td>X</td><td>11</td></tr>
<tr><td></td><td>RL = 3</td><td></td></tr>
</table>
<b>TOTAL RISK LEVEL: [11] / 11</b></td></tr>
</table>

[**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 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 :	File content « 15-msftpsvc1.rtf » :  MSFTPSVC1 Properties General | Sharing | Security Name Administrators (SCOREP001\Administrators) CREATOR OWNER Power Users (SCOREP001\Power Users) SYSTEM Users (SCOREP001\Users) Permissions: Allow Deny Full Control ☐ ☐ Modify ☐ ☐ Read & Execute ☐ ☐ List Folder Contents ☐ ☐ Read ☐ ☐ Write ☐ ☐ Additional permissions are present but not viewable here. Press Advanced to see them. ☑ Allow inheritable permissions from parent to propagate to this object  MSFTPSVC1 Properties General | Sharing | Security Name Administrators (SCOREP001\Administrators) CREATOR OWNER Power Users (SCOREP001\Power Users) SYSTEM Users (SCOREP001\Users) Permissions: Allow Deny Full Control ☐ ☐ Modify ☑ ☐ Read & Execute ☑ ☐ List Folder Contents ☑ ☐ Read ☑ ☐ Write ☑ ☐ ☑ Allow inheritable permissions from parent to propagate to this object



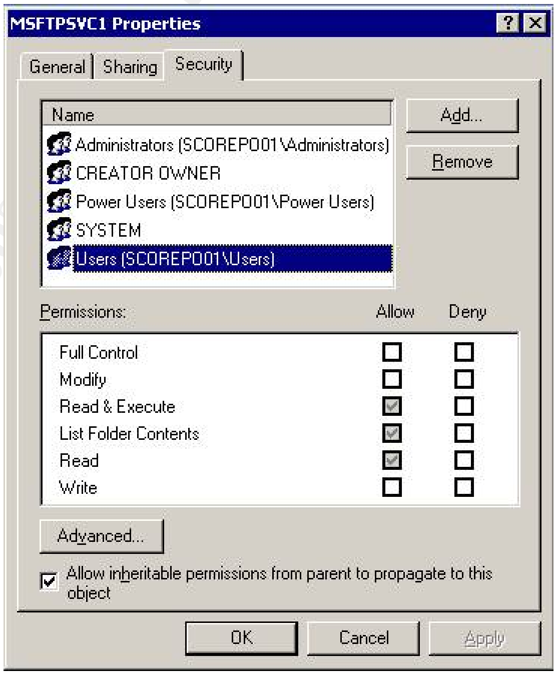
MSFTPSVC1 Properties

Name

- Administrators (SCOREP001\Administrators)
- CREATOR OWNER
- Power Users (SCOREP001\Power Users)
- SYSTEM
- Users (SCOREP001\Users)

Permissions:	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□

☑ Allow inheritable permissions from parent to propagate to this object



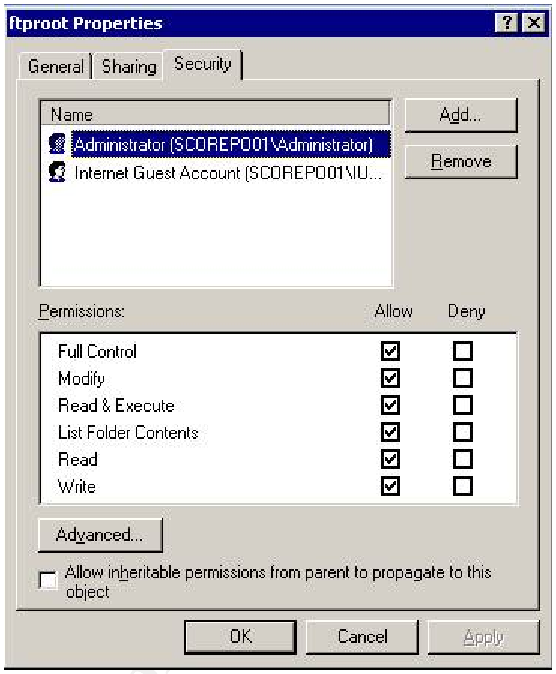
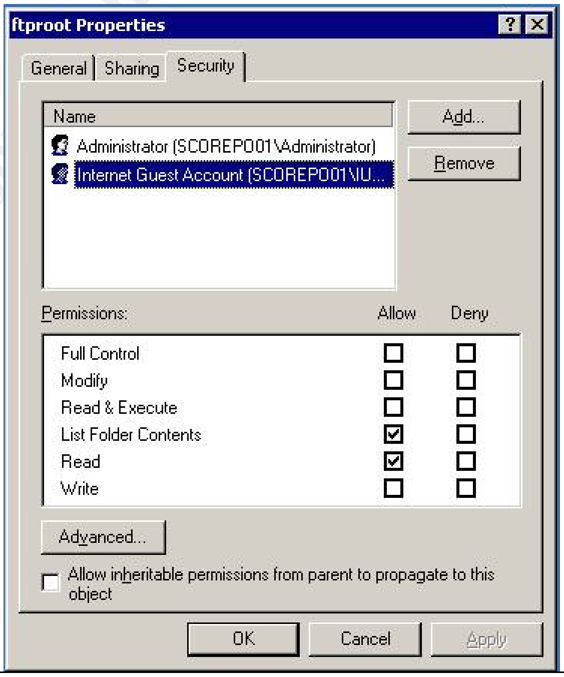
MSFTPSVC1 Properties

Name

- Administrators (SCOREP001\Administrators)
- CREATOR OWNER
- Power Users (SCOREP001\Power Users)
- SYSTEM
- Users (SCOREP001\Users)

Permissions:	Allow	Deny
Full Control	□	□
Modify	□	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	□	□

☑ Allow inheritable permissions from parent to propagate to this object

	File content « 15-ftproot.rft » :  ftproot Properties General Sharing Security Add... Remove Advanced... OK Cancel Apply Name Administrator (SCOREP001\Administrator) Internet Guest Account (SCOREP001\IU... Permissions: Allow Deny Full Control ☑ □ Modify ☑ □ Read & Execute ☑ □ List Folder Contents ☑ □ Read ☑ □ Write ☑ □ □ Allow inheritable permissions from parent to propagate to this object  ftproot Properties General Sharing Security Add... Remove Advanced... OK Cancel Apply Name Administrator (SCOREP001\Administrator) Internet Guest Account (SCOREP001\IU... Permissions: Allow Deny Full Control □ □ Modify □ □ Read & Execute □ □ List Folder Contents ☑ □ Read ☑ □ Write □ □ □ Allow inheritable permissions from parent to propagate to this object
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		0
	RL = 3	

If not, which ? :

____

____

____

Do the rest of the groups (if existing) have only an authorization « Read » on the directory « **MSFTPSVC1 »** ?

YES	NO	RL total
	X	3
	RL = 3	

If not, which ? :

____

____

____

Does the group « Everyone » have rights on the directory « **MSFTPSVC1 »** ?

YES	NO	RL total
	X	3
RL = 3		

Does only the group « Administrators » have an authorization « Full Control » on the directory « **Ftproot** » ?

YES	NO	RL total
X		3
	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
X	RL = 3	3

If not, which ? :

____

____

____

Does the group « Everyone » have rights on the directory « **Ftproot »** ?

YES	NO	RL total
RL = 3	X	3

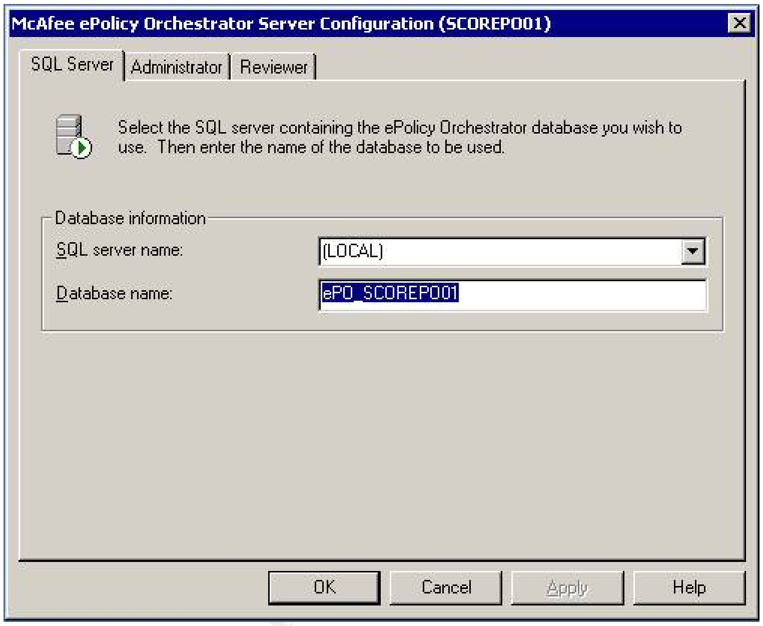
TOTAL RISK LEVEL: [3] / 18

[**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) 5. 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 :** 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 : - 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 :

File content « 16-sapw.rft » :

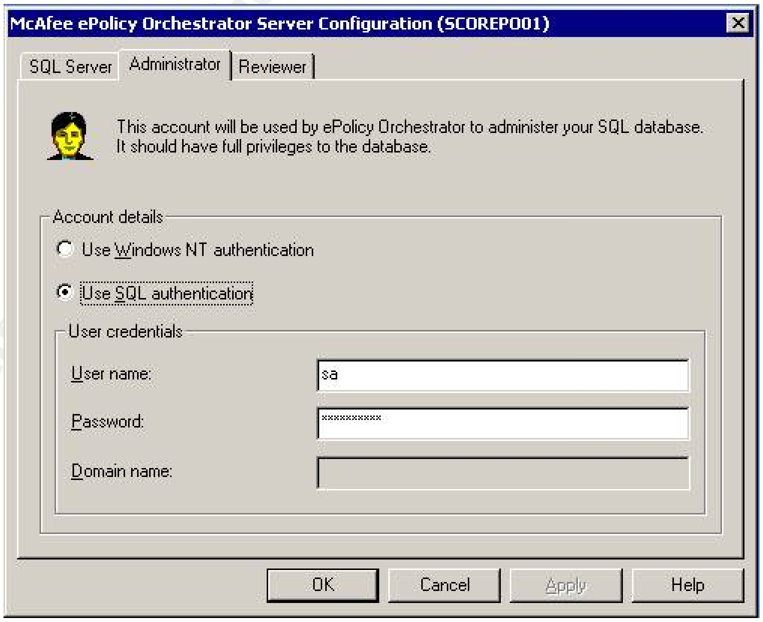

McAfee ePolicy Orchestrator Server Configuration (SCOREPO01)
SQL Server
Administrator
Reviewer
OK
Cancel
Apply
Help

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: (LOCAL)

Database name: ePO_SCOREPO01


McAfee ePolicy Orchestrator Server Configuration (SCOREPO01)
SQL Server
Administrator
Reviewer
OK
Cancel
Apply
Help

This account will be used by ePolicy Orchestrator to administer your SQL database. It should have full privileges to the database.

Account details

○ Use Windows NT authentication

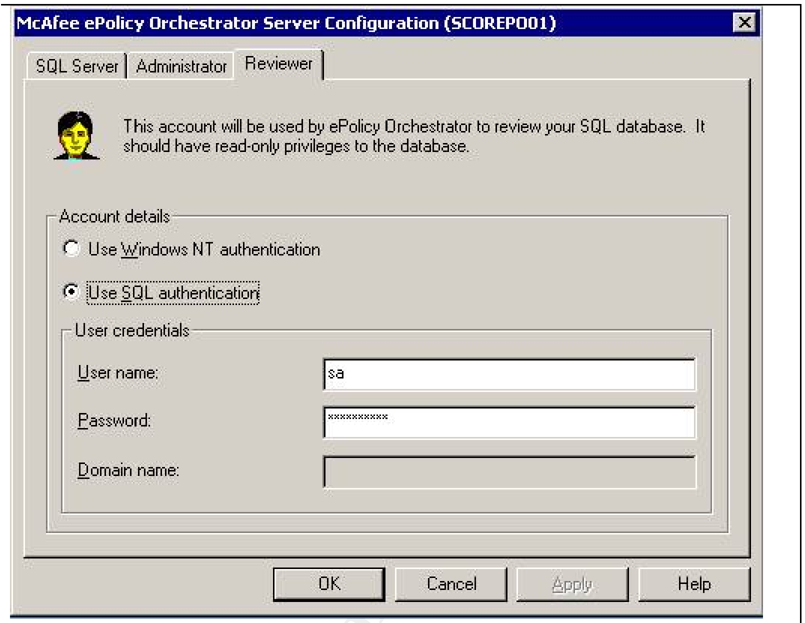
● Use SQL authentication

User credentials

User name: sa

Password: **********

Domain name:



McAfee ePolicy Orchestrator Server Configuration (SCOREPO01)
SQL Server
Administrator
Reviewer
OK
Cancel
Apply
Help

This account will be used by ePolicy Orchestrator to review your SQL database. It should have read-only privileges to the database.

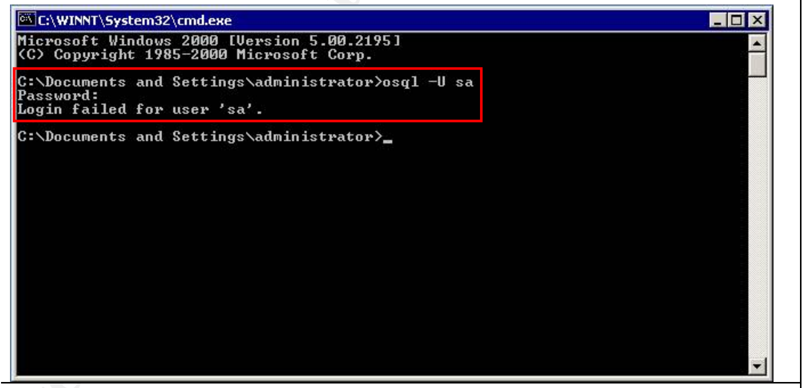
Account details

○ Use Windows NT authentication

● Use SQL authentication

User credentials

User name:	sa
Password:	**********
Domain name:	



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\Documents and Settings\administrator>osql -U sa
Password:
Login failed for user 'sa'.

C:\Documents and Settings\administrator>_
```

Summary Brief explanation of risk :

Without a robust authentification (including small letter, 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
X	RL = 4	0

Is the password for the account « SA » composed of 14 characters ?

YES	NO	RL total
	X	2
	RL = 2	

Is the password different from the one for authentification to the server (i.e. : Windows) ?

YES	NO	RL total
X		2
	RL = 3	

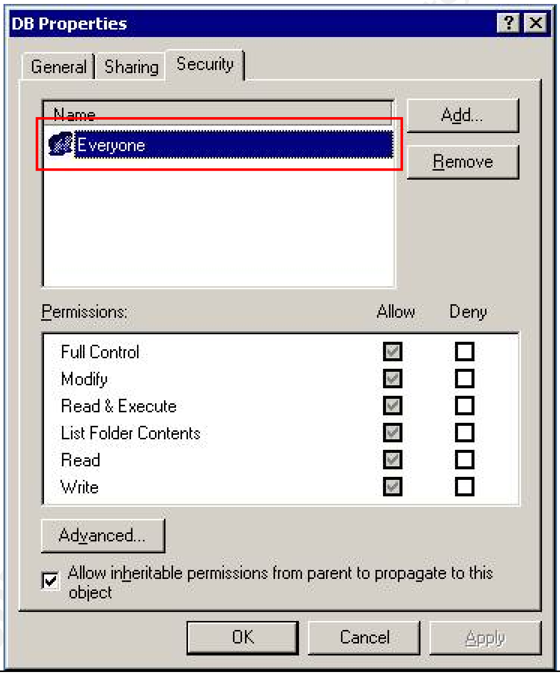
Is the password different from the one for authentification to an ePO console ?

YES	NO	RL total
	X	6
	RL = 4	

TOTAL RISK LEVEL: [6] / 12

[**17**] Control objective :	Verification of access rights on certain important files of ePolicy Orchestrator.
Test location :	□ From the auditor station ☒ From the server audited
Tests to be conducted :	Observe the following instructions: 1. Conduct a search on all the drives for « **DB** » using « Start » - « Search » – « For File and Folders » (or touch windows + f) 2. Right button on the file « **DB** » found in the directory « **\ePO\2.0** » 3. Choose « **Properties** » 4. Choose the tab « **Security** » 5. 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

<table>
<tr><td>Expected results :</td><td>Only the group « <b>administrators</b> » should have access in « <b>Full Control</b> » to the file « <b>DB</b> ».

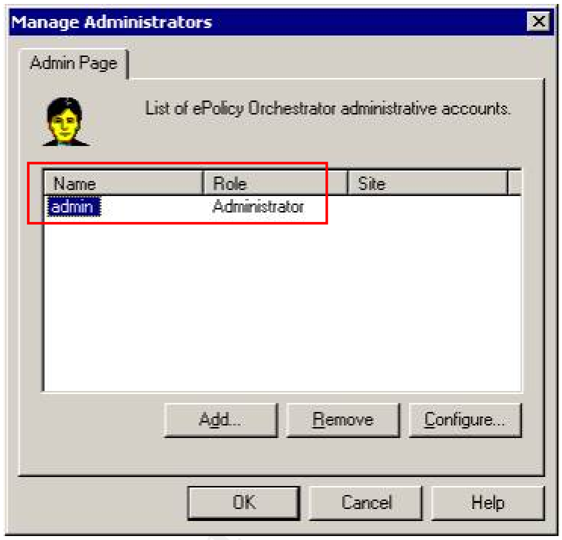
<b>Note :</b> The group « <b>Backup Operators</b> » could also be present (if required by the saving software).</td></tr>
<tr><td>Objective / Subjective :</td><td>Objective</td></tr>
<tr><td>Results :</td><td>File content « 17-dbepo.rtf » :

DB Properties
General | Sharing | Security
Name
Everyone
Permissions: Allow Deny
Full Control ☑ □
Modify ☑ □
Read &amp; Execute ☑ □
List Folder Contents ☑ □
Read ☑ □
Write ☑ □
☑ Allow inheritable permissions from parent to propagate to this object
 </td></tr>
<tr><td>Summary Brief explanation of risk :</td><td>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.</td></tr>
<tr><td>Risk evaluation :</td><td>Does only the group « administrators » have an access « Full Control » to the file « DB ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td></td><td>X</td><td>4</td></tr>
<tr><td></td><td>RL = 4</td><td></td></tr>
</table>

If not, which ? :
__Everyone______________________________________
____
____

<b>TOTAL RISK LEVEL: [4] / 4</b></td></tr>
</table>

[**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: 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 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.

<table>
<tr><td>Results :</td><td>File content « 18-epopw.rtf » :



List of ePolicy Orchestrator administrative accounts.

Name	Role	Site
admin	Administrator	
</td></tr>
<tr><td>Summary Brief explanation of risk :</td><td>Without a robust authentification (including small letter, capital letter, number and special character) the probabilities for an attacker to take control of the ePO management console is higher.</td></tr>
<tr><td>Risk evaluation :</td><td>Have access codes been created according to the number of administrators needing to access the ePO management console ?

<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td></td><td>X
RL = 3</td><td>3</td></tr>
</table>

Is the default account « <b>ADMIN</b> » deleted or renamed ?

<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td></td><td>X
RL = 4</td><td>7</td></tr>
</table>

Are all the passwords composed of at least 8 characters and robust ?

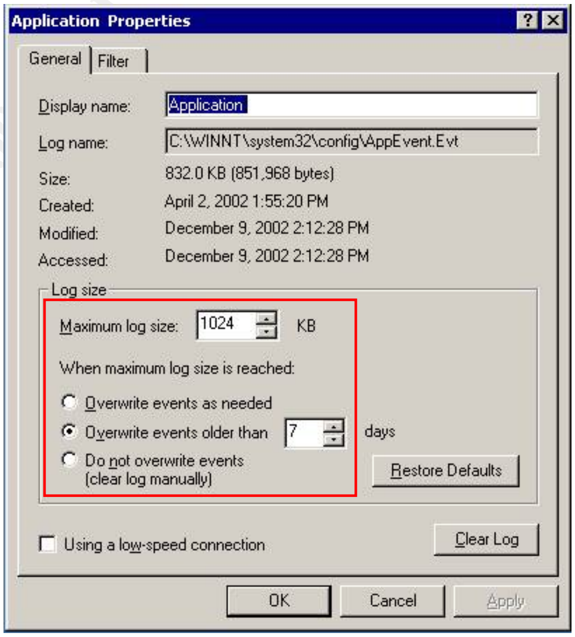
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td>X</td><td>RL = 4</td><td>7</td></tr>
</table>
</td></tr>
</table>

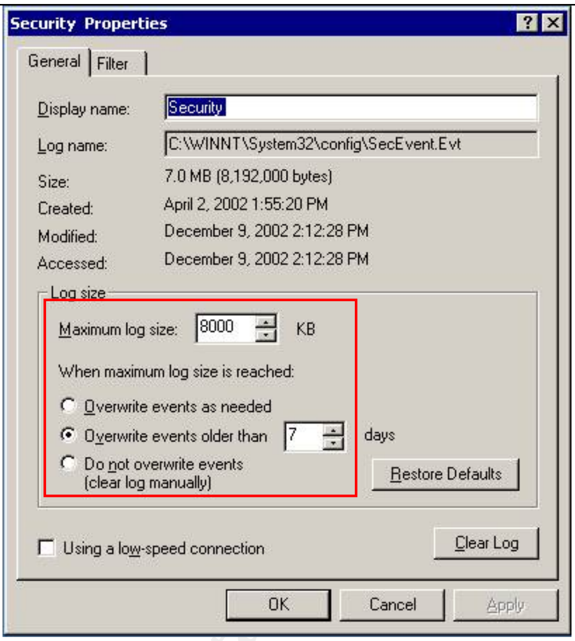
<table>
<tr>
<td></td>
<td>
Are the passwords differents from the one for authentification to the server (i.e. : Windows) ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td>X</td><td>RL = 4</td><td>7</td></tr>
</table>
Are the passwords different from the one for the account « SA » ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td>X</td><td>RL = 4</td><td>7</td></tr>
</table>
<b>TOTAL RISK LEVEL: [7] / 19</b>
</td>
</tr>
</table>

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** » 3. Double click « **Event Viewer** » 4. Right button on the icon « **Application** » and choose « **Properties** » 5. Take a screen capture and save in a Wordpad 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** » : 1. 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
Results :	File content « 19-events.rtf » :  Application Properties General | Filter Display name: Application Log 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 Maximum log size: 1024 KB When maximum log size is reached: ○ Overwrite events as needed ● Overwrite events older than 7 days ○ Do not overwrite events (clear log manually) Restore Defaults □ Using a low-speed connection Clear Log OK Cancel Apply



Display name: Security

Log name: C:\WINNT\System32\config\SecEvent.Evt

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

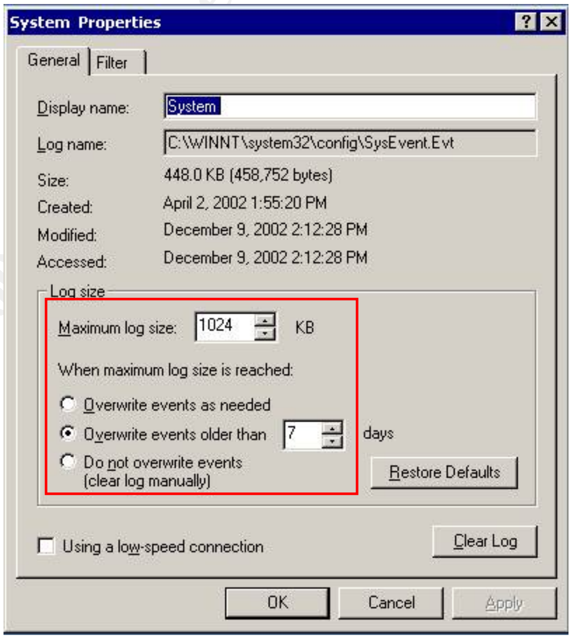
When maximum log size is reached:

○ Overwrite events as needed

● Overwrite events older than 7 days

○ Do not overwrite events (clear log manually)

□ Using a low-speed connection



Display name: System

Log name: C:\WINNT\system32\config\SysEvent.Evt

Size: 448.0 KB (458,752 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

Log size

Maximum log size: 1024 KB

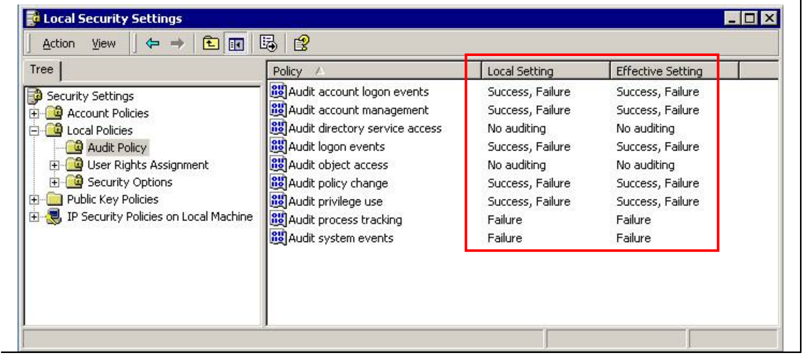
When maximum log size is reached:

○ Overwrite events as needed

● Overwrite events older than 7 days

○ Do not overwrite events (clear log manually)

□ Using a low-speed connection



Policy	Local Setting	Effective Setting
Audit account logon events	Success, Failure	Success, Failure
Audit account management	Success, Failure	Success, Failure
Audit directory service access	No auditing	No auditing
Audit logon events	Success, Failure	Success, Failure
Audit object access	No auditing	No auditing
Audit policy change	Success, Failure	Success, Failure
Audit privilege use	Success, Failure	Success, Failure
Audit process tracking	Failure	Failure
Audit system events	Failure	Failure

<table>
<tr><td>Summary Brief explanation of risk :</td><td>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.</td></tr>
<tr><td>Risk evaluation :</td><td>In the settings for « Application » :

Is the option « Do not overwrite events (clear log manually) » selected ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td rowspan="2"></td><td>X</td><td rowspan="2">2</td></tr>
<tr><td>RL = 2</td></tr>
</table>

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 ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td rowspan="2"></td><td>X</td><td rowspan="2">6</td></tr>
<tr><td>RL = 4</td></tr>
</table>
If not, what is the value ? :
__1024_______________________________________

In the settings of « Security » :

Is the option « Do not overwrite events (clear log manually) » selected ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td rowspan="2"></td><td>X</td><td rowspan="2">9</td></tr>
<tr><td>RL = 3</td></tr>
</table>

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 ?
<table>
<tr><th>YES</th><th>NO</th><th>RL total</th></tr>
<tr><td rowspan="2">X</td><td></td><td rowspan="2">9</td></tr>
<tr><td>RL = 4</td></tr>
</table>
</td></tr>
</table>

If not, what is the value ? :

____

In the settings for « System » :

Is the option « Do not overwrite events (clear log manually) » selected ?

YES	NO	RL total
	X	**11**
	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
	X	**15**
	RL = 4	

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	RL total
	X	**18**
	RL = 3	

If not, which are not ? :
__Missing: Directory Service, Object Acces, ________
__Process Access and System Events_____________
____

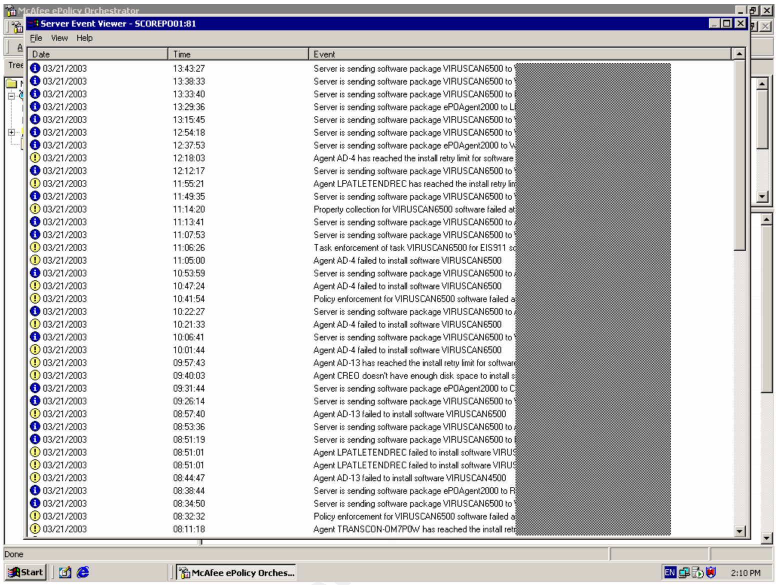
TOTAL RISK LEVEL: [18] / 22

[**20**] Control objective :	Verification of the general process for the verification of the ePO management console.
Test location :	□ From the auditor station ☒ From the server audited
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 : 1. Open the « **ePO** » management console 2. Choose « **Login** » 3. 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 Login** » 5. Double click on « **Reports** » 6. Double click on « **Anti-virus** » 7. Double click on « **Coverage** » 8. 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** »). 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. In the report « **Product Protection Summary** » : - 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 :

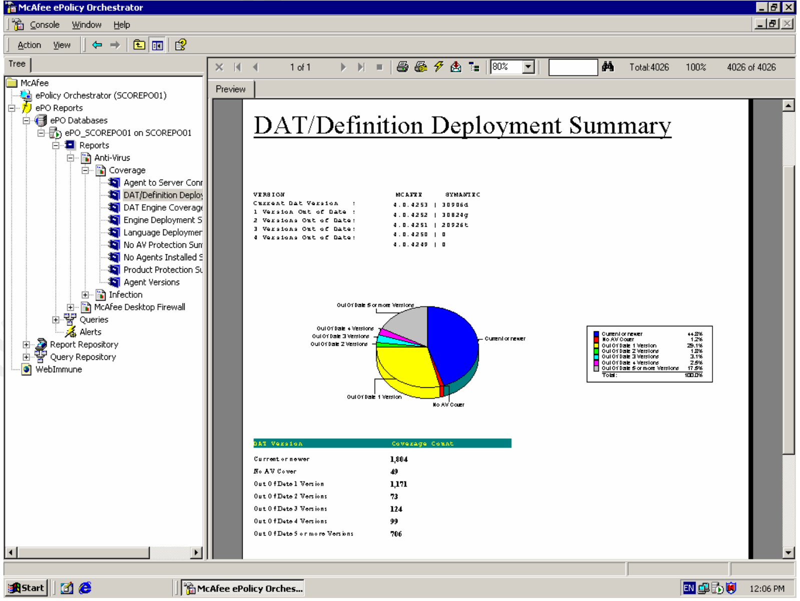
File content « 20-svrevents.rtf » :


McAfee ePolicy Orchestrator
Server Event Viewer - SCOREPO01:81
File
View
Help
Tree
Done
Start
McAfee ePolicy Orches...
EN
2:10 PM

```
Date          Time      Event
03/21/2003    13:43:27  Server is sending software package VIRUSCAN6500 to
03/21/2003    13:38:33  Server is sending software package VIRUSCAN6500 to
03/21/2003    13:33:40  Server is sending software package VIRUSCAN6500 to
03/21/2003    13:29:36  Server is sending software package ePOAgent2000 to
03/21/2003    13:15:45  Server is sending software package VIRUSCAN6500 to
03/21/2003    12:54:18  Server is sending software package VIRUSCAN6500 to
03/21/2003    12:37:53  Server is sending software package ePOAgent2000 to
03/21/2003    12:18:03  Agent AD-4 has reached the install retry limit for software
03/21/2003    12:12:17  Server is sending software package VIRUSCAN6500 to
03/21/2003    11:55:21  Agent LPATLETENDREC has reached the install retry lir
03/21/2003    11:49:35  Server is sending software package VIRUSCAN6500 to
03/21/2003    11:14:20  Property collection for VIRUSCAN6500 software failed at
03/21/2003    11:13:41  Server is sending software package VIRUSCAN6500 to
03/21/2003    11:07:53  Server is sending software package VIRUSCAN6500 to
03/21/2003    11:06:26  Task enforcement of task VIRUSCAN6500 for EIS911 sc
03/21/2003    11:05:00  Agent AD-4 failed to install software VIRUSCAN6500
03/21/2003    10:53:59  Server is sending software package VIRUSCAN6500 to
03/21/2003    10:47:24  Agent AD-4 failed to install software VIRUSCAN6500
03/21/2003    10:41:54  Policy enforcement for VIRUSCAN6500 software failed a
03/21/2003    10:22:27  Server is sending software package VIRUSCAN6500 to
03/21/2003    10:21:33  Agent AD-4 failed to install software VIRUSCAN6500
03/21/2003    10:06:41  Server is sending software package VIRUSCAN6500 to
03/21/2003    10:01:44  Agent AD-4 failed to install software VIRUSCAN6500
03/21/2003    09:57:43  Agent AD-13 has reached the install retry limit for software
03/21/2003    09:40:03  Agent CREO doesn't have enough disk space to install s
03/21/2003    09:31:44  Server is sending software package ePOAgent2000 to
03/21/2003    09:26:14  Server is sending software package VIRUSCAN6500 to
03/21/2003    08:57:40  Agent AD-13 failed to install software VIRUSCAN6500
03/21/2003    08:53:36  Server is sending software package VIRUSCAN6500 to
03/21/2003    08:51:19  Server is sending software package VIRUSCAN6500 to
03/21/2003    08:51:01  Agent LPATLETENDREC failed to install software VIRUS
03/21/2003    08:51:01  Agent LPATLETENDREC failed to install software VIRUS
03/21/2003    08:44:47  Agent AD-13 failed to install software VIRUSCAN4500
03/21/2003    08:38:44  Server is sending software package ePOAgent2000 to
03/21/2003    08:34:50  Server is sending software package VIRUSCAN6500 to
03/21/2003    08:32:32  Policy enforcement for VIRUSCAN6500 software failed a
03/21/2003    08:11:18  Agent TRANSCON-OM7P0W has reached the install retr
```

[redacted]

Example for the report « DAT/Definition Deployement Summary » :

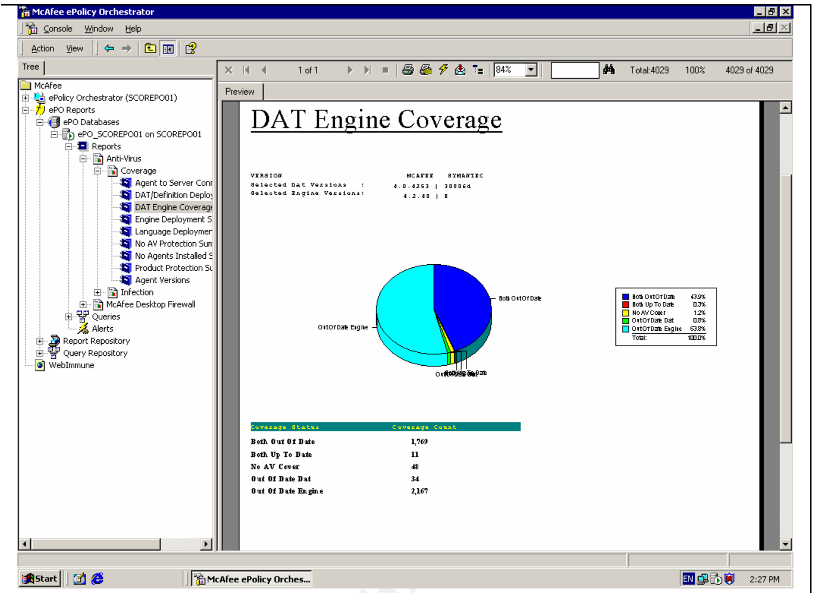


DAT/Definition Deployment Summary

```
VERSION                          MCAFEE      SYMANTEC
Current Dat Version    :         4.0.4253 | 30906d
1 Version Out of Date  :         4.0.4252 | 30824g
2 Versions Out of Date:          4.0.4251 | 20926t
3 Versions Out of Date:          4.0.4250 | 0
4 Versions Out of Date:          4.0.4249 | 0
```

DAT Version	Coverage Count
Current or newer	1,804
No AV Cover	49
Out Of Date 1 Version	1,171
Out Of Date 2 Versions	73
Out Of Date 3 Versions	124
Out Of Date 4 Versions	99
Out Of Date 5 or more Versions	706

Example for the report « DAT Engine Coverage » :

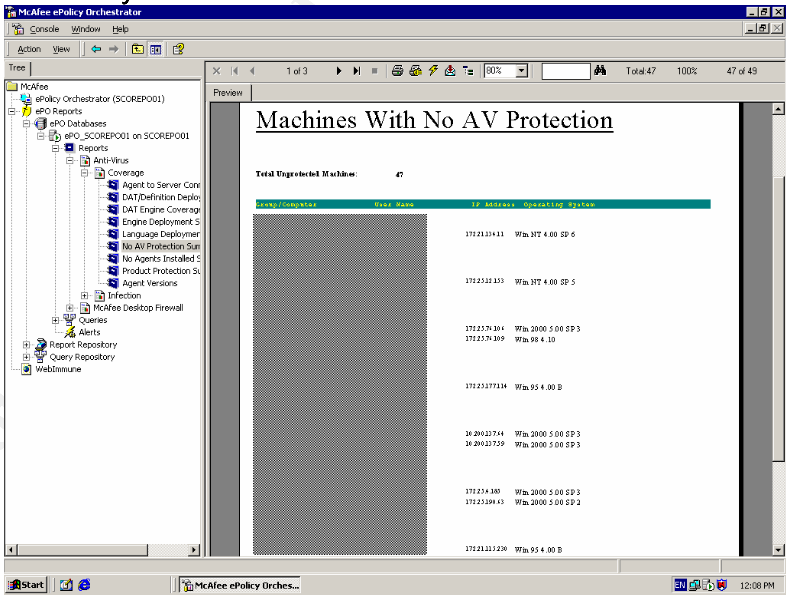


DAT Engine Coverage

```
VERSION                      MCAFEE    SYMANTEC
Selected Dat Versions   :   4.0.4253 | 30906d
Selected Engine Versions:     4.2.40 | 0
```

Coverage Status	Coverage Count
Both Out Of Date	1,769
Both Up To Date	11
No AV Cover	48
Out Of Date Dat	34
Out Of Date Engine	2,167

Example for the report « NO AV Protection Summary » :



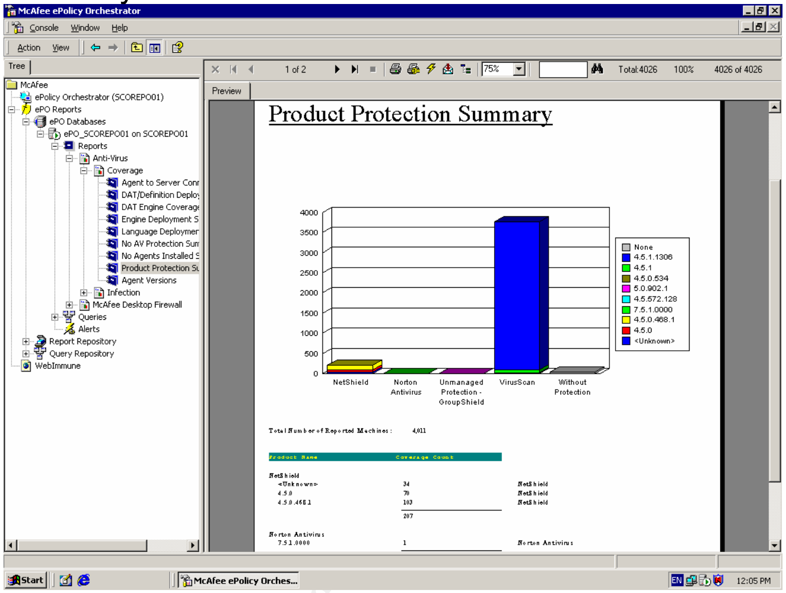
Machines With No AV Protection

Total Unprotected Machines: 47

Group/Computer	User Name	IP Address	Operating System
[redacted]		172.21.134.11	Win NT 4.00 SP 6
[redacted]		172.25.12.153	Win NT 4.00 SP 5
[redacted]		172.25.76.106	Win 2000 5.00 SP 3
[redacted]		172.25.76.109	Win 98 4.10
[redacted]		172.25.177.114	Win 95 4.00 B
[redacted]		10.200.137.64	Win 2000 5.00 SP 3
[redacted]		10.200.137.59	Win 2000 5.00 SP 3
[redacted]		172.25.4.185	Win 2000 5.00 SP 3
[redacted]		172.25.190.63	Win 2000 5.00 SP 2
[redacted]		172.21.115.230	Win 95 4.00 B

<table>
<tr>
<td></td>
<td>

Example for the report « Product Protection Summary » :

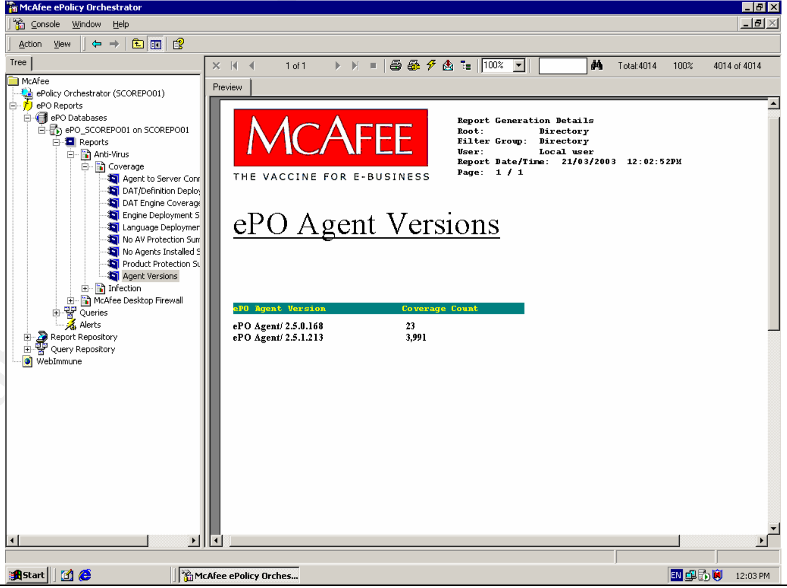


Product Protection Summary

Total Number of Reported Machines : 4,011

Product Name	Coverage Count	
NetShield		
<Unknown>	34	NetShield
4.5.0	70	NetShield
4.5.0.468.1	103	NetShield
	207	
Norton Antivirus		
7.5.1.0000	1	Norton Antivirus

Example for the report « Agent Version » :



```
Report Generation Details
Root:             Directory
Filter Group:     Directory
User:             Local user
Report Date/Time:   21/03/2003   12:02:52PM
Page:   1 / 1
```

ePO Agent Versions

ePO Agent Version	Coverage Count
ePO Agent/ 2.5.0.168	23
ePO Agent/ 2.5.1.213	3,991

</td>
</tr>
<tr>
<td>Summary Brief explanation of risk :</td>
<td>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.</td>
</tr>
</table>

Risk evaluation :

Have suspicious events or mistakes been recorded in the « Server Events » ?

YES	NO	RL total
X		4
RL = 4		

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	8
	RL = 4	

Have some versions of signature older than the one before the latest version been identified ?

YES	NO	RL total
X		12
RL = 4		

If so, explain :
_As much as a quarter of the computer information system does not respect this criteria and an other quarter is overdue by a version___________________
____
____

Have little (or none) version not updated for the engin (« **Out of date Engine** ») been identified ?

YES	NO	RL total
	X	16
	RL = 4	

If not, explain :
__The majority of the computer information system__
does not seem updated to this level. An update has__
just come out at NAI which would explain the situation_
____

Have stations or servers been identified without an antivirus solution ?

YES	NO	RL total
X		20
RL = 4		

If so, explain :
__About 45_____________________________________
____
____
____

Have products considered unknown been identified ?

YES	NO	RL total
X		24
RL = 4		

If so, explain :
__37 out of 207 servers and over 200 stations ________
____
____
____

Have many version of NetShield or VirusScan been identified ?

YES	NO	RL total
X		28
RL = 4		

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

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 (http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/w2ksvrcl.asp)
- 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) (http://www.sans.org/score/checklists/AuditingWindows2000.doc)

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.

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 (http://windowsupdate.microsoft.com), 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, http://www.pwcglobal.com/extweb/ncsurvres.nsf/DocID/845A49566045759E80256B9D003A4773
- 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) http://www.ey.com/global/download.nsf/International/Global_Information_Security_Survey_2002/$file/FF0210.pdf
- The Twenty Most Critical Internet Security Vulnerability Version 2.504, The SANS Institute, May 2, 2002, http://www.sans.org/top20/
- Windows 2000 Security Recommendation Guides, National Security Agency, http://nsa1.www.conxion.com/win2k/download.htm
- Vulnerability Note VU#635463, Center of Internet Security (CERT), http://www.kb.cert.org/vuls/id/635463
- Security Information About SQL Server, http://www-tus.csx.cam.ac.uk/pc_support/security/sqlsecurity.html
- 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, http://www.all.net/books/audit/index.html
- IIS 5.0 Baseline Security Checklist, Microsoft Technet, http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/iis5cl.asp
- Secure Internet Information Services 5 Checklist, Microsoft Technet, http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/iis5chk.asp
- An Overview of Threat and Risk Assessment, James Bayne, Sans Institute Reading Rooms, January 22, 2002, http://www.sans.org/rr/audit/overview.php
- 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