GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

Interested in learning more?

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

Auditing Microsoft Corporate e-mail Solutions (Exchange 5.5 and Outlook 2000)

GSNA Practical Assignment
Version 1.1

Filipe Custódio,
September 2001

© SANS Institute 2000 - 2002, Author retains full rights.

Foreword

E-mail is probably the most successful Internet technology today. In people's homes, it has replaced the letter, the postcard and in some cases the long distance phone call. In the business world, it is replacing traditional letters, faxes and internal memos, as modern companies use it in a day-to-day basis to convey business decisions, corporate information and strategic data. Like with its traditional counterpart, people expect e-mail to provide a private communication channel between the emitter and its recipients. Unlike physical mail, however, e-mail is vulnerable to electronic attacks that take advantage of the Internet's unique characteristics: *automation*, *action at a distance* and *technique propagation*[1].

E-mail exchanged between two individuals is typically considered private information. Private conversation between important decision makers or technological experts may convey corporate confidential information. Loss of privacy or disclosure of confidential information can hurt a company deeply, and hence the importance of regular and thorough security audits targeting the e-mail system.

The purpose of this document is to present a methodology that may be used to audit e-mail systems based on Microsoft Exchange 5.5 and Microsoft Outlook 2000. This methodology is based on the existing standards and checklists, evolving from the current state of practice of e-mail auditing to a specific checklist that is both comprehensive and detailed from a technical point of view.

This document is organized in two parts. Part I develops an audit methodology and presents a checklist to be used in the audit process. Part II presents the application of this methodology to a Real World System.

[1] Schneier, Bruce. "Secrets & Lies". Chapter II, "The changing nature of attacks". 17-22.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Contents

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Part I: Research in Audit, Measurement Practice, and Control

1 Current State of Practice

After extensive research on the Internet, I found no specific checklist to audit an Exchange and Outlook environment. There are several guidelines on how to secure a Microsoft Exchange installation, and articles or checklists and procedures for very specific areas of e-mail security.

From my own professional experience, the current practice of auditing e-mail systems is based on adapting general-purpose audit standards to specific technological environments. The auditor is usually individually responsible for this effort, which causes the audit work to be very dependent on the individual that performs the audit. This is an important shortcoming from the current practice, and one I expect to change with this document.

This white paper will start from a general-purpose security standard and adapt it to the specific technological environment that is the focus of this project. I will use a risk analysis approach to map specific risks listed in the general-purpose standard to the technical issues to look at.

The most widely used audit standard in Europe is British Standard BS7799, which provides an overview of security issues to analyse in several areas.

BS7799 lists the following security risks regarding electronic mail [2]:

a) Vulnerability of messages to unauthorized access or modification or denial of service;
b) Vulnerability to error, e.g. incorrect addressing or misdirection, and the general reliability and availability of the service;
c) Impact of a change of communication media on business processes, e.g. the effect of increased speed of despatch or the effect of sending formal messages from person to person rather than company to company;
d) Legal considerations, such as the potential need for proof of origin, despatch, delivery and acceptance;
e) Implications of publishing externally accessible staff lists;
f) Controlling remote user access to electronic mail accounts.

BS7799 is very comprehensive in the listing of security issues. However, it is technological neutral, which means that it is left to the auditor to choose the methods or checklists used to ensure the mitigation of the listed risks.

Other references I will list throughout this document contain detailed technical information on how to secure or audit a specific environment. These references have varying levels of

[2] BS 7799-1:1999, "8.7.4. Security of electronic mail"

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

breadth and depths, and it is one goal of this white paper to present a checklist that includes their contents in a consistent way.

The audit methodology presented in this document will be compliant with BS7799. Specifically, the following requirements will be followed [3]:

a) Audit requirements should be agreed with appropriate management;
b) The scope of the checks should be agreed and controlled;
c) The checks should be limite d to read-only access to software and data;
d) Access other than read-only should only be allowed for isolated copies of system files, which should be erased when the audit is completed;
e) IT resources for performing the checks should be explicitly identified a nd made available;
f) Requirements for special or additional processing should be identified and agreed;
g) All access should be monitored and logged to produce a reference trail;
h) All procedures, requirements and responsibilities should be documented.

These requirements will be relevant to the tests presented in the checklist (requirement c) and d)) and to the audit procedures described in chapter 4.

© SANS Institute 2000 - 2002, Author retains full rights

[3] BS 7799-1:1999, "12.3.1 System audit controls"

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

2 The Audit Methodology

Security audit methodologies usually use a similar approach, regardless of the specific environment being audited. In three basic steps, a security audit should help answer the following questions:

1. **Where Should We Be?** – Establish the security level that the company should be aiming at, considering the risk level it is willing to assume and the value of the assets being protected;
2. **Where Are We Today?** – Access the current security situation;
3. **How Do We Get There?** – Define the steps that need to be taken to secur e the environment, prioritising them according to the impact each action has on the global security level.

I'll now examine each one of these questions in detail, when applied to corporate e -mail systems.

2.1 Establishing the Goals: Where Should We Be?

No investment should be done in IT security without a clear sense of strategic direction. In lay terms, "if you don't know where you're going, how do you expect to ever get there?"

To establish a goal in e -mail security, one must consider the following aspects:

a) E-mail security goals (as described in the company's E -mail Security Policy or IT Security Plan);
b) Corporate specific security restrictions (specific security -related issues, budget constraints, etc.);
c) Local, Regional or Nation -specific legal restrictions (privacy laws, etc.);
d) Current e-mail security best practices.

E-mail security should be as high as possible, given the above restrictions. The checklist presented in this paper represents ideal goals in e -mail security, according to industry best practices. Every non-conformance to the checklist due to security policy restrictions should be carefully documented.

2.2 Knowing the Current Status: Where Are We Today?

This step is the bulk work of the security audit. Information should be collected to clearly identify how the e -mail security is implemented. This process of data recollection employs several different methods, like:

- Interviews (for the information that cannot be measured objectively);
- Direct observation of configuration parameters (for information th at cannot be tested);
- Specific software tests (for information that can be obtained by software tests).

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Depending on the specific environment of the audit, data recollection can sometimes be challenging. Some guidelines to assist in this critical effort a re the following:

- **When possible, use software tests instead of configuration observation** : Software tests can test both the configuration of the e -mail software and its implementation;
- **Gather information early in the audit process** : Information is the basis of a good audit process. Some information is more volatile than other, and should be collected first;
- **Take special care when interviewing people** : An audit process can sometimes get very messy. It is very important to keep a good professional relationship w ith those being audited. Bad relationship with one of your primary sources of information can undermine the whole audit effort.

2.3 Tracing the Course: How Do We Get There?

The audit report should be a guideline that can, on its own, direct the implementation effort to solve any security problems detected, thus increasing the level of security.

A good audit report will say, down to the technical level, what needs to be done, always keeping in mind the security goals established at the beginning of the work.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

3 E-mail Security Threats

Knowing the threats is fundamental to designing and implementing good protection mechanisms to minimize their likelihood of success. It's also of utmost importance when designing an audit methodology that should test the defences in place.

To conduct a threat analysis, one must know three things: The assets being threatened, the type of attacks possible on those assets, and their likelihood of success.

3.1 Microsoft Exchange Information Assets

The assets that exist in any e-mail system are the following:

- **Message contents**: This is the "crown jewels" of any e-mail system. Any protection mechanism in place should have the defence of the contents of messages exchanged between people as its primary concern;
- **Account database**: Information about valid accounts in any system should always be considered privileged. Knowing which e-mail accounts actually exist at a company is a terribly powerful information for attackers, ranging from UCE [4] senders to social engineers;
- **User credentials**: Most e-mail systems require a user to authenticate with his username and password before being able to read their e-mail. Microsoft Exchange uses a Windows NT Domain Controller to store and validate user credential, thus allowing the credentials used to access system and network resources to be used for mail as well. This "single-sign-on" functionality, although useful to the end-users, results in a security issue, as the same set of username and password is used in many different protocols, with varying levels of security. This means that, for instance, if an attacker captures the username and password of a victim during a POP3 exchange, he automatically gains access to any network resource on the Windows Network that is accessible with that set of credentials;
- **Routing log**: If knowing the contents of messages is important to attackers, knowing who sent messages to whom and at what time is the next best thing. Knowledge about information flow can give attackers hints about active versus inactive users, decision makers versus executive personnel, etc.

Exchange mail systems store much more information that is not totally related to e-mail, and that can also be exploited maliciously. This information includes:

- **Contact databases**: e-mail viruses commonly explore these. The speed at which some of these viruses spread across the World gives us some idea on how contact databases are interlinked. This collective and distributed database of contacts is very valuable to UCE senders and other attackers. It is very important that companies protect their contact database, as it typically holds prime information on the companies customers, partners, suppliers and employees;

[4] UCE: Unsolicited Commercial E-mail

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

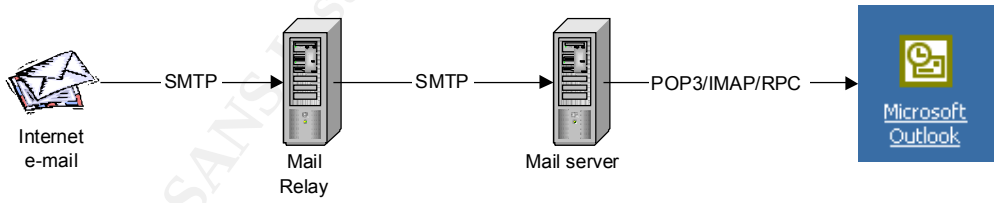
- **Calendar**: One of the groupware functionalities that Exchange provides is a shared company-wide agenda, where each employee can schedule appointments and meetings. This agenda is a primary source of information about what goes on inside the company. If an attacker is able to modify this information, he may be able to inflict harm to the company, for example, by cancelling important meetings with customers.

In a typical Microsoft Exchange mail system, this information can be found in the following locations:

Information Asset	Location
E-mail messages	➢ Exchange private store; ➢ Outlook "Personal Folders" file; ➢ Network.
Account database	➢ Primary domain controller; ➢ Exchange SMTP interface; ➢ Exchange POP3 interface.
User credentials **Routing log**	➢ Network. ➢ Exchange logs.
Contact database	➢ Exchange private store; ➢ Outlook "Personal Folders" file.
Calendar	➢ Exchange private store; ➢ Outlook "Personal Folders" file.

One of the main concerns when analysing Exchange security should be the network links between the Exchange server and the mail clients, other Exchange servers and the Internet.

Exchange uses a wide range of protocols to communicate, each one having its particular security concerns. To better explain this variety, I'll present here a typical incoming e-mail circuit based on Microsoft products:



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Using the above example, the network connections th at exist are the following:

Network connection	Information	Protocols
Internet to Relay server	Mail messages	➢ SMTP
Mail server to Relay server	Mail messages	➢ SMTP ➢ RPC
Outlook client to Mail server	Mail messages, user credentials	➢ SMTP ➢ POP3 ➢ IMAP4 ➢ RPC
Remote e-mail clients to Relay Server	Mail messages, user credentials	➢ SMTP ➢ POP3 ➢ IMAP4 ➢ RPC

3.2 Exchange Information Threats

After enumerating the assets that should be protected, and the location these assets reside in, let's look at the possible threats to this as sets, and how these threats can be executed.

Any information asset may be subject to 3 types of threats:

- Disclosure;
- Availability;
- Integrity.

Crossing these 3 types of threats with the assets we identified earlier, we can obtain a comprehensive knowledge of the possible threats the mail system is subject to:

	Type of Threat		
Asset	Disclosure	Availability	Integrity
Exchange Server		➢ **Availability Attack**	➢ **Availability Attack**
Outlook Client		➢ **Mail Virus**	➢ **Mail Virus**
E-mail messages	➢ **Confidentiality or Privacy Violation**		➢ **Mail Forgery** ➢ **Information Destruction** ➢ **Information Hijack**
Account Database	➢ **Privacy Violation** ➢ **Information Gathering** ➢ **Authentication Attack**	➢ **Availability Attack**	➢ **Availability Attack** ➢ **Identity Theft** ➢ **Information Destruction** ➢ **Information Hijack**
User Creden tials	➢ **Identity Theft** ➢ **Mail Forgery** ➢ **Confidentiality or Privacy Violation**		➢ **Availability Attack**
Routing Log	➢ **Information Gathering**		➢ **Disposing of Evidences**

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

	Type of Threat		
Asset	Disclosure	Availability	Integrity
Contact Database	➢ **Information Gathering** ➢ **Mail Virus**		➢ **Availability Attack** ➢ **Identity Theft** ➢ **Information Destruction** ➢ **Information Hijack**
Calendar	➢ **Confidentiality or Privacy Violation** ➢ **Information Gathering**		➢ **Calendar Attacks** ➢ **Information Destruction** ➢ **Information Hijack**

The above analysis results in the following list of e -mail threats:

- Unsolicited Commercial E -mail
- Mail Forgery
- Availability Attack
- Mail Virus
- Confidentiality or Privacy Violation
- Information Destruction
- Information Hijack
- Information Gathering
- Authentication Attack
- Identity Theft
- Disposing of Evidences
- Calendar Attacks

These threats can be considered under the following risks identified by BS7799 [5]:

E-Mail Security Risk	E-Mail Threat
"Vulnerability of messages to unauthorized access or modification or denial of service"	➢ Availability Attack ➢ Mail Virus ➢ Confidentiality or Privacy Violation ➢ Information De struction ➢ Information Hijack ➢ Information Gathering ➢ Disposing of Evidences
"Vulnerability to error, e.g. incorrect addressing or misdirection, and the general reliability and availability of the service"	➢ Mail Forgery

[5] E-mail security risks quoted from BS 7799 -1:1999, "8.7.4 Security of electronic mail"

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

E-Mail Security Risk	E-Mail Threat
"Implications of publishing externall y accessible staff lists"	➢ Unsolicited Commercial E -mail ➢ Mail Virus
"Controlling remote user access to electronic mail accounts"	➢ Authentication Attack ➢ Identity Theft

© SANS Institute 2000 - 2002, Author retains full rights.

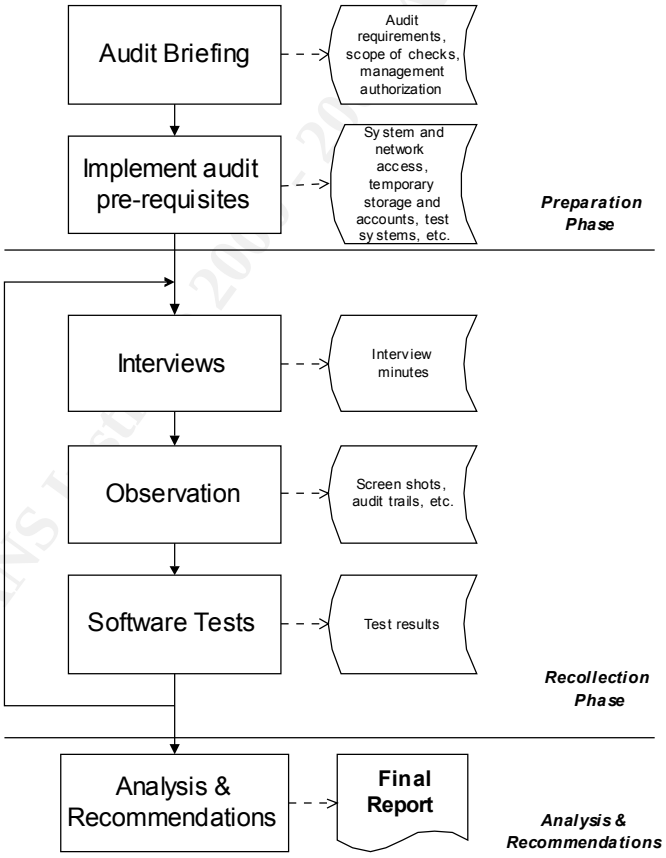
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

4 Audit Procedures

The audit procedures presented here are intended to assure compliance with section 12.3.1 of BS7799[6]. Specifically, the following controls will be regarded by the audit procedures (quoted directly from BS7799):

a) Audit requirements should be agreed with appropriate management;
b) The scope of the checks should be agreed and con trolled;
c) The checks should be limited to read -only access to software and data;
d) Access other than read-only should only be allowed for isolated copies of system files, which should be erased when the audit is completed;
e) IT resources for performing the chec ks should be explicitly identified and made available;
f) Requirements for special or additional processing should be identified and agreed;
g) All access should be monitored and logged to produce a reference trail;
h) All procedures, requirements and responsibilit ies should be documented.

The audit procedures and the deliverables expected in each phase are the following:



[6] BS 7799-1:1999, "12.3.1 System audit controls"

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

To ensure the success of the audit, the following must be observed:

a) Audit scope and requisites should be agreed with the management of the au dit subject;
b) Proper written authorization must be obtained for specific types of tests (for example, vulnerability assessment);
c) All pre-requisites (IT resources, temporary accounts, availability of key personnel, etc.) must be available prior to the audit work;
d) Every input to the audit process must be clearly documented.

© SANS Institute 2000 - 2002, Author retains full rights

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

5 The Checklist

Now that I've explained the basic guidelines of this e-mail auditing methodology, I'll present here a checklist that aims to be as comprehensive as possible, both in the technological and the methodological aspects.

This checklist will contain both objective and subjective tests. The basic rule is that anything that can be measured or replied with a simple "yes" or "no" is listed as an objective test. Anything that requires the subjective input of the auditor is listed as a subjective test.

All tests in this checklist are objective unless there is an explicit indication otherwise. In this case, the auditor is expected to explain his reasoning besides stating a "pass" or "fail" classification.

All checks in this checklist have a binary output. Requisites for passing a test are listed in the test explanation, unless they are self-evident.

Any non-compliance with the audit checklist must be documented in the audit report.

5.1 Generic Security Issues

5.1.1 Secure the Servers

Security of any computer system is only as strong as its weakest component. The operating system is frequently a source of vulnerability.

Securing the operating system is beyond the scope of this document. There are several checklists on securing Windows NT or 2000, including the excellent "Windows NT Security Step by Step" by the SANS Institute.

However, there are a couple of steps that can be done in an e-mail security audit to make sure the system holds minimal security levels. The following checklist should be applied to all Exchange Servers relevant to the e-mail system under audit and their supporting Domain Controllers or Active Directories.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Vulnerability and hot -fix Checklist for all Exchange Servers and supp orting DC or AD	Pass	Fail
Server Name: _____ Date: __/__/____ Auditor: _____		
1. Check for known vulnerabilities *This can be achieved by running a vulnerability scanner against the server. Best results can be obtained by using two different scanners from different manufacturers. "Pass" means no significant vulnerabilities where found.*	☐	☐
2. Security hot-fixes *Make sure all security hot -fixes are up to date.* *The best way to do this is by using Microsoft "HFNetChk" tool [7].* *"Pass" means no significant security hot -fix missing.*	☐	☐

5.1.2 Secure the Desktop OSs

As with servers, desktop computers also need to be up -to-date on hot-fixes. However, it is frequently unpractical to audit all workstations. In these cases, a sample representative group should be used.

Besides indicating the number of systems tested, the total number of systems and, for each test, the number of systems that have passed or failed the test, the auditor should attach the exact results for each of the tested systems.

Vulnerability and hot -fix Checklist for Workstations	Pass	Fail
# systems tested/ # total: ____/____ Date: __/__/____ Auditor: _____		
3. Check for known vulnerabilities *This can be achieved by running a vulnerability scanner against the workstation. Best results can be obtained by using two different scanners from different manufacturers. "Pass" means no significant vulnerabilities where found.*	☐	☐
4. Security hot-fixes *Make sure all security hot -fixes are up to date.* *The best way to do this is by using Mic rosoft "HFNetChk" tool [8] (for Windows NT or 2000 workstations).* *"Pass" means no significant security hot -fix missing.*	☐	☐

5.2 Mail Virus

Evan Morris, in his articles "A Viral Survival Checklist" [9] and "Update to A Viral Survival Checklist" [10] establishes some bas ic rules to secure an Exchange and Outlook environment against e-mail viruses. The checklist presented here is based mainly on those articles:

[7] http://www.microsoft.com/technet/itsolutions/security/tools/hfnetchk.asp
[8] http://www.microsoft.com/technet/itsolutions/security/tools/hfnetchk.asp
[9] Morris, Eva n. "A Viral Survival Checklist". May 2000.
[10] Morris, Evan. "Update to A Viral Survival Checklist". June 2000.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Virus defences Checklist	Pass	Fail
Date: __/__/____ Auditor: _____		
5. End users educated regarding e -mail virus risks (subjective) _____ _____	☐	☐
6. Clear and comprehensive security policy exists regarding e -mail viruses *Policy should contain types of files that should be allowed through the e -mail system, either inbound or outbound. It should also explicitly list the actions users are prohibited to do regarding e -mail.* **Failure in this test precludes tests 7 to 8.**	☐	☐
7. End users comply with security policy (subjective) _____ _____	☐	☐
8. Technology in place complies and enforces existing security policy	☐	☐
9. End users should not read e -mail with local Administrator or Domain Administrator rights (subjective) _____ _____	☐	☐
10. Anti-viral filter exists at the Firewall *List any gateway mail virus filtering software. For each one, a separate "anti -virus software checklist (gateway)" should be present ed:* _____; _____; _____	☐	☐
11. Anti-viral software exists at the Exchange mail server *List any Exchange mailboxes virus filtering software. For each one, a separate "anti -virus software checklist (mail server)" should be presented:* _____; _____; _____	☐	☐
12. Anti-viral software exists at the desktop *List any desktop mail virus protection software. For each one, a separate "anti -virus software checklist (workstation)" s hould be presented:* _____; _____; _____	☐	☐

To check the security of the Outlook clients, the auditor should choose a representative pool of systems to apply the following checklist:

Anti-virus measures fo r Workstations	Pass	Fail
# systems tested/ # total: ____/____ Date: __/__/____ Auditor: _____		
13. Outlook attachment security set to "high" *This setting prevents the opening of attachments without prior notice.*	☐	☐
14. File extensions are visible *By default windows is configured not to show file extensions on known file types. This*	☐	☐

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Anti-virus measures fo r Workstations	Pass	Fail
# systems tested/ # total: ____/____ Date: __/__/____ Auditor: _____		
allows an attacker to disguise a Trojan file under a different apparent extension. For instance, "test.txt.vbs" would be showed as "test.txt".		
15. File extensions for active content types mapped to harmless operation *File extensions "vbs", "vbe", "js", "jse", "wsf" and "wsh" should be mapped in the registry to "edit" instead of "execute".*	☐	☐

For every instance of a Firewall based anti -virus product, the auditor should pres ent the following checklist:

Anti-Virus Software Checklist (Gateway)	Pass	Fail
Product/version: _____ Date: __/__/____ Auditor: _____		
16. EICAR signature detected *Send an e-mail containing the text "X5O!P%@AP[4 \PZX54(P^)7CC)7}$EICAR -STANDARD-ANTIVIRUS-TEST-FILE!$H+H*". Anti -viral software should accuse the presence of the "EICAR test file virus" [11].* **Failure in this test precludes tests 17 to 19.**	☐	☐
17. Infected e-mail was rejected	☐	☐
18. Sender receives virus notification *It is not considered mandatory that notifications be sent, although it is a good practice. A "Fail" in this item will not result in the failure of the audit.*	☐	☐
19. Recipient receives virus notification *It is not consi dered mandatory that notifications be sent, although it is a good practice. A "Fail" in this item will not result in the failure of the audit.*	☐	☐
20. Viral database is up -to-date *If possible, check the date of the last signature update against the latest upd ate file available at the vendor site. If not, check if the last update occurred during the last month.*	☐	☐
21. Updates to viral database are automatic *"Pass" here means there is an automatic procedure to update the viral database on a regular basis that is c ompatible with the anti -virus security policy in place. This automatic update can be a feature of the anti -virus software or any other procedure that does not depend on human intervention.*	☐	☐

For every instance of a Mail Server based anti -virus product, the auditor should present the following checklist:

Anti-Virus Software Checklist (Mail Server)	Pass	Fail
Product/version: _____ Date: __/__/____ Auditor: _____		
22. EICAR signature detected *Post a message containing the text "X5O!P %@AP[4 \PZX54(P^)7CC)7}$EICAR -STANDARD-ANTIVIRUS-TEST-FILE!$H+H*". Anti -viral software should accuse*	☐	☐

[11] For more information: http://www.eicar.com/anti_virus_test_file.htm

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Anti-Virus Software Checklist (Mail Server)	Pass	Fail
Product/version: _____ Date: __/__/____ Auditor: _____		
the presence of the "EICAR test file virus" [12]. **Failure in this test precludes tests 17 to 19.**		
23. Post of an infected message was rejected	☐	☐
24. Sender receives virus notification *It is not considered mandatory that notifications be sent, although it is a good practice. A "Fail" in this item will not result in the failure of the audit.*	☐	☐
25. Viral database is up-to-date *If possible, check the date of the last signature update against the latest update file available at the vendor site. If not, check if the last update occurred during the last month.*	☐	☐
26. Updates to viral database are automatic *"Pass" here means there is an automatic procedure to update the viral database on a regular basis that is compatible with the anti-virus security policy in place. This automatic update can be a feature of the anti-virus software or any other procedure that does not depend on human intervention.*	☐	☐

For every different version of desktop anti-virus software, the auditor should present the following checklist, representing the results of a sample system:

Anti-Virus Software Checklist (Workstation)	Pass	Fail
Product/version: _____ Date: __/__/____ Auditor: _____		
27. EICAR signature detected *Send an e-mail containing the text "X5O!P%@AP[4 \PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*". Anti-viral software should accuse the presence of the "EICAR test file virus"* [13]. **Failure in this test precludes tests 28 to 29.**	☐	☐
28. Infected e-mail fails to open	☐	☐
29. No option exist to open infected e-mail, despite of virus warning	☐	☐
30. Viral database is up-to-date *If possible, check the date of the last signature update against the latest update file available at the vendor site. If not, check if the last update occurred during the last month.*	☐	☐
31. Updates to viral database are automatic *"Pass" here means there is an automatic procedure to update the viral database on a regular basis that is compatible with the anti-virus security policy in place. This automatic update can be a feature of the anti-virus software or any other procedure that does not depend on human intervention.*	☐	☐

[12] For more information: http://www.eicar.com/anti_virus_test_file.htm
[13] For more information: http://www.eicar.com/anti_virus_test_file.htm

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

5.3 Information Confidentiality and Integrity

This section handles risks to the **confidentiality** and **integrity** of e-mail information.

5.3.1 Physical Security

Physical access to an Exchange server can easily compromise the confidenti ality and the integrity of its information. The following physical security checklist is based on BS7799 section 7 "Physical and environmental security". Only the most relevant checks were included:

Physical Security Checklist	Pass	Fail
Location: _____ _____ Date: __/__/____ Auditor: _____		
32. Security perimeter is clearly defined (subjective) _____ _____	☐	☐
33. Perimeter is physically sound (subjective) _____ _____	☐	☐
34. There is a manned reception area responsible for access control and log	☐	☐

5.3.2 Outlook Personal Folders File Protection

Mail messages reside either in the Exchange Server mailbox or in the user's PST file. To protect the confidentiality and integrity of messages, both storage locations have to be considered.

Outlook PST files can be protected from abuse by following the checklist below. Some of these checks are from Microsoft's Q143241 – "XCLN: Improving the Security of PST Files"[14]:

PST File Protection Checklist	Pass	Fail
# systems tested/ # total: ___ /___ Date: __/__/____ Auditor: _____		
35. File level permissions are configured to protect the file from unauthorized copy *Windows 2000 or NT only.*	☐	☐
36. File is accessible through the network	☐	☐
37. File access is logged as a security event	☐	☐
38. PST file is password protected	☐	☐

[14] http://support.microsoft.com/directory/article.asp?ID=KB;EN -US;Q143241

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

5.3.3 *Administrator Rights*

Exchange administrators by default have access to all mailboxes in the system. Domain administrators have access to all PST files stored in the network, besides being allowed to erase Exchange log files. This is why no single user should have domain administrator and exchange administrator rights at the same time.

Administrator Checklist **Date: __/__/____ Auditor: _____**	Pass	Fail
39. No user shares domain admin and exchange admin rights	☐	☐
40. Minimal privilege principle is implemented (subjective) _____ _____	☐	☐
41. Default system accounts are not used	☐	☐

5.3.4 *Alternate Recipients*

It is possible to assign alternate recipients for any Exchange mailbox. Any e-mail delivered to this mailbox will be forwarded to the defined alternate recipients.

This feature can be used to spy on mailboxes. It is therefore important to check the existence of alternate recipients against the defined security policy. This can be achieved by the following checklist:

Alternate Recipient Checklist **Date: __/__/___ Auditor: _____**	Pass	Fail
42. Clear policy exists regarding alternate recipients *Policy should state in which cases alternate recipients are allowed, and how they should be documented.*	☐	☐
43. No illegitimate alternate recipient found	☐	☐

5.3.5 *Access to User's Mailbox*

Whenever a user accesses a mailbox that he does not own, an event with an ID of 1016 is generated in Microsoft Exchange's application log. This event can be used to detect unauthorized access to a user's mailbox. The following checklist checks this:

Access to a different mailbox Checklist **Date: __/__/____ Auditor: __ _____**	Pass	Fail
44. Clear policy exists regarding access to a user's mailbox by an Exchange admin *Policy should state in which cases user's mailboxes can be accessed by Exchange administrators*	☐	☐
45. No indication of violation of policy found	☐	☐

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Part II: Application of Audit Techniques to a Real World System

This audit work was conducted between the 20 th August 2001 and September 14 th 2001. The name of the company and any information that could be used to identify it has been removed for security reasons.

1 The Audit Environment

The environment being audited consists of:

- One Exchange Server 5.5 SP3 running on a Windows NT 4.0 SP6a platform;
- One Primary Domain Controller and two Secondary Domain controllers used for user authentication and authorization;
- About 400 workstations running all flavours of Windows with Outlook 2000 as the mail client.

1.1 Audit Specifics

The company being audited is an IT company with a varying number of highly skilled employees. Most of the employees work at the premises, but a growing number are working from customer sites or even from their homes. They are usually issued company notebooks for this purpose.

The objectives of the audit from the customer point of view were the following:

- Evaluate the level of privacy and confidentiality of electronic mail. Specifically, management wanted to know who in the company had access to which accounts (i.e. can the systems administrator read the mail of the president of the company?);
- Evaluate the global level of e-mail security implemented by the company.

As an outsourced contractor, my work had some restrictions. The most important of these were:

- Physical access to the Exchange server was only possible with the company of a systems administrator;
- No screen shots of the Exchange server console were possible;
- No access to the domain controllers was given;
- Any log file requested was delivered by the systems administrator;
- No domain administrator access was possible;
- Analysis of Outlook workstations was limited to one notebook with the standard configuration directed by company policy.

Although these restrictions sometimes limited my work, they were pre-requisites imposed by the customer. Naturally, all restrictions were listed in the audit report, and a recommendation was given to reduce the restrictions in future audit assignments.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

2 Conducting the Audit

2.1 Audit Briefing

The audit briefing was held on the morning of the 20 th August 2001. The result of the briefing was:

a) Audit scope: check privacy and confidentiality levels of electronic e -mail, test global security level of current implementation;
b) Security checks were to be conducted during business hours, except for vulnerability assessments. These could only be done against the Exchange server after 8 pm. A member of the systems administration staff would stand b y to reboot the server after the security tests;
c) Systems Administrator SA1 (real name removed for security reasons) was appointed as primary contact, and was instructed to provide any required information and assistance;
d) Vulnerability Assessment permission granted in signed agreement, limited to the Exchange server and in the period 8 pm to 9 am;
e) Domain Administrator access denied, SA1 was instructed to provide any necessary information or systems access;
f) Access to a pool of workstations denied; SA1 deliver ed a notebook with the standard company configuration: Windows 2000 Professional, Outlook 2000;
g) Temporary mail account: granted, user name was "audit";
h) Information regarding perimeter anti -virus software: denied on security reasons. Permission was granted to test perimeter anti -virus defences, nevertheless.

2.2 Interviews

Systems administrators SA1, SA2 and SA3 were interviewed. The result of the interviews was the following:

a) The Internet address for the Exchange mail server is "mail2.XXXXXXXX.pt";
b) Remote users use POP3 to connect to the mail server and download their e -mail;
c) User authentication is performed with the domain username and password, authenticated by the domain controllers "XXPDC", "XXBDC" and "XXBDC2";
d) Internal users use Exchange RPC communication with the Exchange server;
e) Anti-viral protection exists at the firewall level and on the workstations;
f) RAS access is disabled;
g) SA1 is responsible for e -mail administration tasks;
h) SA2 is responsible for perimeter and network security;
i) SA3 is responsible for internal user support.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

2.3 Generic Security Issues

2.3.1 Secure the Servers

These checks were performed on the Exchange Server only:

Vulnerability and hot -fix Checklist for all Exchange Servers and supporting DC or AD	Pass	Fail
Server Name: MAIL2.XXXXXXXX.PT Date: 21/08/2001 Auditor: FMC		
1. Check for known vulnerabilities *This can be achieved by running a vulnerability scanner against the server. Best results can be obtained by using two different scanners from different manufacturers.* *"Pass" means no significant v ulnerabilities where found.*	☒	☐
2. Security hot-fixes *Make sure all security hot -fixes are up to date.* *The best way to do this is by using Microsoft "HFNetChk" tool* [15]. *"Pass" means no significant security hot -fix missing.*	☒	☐

To check for common vulnerabili ties, I used nmap to map the ports seen from the outside. The output was:

```
# Nmap (V. nmap) scan initiated 2.53 as: nmap   -sS -vv -O -oN
/tmp/mail2.scan mail2.XXXXXXXX.pt
Interesting ports on  (XXX.XXX.XXX.XXX):
(The 1521 ports scanned but not shown below   are in state: filtered)
Port       State       Service
110/tcp    open        pop -3
143/tcp    open        imap2

TCP Sequence Prediction: Class=trivial time dependency
                         Difficulty=3 (Trivial jo  ke)

Sequence numbers: 5FB14 5FB14 5FB16 5FB22 5FB30 5FB30
Remote operating system guess: NT Server 4.0 SP5 running Checkpoint
Firewall -1
OS Fingerprint:
TSeq(Class=TD%gcd=2%SI=3)
T1(Resp=Y%DF=Y%W=2017%ACK=S++%Flags=AS%Ops=M)
T2(Resp=N)
T3(Resp=Y%DF=Y%W=20 17%ACK=S++%Flags=AS%Ops=M)
T4(Resp=N)
T5(Resp=N)
T6(Resp=N)
T7(Resp=N)
PU(Resp=N)


# Nmap run completed at Mon Sep 17 06:47:17 2001   -- 1 IP address (1 host
up) scanned in 195 seconds
```

[15] http://www.microsoft.com/technet/itsolutions/security/tools/hfnetchk.asp

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The open ports were then given to Nessus (v. 1.0.7) to check for known vulnerabilities. The output was the following:

Nessus Scan Report

Number of hosts which were alive during the test : 1
Number of security holes found : 0
Number of security warnings found : 0
Number of security notes found : 3

List of the tested hosts :

- XXX.XXX.XXX.XXX **(Security notes found)**

[Back to the top]

XXX.XXX.XXX.XXX :

List of open ports :

- *pop-3 (110/tcp) (Security notes found)*
- *imap2 (143/tcp)*
- *general/udp (Security notes found)*
- *general/tcp (Security notes found)*

[back to the list of ports]

Information found on port pop -3 (110/tcp)

The remote POP server banner is :

+OK Microsoft Exchange POP3 server version 5.5.2650.23 ready

[back to the list of ports]

Information found on port general/udp

For your information, here is the traceroute to XXX.XXX.XXX.XXX :

?

[back to the list of ports]

Information found on port general/tcp

QueSO has found out that the remote host OS is

* Reliant Unix from Siemens -Nixdorf

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

CVE : CAN-1999-0454

This file was generated by Nessus, the open-sourced security scanner.

2.3.2 Secure the Desktop OSs

Vulnerability and hot -fix Checklist for Workstations	Pass	Fail
# systems tested/ # total: 1/400 **Date: 11/09/2001** **Auditor: FMC**		
3. Check for known vulnerabilities *This can be achieved by running a vulnerability scann er against the workstation. Best results can be obtained by using two different scanners from different manufacturers.* *"Pass" means no significant vulnerabilities where found.*	☒	☐
4. Security hot-fixes *Make sure all security hot -fixes are up to date.* *The best way to do this is by using Microsoft "HFNetChk" tool [16] (for Windows NT or 2000 workstations).* *"Pass" means no significant security hot -fix missing.*	☐	☒

The output of nmap regarding the notebook being tested was:

```
# Nmap (V. nmap) scan initiated 2.53 as:  nmap -sS -vv -O -oN
/tmp/eneadas.scan 192.168.10.5
Interesting ports on eneadas.XXXXXXXX.pt (192.168.10.5):
(The 1519 ports scanned but not shown below are in state: closed)
Port       State       Service
135/tcp    open        loc -srv
139/tcp    open        netbios -ssn
445/tcp    open        microsoft -ds
1026/tcp   open        nterm

TCP Sequence Prediction: Class=random positive increments
                         Difficulty=9482 (Worthy challe  nge)

Sequence numbers: FE5D451 FE69012 FE78288 FE89875 FE94D79 FEA13BF
No OS matches for host (If you know what OS is running on it, see
http://www.insecure.org/cgi -bin/nmap-submit.cgi).
TCP/IP fingerprint:
TSeq(Class=RI%gcd=1%SI=3547)
TSeq(Class=RI%gcd=1 %SI=2966)
TSeq(Class=RI%gcd=1%SI=250A)
T1(Resp=Y%DF=N%W=402E%ACK=S++%Flags=AS%Ops=MNWNNT)
T2(Resp=Y%DF=N%W=0%ACK=S%Flags=AR%Ops=)
T3(Resp=Y%DF=N%W=402E%ACK=S++%Flags=AS%Ops=MNWNNT)
T4(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%  Ops=)
T6(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T7(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
PU(Resp=N)
```

[16] http://www.microsoft.com/technet/itsolutions/security/tools/hfnetchk.asp

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
# Nmap run completed at Mon Sep 17 07:29:33 2001   -- 1 IP address (1 host
up) scanned in 5 seconds
```

The open ports were then given to Nessus (v. 1.0.7) to ch eck for known vulnerabilities. The output was the following:

Nessus Scan Report

Number of hosts which were alive during the test : 1
Number of security holes found : 1
Number of security warnings found : 3
Number of security notes found : 8

List of the tested hosts :

- 192.168.10.5 **(Security holes found)**

[Back to the top]

192.168.10.5 :

List of open ports :

- *unknown (135/tcp)* *(Security warnings found)*
- *netbios-ssn (139/tcp)* *(Security hole found)*
- *unknown (445/tcp)*
- *unknown (1026/tcp)* *(Security notes found)*
- *unknown (1025/tcp)* *(Security notes found)*
- *general/udp* *(Security notes found)*
- *general/tcp* *(Security warnings found)*
- *general/icmp* *(Security warnings found)*

[back to the list of p orts]

Warning found on port unknown (135/tcp)

DCE services running on the remote can be enumerated by connecting on port 135 and doing the appropriate queries.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

An attacker may use this fact to gain more knowledge
about the remote host.

Solution : filter incoming traffic to this port.
Risk factor : Low

[back to the list of ports]

Information found on port unknown (135/tcp)

The DCE Service 'ntsvcs' is running on this host
Type : ncalrpc
UUID : 7b91f80d-ff5a-11d0-a9b2-c04fb6e60000
Annotation : Messenger Service

[back to the list of ports]

Information found on port unknown (135/tcp)

The DCE Service 'LRPC00000294.00000001' is running on this host
Type : ncalrpc
UUID : f706820d-511f-e80a-3007-6d740be8cee9

[back to the list of ports]

Information found on port unknown (135/tcp)

The DCE Service 'LRPC00000294.00000001' is running on this hos t
Type : ncalrpc
UUID : 8e52b00d-a937-cfc0-1182-2daa51e40000

[back to the list of ports]

Vulnerability found on port netbios -ssn (139/tcp)

. It was possible to log into the remote host using a NULL session.
The concept of a NULL session is to provide a null username and
a null password, which grants the user the 'guest' access

. All the smb tests will be done as "/"

[back to the list of por ts]

Information found on port unknown (1026/tcp)

A DCE service is listening on 192.168.10.5:1026 :

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Type: ncacn_ip_tcp

UUID : 8e52b00d-a937-cfc0-1182-2daa51e40000

[back to the list of ports]

Information found on port unknown (1026/tcp)

A DCE service is listening on 192.168.10.5:1026 :

Type: ncacn_ip_tcp

UUID : f706820d-511f-e80a-3007-6d740be8cee9

[back to the list of ports]

Information found on port unknown (1025/tcp)

A DCE service is listening on 192.168.10.5:1025 :

Type: ncacn_ip_udp

UUID : 7b91f80d-ff5a-11d0-a9b2-c04fb6e60000

Annotation : Messenger Service

[back to the list of po rts]

Information found on port general/udp

For your information, here is the traceroute to 192.168.10.5 :

192.168.10.5

[back to the list of ports]

Warning found on port general/tcp

The remote h ost uses non-random IP IDs, that is, it is possible to predict the next value of the ip_id field of the ip packets sent by this host.

An attacker may use this feature to determine if the remote host sent a packet in reply to another request. This may be used for portscanning and other things.

Solution : Contact your vendor for a patch

Risk factor : Low

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

[back to the list of ports]

Information found on port general/tcp

QueSO has found out that the r emote host OS is

* WindowsNT, Cisco 11.2(10a), HP/3000 DTC, BayStack Switch

CVE : CAN-1999-0454

[back to the list of ports]

Warning found on port general/icmp

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine.

This may help him to defeat all your time based authentifications protocols.

Solution : filter out the icmp timestamp requests (13), and the outgoing icmp timestamp replies (14).

Risk factor : Low

CVE : CAN-1999-0524

This file was generated by Nessus, the open-sourced security scanner.

The security notes Nessus pointed out are not very relevant in an intranet environment. None of them is dangerous enough to cause an audit failure in this test.

To check the current state regarding hot-fixes, I used the "HFNetChk" tool. It's output follows:

```
C:\tools\security>hfnetchk
Microsoft Network Security Hotfix Checker, 3.1
Developed for Microsoft by Shavlik Technologies, LLC
info@shavlik.com (www.shavlik.com)
```


© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
 ** Attempting to download the XML from
http://download.microsoft.com/download/x
ml/security/1.0/NT5/EN -US/mssecure.cab. **


 ** File was successfully downloaded. **


 ** Attempting to load C: \tools\security\mssecure.xml. **

Using XML data version = 1.0.1.145  Last modified on 9/11/2001.

Scanning ENEADAS
.................
Done scanning ENEADAS
---------------------------
ENEADAS
---------------------------


        WINDOWS 2000 SP2

                WARNING         MS01 -022       Q296441
                Patch NOT Found MS01 -025       Q2961 85
                Patch NOT Found MS01 -031       Q299553
                Patch NOT Found MS01 -037       Q302755
                Patch NOT Found MS01 -041       Q298012
                Patch NOT Found MS01 -046       Q252795

        Internet Explorer 5. 01 SP2

                Patch NOT Found MS01 -027       Q295106

C:\tools\security>
```

There are a number of hot-fixes missing, hence the audit failure in the checklist.

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

2.4 Mail Virus

Virus defences Checklist	Pass	Fail
Date: 22/08/2001 Auditor: FMC		
5. End users educated regarding e-mail virus risks (subjective) When asked about e-mail virus outbreaks, SA1 mentioned several (more that 10) during the past 12 months. There is no official training program or mandatory reading material regarding this issue.	☐	☒
6. Clear and comprehensive security policy exists regarding e-mail viruses *Policy should contain types of files that should be allowed through the e-mail system, either inbound or outbound. It should also explicitly list the actions users are prohibited to do regarding e-mail.* **Failure in this test precludes tests 7 to 8.**	☐	☒
7. End users comply with security policy (subjective) _____ _____	☐	☐
8. Technology in place complies and enforces existing security policy	☐	☐
9. End users should not read e-mail with local Administrator or Domain Administrator rights (subjective) Most users have administrator rights over their machines. All the support workers SA1 to SA11 had domain administrator rights.	☐	☒
10. Anti-viral filter exists at the Firewall *List any gateway mail virus filtering software. For each one, a separate "anti-virus software checklist (gateway)" should be presented:* Undisclosed anti-virus software	☒	☐
11. Anti-viral software exists at the Exchange mail server *List any Exchange mailboxes virus filtering software. For each one, a separate "anti-virus software checklist (mail server)" should be presented:* _____; _____; _____	☐	☒
12. Anti-viral software exists at the desktop *List any desktop mail virus protection software. For each one, a separate "anti-virus software checklist (workstation)" should be presented:* McAfee VirusScan v4.5.0	☒	☐

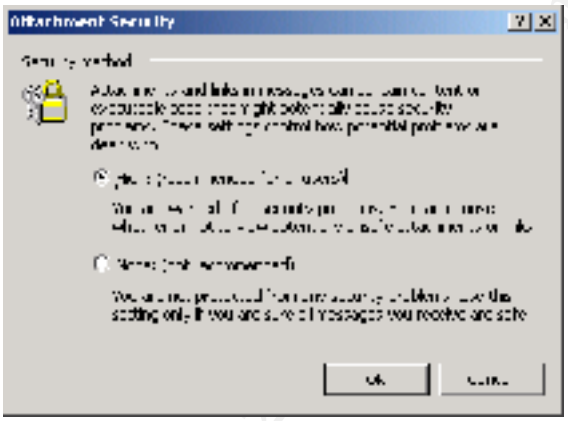
Anti-virus measures for Workstations	Pass	Fail
# systems tested/ # total: 1/400 Date: 22/08/2001 Auditor: FMC		
13. Outlook attachment security set to "high" *This setting prevents the opening of attachments without prior notice.*	☒	☐

© SANS Institute 2000 - 2002, Author retains full rights.

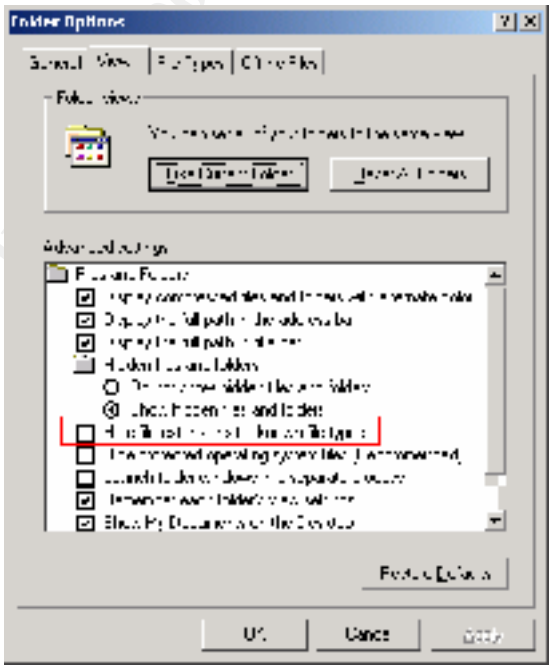
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Anti-virus measures for Workstations			Pass	Fail
# systems tested/ # total: 1/400	**Date: 22/08/2001**	**Auditor: FMC**		
14. File extensions are visible *By default windows is configured not to show file extensions on known file types. This allows an attacker to disguise a Trojan file under a different apparent extension. For instance, "test.txt.vbs" would be showed as "test.txt".*			☒	☐
15. File extensions for active content types mapped to harmless operation *File extensions "vbs", "vbe", "js", "jse", "wsf" and "wsh" should be mapped in the registry to "edit" instead of "execute".*			☐	☒

Outlook attachments:

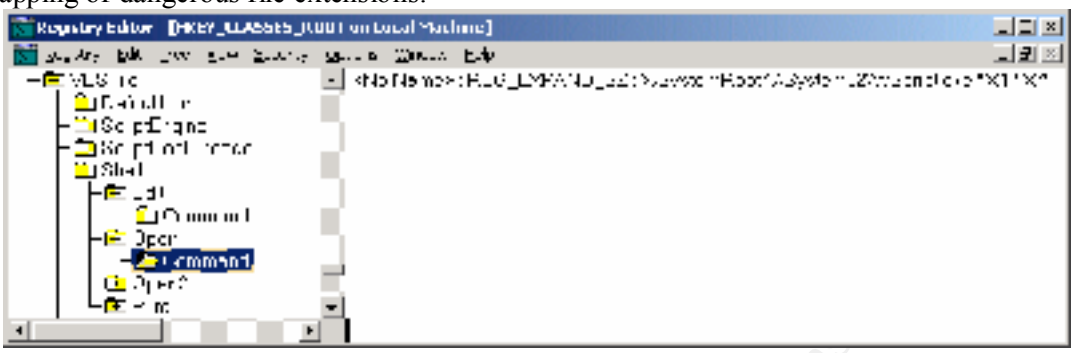


File extensions are visible:



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Mapping of dangerous file extensions:



It is recommended here to either replace "Wscript.exe" with "notepad.exe" or add the following keys to the registry [17]:

```
[HKEY_CLASSES_ROOT \VBSFile \Shell]
@="Edit"
[HKEY_CLASSES_ROOT \VBEFile \Shell]
@="Edit"
[HKEY_CLASSES_ROOT \JSFile \Shell]
@="Edit"
[HKEY_CLASSES_ROOT \JSEFile \Shell]
@="Edit"
[HKEY_CLASSES_ROOT \WSFFile \Shell]
@="Edit"
[HKEY_CLASSES_ROOT \WSHFile \Shell]
@="Edit"
```

The following tests were applied to the unkn own firewall anti-virus protection system:

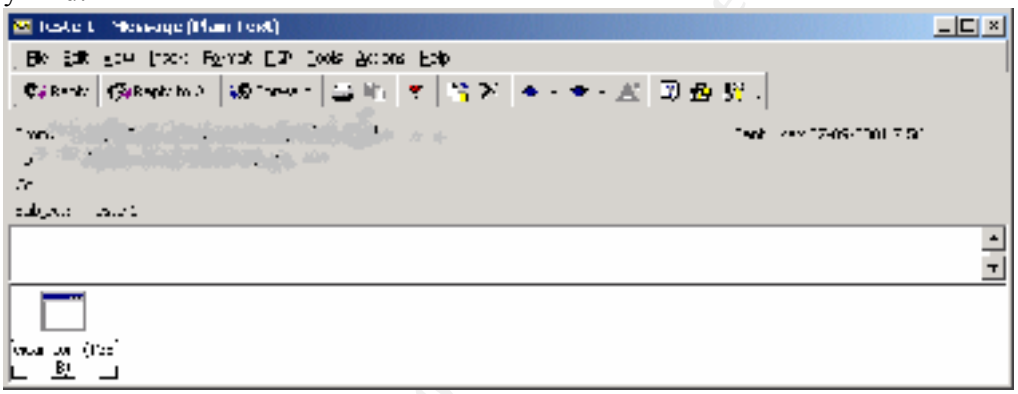
Anti-Virus Software Checklist (Gateway)	Pass	Fail
Product/version: Undisclosed **Date: 7/09/2001** **Auditor: FMC**		
16. EICAR signature detected *Send an e-mail containing the text "X5O!P%@AP[4 \PZX54(P^)7CC)7}$EICAR -STANDARD-ANTIVIRUS-TEST-FILE!$H+H*". Anti-viral software should accuse the presence of the "EICAR test file virus" [18].* **Failure in this test precludes tests 17 to 19.**	☐	☒
17. Infected e-mail was rejected	☐	☒
18. Sender receives virus notification *It is not considered mandatory that notifications be sent, although it is a good practice. A "Fail" in this item will not result in the failure of the audit.*	☐	☒
19. Recipient receives virus notification *It is not considered mandatory that notifications be sent, although it is a good practice. A "Fail" in this item will not result in the failure of the audit.*	☐	☒

[17] Quoted from Morris, Ev an. "Update to a Virus Survival Checklist"
[18] For more information: http://www.eicar.com/anti_virus_test_file.htm

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Anti-Virus Software Checklist (Gateway)	Pass	Fail
Product/version: Undisclosed **Date: 7/09/2001** **Auditor: FMC**		
20. Viral database is up -to-date *If possible, check the date of the last signature update against the latest update file available at the vendor site. If not, check if the last update occurred during the last month.*	☐	☒
21. Updates to viral database are automatic *"Pass" here means there is an automatic procedure to update the viral database on a regular basis that is compatible with the anti-virus security policy in place. This automatic update can be a feature of the anti-virus software or any other procedure that does not depend on human intervention.*	☐	☒

Microsoft Outlook received the mail with the EICAR signature with no indication of filtering of any kind:



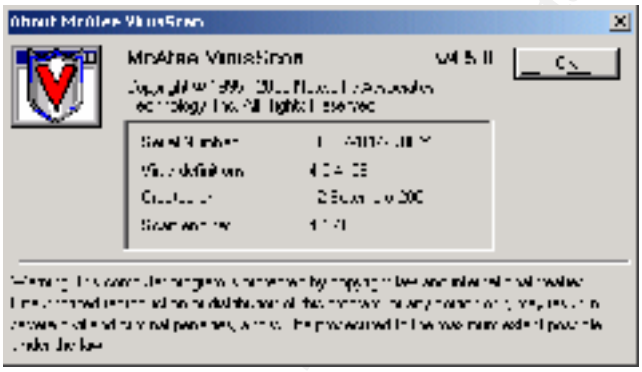
Anti-Virus Software Checklist (Workstation)	Pass	Fail
Product/version: McAfee VirusScan v4.5.0 **Date: 12/9/2001** **Auditor: FMC**		
22. EICAR signature detected *Send an e-mail containing the text "X5O!P%@A P[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*". Anti-viral software should accuse the presence of the "EICAR test file virus"* [19]. **Failure in this test precludes tests 28 to 29.**	☒	☐
23. Infected e-mail fails to open	☒	☐
24. No option exist to open infected e-mail, despite of virus warning	☐	☒
25. Viral database is up -to-date *If possible, check the date of the last signature update against the latest update file available at the vendor site. If not, check if the last update occurred during the last month.*	☒	☐
26. Updates to viral database are automatic *"Pass" here means there is an automatic procedure to update the viral database on a regular basis that is compatible with the anti-virus security policy in place. This automatic update can be a feature of the anti-virus software or any other procedure that does not depend on human intervention.*	☒	☐

[19] For more information: http://www.eicar.com/anti_virus_test_file.htm

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Virus detection screen shot:

Virus database:



Automatic updates:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

2.5 Information Confidentiality and In tegrity

2.5.1 Physical Security

Physical Security Checklist	Pass	Fail
Location: Company Data Centre **Date: 23/08/2001** **Auditor: FMC**		
27. Security perimeter is clearly defined (subjective) Data Centre is physically separated from the rest of the IT area, in a differe nt room.	☒	☐
28. Perimeter is physically sound (subjective) Although the walls are not very strong, the security of the room is consistent with that of the rest of the company.	☒	☐
29. There is a manned reception area responsible for access control and log	☐	☒

2.5.2 Outlook PST File Permissions

PST File Protection Checklist **# systems tested/ # total: 1/400** **Date: 24/08/2001** **Auditor: FMC**	Pass	Fail
30. File level permissions are configured to protect the file from unauthorized copy *Windows 2000 or NT only.*	☐	☒
31. File is accessible through the network	☐	☒
32. File access is logged as a security event	☐	☒
33. PST file is password protected	☒	☐

2.5.3 Administrator Rights

Administrator Checklist	Pass	Fail
Date: 24/08/2001 **Auditor: FMC**		
34. No user shares domain admin and exchange adm in rights	☐	☒
35. Minimal privilege principle is implemented (subjective) 11 users (SA1 to SA11) had both domain admin and Exchange admin privileges.	☐	☒
36. Default system accounts are not used	☐	☒

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

2.5.4 *Alternate Recipients*

Alternate Recipient Checklist	Pass	Fail
Date: 24/08/2001 **Auditor: FMC**		
37. Clear policy exists regarding alternate recipients *Policy should state in which cases alternate recipients are allowed, and how they should be documented.*	☐	☒
38. No illegitimate alternate recipient found	☒	☐

2.5.5 *Access to User's Mailbox*

Whenever a user accesses a mailbox that he does not own, an event with an ID of 1016 is generated in Microsoft Exchange's application log. This event can be used to detect unauthorized access to a user's mailbox. The following checklist checks this:

Access to a different mailbox Checklist	Pass	Fail
Date: 24/08/2001 **Auditor: FMC**		
46. Clear policy exists regarding access to a user's mailbox by an Exchange admin *Policy should state in which cases user's mailboxes can be accessed by Exchange administrators*	☒	☐
47. No indication of violation of policy found	☐	☒

The following access was found:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

3 Evaluation of the Audit

Mainly due to the very specific requirements of my customer, this audit did not cover some areas that are very important, like:

- Network interface security (POP3, SMTP, RPC, etc.);
- Exchange configuration issues;
- Vulnerability to natural disasters;
- Backup plans.

However, it was sufficient to draw the following conclusions:

1. Mail Virus protection is inefficient;
2. Administrative procedures are poorly documented and implemented;
3. Mail confidentiality and integrity is at risk, mostly from an internal threat.

The actual audit report that was delivered to my customer included detailed recommendations for each of the audit failures. A new audit was scheduled in three months time.

The major difficulty I found when designing and implementing this audit methodology was how to audit the workstations, when their number is significant. Although in this case the notebook I was issued had some security problems (most of all about hot-fixes that were not applied), the conclusions about this particular machine don't naturally apply to the rest of the workstations.

In conclusion, the audit methodology developed in this document did measure up well to a very specific Real World audit assignment, resulting in an audit report which brings value to the customer, clearly indicating the areas that need improvement in his e-mail infrastructure.

4 Directions for Future Work

Given the risk analysis done in chapter 3, it is clear to me that the checklist developed in this document does not cover every possible e-mail security threat. The future work on this document will probably be focused on:

a) Implementing new checklists that cover e-mail security risks not covered by the current set (Unsolicited Commercial E-Mail, Network security, etc.);

b) Use practical feedback from Real World audits to refine existing checklists;

c) Evolve to new areas like PKI based e-mail.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

References

1. Schneier, Bruce. "Secrets and Lies: digital security in a networked world". John Wiley & Sons, Inc, 2000.

2. British Standards Institute. "BS 7799 -1:1999 Information security management – Part 1: Code of practice for information security management". British Standards Institute, February 2000.

3. Morris, Evan. "A Viral Survival Checklist". May 2000. http://www.exchangeadmin.com/Articles/Index.cfm?ArticleID=8513 (11/9/2001)

4. Morris, Evan. "Update to A Viral Survival Checklist". June 2000. http://www.exchangeadmin.com/Articles/Index.cfm?ArticleID=8778 (11/9/2001)

5. The SANS Institute. "Windows NT Security step by step – A survival guide for Windows NT security". Version 3.03. February 2001.

6. Microsoft. "XCLN: Improving the Security of PST Files". December 10, 2000. http://support.microsoft.com/directory/article.asp?ID=KB;EN-US;Q143241 (17/9/2001)

© SANS Institute 2000 - 2002 author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.