**Assignment: Auditing Enterprise Email Service**

Auditing Networks, Perimeters, and Systems

GSNA Practical Assignment Version 1.0 Current as of May 22, 2001

Submitted by: **Tapan Meshram** 15th October, 2001

## Contents Page

**Assignment 1: Auditing Enterprise Email Service**
Tapan Meshram
14th September, 2001

## Section A: Introduction to current state of audit practice

Email has become the most popular means of transferring information. Almost all business es are using email for information exchange between employees. A lot of companies have deployed exclusive enterprise email service (Example: tapan@mydomain.com) for communications with remote employees, business partners, etc. However, any communication over the Internet without sufficient security measures is at risk. Let us look at some of the risks associated with email service infrastructure.

1. The greatest threat noticed with email is the viruses it spreads as attachments. A vivid example of the chaos viruses coming through email can cause is given in the following article: **SirCam clogs mailboxes, spreads secrets** . After reading this it is evident, how email security breach can cause a comp romise of integrity, availability & confidentiality of information.
2. Email is mostly sent as plain text. This is highly susceptible to being intercepted on the way and being modified.
3. A great danger to network integrity is 'spam' mail. This basically refer s to malicious attempt to cause 'denial of service' by sending bulk mails to a particular location thereby choking the bandwidth and effecting the normal functioning of the email server. The server is unable to handle the load and end users suffer since im portant mails may be delayed or blocked.
4. Unauthorized people can use your mail servers for third party relay, and multiply the Spam problem. This can have a legal implication for the organization, since it has to take the responsibility for its servers.

Email is notoriously insecure, it can cause both personal and organization embarrassment. Enterprise email service can put the companies information systems at risk. Depending on the nature of business, the impact information loss may vary. And without prop er security measures, it is not advisable to transfer sensitive information using email, or to put too much trust on information received via email.

How do we evaluate whether our enterprise email service is exposed to these risks? Do your organization have security measures against these risks?

The process of audit can give the answers to these questions. It can help us to objectively evaluate the current state of practice & gives us direction to focus our improvement efforts.

During the research on this subject the best (freely available) practice for email security was found at http://www.dsd.gov.au/infosec/acsi33/HB10.html . After the research I categorized the major issues with email securit y as follows:

1. Usage of Encrypted Transactions and Public Key Infrastructure for email exchange
2. Protection the integrity of the email infrastructure
3. Maintaining the confidentiality of emails.
4. Securing the email server
5. Auditing of email server to ensure logg ing
6. Securing the email client

**Shortcomings in the current state of practice are**

1. Only one freely available comprehensive document, which explains the risks with email service.
2. There is no freely available document on how to carry out audit of enterprise e mail service?

3. Lack of an evaluation scheme, which can help one to arrive at a numerical score.
4. A comparison of scores across the companies can help in sharing the best practices. With the existing resources on this subject, two different enterprise email s ervice cannot be compared.
5. Lack of emphasis on email service user's training /awareness in these documents. Section E explains few more issues I discovered after conducting the audit.

- **Audit Scope**

This document is prepared specifically for auditing of a c ompanies internal mail servers. Example: If you are working with Sans.org then the mail service of people@sans.org will be audited. The auditing of email security risks with web -mail (example: people@yahoo.com), used by employees through browser is out of the scope. Remember this when you go through this document.

**What is the objective of audit?**

The audit will address email service availability, confidentiality, integrity and n on-repudiation. An explanation of the objectives [1] is as follows:

1.To protect the confidentiality of identified information by preventing leakage of information to those without the need -to-know.

2.To ensure an appropriate level of sender authentication an d non-repudiation.

3.To ensure an appropriate level of email integrity.

4.To protect the availability of the system by controlling access to critical system functions and preventing malicious code based denial of service attacks.

[1] http://www.dsd.gov.au/infosec/acsi33/HB11.html

**Who is subjected to the audit?**

The following people will be directly subjected to the audit:

1. The information security officer (ISO)
2. The mail server administrator
3. The network administrator
4. The desktop administrator
5. The email user

- **Audited Infrastructure**
    1. Email server: Qmail version 1.03 running on a Linux Red Hat 6.2
    2. Email client: Microsoft Outlook Express version 5.0
    3. Network: Local area network 100 Mbps LAN, machine s are connected with hub.

**Section B: Audit Strategy & Scoring Scheme**

Audit involves asking questions to validate the availability of security measures to protect from various security risks. One risk may not have same impact on the organization's information systems as the other. It is the responsibility of the auditor to arrive at the checklist, which consists of prioritized risk evaluation questions. To put this to practice each risk area has been assigned a different weight age. You are free to assign y our own weight age for the risk areas. In my checklist I have assigned higher weight age to risk areas pertaining to basic information security practices. Example: physical security is given higher weight age than the secure POP3 implementation. I took a simple approach for preparing the audit checklist & scoring strategy. I addressed each risk area with the basic Who?, Why? & What? questions. This approach also helped in arriving at improvement focus areas. A numerical score of 20, 30 & 50 has been assig ned respectively to Who, Why & What questions. Guidelines for Who, Why & What come in section A, B & C of each clause respectively. Let us examine few basics of this approach.

**Who?**

The question "Who?" will identify the person responsible for taking action related to a issue. It is the most important concern, lack of which will lead to a situation the following situation: "everybody thought somebody will do it, and nobody did it".

The questions in "Who" section are the binary ("Ok or not Ok") questions. Ful l marks must be given if there is somebody assigned to tackle the issue or else give zero marks. The titles and designations may vary across organizations but as long there is somebody to address the risk, its fine.

**Why?**

The question "Why?" will help us fi nd out if the responsible person has enough knowledge and training to address the risk. Poor understanding of the subject would mean the responsible person will not be able to trouble -shoot in case of an attack. It implies that the organization needs to gi ve better technical training to its personnel.

Each "Why" question tests the technical knowledge of the person responsible for tackling the risk. Therefore each "Why" section(i.e. section B) comes with a little brief for the auditor. Though the auditor has the flexibility to assign anything between 0 -30 in the section. But if the person audited is aware of the information in section B, then you can give full marks.

**What?**

The question "What?" will help us validate if the security measures implemented are sufficient to address the issue or not. This question is the superset of 'How' the solution will be implemented? 'When' it is implemented/reviewed, and 'Where' is it implemented? Any shortcomings in "What?" would mean better procedure/solution is required.

The questions in the "What" section are mixed. For the objective questions, if the answer is Ok one get full marks or else 0. Some of the questions require a descriptive check with command lines & user interface. Command lines and tools user interface snapshots for verification of the implemented solutions are given, *wherever required in italics*, after the question.

**1. Physical security**
1.A. The information security officer should be responsible for the physical security and access control of the mail server . (20)
1.B. The mail server is the heart of the enterprise email, it receives and delivers email messages. A lot of information resides on the mail server. Physical access to the machine running the mail server should be restricted to authorized users. A simple manipulation like a simple ".forward" can leak confidential information in unauthorized hands. It is important to ensure mail server safety from incidents like fire hazards, etc. (30)
1.C.1. Is the mail server kept at a secure location not accessible by visitors/outsiders? (20)
1.C.2. Is it locked in a server room, accessible only to the system administrator and authorized persons through electronic lock/swipe card access system? (10)
1.C.3. Is there protection from fire hazards using a fire alarm system and smoke detector? Is there a fire extinguisher nearby to overcome such a disaster? (10)
1.C.4. Is there a closed circuit camera to watch over the activities on and around the mail server? (10)

**2. Network security**
2.A. The information security office r & network administrator are responsible. (20)
2.B. A mail server requires being on the Internet to send and receive mails. If not properly configured, this causes a potentially dangerous situation, where an intruder may gain access to the server and subsequently to the organization's entire network. Depending on the extent of the attack, this may compromise the confidentiality, integrity and availability of the network, the servers and the end users. Thus, it should be kept in the DMZ (De -militarized zone). The DMZ should also be protected from the Internet by a firewall and an intrusion detection system. (30)
2.C.1. Is the mail server kept in the DMZ of the organization's network? (10)
Verify the network properties with the following command:
*ifconfig*
2.C.2. Is there a firewall/Intrusion detection system to protect the mail server? (5)
Verify the rules on the mail server to see if it has ipchains configured for access control and firewall functionality:
*ipchains –n -L*
Verify if intrusion detection system (e.g. Snort) is running on the machine, with the following command:
*ps –auwx | grep snort*
2.C.3. Is the firewall configured to allow only SMTP/POP3/IMAP traffic to the mail server from other networks? (10)
Verify with the ipchains rules again for rules specific to mail server (192.168.30.2):
*ipchains –L | grep 192.168.0.2*
2.C.4. Is the intrusion detection system configured to catch any suspicious traffic to the mail server? (15)
Verify with an editor like vi, if the rules file (e.g. snort.rules) of the intrusion detection system (e.g. Snort) has specific rules for analyzing traffic for the mail server (192.168.30.2)
*vi snort.rules*

*/192.168.0.2*

2.C.5. Does the information security officer do a daily review of firewall and IDS for malicious activity? (10)
Hint: Verify the written review records.

**3. Service control**

3.A. The information security officer & mail server administrator are responsible. (20)

3.B. Network services are the gateway for communicating on the network. However running services like finger, named, httpd, when not required, is an open invitation to exploits. It is easier to administer mail server for mail receipt/delivery related services. Therefore, if you can afford, the mail server machine should be dedicated for the purpose of mail handling alone. All other services (i.e. network ports) should be closed and monitored. (30)

3.C.1. Is the mail server dedicated for the purpose of mail handling? (10)
Verify that only the mail server is running:
*ps –auxw*

3.C.2. Did the mail server go through an Operating system hardening process before activation? (10)
Verify if there is any evidence for hardening, e.g. the document used for hardening of the machine.

3.C.3. Is it only running the required & necessary services/daemons? (15)
*lsof –i +M*

3.C.4. Are the ports/services regularly monitored for unauthorized activation/closure of ports? (15)
Verify if nmap and ndiff are installed
*nmap --help*
*ndiff --help*
Verify availability of previously done scans.

**4. Operating system access control**

4.A. The information security officer & mail server administrator are responsible. (20)

4.B. Access to the mail server operating system should be controlled. If permissions are not applied properly then not only will a user be able to view or modify other users' confidential information (mails information) but also manipulate the configuration of the mail server application. An intruder can gain access to the operating system by exploiting vulnerability in mail server application. Thus for protection of the mail server, it should be set to run as a user with minimal file system or operating system privileges. (30)

4.C.1. Did the mail server administrator use Linux -conf to create special (mail only user) POP accounts for mail users? (10)

4.C.2. Does the /etc/passwd file confirm that the mail users do not have extra privileges? (10)
*ls –l /etc/passwd*
*ls –l /etc/shadow*
*cat /etc/passwd*

4.C.3. Are the directory permissions limited to the users incoming and outgoing mail archive? (10)
*ls –l /var/spool/mail**

4.C.4. Is the telnet, ftp, and shell access limited to the administrator's IP address? (10)
Verify with the following if TCP wrappers is configured for access control:
*more /etc/hosts.deny*
*more /etc/hosts.allow*
Else check for the ipchains rule set with if access control is implemented at IP level:

*ipchains –n -l*
4.C.5. Does the administrator periodically check for any change in the user privileges? (10)

**5. Audit of logs**
5.A. The information security officer & mail server administrator should be responsible. (20)
5.B. Audit logs serve a dual purpose of helping to maintain mail server security as well as to keep an account of usage. Mail server auditing may be enabled in the same way as enabling operating system auditing. Effectively utilizing these audit logs is not an easy task since it involves constant maintenance and monitoring by concerned people.
The auditing of a mail server can result in significant benefits to the organization, which include [2]:

- Logs that can identify the source of hacking attempts or denial of service a ttacks.
- Logs that can pinpoint problems with your mail server configuration.
- Usage statistics that can identify when an upgrade of network bandwidth is likely to be required.

A major problem commonly faced by mail servers is 'spam' mail or bulk mail that causes 'denial of service'. This happens when a very large number of mails are targeted towards the mail server. In such a situation if auditing is enabled then the file system may fill up so quickly and damage the system even before the attack is detecte d. To prevent this, logging should be redirected to a separate disk with automatic log rotation.
[2] http://www.dsd.gov.au/infosec/acsi33/HB11.html (30)

5.C.1. Is the auditing application instal led & is the auditing software configured to capture all security related messages? (10)
*ps –aux |grep syslogd*
*cat /etc/syslog.conf*
5.C.2. Is the audit information protected by access controls so that it cannot be easily read or overwritten? (10)
*ls –l /var/log/**
5.C.3. Is the auditing software configured to send logs to offline storage, or removed from the file system when no longer required? (10)
*cat /etc/syslog.conf*
5.C.4. Is there an application installed for log analysis and display? (10)
*find / -name isoqlog -print*
5.C.5. Is the file system observed to ensure that disk space does not fill, and therefore contribute to a denial of service situation? (10)
*df –h*
*du -ch /var/spool/mail/**

**6. Hot fixes & security patches**
6.A. The mail server administra tor is responsible. (20)
6.B. Everyday new vulnerabilities/exploits are discovered in applications. In response to these vulnerabilities application vendors take out patches and hot fixes to overcome the exploit. It is important to update the mailing appli cations with these patches before a malicious user exploits the vulnerability to gain unauthorized access. Often, security patches crash the application and operating system. Therefore they should be tested on a test machine before applying to the producti on server. (30)
6.C.1. Is the mail server application of the latest version? (10)
6.C.2. Does the mail server administrator keep track of the latest vulnerability and exploits in the mail server application through the Internet? (10)
6.C.3. Does the mail s erver application have the latest security patch/hot fix installed? (15)
6.C.4. Is the patch/hot fix tested on the testing machine before being applied to the production mail server? (15)

**7. Server virus scanning**
7.A. The Information security officer & ma il server administrator are responsible. (20)
7.B. The problem of viruses in the cyber world has become even more severe than the real world viruses. The cyber world releases more “In the wild” viruses than ever now. In fact, it is recognized as the greate st risk to the organizations information system resources. Malicious users can introduce viruses, Trojan horses, or VBS script in the organization via email attachment and gain unauthorized access to the machine, damage the server & network. They can also use the same Trojans to capture confidential information from the network or server. Antivirus implementation can be at both the client and server side. The next section will discuss about client side. The anti virus protection should be applied at the mai l server itself. This would ensure that viruses don’t percolate the network and reach the desktop of individual users. Please refer to www.amavis.org/amavis.html for details on how to install and use mail se rver virus scanners. (30)
7.C.1. Is the mail administrator using any mail server virus scanners? (10)
7.C.2. Are the virus scanner, mail transfer agent, mime handlers, decompressors and file type recognizers installed in -order to use the mail server virus scanner? (20)
7.C.3. Does the mail administrator regularly update the virus signatures of the anti virus tool on the server? (20)

**8. Mail client settings**

8.A. The desktop administrator is responsible. (20)

8.B. One of the major client-side security risks come in the form of innocent-looking HTML messages and messages containing applets and Active -X controls. Besides this, any piece of executable code or even a software that has embedded code, that is received as an attachment via email, may contain damagin g code meant to harm the local system on which it is downloaded. The damage caused by such code can be severe. Example: It can help the malicious user to access confidential information. The code can be a virus, which may percolate in the complete network and in some cases even bring the servers down. Besides configuring the mail client to reject executables and malicious code it is also important to train the individual mail users about the dangers with opening attachments from not trusted senders. (30)

8.C.1. Is the email client of the latest version updated with the latest security patches? (10)

8.C.2. Is the anti virus on the user's individual machine configured to check for viruses in the email attachments? (20)

8.C.3. Is the anti virus updated with the latest signatures? (20)

**9. Secure POP3 and IMAP**

9.A. The information security officer and desktop administrator are responsible. (20)

9.B. The use of secure POP3 and IMAP is required for users who access a lot of business critical information through the ir emails. It is even more essential for roaming users, who access their email from more vulnerable environments like hotel LAN, etc. One of the freely available servers for this purpose is Qpopper. Therefore to avoid the danger of sending clear text passwords over the network use Qpopper type packages. Remember to install the latest package though as earlier versions were susceptible to buffer overflow problems. With a buffer overflow vulnerability gaining root access becomes a trivial task. (30)

9.C.1. Is there an application installed for secure POP3 and IMAP? (10)

*cat /etc/inetd.conf |grep imap*

*cat /etc/inetd.conf | grep qpopper*

9.C.2. Is the application of the latest version and not vulnerable to known exploits? (10)

*telnet 192.168.0.2 110*

*telnet 192.168.0.2 143*

9.C.3. Is APOP, Kerberose & TLS/SSL configured with this application at compile time? (10)

Example of compile time configuration for APOP is as following:

*./configure –enable-apop=/etc/pop.auth*

9.C.4. Is the client side configuration for secure POP3 correctly done? (10)

9.C.5. Are the individual users using secure POP3 & IMAP service? (10)

**10. Mail filtering**

10.A. Information security & mail administrator officer should be responsible. (20)

10.B. Incoming mail needs to be scanned to detect and prevent 'Spam' or bulk mails from resulting in a 'denial of service' since this will effect the productivity of the mail server and end users. Moreover, incoming mails may contain objectionable contents such as pornography and viruses, which need to be pre vented as it may compromise the security and may even result in legal complications for the organization.

Outgoing mail needs to be scanned to prevent leakage of sensitive information such as trade secrets, financial and strategic data, etc. This could be accomplished by configuring the mail server to lexically scan the contents of outgoing emails.

10.C.1. Is the mail server configured to block third party relay attempts from external domains? (10*)*
*vi /etc/tcp.smtp*
10.C.2. Is there a message filtering appli cation installed? (10)
*whereis procmail*
10.C.3. Is the application of the latest version & patched up for known exploits? (10)
*procmail -v*
10.C.4. Has the administrator created the required configuration files for filtering? (10)
*whereis .procmailrc*
10.C.5. Does the application send the defaulters mail to the administrator? (10)
*cat /var/qmail/alias/.qmail -mailer-daemon*

**11. Encrypted mail content and digital signature**
11.A. The desktop administrator & mail server administrator are responsible. (20)
11.B. Mails are sent and received over the Internet. They travel through several routers and servers to reach their destination. During this time it is possible to intercept them and read or modify the contents. It may not be possible to prevent the interception but the contents of the mail can be protected, by sending it as encrypted data instead of plain text. There are several options available to enable encryption of mail message. Two widely accepted mechanisms are PGP and S/MIME. They both provide the same features, i.e. encryption of messages, digital signatures and key certification. Both systems ensure information integrity, confidentiality and non-repudiation. (30)
PGP (Pretty Good Privacy) has long history as a freeware product, and has therefore seen extensive use worldwide. Refer http://www.pgpi.org/doc/pgpintro/ for details.
S/MIME is a set of standards developed by RSA Laboratories. S/MIME is based on X.509 key certification standard, which is the same standard used for SSL certificates, which help to secure communication between browsers and web servers. The X.509 standard has been designed for a centralized certification, therefore it is easy to implement within an organization. However, it become s complicated to extend the same over several organizations and may require certificate authorities to come into the picture. Refer http://www.rsasecurity.com/standards/smime/ for details.
11.C.1. Is the application, for encrypting mail content, installed on the user desktop? (10)
11.C.2. Is the application configured to send encrypted email messages? (10)
11.C.3. Does the email user encrypt his message before sending? (10)
11.C.4. Is the user's public key available on public servers? (10)
11.C.5. Does the organization have an internal server for maintaining the keys? (10)

**12. User awareness**
12.A. The Information security officer should be responsible for this. (20)
12.B. Success of security poli cy depends on how closely they are followed. Awareness amongst users regarding issues pertaining to email security plays a very significant role in the success. Few examples to illustrate the failure are:

1. Unless users are informed of risk associated with o pening executable attachments from ambiguous source, all other security measures will fail.
2. Even if encryption is being used in sending and receiving mail messages, these are often stored as plain text in the user's 'Inbox' or 'Sent Items' folders. If des ktop screen is not locked while leaving the desk these folders become accessible to all passer by.

3. The user should be careful about attachments, coming with the mails he checks through the browsers. The associated files should be scanned for virus before downloading.
4. Another commonly followed practice while sending mails is to 'cc' (carbon copy) it to several other concerned people to make them aware of the communication. The recipient in turn may unintentionally reply to all those included in the list. This may compromise the confidentiality of the data since it is sent to a wider distribution list than required. Thus, one must ensure that the mail is being sent to only the relevant people.

The above examples explain how lack of user awareness can lead to compromise of email security. As part of the solution a session on risks associated with email communication can be included in the "new" employees induction process. Periodically updating the users through mail and informal session can be good & effective solution. (30)

12.C.1. Is the end user aware of the level of protection enabled at the client side and how to use it? (10)

12.C.2. Does the user check, files downloaded using web browser (i.e. web -mail like yahoo, hotmail, etc.), for virus? (10)

12.C.3. Does the email user scan attachments with an updated anti virus program before downloading it to the local machine? (10)

12.C.4. Does the end user lock his screen when he leaves his desk? (10)

12.C.5. Is the user aware of the "cascading carbon copy" risk? (10)

- **Sample checklist**

| *S.no* | *Action points* | *Total weight age=10* | *A. Who (20)* | *B. Why (30)* | *C.1. (C=50)* | *C.2.* | *C.3.* | *C.4.* | *C.5.* | *Cumulative score* |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Physical security | 0.9 | | | | | | | | |
| 2 | Network Security | 0.9 | | | | | | | | |
| 3 | Service control | 0.8 | | | | | | | | |
| 4 | Operating system access control | 0.85 | | | | | | | | |
| 5 | Auditing of logs | 0.8 | | | | | | | | |
| 6 | Hot fixes & security patches | 0.85 | | | | | | | | |
| 7 | Sever virus scanning | 0.9 | | | | | | | | |
| 8 | Mail client settings | 0.85 | | | | | | | | |
| 9 | Secure POP3 and IMAP | 0.75 | | | | | | | | |
| 10 | Mail filtering | 0.75 | | | | | | | | |
| 11 | Encryption & digital signature | 0.7 | | | | | | | | |
| 12 | User awareness | 0.95 | | | | | | | | |
| | *Sub total of columns* | | | | | | | | | |
| | *Total Score* | | | | | | | | | |

**Assignment 2:Auditing Enterprise Email Service**
Tapan Meshram
14th September, 2001

**Section C: Results of the audit practical**

The audit was conducted on 10 th August 2001 on our production mail server.
This document consists of the filled checklist & th e results of descriptive questions, checked during the audit. The specific command lines are between ***** and their results follow immediately. Use it along with the auditing document. The answer to objective questions will be clear from the score. The ne xt section on audit evaluation describes the observations made during the audit.

*Note:*

Some of the results have been sanitized to safeguard confidential information.
# Implies no corresponding question for the section.

- **Checklist with score**

| *S.no* | *Action points* | *Total weightage=10* | *A.Who* | *B.Why* | *C.1(What)* | *C.2(What)* | *C.3(What)* | *C.4(What)* | *C.5(What)* | *Cumulative score* |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Physical security | 0.9 | 20 | 30 | 20 | 10 | 10 | 0 | # | 81 |
| 2 | Network Security | 0.9 | 0 | 15 | 0 | 0 | 0 | 0 | # | 13.5 |
| 3 | Service control | 0.8 | 0 | 15 | 0 | 0 | 0 | 0 | 0 | 12 |
| 4 | Operating system access control | 0.85 | 20 | 30 | 10 | 10 | 10 | 10 | 10 | 85 |
| 5 | Auditing of logs | 0.8 | 20 | 30 | 10 | 10 | 0 | 10 | 10 | 72 |
| 6 | Hot fixes & security patches | 0.85 | 20 | 30 | 10 | 10 | 15 | 0 | # | 72.25 |
| 7 | Sever virus scanning | 0.9 | 0 | 0 | 0 | 0 | 0 | # | # | 0 |
| 8 | Mail client settings | 0.85 | 20 | 30 | 10 | 20 | 20 | # | # | 85 |
| 9 | Secure POP3 and IMAP | 0.75 | 20 | 15 | 10 | 10 | 0 | 0 | 0 | 41.25 |
| 10 | Mail filtering | 0.75 | 0 | 15 | 10 | 10 | 10 | 0 | 0 | 33.75 |
| 11 | Encryption & digital signature | 0.7 | 20 | 30 | 10 | 10 | 10 | 10 | 0 | 63 |
| 12 | User awareness | 0.95 | 0 | 0 | 0 | 0 | 10 | 0 | 10 | 9.5 |
|  | *Sub total of columns* |  | 140 | 240 |  |  | 315 |  |  |  |
|  | *Total Score* |  |  |  |  |  |  |  |  | 568.25 |

- **Descriptive answers (command lines and snapshots)**

2.C.1 SCORE: 0/5
***************

```
ifconfig
****************
eth0     Link encap:Ethernet  HWaddr 00:01:02:57:2A:D7
       inet addr:192.168.0.2  Bcast:192 .168.0.255  Mask:255.255.255.0
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:70314 errors:0 dropped:0 overruns:0 frame:0
       TX packets:42032 errors:0 dropped:0 overruns:0 carrier:0
       collisions:1287 txqueu elen:100
       Interrupt:11 Base address:0xec00

eth1     Link encap:Ethernet  HWaddr 00:50:BA:B1:E9:62
       inet addr:12.10.198.138  Bcast:12.10.198.143  Mask:255.255.255.248
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:736956 errors:0 dropped:0 overruns:0 frame:0
       TX packets:45702 errors:0 dropped:0 overruns:0 carrier:0
       collisions:12 txqueuelen:100
       Interrupt:10 Base address:0xe880

lo      Link encap:Local Loopback
       inet addr:127.0.0.1  Mask:255.0.0.0
       UP LOOPBACK RUNNING  MTU:3924  Metric:1
       RX packets:9126 errors:0 dropped:0 overruns:0 frame:0
       TX packets:9126 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:0
```

REMARK: The mail server is in the same subnet as all other machines, and there is no DMZ (de-militarized zone)

2.C.2 SCORE: 0/5

```
****************
ipchains –L
****************
Chain input (policy ACCEPT):
Chain forward (policy ACCEPT):
Chain output (policy ACCEPT ):
****************
```

*ps –auwx | grep snort*

```
****************
```

REMARK :-  No Firewall and IDS Installed on the machine or in that network.

3. C.1 SCORE: 0/10

```
****************
Command ps  -auxw|more
****************
USER       PID %CPU %MEM   VSZ  RSS TTY        STAT START   TIME COMMAND
root         1  0.0  0.1  1120  124 ?         S    Aug14   0:04 init [3]
root         2  0.0  0.0     0    0 ?         SW   Aug14   0:00 [kflushd]
root         3  0.0  0.0     0    0 ?         SW   Aug14   0:00 [kupdate]
root          4  0.0  0.0     0    0 ?         SW   Aug14   0:00 [kpiod]
root         5  0.0  0.0     0    0 ?         SW   Aug14   0:00 [kswapd]
root         6  0.0  0.0     0    0 ?         SW<  Aug14   0:00
[mdrecoveryd]
bin        405  0.0  0.5  1212  344 ?         S      Aug14   0:00 portmap
```

```
root       420  0.0  0.0     0    0 ?        SW   Aug14   0:00 [lockd]
root       421  0.0  0.0     0    0 ?        SW   Aug14   0:00 [rpciod]
root       430  0.0  0.0  1156    0 ?        SW   Aug14   0:00 [rpc.statd]
root       444  0.0  0.0  1104    0 ?        SW   Aug14   0:00 [apmd]
root       511  0.0  0.2  1168  160 ?        S    Aug14   0:04 syslogd    -m 0
root       520  0.0  0.0  1448    0 ?        SW   Aug14   0:00 [klogd]
nobody     534  0.0  0.5  2316  344 ?        S    Aug 14   0:00 identd -e -o
nobody     537  0.0  0.5  2316  344 ?        S    Aug14   0:00 identd    -e -o
nobody     538  0.0  0.5  2316  344 ?        S    Aug14   0:00 identd    -e -o
nobody     540  0.0  0.5  2316  344 ?        S    Aug14   0:00 identd    -e -o
nobody     541  0.0  0.5  2316  344 ?        S    Aug14   0:00 identd    -e -o
daemon     552  0.0  0.4  1144  308 ?        S    Aug14   0:00
/usr/sbin/atd
root       566  0.0  0.1  1328  112 ?        S    Aug14   0:00 crond
root       580  0.0  0.3  1168  240 ?         S    Aug14   0:00 inetd
named      594  0.0  2.2  2752 1388 ?        S    Aug14   0:01 named    -u
named
root       631  0.0  0.5  1152  344 ?        S    Aug14   0:00 gpm    -t ps/2
root       645  0.0  3.4  6036 2148 ?        S    Aug14   0:01 httpd
nobody     659  0.0  3.4  6208 2160 ?        S    Aug14   0:00 httpd
nobody     660  0.0  3.4  6208 2160 ?        S    Aug14   0:00 httpd
nobody     661  0.0  3.4  6208 2160 ?        S    Aug14   0:00 httpd
nobody     662  0.0  3.4  6208 2160 ?        S    Aug 14   0:00 httpd
nobody     663  0.0  3.4  6208 2160 ?        S    Aug14   0:00 httpd
nobody     664  0.0  3.4  6208 2160 ?        S    Aug14   0:00 httpd
nobody     665  0.0  3.4  6208 2160 ?        S    Aug14   0:00 httpd
nobody     666  0.0  3.4  6208 21 60 ?        S    Aug14   0:00 httpd
root       667  0.0  2.8  3840 1804 ?        S    Aug14   0:00
/usr/sbin/nessusd -D
xfs        706  0.0  0.1  2060   68 ?        S    Aug14   0:00 xfs    -
droppriv -daemon -port -1
qmails     744  0.0  0.2  1140  148 ?         S    Aug14   0:06 qmail -send
qmaild     745  0.0  0.0  1208   60 ?        S    Aug14   0:00
/usr/local/bin/tcpserver  -R -x/etc/tcp.cdb  -c150 -u501 -g501 0 smtp /
qmaill     751  0.0  0.2  1112  188 ?        S    Aug14   0:00 splogger
qmail
root       75 2  0.0  0.1  1100   72 ?        S    Aug14   0:00 qmail  -lspawn
|preline procmail
qmailr     753  0.0  0.1  1100  100 ?        S    Aug14   0:00 qmail   -rspawn
qmailq     754  0.0  0.1  1092   92 ?        S    Aug14   0:00 qmail   -clean
root       775  0.0  0.0   1092    0 tty2     SW   Aug14   0:00 [mingetty]
root       776  0.0  0.0  1092    0 tty3     SW   Aug14   0:00 [mingetty]
root       777  0.0  0.0  1092    0 tty4     SW   Aug14   0:00 [mingetty]
root       778  0.0  0.0  1092    0 tty5     SW   Aug14     0:00 [mingetty]
nobody    1524  0.0  3.3  6132 2100 ?        S    Aug14   0:00 httpd
root      2843  0.0  0.6  1092  408 tty6     S    03:54   0:00
/sbin/mingetty tty6
qmailr    3111  0.0  0.7  1168  464 ?        S    04:35   0:00 qmail   -remote
Lotusinterwo rks.com alok@tegora.stpn.soft.net jfashae@Lo
qmailr    3114  0.0  0.7  1168  464 ?        S    04:35   0:00 qmail   -remote
lotusinterworks.com alok@tegora.stpn.soft.net jmustin@lo
qmailr    3115  0.0  0.7  1168  464 ?        S    04:35   0:01 qmail   -remote
lotusinterworks.com alok@tegora.stpn.soft.net sunilmamid
root      3179  0.0  1.6  2224 1036 tty1     S    04:37   0:00 login    --
root
root      3241  0.1  1.8  2672 1144 ?        S    05:13   0:00 ipop3d
root      3243  0.1  1.5  1700  948 tty1     S      05:13   0:00  -bash
root      3264  0.0  1.3  2508  824 tty1     R    05:14   0:00 ps    -auxw
root      3265  0.0  0.7  1288  480 tty1     S    05:14   0:00 more
```

REMARK: A lot of irrelevant and vulnerable services are running as daemons. Example : named (DNS server)

3. C.3 SCORE: 0/15

```
****************
lsof –i +M
****************
named      583 root   25u  IPv4    592      TCP 12.10.198.138:domain (LISTEN)
httpd      635 root   16u  IPv4    668      TCP tegora.stpn.soft.net:www (LISTEN)
nessusd    659 roo t   5u  IPv4   2839      TCP *:3001 (LISTEN)
tcpserver  738 root    3u  IPv4   2906      TCP *:smtp (LISTEN)
httpd    16663 root   16u  IPv4    668      TCP tegora.stpn.soft.net:www (LISTEN)
httpd    16949 root    3u  IPv4 102091      TCP tegora.st pn.soft.net:www -
>192.168.0.12:2822 (ESTABLISHED)
httpd    16949 root    4u  IPv4 102102      TCP 12.10.198.138:4519  -
>httpes6.msg.yahoo.com:www (SYN_SENT)
inetd      569 root    5u  IPv4    570      TCP *:pop3 (LISTEN)
inetd      569 root    6u  IPv4    571      TCP *:imap2 (LISTEN)
inetd      569 root    9u  IPv4    574      TCP *:linuxconf (LISTEN)
```

REMARK: The web server is also running on this machine. This machine does not require it so it is non-compliance

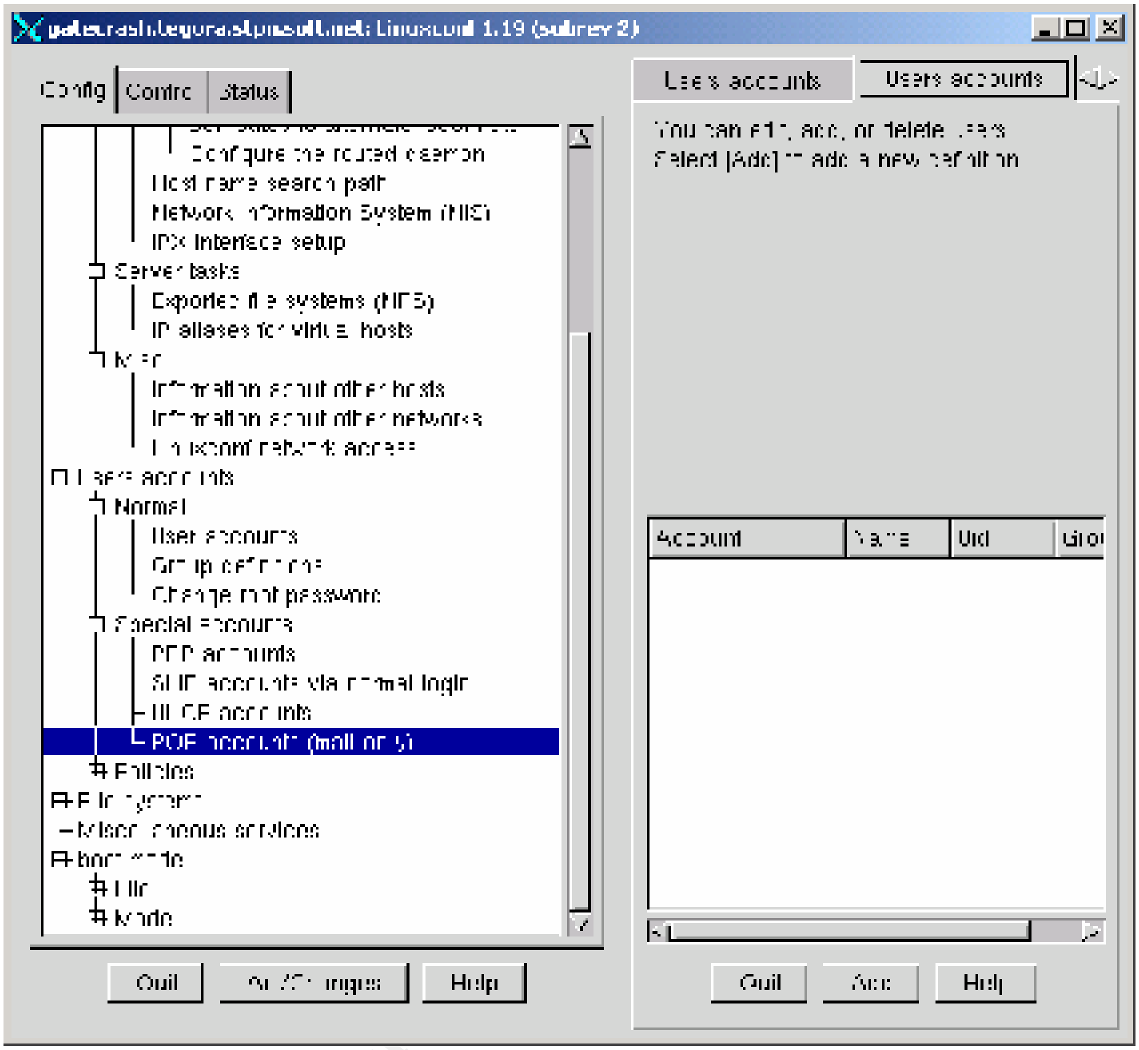
3. C.4 SCORE: 0/15

```
****************
Command nmap --help
****************
nmap V. 2.53 Usage: nmap [Scan Type(s)] [Options] <host or net list>
Some Common Scan Types ('*' options require root privileges)
  -sT TCP connect() port scan (default)
* -sS TCP SYN stealth port scan (best all -around TC P scan)
* -sU UDP port scan
  -sP ping scan (Find any reachable machines)
* -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)
  -sR/-I RPC/Identd scan (use with other scan types)
Some Common Options (none are required, most can be combined):
* -O Use TCP/IP fingerprinting to guess remote operating system
  -p <range> ports to scan.  Example range: '1 -1024,1080,6666,31337'
  -F Only scans ports listed in nmap -services
  -v Verbose. Its use is recommended.  Use twice for greater effect.
  -P0 Don't p ing hosts (needed to scan www.microsoft.com and others)
* -Ddecoy_host1,decoy2[,...] Hide scan using many decoys
  -T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing
policy
  -n/-R Never do DNS resolution/Always resolve [default: sometimes   resolve]
  -oN/-oM <logfile> Output normal/machine parsable scan logs to <logfile>
  -iL <inputfile> Get targets from file; Use '  -' for stdin
* -S <your_IP>/-e <devicename> Specify source address or network interface
  --interactive Go into interactive mo de (then press h for help)
Example: nmap -v -sS -O www.my.com 192.168.0.0/16 '192.88 -90.*.*'
SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLE

****************
ndiff --help
****************
ndiff    [-b|-baseline  <file-or-:tag>]   [-o|-observed  <file-or-:tag>]
          [-op|-output-ports <ocufx>]      [-of|-output-hosts <nmc>]
          [-fmt|-format <terse | minimal | verbose | machine | html |
htmle>]
```

REMARK : The tools are installed but there is no record of usage.

4.C.1 SCORE: 10/10



You can edit, add, or delete users
Select [Add] to add a new definition

REMARK: The special POP only accounts were created but are not displayed for security reasons.

4.C.2 SCORE: 10/10

```
*******************
ls -al /etc/passwd
*******************
-rw-r--r--    1 root     root        1779 Aug 14 23:30 /etc/passwd

********** *********
ls -al /etc/shadow
*******************
-r--------    1 root     root        1779 Aug 14 23:31 /etc/shadow

****************
```

cat /etc/passwd

```
****************
```

alok:x:508:45:Alok Dadarya:/home/alok:/bin/false
mrinal:x:509:45:Mrinal Biswas:/home/m rinal:/bin/false
sushil:x:511:45:Sushil :/home/sushil:/bin/false
vimal:x:513:513:Vimal:/home/vimal:/bin/bash
pranamesh:x:514:45:Pranamesh Das:/home/pranamesh:/bin/false

```
vinay:x:516:45:Vinay Joshi:/home/vinay:/bin/false
akshay:x:517:45:Akshay Kumar:/home/akshay:/bin/false
pravar:x:518:45:Pravar:/home/pravar:/bin/false
```

REMARK: The permissions have denied a shell access to the mail users.

4.C.3 SCORE: 10/10

```
****************
ls –l /var/spool/mail/*
****************
-rwxrw-r--    1 akshay   popusers      553  Jul 31 06:54 /var/spool/mail/akshay
-rwxrw-r--    1 alias    mail       256319 May 14 07:05 /var/spool/mail/alias
-rwxrw-r--    1 alok     mail          553 Aug  1 03:37 /var/spool/mail/alok
-rwxrw-r--  1 amit     mail         2920 Aug  1 04:04 /var/spool/mail/amit
-rwxrw-r--    1 atul     popusers        0 Jul 11 02:44 /var/spool/mail/atul
-rwxrw-r--    1 bigb     bigb      1950998 Jul 17 12:37 /var/spool/mail/bigb
```

REMARK: The permission allows only the administrator to read , write and execute. The group is not allowed to read , which is correct.

4.C.4 SCORE: 10/10

```
****************
more hosts.deny
****************
# hosts.deny    This file describes the names of the hosts which are
#               *not* allowed to use the local INET services, as decided
#               by the '/usr/sbin/tcpd' server.
#
# The portmap line is redundant, but it is left to remind you that
# the new secure portmap uses hosts.deny and hosts.allow.  In particular
# you should know that NFS uses portmap!
#ALL:ALL  @ ALL,PARANOID
ALL:ALL
****************
more hosts.allow
****************
#  hosts.allow   This file describes the names of the hosts which are
#               allowed to use the local INET services, as decided
#               by the '/usr/sbin/tcpd' server.
#
ipop3d: 192.168.0.0/255.255.255.0
ipop3d: ALL
imapd:  192.168.0.0/255.255.255.0
in.telnetd: 192.168.0.101,192.168.0.55
#in.telnetd: ALL
# ALL: 192.168.0.0/255.255.255.0
#sshd:ALL
```

REMARK: Telnet access is allowed only to the administrator machines.

```
****************
ipchains –L
****************
```

Please check the output in 2.C.2

5.C.1 SCORE:10/10

```
***********************
ps -aux|grep syslogd
***********************

root       511  0.0  0.2  1168  160 ?        S     Aug14   0:04 syslogd    -m 0
root      3289  0.0  0 .8  1360  508 tty1     S     05:28   0:00 grep syslogd

****************
cat /etc/syslog.conf
****************
# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*                                       /dev /console
# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;news.none;authpriv.none        /var/log/messages
# The authpriv file has restricted access.
authpriv.*                                     /var/log/secure
authpriv.*                                    @alokd.tegora.stpn.soft.net
# Log all the mail messages in one place.
mail.*                                        /var/log/maillog
# Log cron stuff
cron.*                                        /var/log/cron
cron.*                                        @alokd.tegora.stpn.soft.net
# Everybody gets emergency messages, plus log them on another machine.
*.emerg                                        *
*.emerg                                        @alokd.tegora.stpn.soft.net
# Save mail and news errors of level err and higher in a special file.
uucp,news.crit                                  /var/log/spooler
# Save boot messages also to boot.log
local7.*                                      /var/log/boot.log
local17.*                                      @alokd.tegora.stpn.soft.net
# INN
news.=crit                                  /var/log/news  /news.crit
news.=err                                   /var/log/news/news.err
news.notice                                  /var/log/news/news.notice
```

5.C.2 SCORE :0/10

```
****************
ls –l /var/log/*
****************
-rw-------    1 root    root        5094 Jul 30 05:05 /var/log/boot.log
-rw-------    1 root    root       60288 Jul 31 19:26 /var/log/btmp
-rw-------    1 root    root       39244 Aug  1 05:30 /var/log/cron
-rw-------    1 root    root       79279 Jul  8 04:02 /var/log/cro  n.4
-rw-------    1 root    root           0 Jul 29 04:02 /var/log/spooler
-rw-------    1 root    utmp           0 Aug  1 04:02 /var/log/wtmp
-rw-------    1 root    utmp      391296 Aug  1 03:26 /var/log/wtmp
 -rw-------    1 root    root      69 2944 Aug  1 05:35 /var/log/maillog
```

REMARK: Access control in place. Log are not being streamed to separate server or written to a write protect media.

5.C.3    SCORE :0/10

```
****************
cat /etc/syslog.conf
****************
```

Please check the output of  5. C.4

REMARK: Offline backup is not being taken.

5.C.4    SCORE :10/10

```
****************
find / -name isoqlog -print
****************
/var/log/qmail/isoqlog
/var/www/html/isoqlog
/usr/local/isoqlog
```

REMARK: Isoqlog log analyzer is installed and running.

5.C.5    SCORE :10/10

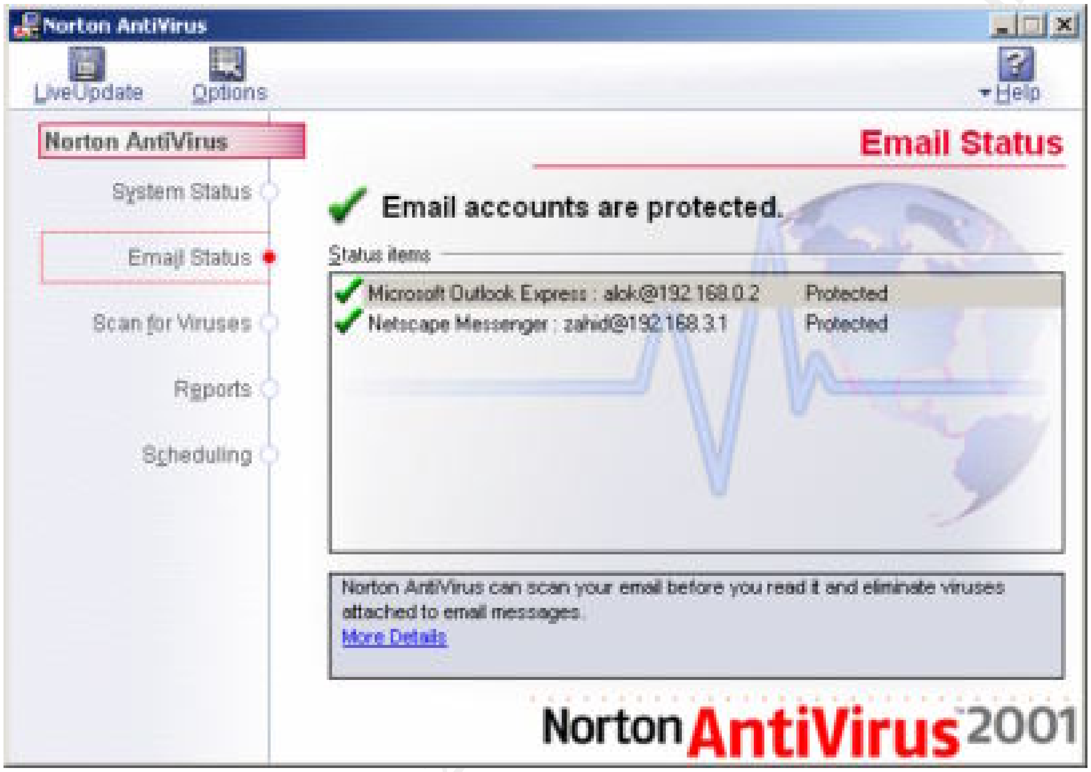
```
****************
df  -h
****************
Filesystem            Size  Used Avail Use% Mounted on
/dev/hda1             200M   66M  123M  35% /
/dev/hda10             100M  2.4M   92M   3% /boot
/dev/hda6             1.2G  2.8M  1.1G   0% /home
/dev/hda9             100M   13k   95M   0% /opt
/dev/hda11              50M  1.1M   46M   2% /tmp
/dev/hda5             1.4G  650M  757M  46% /usr
/dev/hda12             200M  4.3M  185M   2% /usr/local
/dev/hda7             574M   42M  503M   8% /var
```

REMARKS: File system is being checked regularly.

```
****************
du -ch /var/spool/mail/*
****************
72k    /var/spool/mail/akshay
256k   /var/spool/mail/alias
4.0k   /var/spool/mail/alok
4.0k   /var/spool/mail/alokd
28k    /var/spool/mail/amit
1.9M   /var/spool/mail/ bigb
100k   /var/spool/mail/core
0      /var/spool/mail/jamsheed
4.0k   /var/spool/mail/manish
2.6M   /var/spool/mail/mrinal
1.6M   /var/spool/mail/postec
4.0k   /var/spool/mail/pranamesh
528k   /var/spool/mail/pravar
44k    /var/spool/mail/rajeev
4.0k   /var/spool/mail/saad
4.0k   /var/spool/mail/sameer
4.0k   /var/spool/mail/sushil
```

```
6.6M   /var/spool/mail/tapan
224k   /var/spool/mail/vibhor
6.0M   /var/spool/mail/vimal
4.0k   /var/spool/mail/zahid
4.0k   /var/spool/mail/zoro
20M    total
```

8.C.2



Email Status

Email accounts are protected.

Status items

| | |
|---|---|
| Microsoft Outlook Express : alok@192.168.0.2 | Protected |
| Netscape Messenger : zahid@192.168.3.1 | Protected |

Norton AntiVirus can scan your email before you read it and eliminate viruses attached to email messages.
More Details

REMARK: Automatic scanning of the email, when ex tracted by the email client, is activated in the anti virus settings.

9.C.1 SCORE: 10/10

```
***************
cat /etc/inetd.conf |grep imap
***************
imap   stream  tcp   nowait  root   /usr/sbin/tcpd  imapd

***************
cat /etc/inetd.conf | grep qpopper
***************
pop3 stream tcp nowait root /usr/local/lib/popper qpopper   -s
```

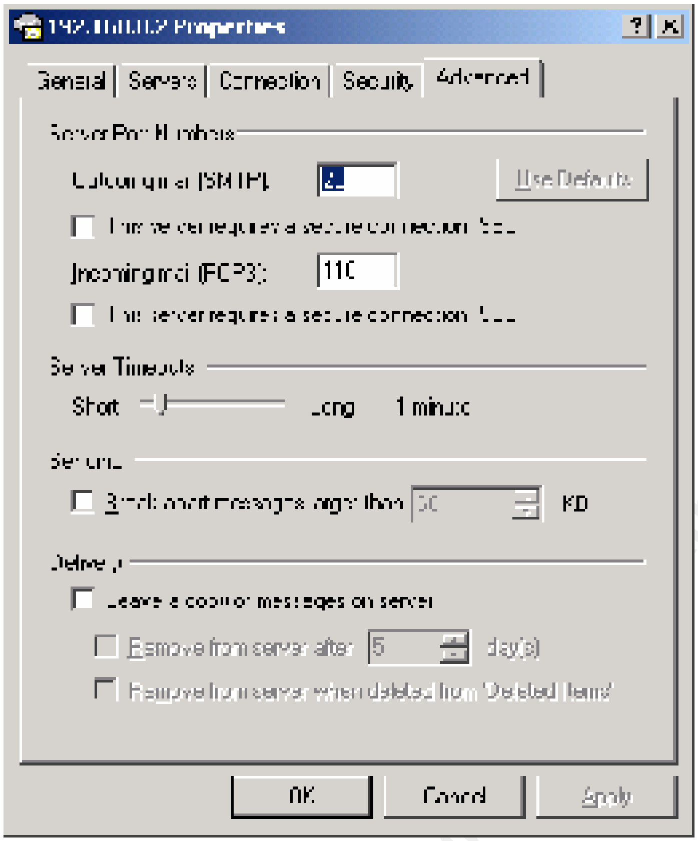
9.C.2 SCORE: 10/10

```
***************
telnet 192.168.0.2  110
***************
OK tegora.stpn.soft.net POP3(Qpopper.versionxxx.) server ready

***************
telnet 192.168.0.2  143
```

```
***************
OK tegora.stpn.soft.net IMAPrev1 v12.264 server ready
```

9.C.4 SCORE:0/10



192.168.0.2 Properties

Server Port Numbers

Outgoing mail (SMTP): 2

☐ This server requires a secure connection (SSL)

Incoming mail (POP3): 110

☐ This server requires a secure connection (SSL)

Server Timeouts

Short — Long 1 minute

Sending

☐ Break apart messages larger than 60 KB

Delivery

☐ Leave a copy of messages on server

☐ Remove from server after 5 day(s)

☐ Remove from server when deleted from 'Deleted Items'

REMARK: This setting for secure socket layer(SSL) communication is not activated.

10.C.1 SCORE: 10/10

```
***************
vi  /etc/tcp.smtp
***************
        192.168.0.:allow,RELAYCLIENT=""
        127.:allow,RELAYCLIENT=""
        :allow
```

REMARK: This confirms that only internal private address and the local machine is allowed for relay.

10.C.2 SCORE: 10/10

```
***************
whereis procmail
***************
/usr/bin/procmail
```

10.C.3 SCORE: 10/10

```
***************
procmail -v
***************
```

```
procmail v3.14 1999/11/22, Copyright (c) 1999, Stephen R. van den Berg
        <srb@cuci.nl>
Submit questions/answers to the procmail -related mailinglist by sending to:
<procmail-users@procmail.org>
And of course, subscription and information requests for this list to:
        <procmail-users-request@procmail.org>
Locking strategies:  dotlocking, fcntl()
Default rcfile:   $HOME/.procmailrc
It may be writable by your primary group
Your system mailbox:    /var/spool/mail/root
```

10.C.4 SCORE: 0/10

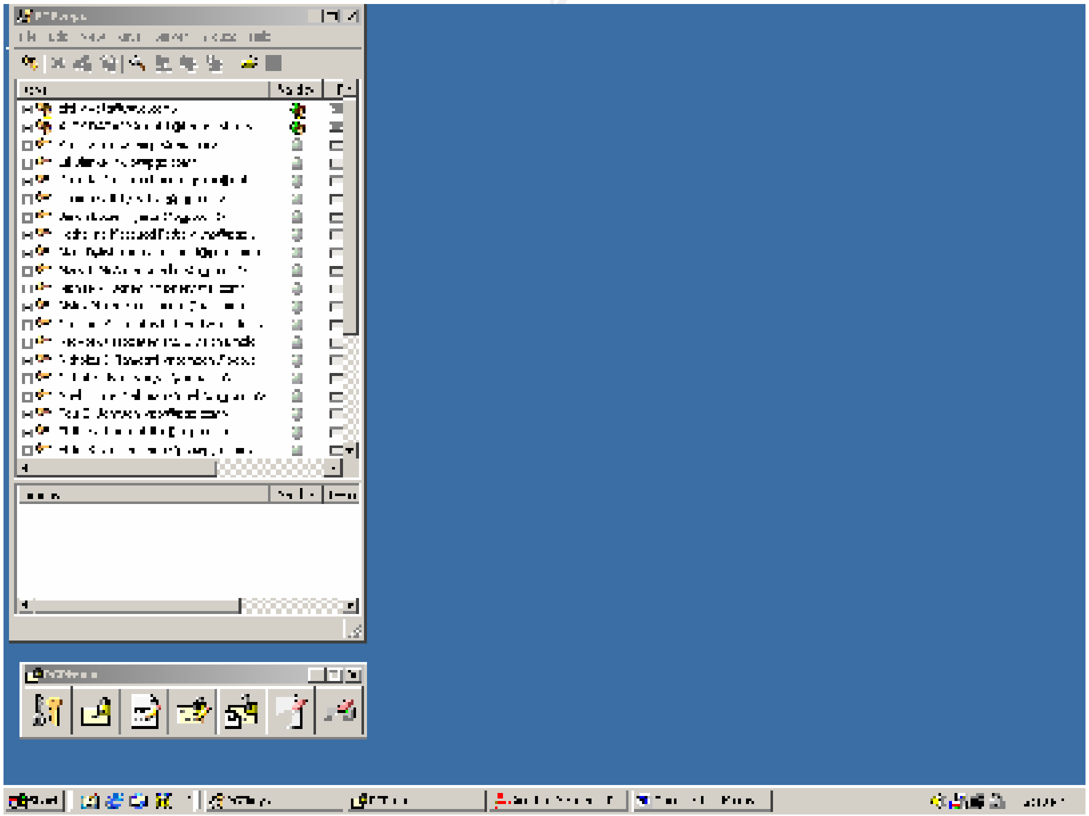
```
***************
whereis  .procmailrc
***************
.procmailrc:
```

REMARKS: Procmail  Installed but not configured

10.C.5 SCORE: 0/10

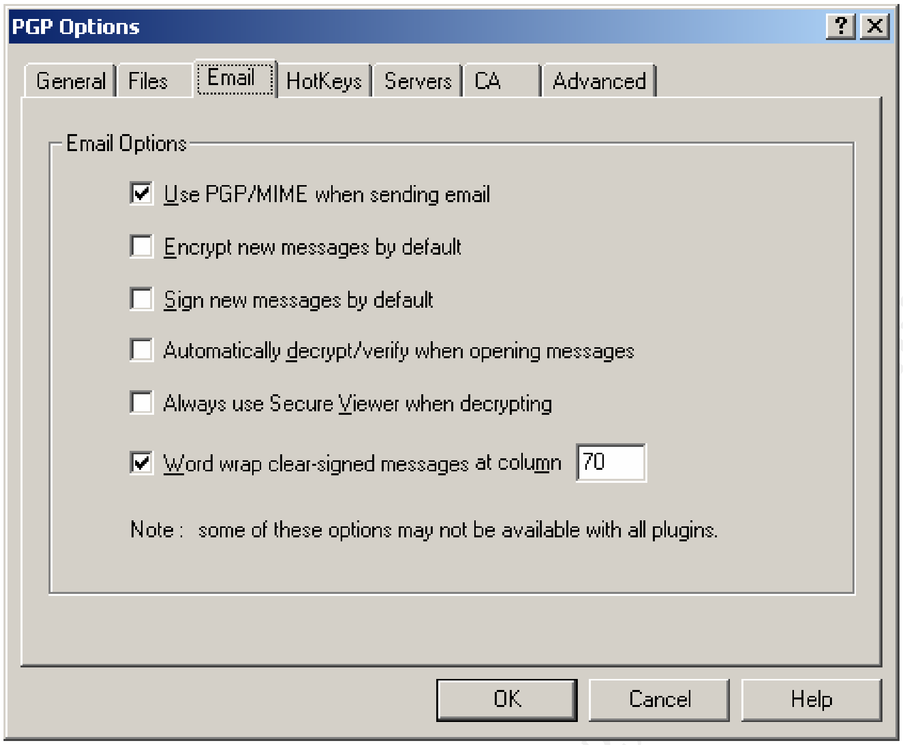
```
***************
cat /var/qmail/alias/.qmail-mailer-daemon
***************
cat: /var/qmail/alias/.qmail-mailer-daemon: No such file or directory
```

11.C.1 SCORE: 10/10



REMARK: These snapshots show that PGP is installed.

11.C.2 SCORE: 10/10



Email Options

☑ Use PGP/MIME when sending email

□ Encrypt new messages by default

□ Sign new messages by default

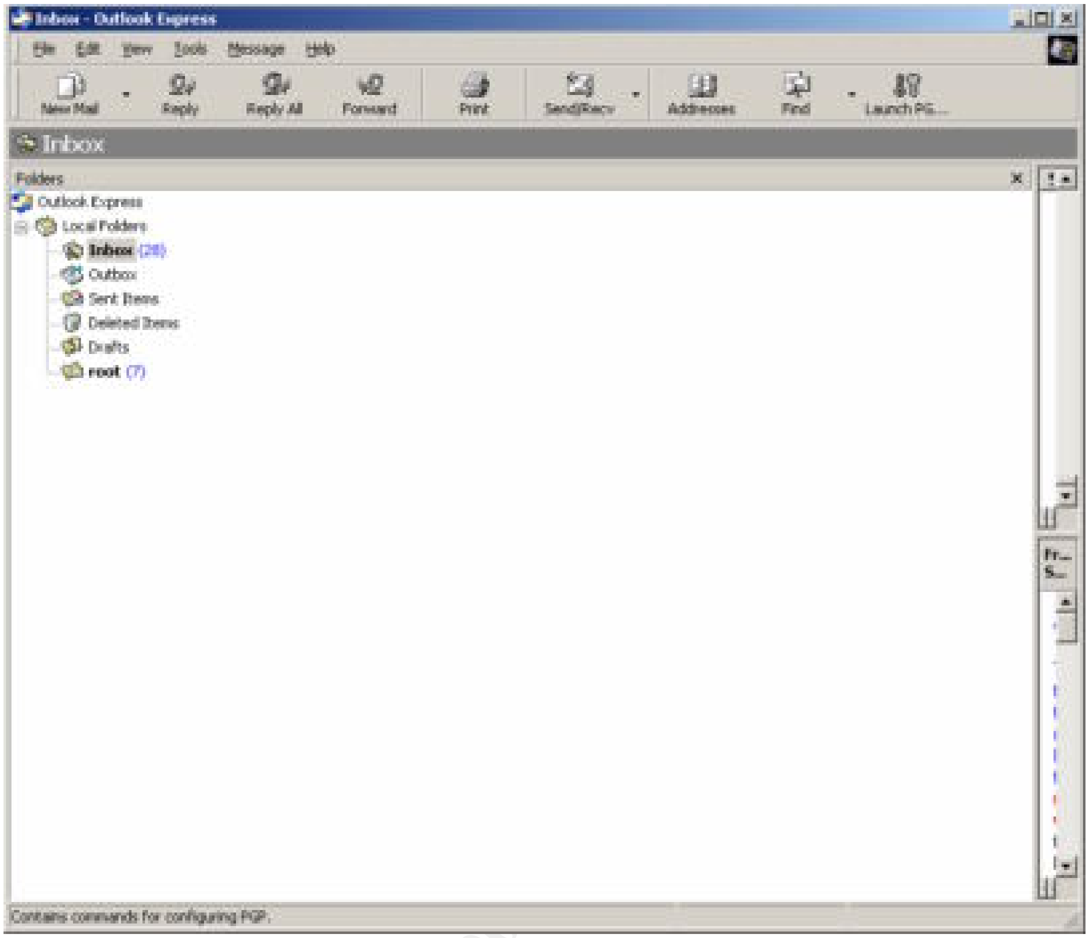
□ Automatically decrypt/verify when opening messages

□ Always use Secure Viewer when decrypting

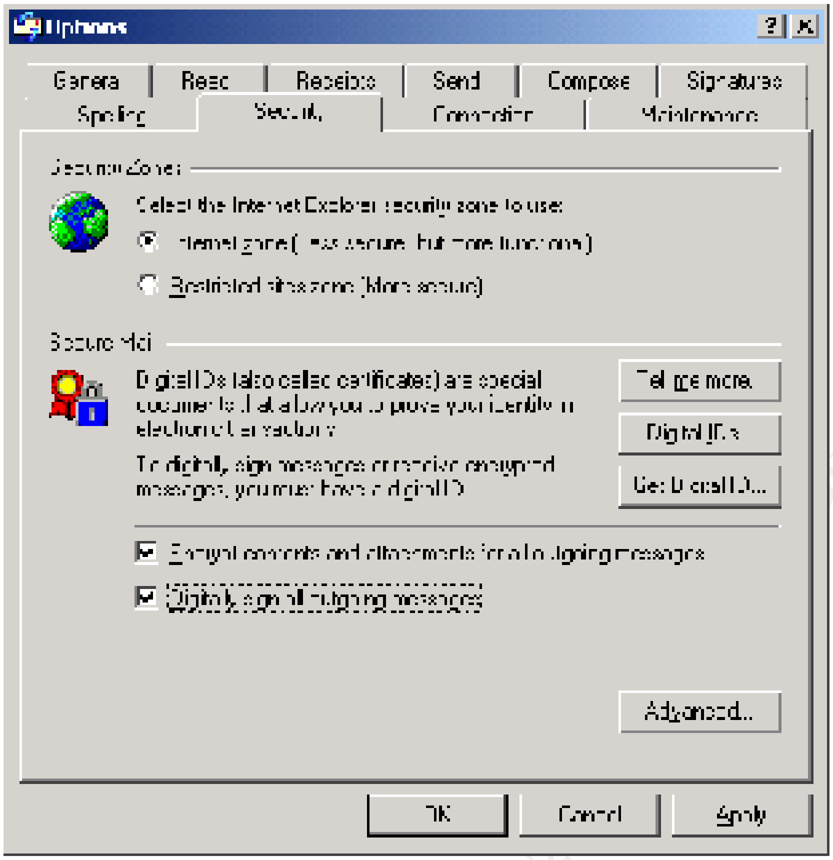
☑ Word wrap clear-signed messages at column 70

Note : some of these options may not be available with all plugins.

11.C.3 SCORE: 10/10



Contains commands for configuring PGP.



Security Zones

Select the Internet Explorer security zone to use:

● Internet zone (Less secure, but more functional)

○ Restricted sites zone (More secure)

Secure Mail

Digital IDs (also called certificates) are special documents that allow you to prove your identity in electronic transactions.

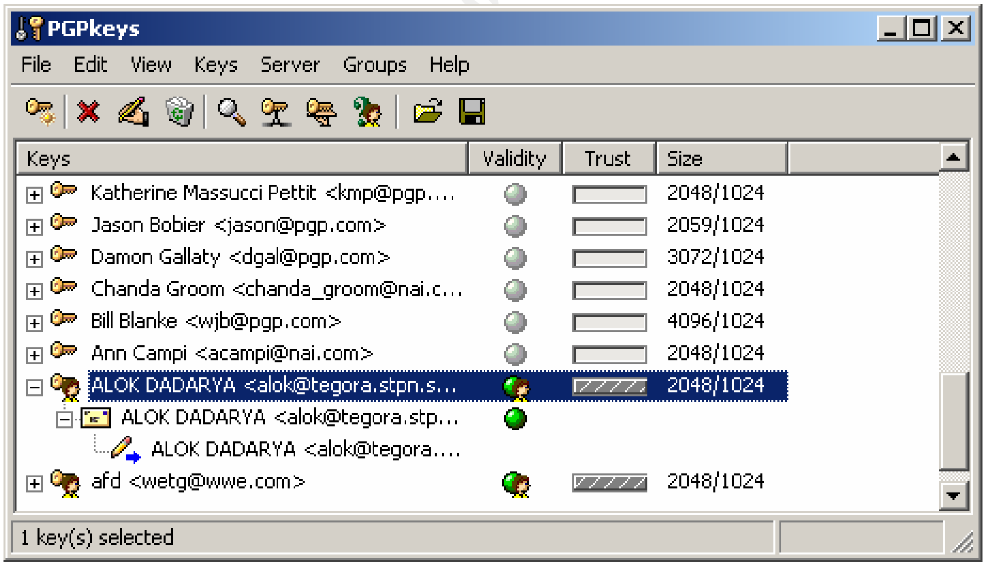
To digitally sign messages or receive encrypted messages, you must have a digital ID.

☑ Encrypt contents and attachments for all outgoing messages

☑ Digitally sign all outgoing messages

REMARK: The user encrypts the messages before sending.

11.C.4 SCORE: 10/10



| Keys | Validity | Trust | Size |
|---|---|---|---|
| Katherine Massucci Pettit <kmp@pgp.... | ● | ▭ | 2048/1024 |
| Jason Bobier <jason@pgp.com> | ● | ▭ | 2059/1024 |
| Damon Gallaty <dgal@pgp.com> | ● | ▭ | 3072/1024 |
| Chanda Groom <chanda_groom@nai.c... | ● | ▭ | 2048/1024 |
| Bill Blanke <wjb@pgp.com> | ● | ▭ | 4096/1024 |
| Ann Campi <acampi@nai.com> | ● | ▭ | 2048/1024 |
| ALOK DADARYA <alok@tegora.stpn.s... | ● | ▨ | 2048/1024 |
| ALOK DADARYA <alok@tegora.stp... | ● | | |
| ALOK DADARYA <alok@tegora.... | | | |
| afd <wetg@wwe.com> | ● | ▨ | 2048/1024 |

1 key(s) selected

REMARK: The users key is available on the public server.

**Section D: Evaluation of the audit**

The final audit score for the organization is 568 (56.8 %). The organization has scored 140 (58.3%) in the "Who" section. The organization h as ample resources for tackling the issues related to mail server security. The score in the "Why" section is 240 (66.6%). The mail server administrator is aware of many of the issues pertaining to email security. Score in "What" section is 315 (53%). The implementation strategy for security solutions is poor. The relevant tools are installed but not configured. The organization particularly requires a strong implementation strategy for mail filtering, secure POP3 & IMAP & hot fixes. The areas where the organization requires extensive training & support are mail proxy virus scanning, configuration & network security of the mail server. The security risks observed during the audit are listed in decreasing priority below. The priority is based on the weight ag e assigned earlier, with the consensus of management & information systems team. The security officer must maintain his existing strengths and target the weaknesses in the priority of their mention in the next few pages.

**1. User awareness**

The end user awareness is very poor. There is no training given to the users regarding security in general. Most of the users are even unaware of the impact information -pilferage through emails can have on the organization. The users are completely dependent on the administrator to the extent that even the update of virus signatures in the anti virus tool have to done by the desktop administrator. The organization has been advised to train their employees in the area of information security. The information security offi cer has been made responsible for this.

**2. Physical security**

The organization has a sound arrangement for the physical safety of the mail server. The mail server is kept in a server room and under a lock. Movement to the server room is controlled but there is no close circuit camera.

**3. Network security**

The organization has no perimeter protection mechanism. The network is poorly organized and all the machines in the organization are in the same subnet, including the machines with valid external IP addresses too. The machines with external IP addresses, like mail -server, web-server, etc should be kept in the DMZ (de -militarized zone). The creation of separate DMZ helps in protecting the internal network if a machine, connected directly to the Internet is attacked and hacked. In order to protect an organization from external attacks minimally a firewall & IDS are required.

**4. Server virus scanning**

As explained earlier in this document it is very important to protect the organization from the threat of viruses and worms. The virus attacks are the greatest nuisance makers. The organization has no server side protection for viruses. There is no virus scanning of the mails entering or leaving the organization. The organization is advised to immediately implem ent solution for server side virus protection.

**5. Mail client settings**

The client side security is well implemented. The email client is of the latest version and the anti virus is regularly updated. Though the user in quite unaware but the desktop administrator is taking good action to protect the systems.

**6. Operating system access control**

The evaluation of the audit can only be as fare, as the auditor knows his subject. The organization has fared well in my checklist for this section. But I have mentio ned in the direction for future work section that this section needs some more inputs. So till we have a stricter auditor, the organization enjoys a high score in this section.

**7. Hot fixes & security patches**

The mail server application is Qmail 1.03, t he latest version as on 09/06/01. The administrator is a vivid reader of literature on www.lifewithqmail.org. He keeps track of all the vulnerabilities. There is no provision of testing the new versions on test machine before putting on the mail server. Though the organization has been lucky so far and none of the software crashed the production server. But it should be mandatory to test all patches on a test machine before applying them on the production server .

**8. Auditing of logs**

The logs are generated and analyzed. But there is no rotation of the logs to a remote server. In the present scenario the attacker can clear his footprints by erasing all logs. Thus it is important for the organization to have a sysl ogd server, which can collect logs across servers in the network.

**9. Service control**

The machine is not dedicated for the purpose of the mail server. The irrelevant services running on the machine are exposing the server to further risk. And an attacker can exploit any of these services to gain privileged access to the mail server. The administrator is not monitoring services regularly. Tool like Nmap are installed, but there are two problems. First it is not used for finding out ports open on the machine . Second if an attacker gains access then he will use it for port scanning other machines on the network. Therefore administrator has been advised to close all the irrelevant services.

**10. Mail filtering**

The server is protected from being used for third party relay. The latest version of Procmail (a very popular and successful filtering application) is installed, but not configured. The mail server administrator needs to be trained on Procmail configuration. For more information refer http://www.procmail.org/

**11. Secure POP3 and IMAP**

The applications for secure email (Qpopper, latest version) transfer, is installed. But the compile time configuration of the applications to support APOP, Kerberose & TLS/SSL was not correctly done. The client side configuration, to communicate with a secure POP3 & IMAP server, is incorrect. In the existing scenario the users can't avail this facility. For more information refer http://www.eudora.com/qpopper/documentation.html

**12. Encryption & digital signature**

The users have PGP installed for encrypting and digitally signing the mails. The organization is using the public servers for storing their public keys. The or ganization can keep a private encryption key server. This would help in encrypting and digitally signing the mails rotated within the organization network, without any interaction with external world.

**Section E: Direction for future work**

The audit document in Section B should be treated as a live document and I request all, to continuously improve it through their experience and thus keep it compliant with the latest risks. This can be best achieved, when you submit your organization to an audit with this document and identify the deficiencies. Few risk areas I came across, while conducting the audit, are listed below.

**1. Password protection of mail client**
It is a very common situation to leave our desk without locking our desktop screen. Temporarily some one may get access to your machine. He can open your mail client and read all your mails. Such a situation can be avoided in two ways. First is to lock your screen, each time you leave the desk. Second would be to password protect the email client. You can password protect your identity. The Microsoft Outlook Express email client stores files .dbx and .pst files. These files should also be password protected otherwise anyone with access to these files can open them in Microsoft outlook express and outlook c lient. This should ideally become part of the user awareness section in the audit document.

**2. Periodic backup of business critical mails**
While I was conducting the audit I came across another very common situation. The senior software developer came runn ing to the system administrator and said: " My Machine has crashed". The mailbox was on the same partition that got damaged. Thereafter it was a hard time to console this guy. Well because according to him all his work records exchanged with his boss were in those mails. The lesson to be learnt and added in the audit document is to back up and keep the business critical mails. Including it in the backup policy and informing the backup administrator will be an easy implementation of this.

**3. Protection from Denial service attack**
Availability of the mail server is by far the greatest concern for management. They would not want their mails to bounce back or be stuck in the mail server due to non -delivery. The situation could become verse if some third party ga rbage mails traffic starts affecting the mail server and the real mail traffic gets clogged. There can be various reasons behind a mail server coming to a halt. But one of the recent most threats has been Denial of service attacks. Denial of service attack s grew to a notorious scale in the year 2000 and the damage done by them was enormous. The audit checklist should include questions to verify whether the mail service is subject to such attacks. It is important to look into the immunity to denial of servic e attacks from internal network as well.

**4. Standby mail server**
It is very important to always have a standby mail server ready. Email is a round the clock service for information transfer, especially for businesses spread across time zones. The mail server could come down due to various reasons (example: Operating system crash, etc). In such an eventuality it is advised to have another machine with the same software/hardware configuration ready. It will greatly reduce the time required to bring the mail s ervice to life. A word of caution, make sure it is tested as well in order to avoid last minute rush.

**5. Protection of files**
How can you tell, if a log file has been modified by an attacker? How can you tell if somebody reads the mails while they are wait ing to be retrieved by the email client?
Thus while considering the audit of the mail server in particular it is important to include the provision of protection of files and mails lying on the mail server. There are file integrity tools, which can help us determine this. They will give us information on when a particular file was last accessed, written, etc. This would also include which user has changed the file. Thus an thorough exploration into this subject and its inclusion in the audit document would be a value addition.

**6. Operating system privileges**
A significant contribution would be the mail -sever operating system privileges and how to run it in a non-privileged mode to minimize the harm if someone exploits vulnerability & gains access. Due to my lack of understanding of how to run non -privileged daemons, I could not do much justice to the section on mail server operating system access control. So please come forward and contribute a section in the future exercise on email auditing.

**7. Corrective action process (CAP)**
The relevance of the questions in the audit document is decided by there compliance to the policies defined by the organization. But if a noncompliance is found how is it rectified?
Let us take an example. If the organization found, in their logs that an unauthorized user in the internal network is attempting to gain super user access through a telnet session. Does it take any action against him? If yes then what? If not then it is important to have a defined process (& a person) assign ed to take action against such malicious activities. A section on this CAP should necessarily cover discrepancies caused by both external and internal sources. Discrepancies identified during audit can be corrected using an effective CAP approach.

**References**

1. Ian Fried "SirCam clogs mailboxes, spreads secrets" July 23, 2001, 3:30 p.m. PT. URL: http://news.cnet.com/news/0 -1003-200-6647394.html
2. India's IT Security portal, "Whitepaper on emai l security".1 st September, 2001 URL:www.itsecurity.gov.in/general_security/application/email_security.htm
3. DSD's Information security group, "Handbook 11 -email security".1 st September, 2001. URL: http://www.dsd.gov.au/infosec/acsi33/HB10.html
4. David Wood. Programming Internet Email, 1 st edition. O'reilly Publication. August 1999.
5. Dave Sill, "Life with q mail", 13 June 2001URL: www.lifewithqmail.org/lwq.html
6. Martin Roesch, "Snort Users Manual Snort Release: 1.8.1". 1 st September 2001. URL: http://www.snort.org/docs/writing_rules/
7. William wong, "Linux Networking: Using Ipchains" 1 st September 2001. URL:http://www.linuxplanet.com/linuxplanet/tutorials/2100/1/
8. Fyodor, "Introduction to Nmap", Thursday, 21 -Jun-2001 19:51:51 PDT. URL: http://www.insecure.org/nmap/
9. jdl@vinecorp.com , "Ndiff Quickstart guide", 1st September 2001. URL: http://www.vinecorp.com/ndiff/NDiff_Quickstart.html
10. Wietse Venema "Tools and papers (download page for Tcp wrapper reference)", 1 st September, 2001.URL: ftp://ftp.porcupine.org/pub/security/
11. Stephen R. van den Berg & Philip Guenther, "Welcome to Procmail.org", 1 st September 2001. URL: http://www.procmail.org/
12. Ismail Yenigul, "Details of IsoQlog", 1 st September 2001. URL:http://www.enderunix.org/isoqlog/
13. Christian Bricart & Rainer link, "Amavis - A mail virus scanner", 1 st September 2001. URL: http://www.amavis.org/amavis.html
14. QUALCOMM Incorporated, "Qpopper 4.0 Documentation", 1 st September 2001. URL: http://www.eudora.com/qpopper/documentation.html
15. The international PGP home page, " H ow PGP works ", 1 st September, 2001 URL: http://www.pgpi.org/doc/pgpintro/

16. The RSA security's web site for SMIME "S/MIME Central, 1st September, 2001
URL: http://www.rsasecurity.com/standards/smime/