CERT-In Guideline CISG -2003-04

CERT-In

Indian Computer Emergency Response Team

Handling

Computer Security Incidents

System Security Guidelines

Department of Information Technology
Ministry of Communications and Information Technology
(a) Government of India

Contents

1. Server Operating System Security Guidelines

1.1. Introduction

The following document is intended as CERT-In recommended guidelines for setting up a server. The document provides detailed steps for System Administrator (SA) /system integrators to verify their already installed Servers & guidance for new server setup. The document covers general topics required for setting up a server in secure environment. The document is Operating System (OS) independent & recommending in nature.

1.2. Planning

1.2.1 Identification of Server role

Before installation of server one should first identify role of the server. The server role means applications running on the server. The server can be deployed as a file server, print server, mail server, web server or database server. Based on the server role or applications running on it, System Administrator (SA) can categorize the server under low, medium or high threat perception. In all cases the SA have to plan for adequate server security to ensure confidentiality, integrity and availability of data.

1.2.2 Identification of network services

Network services will depend upon the role of the server like Account server, Web server, Mail server, Database server etc. As a general rule, a network server should be dedicated to a single service. This usually simplifies the configuration, which reduces the likelihood of configuration errors. It also eliminates unexpected and unsafe interactions among the services that present opportunities for intruders. In some cases, it may be appropriate to offer more than one service on a single host computer. For example, the server software from many vendors combines the file transfer protocol (FTP) and the hypertext transfer protocol (HTTP) services in a single package. For some organizations, it may be appropriate to provide access to public information via both protocols from the same server host, but it is not recommended since it is a less secure configuration.

1.2.3 Physical security

Access to a server is very important, physical access to a server should be limited to only administrator and other server operators for backup etc. There should be no free access to servers. In general following guidelines should be adhered to

- Protect the system from unauthorized use, loss or damage, e.g. the door should be locked when not in the office

- Keep portable equipment secure
- Position monitor and printers so that others cannot see sensitive data
- Keep floppy disks and other media in a secure place
- Seek advice on disposing of equipment
- Report any loss of data or accessories to the SA
- Keep the system and sensitive data secure from outsiders
- Get authorization before taking equipment off-site
- Take care when moving equipment
- Log out, shut down or lock the system when leaving office
- Install UPS system with adequate battery backups to avoid any data loss or corruption due to power failure

1.2.4 Methods of authentication

Depending on the level of threat exposure to the server, authentication method should be chosen

For **Low Threat Exposure** in build user/password mechanism available with the OS is an acceptable practice.

For **Medium Threat Exposure** a choice could be made from user/password combination implemented by sever only with strong password policy or an external authentication server like TACKAC, RADIUS or KERBOUS may be implemented. For example an external POP mail server may have radius server authenticating the user access.

For **High Threat Exposure** a choice could be made from tokens, smart cards and biometrics devices (devices that recognize a person based on biological characteristics such as fingerprints or patterns of the retinal blood vessels.

1.3 Installation & Configuration

The installation should be carried out from the original media, supplied by the vendor. The OS hardening should be done following the steps listed in the guidelines provided by the vendor for this purpose. This includes installation of patches, disabling of unwanted ports, etc. Care should be taken to match the release of patches with the OS version number.

1.3.1 OS Hardening

1.3.1.1 Patches

One of the most important tasks of the SA is to keep the most current patches for the OS and application software installed on a server. Many of these patches fix security vulnerabilities that are well known to intruders. There are two types of patches in general viz. Service Packs and Hotfixes. Installing these patches in order is important. Service Packs must be installed before the Hotfixes.

Service packs are used to patch a wide range of vulnerabilities and bugs. The latest service pack that has been tested to work in one's environment should always be applied after installing the operating system. Service packs are cumulative; users need to install the latest Service Pack.

Hotfixes are released more frequently than service packs and are meant to patch a more specific problem. Not all hotfixes may be needed for a particular system. Before installing these fixes on critical systems or installing them on a large number of devices, hotfixes should be tested to ensure that there is no conflict with other third party drivers.

1.3.1.2 Disabling unwanted services and protocols

Only required network services should be installed in the server. There are many default services with the standard OS software. Depending upon the role of server one should load only required network services, like on a mail server DNS service is not required.

Disable unneeded network protocols, as each installed protocol takes server resources. Only essential protocols should be loaded on the server. Each network protocol should be configured for security settings, *like in case of TCP/IP protocol* ***only essential ports should be enabled***. For example, on MS Windows NT Server disable inbound and outbound traffic to the external connections for TCP and UDP ports 135, 137, 139 and UDP port 138. Blocking these ports prevents potential intruders from gathering useful information such as computer names, usernames, and services running on those computers.

A list of ports used by Windows NT version 4.0 services is as under:

Function	*Static ports*
Browsing	UDP:137,138
DHCP Lease	UDP:67,68
DHCP Manager	TCP:135
Directory Replication	UDP:138 TCP:139
DNS Administration	TCP:139
DNS Resolution	UDP:53
Event Viewer	TCP:139
File Sharing	TCP:139
Logon Sequence	UDP:137,138 TCP139
NetLogon	UDP:138
Pass Through Validation	UDP:137,138 TCP:139
Performance Monitor	TCP:139
PPTP	TCP:1723 IP Protocol:47
Printing	UDP:137,138 TCP:139
Registry Editor	TCP:139
Server Manager	TCP:139

Trusts	UDP:137,138 TCP:139
User Manager	TCP:139
WinNT Diagnostics	TCP:139
WinNT Secure Channel	UDP:137,138 TCP:139
WINS Replication	TCP:42
WINS Manager	TCP:135
WINS Registration	TCP:137

Security scanner tools like NMAP, NESSUS should be run to know which ports or services are currently open or running on the server. Any unwanted port/service should be stopped.

1.3.2 Protecting server against unauthorized network access

Firewalls and Intrusion Detection System (IDS) should be used on network infrastructure of the organization. The attacks like Denial of Service (DOS) can be avoided with the deployment of firewalls & IDS. For further details on firewalls refer to CERT-In Firewall Security Guidelines.

1.3.3 Encryption

Encryption technologies on servers and networking equipment should be used for remote server administration. It prevents administrator passwords and other sensitive information from crossing one's network in clear-text. Use strong authentication when accessing hosts in one's domain to reduce the risk of a security breach due to false credentials, like in UNIX based systems SSH protocol employs public key cryptography and provides both encryption and strong authentication.

1.3.4 File system security

1.3.4.1 General

All file level security depends upon the file system. Only the most secure file system should be chosen for the server. Then user permission for individual files, folders, drives should be set. Any default shares should be removed. Only required file and object shares should be enabled on the server.

1.3.4.2 File permissions and access control

- Configure access controls for all protected files, directories, devices, and every change or decision not to change each object's permission should be documented along with the rationale
- Disable write/modify access permissions for all executable and binary files
- Restrict access of operating system source files, configuration files, and their directories to authorized administrators

- For UNIX systems, there should be no group/world-writable files unless specifically required by necessary application programs
- For NT systems, there should be no permissions set such that "the Everyone group has Modify permissions to files"
- Assign minimum level of access permission to all kernel files
- Establish all log files as "append only" if that option is available
- As a goal, preclude users from installing, removing, or editing scripts without administrative review. Proper procedure for enabling and enforcing the same may be established and fully documented
- Pay attention to access control inheritance when defining categories of files and users. Ensure that operating system should be configured so as newly created files and directories inherit appropriate access controls, and that access controls propagate down the directory hierarchies as intended when one assigns them
- Administrators should disable a subdirectory's ability to override top-level security directives unless that override is required

1.3.4.3 Tools

Install tools for checking integrity of files on the server. This will also help in analyzing and tracking intruders, in case of an intrusion. For UNIX, file integrity and analysis tools like ***Tiger, Tripwire, Coroner's Toolkit*** can be used.

After configuring the server OS file checksum should be generated and stored on a removable media safely. SA should run file checksum utility 2-3 times a day to compare with the configured checksum, any differences should be analyzed suitably. Whenever server is reconfigured, a new checksum should be generated, discarding the old checksum.

1.3.5 Account Policy

1.3.5.1 User privileges & rights

Document the categories of users that will be allowed access to the provided services. Categorize users by their organizational department, physical location, or job responsibilities. A category of administrative users who will need access to administer the network server and a category for backup operators needs to be created. Normally, access to network servers should be restricted to only those administrators responsible for operating and maintaining the server. Determine the privileges that each category of user will have on the computer. To document privileges, create a matrix that shows the users or user categories cross-listed with the privileges they will possess. The privileges are customarily placed in groups that define what system resources or services a user can read, write, change, execute, create, delete, install, remove, turn on, or turn off. For many resources, such as program and data files, the access controls provided by the OS are the most obvious means to enforce access privileges. Also, consider using encryption technologies to protect the confidentiality of sensitive information.

1.3.5.2 Passwords

There should be password policy in the organization. The most common method of authentication is password. The responsibility of selecting a password that is hard to guess generally falls on users. To decrease the chances of guessing password, user must select a hard-to-guess, or **strong** password.

A strong password must:

- Be as long as possible
- Include mixed-case letters.
- Include digits and punctuation marks.
- Not be based on any personal information.
- Not be based on any dictionary word, in any language.

While most shared systems can enforce at least some of these rules, almost none have features to enforce all of them. Despite all these efforts the passwords could be guessed given enough time. Thus a user must also:

- Change his/her password regularly, in order to limit the amount of time available to persons to guess it. All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed regularly.
- Never use the same password twice.

Some systems have a password expiry feature, which forces user to change his password periodically. Some systems incorporate a password history feature, which disallows user from reusing one of his last *n* passwords. When faced with a password history mechanism, some users may change their password *n* times, and return it to its original value, so as to avoid having to remember a new password value. To prevent this, systems should either have an unlimited-length password history, or prevent users from changing their password more than once daily.

1.4 Operations & Maintenance

1.4.1 Patches

The server should be updated regularly for any latest service packs and hotfixes. With this some of the known attacks can be avoided. Server software like mail server, web server, database server etc. should always be updated for latest patches or software versions. The application software installed on server (if any) like web browser, should also be regularly updated with latest patches. This keeps the server secure, from any attacker to exploit bugs or vulnerabilities in the server software. All new patches should be tested offline and then only put on the actual servers. After the patches are applied OS hardening should be redone.

1.4.2 Anti-virus

Computer viruses spread easily through floppy disks, email, or programs downloaded from the Internet. Potential problems range from changing data to reformatting system hard drive. Once created, viruses can spread without help from their creators. One can get them from computers at the office, from using computer at home, or from an email. To protect the systems, it is recommended that a virus scanning/detecting/cleaning program must be installed on the computer systems and It should be regularly updated.

New viruses are created continuously, and vendors of virus detection software offer updates to detect them. To get the latest updates, check the vendor web page. Some virus detection software allows getting the updates automatically via the Internet. The anti-virus software should be configured to schedule these updates at least twice a week.

It is recommended that computers do a quick scan when the system is booted, as programs are loaded into memory, and when new data is detected (from email, removable media). Computers should get a full system scan periodically which can be scheduled to run when the users are away for the evening.

Prior to making software available to many machines on a network, install it on a stand-alone device and scan it for computer viruses.

1.4.3 System monitoring

1.4.3.1 Performance

Server performance should be monitored on regular basis. There are built-in tools in the server OS. These tools can monitor server health for hardware components like CPU, memory, hard disk, I/O etc. and also application software on the server like web server application, database server application etc. Any degradation in the server performance can also be linked with triggers and alarms, which sends warning or alert messages to the SA, who can take necessary remedial actions. Server performance monitoring also helps in detecting attacks, like when a hacker misuse some server to launch attacks, the processes running to accomplish attack may degrade server performance.

1.4.3.2 Audit & logs

Server should be regularly audited and log files scanned for knowing any attacks and intrusions, preferably daily. For small organizations separate logging server with hardened OS should be implemented. Server to logging server communication should also take place over a secure i.e. encrypted channel. Additionally the logs must also be encrypted & access to it should be highly restricted. For very high threat exposure IDS should be installed.

The following guidelines should also be followed

- Make use of facilities provided with server OS to assist with disseminating log files e.g. FreeBSD emails a summary of important system and security information to root as part of its pre-configured crontab
- Use a reliable mechanism for log rotation. This may include replacing an existing logging daemon/service with a more secure or full-featured one.
- Implement automated reporting facilities so that scans of one's network are reported immediately to the SA.
- Keep a logbook of all system administration activities on each server.

1.4.4 Incident detection tools

Appropriate Tools for Incident Detection must be installed on the server. The reports generated by the tools should be monitored regularly to check any change in the system, unauthorized access, DoS attacks etc. The alarms and event notifications should also be set appropriately.

Some of the tools are

Windows based servers	*SamSpade, Retina, Fport, NBTScan*
Unix based server	*NMAP, SAINT, SARA, THC-Amap, THC-Hydra*

These tools are very helpful in detecting server compromise and similar attacks.

1.4.5 Backups

For the purpose of data safety, Backup policy must be made. It should cover methods like cold, warm and hot backups, role of backup operators and their access rights. All users must recognize that all forms of data storage are subject to data loss. For example, a disk crash may result in loss of server data. Users must therefore take steps to ensure there are copies of important data, called backups. Users should ensure security of data on the equipment including backups of important data held on it. Information stored on central servers is to be backed up regularly by the System Administrator.

All users should follow the following guidelines:

- Wherever possible, save important data onto centrally managed network drives, which are generally backed up daily
- Keep paper copy of server configuration file
- Keep the DATs or other removable media in a secure location away from the computer
- Regularly check that another system can read the removable media

1.4.6 Recovery

There could arise the situation when server crashes due to some hardware faults like disk failures, network failures, etc. For such failures, recovery methods of running server without affecting server services should be defined like disk mirroring, disk arrays or recovery from backup media. In case of software failures also, steps should be defined to reload the server services or OS accordingly. Recovery tools should be installed on the server like hard disk recovery software. With the help of such tools server OS is recovered without loss of time. For critical applications *fault tolerant* systems may be installed.

1.5 Incident Handling

1.5.1 What is an Incident

An Incident is an act of violating an explicit or implied security policy, assuming there exists security policy in the organization. The types of activity considered as violation of a typical security policy are characterized below. These activities include but are not limited to:

- security violation in which a system resource is exposed or is potentially exposed to unauthorized access
- unwanted disruption or denial of service
- any adverse event which compromises some aspect of computer or network security
- the unauthorized use of a system for the processing or storage of data
- changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction or consent

1.5.2 Incident detection

Tools installed for monitoring server performance and incident detection helps in detecting an incident. The symptoms of an incident could be like sudden degradation in server performance, server compromise, failure of service(s), defacement of web site contents, spam mails, mail route abuse etc.

1.5.3 Safeguard measures after incident

When a SA finds that some abnormal behaviour in server performance or alarms through incident detection tools are noted the following steps should be taken

- Change administrator password of the server
- Disconnect the server from network, depending upon the severity of Incident
- Or stop server services like web server, mail server etc.
- Or worst is switch off server

1.5.4 Incident reporting

An Incident should immediately be informed to CERT-In by means of telephone, fax, email or web. The site address of CERT-In is www.cert-in.org.in. After reporting the incident to CERT-In, advisory notes of CERT-In should be followed for recovering from incident.

1.6 References

- Securing Network Servers- Security Improvement Module- CMU/SEI-SIM-010
- http://www.staffs.ac.uk/services/information_technology/content/regs/seurity/security_guidelines.pdf
- http://psynch.com/docs/strength.html
- www.sans.org
- www.cert.org
- www.nsa.org
- www.auscert.org
- www.fedcirc.org
- RFC 2828 document

2. Workstation Operating System Security Guidelines

2.1 Introduction

The word "workstation" is used in this module to mean the combination of the hardware, operating system, application software, and network connection.

Workstations must be configured and used in a secure manner. To secure a workstation, a staged approach is recommended for implementation of security practices in the following areas:

- Planning and executing the deployment of workstation.
- Configuring workstation to help make them less vulnerable to attack.
- Maintaining the integrity of deployed workstation.
- Improving user awareness of security issues.

2.2 Planning

Securing desktop workstations should be a significant part of the network and information-security strategy because sensitive information is often stored on workstations, which are connected to the rest of the networked world. It can eliminate many networked systems vulnerabilities and prevent many security problems if workstation is configured securely before its deployment. Vendors typically set computer defaults to maximise available functions, so usually there is a need to change defaults to meet the organisation's security requirements.

2.2.1 Purpose of Workstation

Following points should be considered to secure a workstation:

- What categories of information will be stored on the workstation?
- What categories of information will be processed on the workstation (but retrieved from and stored on another workstation)?
- What are the security requirements for that information?
- What network service(s) will be provided by the workstation?
- What are the security requirements for those services?

2.2.2 Network Service Software

Many operating system vendors bundle network service software for both clients and servers. For major services, however, third party vendors may provide products that offer much better security. When making a choice, special attention should be paid to the ability of candidate packages to meet the organisation’s security requirements, and the same should be documented. Also identify other applications or utility software that are

required to be installed on the computer. Include not only user-oriented application software, but also system-related software and security-related software.

2.2.3 User Categorisation

For workstations, the categories of users should be defined. The categories should be based on user roles that reflect their authorised activity. The roles are often based on similar work assignments and similar needs for access to particular information resources-system administrators, software developers, data entry personnel, etc. If appropriate, remote users should be categorised as temporary or guest users.

2.2.4 User Privileges

Create a matrix that shows the users or user categories cross-listed with their privileges. The privileges are customarily placed in groups that define what system resources or services a user can read, write, change, execute, create, delete, install, remove, turn on, or turn off.

2.2.5 Develop and follow a Documented procedure for installing an Operating system

During installation of Operating System, all the steps made to implement the security policy of the organisation, should be documented and all the parameters that are set should be described. The installation procedure should also specify the vendor's security-related updates or patches that are to be applied to the operating system. If possible, have a single person perform the installation procedure for each workstation and capture each installation step in a documented manner such as through using a checklist.

2.3 Installation and Configuration

2.3.1 OS and Application S/W Hardening

- OS media should be procured only from an authorised vendor of the manufacturer.
- To patch up the vulnerabilities and loopholes of the OS, install all the latest service packs, security patches, hot-fixes, OS updates, etc. as available and applicable for this version at the time of installation. These patches/updates etc. are available from the vendors as well as from their websites.
- Boot on “OS banner” should be disabled, if possible.
- Initially, all the ports should be closed/disabled and may be enabled/opened as and when required.
- Turn off all network services that are not needed.
- Define how long the computer or application can be used. Create a mandatory automated logoff policy based on inactivity or time of day.

- Disable application features that expose vulnerability through configuration changes.
- Control access to settings, control panels and run functions. Define who has access to applications by location, time of day or time period.

2.3.2 Stick to Essentials on the Network

Most desktop workstations do not need all the settings enabled by default, so the operating system should be configured to provide only the services specified in the deployment plan.

- Disable and remove all the network services that are not required by the deployment plan. It is recommended that workstation should be configured to offer only the services as per the deployment plan.
- It is recommended to use the configuration principle "deny first, and then allow", that is, turn off as many services and applications as possible and then selectively turn on those that are essential.

2.3.3 Configure multiple computers using a tested model replication procedure

When deploying several computers, especially desktop workstations, across an organisation, it is better to configure one appropriately and then propagate that configuration to all the others. It should be ensured that this is done in a secure manner, especially if a network is used for propagation. This helps in establishing a consistent level of security on all the computers to LAN. It also facilitates consistent updating of all computers as and when necessary.

2.3.4 Configure Network Service clients to Enhance Security

For the network services, organisation’s deployment plan should include electronic mail, access to the Web, Domain name services, file transfers, and access to corporate databases. For each service, the workstation should be configured as a client or as a server mode. Workstations are normally configured as clients for several network services. Therefore, these should be configured for the planned behavior of those clients: the levels of access required, the type of access (read, write, etc.), and other aspects of the configurations required for client software.

2.3.5 Access to Information

For many resources, such as program and data files, the access controls provided by the operating system are the most obvious means to enforce access privileges. Also, consider using encryption technologies to protect the confidentiality of sensitive information. In some cases, protection mechanisms will need to be augmented by policies that guide user's behavior related to their workstations.

2.3.6 LAN Security

Many organisations use a broadcast technology such as Ethernet for their local area networks. In these cases, information traversing a network segment can be seen by any computer on that segment. So, only trusted computers should be placed on the same network segment, or else the information should be encrypted before transmitting it. For securing LAN, the guidelines, to be followed, are :

- If, a workstation is connected to LAN, users should not be allowed to use a modem.
- Unauthorised copies of software should be removed from all the systems connected through LAN.
- If users are allowed to install personal software on their workstations, ensure that:
    - the software is licensed; and
    - the software does not compromise any security mechanisms implemented on the LAN. For example, software that can be used to "sniff" network traffic should not be permitted on the LAN.

2.3.7 Password

There should be a password policy in the organisation. The most common method of authentication is password. The responsibility of selecting a password, that is hard to guess, falls on users. To decrease the chances of guessing password, user must select a hard-to-guess, or strong password. Detailed procedure for password selection has been provided in the Server OS Guidelines.

2.4 Maintenance & Operations

- Keep the operating system and application software up to date. Updates are available from vendors on a regular basis.

- Delete all un-sanctioned programs and directories from the workstation. They can be cleverly renamed as keystroke-capturing programs, network sniffer programs, or viruses.

- To prevent the last logged-in user name from being displayed, use security procedures at installation stage. For example, in Windows based systems when Ctrl-Alt-Del is pressed, a login dialog box appears which displays the name of the last user who logged in to the computer, and makes it easier to know a user's name that can later be used in a password-guessing attack. This can be disabled using the security templates provided on the installation CD.

- Enforce system file hardening and configuration against attack from virus, worms, Trojan horse or other malicious software.

- Use keywords to restrict data from being sent or received through the Internet.
- Lock folders and files to prevent unwanted access.
- Prevent rename, delete, copy, move or changes to file attributes.
- Customise application to show only desired menu options.
- Restrict access to dialog boxes such as print, save, import, etc.

2.4.1 Protection from Viruses, Trojan Horse and Malicious scripts

Install virus protection software on the workstation, and update it on a regular basis. Updates for the new viruses are generally made available every week. Configure the Anti-virus software properly, so that it actively scans all incoming objects for virus infections.

- Never execute a program (".exe" file) if one does not know what it is/does. This is particularly the case for files that are received via e-mail as attachments, or are downloaded from a website that can not be trusted.
- Make sure that on every occasion, whenever diskettes and other media are brought in, they are checked for viruses.
- Do not install / use illegal or "pirated" software.
- Do not use shareware unless absolutely sure that the software is free of viruses.
- Do not install any software without permission of the System Administrator.
- If any program is downloaded from Bulletin Board or the Internet, scan it for viruses before using.
- Do not install or play games on the computers. Games are commonly used as a way to spread viruses.
- Make sure that diskettes used to store software programs are write-protected. This prevents viruses from being copied onto such diskettes.
- If a computer has come with pre-loaded software or its hard drive is pre-formatted, scan the hard drive for viruses before using the computer.
- Do not boot computers with any diskette that has not been scanned for viruses.
- Public-domain software should not be used until it is tested and allowed by SA.

2.4.2 Deployment of Personal Firewall/IDS

- To prevent intruders from hacking into systems via LAN / Internet connection firewall must be installed & configured.
- The "intruder alert" facility, should be activated and all alerts should be acted upon.
- To detect unauthorised access of a system, IDS must be installed & configured.

2.4.3 System Access Control

- Allow file sharing on machines after securing them, and that too only to authorised users only. Make sure that object, device, and file access controls are appropriate. Protect files and folders by making them as read-only for shared use.
- Do not allow anonymous access of any kind (e.g., FTP, dial-up) to a workstation

2.4.4 Internet access, S/w Download & E-mail Attachments

- Only allow users' access to approved websites.
- Do not open e-mail received from Unknown person.
- Define the time period of Internet access and email usage.

2.4.5 Audit Trails & Logs

Log files may be the only record of suspicious behavior. These should be activated. Log files are required for the following:

- To alert for the suspicious activity that requires further investigation.
- To determine the extent of an intruder's activity.
- To recover operating system software.
- To provide information required for legal proceedings
- To investigate workstation hard disks on a regular basis for suspicious files. Use a naming convention for files and directories. Be sure to look for hidden files and directories.
  Security audits should be done periodically to expose system vulnerabilities.

2.4.6 Data Encryption

- Consider employing a file encryption program if the information stored on a workstation is highly confidential. Similarly, consider a mail program that supports encryption (S/MIME or PGP), if sending highly confidential information in messages.

- Enable Encrypting File System. This will help in preventing a hacker from accessing files by physically mounting the hard drive on another PC and taking

ownership of files. Be sure to enable encryption on Folders, and not files. All files that are placed in that folder will be encrypted automatically.

2.4.7 Backups

- Always backup files & folders periodically using standard backup utilities.
- Make separate backups of data files and software and store backup diskettes/tapes in a safe and secure location away from computer. Backups may be the only source to recover any destroyed file.
- Always backup the data before leaving the workstation.

2.4.8 Data recovery from Backups

Recovery tools should be installed on the workstation like hard disk recovery software. With the help of such tools workstation OS is recovered without loss of time.

2.5 Incident Handling

In case of occurrence of any incident, like workstation Break-in, DoS attack, Trojan Horse attack, etc, steps should be defined how to know about incident, incident reporting and recovery thereafter.

2.5.1 What is an Incident ?

An Incident is an act of violating an explicit or implied security policy, assuming there exists a security policy in the organisation. The types of activity considered as violation of a typical security policy are characterised below :

- Security violation in which a system resource is exposed or is potentially exposed to unauthorised access.
- Unwanted disruption or denial of service.
- Any adverse event which compromises some aspect of computer or network security.
- Unauthorised use of a system for the processing or storage of data.
- Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction or consent.

2.5.2 Incident detection

Tools installed for monitoring workstation performance and incident detection help in detecting an incident. The symptoms of an incident could be like sudden degradation in workstation performance, workstation compromise, failure of service(s), abuse etc.

2.5.3 Safeguard measures after incident

When a system administrator finds some abnormal behavior in workstation performance; or alarms through incident detection tools are noted, the following steps should be taken :

- Change administrator password of the workstation
- Disconnect the workstation from network, depending upon the severity of the incident.

2.5.4 Incident reporting

An Incident should immediately be informed to CERT-In by means of telephone, fax, email or web. The site address of CERT-In is www.cert-in.org.in. After reporting the incident to CERT-In, advisory notes of CERT-In should be followed for recovering from incident.

2.6 References

- http://www.cert.org/securityimprovement/modules
- http://www.utoronto.ca/security
- http://www.its.uiwa.edu/cio/itsecurity/bestprac/

3. Web Server Security Guidelines

3.1 Introduction

A web server is a program, which listens for http requests on a TCP/IP port (normally either port 80 or port 443) and serves html pages in response.

There are several web servers currently in the market. The most popular are:

- Apache
- SunONE
- Internet Information Server (IIS)
- NCSA

Specific methods for securing a web server largely depend on the operating system (OS) and web server software used. Apache can run on the Windows platform, but usually runs on Linux or some other flavor of Unix. IIS runs on the Windows server platforms. SunONE is the sum of sites running iPlanet-Enterprise, Netscape-Enterprise, Netscape-FastTrack, Netscape-Commerce, Netscape-Communications, Netsite-Commerce & Netsite-Communications.

Once a web server is set up, it is an invitation to the world to connect to it. The users may include potential hackers as well. The attackers may deface the web site, causing embarrassment. Or they may download confidential information, or steal credit card information. Or they may use the host as part of a distributed denial-of-service (DDOS) attack on another host.

In a defacing incident, the Web Manager may come to know that the web site has been hacked. But in other cases, it may not even be known that the site has been compromised. Hence, the security of a Web Server is of prime importance.

Before going into the specifics of securing computers and their services, we need to define the policies for how and by whom the Web Server will be used. This includes an acceptable use policy (AUP) for all users and a security policy. This policy is intended to define the rights and responsibilities of both the users and system administrators as well as define who these people are. This is really the first step in the security of any server as it sets out the rules that everyone is to follow. And when the rules are broken, the AUP also defines what happens to those who have broken them.

3.2 Planning

The organization should include explicit security requirements when selecting servers. There are many server vendors, and the security capabilities of their products vary accordingly. Many of the known and frequently exploited network server

vulnerabilities apply only to certain products and platforms. If one considers security requirements when selecting servers, then it is possible to choose products with fewer vulnerabilities or select better security-related features, which can result in a substantially more secure site. This makes the long-term operation of web site more economical because by reducing the costs associated with administration tasks (such as patching systems) as well reduce costs caused by intrusions and their effects.

The Web Servers are tempting targets for intruders because of the following reasons:

- Public servers often have publicly known host names and IP addresses.
- Public servers may be deployed outside an organization's firewall or other perimeter defenses.
- Servers usually actively listen for requests for services on known ports, and they try to process such requests.

The vulnerabilities are exploited by the intruders due to the operational issues not addressed by the System Administrators. Improper configuration or operation of the Web server can result in the inadvertent disclosure or alteration of confidential information.

Some of the effects of Web Server being compromised are as follows.

- Information assets of the organization are at risk.
- Information about the configuration of the server or network could be exploited for subsequent attacks
- Information about who requested which documents from the server is known
- Sensitive customer or user information is at risk
- The intruder may change the information stored on the Web server host machine, particularly the information intended to publish
- Execute unauthorized commands or programs on the server host machine including ones that the intruder has installed
- Gain unauthorized access to resources elsewhere in the organization's computer network
- Launch attacks on external sites from the server host machine, thus concealing the intruders' identities, and perhaps making the organization liable for damages
- Users can be disabled from accessing the Web site if all of its resources are consumed by a denial-of-service attack.

It is therefore essential to secure a Web Server through the following steps:

- Installing a Secure Server
- Configuring Web Server Software and the underlying Web Server host operating system
- Maintaining the Web Server's Integrity

3.3 Installation & Configuration

It is recommended that a web server deployment plan be developed. It should take into consideration security issues related to the network architecture and the location of the Web servers. The deployment plan also involves following practices for increased security:

a. Determining how the Web Server will be connected to the network
b. Identifying the security concerns related to day-to-day administration of the Server.
c. Identifying the services offered by the server.
d. Identifying the network services that will be provided on the server.
e. Identifying the users or categories of users of the Web Server
f. Deciding how users will be authenticated and how authentication data will be protected
g. Developing intrusion detection strategies for the server
h. Documenting procedures for backup and recovery of information resources stored on the server.
i. Determining how network services will be maintained or restored after various kinds of faults

Practices that should be adopted by organization for installing and configuring web server are as follows:

3.3.1 Isolate the Web server from public networks and the organization's internal networks.

Care must be taken while placing a public Web server on an organization's network. It is highly recommended that the server be placed on a separate, protected subnetwork. This will ensure that traffic between the Internet and the server does not traverse any part of the private internal network and that no internal network traffic is visible to the server. To accomplish this, following steps may be taken:

- Place the web server on a subnet isolated from public and internal network.
- Use firewall technology to restrict traffic between a public network and the web server and between the web server and the internal network.
- Place the servers providing email, directory and database services in support of the web site on a protected subnetwork.
- Disable all source routing functions in the firewalls and routers protecting the public web server.
- Disable IP forwarding and source routing on the web server and the server hosts that provide supporting services.

3.3.2 Configure the Web server with appropriate object, device, and file access controls. This is necessary for the following reasons

- To limit access to the Web server software
- To apply access controls specific to the Web server where more detailed levels of access control are required

To configure this, following steps may be taken:

- The web server should be configured to execute under a unique individual user and group identity. This is important for implementing access controls on various files, viz. Server log files, system software and configuration files, password files etc.
- The protection needed for various files, devices and objects specific to the web server should be identified.
- Time-outs and other controls to mitigate the effects of DOS attacks should be configured.
- The file serving of web server file listings should be disabled.

3.3.3 Identify and enable Web-server-specific logging mechanisms.

Web server logs are needed to:

- Alert about suspicious activity that requires further investigation
- Determine the extent of an intruder's activity
- Help to recover the systems
- Help to conduct an investigation
- Provide information required for legal proceedings

This can be accomplished by

- Identifying the web server software information to be logged, viz. Transfer log, Error log, Agent log, Referer log etc.
- Logging mechanism may also be required for capturing the performance of various programs, scripts, and plug-ins supported by the web server.

3.3.4 Consider security implications before selecting programs, scripts, and plug-ins for the Web server. To overcome the vulnerabilities following steps may be undertaken:

- Programs, scripts and plug-ins should be selected from a trustworthy source.

- The functionality that the external programs provide should be well understood.

3.3.5 Configure the Web server to minimize the functionality of programs, scripts, and plug-ins.

Security vulnerabilities can be easily introduced in the acquisition, installation, configuration, deployment, and operation of external programs (Programs, scripts, and plug-ins). To accomplish this following steps may be taken:

- Verification of the acquired copy of the external program to check if it is authentic.
- The external program acquired should be tested prior to putting it on the public web server.
- Security tools for checking vulnerabilities in these acquired programs should be used.
- Server Side Include functionality use should be disabled or restricted.
- Execution of external programs present in the web server should be disabled. These external programs may be present in the default web server configuration, they should be located and disabled if not essential.
- Configure the web server host operating system and the web server software access controls to restrict access to external programs.

3.3.6 Configure the Web server to use authentication and encryption technologies, where required.

Without strong user authentication, one may not be able to restrict access to specific information by authorized users. Before placing any sensitive or restricted (i.e. not for public consumption) information on a public Web server, one needs to determine the specific security and protection requirements and confirm that the available technologies, like SSL (Secure Socket Layer), S/HTTP (Secure Hypertext Transport Protocol), and SET (Secure Electronic Transaction). can meet these requirements.

3.3.7 Install security tools like whisker, ISS Internet Scanner, Nikto (A more comprehensive web scanner), SPIKE Proxy an open source HTTP proxy for finding security flaws in web sites. These tools help in finding the flaws in the web site as well as web server.

3.4 Operations & Maintenance

3.4.1 Maintain an authoritative copy of the Web site content on a secure host. The authoritative (i.e., verified, correct, trusted) copy of the public Web site content needs to be stored on a host that is separate from (and more secure than) the

public Web server. The more secure host should preferably be on the internal network of the organization and protected behind one or more firewalls.

Protect the Web server against common attacks. To accomplish this following actions are essential:

- Install Security tools like IDS, Integrity Checkers, Blocking and Filtering tools.
- Update the installed detection tools to detect new attack patterns or events
- Reduce attacks by updating firewall filtering mechanisms to deny new attacks
- Temporarily disable specific services that might be vulnerable to attack
- Use secure methods for restoration

3.4.2 The best practices for the operation of a web server can be summarized as below:

- Place the web server(s) in a DMZ. Set the firewall to drop connections to the web server on all ports but http (port 80) or https (port 443).
- Remove all unneeded services from the web server, keeping FTP (but only if it is required) and a secure login capability such as secure shell. An unneeded service can become an avenue of attack.
- Disallow all remote administration as far as possible.
- Limit the number of persons having administrator or root level access. Keep a record of the persons allowed such access.
- Log all user activity and maintain those logs either in an encrypted form on the web server or store them on a separate machine on the Intranet of the organization.
- Monitor system logs regularly for any suspicious activity. Install some trap macros to watch for attacks on the server. Create macros that run every hour or so that it would check the integrity of passwd and other critical files. When the macros detect a change, they should send e-mail to the system manager.
- Remove ALL unnecessary files from the scripts directory for example /cgi-bin in Unix.
- Remove the "default" document trees that are shipped with Web servers.

- Apply all relevant security patches as soon as they are announced.

- If the machine must be administered remotely, require that a secure capability such as secure shell is used to make a secure connection. Do not allow telnet or non-anonymous ftp (those requiring a username and password) connections to this machine from any untrusted site. It would also be good to limit these connections only to a minimum number of secure machines and have those machines reside within the Intranet of the organization.

- Run the web server in a safe part of the directory tree so it cannot access the real system files.

- Run the anonymous FTP server in a safe part of the directory tree that is different from the web server's tree.

- Do all updates from the Intranet. Maintain the web page originals on a server on the Intranet and make all changes and updates here; then "push" these updates to the public server through an SSL connection. If this is done on an hourly basis, this practice will help avoid having a corrupted server exposed for a long period of time.

- Scan the web server periodically with tools to look for vulnerabilities.

- Have intrusion detection software monitor the connections to the server. Set the detector to alarm on known exploits and suspicious activities and to capture these sessions for review. This information can help recover from an intrusion and strengthen the defenses.

3.5 Incident Handling

A web server administrator should take the following steps after discovering a successful compromise:

- Isolate compromised system(s) or take steps to contain attack so additional evidence can be collected
- Consult, as appropriate, with management, legal counsel, and law enforcement expeditiously and consult the organization's security policy.
- Investigate "similar" hosts to determine if the attacker also has compromised other systems
- Analyze the intrusion, including:
  - Modifications made to the system's software and configuration
  - Modifications made to the data
  - Tools or data left behind by intruder
  - Review system logs, intrusion detection, and firewall log files.
  - Restore the system

- Install clean version of operating system, or Restore from backups
  - Disable unnecessary services
  - Apply all patches
  - Change all passwords (even on uncompromised hosts as required)
- Reconfigure network security elements (firewall, router, IDS) to provide
  - Additional protection and notification.
  - Test system to ensure security
  - Reconnect system to network
  - Monitor system and network for signs that the attacker is attempting to access the system or network again.
- Report incident to CERT-In.
- Document lessons learned.

3.6 References

- http://www.cert.org/security-improvement/
- http://security.uchicago.edu/
- http://www.ciac.org/ciac/
- http://csrc.nist.gov/publications
- http://www.garykessler.net/library/web_security.html

4. Mail Server Security Guidelines

4.1 Introduction

Electronic mail (email) is the most popularly used system for exchanging information over the Internet (or any other computer network). After Web servers, mail servers are the hosts on an organization's network that are most often targeted by attackers. This document is intended to assist organizations in installing, configuring, and maintaining secure mail servers and mail clients. This document discusses about –

- Planning of mail server: This section suggests about client access methods, preferred location of mail servers, encryption technologies etc.
- Configuration and Installation: Which includes hardening the operating system, mail server application, mail client application and network to prevent malicious entities from directly attacking the mail server.
- Maintenance and Incident handling of mail servers.

4.2 Planning

Organizations should carefully plan and address the security aspects of the deployment of a Mail server. The plan must include selection of mail server, selection of client access protocols, location of mail server in the network, antivirus policy, network security policy etc.

4.2.1 Location of Mail Server

It is important to properly plan the location of a mail server within the network of an organization.

A typical position of Mail server will be to place it in the DMZ. A two-firewall DMZ configuration offers superior protection over a router-firewall DMZ since the dedicated firewalls can have a more complex and powerful security rule set. In addition, the dedicated firewall is often able to analyze incoming and outgoing mail traffic, it can detect and protect against application layer attacks aimed at the mail server. Depending on the configuration of the firewalls and the level of traffic the DMZ receives; this type of DMZ may result in some performance degradation.

For organizations which desire the security of the two firewall DMZ but do not have the resources to purchase two firewalls, there exists another option called the "service leg" DMZ. In this configuration, a firewall is constructed with three (or more) network interfaces. One network interface attaches to the border router, another interface attaches to the internal network, and a third network interface connects to the DMZ.

4.2.2 Client access methods

Several methods exist for users to access their mailboxes. That can be a command line access (using pine or mail etc) or can be on some standard protocol like POP3 or IMAP based client.

Allowing users, to have access to a command-line interface is a significant security risk. Adoption of protocols like POP3 or IMAP can mitigate these risks.

4.2.3 Using a mail Gateway

A mail gateway acts as a proxy between the real mail server and the Internet. All messages and communications must go through proxy before they are forwarded to the mail server. This breaks the direct line of communication between the Internet and the mail server making it much more difficult to attack the mail server. Since the mail gateway generally requires only limited functionality, it is much easier to harden and secure than a fully functional mail server.

4.2.4 Protecting Email from Malicious Code

4.2.4.1 Virus Scanning

To protect against viruses and other malicious code, it will be necessary to implement scanning at one or more points within the email delivery process. Virus scanning can be implemented on the firewall as the mail data enters the organization's network, on the mail server or mail relay and/or on the end user's host. Scanning for viruses at the firewall (application proxy) or mail relay is a popular option In this instance, the firewall or mail relay intercepts messages before they reach the organization's mail server. The firewall or mail relay scans each message and if no viruses are found, forwards the message on to the organization's mail server for delivery. The firewall or mail relay listens on the TCP port 25 for SMTP connections, receives the message, scans the message, then forwards the message on to the mail server, which is configured to listen on an unprivileged, unused port, rather than the usual port 25.

4.2.4.2 Content Filtering

Content filtering works in a similar manner to virus scanning at the firewall or mail server except that it takes this concept in a different direction. It looks at the content of emails for characteristics other than malicious code that might be of interest to the organization. When implementing file-type restrictions and virus scanning, only a certain level of security is provided. The contents of an email message or its attachments could prove much more damaging to an organization than a virus or rogue executable. For this case, some sort of content filtering mechanism should be employed.

In general, rules are defined to forward, quarantine, park, clean, block or delete any data passing through the server depending the results of the scan. Typical items that would be caught by the filter and possible action taken on them could be as follows:

- Email that contains suspicious active content (e.g., ActiveX, JavaScript) is stripped of the active code and forwarded to recipient.
- Spam email may be deleted
- Extra large files might be parked for delivery at off peak hours.

4.2.5 Adoption of Encryption Technologies

Common factors that can influence the choice of an encryption algorithm include the following items

- Required security
  Value of the data to the organization and/or other entities. The more valuable the data, the stronger the required encryption.
- Time value of data.
  If data are valuable for only a short time period (e.g., days as opposed to years), then a weaker encryption algorithm can be used. An example would be passwords that are changed on a daily basis because the encryption needs to protect the password for only a 24-hour period.
- Threat to data.
  The higher the threat level, the stronger the required encryption.
- Required performance.
  Higher performance requirements may necessitate weaker encryption, but this is not normally a consideration with email. System resources. Less resources such as processor speed and memory size may necessitate weaker encryption, but are not typically a factor in email.
- Import, export, or usage restrictions.
  Encryption schemes supported by mail client applications and operating systems.
- Other protective measures may reduce the need for stronger encryption. An example would be using protected methods of communications such as dedicated circuits instead of the public Internet.

4.3 Configuration

The first step in securing a mail server is securing the underlying operating system. Most commonly available mail servers operate on a general-purpose operating system. Many security issues can be avoided if the operating systems underlying mail servers are configured appropriately.

Following steps should be taken to secure a mail server

4.3.1 Securely Installing the Mail Server

- Install the server software on a dedicated host
- Install minimal Internet services required
- Apply all patches or upgrades to correct for known vulnerabilities
- Create a dedicated physical disk or logical partition (separate from operating system and server application) for mail boxes
- Remove or disable all services installed by the mail server application but not required (e.g. FTP, remote administration, etc)
- Remove all vendor documentation from server
- Remove any example or test files from server
- Reconfigure SMTP, POP, and IMAP service banner (and others as required) NOT to report mail server and operating system type and version (this may not be possible with all mail servers).
- Disable dangerous or unnecessary mail commands (e.g., VRFY and EXPN)

4.3.2 Configuring Operating System and Mail Server Access Controls

- Limit the access of the mail server application to a subset of computational resources
- Limit the access of users through additional access controls enforced by the mail server, where more detailed levels of access control are required.
- Apply proper access control List for the following file types
  - Application software and configuration files
  - Files directly related to security mechanisms:
  - Password hash files and other files used in authentication
  - Files containing authorization information used in controlling access
  - Cryptographic key material used in confidentiality, integrity, and non-
  - repudiation services.
  - Server log and system audit files
  - System software and configuration files.
- To mitigate the effects of certain types of DoS attacks, configure the mail server to limit the amount of operating system resources it can consume. Some examples include:
  - Install users' mailboxes on a different hard drive or logical partition
  - than the operating system and mail server application.
  - Limit the size of attachments that are allowed.
  - Ensure log files are stored in a location that is sized appropriately.
- Protecting Email from Malicious Code
  Filter potentially dangerous attachment types (e.g., .vbs, .ws, .wsc file extensions) at the mail server or mail gateway, while conducting virus scans on allowed file types.

4.3.3 Authenticate Mail Relaying

Two methods are available for controlling mail relay.

- The first is to control the subnet or domain from which messages are being sent. This method is effective if the perimeter of the messaging system resides within known address ranges.
- The second method is to apply Authenticated relaying (SMTPAUTH) which is the SMTP extension that supports user authentication.

4.3.4 Unsolicited Bulk Email (Spam mail)

To control spammed messages, administrators must address two concerns:

- Ensure that UCE (Unsolicited Bulk Email) cannot be sent from mail servers they control and Implement inbound message control
- Mail server administrators can block the inbound mails from mail servers that are often used to send unsolicited email messages.

4.3.5 Securing network infrastructure

Router/Firewall Configuration

A firewall or router (acting as a firewall) that is protecting a mail server should be configured to block all access to the mail server from the Internet except TCP port 25 (SMTP), TCP port 110 (POP3), TCP port 143 (IMAP), TCP port 398 (Lightweight Directory Access Protocol [LDAP]), and TCP port 636 (Secure LDAP).

To successfully protect a mail server using a firewall, ensure that it is capable of and configured to support the following:

- Control all traffic between the Internet and the mail server
- Block all inbound traffic to the mail server except that traffic which is required. This usually includes one or more of the following protocols:
  TCP port 80 and 443 (Web mail)
  TCP port 25 (SMTP)
  TCP port 110 (POP3)
  TCP port 143 (IMAP)
  TCP port 389 (LDAP)
  TCP port 636 (secure LDAP)
- Block (in conjunction with the intrusion detection system IP addresses or subnets that the IDS reports are attacking the organizational network Notify the network or mail server administrator of suspicious activity through an appropriate means (e.g., page, email, network trap)
- Provide content filtering
- Provide virus scanning
- Protect against DoS/DDoS attacks
- Log critical events, including the following details:

Time/date
Interface IP address
Vendor specific event name
Standard attack event (if exists)
Source and destination IP address
Source and destination port numbers
Network protocol used by attack.

4.3.6 Secure Mail Client

The most important step in securing an email client is to ensure that all users are using the latest and/or most secure version of the mail client with all necessary patches applied. A secured mail client should adhere to the following

- Disable automatic message preview.
- Disable automatic opening of next message.
- Disable processing of active content.
- Disable automatic login (remember password and user name)

4.4 Operations and Maintenance

Mail server administrators are system architects responsible for the overall design, implementation, and maintenance of a mail server. Mail server and network administrators must address the security requirements of the specific system(s) for which they are responsible.

4.4.1 Logging

Logging is a cornerstone of a sound security posture. Logging the correct data and then monitoring those logs is critical. Reviews should take place on a daily to weekly basis and when a suspicious activity has been noted or a threat warning has been issued. Automated Log File Analysis Tools can be used for analysis.

The following generic type of logging is recommended. Set logging on the mail server to the most detailed level available.

- Local host related logging
  Mail server configuration errors (e.g., mismatch with DNS: local configuration error, out of date alias database)
  Lack of system resources (disk space, memory, CPU)
- Connection related logging
  Logons (successful and failed)
  Security problems (e.g., spamming)
  Lost communications (network problems)
  Protocol failures
  Connection timeouts
  Connection rejections

Use of VRFY and EXPN commands

- Message-related logging
  Malformed addresses
  Creation of error messages
  Delivery failures (permanent errors)

Messages being deferred (transient errors).

4.4.2 Backup and recovery

A proper backup policy should be in place keeping in consideration of the organizations need. Backup should be taken on the following types

- Configuration files
- Mail Boxes
- Mail queues at specified time interval
- Logs

4.4.3 Security Testing

- Vulnerability Scanning
  Vulnerability scanners are automated tools that are used to identify vulnerabilities and misconfiguration of hosts. Many vulnerability scanners also provide information about mitigating discovered vulnerabilities.
- Penetration Testing
  The purpose of penetration testing is to exercise system protections (particularly
  human response to attack indications) by using common tools and techniques developed by hackers. This testing is highly recommended for complex or critical systems.

4.5. Incident Handling

The first step in recovering from a compromise is to create and document the required policies and procedures for responding to successful intrusions prior to an intrusion. The response procedures should outline the actions that are required to respond to a successful compromise of the mail server and the appropriate sequence of these actions

A mail server administrator should take the following steps after discovering a successful compromise:

- Report incident to **CERT-In**.
- Consult the organization's security policy.
- Isolate compromised system(s) or take steps to contain attack so additional evidence can be collected

- Consult, as appropriate, with management, legal counsel, and law enforcement expeditiously
- Investigate "similar" hosts to determine if the attacker also has compromised other systems
- Analyze the intrusion, including:
  - Modifications made to the system's software and configuration
  - Modifications made to the data
  - Tools or data left behind by intruder
  - Review system logs, intrusion detection, and firewall log files.
- Restore the system
  Install clean version of operating system, or Restore from backups (this option can be more risky, as the backups may have been made after the compromise and restoring from a comprised back may still allow the attacker access to the system).
- Disable unnecessary services
- Apply all patches
- Change all passwords (even on uncompromised hosts as required)
- Reconfigure network security elements (firewall, router, IDS) to provide additional protection and notification.
- Test system to ensure security
- Reconnect system to network
- Monitor system and network for signs that the attacker is attempting to access the system or network again.
- Document lessons learned.

4.6. References

- http://csrc.nist.gov/publications/nistpubs/index.html
- http://www.ietf.org/rfc/rfc0822.txt
- http://www.ietf.org/rfc/1870.txt

5. Firewall Security Guidelines

5.1 Introduction

Firewall technology has improved substantially since it was introduced in the early 1990s. The early firewall technology started with simple packet-filtering firewalls and progressed to more sophisticated firewalls capable of examining multiple layers of network activity and content. As the Internet has developed into the modern, complex network of today, Internet security has become more problematic, with break-ins and attacks now so commonplace as to be considered part of doing business. Now, firewall technology is a standard part of any organizations network security architecture.

Modern firewalls are able to work in conjunction with tools such as intrusion detection monitors and email/web content scanners for viruses and harmful application code. But firewalls alone do not provide complete protection from Internet-borne problems. As a result, they are just one part of a total information security program. Generally firewalls are viewed as the first line of defense, however it may be better to view them as the *last* line of defense for an organization; organizations should still make the security of their internal systems a high priority. Internal servers, personal computers, and other systems should be kept up-to-date with security patches and anti-virus software.

5.1.1 Document Purpose and Scope

This document provides introductory information about firewalls and firewall policy primarily to assist those responsible for network security. It addresses concepts relating to the design, selection, deployment, and management of firewalls and firewall environments. This document is not intended to provide a mandatory framework for firewalls and firewall environments, but rather to present suggested approaches to the topic.

5.1.2 Audience and Assumptions

The intended audience is technical personnel, as well as management personnel who might require a technical basis for supporting a decision-making process. Non-technical management and those wishing to increase their knowledge of firewalls may find this document useful as well. This document assumes some knowledge of TCP/IP (Transmission Control Protocol/Internet Protocol), the protocol suite used by the Internet, as well as various other aspects of networking and information security.

5.2 General Guidelines

5.2.1 Organizations should view firewalls as their first line of defence from external threats; internal security must still be a top priority. Internal systems must be patched and configured in a timely manner.

5.2.2 Organizations should use firewalls to secure their Internet connections and their connections to other networks. Proper Firewall should be framed and followed

5.2.3 At remote locations, users should use personal firewalls and firewall appliances to secure their connections to the Internet and Internet Service Providers

5.2.4 Organizations must monitor incident response team reports and security websites for information about current attacks and vulnerabilities. The firewall policy should be updated as necessary. A formal process should be used for managing the addition and deletion of firewall rules.

5.2.5 Organizations should recognize that all system administration, especially firewall administration, requires significant time and training. Organizations should ensure that their administrator receive regular training so as to stay current with threats and vulnerabilities.

5.2.6 Ensure that the Firewall and the network cabling related to it are physically secured. Physical access to the firewall or the related network cabling provides opportunities for an intruder to bypass the firewall itself

5.3 Firewall Selection

5.3.1 Organizations should examine carefully which firewall and firewall environment is best suited to their needs.

5.3.2 A firewall environment should be employed to perform the following general functions:

a) Filter packets and protocols
b) Perform Stateful inspection of connections
c) Perform proxy operations on selected applications
d) Log traffic allowed and denied by the firewall
e) Provide authentication to users using a form of authentication that does not rely on static, reusable passwords that can be sniffed

5.3.3 The firewall should be able to filter packets based on the following characteristics:

a) Protocol, e.g., IP, ICMP
b) Source and destination IP addresses
c) Source and destination ports (which identify the applications in use)
d) Interface of the firewall that the packet entered

5.3.4 The proxy operations should, at a minimum, be operable on the content of SMTP, FTP, and HTTP protocol traffic.

5.3.5 Organizations may find that they need several firewalls to accomplish these items.

5.4. Firewall Environment

5.4.1 A boundary router or other firewall should be used at the Internet connection to create an external DMZ. Web servers and other publicly accessible servers should be placed on the DMZ so that they can be accessible as needed and still have some protections from the firewall. Internal users should be protected with an additional firewall.

5.4.2 Figure 1 shows a general picture of a firewall environment. For remote users, a VPN should be considered as an alternative. While a dial-in server could be located behind a firewall, it is more secure to combine it with a VPN server located at the firewall or external to the firewall so that remote connections can be securely authenticated and encrypted.

5.4.3 Intrusion detection is recommended as an additional safeguard against attacks. Figure 1 shows network-based IDS; host-based IDS could be used on systems where high-speed throughput is not an issue, e.g., email servers.

5.4.4 Network address translation and split DNS are recommended to hide internal system names and addresses from external networks.

5.4.5 Remote users should use personal firewalls or firewall appliances when connecting to ISPs, regardless of whether dial-in or higher-speed connections are used.

5.5 Firewall Policy

5.5.1 A general risk assessment and a cost benefits analysis should be performed on the network applications that the organization or agency has chosen to use. This analysis should result in a list of the network applications and the methods that will be used to secure the applications.

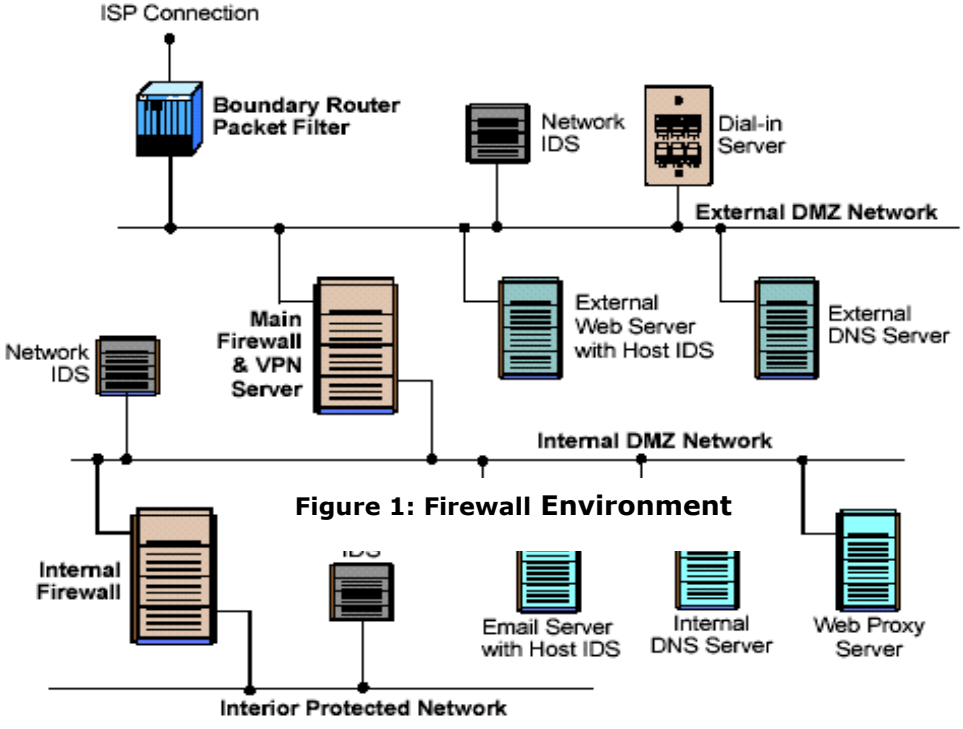

Figure 1: Firewall Environment

5.5.2 A firewall policy should be written to include a network applications matrix (or similar specification). This policy should be maintained and updated frequently as new attacks or vulnerabilities arise or as the organization's needs in terms of network applications change. This policy should make the process of creating the firewall rule set less error-prone and more verifiable, since the rule set can be compared to the applications matrix.

5.5.3 The default policy for the firewall for handling inbound traffic should be to block all packets and connections unless the traffic type and connections have been specifically permitted. This approach is more secure than another approach used often: permit all connections and traffic by default and then block specific traffic and connections.

5.5.4 Organizations should consider using outbound traffic filtering as a technique for further securing their networks and reducing the likelihood of internally based attacks.

5.5.5 As a general rule, any protocol and traffic that is not necessary, i.e., not used or needed by the organization and/or denied by policy, should be blocked via use of a boundary router and packet filtering technology. This will result in reduced risk of attack and will create a network environment that has less traffic and is thus easier to monitor.

5.5.6 Proxy applications should be used for out-bound HTTP connections and for in-bound/outbound email that are capable of the following operations:

a) Blocking Java. Applets and applications
b) ActiveX and JavaScript filtering
c) Blocking specific MIME extensions
d) Scanning for viruses

This is not a recommendation to *enable* blocking of active web content, but to be capable of blocking it, if required. The decision to block active content, excluding viruses, should be weighed carefully, as blocking active content will render many websites unusable or difficult to use.

Executable files in email attachments that could be blocked include the following:

.ade .cmd .eml .ins .mdb .mst .reg .url .wsf
.adp .com .exe .isp .mde .pcd .scr .vb .wsh
.bas .cpl .hlp .js .msc .pif .sct .vbe
.bat .crt .hta .jse .msi .pl .scx .vbs
.chm .dll .inf .lnk .msp .pot .shs .wsc

5.5.7 Organizations should not rely solely on the firewall proxies to remove the above content; web browsers should be set to appropriate security levels, and anti-virus software should be used on personal computers.

5.5.8 As stated previously, the overall policy of the firewall should be to block all inbound traffic unless that traffic is explicitly permitted. Sample policies are available at nist and other websites.

5.5.9 The following types of network traffic always should be blocked:

1) Inbound traffic from a non-authenticated source system with a destination address of the firewall system itself.
2) Inbound traffic with a source address indicating that the packet originated on a network behind the firewall.
3) Inbound traffic from a system using a source address that falls within theaddress ranges set aside in RFC 1918 as being reserved for private networks.
4) Inbound traffic from a non-authenticated source system containing SNMP (Simple Network Management Protocol) traffic.
5) Inbound traffic containing IP Source Routing information.
6) Inbound or outbound network traffic containing a source or destination address of 127.0.0.1 (local host).
7) Inbound or outbound network traffic containing a source or destination of 0.0.0.0.
8) Inbound or outbound traffic containing directed broadcast addresses

5.5.10 It is recommended that procedures exist for testing the firewall before it is the changes are installed on the firewall. If the firewall policy is altered then there need to be a process where by the new policy is tested before it is 'burnt' into the actual firewall. This is done to ensure that the changes to the firewall do not have a negative effect on its operation.

5.5.11 Management should document a formal change control policy for amending the firewall's configuration. This policy should describe the principles and objectives on which change control process should operate. Having defined when changes should be performed, the objectives should describe change requirements (those is-key standards). Change Control is required to ensure that administrators of the firewall are in fact performing the task required of them. This is done to

1. Ensure changes made reflect the change in policy.
2. Ensure the administrators do not perform changes without notification.

Non-conformance may result in loss of control over changes to network devices resulting in unauthorized access into a device and the potential for an unauthorized person to alter security configuration parameters.

5.5.12 Personnel installing changes must be authorized to do so and held accountable for the change. If the organization does not identify the authorized individuals who update the firewall, the risk increases of unauthorized changes to configurations

5.5.13 All network related documentation must be updated and currency of content maintained. Network related documentation should be appropriately identified with date, version number, and commentary as to what changes have been made to the content. All such changes should be managed via a formal change control mechanism. In order to ensure that the firewall is securing the required section of the network a detailed diagram of the network may be required.

This can be used to ensure that the firewall is protecting what it should be protecting and will help in identifying any weaknesses that may exist within the firewall setup.

5.5.14 Firewall documentation should exist, and as a minimum detail the firewall policy and the rational for the inclusion of each individual rule. Documentations should also justify the exclusion of specific rules, where the absence impacts on the security of the firewall and/or the corporate network. In order to de-sign a rule base it is important to have supporting documentation outlining the policies required by the organization. These should be kept up to date to reflect the actually policies in place on the firewall(s).

5.6 Firewall Deployment

5.6.1 Any unused networking protocols should be removed from the firewall operating system build. Unused networking protocols can potentially be used to bypass or damage the firewall environment. Finally, disabling unused protocols ensures that attacks on the firewall utilizing protocol encapsulation techniques will not be effective.

5.6.2 Any unused network services or applications should be removed or disabled. Unused applications are often used to attack firewalls because many administrators neglect to implement default-restrictive firewall access controls. In addition, unused network services and applications are likely to run using default configurations, which are usually much less secure than production-ready application or service configurations.

5.6.3 Any unused user or system accounts should be removed or disabled. This particular issue is operating system specific, since all operating systems vary in terms of which accounts are present by default as well as how accounts can be removed or disabled

5.6.4 Applying all relevant operating system patches is also critical. Since patches and hot fixes are normally released to address security-related issues, they should be

integrated into the firewall build process. Patches should always be tested on a non-production system prior to rollout to any production systems. This pre-rollout testing should include several specific events:

1. A change of the system time (minute-by-minute, and hour-by- hour).
2. A change of the system date (both natural, and manual).
3. Adding and deleting of appropriate system users and groups.
4. Startup and shutdown of the operating system.
5. Startup and shutdown of the firewall software itself.
6. System backups, if appropriate.

5.6.5 Unused physical network interfaces should be disabled or removed from the server chassis.

5.7 Firewall Administration

5.7.1 If the firewall is implemented on a vendor operating system, it should be stripped of unnecessary applications and should be hardened against attack.

5.7.2 It is recommended that only few people (1-5) should be allowed access to the firewall. This includes physical access, local logon (Windows NT) and remote firewall logon.

5.7.3 Each user with read or read/write access to the firewall configuration should be identified by unique usernames.

5.7.4 Hard-to-guess usernames and password should be used

5.7.5 During installation you must set DNS host names and/or IP addresses of those management stations allowed to access the firewall. It is recommend using IP addresses instead of DNS host names, as this increases the risk of spoofed DNS attacks to the firewall management ports.

5.7.6 Firewall backups should be performed via an internally situated backup mechanism, e.g., tape drive. Firewall backups should not be written to any backup servers located on protected networks, as this may open a potential security hole to that network.

5.7.7 Firewalls should log activity, and firewall administrators should examine the logs daily. The Network Time Protocol (NTP) or another appropriate mechanism should be used to synchronize the logs with other logging systems such as intrusion detection.

5.7.8 There should be sufficient space for the log files to reduce the risk that the partition will be deliberately filled by an attacker.

5.7.9 An organization should be prepared to handle incidents that may be inevitable despite the protections afforded by the firewall environment. An incident response team should be created to assist the recovery from and analysis of any incidents

5.7.10 All firewall and security policies should be audited and verified at least quarterly, preferably along with policy of the organization

5.7.11 Ensure that patches to the base operating system and to the firewall are current. For a firewall to be successful it must operate on a secure operating system. If the firewall is running on an inferior system then it is open to attacks not possible according to the firewall. It should be ensured that the system the firewall is run on is secure and that all patches have been applied.

5.7.12 If Alerts are enabled then there should exist a documented procedure for handling the alert

5.8 References

- www.clark.net/pub/mjr/pubs/fwfaq (Marcus Ranum Firewall FAQ)
- www.firewall.com (numerous links to firewall references and software resources)
- www.nfr.com/forum/firewall-wizards.html (Firewall Wizards mailing list and archives)
- www.zeuros.co.uk (Rotherwick Firewall Resources)
- lists.gnac.net (Great Circle Firewalls Digest mailing list and archives)
- www.cert.dfn.de/eng/fwl/ (German CERT firewall laboratory)
- www.nwconnection.com/ (Jan .97 issue - excellent technical tutorial on firewalls)
- www.robertgraham.com/pubs/ (several detailed white papers on firewalls and intrusion detection)
- www.cisco.com (Cisco Website . numerous how-to.s FAQ on router security)
- www.phoneboy.com/fw1/ (Unofficial CheckPoint Firewall-1 FAQ & freeware site)
- www.icsa.net/ (International Computer Security Association . firewall certification)
- icat.nist.gov (ICAT vulnerability database, National Institute of Standards and Tech-nology)
- www.sans.org/ (numerous documents and links to security sources)
- time.nist.gov (information on NTP)