Interested in learning more about security?

SANS Institute InfoSec Reading Room

IT Infrastructure Security-Step by Step

After having worked as a system/network administrator for couple of years, I was instrumental in the design and implementation of my organization's System Networking and Communication Infrastructure. I had been given the responsibility for the installation, improvement and maintenance of security of the entire Information Technology Infrastructure of the organization. During this period, I realized the need for acquiring a high level of understanding of the critical issues of security and implementing the same in a rea...

Name **Karnail Singh**
Version number **1.2e**
Title **IT Infrastructure Security-Step by Step**

Introduction

Bruce Schneier, the renowned security technologist and author, said that the mantra for any good security engineer is “Security is not merely a product, but a process. It's more than designing strong cryptography into a system; it's designing the fail-safe system such that, all security measures, including cryptography, work together."

After having worked as a system/network administrator for couple of years, I was instrumental in the design and implementation of my organization’s System Networking and Communication Infrastructure. I had been given the responsibility for the installation, improvement and maintenance of security of the entire Information Technology Infrastructure of the organization. During this period, I realized the need for acquiring a high level of understanding of the critical issues of security and implementing the same in a real life network and system environment.

While reviewing various papers and books on security, and some security breach incidents, I realized that that there are not many resources available that provide a step-by-step approach for building comprehensive security systems. Most of the existing material talks about particular security breaches or security holes and their remedies.

After working on security issues for over a year, and having studying the GIAC Level One Security Essentials Certification (GSEC) courseware, I am making an attempt in this paper to document the process and methodology for implementing computer security based in corporate networks. It describes the various aspects of security through a layered model.

Intended Audience

This paper is suitable for those who are in the field of Systems/ Network Administration and wish to enhance their knowledge of computer security.

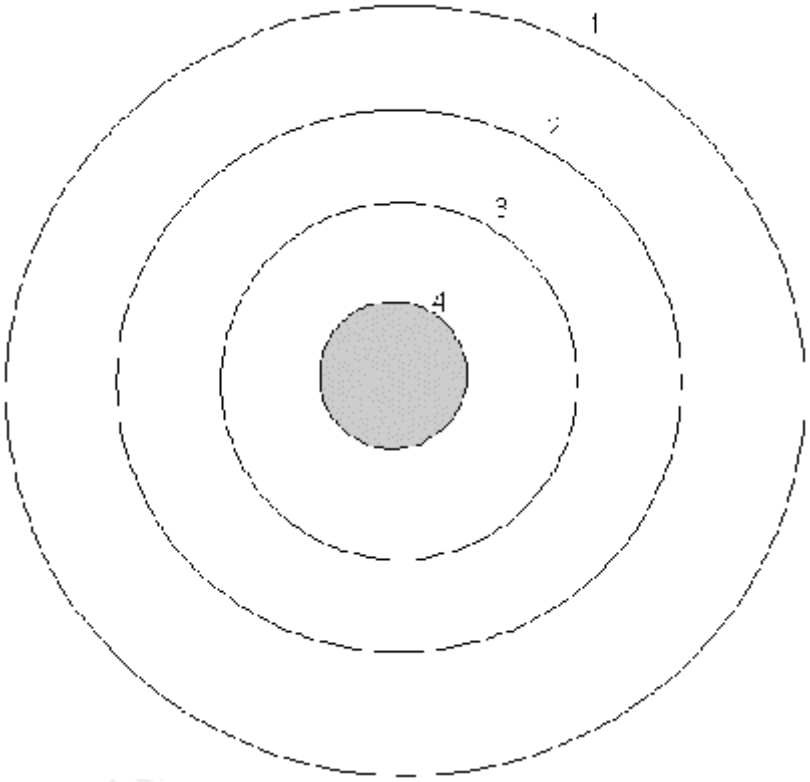
Steps in Security

- Comprehend your IT infrastructure, network (configuration and topology), network traffic and communication system
- Prepare a security policy, processes, procedures, and their implementation plan
- Obtain approval of the above from management
- Implement the above policies and plans
- Maintain a standardized documentation of the entire IT infrastructure
- Periodically test and audit the entire network security (Internet, Intranet and Extranet), update it regularly, and maintain an audit trail of all changes
- Create security awareness among users through training, crash courses or “tip of the day” messages.
- Undertake preventive measures, before corrective measures become necessary.

Security Model

It is said "Defense is in Depth", and I have tried to follow this rule while designing and implementing any security system or model. This security model is represented in the figure below. This model consists of 4 layers of security and each layer is described in detail in this paper.

Layered Security Model



Most of us don't work for organizations with budgets for procurement of security equipment or systems (or security personnel). In this context, I have tried to implement this Layered Security Model with the help of tools/technologies available free on the Internet. These tools perform data collection, analysis, reporting and generation of alarms.

The four key layers of the security model are:

- **Layer-1:** Perimeter Defense
- **Layer-2:** Operating Systems and Servers Protection
- **Layer-3:** Host Protection
- **Layer-4:** Information Protection

Security Layer-1: Perimeter Defense Security Systems

This layer is like the four walls and the roof of a secure house. It includes firewalls, routers and proxy servers. A national survey showed that 70-80% of attacks are internal i.e., from within the organization's internal network. Therefore, securing from internal attacks is the first line of defense. However, having only this line is not enough to protect any network and valuable information.

One of the common attacks on this layer is DoS (Denial of Service) attack, which involves flooding the point of connection to outside world with unproductive traffic. This brings communications with the Internet to a standstill. Some of the common DoS attacks on routers are Smurf, Syn, Ack and Rst attacks. Cisco researchers/security analysts have produced a wonderful document (Refer: http://www.cisco.com/warp/public/707/21.html) on how to configure a router to protect against these attacks. There are numerous solutions documented by various vendors. I have discussed the Cisco's findings here since I am implementing and managing the same in my organization.

The aforesaid paper describes how attacks like Smurf target victim systems using source-spoofed packets originating from a third-party's (middle) system. One of the methods to stop this involves filtering at the point of connection to the Internet in your network or your ISP. Additionally router vendors have added options to disallow packets with spoofed IP source addresses. Cisco has implemented this by adding a command: "[no] ip verify unicast reverse-path".

To prevent one's system from being the middle system (the system used to attack the target), Cisco has added another command: "no ip directed-broadcast" in IOS 12.0. This option is set by default, and protects the OSI layer3 broadcast into OSI layer 2 broadcast.

If you have a DMZ, make sure the filters between your internal network and DMZ are configured properly:

- DMZ is setup as an external network to the internal network (production network)
- DMZ is setup as an internal network for requests from Internet to the DMZ

However, to implement such a security system the following precautions should be taken at a minimum:

Precautionary measures

- Install appropriate filters such as:
  - "access-list *number* deny icmp any any redirect" . This disallows ICPM packets
  - "Anti-spoofing". This will control access through router and would stop packets with source address with internal IP addresses from coming in

- "no ip directed-broadcast". This will stop packets broadcasts.
  Reference: http://www.cisco.com/warp/public/707/21.html#spoofing

- Control and monitor filter configurations in terms of privileges and their use:
  - who can modify
  - who modified
  - when modified
  - why modified
- Update filters:
  - as and when required to implement network changes
  - install new software releases
  - prevent future attacks that may exploit existing or newly discovered vulnerabilities
- Test filters to ensure that the rules are still working:
  - Periodically
  - Break testing
- Configure Anti-virus software for real time scanning at the gateway
- Implement intelligent logging at a level that is enough to trace back the attack
- Trace Intrusions, if any, and analyze them in detail to take corrective measures to harden the security infrastructure
- Maintain detailed documentation of the filter (router and proxy) configurations and follow change management

Security Layer-2: OS and Application Servers Security Systems

This layer holds protection of operating system, the application servers, web servers, and mail servers.

While traffic is regulated at the perimeter depending on the needs of the organization, the applications utilizing the traffic run on different application/webservers which in turn run on operating systems. An abuse of operating system privileges can potentially compromise network security. Users with access to the underlying operating system can jeopardize the availability and integrity of the firewall and expose critical network resources to both internal and external security threats. Hardening this layer will protect the network from number of internal threats.

Vulnerabilities exist in operating systems, web servers, proxy servers, mail servers and application servers that need patches / service packs / hotfixes to fill those holes.

An organization may have multiple operating systems in its network. It is the responsibility of the OS vendors to make their products secure. In addition the user organization also has the responsibility of applying the available security features.

Some of the General Practices to Secure Server Hardware are:

- Place your servers and communication equipment in a secure room

- Give restricted access to server/communication room
- Avoid using server consoles as much as possible
- Match hardware compatibility while buying/installing the server
- Disable CD-ROM or floppy disk boot

Windows NT 4.0 / 2000

Microsoft's Windows NT is C2 compliant. This C2 rating does not guarantee that NT is the operating system with the best security. Out of the box NT has to be configured and patched to meet C2 ratings.

Given below are steps I followed to make NT a secure operating system and feel bit comfortable (I said comfortable not satisfied or done with) about security of my networks

- Install minimum Service Pack 3 in case of NT 4.0, and Service Pack 2 in case of Windows 2000. SP3 for NT allows you to better secure your system. One of its major features is the addition of the "Authenticated Users" group to help eliminate anonymous connections. SP6a is now recommended for NT 4.0 systems. Installing post SP3 hot fixes or having SP4 or later service packs, will protect the server from attacks like GetAdmin and RedButton.
- Enable auditing (it is not by default). Audit failed login as well as successful logins.
- Enable 'change periodic password' policy (not enabled by default). An important aspect of NT passwords that needs to be understood is that NT does not store encrypted passwords, but hashed versions of the password. These hashes are one-way encryption algorithms, which means that they can't be decrypted.
- Another one of NT's biggest problems is that even with SP3 installed, anyone who has network access to an NT machine can find out the name of the administrator, and the privileged shared drives of that box. Disable this by changing the registry key, "HKLM/SYSTEM/CurrentControlSet/Control/LSA: RestrictAnonymous."
- Change the default user rights in "user manager menu". You may like to restrict user to login locally on Primary Domain Controller.
- Make proper backups. Don't rely on NTBACKUP and instead use third party backup software (e.g. ArcServeIT from Computer Associates) depending on whether multiple servers/workstations are to be backed up.
- Have NT registry backed up using RDISK/S or NT-resource kit utilities (Regback.exe)
- Windows 2000 ships with a powerful encryption system that adds an extra layer of security for drives, folders, or files. This helps prevent a hacker from accessing your files by physically mounting the hard drive on another PC and taking ownership of files. Be sure to enable encryption on Folders, not just files. All files that are placed in that folder will be encrypted.
- Applications use the 'temp' folder to store copies of files while they are being updated or modified, but they don't always clean the folder when you close the program. Encrypting the temp folder provides an extra layer of security for your files.

- In Windows 2000, only Administrators and Backup Operators have default network access to the registry, however you may wish to tighten this down even further. To restrict network access to the registry, follow the steps listed in TechNet Article Q153183
- The Pagefile is the temporary swap file Windows NT/2000 uses to manage memory and improve performance. However, some 3rd party programs may store unencrypted passwords in memory, and there may be other sensitive data cache as well. You can clear the pagefile at shutdown by editing the Registry Key, "*HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\Memory Management" and* changing the data value of the ClearPageFileAtShutdown value to 1(for further information, refer TechNet Article Q182086)
- When you press Ctrl-Alt-Del, a login dialog box appears which displays the name of the last user who logged in to the computer, and makes it easier to discover a user name that can later be used in a password-guessing attack. This can be disabled by editing the Registry Key "*HKLM\Software\Microsoft\WindowsNT\ CurrentVersion\Winlogon\DontDisplayLastUserName" and* changing the REG_SZ value to "1
- Have Anti-virus software configured for real-time scanning on all servers

It is an important issue to make sure that the operating system and application servers are patched with updated releases and appropriate hot fixes. (Refer to following books and sites on NT and NT security for more details)

- http://www.microsoft.com/security/default.asp
- http://www.ntsecurity.com/security-news.asp
- http://www.labmice.net/articles/securingwin2000.htm
- http://www.sans.org/infosecFAQ/win2000/win2000_list.htm
- http://windows.microsoft.com/windows2000/en/server/help/default.asp?url=/windows2000/en/server/help/sag_ADtopnode.htm
- NT Network Security; Mathew Strebe, Charles Perkins & Michael G. Moncur

Linux

There are different flavors of UNIX. Linux is one of the widely used and popular variant of UNIX. Like any other operating system, we have to keep fine-tuning Linux too. Some of the precautionary measures related to Linux systems security are as follows:

- Passwords, in Unix are the first line of defense. Make sure you implement a strong password policy and keep checking once a week that the passwords are strong. Also force users to change them at least every 30 days.
- Use "umask" for default file creation on your system
- Make sure that your system files are not open for casual editing by users and groups who shouldn't be doing such system maintenance
- Be very careful while configuring the kernel.
- The Key Parameters one has to be careful about are:
  i. Network Firewalls (CONFIG_FIREWALL)

ii. IP: forwarding/gatewaying (CONFIG_IP_FORWARD)
iii. IP: syn cookies (CONFIG_SYN_COOKIES)
iv. IP: Firewalling (CONFIG_IP_FIREWALL)
v. IP: firewall packet logging (CONFIG_IP_FIREWALL_VERBOSE)
vi. IP: Drop source routed frames (CONFIG_IP_NOSR)
vii. IP: masquerading (CONFIG_IP_MASQUERADE)
viii. IP: ICMP masquerading (CONFIG_IP_MASQUERADE_ICMP)
ix. IP: transparent proxy support (CONFIG_IP_TRANSPARENT_PROXY)
x. IP: always defragment (CONFIG_IP_ALWAYS_DEFRAG)
xi. IP: Firewall packet netlink device (CONFIG_IP_FIREWALL_NETLINK)

For further details related to above listed security parameters refer to http://www.linuxdoc.org/HOWTO/Security-HOWTO.html

- Linux, by default, starts the services like HTTP, FTP, SMB, sendmail, which may not be required but are waiting for some one to connect. Stop the services not required.
- Check for '.rhost' file and avoid using it. This file contains names of systems on which you have an account
- Check for syslog and messages regularly
- Check for unsuccessful as well as successful logons
- Check for suspicious entries in 'inetd.conf'
- Be very careful while configuring anonymous FTP accounts such as, /incoming directory should be made writeable and that too by user root and FTP only. User 'anonymous' should only have read access to /incoming and /pub directories.

Security Layer-3: Host Protection

Now that we have our perimeter defense tightened and the OS fine-tuned, we need to look at another threat from the internal workstations connected to the network. We need to have workstation security for two reasons:

- to protect against someone trying to attack from within the network
- to protect the data stored on workstation from someone coming in through the firewall

Some of the key characteristics related to workstation security are listed below.

- Formulate User Access Policy and implement the same
- Update regularly the patches/hotfixes for the workstation operating system and applications.
- Limit the Network Resources Access from workstations. Assign only what is a "MUST REQUIRED".
- Install Anti-virus software and update it regularly on all the workstations
- Ensure workstation data is included in daily nightly backups

- Allow no modems on workstations
- If nature of work permits (or if you can make it work) allow only one user to login in on each workstation.
- Have as much logging enabled for workstations, as possible
- Have a personal firewall installed on all (if possible) workstations. A popular one is Zone Alarm, which is a free download for personal use with a very nominal fee for commercial use. Its available at http://www.digitalriver.com/dr/v2/ec_MAIN.Entry17c?CID=39974&PN=5&SP=10007&SID=24156&PID=300533&DSP=&CUR=840&CACHE_ID=39974
- Do not retain faulty or old hard disk drives. CRASH THEM if you are planning not to use them.
  (Refer http://www.cert.org/security-improvement/modules/m04.html.)

Security Layer-4: **Data/Information Protection**

With above three layers taken care of, I believe we should have one more layer on our data. Have encryption, whenever possible. I prefer Windows 2000 to Win9x. Given the budget, I would make Windows 2000 the standard for mobile users.

Read more on Windows2000 for mobile computing at http://www.microsoft.com/windows2000/professional/evaluation/business/overview/mobile/default.asp

- Having all the security layers implemented on the corporate network helps secure all the PCs in the network but once the PC is removed for use at home or on the road, security becomes more at risk.
- Data protection can be broken down into three distinct categories: operating system security, sensitive data storage practices, and data encryption.
- Operating system security covers the normal operating system (and services) security best practices.
- Sensitive data storage practices cover the data that has to be on a server and data that can be on a desktop/laptop
- Data encryption covers the need of having the data protected by means of encryption.

Precautionary steps:

i. Do not use any option that "remembers" your password so that you do not have to reenter it the next time you need it
ii. Have all the laptops with windows 2000 installed with encryption enabled
iii. For existing laptops with windows 9x, have third party encryption products like PGP, Norton For Your Eyes Only, RSA SecurePC, and TSS Officelock
iv. Have different password for different accounts
v. Do not use same password for corporate network and public networks (Hotmail.com, Yahoo mail etc.)
vi. Apply newly released operating system patches and application patches

Conclusion

Security cannot be achieved by merely implementing various security systems, tools or products. However security failures are less likely through the implementation of security policy, process, procedure and product(s). Multiple layers of defense need to be applied to design a fail-safe security system. The idea behind multi-layered defense security is to manage the security risk with multiple defensive strategies, so that if one layer of defense turns out to be inadequate, another layer of defense will, ideally, prevent a full breach. The author believes that, at a minimum, managers must apply a range of security perimeter defenses so that their resources are not exposed to external attacks and ensure that the security system is not limited by the weakest link of the security layer.

List of References

Web Sites

- **Cisco-Improving security on Cisco routers**
  - http://www.cisco.com/warp/public/707/21.html
- **Microsoft-How to clear Windows NT password at shutdown**
  - http://support.microsoft.com/directory/article.asp?id=KB;EN-US;q182086
- **NT Security Sites**
  - http://www.microsoft.com/security/default.asp
  - http://www.ntsecurity.com/security-news.asp
  - http://www.labmice.net/articles/securingwin2000.htm
  - http://www.sans.org/infosecFAQ/win2000/win2000_list.htm
  - http://windows.microsoft.com/windows2000/en/server/help/default.asp?url=/windows2000/en/server/help/sag_ADtopnode.htm

Linux Security

- http://www.linuxdoc.org/HOWTO/Security-HOWTO.html

Zone Alarm

- http://www.digitalriver.com/dr/v2/ec_MAIN.Entry17c?CID=39974&PN=5&SP=10007&SID=24156&PID=300533&DSP=&CUR=840&CACHE_ID=39974

Securing Desktop workstations

- http://www.cert.org/security-improvement/modules/m04.html.)

Windows 2000 Professional Security-For Mobile user

- http://www.microsoft.com/windows2000/professional/evaluation/business/overview/mobile/default.asp

Books

- NT Network Security
- By Mathew Strebe, Charles Perkins & Michael G. Moncur
- Building Internet Firewalls
- By Elizabeth D. Zwicky, Simon Cooper and D.Brent Chapman

Magazines and Journals

- Security Administrator By Windows 2000 Magazine (www.win2000mag.com)
- MCP Magazine (http://subscribe.101com.com/mcpmag/)
- Packet from Cisco (http://www.cisco.com/warp/public/784/packet/)
- Network computing (http://as400.halldata.com/qdls/clients/ncsvc.htm)
- PC World by idg.net (www.pcworld.com)

Mailing Lists

- SANS
- Microsoft

Last Updated: April 22nd, 2018

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Blue Team Summit & Training 2018	Louisville, KYUS	Apr 23, 2018 - Apr 30, 2018	Live Event
SANS Riyadh April 2018	Riyadh, SA	Apr 28, 2018 - May 03, 2018	Live Event
SANS Doha 2018	Doha, QA	Apr 28, 2018 - May 03, 2018	Live Event
SANS SEC460: Enterprise Threat Beta Two	Crystal City, VAUS	Apr 30, 2018 - May 05, 2018	Live Event
Automotive Cybersecurity Summit & Training 2018	Chicago, ILUS	May 01, 2018 - May 08, 2018	Live Event
SANS SEC504 in Thai 2018	Bangkok, TH	May 07, 2018 - May 12, 2018	Live Event
SANS Security West 2018	San Diego, CAUS	May 11, 2018 - May 18, 2018	Live Event
SANS Melbourne 2018	Melbourne, AU	May 14, 2018 - May 26, 2018	Live Event
SANS Northern VA Reston Spring 2018	Reston, VAUS	May 20, 2018 - May 25, 2018	Live Event
SANS Amsterdam May 2018	Amsterdam, NL	May 28, 2018 - Jun 02, 2018	Live Event
SANS Atlanta 2018	Atlanta, GAUS	May 29, 2018 - Jun 03, 2018	Live Event
SANS London June 2018	London, GB	Jun 04, 2018 - Jun 12, 2018	Live Event
SANS Rocky Mountain 2018	Denver, COUS	Jun 04, 2018 - Jun 09, 2018	Live Event
SEC487: Open-Source Intel Beta Two	Denver, COUS	Jun 04, 2018 - Jun 09, 2018	Live Event
DFIR Summit & Training 2018	Austin, TXUS	Jun 07, 2018 - Jun 14, 2018	Live Event
Cloud INsecurity Summit - Washington DC	Crystal City, VAUS	Jun 08, 2018 - Jun 08, 2018	Live Event
SANS Milan June 2018	Milan, IT	Jun 11, 2018 - Jun 16, 2018	Live Event
Cloud INsecurity Summit - Austin	Austin, TXUS	Jun 11, 2018 - Jun 11, 2018	Live Event
SANS Oslo June 2018	Oslo, NO	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS ICS Europe Summit and Training 2018	Munich, DE	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Cyber Defence Japan 2018	Tokyo, JP	Jun 18, 2018 - Jun 30, 2018	Live Event
SANS Crystal City 2018	Arlington, VAUS	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Philippines 2018	Manila, PH	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Vancouver 2018	Vancouver, BCCA	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Paris June 2018	Paris, FR	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Cyber Defence Canberra 2018	Canberra, AU	Jun 25, 2018 - Jul 07, 2018	Live Event
SANS Minneapolis 2018	Minneapolis, MNUS	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS London July 2018	London, GB	Jul 02, 2018 - Jul 07, 2018	Live Event
SANS Cyber Defence Singapore 2018	Singapore, SG	Jul 09, 2018 - Jul 14, 2018	Live Event
SANS Charlotte 2018	Charlotte, NCUS	Jul 09, 2018 - Jul 14, 2018	Live Event
SANSFIRE 2018	Washington, DCUS	Jul 14, 2018 - Jul 21, 2018	Live Event
SANS Malaysia 2018	Kuala Lumpur, MY	Jul 16, 2018 - Jul 21, 2018	Live Event
SANS Seattle Spring 2018	OnlineWAUS	Apr 23, 2018 - Apr 28, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced