Linux Security

Prepared by:

William Zereneh
zereneh@scs.ryerson.ca

Introduction

- CISCO routers used in Enterprise Networks
- UNIX/Linux based Networks used in:
  - Universities
  - Small-to-Medium sized companies
- Lecture Covers the following topics:
  - Secure UNIX/Linux workstations & Servers
  - Limiting Resource
  - Kernel tuneable parameters
  - Secure Linux Networks – IPTABLES
  - Firewalls
  - Auditing tools

Introduction Cont..

- Package Management System, Snort, Portsentry
- Intrusion Detection – IDS/NIDS
- OpenSSH
- Performance Tuning of Linux Workstations & Servers
- KERBEROS for authentication
- Partitions, resize partitions, run levels
- Booting into rescue mode
- Planning for disasters, Backup
- IDE hard drive tuning
- Resource Monitoring & Speed up Networks

Security Principles

1. Know Thy System

   Must know how something works before you could secure it

1. Least Privileges

   Users are given least amount of access to perform their jobs

1. Defense In Depth

   Multiple levels of protection

1. Prevention is ideal BUT detection is a must

   Impossible to prevent all attacks, but detecting attack them must be first priority

Risk Management

Securing an infrastructure is done after a thorough analysis of Risk to critical assets

Results of Risk analysis exercise determines the level of security to implement

What is Risk ?

Risk = Threat X Vulnerability

Threat: is the potential to harm

Vulnerability: is a weakness that allows the Threat to manifest itself

Risk of What? CIA

Confidentiality - Information stored on the workstation may be disclosed inappropriately.

Integrity - The integrity of information stored on the workstation may be changed, either accidentally or maliciously.

Availability- Authorized users may be unable to use the workstation, the network, or the information and services stored on each to perform their jobs.

* All are important but must prioritize which is more critical to the organization

1. Security as a Policy

- How do you classify confidential or sensitive information?
- Does the system contain confidential or sensitive information?
- Exactly whom do you want to guard against?
- Do remote users really need access to your system
- Do passwords or encryption provide enough protection?
- Templates:

  http://www.sans.org/resources/policies/#template

2. BIOS

- Disallow booting from floppy/cdrom/usb drive and network
  - Prevent undesired individuals from trying to boot the system with special boot disk
  - Protect against changing BIOS features
    - Reboot machine and change boot sequence to boot Hard Drive ONLY
    - Set a password for BIOS

3. Choose the right Password

- Most IMPORTANT – often neglected
- Set the right values in /etc/login.defs
  - Change PASS_MIN_LEN 5
  - To PASS_MIN_LEN 8 (Handled by PAM)
  - Change PASS_MAX_DAY 99999
  - To PASS_MAX_DAY 63
- apg – Automatic password generator
  http://www.adel.nursat.kz/apg/
- John the Ripper password cracker
  http://www.openwall.com/john/

4. Root Account

- No security imposed on it
- Never login as root on your server
- Set login time out for root account
- Set TMOUT to the time in seconds (TMOUT is a bash environment variable that can be set per user or system wide)
  - edit /etc/profile or ~/.bashrc or /etc/bash.bashrc and set: TMOUT = 7200

5. Administer system using sudo

- Allows an authenticated user to run commands as root or another user
- Normally assumes the identity of root user if no username specified
- Provides auditing trail as all command executed using sudo will be logged
- Configuration file is /etc/sudoers
- Add user or group allowed to run sudo
- Example: sudo vi /etc/shadow

6. Disable remote admin Access

- All administrative accounts will not be able to login remotely; mainly root
- Users must use either sudo or su to administer the system
- Modify /etc/security/access.conf and add the following:

  -:wheel:ALL EXCEPT LOCAL

  - This will disallow access from anyone in the wheel group but local access
  - Note: pam_access module must be enabled for all services for this setting to take effect

7. inetd

- Super server that loads network programs based on request from network
- /etc/inetd.conf
  - Ports to listen to
  - What server to start for each port
- Check for services to offer – deny others
  - Edit /etc/inetd.conf
  - Comment out line to disable uncomment to enable
- chmod 600 /etc/inetd.conf

continued...

7. inetd continued

- stat /etc/inetd.conf – make sure owner is root
- chattr +i /etc/inetd.conf – make file “immutable” cannot be modified, deleted or renamed and no links created
- restart inetd after changes
  /etc/init.d/openbsd-inetd reload
- lsattr/etc/inetd.conf – to verify that “immutable” bit is set

8. /etc/services file

- Convert service name to port number
- Only root allowed to make modifications
- immunize the file
  - chattr +i /etc/services

9. /etc/securetty file

- Which tty devices root is allowed to login on
- File read by the login program, usually /bin/login
- Allow root on tty1 only – use su to switch to root if you need to
- edit /etc/securetty and comment out all but tty1

```
tty1
#tty2
#tty3
.....
```

10. Special Accounts

- Disable all default vendor specific accounts

  e.g. news, games, ...
  - To delete a user - userdel username
  - To delete a group - groupdel groupname
  - immune files
    - *chattr +i /etc/shadow*
    - *chattr +i /etc/passwd*
    - *chattr +i /etc/group*
    - *chattr +i /etc/gshadow*

11. Block su to root

- Allow only root to execute “su”
- Change the file /etc/pam.d/su
  - Uncomment the following line to require a user to be in the "wheel" group

    *auth required pam_wheel.so**
  - *usermod -G10 adminuser*
  - 10 numbered value of the group wheel
  - adminuser: user we want to add to wheel group

    * Read comments in su pam config file for more options

12. Put limits on resources

- /etc/security/limits.conf – important to set limits, to prevent denial of service attacks
  - Add/Change the lines in limits.conf to read:

```
* hard        core         0    # prohibit core files
* hard        rrs       5000 # memory usage 5M
* hard        nproc  20  # number of process
```

- Edit /etc/pam.d/login and make sure the following line exist

```
session     required        /lib/security/pam_limits.so
```

- avoid :(){ :|: &}; :

13. Control mounting filesystem

- More control over mounted file system using the right mount options
  - defaults: Allow everything
  - noquota: Do not set users quotas
  - nosuid: Do not set SUID/SGID
  - nodev: Do not set character or special devices
  - noexec: Do net set execution of any binaries
  - quota: Allow users quota
  - ro: Allow read only
  - rw: Allow read-write
  - suid: Allow SUID/SGID access

14. Unusual or hidden files

Find all unusual or hidden files on the system

- On Linux hidden files start with a .
- To find all hidden files

find / -xdev \(-name ".." -o -name "." \) -print*

- Find all world writable files

find / \(-type f -o -type d \) \(-perm -2 -o -perm -20 \) -exec ls -ld {} \;

15. Shell logging

- bash shell stores up to 500 old commands in the ~/.bash_history file
- Every user will have this file .bash_history
- Reducing the number of old commands the .bash_history file can hold will protect against storing passwords typed on the command line
- Set HISTFILESIZE and HISTSIZE lines in the /etc/profile to:

  HISTFILESIZE = 20

  HISTSIZE = 20

16. Bootloader GRUB

- GRUB configuration files is /boot/grub/menu.1st
- Add timeout=00 – do not show menu
- Generate md5 password by running:

  grub-md5-crypt
- Add password –md5 <md5 password>
- Protect /boot/grub/menu.1st
  - *chmod 600 /boot/grub/menu.1st*
  - *chattr +i /boot/grub/menu.1st*
- Note: Debian 6 uses grub2

17. Disable Ctrl-Alt-Delete

- Pressing Ctrl-Alt-Delete will shutdown the system
- Prevent machine from being rebooted
- Edit /etc/inittab and comment out the following:

```
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
```

18. Tighten scripts under /etc/rc.d/

- Scripts that starts up service reside under /etc/init.d/ directory
- Scripts should be readable by root only
- *chmod -R 700 /etc/init.d/**

19. SUID/GUID root programs

- SUID/GUID root programs will run with the same privileges as root
- Find all SUID/GUID files and determine which one to keep
  - *find / -type f \(-perm -04000 -o -perm -02000 \) \-exec ls -lg {} \;*
- Change permission to remove SUID/GUID bit
  - *chmod a-s filename*

20. Kernel Parameters

- Parameters can be set in /etc/sysctl.conf
- Prevent system from responding to ping
  - edit /etc/sysctl.conf and add

    net.ipv4.icmp.echo.ignore.all = 1
  - restart the network by typing /etc/init.d/network restart
- Refuse responding to broadcast request
  - edit /etc/sysctl.conf and add

    net.ipv4.icmp.echo.ignore.broadcasts = 1
  - restart the network by typing /etc/init.d/network restart

continued...

20. Kernel Parameters cont.

- Disable IP source routing
  - edit /etc/sysctl.conf and add

    net.ipv4.conf.all.accept_source_route = 0
  - restart the network by typing

    /etc/init.d/network restart
- Enable TCP SYN Cookie Protection
  - edit /etc/sysctl.conf and add

    net.ipv4.tcp_syncookies = 1
  - restart the network by typing

    /etc/init.d/network restart

continued...

20. Kernel Parameters cont.

- Disable ICMP redirect acceptance
  - edit /etc/sysctl.conf and add

    net.ipv4.conf.all.accept_redirects = 0
  - restart the network by typing

    /etc/init.d/network restart
- Enable always-defragging protection
  - edit /etc/sysctl.conf and add

    net.ipv4.ip_always_defrag = 1
  - restart the network by typing

    /etc/init.d/network restart

20. Kernel Parameters cont.

- Enable bad error message protection
  - edit /etc/sysctl.conf and add

    net.ipv4.icmp_ignore_bogus_error_responses = 1
  - restart the network by typing

    /etc/init.d/network restart
- Enable IP spoofing protection
  - edit /etc/sysctl.conf and add

    net.ipv4.conf.all.rp_filter = 1
  - restart the network by typing

    /etc/init.d/network restart

20. Kernel Parameters cont.

- Log spoofed, source routed and redirected packets
  - edit /etc/sysctl.conf and add

    net.ipv4.conf.all.log_martians = 1
  - restart the network by typing

    /etc/init.d/network restart

Conclusion

- Set Passwords
- Limit Access
- Keep up with Patches and Updates
- Maintain Logging and Backup
- Turn off unwanted Services
- Check file system regularly
- Hide/Encrypt sensitive binaries and data
- Tune your kernel parameters
- Enforce and maintain a Policy

Network Security Intro.

- Firewalls
- DMZ
- IPTABLES – similar to Access List
  - Introduction to IPTABLES
  - Syntax and examples

- Auditing tools
  - Chkrootkit – scan system for trojans, worms, ..
  - Nessus – Network vulnerability scan

Network Security Intro.

- IDS
  - Tripwire – File integrity checking
  - DPKG – Debian Package Manager
  - Snort – Real-time traffic analyzer & packet logging on IP Network
  - Portsentry – protects against portscan
- Logging
  - Logcheck – logfiles examiner
- OpenSSH – encrypts all traffic
  - Public key authentication
  - Piping data through SSH
  - Port forwarding

Network Security

- Securing gateway server should be a significant part of your network and information-security strategy because of its vital role to the rest of the networked world.
- Many security problems can be avoided if the network is appropriately configured.
- The practices recommended here are designed to help you configure and deploy gateway servers that satisfy your organization's security requirements.
- The practices may also be useful in examining the configuration of previously deployed gateway server.

1. Firewall Function

- Packet filtering
  - Deployed on routers to allow only authorized network traffic to the extent possible
- Application proxies
  - An application program that runs on a firewall system between two networks
  - Application proxies make more complex filtering and access control decision
- Dynamic packet filtering
  - Stateful inspection filtering allows both complex combinations of payload and context filtering decision

2. Firewall Architecture

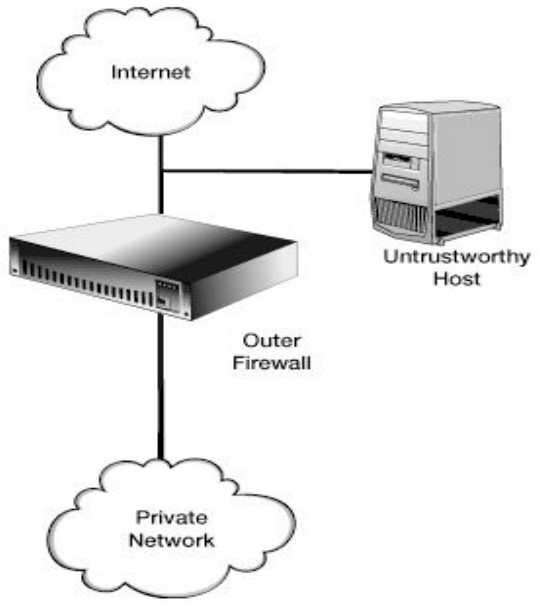
- Basic border firewall
  - A basic border firewall is a single host interconnecting an organization's internal network and some untrusted network; the Internet

Figure 1-4: Basic border firewall architecture

2. Firewall Architecture

- Untrustworthy host
  - Add a host that resides on an untrusted network where the firewall cannot protect

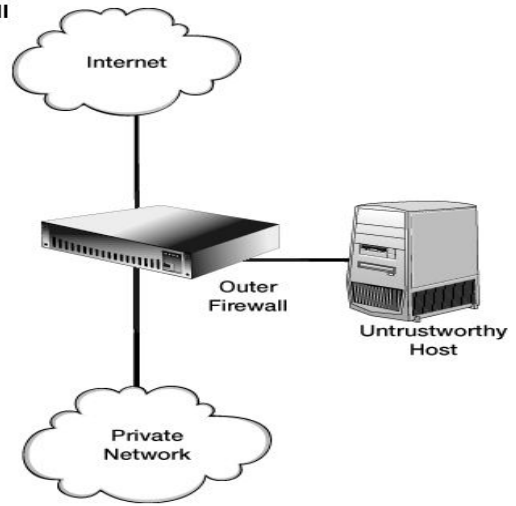
Figure 1-5: Basic firewall with untrustworthy host architecture



2. Firewall Architecture

- Demilitarized Zone DMZ
  - The untrustworthy host is brought inside the firewall
  - Increases security, reliability, and availability of the untrusted host

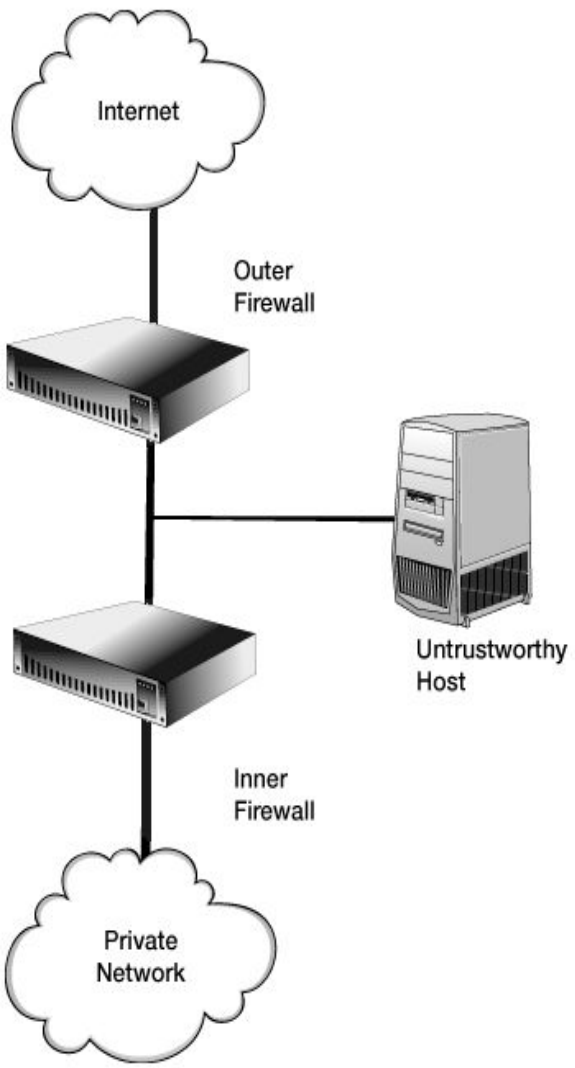
Figure 1-6: Basic firewall with DMZ network architecture



2. Firewall Architecture

- Dual firewall
  - Internal network is further isolated from the untrustworthy network by adding a second firewall host

Figure 1-7: Dual firewall with DMZ network architecture



3. Iptables

- Administration tool for IPv4 packet filtering and NAT
- Iptables is used to setup, maintain and inspect the tables of IP packet filter rules in the Linux kernel
- Several different tables may be defined
- Each table contains a number of built-in chains and may also contain user-defined chains

3. Iptables

- A firewall rule specifies criteria for a packet, and a target
- Targets are:
  - ACCEPT – let the packet through
  - DROP – drop the packet
  - QUEUE – pass the packet to userspace
  - RETURN - stop traversing this chain and resume at the next rule in the previous chain
  - LOG – logs packets

3. Iptables

- There are currently three independent tables
  - filter: the default table and it contains the built-in chains; *INPUT, FORWARD, and OUTPUT*
  - nat: Network Address Translation; contains three built-in chains: *PREROUTING, OUTPUT, and POSTROUTING*
  - mangle: Used for packet alteration; it has five built-in chains: *PREROUTING, OUTPUT, INPUT, FORWARD, and POSTROUTING*

3. Iptables

- A sample rule to drop all incoming traffic from a specific IP

  iptables -I INPUT -i eth0 -s 192.168.0.2 -j DROP

  - iptables - is the command
  - -I INPUT – insert into INPUT chain
  - -i eth0 – input interface
  - -s 192.168.0.2 – source IP address
  - -j DROP - target

3. Iptables

- A sample rule to drop all outgoing traffic from a specific IP

  iptables -I OUTPUT -o eth0 -p tcp -d www.msn.com –dport 80 -j REJECT

  - iptables - is the command
  - -I OUTPUT – insert into OUTPUT chain
  - -o eth0 – output interface
  - -p tcp – tcp protocol
  - -d www.msn.com – destination host
  - --dport 80 – destination port number
  - -j REJECT – reject with an ICMP error

3. Iptables

- Sample rules for a gateway server

  iptables -F
  iptables -P INPUT ACCEPT
  iptables -P FORWARD DROP
  iptables -P OUTPUT ACCEPT
  iptables -A INPUT -s ! 192.168.0.0/24 -i eth1 -j DROP
  iptables -A INPUT -s ! 192.168.0.0/24 -i eth1 -j LOG
  iptables -A FORWARD -o eth0 -m state –state NEW,RELATED,ESTABLISHED -j ACCEPT
  iptables -A FORWARD -i eth0 -m state –state RELATED,ESTABLISHED -j ACCEPT
  iptables -A FORWARD -j LOG
  iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -o eth0 -j MASQUERADE

- GUI software to build firewall rules: firestarter http://www.fs-security.com/

4. Auditing Tools

- chkrootkit – scans system for trojans, worms and exploits
  - For Implementation: http://www.chkrootkit.org

- Nessus - Remote security scanner
  - Performs a network vulnerability scan/security audit
  - For Implementation: http://Nessus.org

5. Intrusion Detection System IDS

- Tripwire – is a file integrity-checking program for UNIX/Linux operating systems
  - Software that alerts you when important files change
  - Tripwire keeps a hash value for each designated file
  - When a file is altered/deleted, tripwire will have a new hash value that is different than the original
  - For implementation refer to:

    http://www.cert.org/security-improvement/implementations/i002.02.html

5. Intrusion Detection System IDS

- dpkg (Debian Package Manager)
  - Debian uses package manager to install software
  - debsum - is an add on package to compute and test checksums
  - debsum_gen - should be executed to generate checksum hashes
  - dpkg –S /bin/netstat – will should which package netstat belongs to
  - debsum net-tools – will show the status of all files in the net-tools package including netstat

5. Intrusion Detection System IDS

- Snort – Network intrusion detection system
  - Performs real-time traffic analysis and packet logging on IP networks
  - It can perform protocol analysis, content searching/matching and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and OS fingerprinting
  - Snort uses a flexible rules language to describe traffic that it should collect or pass
  - For implementation: www.snort.org/docs/

5. Intrusion Detection System IDS

- portsentry – protects against portscan
  - runs as a daemon on the protected host, it listens to TCP/UDP ports and will block scanning hosts from connecting to server
  - For implementation: http://sourceforge.net/projects/sentrytools/

6. Logging

- logcheck – utility designed to allow a system administrator examine logfiles
  - It emails summaries of the logfiles after filtering out normal entries
  - For Implementation: http://sourceforge.net/projects/sentrytools/

7. OpenSSH

- OpenSSH encrypts all traffic, including password, in order to eliminate connection hijacking, eavesdropping, and other network-level attacks.
- More than just a remote shell
- Cryptographic keys – Public key authentication
  - ssh-keygen to generate private/public key
  - check permission on private key (should be private)
  - public key goes in $HOME/.ssh/authorized_keys

8. OpenSSH cont.

- Forwarding X11 traffic
  - ForwardX11 yes
  - Make sure compression is on with -C or Compression Yes
  - Fast cipher such as blowfish -c blowfish
- Forward any port (tunnel)
  - Secure mail – pop3, smtp, …

    ssh -N -f -L 20110:mailserver:110 username@mailserver

    -N no shell

    -f go to background

    -L forward local to remote port

    Works very well as long as you can tell the client to use a specific port

8. OpenSSH Cont.

- Piping data through SSH
  - Printing

    cat print.ps |ssh -l user remote.server lpr -Pprintername
  - Run any command remotely
    - Check printer queue

      ssh -l username remote.server "lpq -Pprintername"
    - Backup files

      tar zc /home|ssh username@remote.server tar zx
    - Run mini shell

      scp files.txt -l username remote.server "(ls -ltr| grep reg)"

8. OpenSSH Cont.

- Real Problems... YourISP.com
  - Some ISPs drop all outgoing smtp traffic, meaning you can not connect to any smtp server outside of their Network...
  - Solution, Firewall bypassing using SSH
    - To use same port, 25

      ssh -N -f -q -L 25:127.0.0.1:25 username@remote.server

      remote.server – any machine outside of ISP Network that can send email
    - To use different port

      ssh -N -f -q -L 2025:127.0.0.1:25 username@remote.server

      remote.server – any machine outside of ISP Network that can send email

References

- www.cert.org
- www.faqs.org/docs/securing
- www.tripwire.com
- www.netfilter.org
- www.snort.org
- http://www.openssh.com