LECTURE 8: SECURITY
OUTLINE

1. Is your OS secure
2. How security is compromised
3. Security tips and philosophy
4. Password and user accounts
5. Pluggable Authentication Modules (PAM)
6. Setuid programs
7. Effective use of chroot
8. Firewalls
9. Certifications
1. IS YOUR OS SECURE
Lecture 8: Security
Is Your OS Secure

- Of course not
  - the moment your OS is communicating via the network your machine is at risk.

- However:
  - you can work hard to make it resistant to attacks but you should keep in mind there is no risk zero.
  - Moreover, the unix fundamental flaws ensure that you will never reach the absolute and ideal security.
Is your OS secure

Lecture 8: Security

Why:

1. The design of Unix or such like system is oriented to convenience which make security manipulation hard.
2. Software development is done by a large community; therefore, security holes has a high probability to occur.
3. Most administrative functions are implemented outside the kernel; however, an attacker has a wide range of activity and access to the system.
2.

HOW SECURITY IS COMPROMISED
• We can resume security lapses into the following taxonomy:
  • Social engineering
  • Software vulnerabilities
  • Configuration errors
Social engineering

- Human user is the weakest link in the security chain.
  - Creating confusion to get information
  - Physical compromises
  - Phishing “email, SMS, phone call, etc.”
LECTURE 8: SECURITY
HOW SECURITY IS COMPROMISED

• Software vulnerabilities
  • Many softwares (commercial and open source) has shown to contain security-sapping bugs.
  • Example:
    • Buffer overflows (risk of being overwritten)
  • What can you do, very little!!
    • No action till the bug is caught in a patch.
• Configuration errors

  • many piece of software can be configured to be very secured and annoying or not that secured and pleasant to use.

  • Most of the time “not that secured and pleasant to use” is the default parameter.

• Example of venerability of host configuration:

  • not requiring password for boot loader (open to physical attack)

• Potential Solution:

  • you can add bios password and of course encrypt your data (but in case of reboot you have to be present physically)
3. SECURITY TIPS AND PHILOSOPHY
LECTURE 8: SECURITY
SECURITY TIPS AND PHILOSOPHY

- Check list:
  - Patches
  - Unnecessary services
  - Remote event logging
  - Backups
  - Viruses, worms and Trojan horses
  - Rootkits
  - Packet filtering
  - Passwords
• Patches:
  • Reasonable packing approach should include the following:
    • A regular schedule for installing routine patches that is diligently followed.
    • Document all change plans of each patches.
    • An understanding of what patches are relevant to the environment.
LECTURE 8: SECURITY
SECURITY TIPS AND PHILOSOPHY

• Unnecessary services
  • Most of the systems comes with default running services.
  • Be sure to disable any unnecessary services.
  • Recall “you can use **netstat** to check up running services”
    
      $$\text{netstat} \ -an \ | \ \text{grep} \ \text{LISTEN}$$

  • In order to identify the service you can run:  $$\text{sudo lsof} \ -i:22$$
  • Then **ps** to identify the specific process:  $$\text{ps} \ <\text{PID}>$$
• Remote event logging
  • Make use of syslog to facilitate forward log information
  • The idea is:
    • Create a centralised log aggregator that can capture logs from variety of devices and alert administrator.
LECTURE 8: SECURITY
SECURITY TIPS AND PHILOSOPHY

• Backups
  • Can be positive and also negative point regarding security
    • Positive
      • Allow you to have an uncontaminated checkpoint from which you can restore
    • Negative
      • if the tapes are stolen
LECTURE 8: SECURITY
SECURITY TIPS AND PHILOSOPHY

• Rootkits
  • Software tools that allow an unauthorised user to take control of your system without being detected
  • Example:
    • Sony’s Trojan horse uses rootlets to stay hidden from the user.
• Packet filtering
  • Necessity to install a packet filtering to control exchange of data.
  • or setting up firewall between the system and outside.

• Passwords
  • setting up password for every account
  • in case of use of remote login rely on ssh or something that secure the remote access to the system.
• General philosophy:

  • Effective system security strangeness rely on the common sense.

  • Avoid to put file that can be interesting for hackers or nosy employees in your system.

  • The site’s security policy should specify how sensitive information is handled.

  • Avoid to leave weak spots in your system that can be used as a nests for hackers.

  • Set traps to help detect an authorised behaviour or intrusions.

  • Keep monitoring the logs generated by security tools.
4. PASSWORDS AND USER ACCOUNTS
• Password management is common security weakness.

FIRST LINE DEFENCE AGAIN INTRUDERS

/etc/passwd  /etc/shadow

• Normally choose by users (not strong sometimes)

• Make it a habit to check shadow file.

• Enforce password complexity requirement. (lockup after many attempts to login in)
• Password aging

**DEFINITION:**
Password aging is technique used to defend against bad password within system or organisation. The idea is that after a specific period (90 days) the user is asked to change his/her password.

**REMARK:**
Users have the tendency to switch between the same passwords, which make the techniques not really effective in some cases.
• Password aging

• In Debian or Linux, "chage" program control and manage password aging.

• Therefore you can:
  ▶ Enforce minimum and maximum times between password changes,
  ▶ Setting up password expiration dates
  ▶ Control the number of days to warn users before their passwords expire,
  ▶ Control the number of days of inactivity that are permissible before accounts are automatically locked,
  ▶ etc.
LEcTURe 8: SECuRiTy
PASswoRDS AnD uSER ACCouNTS

• Group login and shared logins
  • User shell:
    • Set the shell for a user about any program with customise script. (theory)
  • Rootly entries
    • do not allow root to login remotely
      • changes has to be done in OpenSSH.
5. PLUGGABLE AUTHENTIC AUTHENTICATION MODULES
LECTURE 8: SECURITY
PAM

DEFINITION:
PAM is a mechanism to integrate multiple low-level authentication schemes into a high-level application programming interface.

• its Power:
  • it permit programs that rely on authentication to be written independently of the underlying authentication schemes.

• What does it mean:
  • the administrator now has the ability to add new authentication methods simply by installing new PAM models with the modification needed about the authentication policies in the configuration files.
LECTURE 8: SECURITY

PAM

• PAM schema:
6. SETUID PROGRAMS
SETUID PROGRAMS

- Programs that runs *setuid* or *setgid*
  - can be prone to security problems
  - can modify “/etc/passwd” & “/etc/shadow” files

**Solution:**

- minimise the number of *setuid* programs.
- you can disable *setuid* or *setgid* on individual filesystems by specifying the *nosuid* option to mount.
EFFECTIVE USE OF CHROOT
NOTE:

the moment we want to confines a process to a specific directory we need to use chroot system call. This action will disallows access to files outside or above that directory and thereby limits the damage that a process can cause if it should be compromised by a hacker.

• Example situation:

1.
You want to restrict remote users to a specific set of files and commands.

2.
You want to run a non-root daemon process such as Apache or BIND within a restricted filesystem subtree. If the daemon is compromised, the attacker will be restricted to the subtree as long as no privilege escalation vulnerabilities exist.
LECTURE 8: SECURITY

CHROOT

• needed condition for chroot protection to work:

  • All processes in the chroot jail run without root privileges. (Processes that run as root always have the ability to break out of the chroot jail.)

  • You are not using setuid root execution within the jail.

  • The chroot environment is up to date and minimal. (contains only the executables, libraries, and configuration files needed for task)
8. FIREWALLS
### LECTURE 8: SECURITY

#### FIREWALLS

**DEFINITION:**

A firewall is a network security system that monitors the network by allowing or blocking the traffic into or out of a private network or from the users computer.

- **Firewalls classification:**
  - Packet filtering
  - Circuit gateways
  - Application gateways
  - Dynamic packet filter (combination of the above)
firewall is a network security system that monitors the network by allowing or blocking the traffic into or out of a private network or from the users computer.

- Firewalls classification:
  - Packet filtering
  - Circuit gateways
  - Application gateways
Lecture 8: Security

Firewalls

- Packets Filters
Packet-Filters

- it is the simplest components
- Uses transport-layer information as a mean for checking:
  - IP Source and destination
  - TCP, UDP, ICMP
  - TCP flags
  - etc.
Packet-filters

Usage of packet-filters

- Filtering based on incoming or outgoing interface
  - e.g. egress filtering

- Allows or denies certain services
  - Requires intimate knowledge of TCP and UDP port usages.
Configuring packet-filters:

- First: define security policy
- Second: configuring Ipchains and Iptables
- Third: tcpwrappers
- Fourth: PortSentry

General rule: least privileges “if you don’t need it, get rid of it”
firewall is a network security system that monitors the network by allowing or blocking the traffic into or out of a private network or from the users computer.

- Firewalls classification:
  - Packet filtering
  - Circuit gateways
  - Application gateways
LECTURE 8: SECURITY

FIREWALLS

- Circuit gateways

![Diagram of Circuit-level Gateways]

Outside host → Circuit-level Gateways → Inside host

Outside connection → Inside connection
• Circuit gateways
• Based on TCP connections
• Controls by limiting which connection are permitted
• The moment they are created the relays traffic without checking the contents
• SOCKS commonly used for this purpose
firewall is a network security system that monitors the network by allowing or blocking the traffic into or out of a private network or from the users computer.

- Firewalls classification:
  - Packet filtering
  - Circuit gateways
  - Application gateways
• Application gateways

Outside host

Outside connection

Application-level Gateways

Inside host

Inside connection

Outside host

Inside host

Outside connection

Application gateways

Application-level Gateways

Outside host

Inside host

Outside connection

Application-level Gateways

Inside connection

Application gateways
LECTURE 8: SECURITY

FIREWALLS

• Application gateways
  • Full access to protocol
    • User initiate the request from proxy
    • proxy validate request
    • Next request actioned and returns results to user

• Necessity of separate proxies for each service:
  • e.g. SMTP, DNS, NTP, etc.
• Application gateways

• Architecture:

DAEMON SPAWNS PROXY WHEN COMMUNICATION DETECTED
9. CERTIFICATIONS

STANDARDS & CERTIFICATIONS
LECTURE 8: SECURITY

CERTIFICATIONS

• The most basic philosophical principle in information systems and should be considered during the design or implementation or maintenance of your system is “CIA triad”.

  • Confidentiality
  
  • Integrity
  
  • Availability
The most basic philosophical principle in information systems and should be considered during the design or implementation or maintenance of your system is “CIA triad”.

- CIA stands for:
  - Confidentiality
  - Concerns the privacy of data.
  - Integrity
  - Availability
The most basic philosophical principle in information systems and should be considered during the design or implementation or maintenance of your system is “CIA triad”.

- CIA stands for:
  - Confidentiality
  - Integrity
  - Related to authenticity of information
  - Availability
The most basic philosophical principle in information systems and should be considered during the design or implementation or maintenance of your system is “CIA triad”.

- CIA triad stands for:
  - Confidentiality
  - Integrity
  - Availability
  - Accessibility to authorised users when they need information.
CERTIFICATIONS

LECTURE 8: SECURITY

• Certificate functions

• Strong authentication
  • An external authority vouches for your identity

• Contains:
  • public key of the certificate holder which allows entity to encrypt messages that only the certificate holder can decrypt.

• Represent the foundation of privacy and security in the web.
Lecture 8: Security

Certifications

- Keys (private and public) are generated on your computer (private key should never leave your machine)
  - can also be done using web browser or application program. e.g. PGP, SSH, etc.
  - For getting the certificate for your browser visit Certificate Authority (CA) website and apply for it.
    - submit proof of identity
    - pay a fee
CERTIFICATIONS

LECTURE 8: SECURITY

• What does the certificate contains.
  • Subject Name information (Distinguished name, or DN)
  • Holder’s public key
  • Certificate is signed by CA with its private key
  • The DN info is available to the web server.
LECTURE 8: SECURITY
CERTIFICATIONS

• With the certificate and keys you are able to create a digital signature.
  
  • the use of digital signature
  
  • sign document to assure that they are authentic
  
  • Encrypt a document for privacy
  
  • Ensure the document does not change by making a secure hash.
LECTURE 8: SECURITY
CERTIFICATIONS

• Certificate in action