HARDENING LINUX

OVERVIEW

A. Hardening with SELinux

B. Access Control Lists

C. Firewalld

D. SELinux Port Security

Image by rawpixel.com

A. SELINUX

A. File Permissions / Users & Groups

- SELinux controls access to files & resources much more precisely than standard user permissions do
- A "mask" can be set (+ icon at end of file permissions indicates mask applied) to enforce read, write, and execute permissions to the 'groups' and 'others' categories
- With a mask set, most restrictive rules take precedence.

ACLS can be configured on: user/group/mask/others

- **<u>Show SELinux information on a file:</u>** 'ls -Z filename'
- **<u>Show SELinux information on a directory:</u>** 'ls -Zd directoryName'

B. What does SELinux consist of

1. **Labels**
    a. SELinux User, Role, Type, Level, File
2. **Modes**
    a. **Enforcing -** record events in logs and take action on them by denying access
    b. **Permissive -** store events in logs, but take no actions on them; used for testing & trouble-shooting
    c. **Disabled -** SELinux turned off entirely; no recording of events in logs, nor actions taken for events
3. **Mask Setting**
    a. Override special permissions (most restrictive take precedence)

C. Target Policy

a. Target policy specifies what actions and access are enabled for users part of 'unconfined' and 'confined' domains in regards to particular processes

b. If a process is in the 'unconfined' domain, no restrictions are in place (default), leaving a large vulnerability

c. If a perpetrator is able to access a 'confined' service, their potential damage is limited to some extent because the process is restricted to run in its own domain.

D. Show/Select Enforcement Modes

a. Show current active mode:

   i. '**getenforce**' command

b. Set modes:

   i. Enforcing - '**setenforce 1**'

   ii. Permissive - '**setenforce 0**'

c. Turn SELinux on/off:

   i. Enable SELinux - '**selinux=1**'

   ii. Disable SELinux - '**selinux=0**'

B. ACCESS CONTROL LISTS

i

Access Control Lists are used to manage permission sets on files that are different from standard file permissions.

File systems must be mounted using:

1. The ACL option with the mount command
2. Edit the file system's entry in **/etc/fstab** config. file

XFS, ex3 and ex4 file systems come with ACL support enabled.

<u>Show minimal ACL settings on a file:</u> **'ls -l *filename.txt*'**

<u>Display detailed file ACL settings:</u> '**getfacl *filename.txt***'

Purpose	Operation
Display directory ACL	**getfacl /directory**
Named user with read/execute file permissions	**user: michael: rx file**
File owner with read/execute file permissions	**user: :rx file**
Read/write directory permissions given to directory group owner	**group : hug : rwx /director**
Read/execute permissions set as directory's default mask	**default : m : : rx /directory**

C. FIREWALLD

Firewalld is a dynamic firewall manager and front-end to **nftables'** framework. The firewalld RPM package includes the firewalld subsystem, which is included in a base installation, but not a minimal install.

With the use of zones, firewall management becomes simplified by classifying all network traffic.

Predefined firewalld Zones

Key:

▲ – reject incoming traffic unless related to outgoing traffic
🟥 - ssh
🟧 - mdns
⬜ – ipp-client
🟦 – samba-client
🟨 – dhcpv6-client

(squares are pre-defined services)

trusted	Allow all inc. traffic
home	▲ or matching 🟥🟧⬜🟦🟨
internal	▲ or matching 🟥🟧⬜🟦🟨 (same as home zone to start)
work	▲ or matching 🟥⬜🟨
public	▲ or matching 🟥🟨 **(default zone for new netw. ints.)**
external	▲ or matching 🟥 **(Outgoing IPv4 traffic forwarded through this zone is masqueraded to be originating from IPv4 of outgoing netw. int.)**
dmz	▲ or matching 🟥
block	▲
drop	Drop all inc. traffic, unless related to outgoing traffic (no ICMP error responding)

`firewall-cmd`

Command overview

Used to interact with firewalld for firewall setup or query of running configurations

--permanent	Save changes to permanent config. over reboot
--reload	Reload firewall rules & keep state info
--get-default-zone=	Return default zone for connections & ints.
--get-zones	Return predefined zones
--get-active-zones	Return only active zones with related ints. & sources
--add-source=	Add source for specified zone (zone omitted = default zone)
--remove-source	Remove binding of /list/source from specified zone (omitted zone = default zone)
--add-interface=	Bind specified interface to specified zone (zone omitted = default zone)
--remove-port=	Remove port number from specified zone (if zone omitted, default zone used)
--add-port=	Add port number to firewalld
--add-service=	Add network service to firewalld
--remove-service=	Remove network service from firewalld

D. SELINUX PORT SECURITY

In addition to fiile and process protection, an SELinux policy can also be used to enforce network traffic.

semanage port	
Command overview **Config. SELinux policy to control port num to port type definitions**	
-l	List records of specified object type
-a	Add record of specified object type
-t	SELinux type for object
-C	List local customizations
Example(s): Semanage port -a -t http_port_t -p tcp 1001	

By default, SELinux will block traffic on a service trying to run on a nonstandard port. For example, if a perpetrator appends the **/etc/httpd/conf** file to additionally listen on port 1001, **httpd.service** will not be allowed to run. This is because http is bound to port 80 by default.

The command **semanage port** above can be used to get around this. In the above example, http will be configured with **semanage port** to listen on port 1001.