information technology & management

viabiliitjit

INTRO TO OPEN SOURCE OPERATING SYSTEMS

ILLINOIS INSTITUTE OF TECHNOLOGY

ITMO456

Linux Troubleshooting & Security

Sean Hughes-Durkin

ITMO/IT-O 456 Fall 2017

Information Technology & Management Programs

School of Applied Technology

Objectives

At the end of this lesson students should be able to:

- Describe and outline common troubleshooting procedures
- Effectively troubleshoot common hardware- & software-related problems
- Monitor system performance using command-line and graphical utilities
- Identify and fix common performance problems

Objectives

At the end of this lesson students should be able to:

- Describe different facets of Linux security
- Increase the security of a Linux computer
  - Outline measures and utilities that can be used to detect a Linux security breach
- Explain the basics of SELinux
  - Describe SELinux running modes: enabled, disabled, permissive authentication

Objectives

At the end of this lesson students should be able to:

- Describe remote access facilities using the following:
  - SSH (secure tunnels, SFTP, X11 forwarding, keygen)

Troubleshooting Methodology

- After installing, configuring, and documenting your Linux system
  - You must maintain the system's integrity over time
- This includes:
  - Monitoring
  - Proactive maintenance
  - Reactive maintenance

Troubleshooting Methodology

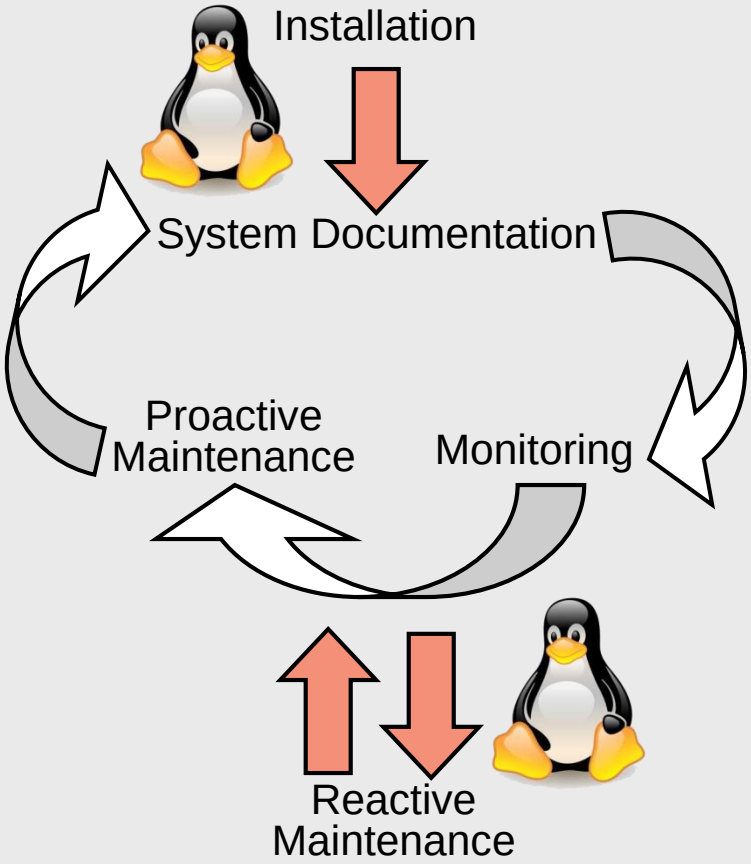


Figure 14-1: The maintenance cycle (penguins optional)

Troubleshooting Methodology

- Monitoring
  - Examining log files and running performance utilities system to identify problems and their causes
- Proactive maintenance
  - Measures taken to minimize chances of future system problems
  - e.g., perform regular system backups

Troubleshooting Methodology

- Reactive maintenance
  - Correcting problems when they arise
  - Documenting solutions
  - Developing better proactive maintenance methods
- Documentation
  - System information that is stored in a log book for future references
  - All maintenance actions should be documented

Troubleshooting Methodology

- Troubleshooting procedures
  - Tasks performed when solving system problems

Troubleshooting Methodology

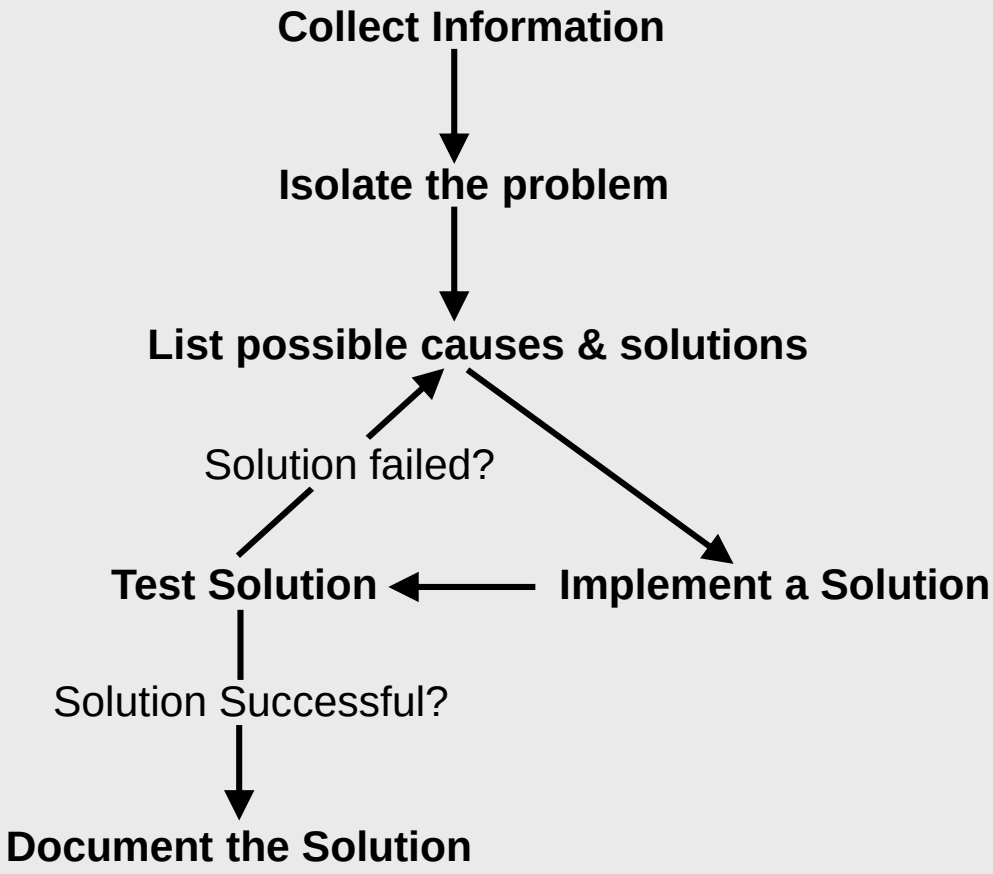


Figure 14-2: Common troubleshooting procedures

Troubleshooting Methodology

- Two troubleshooting golden rules
  - Prioritize problems according to severity
    - Spend a reasonable amount of time on each problem given its priority
    - Ask for help if you can't solve the problem
  - Try to solve the root of the problem
    - Avoid missing the underlying cause
    - Justify why a certain solution is successful

Resolving Common System Problems

- Three categories of problems:
  - Hardware-related
  - Software-related
  - User interface-related

Hardware-Related Problems

- Often involve improper hardware or software configuration
  - SCSI termination
  - Video card and monitor configuration
  - POST test alerts
    - Loose hardware connections
  - IRQ or I/O address conflicts
    - View output of **`dmesg`** command or **`journalctl -b`**
  - Problems specific to type of hardware
    - View output of **`dmesg`** command or **`journalctl -b`**
    - View content of **`/var/log/boot.log`**, **`/var/log/messages`**, **`jouranlctl`**

Hardware-Related Problems

- Absence of device drivers prevent OS from using associated devices
  - **`dmesg`** or **`lshw`**
    - Displays hardware detected by the kernel
  - **`lsusb`**
    - Displays USB devices detected by the kernel
  - **`lspci`**
    - Displays PCI devices detected by the kernel
  - Compare outputs of commands to output of **`lsmod`** to determine if driver module is missing from kernel

Hardware-Related Problems

- Hardware failure can render a device unusable
- HDDs most common device to fail
  - Good idea to use RAID

Hardware-Related Problems

- If HDD containing partitions mounted on noncritical directories fails:
  - Power down computer, replace failed HDD
  - Boot Linux system
  - Use **`fdisk`** to create partitions on new HDD
  - Use **`mkfs`** to create filesystems
  - Restore original data **(assumes backup!)**
  - Ensure **`/etc/fstab`** has appropriate entries to mount filesystems

Hardware-Related Problems

- If HDD containing the **/** filesystem fails
  - Power down computer replace the failed hard disk
  - Reinstall Linux on the new hard disk
  - Restore the original configuration and data files using a back-up utility
    - (**Important:** This assumes you have a current back-up not on the failed hard drive!)

Hardware-Related Problems

- Saving the disk if the bootsector is corrupt or the boot partition has failed
  - Install a new hard drive and do a clean install of Linux
  - Mount the appropriate partition from the old drive (assuming new drive is **hda**)

    ```
    mkdir /mnt/olddrive
    mount /dev/hdb1 /mnt/olddrive
    ```
  - Copy the necessary user, system and configuration files to the new drive

Software: Proactive Maintenance

- Software-related problems are typically more difficult to identify and resolve than hardware-related problems
- Identify whether the softwarerelated problem is related to application software or operating system software

Software: Proactive Maintenance

- Update packages!
  - Run **`yum update`** or **`apt-get update`** on a regular basis to ensure latest version of all packages are installed
    - Even though Linux viruses are rare, malicious attackers will exploit almost any system vulnerability
    - Regular updates minimize vulnerabilities; Linux is no different than Microsoft in this regard

Software: Application-Related Problems

- Reasons for failures: Missing program libraries/files, process restrictions, or conflicting applications
- Dependencies
  - Prerequisite shared libraries or packages required for program execution
  - Programs usually check dependencies at installation
  - Package files may be removed accidentally

Software: Application-Related Problems

- **`rpm -V`** command
  - Identify missing files in a package or package dependency
- **`ldd`** command
  - Used to display shared libraries used by a certain program
- **`ldconfig`** command
  - Updates **`/etc/ld.so.conf`** and **`/etc/ld.so.cache`** files

Software: Application-Related Problems

- **`/etc/ld.so.conf`** files
  - File that contains a list of directories that contain shared libraries
- **`/etc/ld.so.cache`** file
  - File that contains the location of shared library files
- compressor/decompressor (codec) file
  - Contains rules to compress or decompress multimedia information

Software: Application-Related Problems

- Too many running processes
  - Solve by killing parent process of zombie processes
- Filehandles
  - Connection that a program makes to files on a filesystem
- **`ulimit`** command
  - Modify process limit parameters in the current shell
    - Can also modify max number of filehandles

Software: Application-Related Problems

- **`/var/log`** directory
  - Contains most system log files
- If applications stop functioning due to difficulty gaining resources, restart using SIGHUP
  - Determine if another process is trying to access the same resources
    - Attempt to start app in Single User Mode
    - If resource conflicts caused the problem, download newer version of application or application fix

Software: OS-Related Problems

- Most software-related problems related to the OS itself
  - X windows, boot loader, and filesystem problems
- Problem detecting video card or monitors by the kernel
  - To isolate problem starting X Windows or gdm:
    - View **`/var/log/Xorg.0.log`** file
    - Execute **`xwininfo`** or **`xdpyinfo`**

Software: OS-Related Problems

- GRUB and GRUB2 problems
  - Typically result of missing files in **`/boot`**
- Ensure Linux kernel resides before 1024th cylinder and lba32 keyword is in configuration file
  - Eliminates BIOS problems with large HDDs

Software: OS-Related Problems

- If filesystem on partition mounted to noncritical directory (**`/home, /var`**) becomes corrupted
  - Unmount filesystem
  - Run **`fsck`** command with **`-f`** (full) option
  - If **`fsck`** command cannot repair filesystem, use **`mkfs`** command to re-create the filesystem
  - Restore filesystem's original data

Software: OS-Related Problems

- If `/` filesystem is corrupted:
  - Boot from Fedora installation media and enter System Rescue
  - At shell prompt within System Rescue:
    - Use **`mkfs`** to recreate the filesystem
    - Use backup utility to restore original data to the re-created `/` filesystem
  - Exit System Rescue and reboot system

Software: OS-Related Problems

- Lost root password
  - Boot into single user mode
    - At GRUB opening screen, type **e**
    - When the edit screen appears, scroll to the line with "**kernel**" as the first word and type **e**
    - Add a space and a **1** to the end of the kernel line and press **Enter**
    - Type **b** to boot
  - In the single-user mode, type passwd
  - Enter the new root password
  - Type **exit** and press **Enter**

Software: OS-Related Problems

- Using “boot-from-CD” Linux versions like Knoppix Linux / SystemRescueCd
  - These can be used for a wide variety of troubleshooting when the system has problems booting from the hard drive
- If you have a floppy drive, make sure you have a boot floppy as well
  - In systems in secure areas or at home, just leave it sitting in the floppy drive but not pushed all the way in

Software: OS-Related Problems

- Knoppix Linux, Ubuntu Rescue Remix, and SystemRescueCd
  - Bootable CD-based Linux distributions containing many filesystem repair utilities
- **`setserial`** command
  - Set IRQ, I/O address, and speed of serial devices

Software: User Interface Problems

- Assistive technologies: tools that users can use to modify their desktop experience
  - Configured within Fedora 20 using the Universal Access utility
    - Turn on the Always Show Universal Access Menu option to enable and disable each assistive technology using the Universal Access icon in the upper right of the GNOME desktop

Software: User Interface Problems

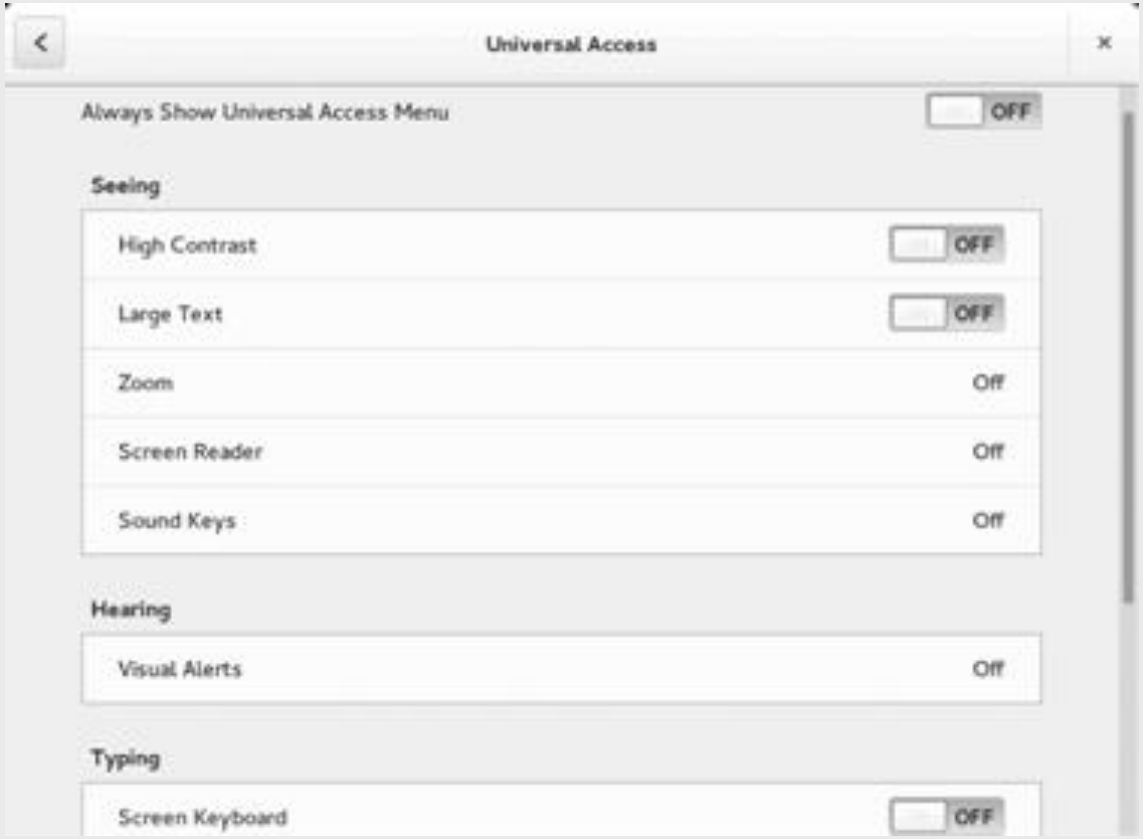


Figure 14-3: The Universal Access utility

Performance Monitoring

- Improperly configured hardware might still work, but at a slower speed
- Jabbering
  - Failing hardware components send large amounts of information to the CPU
- Other causes of poor performance
  - Software monopolizes system resources
  - Too many processes
  - Too many read/write requests to HDD
  - Zombie processes

Performance Monitoring

- To solve software performance issues:
  - Remove software from the system
  - Move software to another Linux system
  - Add CPU or otherwise alter hardware
- Bus mastering
  - Peripheral components perform tasks normally executed by CPU
  - Reduces the amount of processing CPU must perform & increases system speed

Performance Monitoring

- Ways to increase performance
  - Add RAM
  - Upgrade to faster HDDs
  - Disk Striping RAID
  - Decrease kernel size

Performance Monitoring

- Run performance utilities on a regular basis
  - Record results in a system log book
  - Eases identification of performance problems
- Baseline
  - Measure of normal system activity

Monitoring Performance with sysstat

- System Statistics (**`sysstat`**) package
  - Contains wide range of system monitoring utilities such as **`mpstat`**, **`iostat`**, **`sar`**, **`isag`**
  - **Not included** in current distributions of Linux – (use KDE System Guard instead)
  - Use **`yum install sysstat`** or **`apt-get install sysstat`** to install

Monitoring Performance with sysstat

- Multiple Processor Statistics (**`mpstat`**) utility
  - Command that displays CPU statistics
  - Used to monitor CPU performance
  - Can specify interval and number of measurements rather than displaying average values
  - **`%sys`** should be smaller than **`%usr`** and **`%nice`** combined

Monitoring Performance with sysstat

- Input/Output Statistics (**`iostat`**)
  - Measures flow of information to and from disk devices
  - Displays CPU statistics similar to **`mpstat`**
  - Displays statistics for each disk device on the system
  - Output includes:
    - Transfers per second
    - Number of blocks read and written per second
    - Total number of blocks read and written for the device

Monitoring Performance with sysstat

- System Activity Reporter (**sar**) command
  - Displays various system statistics taken in the last day
  - Provides more information than **`mpstat`** and **`iostat`**
  - By default scheduled to run every 10 minutes
    - Output logged to a file in **`/var/log/sa`** directory
  - **`-f`** option: View statistics from a specific file
  - Can take current system measurements

Monitoring Performance with sysstat

- Additional **`sar`** options:
  - **`-q`** option: Displays processor queue statistics
    - **`runq -sz`** value: Number of processes waiting for execution on processor run queue
    - **`plist -sz`** value: Indicates number of processes currently running
    - **`ldavg`** values: Represent average CPU load
  - **`-W`** option: Displays number of pages sent to and taken from swap partition
    - Large number causes slower performance
    - Add RAM to resolve

Monitoring Performance with sysstat

Option	Description
`-A`	Displays the most information; this option is equivalent to all options
`-b`	Displays I/O statistics
`-B`	Displays swap statistics
`-d`	Displays Input/Output statistics for each block device on the system
`-f file_name`	Displays information from the specified file; these files typically reside in the /var/log/sa directory
`-n ALL`	Reports all network statistics
`-o file_name`	Saves the output to a file in binary format
`-P CPU#`	Specifies statistics for a single CPU (the first CPU is 0, the second CPU is 1, and so on)
`-q`	Displays statistics for the processor queue
`-r`	Displays memory and swap statistics
`-R`	Displays memory statistics
`-u`	Displays CPU statistics; this is the default action when no options are specified
`-v`	Displays kernel-related filesystem statistics
`-W`	Displays swapping statistics

Table 14-1: Common options to the `sar` command

Monitoring Performance with sysstat

- Large number of pages being sent to and taken from the swap partition
  - System will suffer from slower performance
  - Add more physical memory (RAM) to resolve
- Interactive System Activity Grapher (**`isag`**) command
  - Used to graph system performance information stored in the **`/var/log/sa`** directory

Other Performance Monitoring Utilities

- **`top`** command
  - Displays CPU statistics, swap usage, memory usage and average CPU load
- **`free`** command
  - Displays total amounts of physical and swap memory and their utilizations
  - Can be used to indicate whether more physical memory is required

Other Performance Monitoring Utilities

- **`vmstat`** command
  - Displays memory, CPU, & swap statistics
  - Can be used to indicate whether more physical memory is required
- System Monitor
  - Current GUI tool for performance monitoring
  - Generally GNOME System Manager
    - May be desirable to use KDE System Guard instead

Security

- Linux systems typically made available across networks such as the Internet
  - More prone to security loopholes and attacks
- To protect Linux systems, you should
  - Improve local and network security
  - Understand how to detect intruders who breach the system

Securing the Local Computer

- Limit access to the physical computer
  - Prevent malicious users from accessing files by directly booting the computer with their own device
  - Remove floppy, CD, and DVD drives from workstations
- Server closet
  - Secured room to store servers

Securing the Local Computer

- Ensure BIOS prevents booting from USB ports
  - Ensure BIOS password is set
- Set boot loader password in LILO or GRUB configuration file
  - Prevents intruder from interacting with boot loader

Securing the Local Computer

- Limit access to graphical desktops and shells
  - Exit command-line shell before leaving computer
    - The **nohup** command prevents background processes from being killed when parent shell is killed or exited
  - Lock screen using GNOME or KDE

Securing the Local Computer

- Minimize root user's time logged in
- **`su`** (switch user) command
  - Switch current user account to another
  - Used to switch between root user and regular user
- **`sudo`** command
  - Perform commands as another user if you have the rights to do that listed in **`/etc/sudoers`** file

Protecting Against Network Attacks

- Always a possibility that hackers can manipulate a network service by interacting with it in unusual ways
- Buffer overrun
  - Could allow program information for a network service to be altered in memory

Network Security Essentials

- Minimize number of running network services
- **`nmap`** (network mapper) command
  - Scans ports on network computers
  - Allows users to determine what network services are running
- Ensure that services not needed are not automatically started when entering the runlevel

Protecting Against Network Attacks

```
[root@itm456fedora itm456]# nmap -sT localhost

Starting Nmap 5.21 ( http://nmap.org ) at 2010-11-22 18:42
CST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0011s latency).
Hostname localhost resolves to 2 IPs. Only scanned 127.0.0.1
rDNS record for 127.0.0.1: itmo456fedora
Not shown: 996 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
111/tcp open  rpcbind
631/tcp open  ipp

Nmap done: 1 IP address (1 host up) scanned in 0.67 seconds
```

Protecting Against Network Attacks

- **`netstat`** (network state) command
  - Monitor network port usage
  - **`-ap`** shows all ports listening or connected and process using the port
  - **`-lp`** shows only posts listening and process using the port

Protecting Against Network Attacks

```
[root@itmo456fedora itmo456]# netstat -lp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State       PID/Program name
tcp        0      0 *:ssh                       *:*                         LISTEN      1471/sshd
tcp        0      0 itm456fedora:ipp            *:*                         LISTEN      1257/cupsd
tcp        0      0 itm456fedora:smtp           *:*                         LISTEN      1495/sendmail: acce
tcp        0      0 *:41289                     *:*                         LISTEN      1214/rpc.statd
tcp        0      0 *:sunrpc                    *:*                         LISTEN      1152/rpcbind
tcp        0      0 *:ssh                       *:*                         LISTEN      1471/sshd
tcp        0      0 localhost:ipp               *:*                         LISTEN      1257/cupsd
tcp        0      0 *:43882                     *:*                         LISTEN      1214/rpc.statd
tcp        0      0 *:sunrpc                    *:*                         LISTEN      1152/rpcbind
udp        0      0 *:38549                     *:*                                     1214/rpc.statd
udp        0      0 *:mdns                      *:*                                     1198/avahi-daemon:
udp        0      0 *:ideafarm-panic            *:*                                     1152/rpcbind
udp        0      0 *:966                       *:*                                     1214/rpc.statd
udp        0      0 *:42997                     *:*                                     1198/avahi-daemon:
udp        0      0 *:bootpc                    *:*                                     1194/dhclient
udp        0      0 *:sunrpc                    *:*                                     1152/rpcbind
udp        0      0 *:ipp                       *:*                                     1257/cupsd
udp        0      0 10.0.2.15:ntp               *:*                                     1479/ntpd
udp        0      0 itm456fedora:ntp            *:*                                     1479/ntpd
udp        0      0 *:ntp                       *:*                                     1479/ntpd
udp        0      0 *:59571                     *:*                                     1214/rpc.statd
udp        0      0 *:ideafarm-panic            *:*                                     1152/rpcbind
udp        0      0 *:sunrpc                    *:*                                     1152/rpcbind
udp        0      0 fe80::a00:27ff:fea2:ntp     *:*                                     1479/ntpd
udp        0      0 localhost:ntp               *:*                                     1479/ntpd
udp        0      0 *:ntp                       *:*                                     1479/ntpd
```

Protecting Against Network Attacks

```
[root@itmo456fedora itmo456]# # lsof -i
COMMAND  PID        USER    FD TYPE  DEVICE   SIZE  NODE  NAME
ssh     2498     rodsmith   3u IPv4  3292662       TCP   ➦
nessus.rodsbooks.com:53106->seeker.rodsbooks.com:ssh (ESTABLISHED)
exim4   4827  Debian-exim   5u IPv4  3369596       TCP   *:smtp (LISTEN)
sshd    4997         root   3u IPv4  13273         TCP   *:ssh (LISTEN)
```

Protecting Against Network Attacks

- **`lsof -i`** (list open files) command
  - Returns a list of all open files and the processes that opened them
  - **`-i`** lists IP sockets, showing files connecting to the network
  - Can be used instead of **`netstat`**
- Enable encryption on essential network services

Protecting Against Network Attacks

- TCP wrapper
  - Run network daemon with additional security via **`/etc/hosts.allow`** and **`/etc/hosts.deny`** files
  - Not normally used with **`xinitd`**
- Examine permissions for files and directories associated with system and network services

Network Security Essentials

- Ensure network service daemons for essential services not run as root user when possible
- Ensure shell listed in **`/etc/passwd`** for daemons is set to **`/sbin/nologin`**
  - Hacker cannot get BASH shell
- New network service versions usually include fixes for known network attacks
  - Keep network services up-to-date

Securing the Operating System

- Manage users
  - Set up user accounts for each user
  - Use groups for shared resources/ privileges
  - Require strong passwords
  - Use password expiration

Securing the Operating System

- Strong Passwords
  - Password: a private word or combination of characters that only the user should know
- Good rule of thumb for passwords:
  - At least 8 characters long but 9 is best
  - Contain at least one numeral
  - Contain at least one special character (i.e. ~!@#$%^&*()_+|\`{}[]:";'<>?,./)

firewalld Service

- firewalld used in Fedora
  - Replacing iptables
- Does not need to be reloaded
  - Changes added dynamically
- Must change firewall settings using firewalld service
- Managed by systemd

firewalld Service

- Netfilter
  - Runs in kernelspace
  - Set of tables that hold rules the kernel uses to control network packet filtering
  - Requires front end
- Firewalld
  - Runs in userspace
  - Allows admin to configure firewall rules

firewalld Configuration

- Runtime config
  - Changes ruleset dynamically
- Permanent config
  - Changes ruleset on reboot/service restart

firewalld Configuration

- Zones
  - Defines a level of trust for a network connection
  - May change based on location
    - Airport vs work
  - Default zone is public
- Services
  - Define protocol, port and optionally destination

firewalld Configuration

Table 25-1 The **firewalld** zones

Zone	Function
drop	Drop incoming packets with no reply; allow outgoing connections
block	Reject incoming connections with icmp-host-prohibited (ipv4) or icmp6-adm-prohibited (ipv6); allow outgoing connections; see page 1254 for a definition of ICMP
public	Do not trust other systems not to harm the local system; accept the **ssh**, **mdns**, and **dhcpv6-client** services (the default zone)
external	Do not trust other systems not to harm the local system; for use on external networks with masquerading enabled (especially for routers); accept selected incoming connections
dmz	For use on publicly accessible computers in the local DMZ (page 890) that have limited access to the local network; accept selected incoming connections
work	Mostly trust other systems not to harm the local system; accept selected incoming connections
home	Mostly trust other systems not to harm the local system; accept selected incoming connections
internal	Mostly trust other systems not to harm the local system; accept selected incoming connections
trusted	Completely trust other systems not to harm the local system; accept all connections

firewalld Configuration

- Can configure via GUI or cmd line
- Use **`firewall-config`** for GUI interface
- Use **`firewall-cmd`** for command line interaction

firewall-config

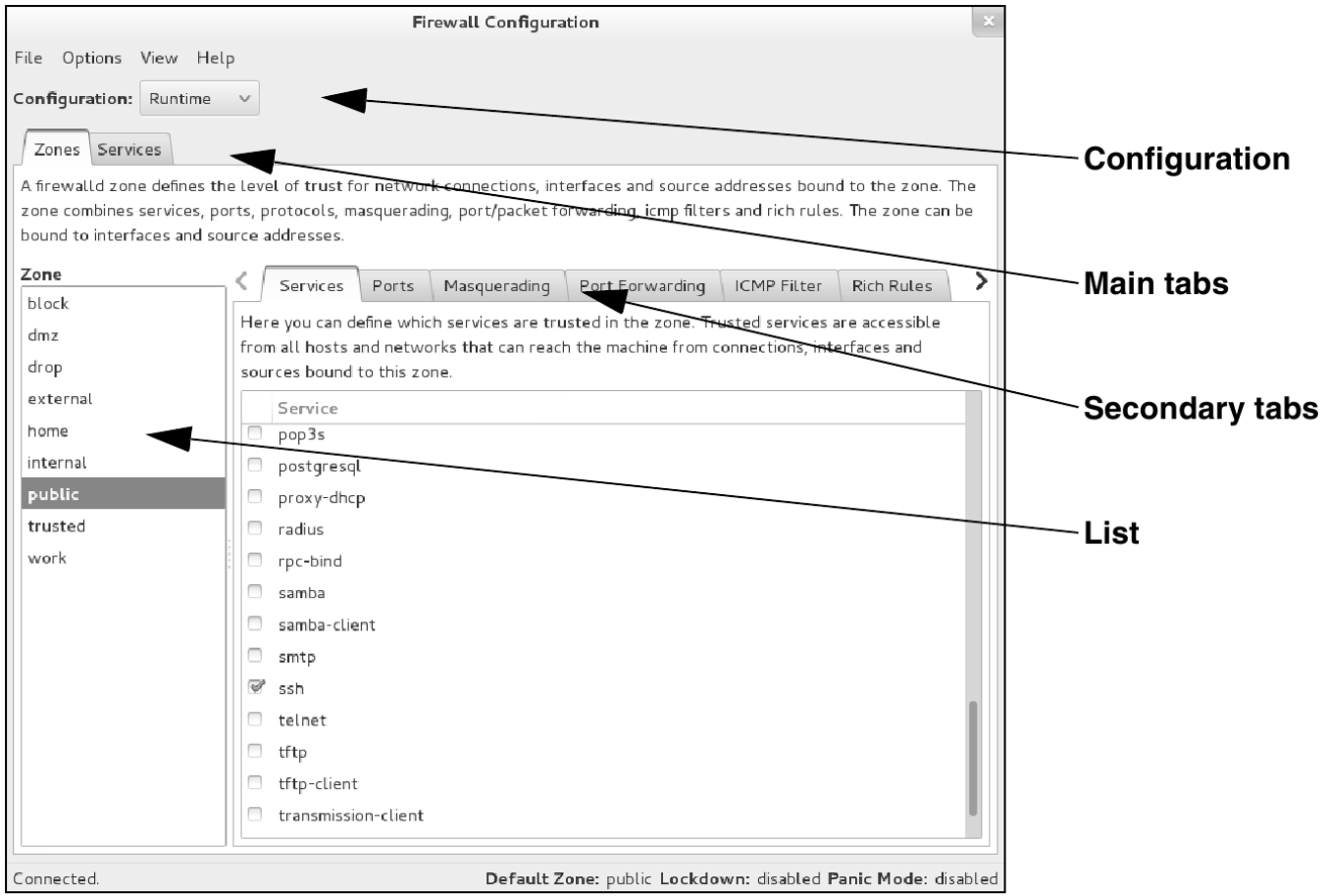


Figure 25-1 Firewall Configuration window

firewall-cmd

```
[student@localhost ~]$ firewall-cmd --state
running
[student@localhost ~]$ firewall-cmd --get-default-zone
public
[student@localhost ~]$ firewall-cmd --get-active-zones
public
  interfaces: eno16777736
[student@localhost ~]$ firewall-cmd --list-services
dhcpv6-client mdns ssh
[student@localhost ~]$ firewall-cmd --permanent --list-services
dhcpv6-client mdns ssh
[student@localhost ~]$
```

firewall-cmd

```
[student@localhost ~]$ firewall-cmd --add-service=http
success
[student@localhost ~]$ firewall-cmd --add-service=https
success
[student@localhost ~]$ firewall-cmd --list-services
dhcpv6-client http https mdns ssh
[student@localhost ~]$
```

firewall-cmd

```
[student@localhost ~]$ firewall-cmd --permanent --add-service=http
success
[student@localhost ~]$ firewall-cmd --permanent --add-service=https
success
[student@localhost ~]$ firewall-cmd --permanent --list-services
dhcpv6-client http https mdns ssh
[student@localhost ~]$
```

firewall-cmd

```
[student@localhost ~]$ firewall-cmd --permanent --remove-service=http
success
[student@localhost ~]$ firewall-cmd --permanent --remove-service=https
success
[student@localhost ~]$ firewall-cmd --permanent --list-services
dhcpv6-client mdns ssh
[student@localhost ~]$
```

firewall-cmd

```
[root@localhost ~]# firewall-cmd --add-port=80/tcp
success
[root@localhost ~]# firewall-cmd --add-port=443/tcp
success
[root@localhost ~]# firewall-cmd --list-ports
443/tcp 80/tcp
[root@localhost ~]#
```

iptables

- IPTables is flexible and extensible, allowing you to set up both simple and complex network packet filtering in the Linux kernel
- Netfilter
  - Discussed previously
- IPTables
  - Runs in userspace to control packet filtering

Iptables Enabling Service

```
[root@itm456 ~]# systemctl mask firewalld
ln -s '/dev/null' '/etc/systemd/system/firewalld.service'
[root@itm456 ~]# systemctl enable iptables
[root@itm456 ~]# vi /etc/sysconfig/iptables
[root@itm456 ~]# systemctl stop firewalld
[root@itm456 ~]# systemctl start iptables
[root@itm456 ~]# iptables -nL
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:443
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:22
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:80
REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

iptables Syntax

- **iptables –flush or iptables -F**
- **iptables --policy INPUT DROP or –P can be used**
- **iptables --policy OUTPUT DROP or –P can be used**
- **iptables --policy FORWARD DROP or –P can be used**

Firewall Services: Commands

Option	Description
-s address	Specifies a source address of packets for a rule.
-d address	Specifies the destination address of packets for a rule.
-p protocol	Specifies the protocol type for a rule.
-j action	Specifies the action that is taken for a rule.
-L chain	Lists rules for a certain chain. If no chain is specified, all chains are listed.
-P chain policy	Specifies the default policy for a certain chain type.
-D number	Deletes a rule for a chain specified by additional arguments. Rules start at number 1.
-R number	Replaces a rule for a chain specified by additional arguments. Rules start at number 1.
-F chain	Removes all rules for a certain chain. If no chain is specified, it removes all rules for all chains.

Table 14-2: Common **`iptables`** commands

iptables Targets

- ACCEPT
  - let the packet through
- DROP
  - drop the packet
- QUEUE
  - pass the packet to the userspace

Iptables Chains

- INPUT chain
  - Incoming to the system
- OUTPUT chain
  - Outgoing from the system
- FORWARD chain
  - Passing from one interface to another
    - Eg: eth1 to eth2 (2 different networks)

iptables Sample Rules

Inbound SSH

```
iptables -A INPUT -i eth0 -p tcp --dport 22
-m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 22
-m state --state ESTABLISHED -j ACCEPT
```

Outbound DNS

```
iptables -A OUTPUT -o eth0 -p udp --dport 53
-j ACCEPT
iptables -A INPUT -i eth0 -p udp --sport 53
-j ACCEPT
```

iptables Logic

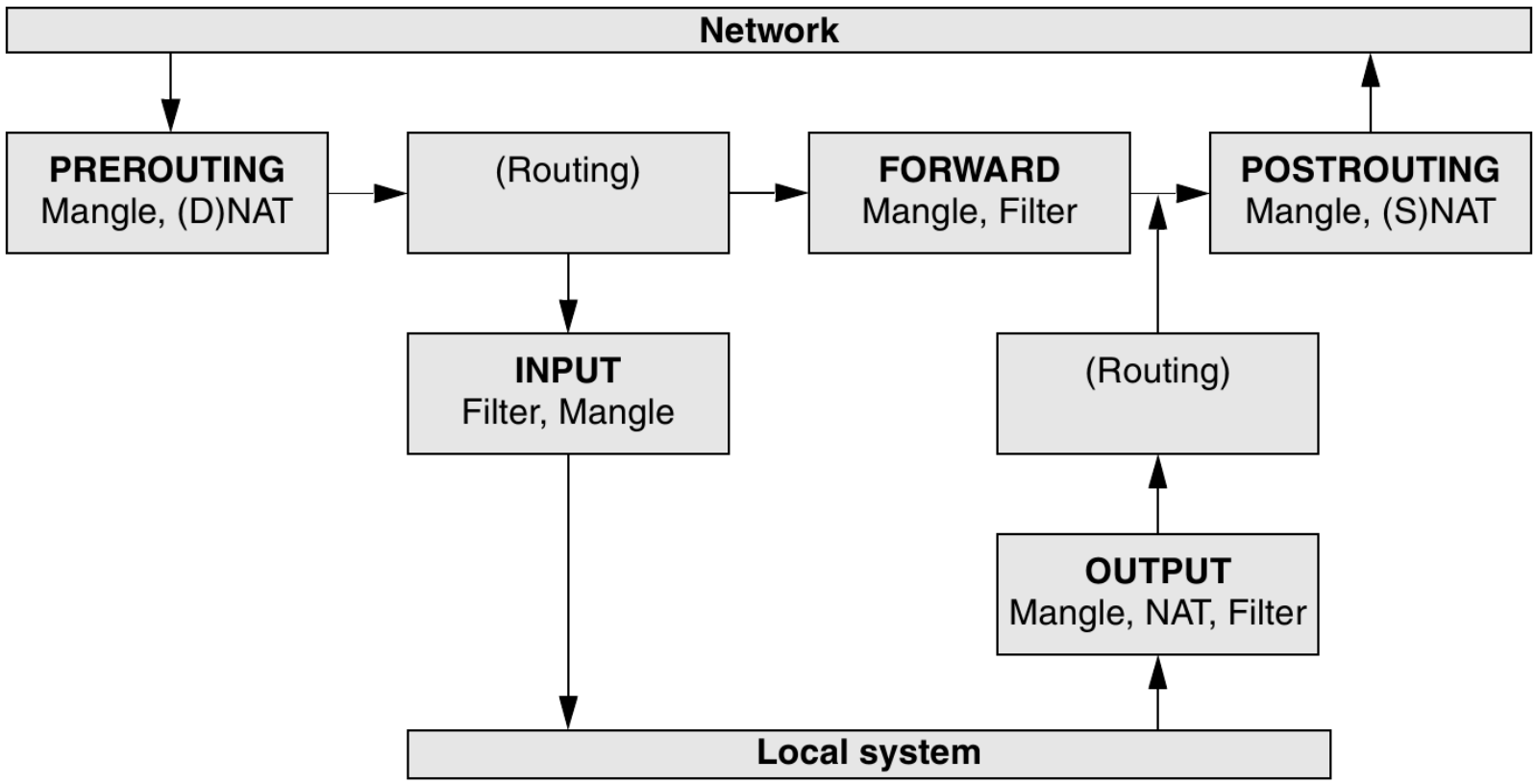


Figure 25-5 Filtering a packet in the kernel

Detecting Intrusion

- Log files can contain information or irregularities indicating an intrusion
- Review system log files associated with authentication
- Pluggable Authentication Module (PAM)
  - Handles authentication requests by daemons
  - Log file in **`/var/log/secure`**

Detecting Intrusion

- Check **`who /var/log/wtmp`** log file
  - Lists users who receive BASH shells
- **`lsof`** (list open files) command: lists files that are currently being edited
- Periodically search for files that have SUID bit set
- Tripwire Monitors files and directories
- Intrusion Detection System (IDS) used to detect intruders on a system

Detecting Intrusion (continued)

Name	Description
Snort	A complex IDS that can be used to capture and monitor network packets. It can be used to detect a wide range of network attacks and port probing.
Advanced Intrusion Detection Environment (AIDE)	An alternative to tripwire that has added functionality for checking the integrity of files and directories.
Integrity Checking Utility (ICU)	A Perl-based program that is designed to work with AIDE to check the integrity of Linux computers remotely across a network.
PortSentry	An IDS that monitors traffic on all ports and allows you to detect whether crackers are probing your ports using port scanning utilities such as nmap
Linux Intrusion Detection System (LIDS)	An IDS that involves modifying the Linux kernel to increase process and file security as well as detect security breaches. Now outdated.
Simple WATCHer (SWATCH)	Monitors log files and alerts administrators when an intrusion is detected. Written in Perl.

Common Linux intrusion detection systems

SELinux

- A system to enforce security policies including DOD-style mandatory access controls
- Uses Linux Security Modules (LSM) included in the Linux kernel
- Has several modes: enabled, disabled, permissive authentication
- Works by mapping Linux users to confined SELinux users

Configuring SELinux

- By default, configured and enabled during Fedora installation
  - Series of kernel patches and utilities created by NSA
    - Enforces role-based security
- To enable, edit **`/etc/selinux/config`**
  - Configure SELINUXTYPE option

```
SELINUX = enforcing
SELINUX = permissive
SELINUX = disabled
```

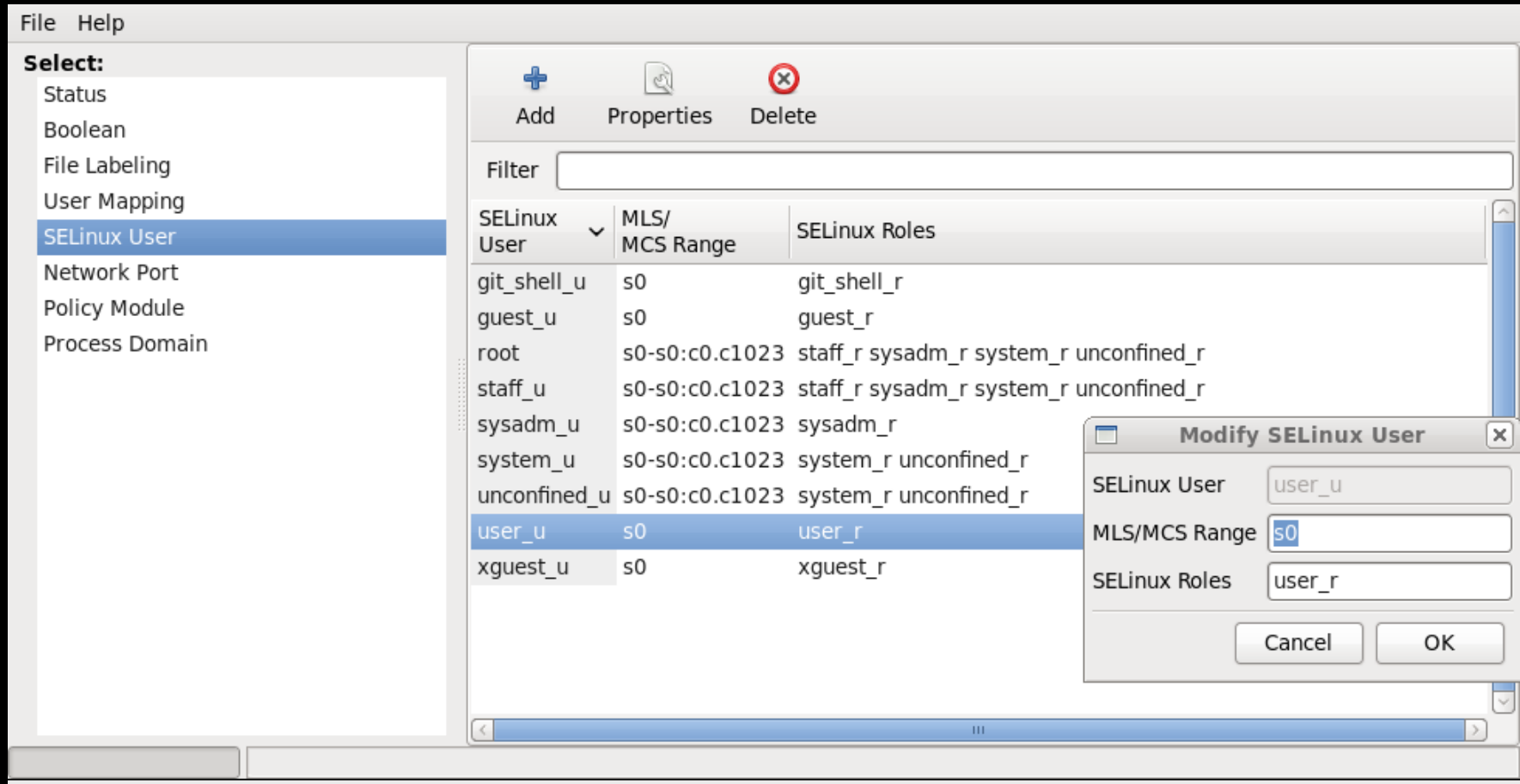
Configuring SELinux

- Next, select an SELINUX policy by configuring one of the following options within **`/etc/selinux/config:`**

  `SELINUXTYPE = targeted`

  `SELINUXTYPE = strict`
- After enabling SELinux, you must reboot to relabel the system for the changes to take effect
- **`sestatus`** command
  - View current SELinux status

SELinux



SELinux User Configuration Window

ITMO456

SELinux Permissive Authentication

- Permissive Mode is a state in which SELinux restrictions are not enforced, but SELinux policy violations that would have normally been prevented are audited and logged
  - Used for troubleshooting/debugging SELinux issues

Configuring AppArmor

- AppArmor: alternative to SELinux that provides similar protection
  - Consists of a kernel module and utilities that can be used to associate a set of restrictions for individual programs on a Linux system
- Restrictions stored within text files under the **`/etc/apparmor.d`** directory
  - Each file is called an AppArmor profile
- To view AppArmor profiles, run **`apparmor_status`**

Configuring AppArmor

- To switch an AppArmor profile to enforce mode, use **`aa-enforce`**
- Use **`aa-complain`** to switch an AppArmor profile to complain mode

Using Encryption to Protect Network Data

- Use encryption algorithms to protect data before it's transmitted
- Asymmetric encryption uses pair of keys uniquely generated on each system
  - Public key is freely distributed
  - Private key is used only by the system, never distributed
    - Can be used to authenticate messages
- Digital signature
  - Message encrypted using a private key

Communicating Securely with **ssh**

- The secure shell daemon (**sshd**) establishes a secure connection using public-key encryption to run a shell or other protocols between systems
- Can be used for X11 port forwarding allowing secure remote GUI access
- Can also be used a a *tunneling protocol* to allow encrypted forwarding of normally unencrypted ports such as **smb**

Communicating Securely with `ssh`

- Always provides SFTP, a secure FTP implementation tunneled though **`ssh`**
  - Works the same as FTP except securely
- Uses a *keygen* to generate public/ private key pairs & to forward private keys using the initial public key
  - Also supports use of external mechanisms such as Kerberos 5 or NTLM, providing single sign-on capability

OpenSSH History

- SSH1, originally completely free with source code, then license changed with version 1.2.13
- SSH2, originally only commercial, but now free for some uses.
- OpenSSH team took the last free SSH1 release, fixed bugs & security issues, added features, and added support for the SSH2 protocol.

OpenSSH How it Works

- How it works
  - Starts an encrypted connection
  - Then authenticates the user
- Keys
  - Uses host key and session key to negotiate an encrypted connection
- Host Key
  - Public/private key pair that is established the first time the server runs **sshd**

OpenSSH How it Works

- Session Key
  - Symmetric key that the server and client share to encrypt the connection
- The first time a ssh client connects to the ssh server, the client is required to accept the servers public key
  - This public key is stored in the known_hosts file on the client
  - This is to prevent MiTM attacks
  - When client connects again, the key stored is compared to the key provided by the server

OpenSSH How it Works

- Session Key continued
  - Client generates a random key
  - Client uses servers public host key to encrypt random key and sends to server
  - Server uses private host key to decrypt message for random key
  - Random key becomes the session key to encrypt communication

OpenSSH Global Files

- Located in **`/etc/ssh/`** directory
- Contains server and client configurations
  - **`sshd_config`**
  - **`ssh_config`**
- Contains server's hostkey file used to identify remote server
  - Used to identify server
  - Prevent MiTM attacks

OpenSSH User Files

- Located in **`~/.ssh/`** directory
- Contains certain files
  - **`authorized_keys`**
    - Used for public key authentication
  - **`id_rsa and id_rsa.pub`**
    - Keys used for authentication to remote server
  - **`known_hosts`**
    - Contains public RSA key of servers
      - Used to identify server and prevent MiTM

OpenSSH MiTM Message

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
f1:6f:ea:87:bb:1b:df:cd:e3:45:24:60:d3:25:b1:0a.
Please contact your system administrator.
Add correct host key in /home/sam/.ssh/known_hosts to get rid of this message.
Offending key in /home/sam/.ssh/known_hosts:1
RSA host key for plum has changed and you have requested strict checking.
Host key verification failed.
```

OpenSSH Port Forwarding

- I want to listen on port 5110 on this machine; all packets arriving here get sent to mailserver, port 110:
  - **`ssh –L 5110:mailserver:110 mailserver`**

OpenSSH Key Creation

- **`ssh-keygen -t rsa`**
- Prompts where to store the file
- Prompts for passphrase
  - Used to encrypt the private key

OpenSSH Public Key Auth

- On local system
  - After running **`ssh-keygen`** take the contents of **`~/.ssh/id_rsa.pub`**
- On remote server
  - Copy the id_rsa.pub to **`~/.ssh/authorized_keys`**
  - Uncomment lines in sshd_config to allow public key auth
    - **`PubkeyAuthentication yes`**
    - **`AuthorizedKeysFile>.ssh/authorized_keys`**
- Can use **ssh-copy-id** command to copy keys to remote system

OpenSSH Troubleshooting

- Review logs
  - /var/log/secure
  - /var/log/messages
- Use verbosity on client
  - Will display debug information
  - **ssh -v user@machine**
- Debug from the server
  - With root privileges run
    - **/usr/sbin/sshd -de**
  - Runs server in foreground and displays server information to terminal

Working with GPG

- Open source version of PGP
- Each user has a key pair used for encryption and authentication
  - Authentication uses trust model
- Typically uses RSA and DSA key pairs for asymmetric encryption and digital signing
- Can manage GPG keys and encrypt data using:
  - **gpg** command
  - Graphical utility such as Passwords and Encryption Keys utility

Access Control Devices

- Access control encompasses two processes:
  - Confirming identity of entity accessing a logical or physical area (authentication)
  - Determining which actions that entity can perform in that physical or logical area (authorization)
- A successful access control approach—whether intended to control physical access or logical access—always consists of both authentication and authorization

Authentication Mechanisms

- Mechanism types:
  - Something you know
  - Something you have
  - Something you are
  - Something you produce
- Strong authentication uses at least two different authentication mechanism types (two-factor authentication)

Authentication Architectures

- PAM (pluggable authentication modules)
  - Allows programs using authentication to be written independently of the underlying authentication scheme
  - Implemented in Linux
- LDAP (Lightweight Directory Access Protocol)
  - Directory structure for organizing info on system users/account holders
  - Intended to be public and may not be secure unless used with other protocols

Authentication Architectures

- RADIUS (Remote Authentication Dial In User Service)
  - Provides centralized Authentication, Authorization, and Accounting (AAA) management to connect to and use a network service
- RADIUS used to
  - authenticate users or devices before granting them access to a network
  - authorize those users or devices for certain network services and
  - account for usage of those services

Authentication Architectures

- *Two-factor authentication* uses two different factors in conjunction to authenticate a user
  - Could be a password and a token, password and a digital certificate, password and biometric info, password and a smart card, PIN and a smart card
  - U.S. government uses password or PIN and a smart card
  - More secure

Access Control Tokens

Access Control Tokens

Source: RSA Security

Smart Cards

Smart Cards In Use

Securing Linux

- Securing a Linux computer involves improving local and network security as well as monitoring to detect intruders
- By restricting access to your Linux computer and using the root account only when required, you greatly improve local Linux security

Securing Linux

- Reducing the number of network services, using firewalls, preventing services from running as the root user, restricting permissions on key files, and using TCP wrappers can greatly reduce the chance of network attacks
- Log files and IDS applications can be used to detect intruders on a Linux network

Summary

- Administrators monitor the system, perform proactive/reactive maintenance, and document system information
- Common troubleshooting procedures involve:
  - Isolating and determining the cause of system problems and implementing and testing solutions that can be documented for future use

Summary

- Invalid hardware settings, absence of device drivers, and hard disk failure are common hardware-related problems
- Software-related problems can be application-related or OS-related
- Users can use assistive technologies to modify their desktop experience

Summary

- System performance is affected by a variety of hardware & software factors
  - Using performance monitoring utilities to create a baseline is helpful for diagnosing future performance problems
- Securing a Linux computer involves:
  - Improving local and network security and monitoring to detect intruders

Summary

- Greatly improve local security by:
  - Restricting access to the computer and using root account only when required via su and sudo commands
- Reduce chance of network attacks by:
  - Reducing number of network services, implementing firewalls, SELinux, service updates, encryption, and TCP wrappers, and restricting services from running as root user and permissions on key files

Summary

- Analyzing log files and key system files and running IDS applications can be used to detect intruders

The End…

- Questions?