RED HAT :: BOSTON :: 2008

SUMMIT

JUNE 18–20, 2008

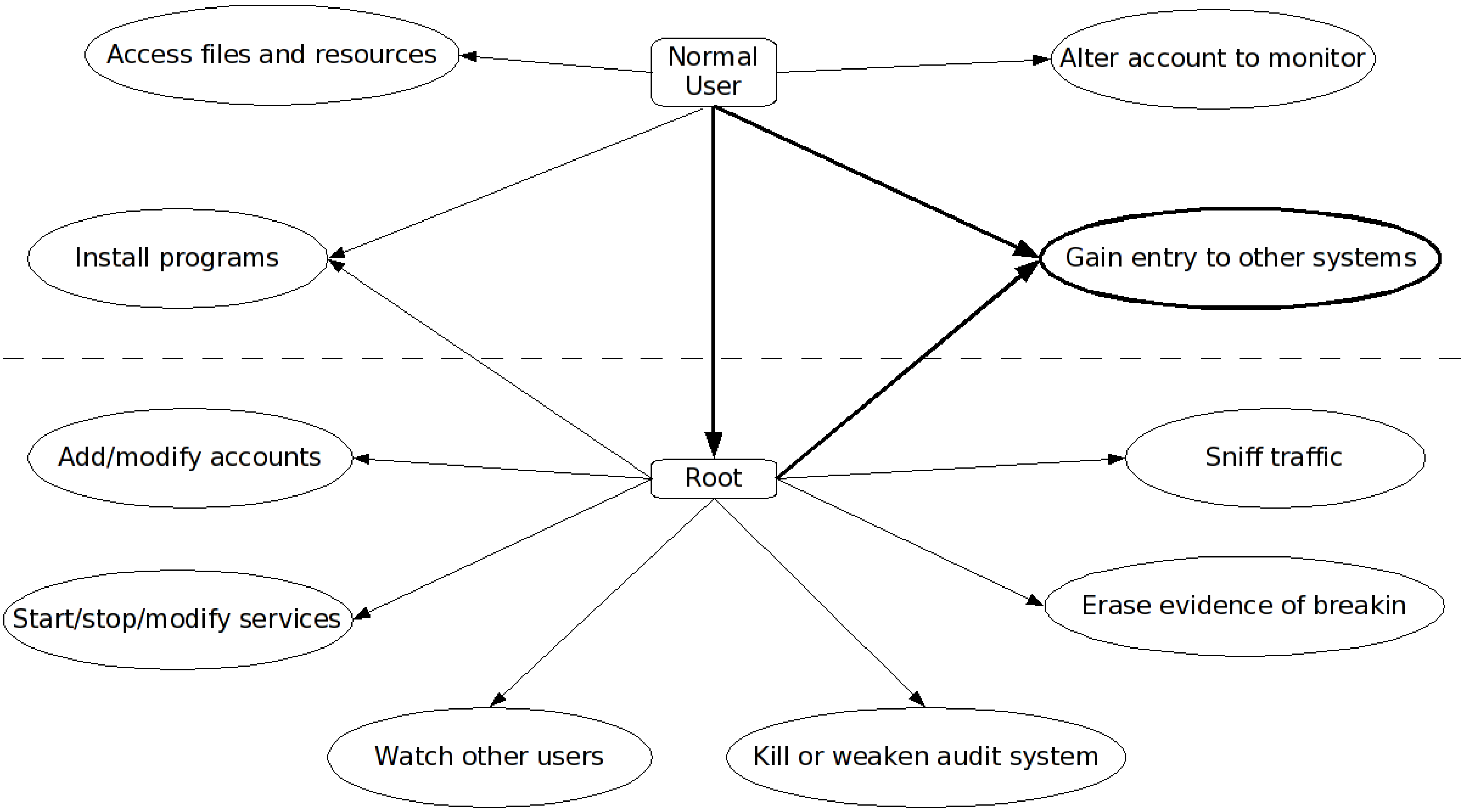
Hardening Red Hat Enterprise Linux 5

Steve Grubb, Red Hat

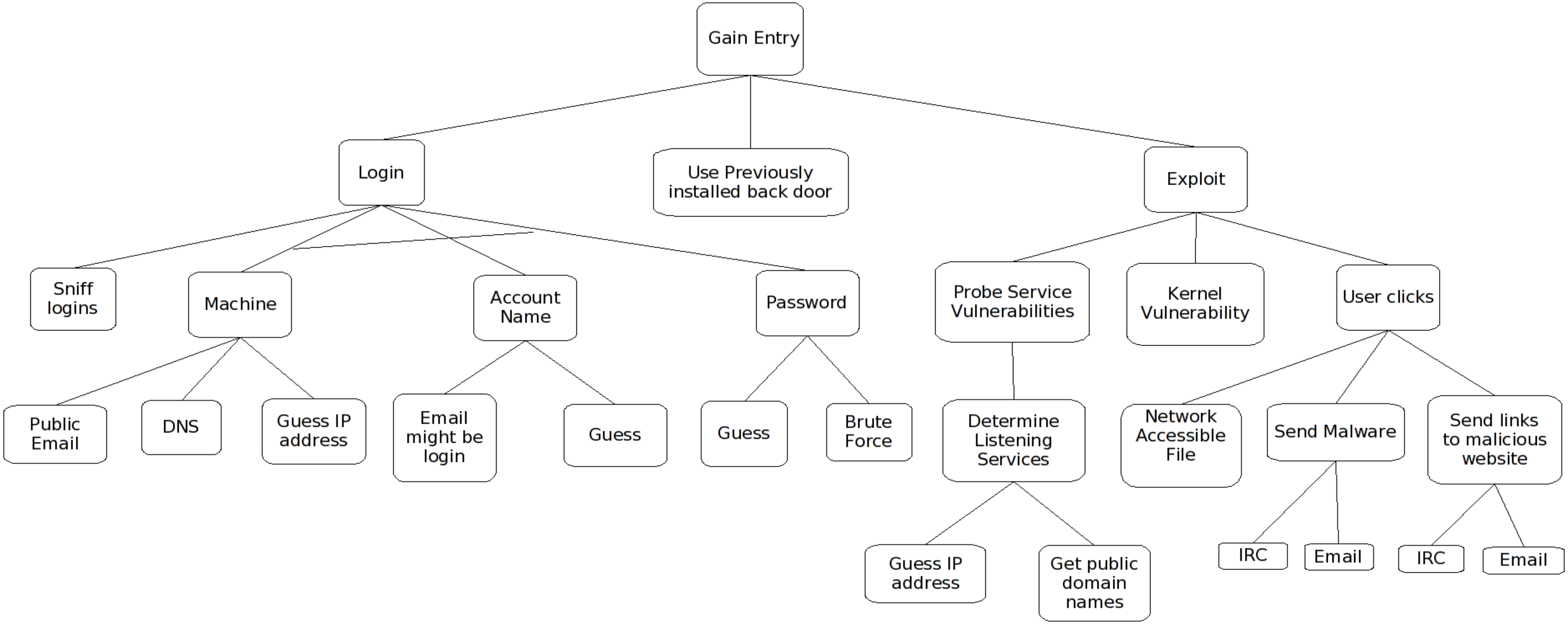
Hardening RHEL5

- Learn a little about some threats
- Go over some often missed configuration items
- Show how to make the system security better

Intrusion Goals

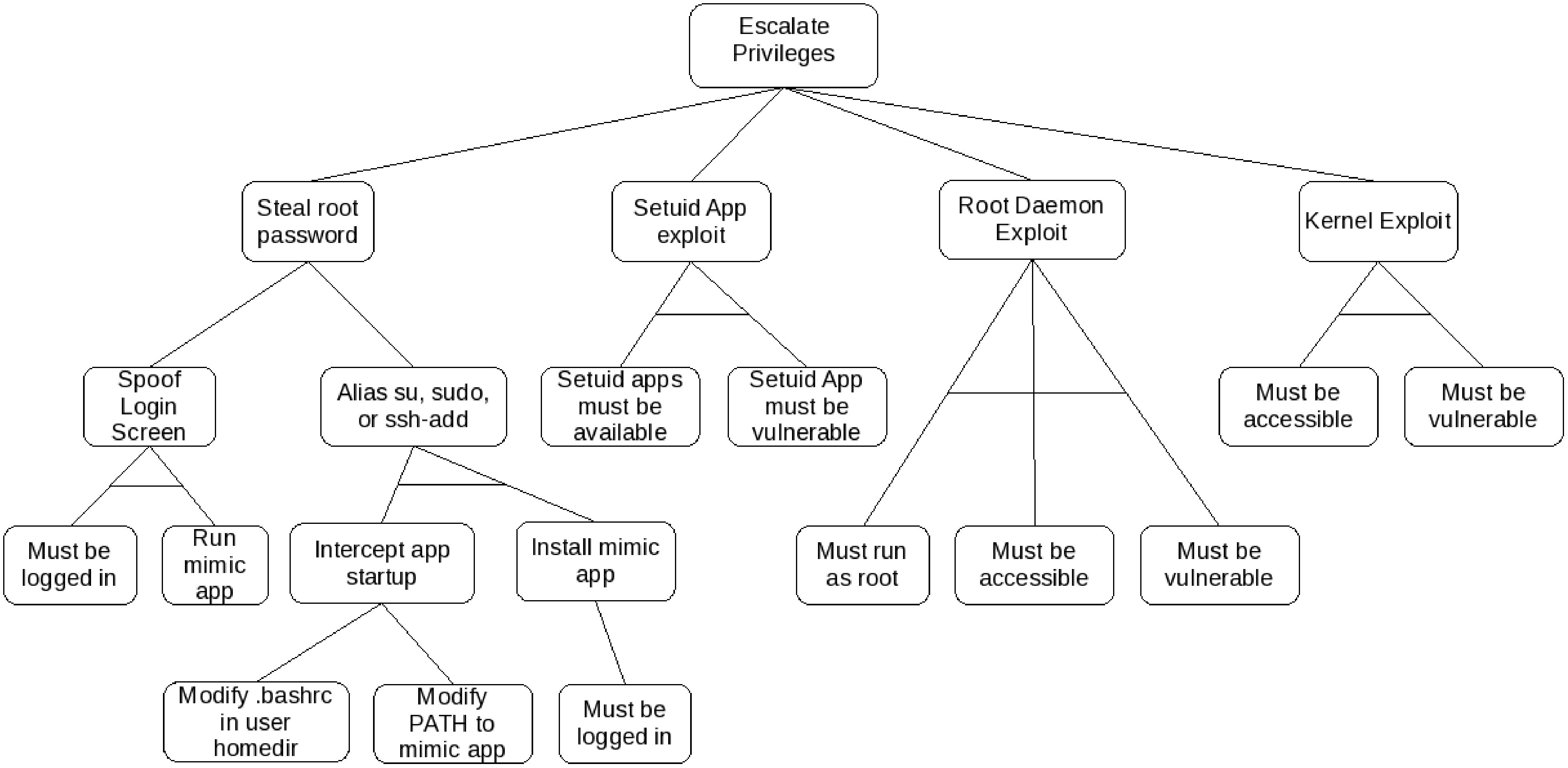

Normal User
Access files and resources
Alter account to monitor
Install programs
Gain entry to other systems
Root
Add/modify accounts
Sniff traffic
Start/stop/modify services
Erase evidence of breakin
Watch other users
Kill or weaken audit system

Network Intrusion Attack Tree



Steve Grubb, Red Hat

Privilege Escalation Attack Tree



System Update

Keep your system updated!

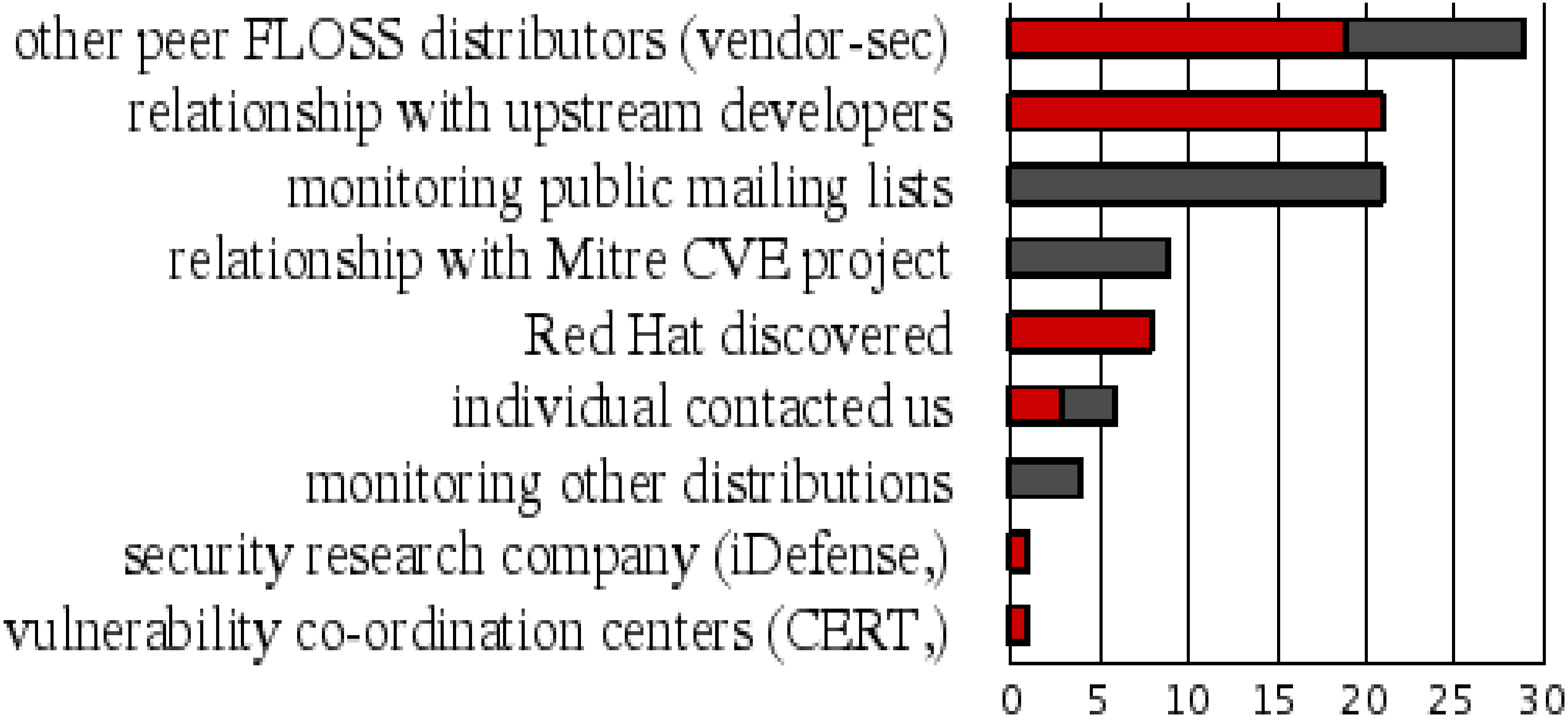
- If we know there is a problem, you should seriously consider taking the update

Some vulnerabilities can be mitigated by configuration

Some cannot

How Do We Find Vulnerabilities?

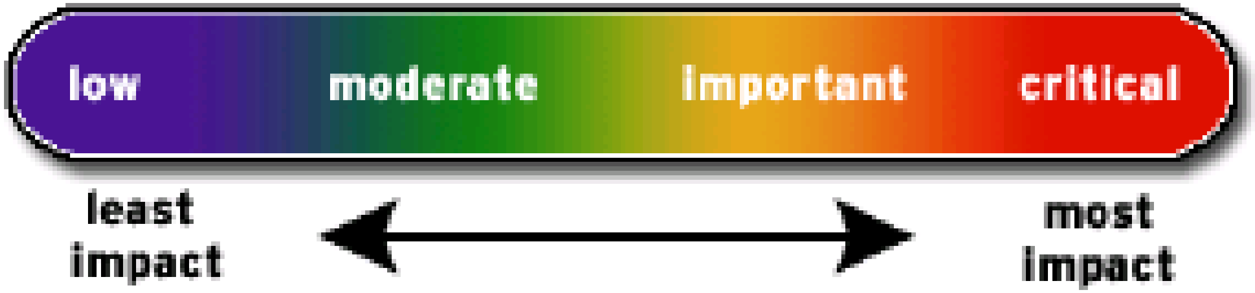
March 2005 – March 2007



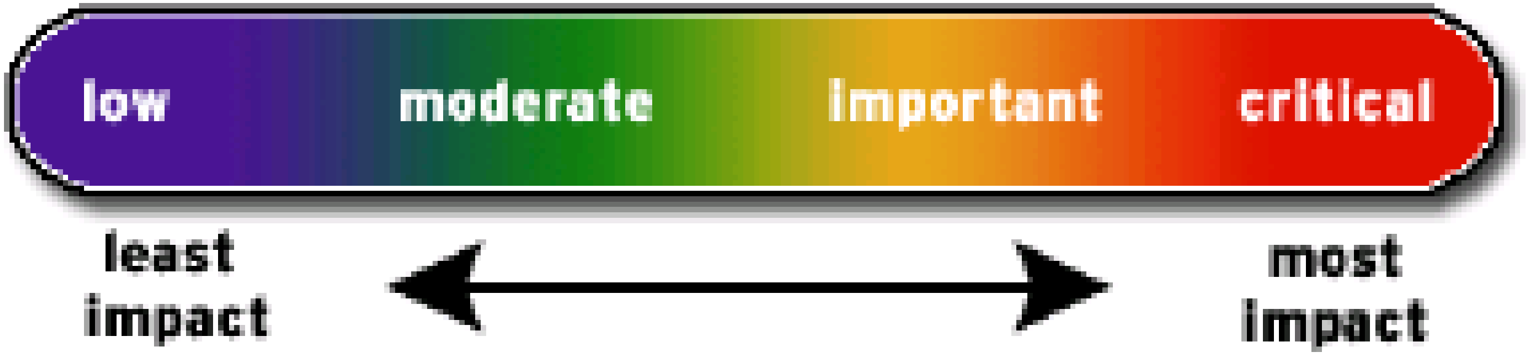
Setting a severity rating

Based on a technical assessment of the flaw, not the threat

- Unique to each Red Hat Enterprise Linux distribution
- Sets the priority through Engineering and QA
- Trend tracking (source, reported, public)



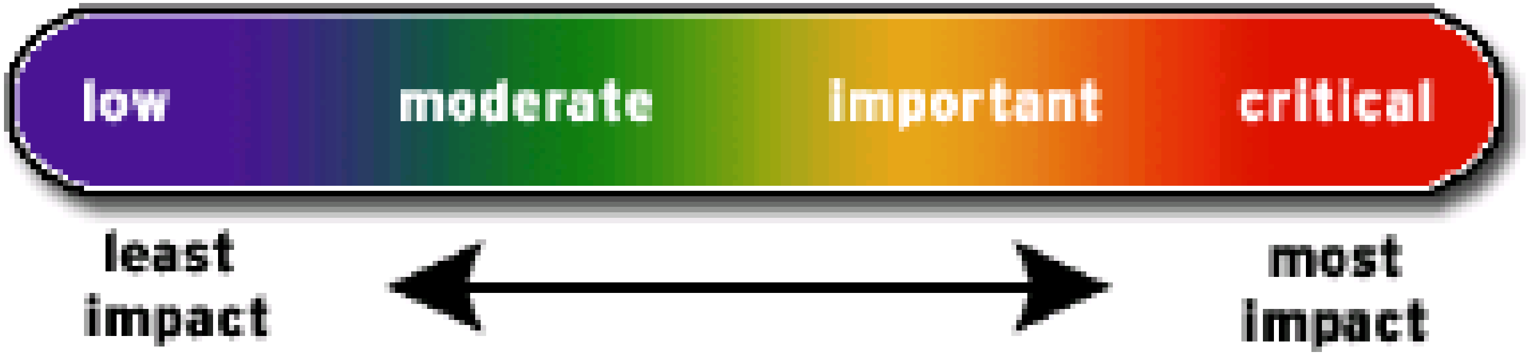
Severity Rating



Critical

> *"A vulnerability whose exploitation could allow the propagation of an Internet worm without user action."*

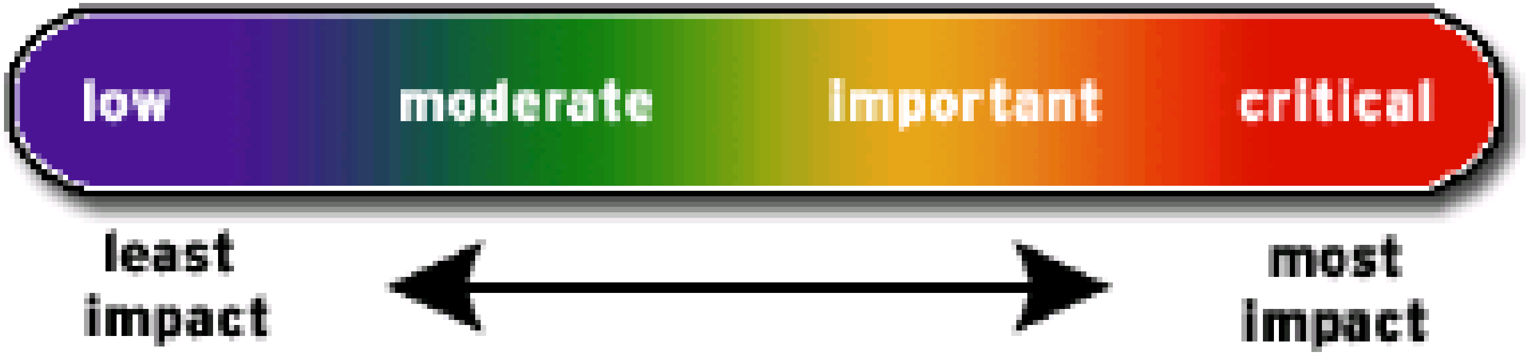
Severity Rating



Important

“easily compromise the Confidentiality, Integrity or Availability of resources”

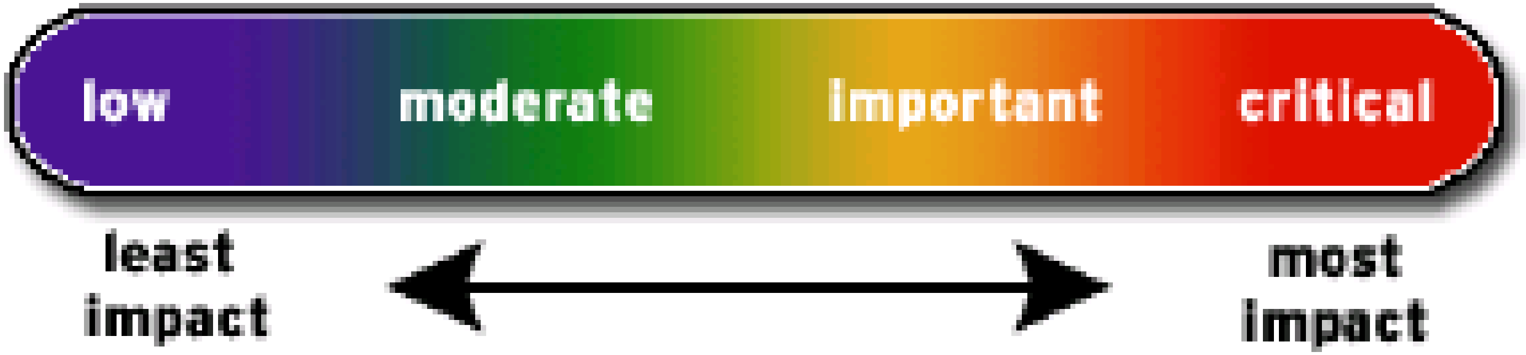
Severity Rating



Moderate

“harder or more unlikely to be exploitable”

Severity Rating



Low

> *“unlikely circumstances .. or where a successful exploit would lead to minimal consequences”*

Release Policy

- For critical vulnerabilities
  - Will be pushed immediately as embargo is lifted, or when passed QE
  - Will be pushed at any time or day
- For important vulnerabilities
  - May be held until reasonable time or day
- For moderate or low vulnerabilities
  - May be held until other issues come up in the same package, or the next Update release
- secalert @redhat.com - Address used for internal and external customers to ask security vulnerability related questions
  - Reporting new vulnerabilities
  - Asking how we addressed various vulnerabilities

Partitioning

Keep directories that users can write to on their own partition

- Prevents hard linking to setuid programs
- Allows precise control over mount options

```
$ ls -li test
13697075 -rwsr-x--- 1 root root 8666 2008-02-15 14:20 test

$ ln ./test test2

$ ls -li test2
13697075 -rwsr-x--- 2 root root 8666 2008-02-15 14:20 test2

$ make
gcc -g -W -Wall -Wundef test.c -o test

$ ls -li test
13697055 -rwsr-x--- 1 root root 8948 2008-02-17 15:53 test

$ ls -li test2
13697075 -rwsr-x--- 1 root root 8666 2008-02-15 14:20 test2
```

Partitioning

Allow minimal privileges via mount options

- Noexec on everything possible
- Nodev everywhere except / and chroot partitions
- Nosetuid everywhere except /
- Consider making /var/tmp link to /tmp, or maybe mount –bind option

A reasonable /etc/fstab:

```
LABEL=/               /               ext3    defaults                      1 1
LABEL=/tmp            /tmp            ext3    defaults,nosuid,noexec,nodev  1 2
LABEL=/var/log/audit  /var/log/audit  ext3    defaults,nosuid,noexec,nodev  1 2
LABEL=/home           /home           ext3    defaults,nosuid,nodev         1 2
LABEL=/var            /var            ext3    defaults,nosuid               1 2
LABEL=/boot           /boot           ext3    defaults,nosuid,noexec,nodev  1 2
/tmp                  /var/tmp        ext3    defaults,bind,nosuid,noexec,nodev  1 2
tmpfs                 /dev/shm        tmpfs   defaults                      0 0
devpts                /dev/pts        devpts  gid=5,mode=620                0 0
sysfs                 /sys            sysfs   defaults                      0 0
proc                  /proc           proc    defaults                      0 0
LABEL=SWAP-sda6       swap            swap    defaults                      0 0
```

Network Configuration

Strategy

- Minimize protocols being used
- Minimize addresses being listened to
- Minimize ports being listened on

Tools that help

- ifconfig – look at device and address mappings
- netstat – look at processes and their socket states
- route – look at the routing table
- nmap – scan the system from outside the firewall

Network Configuration

- IPv6
  - On by default
  - There are daemons that are IPv6 aware: sshd, apache, bind, xinetd, etc
  - Ip6tables has to be specifically setup
  - Could have service unexpectedly open to attack
- Detection
  - ifconfig | grep inet6
  - inet6 addr: fe80::21d:7eff:fe00:af5d/64 Scope:Link
  - inet6 addr: ::1/128 Scope:Host
- Disabling
  - Create a file /etc/modprobe.d/ipv6
  - Add this line inside: install ipv6 /bin/true

Network Configuration

Zeroconf

- On by default
- Used by avahi for local service discovery
  - Requires a hole in firewall to allow access
  - Advertises services to others

Detection

- route | grep link-local
- `link-local      *               255.255.0.0     U     0      0        0 eth2`

Disabling

- Edit /etc/sysconfig/network
- Add   NOZEROCONF=yes
- Then remove the avahi package and its dependencies

Network Configuration

Review Listening Daemons

- Default install is tuned for general use
- Probably a few things that are unnecessary

Detection

- netstat -tanp | grep LISTEN

Typical output:

```
[root ~]# netstat -tanp | grep LISTEN
tcp     0     0 127.0.0.1:8000     0.0.0.0:*       LISTEN      2256/nasd
tcp     0     0 127.0.0.1:3306     0.0.0.0:*       LISTEN      2166/mysqld
tcp     0     0 127.0.0.1:4690     0.0.0.0:*       LISTEN      2376/prelude-manage
tcp     0     0 127.0.0.1:631      0.0.0.0:*       LISTEN      2057/cupsd
tcp     0     0 127.0.0.1:25       0.0.0.0:*       LISTEN      2244/master
tcp     0     0 :::22              :::*            LISTEN      2068/sshd
```

Network Configuration

Disabling Listening Daemons

- Locate the pid in the netstat command
- cat /proc/<pid>/cmdline
- If not full path, run which or locate to find utility
- rpm -qf full-path-of-daemon
- rpm -e package
- If difficult to remove due to dependencies:
  - chkconfig <service> off

Network Configuration

/etc/sysctl.conf settings

```
# Don't reply to broadcasts. Prevents joining a smurf attack
net.ipv4.icmp_echo_ignore_broadcasts = 1

# Enable protection for bad icmp error messages
net.ipv4.icmp_ignore_bogus_error_responses = 1

# Enable syncookies for SYN flood attack protection
net.ipv4.tcp_syncookies = 1

#  Log spoofed, source routed, and redirect packets
net.ipv4.conf.all.log_martians = 1
net.ipv4.conf.default.log_martians = 1
```

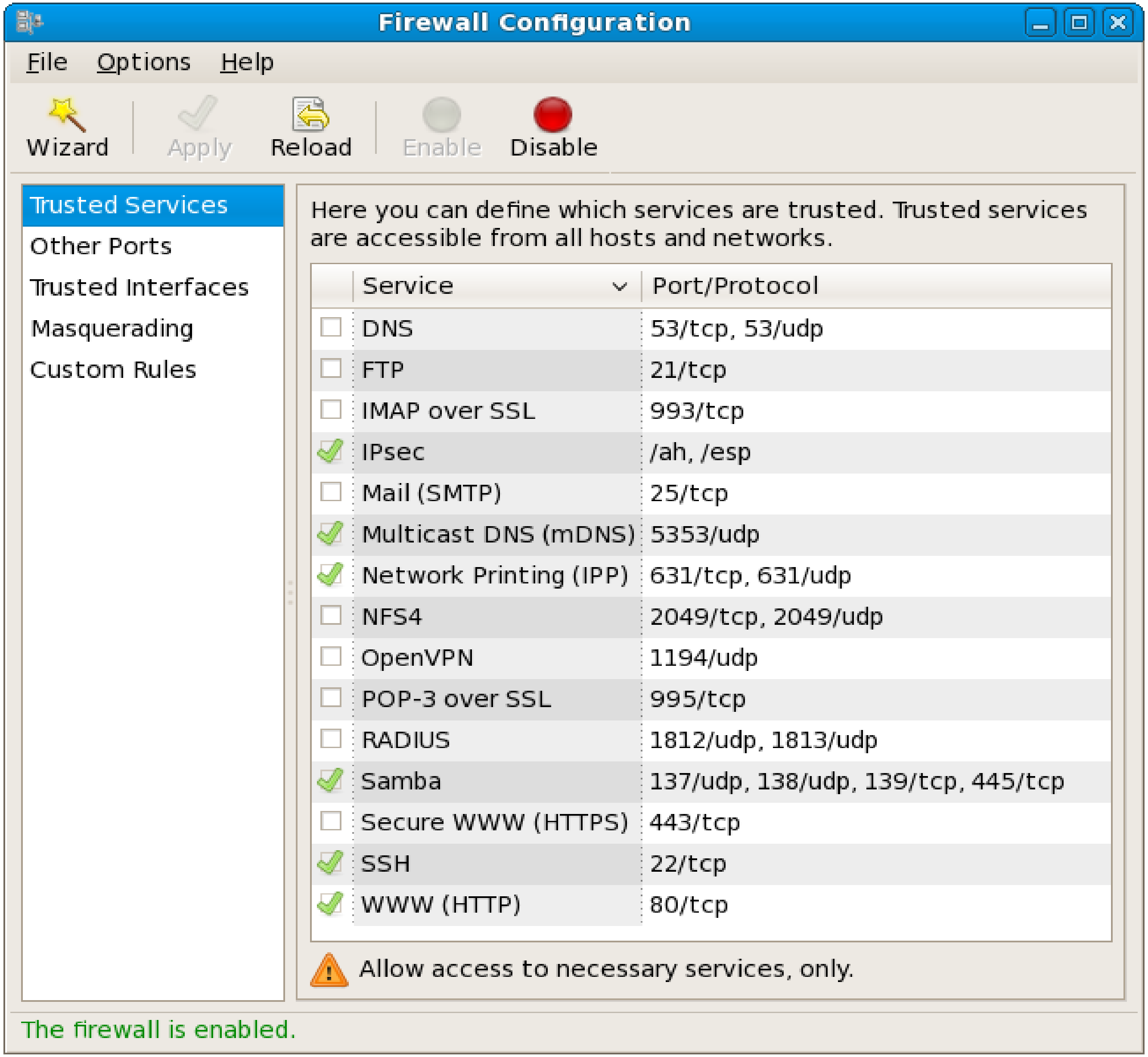
Network Configuration

```
# Don't allow source routed packets
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.default.accept_source_route = 0

# Turn on reverse path filtering
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.default.rp_filter = 1

# Don't allow outsiders to alter the routing tables
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.default.secure_redirects = 0

# Don't pass traffic between networks or act as a router
net.ipv4.ip_forward = 0
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0
```

Network Configuration

Iptables

- Default should be pretty good
- To see rules: service iptables status
- Use a GUI tool if not familiar with iptables rule syntax
- Use nmap from another machine to check effectiveness



Here you can define which services are trusted. Trusted services are accessible from all hosts and networks.

	Service	Port/Protocol
□	DNS	53/tcp, 53/udp
□	FTP	21/tcp
□	IMAP over SSL	993/tcp
☑	IPsec	/ah, /esp
□	Mail (SMTP)	25/tcp
☑	Multicast DNS (mDNS)	5353/udp
☑	Network Printing (IPP)	631/tcp, 631/udp
□	NFS4	2049/tcp, 2049/udp
□	OpenVPN	1194/udp
□	POP-3 over SSL	995/tcp
□	RADIUS	1812/udp, 1813/udp
☑	Samba	137/udp, 138/udp, 139/tcp, 445/tcp
□	Secure WWW (HTTPS)	443/tcp
☑	SSH	22/tcp
☑	WWW (HTTP)	80/tcp

⚠ Allow access to necessary services, only.

The firewall is enabled.

Network Configuration

tcp_wrappers

- Even if iptables is in use, configure this just in case
- Set /etc/hosts.deny to ALL: ALL
- Many daemons compiled with support
- Find by using: egrep libwrap /usr/bin/* /usr/sbin/* | sort
- For each program found, use its base name to set expected access rights (if there are any)
- Example: smbd: 192.168.1.

Unused Daemon Removal

Remove all daemons (and packages) not being used

- This reduces attack footprint and improves performance
- Many daemons listen on the network and could be accessible

Viewing

- chkconfig –list

Disabling

- rpm -qf /etc/rc.d/init.d/name

  rpm -e package-name
- OR   chkconfig <service> off

- Notes
  - Leave cpuspeed for speedshifting cpu and irqbalance for multicore CPU
  - Disable readahead, mcstransd, firstboot, (and NetworkManager for machines without wireless networking) since they are not needed.

System Time

Keep system time in sync

- You may need to correlate the time of disparate events across several machines to determine a chain of events
- Near impossible without common time base

Use ntp in cron job

- Create a file /etc/cron.daily/ntpdate containing the following crontab:

```
#!/bin/sh
/usr/sbin/ntpdate ntp-server
```

where ntp-server is the hostname or IP address of the site NTP server

Configure Remaining Daemons

At & cron

- Only allow root and people with verified need to run cron jobs
- Setup cron.allow and cron.deny
- Setup equivalents if you have 'at' installed

Sshd

- Enable only ssh2 protocol (this is default in RHEL5)
- If multi-homed, consider if it needs to listen on all addresses or just one
- Do not allow root logins
- Consider adding group permission for logins,   AllowGroups wheel

MySQL

- If database is used internally to machine, make it listen on localhost
- Change passwords

Configure Remaining Daemons

Bind

- Use chroot package
- Use ACLs
- Consider who the DNS server is used for (internal/external) and only serve DNS for those. Do not do both in one server instance.
- Do not allow zone transfers
- Do not do recursion

Apache

- Remove all unneeded modules
- Use mod_security to weed out injection attacks
- Set correct SE Linux Booleans to maintain functionality and protection

Configure Remaining Daemons

Init

- Disable interactive boot by editing /etc/sysconfig/init
- Make   PROMPT=no   to disable

- Also add password to single user mode. Edit /etc/inittab
- Add the following   ~~:S:wait:/sbin/sulogin

SE Linux

Leave enabled and in enforcing mode

- Does not affect daemons it doesn't know about - unless they are started in a confined domain, apache cgi-bin programs for example
- Provides a behavioral model that known applications should be following
- Can stop attacks before they become complete system breaches

Use targeted policy

- Strict and MLS should be used only if you need that kind of protection

Do boolean lockdown

- Review all booleans and set appropriately
- getsebool -a
- Generally, to secure the machine, look at things that are set to 'on' and change to 'off' if they do not apply

SE Linux Boolean Lockdown

```
[root ~]# getsebool -a | grep ' on'
allow_daemons_dump_core --> on
allow_daemons_use_tty --> on
allow_execmem --> on
allow_execstack --> on
allow_gadmin_exec_content --> on
allow_gssd_read_tmp --> on
allow_kerberos --> on
allow_mounton_anydir --> on
allow_postfix_local_write_mail_spool --> on
allow_staff_exec_content --> on
allow_sysadm_exec_content --> on
allow_unconfined_exec_content --> on
allow_unlabeled_packets --> on
allow_user_exec_content --> on
allow_xserver_execmem --> on
allow_zebra_write_config --> on
browser_confine_xguest --> on
httpd_builtin_scripting --> on
httpd_enable_cgi --> on
httpd_enable_homedirs --> on
httpd_tty_comm --> on
httpd_unified --> on
nfs_export_all_ro --> on
nfs_export_all_rw --> on
read_default_t --> on
samba_run_unconfined --> on
spamd_enable_home_dirs --> on
use_nfs_home_dirs --> on
user_ping --> on
```

Audit

Enable

- Install auditd
- chkconfig auditd on
- Audit daemon will turn on kernel auditing at boot and load rules

Setup correctly

- Add audit=1 to grub.conf kernel config line
- Have /var/log/audit on its own partition
- Edit /etc/audit/auditd.conf
- flush parameter should be set to sync or data
- max_log_file and num_logs need to be adjusted so that you get complete use of your partition
- space_left should be set to a number that gives the admin enough time to react to any alert message and perform some maintenance to free up disk space
- disk_full_action is triggered when no more room exists on the partition. All access should be terminated since no more audit capability exists.

Auditd

Set some defaults

- Place watches on critical files
  - Edit /etc/audit/audit.rules
  - -w /etc/shadow -p wa -k shadow
- Monitor important syscalls
  - -a exit,always -S open -S openat -F exit=-EPERM
- Auditd package has CAPP, LSPP, and NISPOM rules for samples
- Syscall rules are evaluated for every syscall of every program! Use judiciously

Review aureport output regularly

- Aureport gives system security summary report

Aureport system summary

```
Summary Report
======================
Range of time in logs: 07/22/2006 08:29:01.394 - 05/07/2007 16:12:29.832
Selected time for report: 05/01/2007 00:00:01 - 05/07/2007 16:12:29.832
Number of changes in configuration: 85
Number of changes to accounts, groups, or roles: 2
Number of logins: 25
Number of failed logins: 1
Number of authentications: 29
Number of failed authentications: 1
Number of users: 2
Number of terminals: 11
Number of host names: 3
Number of executables: 59
Number of files: 3
Number of AVC denials: 46
Number of MAC events: 21
Number of failed syscalls: 16
Number of anomaly events: 33
Number of responses to anomaly events: 0
Number of crypto events: 0
Number of process IDs: 4087
Number of events: 5885
```

Access Control

Do not allow root logins

- This messes up the audit system since root is a shared account
- Sshd and gdm have settings to disallow root login

pam_tally2

- This is used to lockout an account for consecutive failed login attempts

pam_access

- Used to forbid logins from certain locations, consoles, and accounts
- /etc/security/access.conf controls its config

pam_time

- Used to forbid logins during non-business hours
- /etc/security/time.conf controls its config

Access Control

pam_limits

- Used to limit maximum concurrent sessions and other user restrictions
- /etc/security/limits.conf controls its config

pam_loginuid

- Used for all entry point daemons to set the task's loginuid and session identifier
- Loginuid and session ID are inherited by all processes at fork
- Stored inside the task struct in the kernel
- Using require-auditd module option will forbid login if auditd is not running

Limit access to su command

- Edit /etc/pam.d/su
- Uncomment the line saying require wheel to allow uid change
- auth   required   pam_wheel.so use_uid

Disable Unused Devices

USB Mass Storage

- This can be used to transfer files in and out of the system
- Best to disable when possible by editing a file /etc/modprobe.d/no-usb
- Add this line inside: install usb-storage /bin/true

Wireless

- Disable in BIOS
- rm -rf /lib/modules/2.6.18*/kernel/drivers/net/wireless/*
- Must be run after each upgrade – working on something better

Firewire

- Check for /etc/modprobe.d/blacklist-firewire
- If not there, disable when possible by creating a file /etc/modprobe.d/no-firewire
- Add this line inside: install firewire_ohci /bin/true

Secure Physical Machine

Disable boot to anything except hard drive

- Do not allow booting from CD/DVD or USB devices

Disable any hardware unused

- Protects against device driver flaws should any ever be found

Lock BIOS

- After making sure to disallow USB booting, you don't want anyone to undo it

Set grub password

Integrity Checking

Amtu

- Abstract Machine Test utility
- Memory, network, disk, cpu security tests
- Can be run as cron job to repeatedly assure basic security assumptions
- Results sent to audit system

Aide

- File Integrity testing utility
- Configured by /etc/aide.conf
- --init snapshots the disksystem to /var/lib/aide/aide.db.new.gz
- Copy snapshot to immutable or safe location
- Rename snapshot to /var/lib/aide/aide.db.gz before doing comparison
- --check will compare current with snapshot for differences
- Summary sent to audit system

New Security Features since RHEL5 GA

NULL Pointer Dereference Protection

- MAP_FIXED flag to mmap syscall can be used to map page 0.
- vm.mmap_min_addr sysctl defaults to 64k
- SE Linux policy arbitrates access and CAP_SYS_RAWIO for DAC

SHA256 Password hashes

- Previously only md5 and des, now sha256 and sha512 have been added
- authconfig --passalgo=sha256 --update

Rsyslog

- Regex file splitting
- Execute commands
- TCP connection
- Database backend

TCG/TPM

- Tech preview in 5.2, supported in 5.3

Questions?

NSA guidance: http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/os/redhat/rhel5-guide-i731.pdf

Email: sgrubb @redhat.com