Hardening RHEL, in the real world.

Dallas, TX RHUG
Q1/2014

Marc Skinner
Principal Solutions Architect

RED HAT® ENTERPRISE LINUX®

Red Hat Expectation?

- Selinux enforcing

Reality?

- Selinux disabled

What is real world security?

- Package manifest – everything?
- Trusted RPMs?
- Chkconfig unused services?
- Which run level 3 or 5?
- Host based firewalls?
- SUDO tables?
- Telnet anyone?
- SSH hardening?
- Auditing?
- Central logging?
- Selinux?
- Password strength?
- Quarterly scans?
- More training?

Package manifest

- Install everything?
- @base install
  - Selectively build your image – takes time, but worth it
  - Why install RPMs that you will not need - but will need to patch
    - **Decrease your attack vector!**

Trusted RPMs

- GPG sign your 3rd party, custom or home built RPMs
- Create a signing account “GPGAdmin”
  - gpg –gen-key
  - gpg –export -a “GPGAdmin” > RPM-GPG-KEY-mycompany
  - rpm –import RPM-GPG-KEY-mycompany
  - Create the following file: ~./rpmmacros
    - “%_signature gpg”
    - “_gpg_name GPGAdmin”
  - rpm –addsign custom.rpm
  - rpm –checksig custom.rpm
  - rpmbuild -ba –sign custom.spec
- On server
  - rpm –import RPM-GPG-KEY-mycompany

Disabled unused services

- chkconfig –list
- chkconfig –list | grep cups
  - cups 0:off 1:off 2:on 3:on 4:on 5:on 6:off
- chkconfig cups off
  - cups 0:off 1:off 2:off 3:off 4:off 5:off 6:off
- **Disable all services you are not using. Decrease attack vectors!**

Which run level should I run?

- Configuration file
  - /etc/inittab
    - id:3:initdefault:
- Run level 3 versus 5
  - 3 = multi user mode with networking
  - 5 = multi user mode with networking + display manager
    - Do you need display manager?
    - Could you just use X11 libraries and VNC?
    - Make VNC secure with SSH port forwarding:
      - ssh -X -C -L 5902:localhost:5902 mskinner@server.mycompany.com
      - vncviewer localhost:5902

IPtables

- Configuration file
  - Use system-config-firewall-tui
  - /etc/sysconfig/iptables
    - :INPUT ACCEPT [0:0]
    - :FORWARD ACCEPT [0:0]
    - :OUTPUT ACCEPT [0:0]
    - -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
    - -A INPUT -p icmp -j ACCEPT
    - -A INPUT -i lo -j ACCEPT
    - -A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
    - -A INPUT -j REJECT --reject-with icmp-host-prohibited
    - -A FORWARD -j REJECT --reject-with icmp-host-prohibited
    - COMMIT
  - /etc/sysconfig/iptables-config (nat helpers - /lib/modules/2.6.32-220.17.1.el6.x86_64/kernel/net/[ipv4,netfilter]*_conntrack*)

IPtables

- One quick tweak to /etc/sysconfig/iptables then service restart iptables
  - Allows all connections into SSH
    - -A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
  - Allows only local subnet and localhost into SSH
    - -A INPUT -m state --state NEW -m tcp -p tcp **-s 192.168.33.0/24,localhost** --dport 22 -j ACCEPT

IPtables

- Error logs
  - None
- Update a few things:
  - /etc/sysconfig/iptables
    - -A INPUT -m limit --limit 15/minute -j LOG --log-level 7 --log-prefix "Dropped by firewall: "
    - -A OUTPUT -m limit --limit 15/minute -j LOG --log-level 7 --log-prefix "Dropped by firewall: "
  - /etc/rsyslog.conf (service rsyslogd restart)
    - kern.=debug /var/log/iptables
  - Sep 24 16:10:49 rh6-client kernel: Dropped by firewall: IN=eth0 OUT= MAC=52:54:00:63:23:2f:00:24:7e:16:0b:b3:08:00 **SRC=192.168.100.233** DST=192.168.33.129 LEN=100 TOS=0x00 PREC=0x00 TTL=64 ID=44292 DF PROTO=TCP SPT=43450 **DPT=22** WINDOW=808 RES=0x00 ACK PSH URGP=0

SUDO Tables

- Configuration Files
  - /etc/sudoers (USE visudo!)
    - mskinner ALL=(ALL) ALL
    - %dba ALL=(ALL) ALL
    - mskinner ALL=SOFTWARE
    - Look at Cmnd_Alias list
      - # Cmnd_Alias SOFTWARE = /bin/rpm, /usr/bin/up2date, /usr/bin/yum
      - # Cmnd_Alias PROCESSES = /bin/nice, /bin/kill, /usr/bin/kill, /usr/bin/killall
- Error Logs
  - /var/log/secure
    - Sep 24 15:36:48 rh6-client sudo: mskinner : **command not allowed** ; TTY=pts/1 ; PWD=/home/mskinner ; USER=root ; **COMMAND=/usr/bin/uptime**

TCP Wrappers

- Configuration files
  - /etc/hosts.allow
    - sshd: .mycompany.com EXCEPT fw.mycompany.com
  - /etc/hosts.deny
    - ALL:ALL versus sshd:ALL
- Error Logs
  - /var/log/secure
    - Sep 24 15:08:22 t500 sshd[4075]: warning: /etc/hosts.allow, line 11: host name/address mismatch: 192.168.33.11 != katzj-temp.test.redhat.com
    - Sep 24 15:08:22 t500 sshd[4075]: refused connect from 192.168.33.11 (192.168.33.11)
- Applications
  - ldd /sbin/sshd | grep wrap
    - libwrap.so.0 => /lib64/libwrap.so.0 (0x00007fa2a08db000)

Telnet?

- If you must – set up a Kerberos Realm – protect your credentials!
  - telnet serverhostname -l user -k kerbDOMAIN

SSHD hardening

- Configuration files – USE KEYS!
  - /etc/ssh/sshd_config
    - #AllowUsers or #AllowGroups and #DenyUsers or #DenyGroups
    - #PermitRootLogin yes -> no
    - #MaxAuthTries 6 -> 3
    - #MaxSessions 10
    - X11Forwarding yes -> no
    - #Match User mskinner
      - X11Forwarding yes
- Error logs:
  - /var/log/secure
    - Sep 24 16:35:59 rh6-client sshd[14113]: Accepted password for mskinner from 192.168.33.233 port 43906 ssh2
    - Sep 24 16:36:00 rh6-client sshd[14113]: pam_unix(sshd:session): session opened for user mskinner by (uid=0)

Auditing

- Configuration files:
  - /etc/audit/auditd.conf

- Error logs:
  - /var/log/audit/audit.log
    - type=**CRYPTO_SESSION** msg=audit(1348530342.106:44): user pid=**2493** uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=start direction=from-client cipher=aes128-ctr ksize=128 spid=2494 suid=74 rport=43944 laddr=192.168.33.129 lport=22 exe="**/usr/sbin/sshd"** hostname=? addr=192.168.33.233 terminal=? **res=success**'
    - type**=USER_LOGIN** msg=audit(1348530342.161:46): user pid=**2493** uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=login acct=28756E6B6E6F776E207573657229 exe="**/usr/sbin/sshd**" hostname=? addr=192.168.33.233 terminal=ssh **res=failed**'
    - type=**USER_AUTH** msg=audit(1348530345.651:47): user pid=**2493** uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=PAM:authentication acct="?" exe="**/usr/sbin/sshd"** hostname=192.168.33.233 addr=192.168.33.233 terminal=ssh **res=failed'**
  - Correlate - /var/log/secure
    - Sep 24 18:45:43 rh6-client sshd[**2493**]: pam_succeed_if(sshd:auth): error retrieving information about user **bob**
    - Sep 24 18:45:45 rh6-client sshd[**2493**]: Failed password for invalid user bob from 192.168.33.233 port 43944 ssh2

Central logging

- Configuration file:
  - Central Server - /etc/rsyslog.conf
    - # Provides UDP syslog reception
    - $ModLoad imudp.so
    - $UDPServerRun 514
  - Local Server - /etc/rsyslog.conf
    - *.info @ip address of Central Server

- Restart both rsyslog daemons
- How to test: logger “This is a test”
- **Separation of duties!**

Selinux

- Configuration file:
  - /etc/sysconfig/selinux
    - selinux permissive
    - touch /.autorelabel
    - reboot
- Selinux tools
  - getsebool -a
  - setsebool -P use_samba_home_dirs=on
  - audit2allow (yum install policycoreutils-python)
    - audit2allow -M mynewRule < /var/log/audit/audit.log
    - semodule -i mynewRule.pp (installs new rule)
- Error logs
  - /var/log/audit/audit.log

Hardening passwords

- Edit /etc/pam.d/system-auth
  - Default line: password requisite pam_cracklib.so ...
  - Options:
    - retry=N (password retries)
    - minlen=N (password minimum length)
    - reject_username (reject username as password)
    - Complexity – credit system, if N=-1 that is 1 requirement
      - dcredit=N (number of digits required)
      - lcredit=N (number of lower case letters required)
      - ocredit=N (number of other characters required)
      - ucredit=N (number of upper case letters required)

Internal Scans

- Nmap and Nmap-frontend
  - [root@rh6-client ~]# nmap localhost
  - Starting Nmap 5.51 (http://nmap.org) at 2012-09-24 15:54 CDT
  - Nmap scan report for localhost (127.0.0.1)
  - Host is up (0.0000020s latency).
  - Other addresses for localhost (not scanned): 127.0.0.1
  - PORT STATE SERVICE
  - 22/tcp open ssh
  - 111/tcp open rpcbind
  - 631/tcp open ipp
  - 6009/tcp open X11:9
  - Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
- Satellite and OpenSCAP

Red Hat security training

- RHS333 – Red Hat Enterprise Security: Network Services
- RHS429 – Red Hat Enterprise SELinux Policy Administration

- SELinux presentation:
  - Red Hat Summit - SELinux for Mere Mortals by Thomas Cameron
  - http://people.redhat.com/tcameron/Summit2012/SELinux/cameron_w_120_selinux_for_mere_mortals.pdf
- OpenSCAP presentation:
  - RHUG MN - OpenSCAP Primer by Marc Skinner
  - http://people.redhat.com/mskinner/rhug/q1.2013/satellite-openscap-primer.pdf