Fundamentals of Linux Platform Security

Security Training Course

Dr. Charles J. Antonelli
The University of Michigan
2012
Fundamentals of Linux Platform Security

Module 10
Platform Security
Roadmap

- Real-World Linux Security
- RHEL Security Guides
- Host-based Intrusion Detection
  - TripWire
  - Bastille Linux
Real-World Linux Security
The seven deadly sins

- Weak/default passwords
- Open network ports
- Old software versions
- Insecure programs
- Insufficient resources
- Stale/unnecessary accounts
- Procrastination

**Turn off insecure passwords**

- Use SHA-512 & passphrases
  - Password hashes in `/etc/shadow` should start with `$6$`
  - Maximum password length is 256 characters
- Use `/etc/shadow`
- Both defined by default
Prevent ARP Cache Poisoning

- Prevent ARP entries from being spoofed by making them permanent
  - add known ARP entries to /etc/ethers
  - add following to /etc/rc.d/rc.local
    - `arp -f /etc/ethers`
    - entries read from file are marked permanent

- Use network switch port configurations
arp

• /sbin/arp command
  - w/o args, displays contents of ARP cache
  - -a show all cache entries
  - -d h delete entry for host h
  - -s h e set permanent entry for host h with layer 2 address e
  - -s h e temp set temporary entry for host h with layer 2 address e
  - -f f read (default permanent) entries from file f
  - -n don’t convert host addresses to names
arping

• Similar to ping, but uses ARP requests and replies for probing
  ▪ Doesn’t require sender to have an IP address
  ▪ Limited to local subnet, unless proxy ARP
arping

- /sbin/arping destination
  - w/o args, displays usage
  - -I i use interface i (required)
  - -b use only Layer 2 broadcasts
  - -s s use source address s
  - -U unsolicited ARP
  - -D detect duplicate IP addr (RFC 2131)
arpwatch

• Monitors ARP traffic
• Detects Layer 2 / Layer 3 address pairing changes
  ▪ Records to syslog
  ▪ Emails to administrator
• Changes detected
  ▪ New station – new pairing using previously unseen layer 2 address
  ▪ New activity – new pairing using previously seen layer 2 address
  ▪ Flip flop – layer 2 address changed in existing pairing
  ▪ Changed ethernet address – layer 2 address changed on host
arpwatch lab

- Look at man page
  - `man arpwatch`
- Display syslog messages
  - Start another terminal window
  - `sudo tail -f /var/log/messages`
- Edit config file
  - `sudo vi /etc/sysconfig/arpwatch`
  - Insert "-i ethN" into OPTIONS if needed, adjust others as necessary
- (Optional) set arpwatch to start on boot
  - `chkconfig --list arpwatch`
  - `chkconfig arpwatch on`
  - `chkconfig --list arpwatch`
- Start arpwatch
  - `sudo service arpwatch start`
  - You should see ethN entering promiscuous mode in the syslog
- Generate some ARP traffic
  - Empty, then list your ARP cache
  - You should see something like the following in the log (and in an email message, if you’ve set that up)
    - Apr 21 16:10:58 localhost arpswitch: new station 172.16.234.2 0:50:56:e7:f7:34
- No output? Get arpwatch to forget:
  - `sudo service arpwatch stop`
  - `sudo cp /dev/null /var/lib/arpwatch/arp.dat`
  - `sudo service arpwatch start`
RHEL Security Guides

• Canonical step-by-step guide
  ▪ Security overview
  ▪ Attackers and Vulnerabilities
  ▪ Security Updates
  ▪ Workstation Security
  ▪ Server Security
  ▪ Virtual Private Networks
  ▪ Firewalls
  ▪ Vulnerability Assessment
  ▪ Intrusion Detection
  ▪ Incident Response
Security Guides

• Three guides:
Host-based IDS
Host Based IDS (HIDS)

- Intrusion Detection performed on the host
  - (Host) network layer
    - Not vulnerable to obfuscation games
    - HIDS sees exactly what the application layer sees
  - Library proxy
    - Entercept/Cisco CSA/etc
    - Did you really get every one?
      - Multiple kernel entry points in Windows
        - Hundreds of ways to execute a program
HIDS

- Behavioral
  - Behavior is learned
  - Has this program ever executed `cmd.exe` before?
  - Has it ever generated network traffic to this host?
- System call shim
  - Behavior is explicitly specified

\[\text{systrace}\]
Tripwire

- Binary checksums
  - Tripwire
- Log aggregators can take both HIDS & NIDS input
  - Correlate your own events
- HIDS are “push”, NIDS are “pull”
  - Have to manually deploy HIDS
  - NIDS see everything
Tripwire

- HIDS tool
- Initially creates hashes of all stored files in a database
- Subsequently compares stored hashes to files and reports any changes

Configuration
- twcfg.txt - general configuration
- twpol.txt - policy: what files to monitor, what file attributes to monitor for change, what to do if changes are detected
  - As shipped, monitors a large set of standard files
  - You will want to modify this file for your site

Security
- Site passphrase - encrypts and signs Tripwire files
- Local passphrase - needed to run Tripwire
Tripwire lab

• Install
  ▪ cd /usr/local/lab/tripwire
  ▪ sudo ./INSTALL.sh
  ▪ File /tmp/victim created for Tripwire to trip over later

• Configure
  ▪ sudo tripwire-setup-keyfiles
    ▼ Create passphrases when prompted
  ▪ Signs and encrypts the Tripwire configuration and policy files
    ▼ Enter passphrases when prompted

• Initialize database
  ▪ sudo tripwire --init
    ▼ Enter passphrase when prompted
  ▪ Creates the encrypted database
Tripwire lab

- Check integrity -- should show no changes
  - `sudo tripwire --check`
  - ▼ Report sent to standard output and saved as *.twr in report directory

- Change something and re-check integrity -- should show change
  - Change something about `/tmp/victim`
  - `sudo tripwire --check`
  - ▼ Shows changes
  - `sudo twprint -m r -r /var/lib/tripwire/report/[report].twr`
  - ▼ Substitute appropriate report file name for [report]
  - ▼ List `/var/lib/tripwire/report` to find the right one
    - » File name reflects date and time file was generated
Bastille Linux

  - Cybersquatter on bastille-linux.org
- Wizard for locking down Linux
- Support for the major distributions
- Step-by-step walkthroughs
  - … including iptables
- Undo feature
Bastille lab

• Install bastille
  ▪ cd /usr/local/lab/bastille
  ▪ sudo ./INSTALL.sh

• Run bastille
  ▪ man bastille
  ▪ sudo bastille --assess ("guaranteed" read-only)
    ▼ Accept the terms ...
  ▪ sudo bastille
    ▼ Explore
References

• Tripwire http://sourceforge.net/projects/tripwire/
• Bastille http://www.bastille-unix.org/