

Introduction to Linux Security 2

Jared Bater & Theo Baschak

CDC Prep January 25, 2014

Online HTML5 Slides

Presentation source/download available at
github.com/tbaschak/intro-linux-security

Introductions

Funny Joke

- ▶ You have been infected by the UNIX version of the I LOVE YOU virus.
- ▶ This virus operates on the honor system.
- ▶ Please delete a few hundred random files from your hard drive and forward this message to everyone you know.

Topics to be covered

- ▶ Good Practices
- ▶ Passwords
- ▶ File System Integrity
- ▶ Processes and sockets (ps and netstat)
- ▶ Boot process
- ▶ Run levels
- ▶ Services
- ▶ iptables
- ▶ Logs
- ▶ SE Linux
- ▶ Updating (APT / Yum, etc)

Good Practices

- ▶ Check signatures on packages/sources (GPG, MD5, SHA)
- ▶ Use sudo instead of su, or logging in as root
- ▶ Don't use/offer plaintext authenticated services
- ▶ Don't add . to root's \$PATH

Passwords

- ▶ Define minimum password lengths, complexity, and validity period
- ▶ Passwords should always be stored salted and hashed
- ▶ Low-length passwords can be cracked programmatically in surprisingly low time
- ▶ Local authentication can give access to other services (SMTP credentials)

File System Integrity

- ▶ We want to know if critical files change on our filesystems
- ▶ Various tools to compare file checksums:
 - ▶ Tripwire (Commercial)
 - ▶ OSSEC (Open Source)
 - ▶ AIDE (Open Source)
 - ▶ Distribution built-in (`rpm -Va`)

Processes & Sockets

- ▶ A process is a program running on a Linux system
 - ▶ Identified by its Process Identifier or PID
 - ▶ Can be listed using `ps`
- ▶ An IPC or Unix Domain socket is a special type of file for exchanging data between processes
- ▶ Sockets, and which PIDs own them can be monitored using `lsof`

Boot Process

Run Levels

- ▶ 0 -> Halt, 1 -> Single User, 2 -> Multi User (without NFS), 3 -> Multi User 4 -> Unused, 5 -> Multi User (graphical login), 6 -> Reboot
- ▶ Can be changed using `telinit`
- ▶ Servers usually run at 3, Desktops at 5

Services

- ▶ If you don't need it, turn it off
- ▶ Patch a disabled service? (Hint: Yes)
- ▶ The `service` command stops/starts services (System V init scripts)
- ▶ the `chkconfig` command sets services to start at boot
- ▶ Some newer distros use `systemd(1)` to manage services and systems

iptables (Firewalls)

- ▶ Default Allow (or can be configured to default deny)
- ▶ Various chains (INPUT, OUTPUT, FORWARD by default)
- ▶ Can create other chains for custom rulesets
- ▶ Can interact with iptables directly or use a front end such as ufw, Shorewall, FirewallID, others

Block All Inbound

```
/sbin/iptables -P INPUT DROP
```

```
/sbin/iptables -P FORWARD DROP
```

```
/sbin/iptables -P OUTPUT ACCEPT
```

```
/sbin/iptables -A INPUT -m state --state NEW,ESTABLISHED -j
```

```
/sbin/iptables -L -v -n
```

Logs

- ▶ Most logs live in `/var/log/`
- ▶ Most logs are plain text, but some are binary (`wtmpx`, `utmpx`, `lastlog`)
- ▶ `/var/log/messages` : major events, failed logins, SU to root
- ▶ `/var/log/secure` : failed logins, added / deleted users
- ▶ `/var/log/maillog` : mail system logs
- ▶ `/var/log/wtmpx` : Who is currently logged in and from where. Use the `w` command
- ▶ `/var/log/utmpx` : History of logins and reboots of the system. Use the `last` command
- ▶ Logs should be reviewed or watched by another process such as OSSEC

SELinux (Security-Enhanced Linux)

- ▶ Mandatory Access Control (MAC vs. DAC)
- ▶ Fine-grained control over processes, files, sockets, etc
- ▶ Enhances existing security in Linux
- ▶ <http://stopdisablinglinux.com>

Updating

- ▶ Small updates usually easier than large updates
- ▶ Redhat/Centos => `yum update`
- ▶ Debian/Ubuntu => `apt-get update`; `apt-get upgrade`
- ▶ Most distros have automatic update mechanism. This may or may not be appropriate

Questions / End

- ▶ Question & Answer period as time permits.

Questions / End

- ▶ Question & Answer period as time permits.
- ▶ Presentation source/download available at [github](#)