# CyberPatriot

## How to Win CyberPatriot (Linux edition)

. . .

LASA {CSCLUBS}

# General Steps

1. README
2. Forensics
3. Script
    a. User auditing
    b. Updates
    c. Application security
4. Baselining

# README

## User Management

- Adding a user: `sudo useradd <name>`
- Adding a user to a group: `sudo usermod -aG <group> <user>`

## Installing a Service

- Example for Apache Web Server: `sudo apt-get install <service-name>`
- Ensure service is running: `sudo systemctl status <service-name>`
- SECURE THE SERVICE!!! (somewhere in /etc, example for Apache)
  - I'd recommend getting several sources and doing all of them
  - Save the configured files for reuse!!

# Forensics

Finding Files (txt, mp3, etc.)

- Example for mp3 files: `sudo find / -name '*.<extension>' 2>/dev/null`
- !! REMOVE AFTER !!

Users/Groups

- List members of group: `members <group>`
  - `sudo apt-get install members`
- List groups of user: `groups <user>`

Ciphers/codes

- CyberChef (with Magic)

# Forensics

## Finding Backdoors

- List running processes: `sudo ps aux`
  - Baseline!
- List processes listening to a port: `sudo lsof | grep LISTEN`
  - Baseline!
- Get process path: `sudo readlink /proc/<pid>/exe`
- Get process command: `sudo cat /proc/<pid>/cmdline`
  - `sudo cat /proc/<pid>/cmdline | sed -e "s/\x00/ /g"; echo`
  - Important for Python & Perl
- !! REMOVE AFTER !!

## Misc/Other

- Google it!!
- Get other teammates to look at it

# Scripting – Basic Setup and Tips

- Python (comes installed)
- Make it modular (I organized mine by CIS modules) with one main runner
- Use libraries: `sudo pip3 install <pkg>`
- Run main file with `sudo` so it doesn't have to be all over your code
- Log info!! Human intuition is powerful
- Rather than editing files in place, make a secure version then just copy it
  - MAKE A BACKUP BEFORE COPYING
- Set all passwords to the same (secure) thing

# Scripting – Integrate Bash

```
def run(command, capture_output=False):
    tmp = tempfile.NamedTemporaryFile(delete=True)
    with open(tmp.name, 'w') as f:
        f.write('#!/bin/bash\n')
        f.write(command)

    os.chmod(tmp.name, stat.S_IEXEC | stat.S_IREAD)
    tmp.file.close()

    return subprocess.run(['bash', tmp.name], stdout=subprocess.PIPE if capture_output or
threading.current_thread() is not threading.main_thread() else None)
```

```
def get_output(command):
    return run(command, True).stdout.decode().strip()
```

```
def get_output_lines(command):
    return list(filter(lambda s: s != '', get_output(command).split('\n')))
```

```
def if_success(command):
    return not run(command).returncode
```

# Scripting – User Auditing

Python

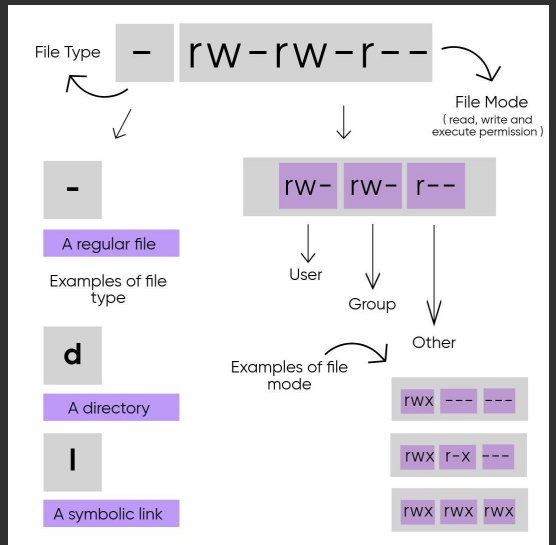
Bash

- List all users: `pwd.getpwall()`
  - `import pwd`
- Add user: `sudo useradd <user>`
- Remove user: `sudo userdel <user>`
- Add admin: `sudo usermod -aG sudo <user>`
- Remove admin: `sudo deluser <user> sudo`
- Set password: `echo '<password>\n<password>' | sudo passwd <user>`

# Interlude – File Permissions `ls -l`

```
drwxr-xr-x  2 malcolmroalson  staff  64 Dec  8 13:04 directory
-rw-r--r--  2 malcolmroalson  staff  12 Dec  8 13:06 file
-rw-r--r--  2 malcolmroalson  staff  12 Dec  8 13:06 hardlink
lrwxr-xr-x@ 1 malcolmroalson  staff   4 Dec  8 13:07 softlink -> file
```

PERMISSIONS | USER | GROUP | SZ | DATE | NAME [ –> LINK]




```
x = 1
w = 2
r = 4
```

```
rwx = 7
rw- = 6
r-x = 5
r-- = 4
```

EX: `chmod 644 /path/to/file`

LASA {CSCLUBS}

# Scripting – Software and Patch Management (CIS 1.3)

- `/etc/apt/sources.list`
- `/etc/apt/trusted.gpg.d`

- Just baseline it: `sudo cp -r /path/to/safe/apt/* /etc/apt`
  - Don't forget to backup `/etc/apt` before messing with it: `sudo cp -r /etc/apt /etc/apt.bak`
- This can break perms: `sudo chmod -R a+rx /etc/apt/trusted.gpg.d`
  - apt needs execution permission

# Scripting – Secure Boot (CIS 1.4)

- Root password: `echo '<password>\n<password>' | sudo passwd root`
- Set grub password: read CIS (copy in files rather than editing in place!)
- Set grub config permissions: `sudo chmod 0600 /boot/grub/grub.cfg`
- Set grub config owner: `sudo chown root:root /boot/grub/grub.cfg`

# Scripting – Process Hardening (CIS 1.5)

- BIG BIG BIG: just **read through the CIS**
- Just replace the files in case CyPat messed with them
- Key files: `/etc/sysctl.conf`, `/etc/sysctl.d/*`

- `kernel.randomize_va_space = 2`

# Scripting – Banner (CIS 1.7)

- Overwrite the following files:
  - `/etc/motd`
  - `/etc/issue`
  - `/etc/issue.net`
- Set permissions on them as well:
  - `sudo chmod 0644 <file>`
  - `sudo chown root:root <file>`

# Scripting – Configuring GDM (CIS 1.7)

- Kind of a pain, so I'm not going to list it all here
- DEFINITELY can get points, especially **DISABLING THE GREETER**
  - `disable-user-list`

- NOT IN CIS: configure LightDM (for Mint)
  - Disable guest account
  - Disable user list
  - Just go through all the settings, make them as secure as possible, then save that secure version to overwrite `/etc/lightdm.conf`
  - https://github.com/canonical/lightdm/blob/main/data/lightdm.conf

# Scripting – Network Hardening (CIS 3.1-3.3)

- BIG BIG BIG: just **read through the CIS**
- Just replace the files in case CyPat messed with them
- Key files: `/etc/sysctl.conf`, `/etc/sysctl.d/*`

- `net.ipv4.icmp_echo_ignore_broadcasts = 1`
- `net.ipv4.conf.all.log_martians = 1`
- `net.ipv4.conf.default.log_martians = 1`
- `net.ipv4.conf.all.accept_redirects = 0`
- `net.ipv4.conf.default.accept_redirects = 0`
- `net.ipv6.conf.all.disable_ipv6 = 1`

# Scripting – UFW (CIS 3.4)

- `sudo ufw enable`
- There’s a lot more you can do (probably worth checking)

# Scripting – SSH (CIS 5.1)

- Securing `/etc/ssh/sshd_config` (server)
- Just read through this and do it all (then save the config file)
- Also Google securing `/etc/ssh/ssh_config`! (client)

# Scripting – Sudoers (CIS 5.2)

- Just replace `/etc/sudoers` and clear `/etc/sudoers.d/*`
- Set permissions:
  - `sudo chmod 0644 /etc/sudoers`
  - `sudo chown root:root /etc/sudoers`

# Scripting – PAM (CIS 5.3)

- HUUUUUGE: go through the benchmark
- Replace `cracklib` w/ `pwquality`
  - `sudo apt-get -y purge libpam-cracklib`
  - `sudo apt-get -y install libpam-pwquality`
- Overwrite these files with secure versions:
  - `/etc/pam.d/common-auth`
  - `/etc/pam.d/common-account`
  - `/etc/pam.d/common-password`
    - `password requisite pam_pwquality.so retry=3 minlen=10`
    - `password required pam_pwhistory.so remember=5`
  - `/etc/security/pwquality.conf`
    - `minlen = 14`
    - `enforcing = 1`
    - `enforce_for_root`

# Interlude – /etc/passwd

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:104::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:105:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
pollinate:x:105:1::/var/cache/pollinate:/bin/false
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
parallels:x:1000:1000:Parallels:/home/parallels:/bin/bash
tss:x:107:112:TPM software stack,,,:/var/lib/tpm:/bin/false
rtkit:x:108:113:RealtimeKit,,,:/proc:/usr/sbin/nologin
syslog:x:109:115::/home/syslog:/usr/sbin/nologin
kernoops:x:110:65534:Kernel Oops Tracking Daemon,,,:/:/usr/sbin/nologin
uuidd:x:111:118::/run/uuidd:/usr/sbin/nologin
systemd-oom:x:112:119:systemd Userspace OOM Killer,,,:/run/systemd:/usr/sbin/nologin
tcpdump:x:113:120::/nonexistent:/usr/sbin/nologin
whoopsie:x:114:121::/nonexistent:/bin/false
avahi-autoipd:x:115:122:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:116:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
nm-openvpn:x:117:123:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
dnsmasq:x:118:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
avahi:x:119:125:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
cups-pk-helper:x:120:126:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
sssd:x:121:127:SSSD system user,,,:/var/lib/sss:/usr/sbin/nologin
speech-dispatcher:x:122:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
saned:x:123:129::/var/lib/saned:/usr/sbin/nologin
colord:x:124:130:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:125:131::/var/lib/geoclue:/usr/sbin/nologin
pulse:x:126:132:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
gnome-initial-setup:x:127:65534::/run/gnome-initial-setup/:/bin/false
hplip:x:128:7:HPLIP system user,,,:/run/hplip:/bin/false
gdm:x:129:134:Gnome Display Manager:/var/lib/gdm3:/bin/false
test:x:1001:1001:,,,:/home/test:/bin/bash
```

# Scripting – Secure User Accounts (CIS 5.4)

- HUUUUUGE: go through the benchmark
- Replace `/etc/login.defs`
- Important configs (but certainly not all):
  - `PASS_MAX_DAYS   90`
  - `PASS_MIN_DAYS   7`
  - `PASS_WARN_AGE   10`
  - `USERGROUPS_ENAB yes`
- Still have to to implement for all users:
  - `sudo chage --mindays 7 --maxdays 90 --warndays 7 --inactive 30 <user>`
- Validate system accounts
  - Make sure all accounts in `/etc/passwd` with UID<1000 are system accounts
  - **Only root should have UID 0**

# Scripting – Secure System Files (CIS 7.1)

- For all these files, do `sudo chmod 644 <file>` and `sudo chown root:root <file>`
  - `/etc/passwd`
  - `/etc/group`
  - `/etc/shells`
- For all these files, do `sudo chmod 640 <file>` and `sudo chown root:root <file>`
  - `/etc/shadow`
  - `/etc/gshadow`
  - `/etc/opasswd`

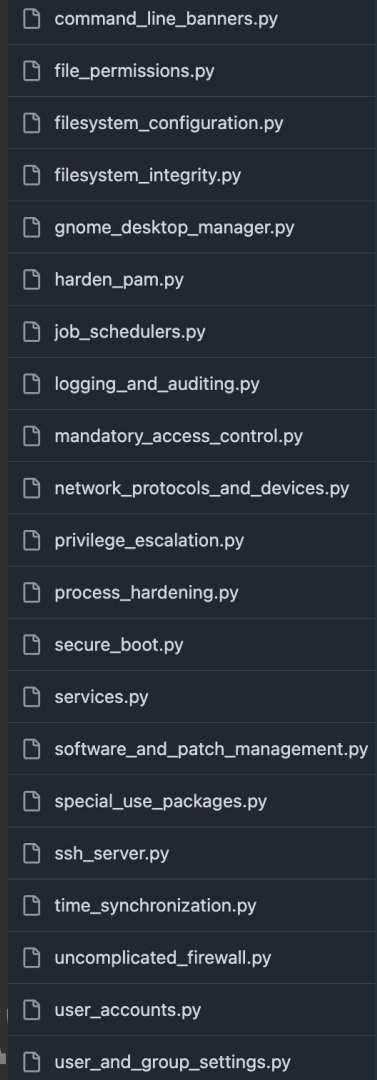
# Scripting – Updates

- `sudo apt-get update` - refresh package lists
- `sudo apt-get upgrade` - download and install updates
- That's it

# Scripting – Other CIS Stuff

Not Covered Here

- Filesystem configuration (`/etc/fstab`, `/tmp`, `autofs`)
- Filesystem integrity (installing and configuring `aide`)
- Mandatory Access Control (installing and configuring apparmor)
- Time Synchronization
- Special Use Packages (remove Avahi, stop Rsync)
- Job Schedulers (clear cron, systemctl services & timers, etc.)
- Securing `su`
- auditd/journald



# Baselining – Application Security

- List of services I've seen, and have pre-configured:
  - Apache2 — `apache2.conf`, `ports.conf`
  - MySQL — `my.cnf`,
  - Bind9 — `named.conf`
  - PHP — `php.ini`
  - PostgreSQL — `postgresql.conf`

# Baselining – File System

- EVERYTHING is a file
- If you store a clean version, you can compare
  - Personally I like meld: `sudo apt-get install meld`

- Baseline installed packages with `apt list --installed`
- Baseline services with `sudo systemctl list-units --type=service`
  - Remove ALL unnecessary packages and services (including SSH server!)

# The Rest

- The majority of the points will be in application and system security

- CIS Benchmark
- **VERY VERY** Important Slides (sysctl, login.defs, and PAM):
  - Slide 12: Scripting – Process Hardening (CIS 1.5)
  - Slide 15: Scripting – Network Hardening (CIS 3.1-3.3)
  - Slide 19: Scripting – PAM (CIS 5.3)
  - Slide 21: Scripting – Secure User Accounts (CIS 5.4)

- Intuition and experience :)