Linux BlueTeam Notes

Harden users

- Configuration Files
  - Inputrc
  - PAM
  - Bashrc, etc..
- Reading your logs
- Monitor the system
  - Network
  - Processes
  - Services

How code runs?

- lots of different things can run programs
- audit these things
- Services
  - Lets make a malicious server
  - Auto Restart when a process is killed
    - systemD, Service Managers
- Cron (runs commands at set time or day)
  - `/etc/crontab`

- Binary Shimming (modifies the legit binary and launches a second malicious script. like running `ls` also executes bad code)
  - hooking processes
- PROMPT_COMMAND (runs commands when prompt is displayed)

Linux Services

- Daemons, background processes
- Run without the need of user interactions
- Managed by the system via Service Manager
  - systemD, sysVinit
- Has a running process while code is running
  - code may not always be running
- View the logs with `journalctl` (one of the most important logs on linux)
  - `journalctl -e`

Users and Groups

- Information is stored in text files

  - `/etc/passwd` - User information
  - `/etc/shadow/` - password hashes
  - `/etc/group/` - Group information

- Users can be configured to authenticate from other computers (AD, NIS)

- Sudo needs to be watched
  - which users can become root
  - `/etc/sudoers` - `visudo` - Sudo configuration files
- Commands for working with users
  - Useradd, userdel, usermod, visudo
  - vim, nano - edit the files directly

Hardening Users

- vim `/etc/passwd`
- vim `/etc/shadow`
- usermod -L BADGUY # Breaks authentication
- usermod -s /bin/false BADGUY # Breaks shell
- Disable users instead of deleting

Configuration Files

- Many core aspects of the system are configurable (even if they shouldnt be)
- Attackers may use these files against you
- Common system configuration files
  - `~/.bashrc, /etc/profile , /etc/bash.bashrc`
  - `/etc/enviroment`
  - `/etc/sudoers`
- Not so common configuration files

  - `/etc/inputrc`
  - `/etc/pam.d`
    - Entirely breaks authentication

Harden SSH

- `/etc/ssh/sshd_config`
  - AllowUsers user1 user2@ip.ip.ip.ip
  - PermitRootLogin no
  - UsePAM no
- Set a custom sshd_config
- Move the port (ask whiteteam)
- Check logs
- Dont use PAM for competition

Why not use SSH Keys in competition?

```
You cannot instantly change them and redeploy across the environment.
If redteam copies SSH keys, you will have to recreate keys and redeploy.
passwords are better since it is used ONCE, and synced once
```

Harden Web

- Check for webshells
  - disable_functions = exec, passthru, shell_exec, system, proc_open
  - Disable them!

- Check your logs!
- Backup your website

Parsing Log Files

- File locations may differ on different flavors on linux.
- Use your command line magic
- grep
  - -A/-B `<NUM>` show NUM lines before/after
  - -E enable regex mode
  - -v `'<exp>'` show everything except EXP
- cut
- head
  - -n `<NUM>` number of lines to show
- tail
  - -n `<NUM>` number of lines to show
  - -f `<filename>` constantly show this file
- journalctl -e

Monitoring Processes and Services

- ps, pgrep, top - Process Information

- systemctl - Systemd service management

- ss - Show network information

- ps -eLf -e everything, -f full output, -L show threads

- ps fuax

- ss -tlpn - -t tcp, -l listening, -p processID, -n numeric

- systemctl list-units --type service

- systemctl list-unit-files

Recon Network

- tcpdump - Watch network traffic in real time
- ss - socketstat/netstat - View information about sockets
- ss -tlpn
- netstat -tlpn
- tcpdump port `<NUM>` 53

LSOF

- list open files
- since everything is a file, we can pretty much find everything that is going on

- find by process
    - lsof -p `<PID>`
- Find by protocol
    - lsof -i 4
- Tracking networking information
    - lsof -P | grep -ie tcp -e sock

Competition Loop!

- Run 5 minute plan
    - Quick check:
        - users
        - default passwords
        - reading the logs
        - firewall rules
    - Read your logs!
        - Track the oddity in log
        - track the issue
        - Try to fix the issue
    - Switch boxes
    - Repeat!
- Dont add complex solutions to 5 minute plan.
- like removing rootkits, installing a logging server

Example:

```
- Change root password
- disable other accounts
- limit sudo
- limit ssh
- limit ssh users
- setup firewall rules
- reinstall critical binaries
        - ssh, nginx, etc..
```

What not to do!?

- Auto kill the users
  - watch -n 1 netstat -tulpan
  - kill -9 `<ssh-sessions>`
- Auto block ips
  - Redteam can get another IP
  - Best bet is to white list IPs
  - redteam can still ssh in and run commands, just have less time
    - ssh root@target 'mv `which kill` /bin/minenow '
- Delete all the malware you find
- Dont start murdering processes

Common reasons services are down

- They are off

    - service nginx start

- blocked by firewall
    - iptables -L
    - iptables -L -t mangle
- Misconfigured
    - /var/log
    - know what good configs look like
- Still dont know?
    - check logs again
    - service nginx status
    - journalctl

Know your enemy

- Think about the variety of persistence that you may face
- Backdoored service files
- malicious cron jobs
- aliased commands
- webshells, bindshells, reverseShells
- pam.d
- backdoored binaries
- default creds
- rootkit?

- modified MBR??
- .bashrc, inputrc, .bash_profile