ZROC102

Module 2 –Privilege Escalation

Internal Recon

Learning as much as possible about the tagert

Hopefully find a path to escalate privileges

Many different ways to escalate

- Sometimes you need to get creative

Scripts

Linux

- LinEnum
  - https://github.com/rebootuser/LinEnum
- Unix privesc
  - http://pentestmonkey.net/tools/audit/unix-privesc-check
- Linprivchecker
  - https://github.com/reider-roque/linpostexp/blob/master/linprivchecker.py

Windows

- Windows Exploits Suggester
- PowerUp
- post/windows/gather/enum_patches

Exploits

Exploiting the system itself

- Dirtycow

Figure out what's running

- uname -a
- cat /proc/version
- cat /etc/issue

Windows find patches

- wmic qfe get Caption,Description,HotFixID,InstalledOn

Services Running Elevated

Some services may have access to run commands

Database software (Multiple)

- Can execute shell commands
- What if this is running as root?
- We find creds via some other method

Sudo

Lower level user execute as higher level

Check which commands you are allowed to run

sudo -l

- Sudo su
- Other commands?
  - Python
  - Man
  - Nmap
  - Awk

https://gtfobins.github.io/

Service only on localhost?

- Services don’t have to be externally listening
  - Netstat crucial during internal recon
  - `Netstat -anlp`
- Webservers, databases, etc

- Don’t forget about exploits like Eternal blue

Restricted Shell

- Some shells have limited access
  - We need a better shell

- Creating our own better shell
  - `python -c 'import pty; pty.spawn("/bin/bash")'`

Stored Credentials (Windows)

- Finding creds somewhere on disk
  - Config file
  - Password manager database
  - Saved in a browser
  - C:\unattend.xml
  - C:\sysprep.inf
  - C:\sysprep\sysprep.xml
- Weak credentials
- `findstr /si password *.txt | *.xml | *.ini`

Unquoted Service Path (Windows)

- Service is running on Windows
  - Service account has higher permissions
  - Binary is writable by other users

- Replace the binary with our own
  - Msfvenom binary

```
wmic service get
name,displayname,pathname,startmode
|findstr /i "Auto" |findstr /i /v
"C:\Windows\\" |findstr /i /v """
```

Insecure Permissions

Registry Permissions (Windows)

- Install a program
  - Likely creates registry entries
  - ImagePath entry points to an executable
- Normal user has permissions to edit the registry key

Service Permissions

- Edit the service directly

Cron jobs / Scripts run as root (Linux)

Always Install Elevated (Windows)

Local Group Policy setting

If enabled, essentially makes all users admins

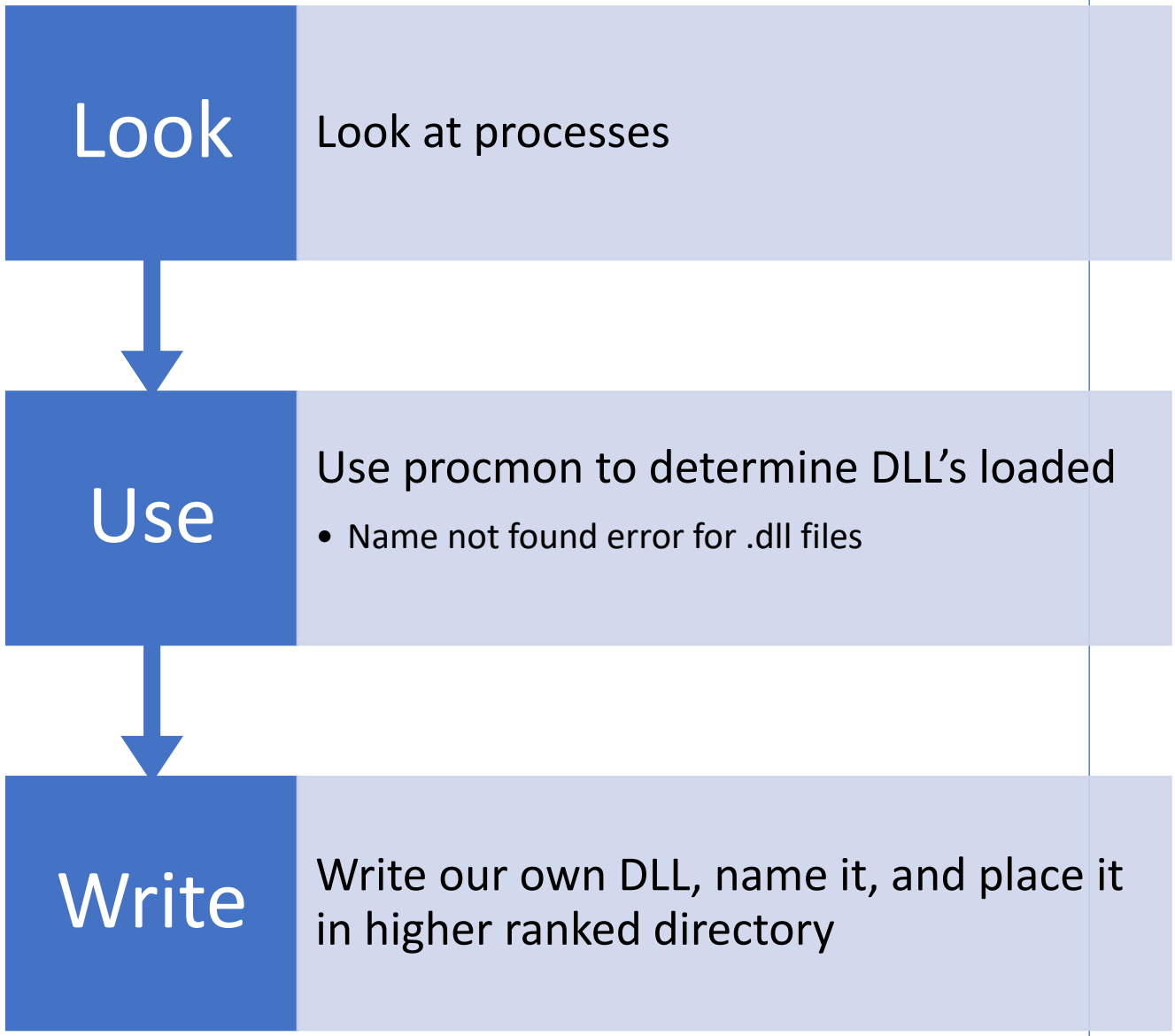
Msfvenom with msi format

DLL Hijacking/Sideloading (Windows)

- Application loads dynamic-link library without fully qualified path
  - Windows searches defined directories
  - https://docs.microsoft.com/en-us/windows/desktop/Dlls/dynamic-link-library-search-order

    - The directory from which the application loaded.
    - The system directory.
    - The 16-bit system directory.
    - The Windows directory.
    - The current directory.
    - The directories that are listed in the PATH environment variable.

DLL Hijacking Process (Windows)



more…

- UAC Bypass
  - Built into some common tools
- Variations of permissions issues
- Escaping restricted shell through other commands

- Finding things laying around on the file system
  - SSH key for the root account in the user account?

Reference

- https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/