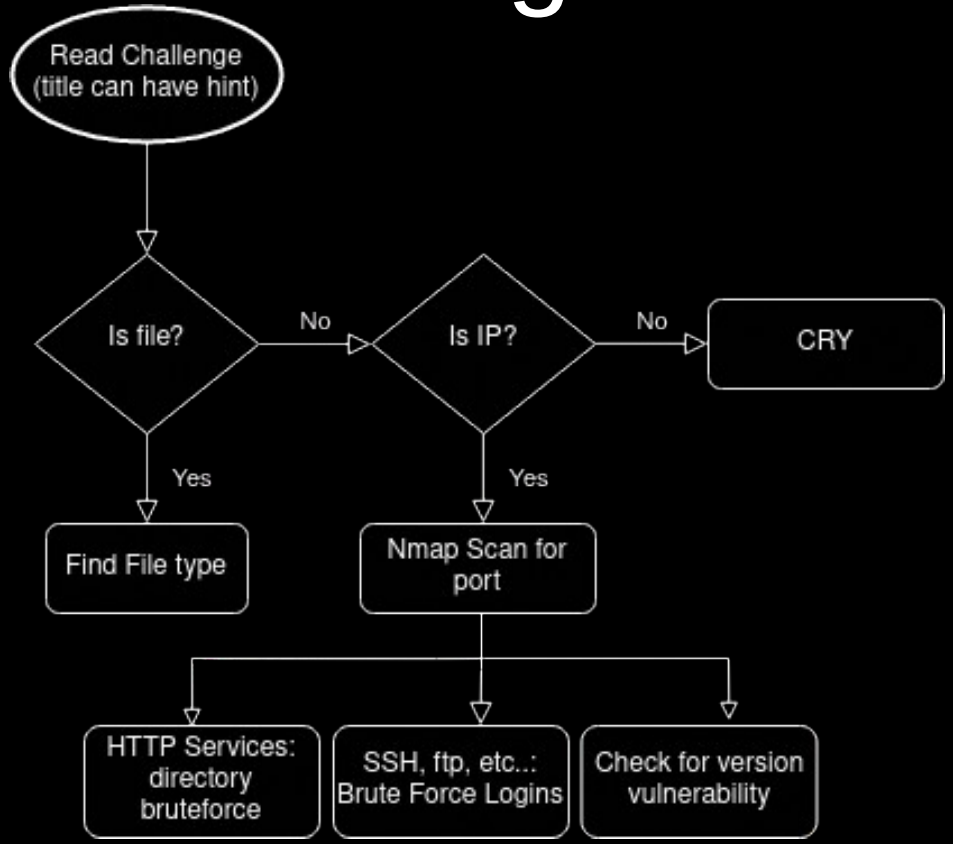
UNIVERSITY OF LIVERPOOL

CYBER SECURITY SOCIETY

CTF stuff

Anatomy of doing most CTF challenges



Port scanning

- Network services are hosted on specific ports e.g. HTTP 80, HTTPS 443
- Port scanning is the process of checking each of these ports to see if a service is hosted there
  - There are standardised ports but people by no means have to abide by them
- Can also do more advanced port scanning to check what service is using the port

Switches (some important ones)

- Scan types
  - -sn : ping scan (doesn’t scan ports, just checks if host online)
  - -sT : TCP connect scan (full TCP handshake)
  - -sS : TCP SYN scan (Just waits for TCP SYN)
  - -sU : UDP scan
- Scan techniques
  - -sV : Probe ports for versions
  - -A : Detect OS, port versions, script scanning, and traceroute
- Timing
  - -T0-5 : Delay between packets (3 or 4 recommended)

Additional tools

- rustscan
  - Does fast SYN scan then uses nmap to do more advanced scans on open ports
- armada
  - Very fast SYN port scanner (doesn’t do advanced scanning)
- masscan
  - Very fast SYN port scanner (doesn’t do advanced scanning)

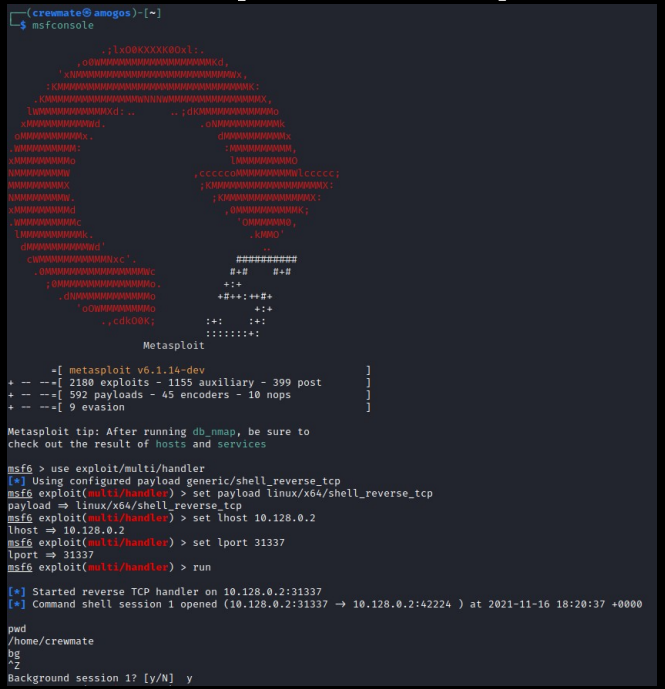
Directory scanning

- Tools
  - dirbuster : GUI, builtin to kali
  - feroxbuster : CLI, install with apt, my preference
  - gobuster : CLI, install with apt
- Lists
  - seclists : Install with apt
  - /usr/share/wordlists/dirbuster/*

```
feroxbuster -ekw /usr/share/seclists/Discovery/Web-Content/big.txt -o "ferox.out" -u "http://10.128.0.1"
```

Reverse shell handling

- Meterpreter (msfconsole)




```
msf6 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type             Information  Connection
  --  ----  ----             -----------  ----------
  1         shell x64/linux               10.128.0.2:31337 → 10.128.0.2:42224  (10.128.0.2)

msf6 exploit(multi/handler) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.128.0.2:4433
[*] Sending stage (984904 bytes) to 10.128.0.2
[*] Meterpreter session 2 opened (10.128.0.2:4433 → 10.128.0.2:49268 ) at 2021-11-16 18:20:59 +0000
[*] Command stager progress: 100.00% (773/773 bytes)
msf6 exploit(multi/handler) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > ls
```

Regex

- Character classes
  - \w
  - [abc21]
  - [1A-Z]
- Groups
  - (text)
  - (?text)
- Repetition
  - \w+
  - \w*
  - \w?
  - \w{1,3}
- Escaping
  - \\

Helpful websites
- regexr.com
- regex101.com

Useful file list

- User info
  - /etc/passwd
  - /etc/shadow
  - C:/Windows/System32/Config/SAM
  - C:/Windows/System32/Config/SECURITY
  - C:/Windows/System32/Config/SYSTEM
- Config files
  - /etc/ssh/sshd_config
  - /etc/nginx/nginx.conf
  - /etc/apache2/apache2.conf
- Logs
  - /var/log/*

Investigating files (strings)

- Strings Is a GNU coreutil (builtin to linux) that prints all ascii strings in a binary
- This can be used to easily find embedded data e.g.
  - flag in a v. easy binexp challenge
  - flag in exif data (might still be better to use proper exif tool)
- Easier to read output
  - strings file | less : scrollable/searchable output (press “/” to search)
  - strings file | grep search term : only print lines matching search term to terminal

Investigating files (file + binwalk)

- file filename : Checks the file signature of a file
- binwalk filename : Scans the file for file signatures
- binwalk -e filename : Scans the file for file signatures and attempts to extract embedded files

Saving output

- When doing challenges it’s a good idea to take notes and save everything your doing in case you want to go back on yourself or continue at a later date
- Saving output of commands on linux
  - ls -la /example > output.txt : write output to file (not output to terminal)
  - ls -la /example | tee output.txt : write output to file (and output to terminal)
  - ls -la /example | xclip -sel clip : write output to clipboard (only works well for text)

Teamwork

- Don’t be afraid to ask other people for ideas, especially If stuck
- When you might not all be doing CTF at same exact times it is useful to share notes
- Have fun, make jokes (or else: mike shallot will get you)