THE ART OF RECON (*W/ SOME NETWORKING*)

Trevon

ANNOUNCEMENTS

- National Cyber League Registration Opens **TODAY** (12 slots)
- Have a question ?
  - **Lab Hours** (Check #lab for more postings)
    - *Monday* 12:00 – 5:30
    - *Tuesday* 2:30 – 6:00
    - *Thursday* 12:00 – 5
    - *Friday* 4:00 - 6:30
- Competition Practice on Friday’s and Saturday’s (Open to Everyone)

WHO AM I

- Graduate Student
- blackmanta (on slack)
- Competition enthusiast
- Linux Junky

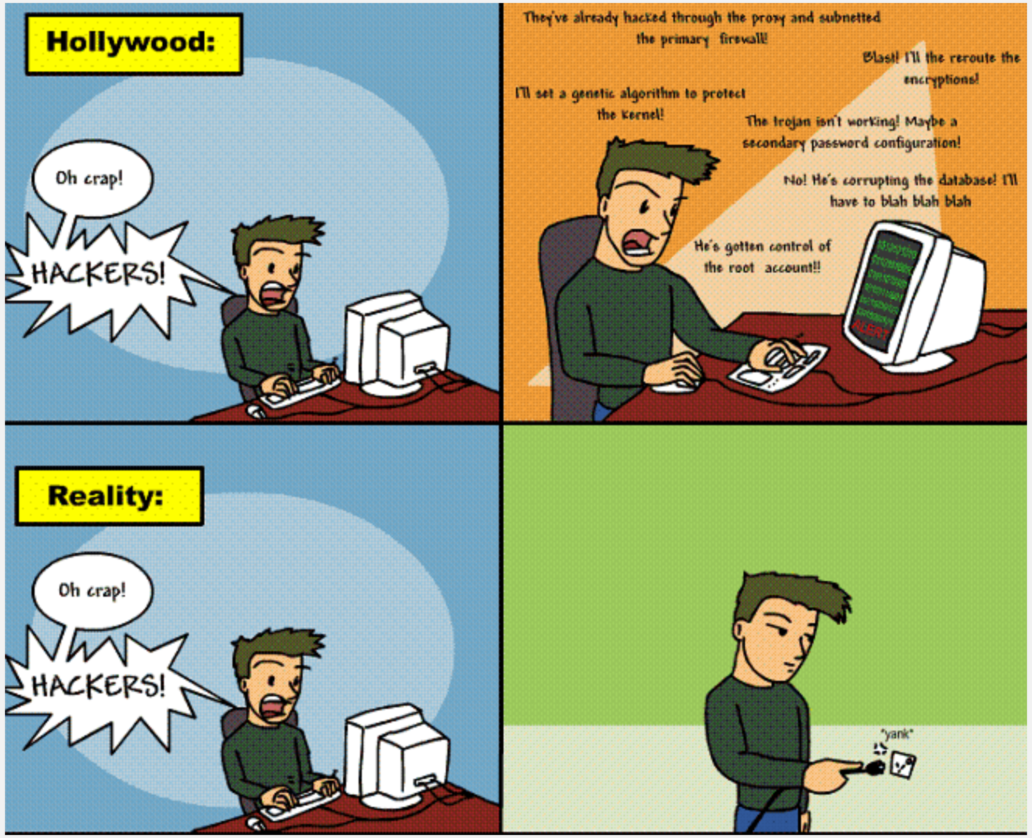
WHAT WE COVERED LAST WEEK…

- *Slides in #education_n_training slack channel*
- What the 49th is about
- Creating a https://hackthebox.eu account
- Build a methodology (*kinda*)
- Some introductory ideas

DISCLAIMER

- Please do not be afraid to ask questions (*I can talk allot*)
- Please do not use what you learn here to hack things unethically
- If you feel intimidated its ok

WHAT IS RECON


Hollywood:
Oh crap!
HACKERS!
They've already hacked through the proxy and subnetted the primary firewall!
Blast! I'll the reroute the encryptions!
I'll set a genetic algorithm to protect the kernel!
The trojan isn't working! Maybe a secondary password configuration!
No! He's corrupting the database! I'll have to blah blah blah
He's gotten control of the root account!!
ALERT
Reality:
Oh crap!
HACKERS!
yank

Not related to the question

RECON

- Gathering information to know how to target systems
  - Fingerprinting, Scanning, Enumeration
- Active and Passive Reconnaissance
  - Active Scanning requires consent
- What about OSINT?

WHAT IS AN EXAMPLE PASSIVE RECON?

WHAT IS AN EXAMPLE ACTIVE RECON?

NETWORK SPECIFIC TOOLS

Not a comprehensive list

- Networking
  - nmap (cli)/Zenmap (gui)
  - Wireshark (passive networking)
  - OWASP Zap, Burp
- Enumeration (Active Scanning)
  - Gobuster, wfuzz, dirb, dirbuster etc.
- Vuln scanner
  - Nmap, searchsploit, nessus etc.

USING NMAP

- What can we use it for?
  - To find live hosts
- Finding Vulns
- Scripting with Lua

NMAP REFERENCES

- Nmap Book
- Nmap Reference Guide
- Nmap Documentation
- Nmap: Network Exploration and Security Auditing

NMAP IN THE WILD (TRAVERXEC)

SOME EXTRA RESOURCES

- Hacker methodology (MITRE ATT&CK)
- Hacking NMAP – Defcon 13
- Getting Started with Wireshark
- OWASP Zap Documentation