MISC

Recon and Enumeration

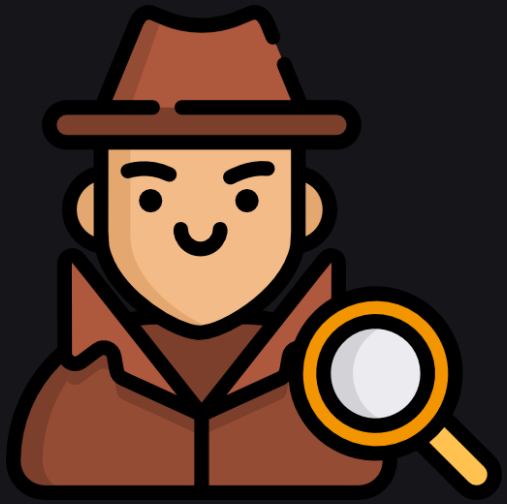
accenture

WHAT IS RECONNAISSANCE (RECON)?

- Gathering information about the target(s)
- Get a good understanding of the technologies being used
- Can be passive (openly available information in the web) or active (interacting with the target)

WHAT IS ENUMERATION?

- Process of extracting useful information from a system
- The attacker interacts with the system and performs scans
- Attempt to identify pre-existing vulnerabilities



RECON vs ENUMERATION

Recon	Enumeration
A very broad process	A subset of recon
Both active and passive	Active
General and Specific	Specific

WHY ARE THEY IMPORTANT?

- A proper recon would provide detailed information – open ports, running services
- Often the scope of our target can be massive – Large corporations with hundreds of subdomains
- Allows us to find the most vulnerable target

THINGS TO LOOK FOR DURING RECON

- Subdomains
- Target's infrastructure
- Credential dumps and API keys
- Cloud servers and services
- Other assets

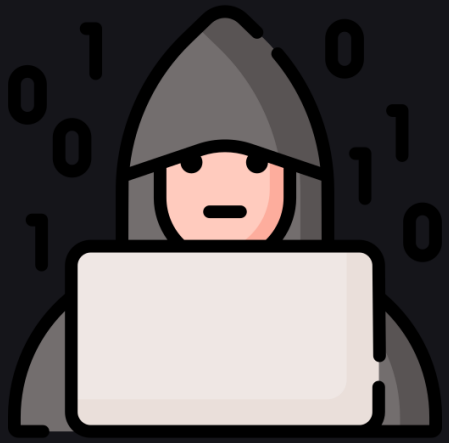
MY RECON FRAMEWORK

1. Target Validation

2. Finding Subdomains

3. Fingerprinting

4. Known data breaches



TARGET VALIDATION

- Determine the scope of target
- Identify whether target is online
- Validate if information are correct
- Tools: WHOIS, nslookup, dnsrecon

FINDING SUBDOMAINS & VALIDATION

- And extension to domain to organise and navigate different section of website
- Particular subdomains can expose relatively vulnerable information
- Not all subdomains we found will be active
- Tools: dig, sublist3r, crt.sh, , httprobe

FINGERPRINTING

- Collecting sensitive information about the target
- Access security posture – firewalls and protections
- Reduce attack area
- Identify vulnerabilities
- Tools: nmap, Wappalyzer, WhatWeb, BuildWith, Netcat

DATA BREACHES AND EXPLOITS

- No need to reinvent the wheel
- Older systems and technologies often have known vulnerabilities
- If the company has faced a data breach before then chances are there are creds still floating in the web
- Tools: ExploitDB, HaveIBeenPwned, Breach Parse, Metasploit

TOOLS

Domains
- Hunter.io
- Theharvester
- Breach parse

Subdomains
- Sublist3r
- Crt.sh
- Owasp Amass
- Httprobe

Web Technologies
- Wappalyzer
- Whatweb
- Buildwith

HTTP/HTTPs
- Nmap
- Nikto

Directory Bustring
- Dirb
- Dirbuster

Active Scanners
- Nmap
- Nessus
- Netcat

Resources

YouTube Videos
https://www.youtube.com/watch?v=ZBi8Qa9m5c0&t=2195s

https://www.youtube.com/watch?v=Wpm2C1LD9ns

Useful Recon Tips
https://www.youtube.com/watch?v=amihlWTtkMA

Automating Recon
https://www.youtube.com/watch?v=YT5Zl2jW3wg

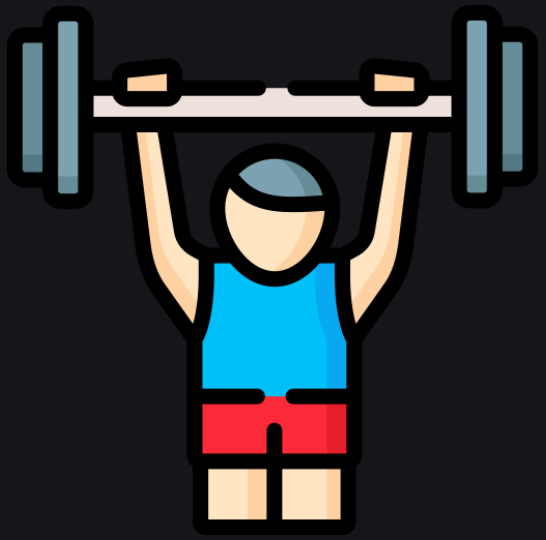
Practice Recon

Live Machines

- HackTheBox
- Vulnhub
- Bug Bounty Programs

YouTubers – Live Recon Sessions

- Nahamsec
- Jason Haddix
- The Cyber Mentor



WANT TO KNOW ABOUT CUTTING EDGE RECON AND INTELLIGENCE?

THANK YOU!

Please ask any questions you have in the chat!