Difficulty: Novice

Ethical Student Hackers

Enumeration - Tools & Techniques

The Legal Bit

- The skills taught in these sessions allow identification and exploitation of security vulnerabilities in systems. We strive to give you a place to practice legally, and can point you to other places to practice. These skills should not be used on systems where you do not have explicit permission from the owner of the system. It is VERY easy to end up in breach of relevant laws, and we can accept no responsibility for anything you do with the skills learnt here.

- If we have reason to believe that you are utilising these skills against systems where you are not authorised you will be banned from our events, and if necessary the relevant authorities will be alerted.

- Remember, if you have any doubts as to if something is legal or authorised, just don't do it until you are able to confirm you are allowed to.

- Relevant UK Law: https://www.legislation.gov.uk/ukpga/1990/18/contents

Code of Conduct

- Before proceeding past this point you must read and agree to our Code of Conduct - this is a requirement from the University for us to operate as a society.

- If you have any doubts or need anything clarified, please ask a member of the committee.

- Breaching the Code of Conduct = immediate ejection and further consequences.

- Code of Conduct can be found at https://shefesh.com/downloads/SESH%20Code%20of%20Conduct.pdf

First - EGM Voting!

Vote here:

https://forms.gle/MG5JSLGY3auw2m9c6

Input your university email - you must have paid for a membership to vote!

What is Enumeration?

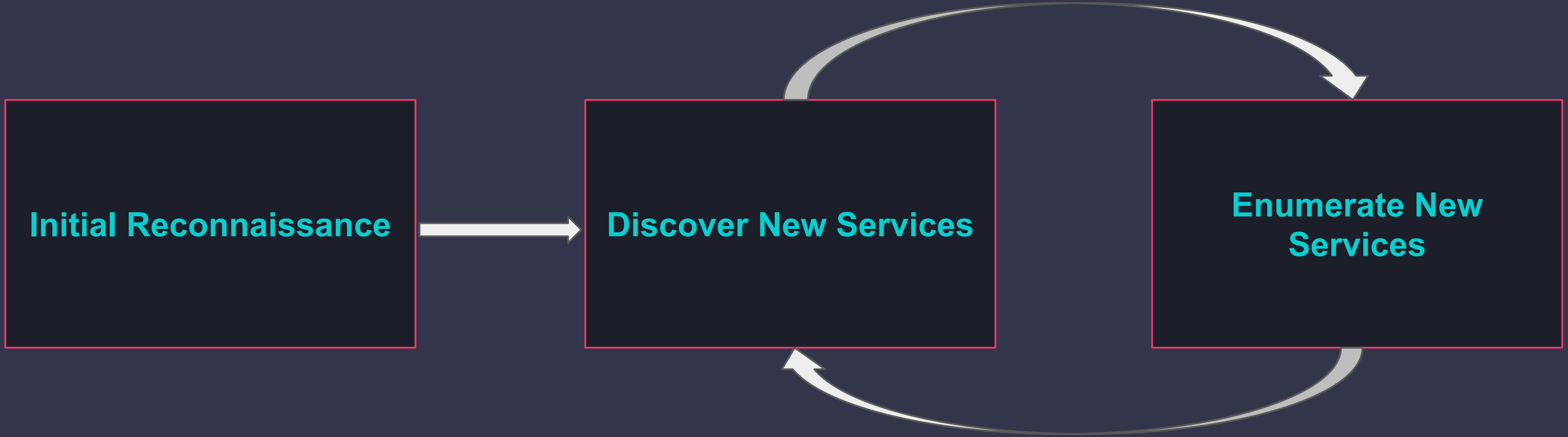
Also known as reconnaissance, enumeration is the first and most important step in a penetration test

The goal is to extract information about your target that will help you compromise them:

- IP addresses of machines belonging to the target
- Information about the target’s operations (how they conduct business / share files / manage staff…)
- Names of users of any systems that are in scope
- Operating system of systems that are in scope
- Services running / software installed on servers or workstations that are in scope
- Version numbers for these services (especially vulnerable ones!)
- Interesting files on an exposed file system
- Credentials that have been leaked or exposed

And anything else that may be useful… You will learn how to identify useful / useless information with experience, but it can often be deceptively useful…

A Recursive Process



Repeat until you are successful or until you decide to leave cybersecurity for good.

Why should you do it?

To figure out the kind of system:

- Is it networked? (Incoming / Outgoing connections, funky protocols, access to critical resources)
- What is its purpose? (A Domain Controller? A file share? An email server? A workstation?)
- What operating system does it use? What services does it provide, and are they up to date?

To figure out a way in:

- Vulnerable software, exposed ports, and leaked credentials
- Interesting files, unusual scheduled processes, local only services, logic flaws

…and a way out:

- Is there a firewall or an EDR? Can you setup a C2 using weird protocols / info you gathered?
- What tools can you use to exfiltrate data? What is your target / the purpose of your attack?

What are you looking for?

This changes at each stage…

Open Source Intelligence Gathering (OSINT) - Names of employees and users, security question answers, lanyard layouts, email and username formats, open articles/guides that imply company processes

Initial Network Reconnaissance

- Addressed machines (and their purposes) in the in-scope address space
  - Workstation? Server? Firewall? Load Balancer? Are they on-prem or in-cloud?
- Domain names associated with network resources
- Evidence of machines that might talk to each other / serve a similar purpose
- Evidence of network partitions (e.g. subnets for certain purposes)
- Services that are running on certain machines

What are you looking for?

Initial Access

- Web Servers: Internal domain names, tech stack version numbers, admin consoles, source code leaks or links, exposed config files…
- Databases: SQL or NoSQL services open to the internet, or vulnerable to SQLi
- Outdated services: Version numbers + google (your most important tool) may reveal easy RCE
- Credentials: Can you test credentials easily? Are there default credentials? Can you find credentials leaked in a web application or some OSINT? If you find credentials, can you reuse them?

Post-Exploitation

- Privilege escalation via running services, kernel exploits, local services, credentials in memory, sudo tokens, misconfigured permissions, and more…
- Firewall rules, antivirus, Endpoint Detection & Response software, etc that may prevent you from exfiltrating data/causing an impact

... and how can you find it?

Let’s stop being so high level - what tools can we use to do this?

Network Enumeration: nmap, dig, nslookup, dnsrecon, nessus, autorecon (but first try doing it manually!)

Webserver Enumeration: feroxbuster, nikto, ffuf, sqlmap

Fileshare Enumeration: smbmap, smbclient, crackmapexec, ftpclient

Domain Controller Enumeration: ldapsearch, rpcclient, crackmapexec, impacket

Post Exploitation: LinPEAS, WinPEAS, Bloodhound

Misc Tools: snmpwalk, deepce, Maltego

Most of these tools come preinstalled on Kali Linux! (along with wordlists to feed them)

Many tools serve the same / multiple purposes, but work differently - it’s important to learn many!

Nmap

Scan an IP/Domain Name: nmap [IP/DOMAIN]

Scan all ports: nmap -p- [IP/DOMAIN]

Scan specific ports: nmap -p 1-1000,8080,9001

Don’t do ping probing: nmap -Pn [IP/DOMAIN]

Run standard scripts and version detection: nmap -sC -sV [IP/DOMAIN]

Scan UDP: nmap -sU [IP/DOMAIN]

Run a specific script: nmap --script=[SCRIPT_NAME] [IP/DOMAIN]

Save your results: nmap -oA [path/to/file] [IP/DOMAIN]

Use verbose mode to see ports as they appear/diagnose issues: nmap -v [IP/DOMAIN]

You can, of course, combine these flags - e.g. scanning specific ports with -sC and -sV flags

Mini Practical

I’ll briefly show you how to connect to TryHackMe and scan a machine with Nmap

Follow along if you wish, but you’ll have a chance to spend more time on it later in the session

https://tryhackme.com/room/kenobi

Enumerating SMB

Try anonymously listing shares: smbclient -L [IP] -N

Use crackmapexec to do the same thing: crackmapexec smb [IP] --shares

Or smbmap: smbmap -H [IP] (anonymously with smbmap -u null -p "" -H [IP])

Connect and explore a share: smbclient \\[IP]\[Share] {-U [username]}

- dir, cd [directory], get [file], put [file], lcd [localdirectory]

Connect anonymously: smbclient -U "" -N

You sometimes may have to play around with -U "" vs -N, or the number of backslashes around the server name and share (e.g. smbclient \\[IP]\[Share] or smbclient \\\\[IP]\\[Share])

Checking writeups of similar machines or cheatsheets is a good way to find new commands to try if you’re stuck!

Webserver Enumeration

Finding new webpages:

- Feroxbuster default config: feroxbuster -u [IP/DOMAIN]
    - Add known file extensions: feroxbuster -u [IP/DOMAIN] -x [extension,extension,...]
    - Ignore certain response codes: feroxbuster -u [IP/DOMAIN] -C [CODE]
    - Add a cookie to request (for auth): feroxbuster -u [IP/DOMAIN] --cookies [COOKIES]
    - With a delay between requests: feroxbuster -u [IP/DOMAIN] -T [DELAY]
    - With a specific wordlist: feroxbuster -u [IP/DOMAIN] -w [/path/to/wordlist]
- Gobuster: gobuster dir -u [IP/DOMAIN] -w [/path/to/wordlist]
- Dirbuster: https://www.kali.org/tools/dirbuster/ (GUI if you prefer, but slower as Java < Rust)

Finding new subdomains:

- ffuf: ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -H "Host: FUZZ.[DOMAIN]" -fc 400,403 -u [DOMAIN] (can do same with wfuzz, using --hc)
    - Ignore certain response lengths: -S [size]
- Gobuster: gobuster vhost -u [DOMAIN] -w [/path/to/wordlist]

Webserver Enumeration

Fuzzing endpoints with ffuf:

- Spray usernames with a found password: ffuf -u [URL]/search -X POST -d username=FUZZ -w /usr/share/seclists/Fuzzing/big-list-of-naughty-strings.txt
- Try bad data in a POST: ffuf -u [URL]/search -X POST -d searchterm=FUZZ -w /usr/share/seclists/Fuzzing/big-list-of-naughty-strings.txt
- Try special characters in a URL parameter: ffuf -u [URL]/profile?id=FUZZ -w /usr/share/seclists/Fuzzing/special-chars.txt
- Fuzz a cookie: ffuf -u [URL] -b "auth=FUZZ"
- Check for LFI: ffuf -u [URL]?page=FUZZ -w /usr/share/seclists/Fuzzing/LFI/LFI-gracefulsecurity-linux.txt

Vulnerability scanning with Nikto: nikto -host=[URL]

Manual things to enumerate:

- Tech stacks leaked in response headers (Server, X-Powered-By, PHPSESSID, etc…)
- Test whether / responds to /index.html, /index.php, /index.asp, etc..
- Provoke errors with unexpected data/characters, unknown URLs…
- Read SSL certificates to look for addresses, domains, etc

No file extension can also be a telltale sign of Flask / NodeJS based webservers

Other Tools!

Massively automated scanners (better to do scansmanually while learning, but good to tick all boxes):

- autorecon (runs Nmap and then all the scripts you might run by default on found services)
- enum4linux (confusingly, for enumerating Windows servers…)

Privilege Escalation Tools (more on these in another session):

- WinPEAS (quintessential privesc script for Windows hosts)
- LinPEAS (as above, for Linux)
- deepce (Docker Enumeration)

Useful for Active Directory (again, we'll cover this in semester 2):

- ldapsearch (for searching AD directories using LDAP and discovering users, computers, etc…)
- rpcclient (rpcclient -U "" -N [DOMAIN] to connect anonymously, enumdomusers to list users)
- Learning to use crackmapexec to its maximum potential is also a crucial skill :)
- BloodHound (AD scanning tool, used after Initial Access, so also for privesc)

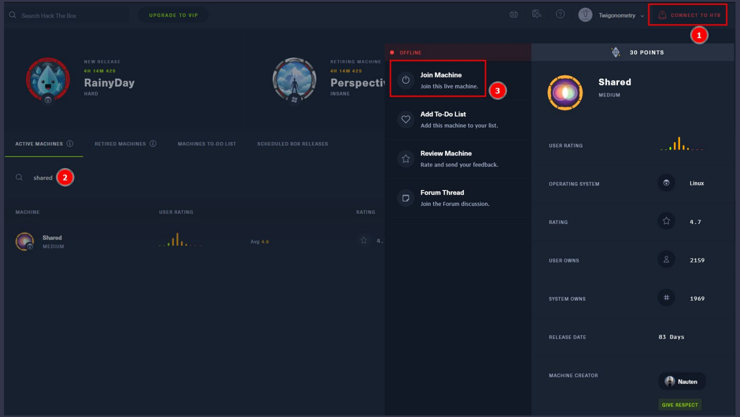
Practical

Over to you!

Practical Enumeration

Hack the Box Challenges (https://hackthebox.com)

- Sign up for an account and download connection pack, then launch a box
- You will need a Linux Distribution / VM
- For each box, identify running services, version numbers, and which operating system the box is
- See next slide for specifics…



MACHINE	USER RATING		RATING
Shared MEDIUM		Avg 4.9	4.

Join Machine — Join this live machine.

Add To-Do List — Add this machine to your list.

Review Machine — Rate and send your feedback.

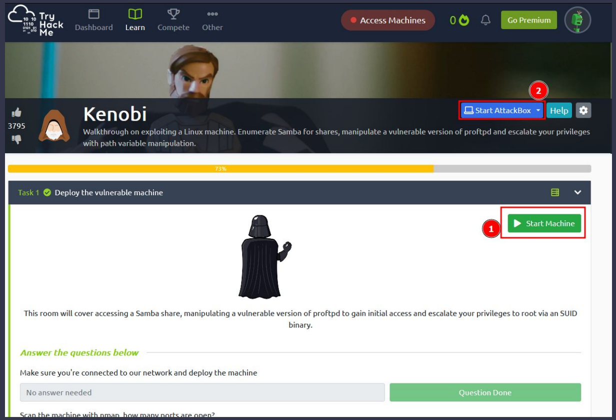
Forum Thread — Join the Forum discussion.

Shared
MEDIUM

USER RATING	
OPERATING SYSTEM	Linux
RATING	4.7
USER OWNS	2159
SYSTEM OWNS	1969
RELEASE DATE	83 Days
MACHINE CREATOR	Nauten

TryHackMe Challenges (https://tryhackme.com)

- For anyone who couldn't set up a Kali VM / doesn't have Unix (or if you want to try it)
- Sign up for a free account
- TryHackMe lets you use their AttackBox VM for up to an hour a day - for free!
- Learn > search for a room, press 'Join Room', then 'Start AttackBox' and answer the questions!



Kenobi

Walkthrough on exploiting a Linux machine. Enumerate Samba for shares, manipulate a vulnerable version of proftpd and escalate your privileges with path variable manipulation.

Task 1 Deploy the vulnerable machine

This room will cover accessing a Samba share, manipulating a vulnerable version of proftpd to gain initial access and escalate your privileges to root via an SUID binary.

Answer the questions below

Make sure you're connected to our network and deploy the machine

No answer needed

Scan the machine with nmap, how many ports are open?

Practical Enumeration

Hack the Box Challenges (https://hackthebox.com)

Pick any number of these/the THM challenges on next slide - but you may get more from focusing on one and doing it well :)

Trick (Easy - 10.10.11.166)

- What is the domain name? Hint: what service deals with domain names?
- What subdomains does the webserver have?
- What tech stack are the site(s) running?
- What server + version is powering the backend?

Outdated (Medium - 10.10.11.175)

- What issue do you find immediately and how do you fix it?
- This one takes a while to scan - can you use nmap's flags to identify ports as the scan finds them, rather than seeing the output at the end?
- Can you access any files with anonymous login credentials?

Shared (Medium - 10.10.11.172)

- What's the domain name?
- Are there any subdomains?
- What technology does the site use?
- What about the sites on other domains?

Practical Enumeration

TryHackMe Challenges (https://tryhackme.com)

- Recommended Rooms (mix of Nmap, SMB, and web scanning)
  - Kenobi (guided enumeration boot2root) - https://tryhackme.com/room/kenobi
  - Blue (another guided boot2root) - https://tryhackme.com/room/blue
  - Blog (less guided, involves web) - https://tryhackme.com/room/blog
  - Attacktive Directory (to really test your enum skills… don't worry about the AD exploitation part as we haven't taught this yet) https://tryhackme.com/room/attacktivedirectory
- If you want to learn more about a specific tool
  - Nmap: https://tryhackme.com/room/furthernmap
  - Other Network Scanning Tools (telnet, nc, ping, traceroute): https://tryhackme.com/room/activerecon

We won't have time to cover the answers to every room, but will look at Kenobi and some HTB machines! You can tackle these in your own time if you wish for more…

Final Thoughts

Enumeration is the most important step and skill, and will inform the whole pentest

Google is your best friend! As are these websites:

- https://book.hacktricks.xyz/ (search “service + hacktricks” for how to enumerate anything)
- https://github.com/swisskyrepo/PayloadsAllTheThings (command examples for many tools/attacks)
- https://ippsec.rocks/?# (search any service for a video about it)
- https://0xdf.gitlab.io/ (detailed writeups with searchable tags)
- https://shefesh.com/wiki/resources (of course, self plug)

Our old enumeration slides have even more examples of Windows + AD Enumeration, if you can’t wait until that session to find out more: https://shefesh.com/assets/wiki/Enumeration.pdf

Upcoming Sessions

What's up next?

www.shefesh.com/sessions

24/10/22 - Bad USBs

We will **not** be changing the regular meeting time - the turnout was not high enough for a definitive answer

Any Questions?

www.shefesh.com

Thanks for coming!