# Ethical Student Hackers

Enumeration

# 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 **shefesh.com/conduct**

# What is Enumeration?

- A reconnaissance process
- Goal is to extract information about your target that will help you compromise them

## What does it involve?

Active information gathering

Detailed data extraction

Vulnerability identification

# Why do we want it?

- To figure out the kind of system:
  - Whether it's networked (outgoing and incoming connections, protocols)
  - What the OS is (Any known exploits? Vulnerable kernel versions?)
  - What its purpose is (web server? Domain controller?)

- To figure out a way in
  - Vulnerable software versions or exposed ports
  - Users and credentials left lying around

- To spot anything out of the ordinary
  - Interesting files, unusual scheduled processes, local only services, logic flaws
  - Remote connections to other services/machines

# What are we looking for?

Examples of information collected

- Usernames - useful for brute-force attacks or social engineering
- Network services - open ports and services running on them (SMB, LDAP, Kerberos)
- Operating system details - knowing the OS and patch level helps identify known vulnerabilities
- Network resources - Mapping out shared folders and network printers can reveal sensitive data or access points

# Nmap

Nmap is one of the first steps in a security assessment - it scans the most common ports (or a specific list of ports), checks if they are open, and tries to discover services on each of them. It comes preinstalled on Kali Linux

A standard command to run nmap on the most common ports is: nmap -sC -sV [ip]

- sC is use default scripts
- sV is enumerate versions/services
- oA [file directory] can be used to output the data in all formats to a directory

You can also specify ports with the -p flag (use -p- to scan all 65535 ports) and control the speed of the scan with the -Tx flag where x is the intensity from 0 to 5 (5 is highest!)

The -O flag discovers the operating system.  Another tip is to run an all ports scan in the background while you test (use nmap -p- [ip])

# 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

# Gobuster

Gobuster is a fast directory/file brute-forcer for web servers. Use it to find hidden directories, files, and common admin pages.

Example command : gobuster dir -u http://10.10.10.5 -w /usr/share/wordlists/dirb/common.txt

- dir : directory discovery mode.
- -u : target URL.
- -w : wordlist path.

**What to look for in results**: 200 means page exists, 301/302 means redirected, 403 means blocked (may still be interesting).

# Gobuster

```
root@ip-10-10-65-99:~# gobuster dir -u "www.offensivetools.thm" -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://www.offensivetools.thm
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 333]
/home                 (Status: 200) [Size: 8818]
/media                (Status: 301) [Size: 332]
/templates            (Status: 301) [Size: 336]
/modules              (Status: 301) [Size: 334]
/plugins              (Status: 301) [Size: 334]
/includes             (Status: 301) [Size: 335]
/language             (Status: 301) [Size: 335]
/components           (Status: 301) [Size: 337]
/api                  (Status: 301) [Size: 330]
/cache                (Status: 301) [Size: 332]
/libraries            (Status: 403) [Size: 287]
/tmp                  (Status: 301) [Size: 330]
/layouts              (Status: 301) [Size: 334]
/secret               (Status: 301) [Size: 333]
/administrator        (Status: 301) [Size: 340]
Progress: 6300 / 218276 (2.89%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 6329 / 218276 (2.90%)
===============================================================
Finished
===============================================================
root@ip-10-10-65-99:~#
```

# Example Enumeration Walkthrough

**Goal**: Discover hidden information on a website (http://10.10.10.5),

1) Discovery with nmap: nmap -sC -sV -p- 10.10.10.5

→ Open ports: 22 (ssh), 80 (http). Apache version and modules identified.

2) Directory discovery (Gobuster): gobuster dir -u 10.10.10.5 -w /path/to/wordlist.txt

→Result: Found /admin/ (200), /dev/config.php (200), /old/ (301).

3) Check folders/files: Investigate results.

→Use those clues safely to continue investigation.

# Practical

- https://tryhackme.com/room/nmap01
  - Walks you through how to use nmap to discover live hosts
- https://tryhackme.com/room/easypeasyctf
  - Make an account
  - Connect using the VPN or use the attack box
    - If it doesn't work go to the /access page and change the region
  - Scan the target machine
  - You don't have to do the cron job bit
- If you finish try:
  - https://tryhackme.com/room/ice
  - https://tryhackme.com/room/kenobi

# Feedback + Inclusion Forms

Please leave your feedback :) We want to know what we can do to improve.

https://forms.gle/VTYd74K5BHqbC7F68

If there's anything preventing you from enjoying our sessions, please let our Inclusions Officer know. You can contact them by email or fill in the form below:

jgledhill2@sheffield.ac.uk

https://forms.gle/Qct6Wyfesv8dWmej7

# Upcoming Sessions

What's up next?

www.shefesh.com/sessions

Next week: YHROCU

# Any Questions?


www.shefesh.com

Thanks for coming!