Ethical Student Hackers

Reconnaissance & Enumeration

SHEFFIELD | Ethical Student Hackers

Breaking into security.

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.

SHEFFIELD Ethical Student Hackers
Breaking into security.

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

SHEFFIELD Ethical Student Hackers
Breaking into security.

What is Reconnaissance?

Professional ethical hackers follow a certain process when testing the security of a system:

1. Reconnaissance
2. Enumeration/Scanning
3. Exploitation
4. Privilege Escalation
5. Covering Tracks
6. Reporting

Reconnaissance is the first and most important step in a penetration test, which involves collecting information about your target without directly interacting with it. Doing it properly facilitates your ability to exploit vulnerabilities later on.

Types of Reconnaissance

1. Passive Reconnaissance

- relies on public information from public resources
- no direct interaction with the target

Examples:
*reading news articles about the target
*looking up DNS records of a domain from a public DNS server


Source: tryhackme.com

2. Active Reconnaissance

- requires engaging with the target

Examples
*connecting to a server, such as HTTP, FTP, SMTP...
*attempting to gather information by making a phone call (social engineering)

Reconnaissance Tools

There are a lot of tools available, both technical and less technical that can help you collect the relevant details that you need.

Even if it seems like hackers use complex tools during the reconnaissance process, that is not always the case, and some of them are used a lot by many people. The ones that are easier to use are:

*Google (Google Dorking)

*Wikipedia

*PeopleFinder.com

*who.is

*hunter.io

*builtwith.com

Enumeration

Once the ethical hacker has finished reconnaissance, they move on to the second step: enumeration. It is now time to interact with the target to find vulnerabilities and the attack surface.

The attack surface determines what the target might be vulnerable to, and that is the purpose of the enumeration process.

Just like reconnaissance, if this step is done properly, it will be much easier to, first of all, find vulnerabilities, and then also exploit them.

Enumeration Tools

Enumeration tools are more specialised than reconnaissance tools, but they can be learnt as you practise using them.

Some useful and popular tools include:

- nmap
- gobuster
- nikto
- metasploit
- burp suite
- dirb
- exploit-db
- enum4linux

Nmap

Nmap (Network Mapper) 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 pre-installed on Kali Linux.

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

- sC is use safe/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), do a “ping scan” with -sn, a UDP scan using -sU.

The -O flag discovers the operating system and -A enables aggressive mode.

Gobuster

Gobuster is a tool that is used for enumerating multiple services, most notably HTTP/S services. However it also supports DNS and vhost enumeration.

After an nmap scan it’s always worth having some form of enumeration running in the background while you actively search for other exploitation paths. An example of this would be to run gobuster file/directory enumeration against the server you're exploiting.

- gobuster dir -w [file/directory wordlist] -u [http:// + ip]
  - -x can be used to specify extensions, e.g. -x php,html,txt
  - -s & -b can be used to add or remove response codes from the filter list
  - -H specifies a HTTP header
  - -k skips SSL certificate verification
  - -a specifies a user agent

Gobuster can also be used for DNS enumeration for subdomains as well as virtual host enumeration.

More flags: https://www.kali.org/tools/gobuster/

Nikto

Nikto is another enumeration tool that scans for common vulnerabilities and provides some information about the web server.

Like the other tools, it has flags that you need to use to tell the tool what exactly it has to do:

* -h specifies the host

* -nossl disables ssl and -ssl forces ssl

* -id is used to specify the username and password
* -plugin selects the plugin to use, --list-plugins list all possible plugins, and -update updates the plugin list

Post-enumeration

The steps that follow after reconnaissance and enumeration are the following:

*Exploitation: this is when the actual attack takes place; the success of it depends heavily on the previous two steps

*Privilege Escalation: attempting to gain the highest possible privilege (administrator/root) post-exploitation

*Covering Tracks: not really necessary for professional hackers because of the agreed contract; however, it is crucial to keep track of and report what you have done during the test

*Reporting: once you are done, reporting your findings and recommendations helps make the tested system more secure

Practical Exercises

1. Reconnaissance & Enumeration Basics

Solve tasks 1-3: https://tryhackme.com/room/hackermethodology

2. Active & Passive Reconnaissance

Solve task 2: https://tryhackme.com/room/passiverecon

3. Useful tools

Solve tasks 1, 3, 4: https://tryhackme.com/room/ccpentesting

Upcoming Sessions

What’s up next?

www.shefesh.com/sessions

8th Nov - Shells

15th Nov – Using Docker

22th Nov – Privilege Escalation

06th Dec – Hack the Box

Any Questions?

www.shefesh.com

Thanks for coming!

SHEFFIELD Ethical Student Hackers

Breaking into security.