Ethical Student Hackers

Pen Testing

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

What is Pen Testing

We have been teaching you aspects of pen testing all along!

- Scope
- Information gathering
- Enumeration/Scanning
- Exploitation
- Privilege Escalation
- Post-Exploitation

Scope

Scope is quite possibly the most important step

- Rules of Engagement
- Permission
- Test Scope - often specific domains - burp suite is awesome for this
- Rules - often what you can’t do

https://hackerone.com/amazonvrp?type=team

Information Gathering

- OSINT
- For web hacking - checkout the domains you are in scope for
- This isnt random - there are manuals and frameworks for standardisation and automation

Frameworks:

- OWASP - web hacking
- OSSTMM - very technical in depth for general systems
- NIST - produces CVE for every known exploit + ratings
- NCSC CAF - This one is mainly for organisations but useful to know

Note: there is no active gathering, only passive (so no port scanning)

Enumeration/Scanning

- Scanning using nmap
- Port services can be obsfucated - port 25 is often SMPT protocol (emails)

Find services

Get version numbers

Check known exploits - https://nvd.nist.gov/vuln/detail/CVE-2024-11477

There are online databases - https://nvd.nist.gov/ (there are many, this is an example)

Exploitation

The ‘hacking’ part

Use the exploit you have found to get deeper access into the system

Cant get access to the service you want to exploit?

Use web hacking skills to get deeper access, and optionally laterally escalate (different user same permissions) to get to the service

Linux Metasploit

Privilege Escalation

Once you have access to the system

Main goal is root

Why?

Could do a whole session on this, it very much depends on what the system is and how it is configured

There are various vectors of attack - common ways of exploiting systems.

Check out: https://tryhackme.com/module/privilege-escalation

Post-Exploitation

We have been teaching you aspects of pen testing all along!

- Scope
- Information gathering
- Enumeration/Scanning
- Exploitation
- Privilege Escalation
- Post-Exploitation

Practical

Try Hack Me:

Very simple walkthrough - dont need to read all of it - good referral tool: https://tryhackme.com/r/room/pentestingfundamentals

↓

Privilege Escalation: https://tryhackme.com/r/room/linprivesc - again dont have to do all of it, checkout the full hack to see which bits are relevant

↓

OpenVPN (NEEDED) https://tryhackme.com/r/room/openvpn

The full hack: https://tryhackme.com/r/room/kenobi

Feedback

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

Please leave constructive and honest feedback only.

https://forms.gle/VTYd74K5BHqbC7F68

Competition

Link: https://forms.gle/QZK86dLEbvcsyPKf9

Upcoming Sessions

What's up next?

www.shefesh.com/sessions

9th December: NO SESSION

16th December: Lockpicking

Any Questions?

www.shefesh.com

Thanks for coming!