Ethical Student Hackers

Penetration 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 **shefesh.com/conduct**

Pentesting - What is it?

Penetration testing (pentesting) is an authorised simulation of real-world cyber attacks on systems, networks, or apps to identify vulnerabilities before attackers do

NCSC Definition : “A method for gaining assurance in the security of an IT system by attempting to breach some or all of that system's security, using the same tools and techniques as an adversary might.”

Core purpose:

- Secure, not break
- Improve security by finding weaknesses

Why do it?

Most companies, governments, and universities now require regular pentests

Pentesting simulates **real-world cyberattacks**. It’s supposed to imitate attack methods that actual hackers will try. Because of this, it can be highly thorough and effective, but pentesters must stay updated on the latest hacking techniques to remain relevant

Pentesting vs. Other Security Testing

Vulnerability Assessment

- Surface-level analysis without actual exploitation
- Produces periodic risk reports, focuses on patching and prevention

Red & Blue teaming

- Expands on pentesting by simulating social engineering, phishing, and physical intrusion
- “red team” are hackers, “blue team” are defenders (they cover human resilience methods)
- Evaluates an organisation’s ability to detect, defend and respond from multi-vector threats

Types of Pentests

Type	Description	Example Scenario
Black Box	Tester has no prior knowledge - essentially simulating an external hacker	Student tries to hack into a University site with no account
White Box	Full insider knowledge and credentials provided. Simulates an attacker with inside access	You’re given access to source code, diagrams and system credentials for the university site
Grey Box	Partial knowledge / access. Target is shared. Privilege escalation is key	Tester has access as a staff member, however not all documents are present

Sometimes known as ‘No-knowledge’, ‘Partial-knowledge’ and ‘Full-knowledge’ pentests

Pentesting Methodology

- Reconnaissance
- Scanning / Enumeration
- Vulnerability Assessment
- Exploitation
- Reporting & Remediation

We already know how to do some of these things, we shall see later

Reconnaissance

Gathering as much information as possible about the target (company, website, network, application etc.)

Open Source Intelligence (OSINT)

Whois

Google dorks

Social Media

Scanning

Trying to identify live hosts, open ports, running services for potential points of weakness

Use tools (Nmap, Gobuster, Masscan, Nessus) to map networks, find live hosts, open ports, directories, services

Potentially find things like an unprotected web admin portal running on a non-standard port, or an exposed database port

Vulnerability Assessment & Exploitation

Focus on finding software flaws, like misconfigurations, vulnerable login forms and weak passwords

Use techniques like

- SQL Injection
- Cross-Site Scripting (XSS)
- privilege escalation

Tools like Nessus, OpenVAS, and SQLMap are excellent for this

Reporting

Compile, organise, and communicate findings and recommendations to stakeholders (people hiring you to do the pentest)

- What was found, how was it exploited and the impact
- Prioritise issues based on risk - critical, high, medium, low
- Remediation advice (crucially) - how to fix each issue

A Doctor wouldn’t be very helpful if they diagnosed you and then didn’t give any treatment options

Common Tools for Pentesters

We’ve already looked into some of these

- Nmap - networks scanning and port finding
- Wireshark - packet analyser
- Hashcat - password cracking
- Aircrack-ng - WiFi auditing and password cracking

Some frameworks we haven’t covered:

- OWASP ZAP (Check out OWASP Top 10)
- Metasploit
- Burp Suite
- John the Ripper (Advanced Hash Cracking)

Hardware like BadUSB, Flipper Zeros are purposefully built for stages of a pentest. Others like Raspberry Pis offer design features that are useful to pentesters

Social Engineering

Test not just tech, but people’s awareness. What red / blue teaming is good for.

Remember the police session? If you scanned the QR Code in the box they would lead you to a google search saying ‘Nice try but this is a red herring’. Most people probably wouldn’t think twice before scanning a QR Code!

Example from W3Schools:

> “Eve” rushes to reception, claiming an urgent job interview, hands over a USB to print a CV (but it’s actually carrying malware). The receptionist tries to help and infects the office PC

Pentesting W3Schools

Practical

Good referral tool, if you’re stuck or want some more information on pentesting:

Pentesting Fundamentals TryHackMe

TryHackMe room:

https://tryhackme.com/room/kenobi

You’ll need some knowledge from previous sessions (nmap and linux), do ask questions!

Burp Suite basics

https://portswigger.net/web-security

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

24th November: CompSoc collab for Hackathon

8th December: Lock Picking

Any Questions?

www.shefesh.com

Thanks for coming!

Links (for Harry)

https://tryhackme.com/room/pentestingfundamentals

https://en.wikipedia.org/wiki/Penetration_test#Tools

https://owasp.org/Top10/2025/0x00_2025-Introduction/

https://tryhackme.com/room/pentestingfundamentals

https://tryhackme.com/module/pentestingtool