# Ethical Student Hackers

Refresher Session

# 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 we are covering

- URL Manipulation & SQL Injections
- XSS
- OSINT
- Password Cracking
- Enumeration
- Residential Wifi
- Pen Testing
- Lockpicking

What I actually want to teach you:
How to approach hacking is more important than knowledge.

You can always teach yourself things
I want to teach/show you the ways you need to think :)

# URL Manipulation & SQL Injections

URL Manipulation:
Directly editing the parameters of a url query to your advantage.
Think about the login challenge you did for the freshers fair and GIAG!

SQL Injections:
Manipulates raw SQL statements to access other data in the database.
E.G. user‘OR1=1;--

# XSS

Cross Site Scripting:
Executing code via a website

Reflected - when information is bounced back to you, like error messages or search queries

Stored - code is stored on website, then executed later, think comments section, twitter tweets

Blind - code is sent through a form and executed later, think feedback forms to staff

# OSINT

OSINT:
Publicly Available Information

- Social media
- Reverse image searches
- Directory lookups
- Metadata

Requires creativity and analysis to find out information about people and companies

# Password Cracking

Password Cracking:
When you breach a database, you can access the password hashes

It is mathematically impossible (if the hash algo is perfect) to reverse the hash

You have to use brute force.

Tools:
Hashcat
John the ripper

# Enumeration

Enumeration:
Find out details about the target

Servers run services - you can scan the servers ports to find out what services are running (with nmap)

Map out the website - find hidden directories and files
(with gobuster)

Look for anything unusual - left-over passwords, usernames, comments revealing how internal systems work

# Residential Wifi

Residential Wifi:
Spoofing attack - set up a fake wifi network
Listen for the handshake when someone connects to the wifi
Take the username and hash
Crack the hash

This also brings in social engineering aspect (which we will cover more of this semester!)

Setting up as FREE_MCDONALDS_WIFI and sitting in a mcdonalds for a few hours is rather effective!

# Pen Testing

Pen Testing:

Codifying and standardising the hacking process.

Steps:
Reconnaissance
Scanning / Enumeration
Vulnerability Assessment
Exploitation
Reporting

# Lockpicking

Lock Picking:
Used to bypass physical security (i.e. doors and padlocks)

General idea is that the pins that keep the lock locked, are not perfectly identical.
This causes them to be lifted up and held in the open position in a particular order.
Once you find the order, you can open the lock.

# Practical Time!!!

# 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

# Inclusions Concerns

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

The week after that

And the week after that

And the week after that

And the week after that

# Any Questions?


www.shefesh.com

Thanks for coming!