Ethical Student Hackers

Give it a Go - Ethical Hacking

An Introduction to Hacking and Encryption

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.

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/conduct

Who Are We?

We are a society that aims to teach you all about hacking!

Ethical Hacking is a fun activity that tests your problem solving and is highly relevant today

Our society runs weekly sessions (Mondays 18:00 - 19:30, location varies)

Each week we cover a different topic with theory and practical

We formed in 2018 and have had people of many disciplines in the society! Diversity makes better hackers :)

Membership is £4 for a year and £7 for two

Visit https://shefesh.com and click “Join Us!”

Our Committee

Echo
President

Jason
Secretary

Josh
Publicity

Keshav
Inclusions Officer

Luca
Treasurer

Abdelrhman
General Member

Erik
Competitions

Interested in joining committee?

Keep an eye out! An EGM is coming soon

What *is* Hacking?

"The intellectual challenge of creatively overcoming the limitations of software systems or electronic hardware (mostly digital electronics), to achieve novel and clever outcomes"

- Gehring, Verna (2004). The Internet in Public Life

What *is* Hacking?

Hacking can be thought of as problem solving in a creative way.

Outside of Cybersecurity, you may have been to a Hackathon or spent hours watching videos of “life hacks”.

In this society we talk about Computer Hacking!

But Cybersecurity involves Human Hacking too (aka Social Engineering)...

Anyone with a ‘hacker’s brain’ will be good at Cybersecurity.

And anyone with the motivation can learn it!

Hackers come from all sorts of backgrounds - you do not have to be a tech expert.

Other Fields of Cybersecurity

Cyber jobs don't just involve Ethical Hacking

- Policy and Assurance
- Malware Analysis & Threat Intelligence
- Security Operations Centre (SOC) Analysts
- Cyber Incident Response Teams (CIRT)
- SIEM Building
- Physical Security Testing
- Social Engineering
- Education & Outreach
- Academic research (Cryptography, Controls)

But it's good to know the basics of Ethical Hacking to inform your wider knowledge - even in defence, you must know your enemy!

You could work for a standards agency, law enforcement, or anything in between...

Steps of a Penetration Test

Reconnaissance - this is where you identify and enumerate a target's network and services

- This may also include Open Source Intelligence gathering (OSINT)

Initial Access - where vulnerabilities are discovered and exploited

- This may include database access or Remote Code Execution (RCE)

Lateral Movement - this involves 'pivoting' across a network of machines to access valuable new targets

Privilege Escalation - this involves moving 'vertically' from a 'low-power' account to a higher one

Post-Exploitation - this may include steps such as persistence, data exfiltration, or denial of service

This is a rough guide, but a widely accepted model can be found at https://attack.mitre.org/

Recognising Common Encodings

There are loads of different encodings that you may come across, but we are only going through a few today being:

- Caesar Cipher: [Too insecure, doesn't really show up apart from examples]
  - A Caesar Cipher can be identified by only using letters
  - Example: Zhofrph wr VkhiHVK iurp wkh Frpplwwhh
- Base64 [Storing data in XML]
  - A Base64 encoding can be identified by using only alphanumeric characters plus "+" & "/". Where the end may be padded with "=" and the length of the text content is a multiple of 4.
  - Example: V2VsY29tZSB0byBTaGVmRVNIIGZyb20gdGhlIENvbW1pdHRlZSE=
- MD5 Hash [Used in file authentication]
  - A MD5 Hash can be identified by only using hexadecimal characters and being a length of 32 characters long.
  - Example: a69d525bab4445fefcd0c1463f777af6

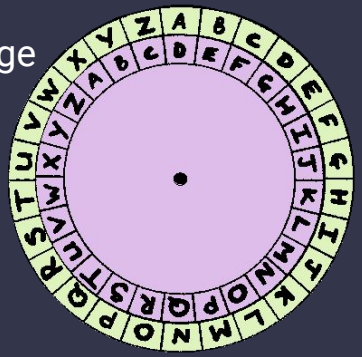
Caesar Cipher

One of the oldest encryption methods is named after the Roman Emperor “Julius Caesar”, where he created the Caesar Cipher which is basically just shifting all letters in the alphabet by 3.

The modern day version of this cipher can shift in any direction, by any amount (not multiples of 26).

This can be done with a wheel with 2 discs, but much easier is to use an online tool like dcode.

In this cipher, the “key” is the number of letters the message is shifted by. A key of 3 would be a shift of 3. Knowing the key can speed up decoding by hand, but with only 25 options, computers are very fast at brute forcing it.



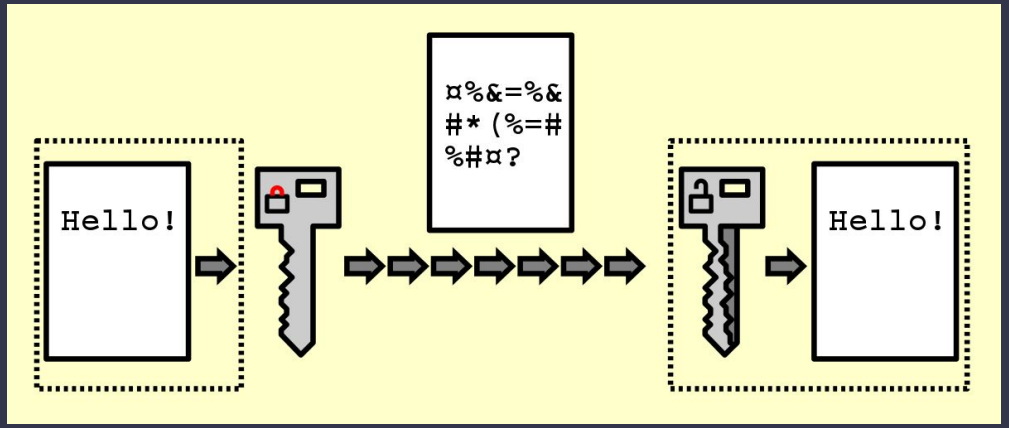
What is Encryption?

Encryption is a way of encoding messages in such a way that they can't be read by outsiders but also where the encoding can be reversed to return the original message.

There are two main types of encryption being:

- Symmetric encryption
- Asymmetric encryption

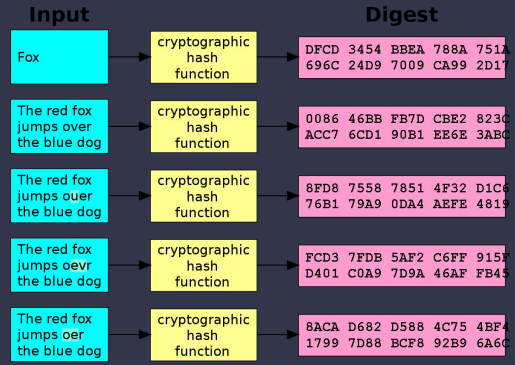
There is also another type of encoding that occurs called "Hashing", which returns a unique summary of the contents.



What is hashing? Tldr

- A hash function creates a digest (small summary) of an input
- It's useful for verifying that data has been transmitted correctly and not tampered with
- Key thing: ideally, there should be a one-to-one correspondence between inputs and outputs
  - but in the real world, *collisions* do sometimes occur

- A common use for hashing is verifying passwords
  - Websites don't actually store your password (this would be insecure!) - they store the digest
  - When you try to log in, they hash the password you enter and check if the digests match
  - A collision would mean that you could log in with the wrong password



Your turn

Identify whether the following messages are Caeser ciphertexts, MD5 hashes or base64-encoded data, and decode them.

1. Zhofrph wr VkhiHVK iurp wkh Frpplwwhh
2. TmV4dCB3ZWVrIHdlIGFyZSBkb2luZyB3ZWIgaGFja2luZywgdGFsa2luZyBhYm91dCBYU1MsIGNvb2tpZXMsIFNRTCBpbmplY3Rpb24=
3. 8306033ea4dcbee910d9b59d14e1cc2e
4.

For an extra challenge (if you have a laptop), can you encode/decode MD5 hashes from the terminal? We cover this in more detail in an upcoming password cracking session.

Inspecting a Webpage

Whistle stop tour of what you can do just with your browser

- View Source: Ctrl + U / Ctrl + Shift + C
  - Look for comments (<!-- ->)
  - Look for URLs in Forms (action=”/url”)
- View Network Traffic (Network Tab)
- View Cookies (Storage Tab)
- View Javascript (look for passwords, interesting functions)
- Look for hidden pages in /robots.txt

There’s plenty more possible with specialised tools, such as editing traffic on the fly and automatically discovering hidden webpages!

Web 101 - Bypassing Login Forms

If you wanted to gain unauthorised access, how might you do it?

- Look for common or weak passwords
- Phishing
- Install a keylogger
- Go via an adjacent connected system that you compromised

Or… you might break the login form itself!

- SQL Injection
- Login flaws
- Passwords accidentally in the page code…

We'll explain this all in more detail on Monday! But this should give you a flavour of what is possible…

Now… Let’s do some Hacking

http://18.133.182.24:5000/

Visit this site in your browser

Can you find the hidden challenge?

Slides: shefesh.com

https://shefesh.com/assets/images/1.jpg

Where to Learn More?

Our sessions! Join at https://shefesh.com and click ‘Join Us’

Fundamental Skills series: https://shefesh.com/wiki/fundamental-skills

Resources page: https://shefesh.com/wiki/resources

Try Hack Me: https://tryhackme.com (perfect for beginners)

Hack the Box: https://hackthebox.eu (more advanced, with less guidance, but more engaging)

Follow us on Twitter, Facebook, and Linkedin - and join our discord!

ethicalhackers@sheffield.ac.uk

Upcoming Sessions

What's up next?

www.shefesh.com/sessions

Activity Fair - 23/09/24 (Tomorrow!)

First Session! More Web Hacking:
30/09/24 18:00 - 19:30
(Diamond workroom 3)

Introduction to Linux:
07/10/24 18:00 - 19:30
(Diamond workroom 3)

Any Questions?

www.shefesh.com

Thanks for coming!