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/downloads/SESH%20Code%20of%20Conduct.pdf

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 19:00 - 20:30, 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

Mac
President
MSc Cybersecurity & AI

Seb
Secretary
MComp Computer Science with a Year in Industry

James
Treasurer
Computer Science

Kimberley
Inclusions Officer
Computer Systems Engineering

Interested in joining committee?

We have space for a General Member and a Publicity Officer to help us create sessions

You don’t have to do a computing-related subject to join the society or committee - we’ve had mathematicians, physicists, and biologists!

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/

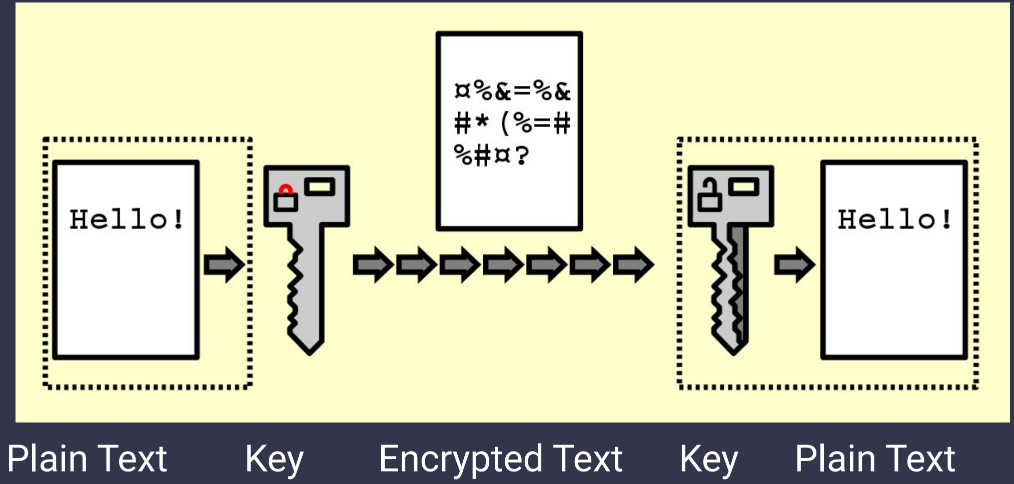
What is Encryption?

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

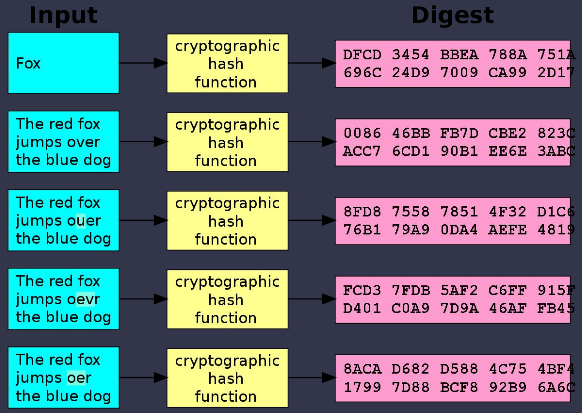
There is also another type of encoding that occurs called “Hashing”, which returns a unique summary of the contents.



What is hashing? Tldr

Hashing in short terms is creating a digest (small summary) of an input, a lot of data is usually lost and this only really used for verification purposes, there are a large variety of hashing algorithms. The key thing however is trying to make them unique where one input corresponds to one hash.

They are typically used with passwords meaning website hosts don't actually store your password but they store the summary and when you log in they summarise what you typed into the password box and check if the summaries matched. If a hash is too small, multiple inputs could easily correspond to a single hash.


Input
Digest
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

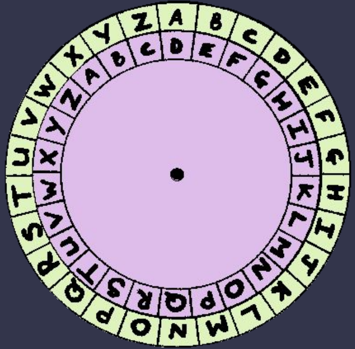
Caesar Cipher

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.

For practical purposes today, we have a small activity for you all where you can create encrypted messages and speak to each other using our home-made caesar cipher wheels, where you can rotate the discs by a specified number and tell the person next to you, where you can both receive and send messages.

We also have paper available so you can write down and encode/decode manually.

If we don’t have enough cipher wheels, you can use the website dcode.fr to encode/decode for you.



Bonus Activity

If you finish early have a go at the caesar cipher and substitution cipher in the worksheet below:

- https://www.cs.ox.ac.uk/stephen.drape/materials/secret.pdf

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

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://3.8.23.223:5000/

Visit this site in your browser

How far can you get?

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!

SHEFFIELD ETHICAL STUDENT HACKERS

Upcoming Sessions

What’s up next?

www.shefesh.com/sessions

Intro to Hacking and Web-Hacking - 26th September

Introduction to Linux and Bash - 3rd October

Introduction to Automation with Python - 10th October (TBC)

We will also have guest talks, operating system security, and more!

Any Questions?

www.shefesh.com

Thanks for coming!