


- **Alan Mills**
- **Lecturer in Cyber Security**
- **Alan.Mills@uwe.ac.uk**
- **2<sup>nd</sup> March 2022**

# ACE CSE TRAINING THE TEACHERS

# Introduction

- Alan Mills - Alan.Mills@uwe.ac.uk



**Position:** Lecturer

**Department:** FET - Computer Science and Creative Technologies

# Introduction

# “Hacking”

- “Hacking” has become a catch all word – Similar to cyber
- A hack was essentially a change or fix that would modify the original function
  - This doesn't have to be malicious
- Now the term is something we associate with someone breaking or mis-using functionality
- If someone brute forces or guesses our password was it really “hacking”?



HACKERS(1995)

# “Hacking”

- This can also be thought of as offensive cyber security
  - Penetration testers
  - Ethical hackers
- On the flip side we have defensive cyber security
  - Security Operations Centres
  - Analysts
- Offensive security is concerned with trying to see what can be “hacked”
- Defensive security is concerned with trying to stop things being “hacked”

# “Hacking”

- The term isn't unique to cyber security though
- A “Hackathon” for example could be an competition to come up with a solution or idea that might solve an existing problem for example
- This is normally aimed at coding a solution but not always

# Capture The Flags (CTFs)

- CTFs are a way for people to practice their cyber security skills in a safe and legal manner
- Often this are built and designed around offensive security scenarios and will involve purposefully insecure or flawed systems
- Defensive security scenarios do exist – These might involve looking through logs or event data
- In either case the goal is to “capture” the flag – Normally a unique value that is hidden somewhere

# Capture The Flags (CTFs) - Examples

- Offensive security scenario
- We are provided with an IP address and told there are X number of flags
- We scan the IP address, find a service using default credentials
- Once we are in we find flag 1 in the default path
- From there we might need to look around, change our user, exploit more services etc
- The ultimate goal of these scenarios tends to be getting root access – The user with the highest privileges



# Capture The Flags (CTFs) - Examples

- Defensive security scenario
- We are provided with logs and told there are X number of flags or questions to answer
- We look through the logs and identify key information
  - Attacking / victim machine
  - Type of attack
  - Timelines
  - Etc
- The ultimate goal tends to be that by the end we can provide a comprehensive overview of what occurred

# Capture The Flags (CTFs)

- By utilising CTFs people can hone their skills and become familiar with new concepts and techniques
- They can be targeted at a range of audiences from complete beginners through to experienced professionals
- There are also multiple platforms for people to choose from:
  - [TryHackMe](#)
  - [OverTheWire](#)
  - [HackTheBox](#)
  - [ImmersiveLabs](#)

# Capture The Flags (CTFs)

- Each platform will have it's own forums (and sub-reddits)
- There are also plenty of other forums and websites dedicated to providing help, hints, tips and guides on various challenges
- This is true of “hacking” as a sub-culture
- However not everyone who uses these forums is entirely trust worthy

# Online Resources

- It is not un-common for people to abuse legitimate forums to ask for illegitimate help or advice

The screenshot shows a forum profile for 'digininja' and a post. The profile includes a robot avatar, a 'Global Moderators' badge, and statistics: 3.9k posts, Gender: Male, Location: Sheffield, UK, and Interests: Hacking, Coding, Climbing. The post, dated April 3, 2019, is a quote from ToxicPhoenix asking for alternative forums for hacking/modding. The forum's response states that illegal requests are not allowed and suggests leaving the forum if the policy is disliked.

**digininja** Posted April 3, 2019

Global Moderators  
3.9k  
Gender: Male  
Location: Sheffield, UK  
Interests: Hacking, Coding, Climbing

On 3/29/2019 at 7:59 PM, ToxicPhoenix said:

I'm looking for other forums, that are about hacking/modding etc...

I need other forums because there is someone called "digininja" that annoys me. Every time i write something he warns me... I don't even know what for (not detailed enough.

You keep asking for people to do illegal things for you on online games, I've explained this in at least a couple of PMs and in the warnings.

If you don't like our policy of not allowing illegal stuff on this forum, feel free to go elsewhere.

+ Quote

Hak5 forum

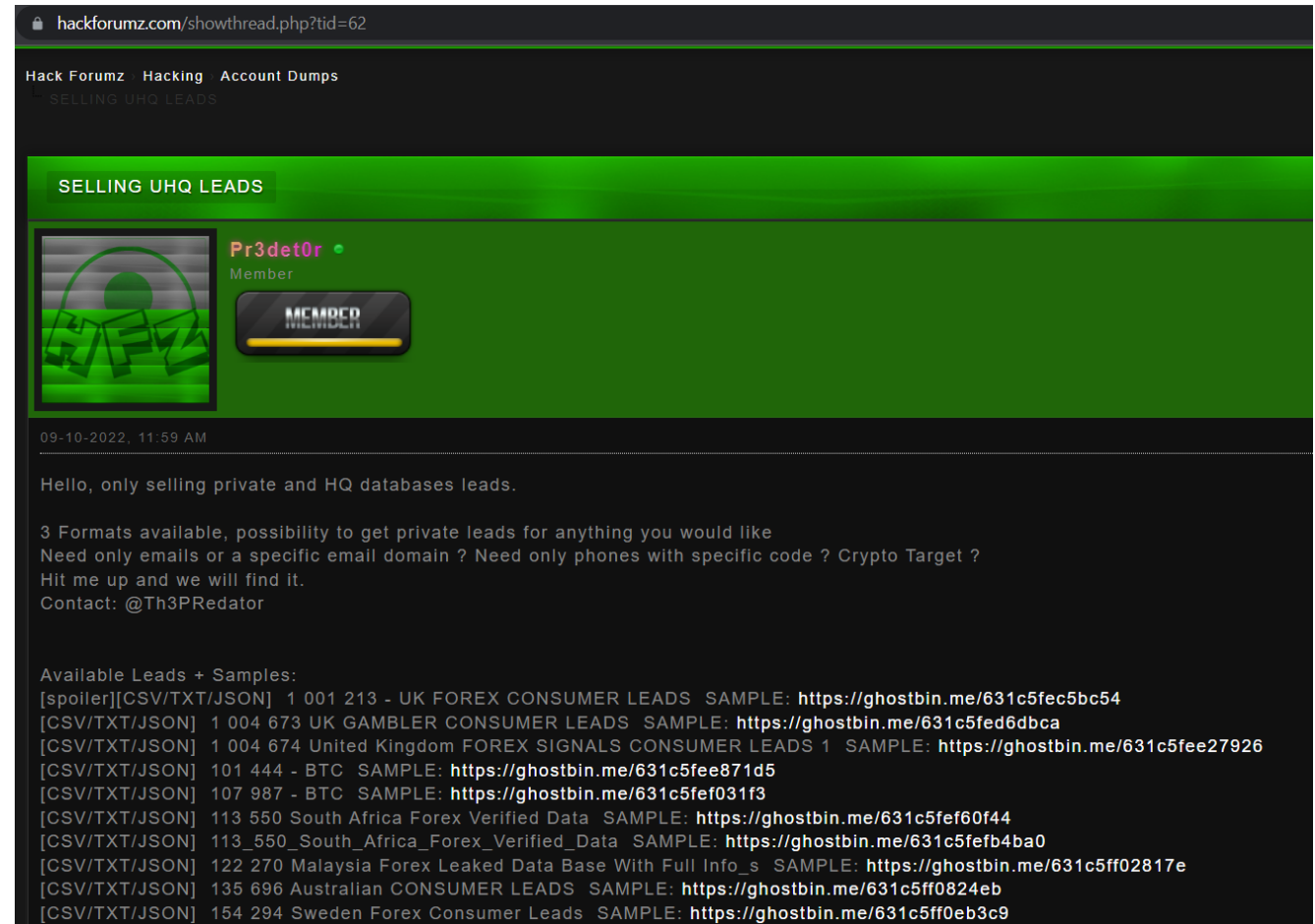
# Online Resources



YouTube – Live Music Stream (Crypto Music for Coding, Programming, Studying — Hacker Time! Chillstep Radio)

# Online Resources

- Entire forums and websites have sprung up around this illegal side of cyber security
- Links like these are more than likely going to contain malware as well as / instead of the promised content



Hackforumz – Thread around selling account details / dumps

# Online Resources – Deep Web

- Then of course there is [the deep web](#)
- The existence (and content) of the deep web has become less and less of a mystery
- As such those who are inclined to look for the sort of content then can find on the deep web will do so
- The use of TOR or the deep web itself isn't illegal – But some of the activity that takes place on there is

# Online Resources

- Whether it is using the surface web or the deep web people can often find illegal hacking content and advice
- Remember – Those people who are giving out this advice or resources are purportedly providing resources which are or can be used illegally
- They are not trust worthy
  - The classic “Alt + F4” fix for windows



# Online Resources

- Two prime examples of this occurred within the last 3 months
- In one instance people looking for cheats and game hacks were being given links to download malware (Sept 22)
- In another people looking to install TOR browser (illegal in China) were being given an installer that was loaded with spyware (Oct 22)

# Online Resources



[Teenage cybercrime: Help your child make the right #CyberChoices - YouTube](#)

# Online Resources

- Of course just as bad might be if the advice or links are as promised
- Cyber crime is not limited to nation states or “professionals” with years of experience
- The members of the [Lapsus\\$](#) group were teenagers here in the UK
- They carried out a number of high profile attacks and since then members 7 have been arrested (aged 16-21)
- The identity of these members were leaked by other members of an online community they annoyed

# Online Resources – Bug Bounties

- If CTFs just aren't enough then bug bounties provide a way for those who are keen to practice and earn
- A bug bounty is a reward that a company gives someone who ethically hacks and discloses a vulnerability in their product
- Often this comes with a scope and details around what is offered

**In Scope Targets** ✓ In scope

<span style="border: 1px solid green; padding: 2px;">P4</span> \$300	<span style="border: 1px solid orange; padding: 2px;">P3</span> \$600	<span style="border: 1px solid orange; padding: 2px;">P2</span> \$6000	<span style="border: 1px solid red; padding: 2px;">P1</span> \$30000	<span style="border: 1px solid gray; padding: 2px;">★</span> \$1000000
--	---	--	--	--

- <Your own 1Password subdomain --> https://<your account domain>.1password.com/
 

Moment.js
Lodash
- <Account (Business, Family) signup page --> https://start.1password.com
 

Moment.js
Lodash
- <White Box Test team --> https://bugcrowd-test.1password.com

**Out of scope targets** ✗ Out of scope

- \*.agilebits.com
 

Website Testing

1Password – Bug Bounty Blog and Scope

# Online Resources – Bug Bounties

- While not what could be considered a typical career path some people earn significant sums of money through bug bounties
- From a BBC news article looking at bug bounties (with a focus on [HackerOne](#)):
  - A record £28 million was earned via bug bounties in 2020
  - The UK's top earner made £370,000 (that year)
  - “[...] for starting security researchers or students, then these commercial bug bounty platforms are great as they offer a lot of protection, resources and are a perfect place to start.”

# SUMMARY

# Q&A

# Links

- <https://thehackernews.com/2022/09/researchers-warn-of-self-spreading.html>
- <https://thehackernews.com/2022/10/popular-youtube-channel-caught.html>
- <https://krebsonsecurity.com/2022/03/a-closer-look-at-the-lapsus-data-extortion-group/>
- <https://www.bugcrowd.com/bug-bounty-list/>
- <https://www.bbc.co.uk/news/technology-56350362>