# Welcome to the CoGrammar

A Toolbox For Ethical Hacking

The session will start shortly...

Questions? Drop them in the chat. We'll have dedicated moderators answering questions.



#### **Cyber Security Session Housekeeping**

- The use of disrespectful language is prohibited in the questions, this is a supportive, learning environment for all - please engage accordingly.
   (Fundamental British Values: Mutual Respect and Tolerance)
- No question is daft or silly ask them!
- There are **Q&A sessions** midway and at the end of the session, should you wish to ask any follow-up questions.
- If you have any questions outside of this lecture, or that are not answered during this lecture, please do submit these for upcoming Academic Sessions. You can submit these questions here: <u>Questions</u>



#### Cyber Security Session Housekeeping cont.

- For all non-academic questions, please submit a query:
  www.hyperiondev.com/support
- We would love your feedback on lectures: <u>Feedback on Lectures</u>
- Find all the lecture content in you <u>Lecture Backpack</u> on GitHub.
- If you are hearing impaired, please kindly use your computer's function through Google chrome to enable captions.

#### Safeguarding & Welfare

We are committed to all our students and staff feeling safe and happy; we want to make sure there is always someone you can turn to if you are worried about anything.

If you are feeling upset or unsafe, are worried about a friend, student or family member. or you feel like something isn't right, speak to our safeguarding team:



Ian Wyles Designated Safeguarding Lead



Simone Botes



Nurhaan Snyman



Rafig Manan

safeguarding concern



Scan to report a

or email the Designated Safeguarding Lead: Ian Wyles safeguarding@hyperiondev.com



Ronald Munodawafa





#### Stay Safe Series:

Mastering Online Safety One week at a Time

While the digital world can be a wonderful place to make education and learning accessible to all, it is unfortunately also a space where harmful threats like online radicalization, extremist propaganda, phishing scams, online blackmail and hackers can flourish.

As a component of this BootCamp the *Stay Safe Series* will guide you through essential measures in order to protect yourself & your community from online dangers, whether they target your privacy, personal information or even attempt to manipulate your beliefs.



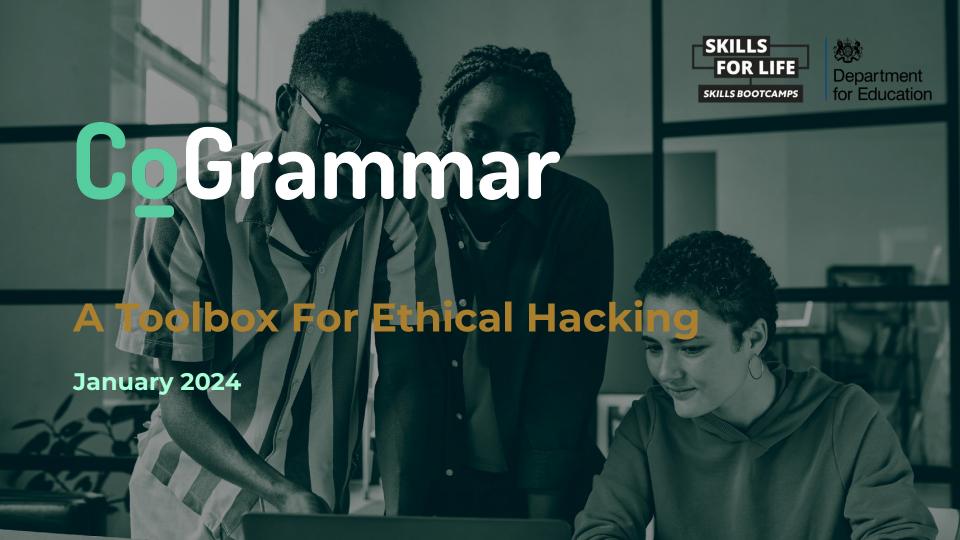
#### **Pause Before You Post:**

#### **Managing Your Digital Presence**

- Impact on Reputation.
- Permanent Record.
- Privacy Concerns.
- Miscommunication.
- Influence on Others.
- Professional Implications.
- Mental Well-being.







#### Learning Objectives & Outcomes

- Demonstrate the use of common penetration testing tools, such as Nmap and Metasploit, in identifying vulnerabilities.
- Analyze the results of a penetration test to identify critical vulnerabilities and their potential impact on system security.
- Perform a full penetration test, from reconnaissance through to reporting, on a test system or sandbox environment.



#### Polls

Please have a look at the poll notification and select an option.

What is a popular tool for vulnerability scanning?

- A. Metasploit
- B. Nessus
- C. John the Ripper
- D. OpenVAS



#### Polls

Please have a look at the poll notification and select an option.

Which tool is commonly used for web application security testing?

- A. Burp Suite
- B. Metasploit
- C. nmap
- D. Nessus



### Verbal Questioning







#### **Tutorial**

- Performing a test exploitation in TryHackMe.
  - a. <u>Tryhackme</u>
- For this tutorial, we'll use an external environment to perform a test exploitation. We'll use the free version of the platform try hackme to create a test server which will act as out target and utilise their kali linux host environment.



## Questions and Answers





Thank you for attending







