Welcome to the CoGrammar

Penetration Testing

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: **Questions**

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: **Feedback on Lectures**
- Find all the lecture **content** in you **Lecture Backpack** 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

Rafiq Manan

Ronald Munodawafa

Tevin Pitts

Scan to report a safeguarding concern

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

CoGrammar HyperionDev

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.

Penetration Testing

December 2024

Learning Objectives & Outcomes

- Explain the penetration testing methodology, including reconnaissance, exploitation, and reporting phases.
- 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.
- Assess the effectiveness of penetration testing strategies and propose actionable improvements for securing systems.

Polls

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

What do you think penetration testing is primarily used for?

A) Fixing hardware issues

B) Checking a system's security against attacks

C) Speeding up software performance

D) Training employees to use software

Verbal Questioning

Why might a company want to test their system for vulnerabilities?

Introduction to Penetration Testing

- **Definition:** Penetration Testing (Pentesting) is a simulated cyberattack on a system to evaluate its security.
- **Objective:** Identify vulnerabilities before attackers exploit them.

Key Benefits:

- Enhance system security.
- Comply with security regulations.
- Protect sensitive data and reputation.

Types of Penetration Testing

Black Box Testing:

- Tester has no prior knowledge of the system.
- Simulates an external attack.

White Box Testing:

- Full knowledge of the system is provided.
- Comprehensive vulnerability analysis.

Gray Box Testing:

- Limited information about the system is provided.
- Simulates an insider threat.

Penetration Testing Methodology

1. **Planning and Reconnaissance (Information Gathering):**
   - Understand the scope and objectives.
   - Gather information about the target.

2. **Scanning and Enumeration:**
   - Identify open ports, services, and vulnerabilities.

3. **Exploitation:**
   - Attempt to exploit vulnerabilities to gain unauthorized access.

Penetration Testing Methodology

4. Remediation:

- Propose solutions to the vulnerabilities discovered in the network system.

5. Maintain access:

- Maintain access to the network by either:
  a. Adding yourself as a user
  b. Adding a scheduled task that includes you running an exploit on the victim's machine

Tools for Penetration Testing

- **Network Scanning:** Nmap, Nessus
- **Web Application Testing:** Burp Suite, OWASP ZAP
- **Exploitation:** Metasploit, SQLmap
- **Password Cracking:** John the Ripper, Hydra
- **Wireless Testing:** Aircrack-ng, Wireshark

Challenges in Penetration Testing

- **Evolving Threat Landscape:** Constant emergence of new vulnerabilities.
- **Complex Environments:** Multi-layered systems and networks.
- **False Positives:** Misinterpreted results can waste time and resources.
- **Legal and Ethical Issues:** Testing without clear authorization can lead to liabilities.

Best Practices for Penetration Testing

- **Define Scope Clearly:** Avoid unauthorized areas.
- **Get Authorization:** Ensure written consent.
- **Use Skilled Professionals:** Engage certified pentesters (e.g., CEH, OSCP).
- **Regular Testing:** Conduct periodic tests to stay ahead of threats.
- **Actionable Reporting:** Provide clear, prioritized remediation steps.

Practical Example:

- For today's practical example, we're going to conduct some scanning and information gathering using tools like nmap and dirbuster.
- Afterwards we're also going to attempt to perform a common exploitation on a known server using metaspoilt. (The vulnerability has a patch so chances of it working on the target server are low)

Polls

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

Which type of penetration testing involves testing without prior knowledge of the system?

- A) White Box Testing
- B) Gray Box Testing
- C) Black Box Testing
- D) External Testing

Polls

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

Which of the following tools is primarily used for network scanning?

A) Burp Suite

B) Metasploit

C) Nmap

D) Aircrack-ng

Questions and Answers

CoGrammar

Thank you for attending

SKILLS FOR LIFE
SKILLS BOOTCAMPS

Department for Education

CoGrammar