CoGrammar

Cyber Security

SKILLS FOR LIFE
SKILLS BOOTCAMPS

Department for Education

Tech Talk Sessions Housekeeping

- The use of disrespectful language is prohibited in the questions, this is a supportive, learning environment for all - please engage accordingly. **(FBV: Mutual Respect.)**
- 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. Moderators are going to be answering questions as the session progresses as well.
- If you have any questions outside of this lecture, or that are not answered during this lecture, please do submit these for upcoming Open Classes. You can submit these questions here:
  SE Open Class Questions or DS Open Class Questions

Tech Talk Sessions Housekeeping cont.

- For all **non-academic questions**, please submit a query: **www.hyperiondev.com/support**
- Report a **safeguarding** incident: **www.hyperiondev.com/safeguardreporting**
- We would love your **feedback** on lectures: **Feedback on Lectures**

Progression Criteria

✅ **Criterion 1: Initial Requirements**

- Complete 15 hours of Guided Learning Hours and the first four tasks within two weeks.

✅ **Criterion 2: Mid-Course Progress**

- Software Engineering: Finish 14 tasks by week 8.
- Data Science: Finish 13 tasks by week 8.

✅ **Criterion 3: Post-Course Progress**

- Complete all mandatory tasks by 24th March 2024.
- Record an Invitation to Interview within 4 weeks of course completion, or by 30th March 2024.
- Achieve 112 GLH by 24th March 2024.

✅ **Criterion 4: Employability**

- Record a Final Job Outcome within 12 weeks of graduation, or by 23rd September 2024.

Lecture Objectives

1. Define penetration testing and why it's important.
2. Investigate the steps/methodology(incl types of tests).
3. Explore different tools that are at your disposal and potential certification paths.

How is this relevant?

- Cybersecurity is essential to Data Science and Software Engineering because it protects sensitive data and maintains system integrity. In Data Science, where large volumes of data are processed and analyzed, cybersecurity measures are essential to protect against data breaches, unauthorized access, and the compromise of valuable insights.

- Similarly, in Software Engineering the development of software that is both secure and robust is crucial. Security considerations are integrated into the software development lifecycle to identify and mitigate potential vulnerabilities.

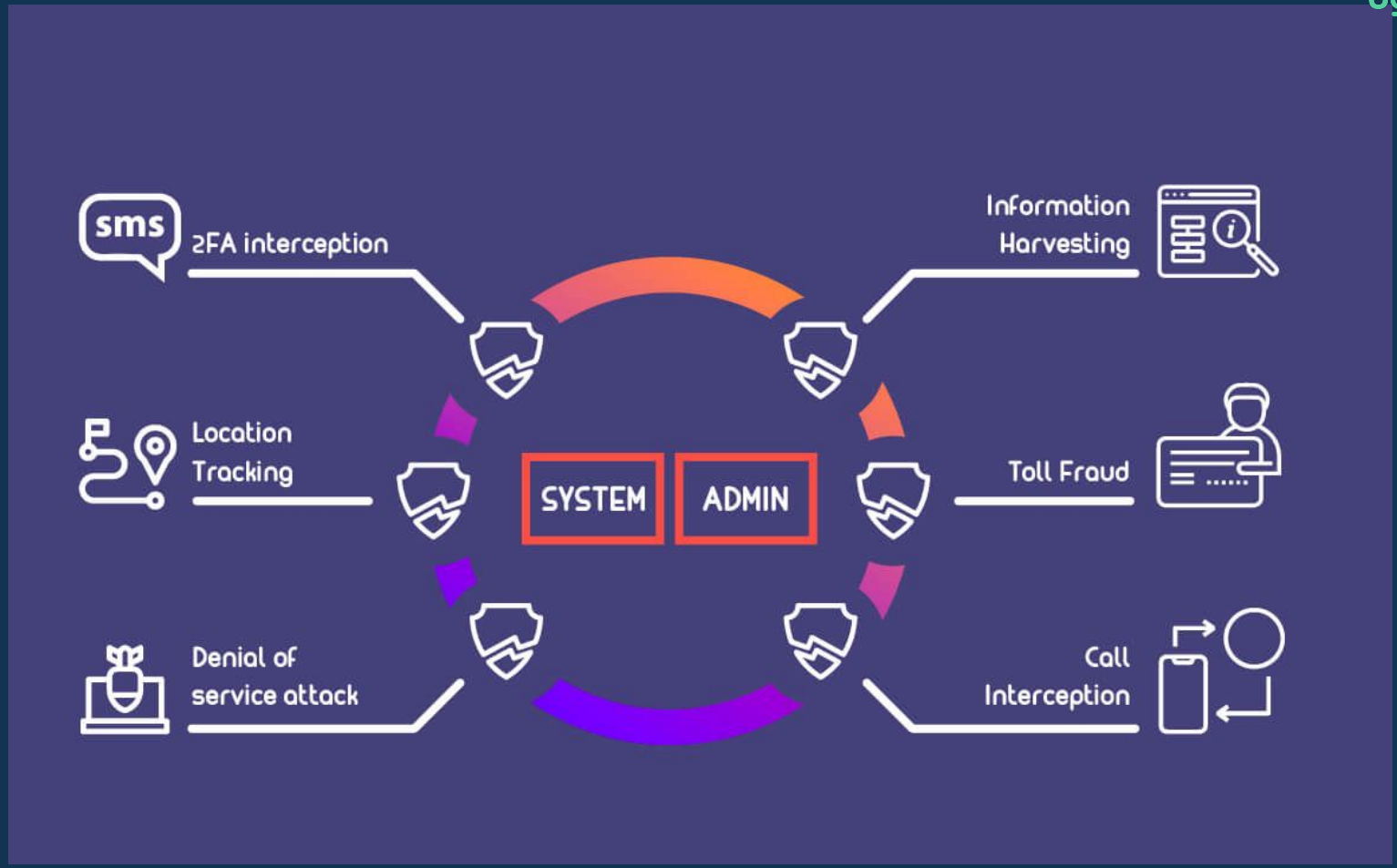
Why Is It Important?

- Enhancing Security: Organizations can strengthen the general security of their systems by using penetration testing to proactively identify and fix vulnerabilities before they are used by malicious attackers.

- Compliance Requirements: As part of their security compliance procedures, many industries and regulatory standards require regular penetration testing.

- Risk reduction: Penetration testing assists in reducing the risk of data breaches, unauthorized access, and potential monetary losses by locating and addressing vulnerabilities.

- Business continuity: Penetration testing identifies vulnerabilities that could result in service interruptions, thereby assisting in ensuring the uninterrupted operation of critical systems.


sms
2FA interception
Location
Tracking
Denial of
service attack
Information
Harvesting
Toll Fraud
Call
Interception
SYSTEM
ADMIN

What Is The Procedure?

- Prepare for the assessment. During this stage, gather pertinent data, get management approval, and lay out the test's steps.

- Create plan. Determine the equipment required to assess the testing candidate's condition. This entails assessing the security measures put in place and identifying any potential vulnerabilities or other access points.

- Assemble Team. To conduct the test, gather the necessary pen testers. The use of internal and external experts may be necessary.

- Determine the goal. Decide on the targeted systems and data.

- Conduct reporting and data analysis. Look over the information gathered during the pen test, analyze it, and decide what needs to be fixed. Create a report for the company management that includes a summary of the test results, the vulnerabilities that were found and exploited, and recommendations for potentially fixing them.


EXTERNAL
Test your internet facing systems using the same techniques as a malicious attacker
INTERNAL
Test your internal systems to eliminate threats that a malicious insider could leverage
WEB APP
Find hidden security risks that tools can't find in your custom web applications
WIRELESS
Discover security weaknesses in your wireless networks before they expose your data beyond the physical perimeter
YOU ARE HERE
(and so are we)
MOBILE
Uncover security vulnerabilities in iOS and Android custom-built software
IoT
Embedded systems often contain hidden security threats; Raxis will find them for you
API
Raxis programmers will test every facet of your API to find hidden security vulnerabilities
SCADA
Often using different techniques than IoT, Raxis has the experience to find security gaps in Industrial Control Systems

Types Of Penetration Tests

- Black box testing: Mimics the manner in which a skilled threat actor would carry out a hack. It begins with no prior knowledge or comprehension of the target's technological foundation or security features. This test aims to quickly locate vulnerabilities that are simple to exploit.

- Gray box testing: Pen-testers frequently have some familiarity with the systems and security precautions of the target. A gray box test aims to uncover information about vulnerabilities that can be exploited more thoroughly than in black box analyses.

- White box testing: The hacker performing this pen test is assumed to be well-versed in every facet of an organization's technological and security infrastructure. The most seasoned pen testing specialists are typically white box testers. They are tasked with finding even the smallest security infrastructure flaws. White box testers can work with system designers and engineers to enhance security within an organization.

More On Types

External Test: Websites, apps, email, and DNS are among the information assets that are attacked in an effort to extract data, conduct transactions, and engage in other activities. Finding vulnerabilities through external attack sources is the aim.

Internal Test: An internal attack aims to demonstrate the potential harm that could be caused if an attacker infiltrates the target system already. This includes insiders who are malicious. Employees who are more likely to fall for social engineering or phishing scams may be found with careful screening.

Blind Test: In this situation, the tester is permitted to obtain publicly available information about the target but has no inside information about the firm or its security resources. By contrast, the target company knows about the attack, including when and where it will occur, and can prepare accordingly. Testers must use all their skills to penetrate the target's defenses.

Double-blind Test: In this test, neither attacker nor target know in advance about the pen test. Testers must, therefore, rely on skills and available tools to achieve success. For the tester, success is penetrating the target's defenses. For the target company, success is preventing the attacker from penetrating its perimeter and defenses.

Common PenTesting Tools

CoGrammar

Metasploit: An open-source framework for exploiting vulnerabilities, with an extensive collection of exploits, payloads, and auxiliary tools.

Nessus: A widely used vulnerability scanner that identifies security weaknesses across various systems and applications.

Burp Suite: A suite of web application testing tools for discovering and exploiting web vulnerabilities.

Wireshark: A network protocol analyzer used for capturing and analyzing network traffic to identify potential security issues.

Hashcat: A powerful password cracking tool that can assist in identifying weak passwords and improving overall password security.

Ethics In Pen-Testing

CoGrammar

1. In keeping with British Values, the significance of honesty, competence, and adherence to the law still applies when conducting penetration testing.

2. Protecting people and organizations by using hacking techniques in an ethical and responsible manner is what Penetration was designed for.

3. Your approach to penetration testing should that with a strong ethical foundation and respect for their privacy and individual rights.

Ethical Hacking Certification:

- **Certified Ethical Hacker (CEH)**
- **Offensive Security Certified Professional (OSCP)**
- **CompTIA PenTest+**
- **GIAC Penetration Tester (GPEN)**

A professional's knowledge and abilities in the field are validated by certification, which also shows that person is committed to using hacking techniques that are morally and responsibly.

Summary

Executive Summary

★ Outlines the test's objectives, scope, expected outcomes, and people who requested it.

Methodology

★ Outlines the general types of tests and testers to be used in the test, such as external tests, black box tests, and in-house testers.

Tools

★ Describes the software tools and non-technological techniques (such as social engineering) required to produce the test's results.

Summary

Technical Approach

★ Simply explains the test's structure and technical approach.

Attack narrative

★ Outlines the actions taken throughout the test, from the beginning to the end, and includes the outcomes of each action.

Results

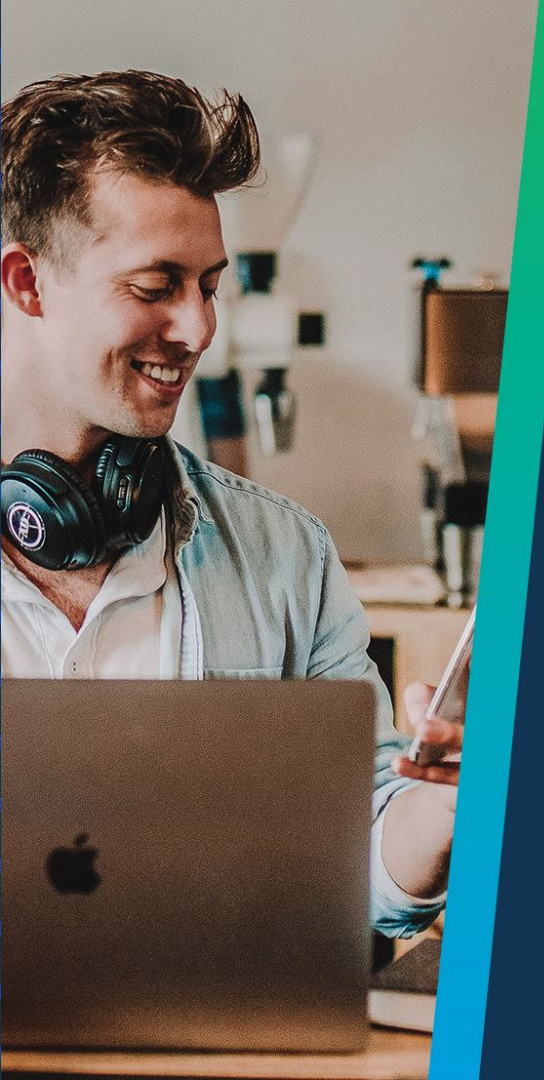
★ Conclusions and suggested next steps are outlined in the results section. It offers practical guidance on how to get the desired outcomes.

Further Learning

- Open Source Tools
- Additional Tools
- Job Description Template
- Blueprint
- Data Science Article
- Software Engineering Article
- News Article

Questions and Answers

Questions around CyberSecurity



CoGrammar

Thank you for joining us

1. Take regular breaks
2. Stay hydrated
3. Avoid prolonged screen time
4. Practice good posture
5. Get regular exercise

"With great power comes great responsibility"