Penetration Testing

HyperionDev

Lecture – Housekeeping

- The use of disrespectful language is prohibited in the questions, this is a supportive, learning environment - please engage accordingly.
- 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.
- You can also submit questions here: hyperiondev.com/sbc4-cs-questions
- For all non-academic questions, please submit a query: www.hyperiondev.com/support
- Report a safeguarding incident: hyperiondev.com/safeguardreporting
- We would love your feedback on lectures: https://hyperionde.wufoo.com/forms/zsgv4m40ui4i0g/

Previously:

- What Ethical Hacking is and why it is important
- Explored the differences between Ethical and Malicious Hackers
- Discovered Ethical hacking phases, techniques and Best Practices

Objectives

- What Penetration Testing is
- The Importance of Penetration Testing
- Steps/Methodology
- Types of Pen Tests
- Tools


strike
binary
target
employee
protected
protection
bugs
construction
transfer
hacker
PENTESTING
bank
memory
wifi error
protection
automated
withdrawal
error
all-moving
briefcase
hacker
shutterstock.com · 1690813600

What is Penetration Testing?

- A proactive and approved security assessment technique called, also referred to as pen testing, simulates actual attacks to find vulnerabilities and evaluate the security posture of computer systems, networks, or applications.

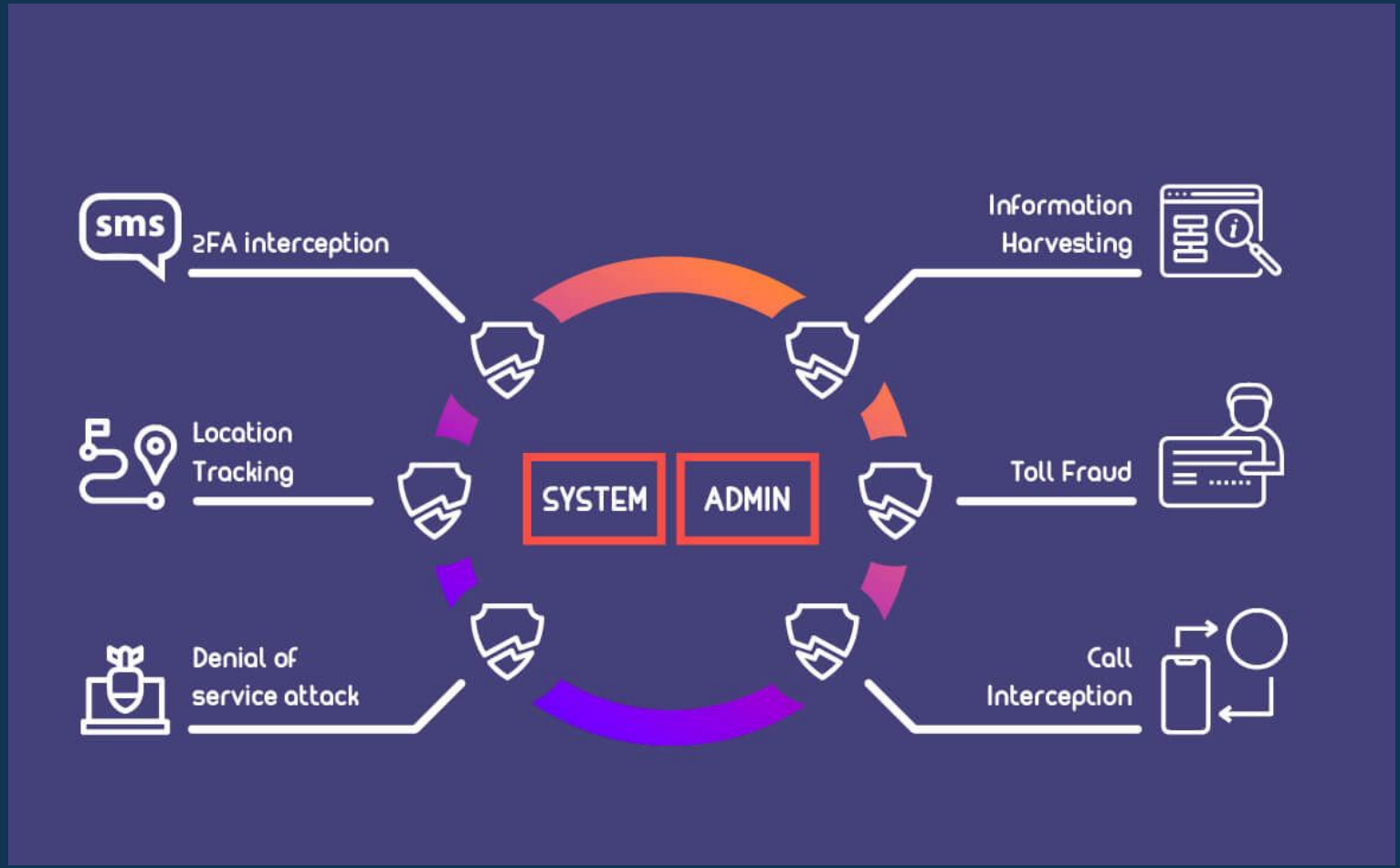
Why is it Important?

- 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

Pentesting Steps

- 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
API
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.

Questions and Answers

Common PenTesting Tools

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 PenTesting

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.

Wrapping Up (Report)

- Executive Summary: Outlines the test's objectives, scope, expected outcomes, and people who requested it.
- Statement of Objectives: The test's overall objectives are described in the statement of objectives, such as to identify external threats and vulnerabilities and suggest countermeasures.
- 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.
- 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.

Next up

- Recap on Vulnerabilities, Threat Vectors and Ethical Hacking

Questions and Answers

Hyperiondev

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"