Cyber Security
Bootcamp

Hyperiondev

Penetration Testing & Ethical Hacking

Lecture - Housekeeping

- ❏ The use of disrespectful language is prohibited in the questions, this is a supportive, learning environment for all - please engage accordingly.
- ❏ No question is daft or silly - ask them!
- ❏ There are Q/A sessions at the end of the session, should you wish to ask any follow-up questions.
- ❏ For all non-academic questions, please submit a query: www.hyperiondev.com/support
- ❏ Report a safeguarding incident: http://hyperiondev.com/safeguardreporting

Objective s

1. Define penetration testing and explain its purpose in cybersecurity.

2. Describe the importance of penetration testing in identifying and mitigating security vulnerabilities.

3. Identify and differentiate between various types of penetration tests, such as black-box, white-box, and gray-box testing.

4. List commonly used penetration testing tools and demonstrate their basic functionality in a simulated environment.

Previously:

Defined SQL as the language used to interact with RDBMS.

Additionally we demonstrated how application that do not make use of input validation and parameterized queries are susceptible to SQL injections

Penetration Testing

shutterstock.com · 1690813600

What is PenTesting?

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.

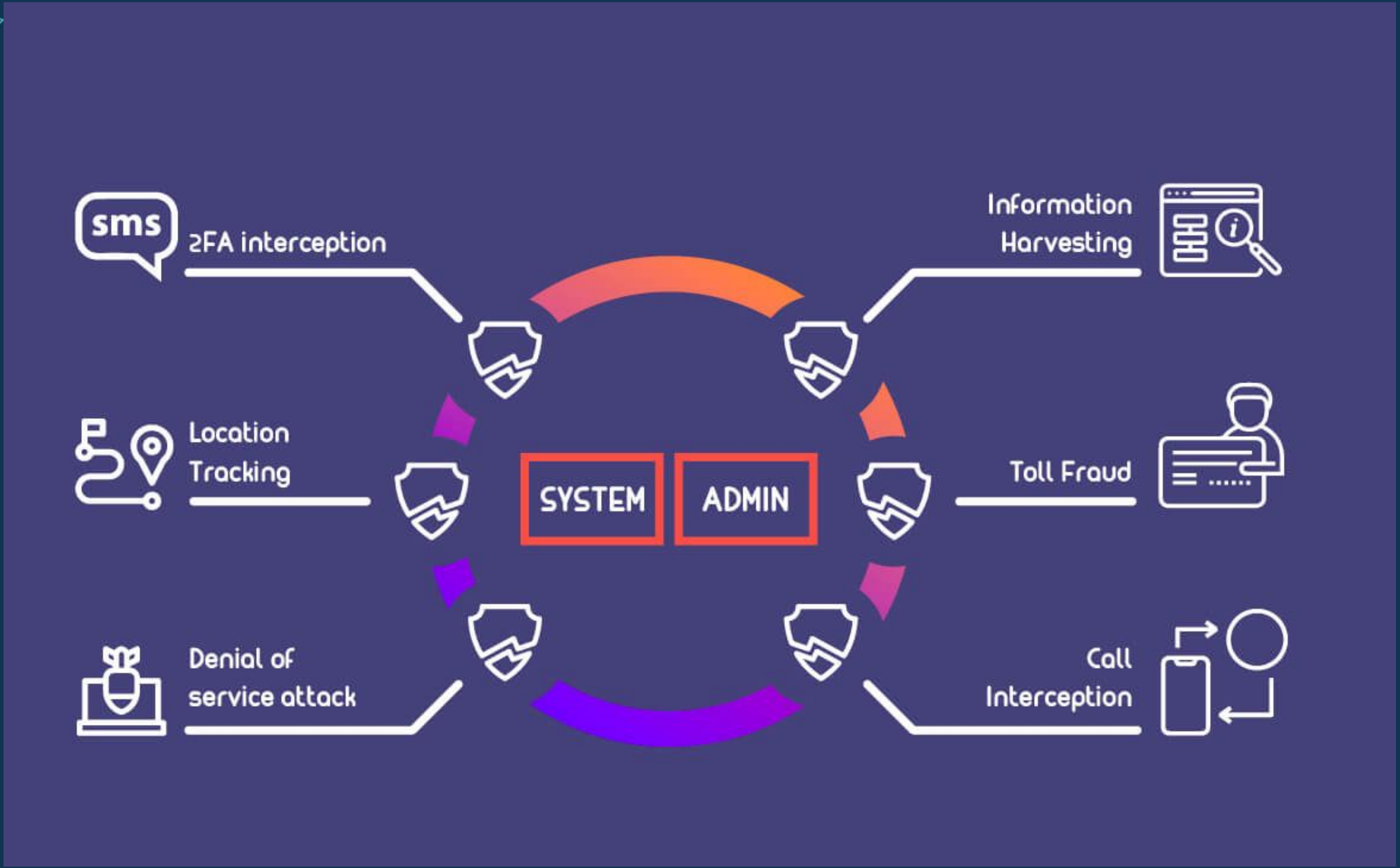
Significance of Pentesting

Enhancing Security

Compliance Requirements

Risk reduction

Business continuity

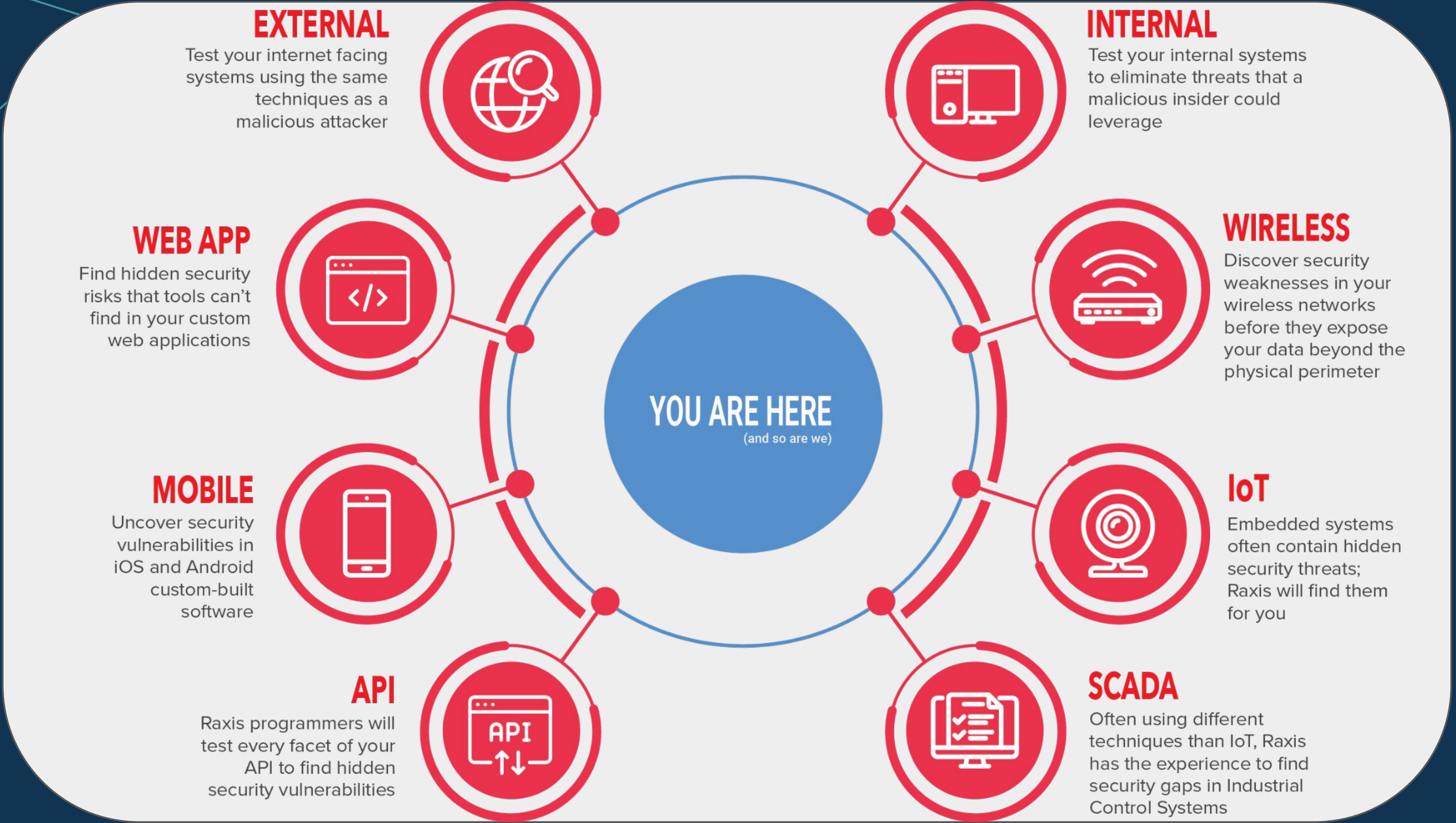


https://www.spiceworks.com/it-security/data-security/articles/man-in-the-middle-attack/

Steps

Pentesting Steps

1. **Prepare for the assessment.**
2. **Create plan.**
3. **Assemble Team.**
4. **Determine the goal.**
5. **Conduct reporting and data analysis.**



YOU ARE HERE
(and so are we)

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

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 Pentests

Types of tests

- External Test
- Internal Test
- Blind Test
- Double-blind Test

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.

Ethical Hacking

Ethics in PenTesting

1. 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.

Conclusion

Session Recap

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.

Hyperiondev

Q & A Section

Please use this time to ask any questions relating to the topic explained, should you have any

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”