Challenges for each chapter

Chapter 1. Organizational Penetration Testing

01_01. Understanding penetration testing

Q. Describe the goal of a penetration testing exercise.

01_02. Auditing security mechanisms

Q. Explain how an audit can help identify any gaps in security controls.

01_03. Managing risk

Q. Risk is when a person, place, or thing is open or exposed to harm, which can result in injury, death, or destruction. Describe the relationship between risk, threats, and vulnerabilities.

01_04. Analyzing risk

Q. Risk analysis is an important first step in reducing risk. Describe the steps taken during a security risk assessment.

01_05. Recognizing the attack surface

Q. An attack surface represents the combined number of attack vectors a malicious actor can use to gain access to a system. Describe some of the different attack surfaces.

Chapter 2. Types of Penetration Testing

02_01. Comparing different environments

Q. Compare unknown, known, and partially known environment testing, as it relates to how much knowledge the analyst has about the system, prior to testing.

02_02. Checking from the outside in

Q. Organizations seek to secure their systems and allow only authorized individuals to access resources. Explain the benefit of using an unknown environment approach during the penetration test.

02_03. Looking inside the organization

Q. Known environment testing digs into the system to have a thorough look inside an organization's systems. Explain how using known environment testing can help identify internal threats.

02_04. Determining testing methods

Q. When conducting penetration testing, the team can use a variety of methods. Compare automated and manual, along with announced and unannounced, testing.

02_05. Discovering penetration testing tools

Note: Always get clear written permission before you scan a system you do not own. However, if you would like to try a scan with Zenmap, you can use scanme.nmap.org, which allows an authorized scan to test to see if the scan is working properly.

Q. In every penetration tester's arsenal, there are tools that help complete the job. Discuss how reconnaissance tools, scanners, and password crackers are used during testing.

02_06. Challenge and solution: Explain the NIST five framework core functions

We know the purpose of a penetration testing exercise is to strengthen an organization's overall security posture. When providing recommendations on how to better secure your organization, there is help. One of the resources is NIST. Publications in the NIST Special Publications (SP) 800 series were developed to address and support the security and privacy needs of US federal government information and information systems. They are freely available and can provide a ton of valuable information. Learn more here: https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information

Obtain the NIST Cybersecurity Framework, found at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf, which outlines the five functions of the cybersecurity framework. Those functions include identify, protect, detect, respond, and recover.

- For this challenge, provide a brief overview of each of the five functions. The challenge should take you about 10 minutes.

Chapter 3. Penetration Testing Techniques

03_01. Following a structured plan

Q. When conducting a penetration testing exercise, its best to follow a structured plan. Outline the logical sequence of a penetration test.

03_02. Planning the penetration test

Q. When planning a security audit, it's important to involve all stakeholders, including the CEO, managers, and IT. Describe what's involved when planning the penetration test, such as establishing goals, along with obtaining policies and network documentation.

03_03. Footprinting the target

Q. Before beginning the penetration test, the team must complete a thorough information-gathering exercise on the target. Outline what's involved during the footprinting phase of ethical hacking.

03_04. Escalating privileges

Q. While penetration testing, various techniques leverage exploits to gain access to other systems. In this segment, we'll outline ways to escalate privileges to reach the target system.

03_05. Attacking the system

Q. During penetration testing, the ethical hacker must avoid disrupting critical systems, or compromise data. Discuss reasons why the ethical hacker must respect timing and duration when conducting the tests and have a clear understanding of what data to avoid.

03_06. Delivering the results

Q. After the penetration test is complete, the analyst compiles the results of the test. Describe the components of the report, including the executive summary, technical details, and remediation suggestions.

03_07. Outlining remediation strategies

Q. Outline why remediating any deficiencies found during penetration testing is a necessary step.

Chapter 4. Penetration Testing Blueprint

04_01. Checking physical security

Q. Physical methods can be an entry point and the first step in a data breach. Discuss what methods should be in place to stop a would-be attacker from gaining access to your systems.

04_02. Identifying wireless vulnerabilities

Q. Describe how wireless penetration testing identifies vulnerabilities specific to a wireless environment.

04_03. Testing the website

Q. A major breach using a vulnerable website has many implications, including the potential for a complete loss or compromise of sensitive data. Discuss what's involved when testing the website.

04_04. Leaking data via email or VoIP

Q. Malicious email can lead to a data breach. VoIP is also a concern, as it is vulnerable to numerous security threats. Discuss why it's important to test for weaknesses, in either email or VoIP systems.

04_05. Safeguarding cloud services

Q. What are three good practice activities when dealing with cloud services?

04_06. Assessing the mobile infrastructure

Q. Mobile devices have become pervasive in recent years. Discuss the importance of testing mobile devices for security vulnerabilities.

04_07. Hacking the human

Q. Network defenses get stronger every day. Hackers often will go after the weakest link – the people in an organization. Discuss why social engineering should be a part of every penetration test.

Chapter 5. Outsourcing Penetration Testing

05_01. Contracting the penetration test

Q. A company might choose to outsource a penetration test, instead of using in-house staff. Explain why outsourcing the penetration test might be an appropriate option for an organization.

05_02. Defining the project scope

Q. Before the penetration test begins, all stakeholders must agree on a clearly defined scope. Explain why it's important to outline the scope and identify what objectives must be met, in order to achieve a satisfactory result.

05_03. Hiring consultants

Q. When outsourcing penetration testing, the next step is to select and hire the consultants. Describe why it's important to check team credentials, spell out all requirements, and agree on the terms before testing begins.

05_04. Agreeing on terms

Q. Describe the importance of outlining the terms before entering a full-blown ethical hacking exercise.

05_05. Creating the contracts

Q. Explain the purpose of the nondisclosure agreement (NDA), statement of work (SOW), and master service agreement (MSA).