Lesson 7 - Introduction to Linux

In this lesson, students will learn about the importance of assessing organizational security and how to use different tools to conduct security assessments. They will be introduced to four key tools: network reconnaissance and discovery, file manipulation, shell and script environments, and packet capture and replay. Through guided practice and independent group work, students will have the opportunity to apply these tools to assess the security of various scenarios. The lesson will conclude with a review of the tools covered and a discussion on the ongoing need for security assessments to protect against evolving threats.

Objectives:

- Understand the importance of assessing organizational security

- Learn how to use different tools to assess organizational security

- Develop skills in network reconnaissance and discovery, file manipulation, shell and script environments, and packet capture and replay

Materials:

- Computers with internet access

- Security assessment tools (e.g., Nmap, Wireshark, Metasploit)

- Scenario for assessment

Bell-Ringer Activity:

- Display a scenario on the board or projector screen: "You have been hired as a security consultant for a company. Your task is to assess the organization's security and identify any vulnerabilities. What tools or methods would you use for this assessment?"

- Give students a few minutes to think and write down their answers individually.

- Afterward, ask a few students to share their responses with the class.

Introduction:

- Explain to students that assessing organizational security is crucial to identify vulnerabilities and protect against potential threats.

- Discuss the importance of using appropriate tools for different assessment tasks.

- Introduce the four tools that will be covered in this lesson: network reconnaissance and discovery, file manipulation, shell and script environments, and packet capture and replay.

Direct Instruction:

- Provide an overview of each tool and its purpose:

- Network reconnaissance and discovery: Used to gather information about a network, such as IP addresses, open ports, and services running on those ports. This helps identify potential entry points for attackers.

- File manipulation: Involves modifying or accessing files on a system to test for vulnerabilities or gain unauthorized access.

- Shell and script environments: Provide a command-line interface to interact with a system, allowing for more advanced security assessments and exploitation.

- Packet capture and replay: Involves capturing network traffic and analyzing it to identify potential security issues or replaying captured packets for further analysis.

Guided Practice:

- Demonstrate the use of each tool using a sample scenario.

- Show students how to perform network reconnaissance and discovery using Nmap, including scanning for open ports and services.

- Explain how to manipulate files on a system using appropriate tools, such as modifying permissions or accessing sensitive files.

- Walk students through using a shell or script environment to execute commands and perform advanced security assessments.

- Show how to capture and analyze network traffic using Wireshark, and discuss the importance of packet analysis in identifying potential security threats.

Independent Practice:

- Divide students into small groups.

- Provide each group with a different scenario related to organizational security assessment.

- Instruct each group to use the appropriate tool(s) to assess the security of the given scenario.

- Encourage students to document their findings and any vulnerabilities they discover.

Exit Ticket:

- Distribute an exit ticket to each student.

- Ask students to write a brief summary of the importance of assessing organizational security and one tool they found most useful during the lesson.

- Collect the exit tickets before the end of the class.

Closure:

- Review the importance of assessing organizational security and the role of different tools in this process.

- Recap the four tools covered in the lesson: network reconnaissance and discovery, file manipulation, shell and script environments, and packet capture and replay.

- Emphasize the need for ongoing security assessments to protect against evolving threats.

- Encourage students to continue exploring and learning about different tools and techniques for assessing organizational security.