**LESSON 3 – NETWORK SECURITY**

**PROJECT 3.2.6 – ERADICATE THE VULNERABILITIES**

Students should use the Pen Test Considerations as a set of guidelines for their work. It should help them plan the tasks they need to complete.

**SAMPLE PENETRATION TEST CONSIDERATIONS**

* **Reconnaissance**

We learned about three types of scans in Zenmap: Ping scan, Quick Scan, and Quick Scan Plus. We decided to use Quick Scan Plus because it is the one that provides the most information about the open ports and the services (software versions) running on these ports.

* **Scanning**We plan to reuse the Nessus Advanced Scan we generated in Activity 3.2.5 and not generate a new one. It takes a long time to run (approximately 15 minutes), and it will generate the exact same report (same network topology).
The Nessus scan lists all the known vulnerabilities in the network. That information, along with the Zenmap report, can be used to choose the vulnerabilities we are planning to exploit.
* **Compromise**We plan to use PowerShell, PuTTY, or Metasploit as we did in Activity 3.2.5. Which ones we use will depend on the exploits we plan to perform.
* **Remediation**
	+ Edit configurations to address the vulnerabilities (could be firewall rules/iptables)
	+ Test the exploits again and verify the vulnerabilities are fixed.
	+ Document observations and take screenshots as evidence.

**ETHICAL SCENARIO**

What is the ethical dilemma or consideration in this situation?

|  |
| --- |
|  |

What are the various perspectives that individuals might have when considering this scenario?

|  |
| --- |
|  |

What is your personal perspective on this scenario?

|  |
| --- |
|  |

What is a new perspective you previously had not considered?

|  |
| --- |
|  |

What would it take for you to change your mind?

|  |
| --- |
|  |

**PENETRATION TEST**

1. Reconnaissance:
	1. Identify the tool and the type of scan(s) you used to discover the network structure including any resources you already have.

|  |
| --- |
|  |

* 1. What hosts and services look vulnerable as far as you can tell from the report?

|  |
| --- |
|  |

* 1. Provide a copy of the scan(s) you performed.

|  |
| --- |
|  |

1. Scanning:
	1. Identify the tool and the scan(s) you used to discover ports and services.

|  |
| --- |
|  |

* 1. Provide a copy of the scan(s) you performed.

|  |
| --- |
|  |

* 1. Describe two vulnerabilities that you plan to exploit, their severity, and recommended solutions.

|  |
| --- |
|  |

1. Compromise:
	1. Identify the tool(s) you used for your exploits.

|  |
| --- |
|  |

* 1. Take screenshots of the results of each exploit you completed.

|  |
| --- |
|  |

* 1. Describe what you observed.

|  |
| --- |
|  |

1. Remediation:
	1. Document your plan of action to ensure the system is secure against each of the exploits.

|  |
| --- |
|  |

* 1. Describe the steps you took in the lab to resolve these exploits.
		1. Take screenshots of the setups you completed to eradicate the vulnerabilities.

|  |
| --- |
|  |

* 1. Verify that your plan worked.
		1. Take screenshots as evidence of the resolution.

|  |
| --- |
|  |

* 1. Document any other recommend future remediation for the documented vulnerabilities.

|  |
| --- |
|  |

**Open your saved scan files on your local school machine. Record what you see in the scan files (After Step #9)**

For the Ping scan, confirm the IP addresses match your topology diagram of the water treatment facility network. Recall that some of the addresses are responsible for running the virtual lab.

|  |
| --- |
|  |

**For the Quick Scan Plus:**

1. What does this scan provide that isn’t available in the Quick Scan (used in Activity 3.2.3)?

|  |
| --- |
|  |

1. Record the detailed information for the required services on PumpPLC.

|  |
| --- |
|  |

1. For the essential services, which of these should be accessible from outside the firewall?

|  |
| --- |
|  |

1. How would an unethical hacker use information from these scans to their advantage in developing an attack plan?

|  |
| --- |
|  |

**CONCLUSION**

**What principles and practices should an ethical hacker follow?**

|  |
| --- |
|  |

**Write a summary about your experience in this project. Your summary should address the following questions:**

What alternatives could you have considered to the fixes that you implemented?

|  |
| --- |
|  |

What special ethical obligations are in place to protect and secure networks that operate critical infrastructures?

|  |
| --- |
|  |