**LESSON 3 – NETWORK SECURITY**

**ACTIVITY 3.2.5 – EXPLORING SECURITY FRAMEWORKS**

**ATTENTION -** *Download your scan file to your school’s local machine.*

**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?

|  |
| --- |
|  |

**While Nessus is scanning, research an example of a plug-in and the impact an exploit of its service may have on a system. (Step #20)**

1. Research Plugin ID 84215 on the Nessus Tenable website. In a new browser tab, search “nessus tenable” to find their site. (Do not select an Ad-based or Download link.)
2. On the home page, find a link similar to “Explore our latest research”. As of this writing, it’s in a section showing “137,000+ Plugins”.
3. Navigate to the link that lets you search for plugins, such as the link “Plugins and Detections”, and search for **84215**.
4. Describe this plug-in and its severity. What is the potential impact of exploiting this vulnerability?

|  |
| --- |
|  |

You should see a critical vulnerability related to ProFTPD. (If not, wait until the scan finds and reports it on this page.) Save a screenshot of the Vulnerabilities page that include the first few entries. (Step #22)

|  |
| --- |
|  |

Select the ProFTPD vulnerability and save a screenshot of its details. (If necessary, you can select the **Vulnerabilities** tab again to return to the list of vulnerabilities.) (Step #23)

|  |
| --- |
|  |

**Using your screenshots, review the details of ProFTPD plug-in. (Step #24)**

1. What is the service and software (version) exploited in the vulnerability?

|  |
| --- |
|  |

1. What port(s) and protocol(s) are affected?

|  |
| --- |
|  |

1. When was the plug-in published?

|  |
| --- |
|  |

1. When was it last modified?

|  |
| --- |
|  |

1. What are the solutions? What will they achieve?

|  |
| --- |
|  |

**To further confirm access, cat the /etc/passwd file that contains a list of all users on PumpPLC. Finding this sensitive user information confirms that you were able to access the system through the backdoor created by the exploit. As the pen tester, you have found and confirmed a major vulnerability on your network! (Step #39)**

***HINT: Students install their exploit and then access the system with root permissions through the backdoor.***

What were the effects of launching the exploit?

|  |
| --- |
|  |

What are the ethical consequences and responsibilities of testing this vulnerability?

|  |
| --- |
|  |

**Refer to your iptables commands in your notebook to answer the following questions: (Step #41)**

1. How do you designate the protocol used by FTP and SSH?

|  |
| --- |
|  |

1. What is the port designation for FTP and SSH?

|  |
| --- |
|  |

1. How do you establish the source of inbound traffic for each service?

|  |
| --- |
|  |

1. What is the general policy you want to create?

|  |
| --- |
|  |

denote which commands you will use to provide remediation for PumpPLC. Compare your team’s commands to that of another team and make any adjustments you deem appropriate.

|  |
| --- |
| **Students should implement the following commands to configure PumpPLC’s firewall and mitigate the exploits. Note these commands all require sudo.*** **Clear rules for current inbound traffic: iptables -F INPUT**
* **Allow .....iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT**
* **Allow SSH traffic iptables -A INPUT -p tcp --dport ssh -j ACCEPT**
* **Allow FTP traffic only from PumpMonitor iptables -A INPUT -p tcp --dport ftp -s 10.2.0.6 -j ACCEPT**
* **Deny all other traffic sudo iptables --policy INPUT DROP**
* **Confirm the rules iptables -L INPUT**
* **Save iptables-save**
 |

Verify that your remediation addressed the vulnerability. ***Take screenshots of your results as evidence of your successful remediation.* (Step #44)**

|  |
| --- |
|  |

Confirm you did not remove any operational functionality. ***Take a screenshot of your results as evidence of your operational requirements test.* (Step #45)**

|  |
| --- |
|  |

**CONCLUSION**

What are some features of security frameworks like Metasploit that are useful to the ethical hacker?

|  |
| --- |
|  |

What general protection strategies are available to counter network attacks?

|  |
| --- |
|  |