Performing Network Reconnaissance and Vulnerability Scanning

(CompTIA Security + SY – 601)

Objectives:

1.1 Given a scenario, analyze indicators of compromise and determine the type of malware
1.2 Given a scenario, use appropriate software tools to assess the security posture of an organization
1.3 Given a scenario, troubleshoot common security issues
1.4 Given a scenario, analyze and interpret output from security terminologies

Resources:

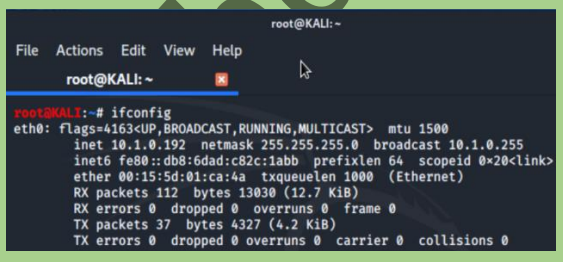
1. Windows Virtual Machine VM
2. Kali Virtual Machine VM
3. LX1 (CentOS Linux)
4. Command line tools

Instructions:

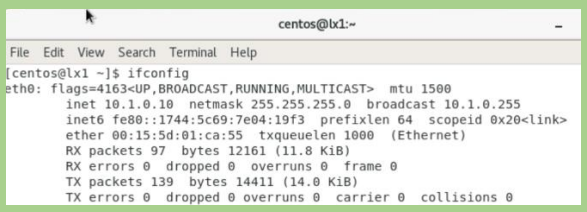
Discover the Network

1) Use any virtual Machine to discover the IP address for the Virtual Machines listed below:
- ip addr
- ifconfig
- ipconfig

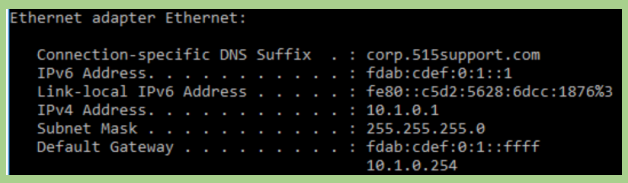
2) PT Kali (Kali Linux)



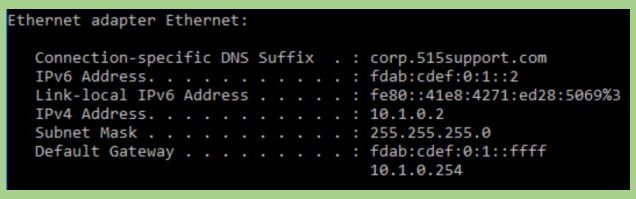
3) LX1 (CentOS Linux)



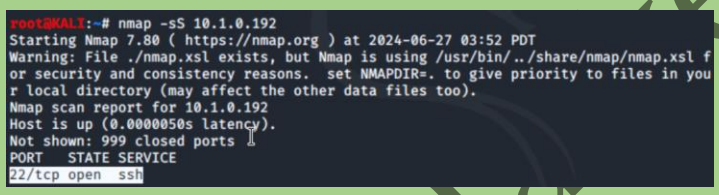
4) DC1 (Windows Server 2016)



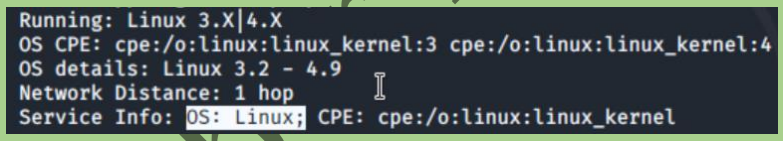
5) MS1 (Windows Server 2016)



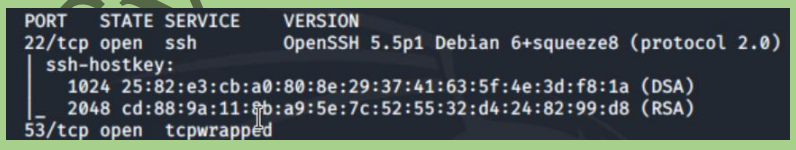
6) On the Kali Virtual Machine (VM) run an nmap scan to display the VMs own ports



7) What port is open on PT1Kali VM ?
8) What operating system is running on 10.1.0.254 ?

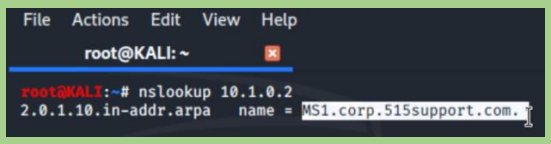


9) What two ports are open on 10.1.0.254 ?

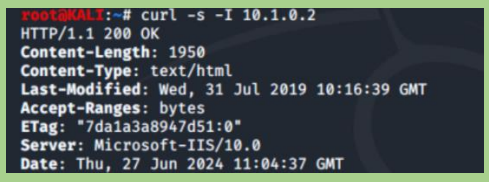


Gather Information on the Web Server

1) Sign in on the Kali VM Machine
2) Use the nslookup command on Kali VM to display the FQDN



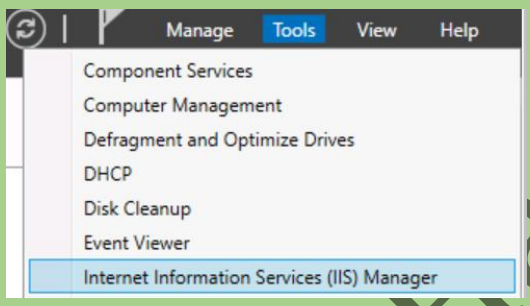
3) What is the FDQN of 10.1.0.2 ?
4) Run the following command to connect to the 10.1.0.2 HTTP server by using cURL



5) What web server and version is used on the 10.1.0.2 Virtual Machine ?

Configure the Web Server for Authentication

1. Switch to MS1 VM
2. Launch the Internet Information Service (IIS) Management

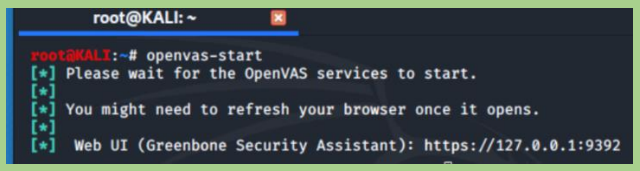


3. Use the Authentication applet in the **Default web** site Home page to disable **Anonymous Authentication** and **Enable Basic Authentication**
4. Close the **IIS Manager**
5. Switch to PT1-Kali VM
6. Open the Terminal console and then run the following command
7. Launch Wireshark application. Use Wireshark to open the auth.txt file from the root user's home directory
8. Examine the HTTP **GET** messages to answer the following question for authentication information
9. Which of the following information shows how the authentication information is displayed ?

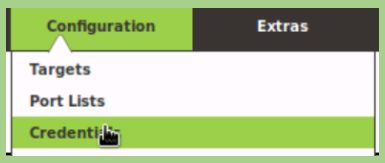
Run the OpenVAS Scanner

1. Switch to PT1-Kali VM
2. In the menu at the top of the desktop select Terminal

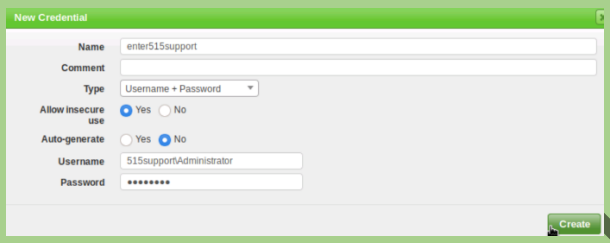
3. In the Terminal type openvas-start and type Enter



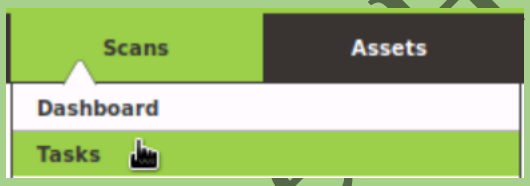
4. The firefox browser will automatically launch when the openvas starts
5. Log in with the username **admin** and Password **Pa$$w0rd**
6. From the **configuration** menu select **Credentials** to create a credentialed scan



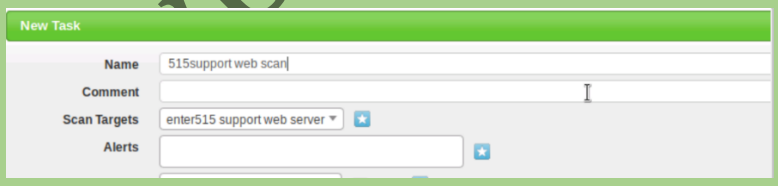
7. Select the blue star icon on the left to open the New Credential web dialog box



8. Enter the given credentials
9. Select create
10. Next configure a **scan task**. From the scan menu select **Tasks**

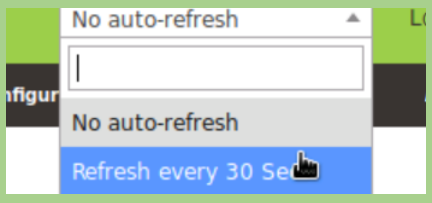


11. Select the **blue star** icon on the left to open the **New Task** Web dialog



12. Enter the given credentials
13. Select create
14. Under the name at the bottom of the screen, select the **515support-Full and Fast-Daily Task**
15. Select start **green arrow** button to run the scan manually

16. From the *No auto-refresh* box on the green bar header, select **Refresh every 30 seconds**

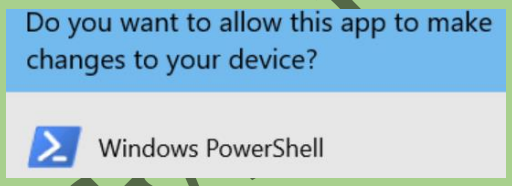


17. Select scan reports
18. In the **Date** column at the bottom of the Reports page select the task with the Today's date to see the results
19. From the small triangle pull down menu by the **'ReportResults'** title choose **Report.Hosts** to display the discovered hosts and their related vulnerability information

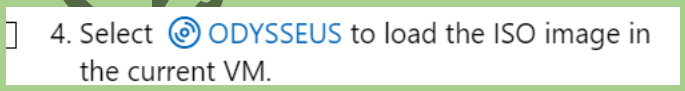
20. In the pull-down menu at the upper left of the page, select HTML. The select the green **Download filtered Report** button
21. When prompted select **Save File** to download the report to the default **Downloads Folder**
22. Close the OpenVAS administration site in firefox

Install Malware

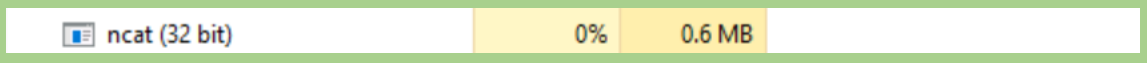
1. Switch to the MS1
2. From an **Administrator: Windows PowerShell** console, run the following command to disable Windows Defender online scanning



3. Select **ODYSSEUS** ISO image in the current VM

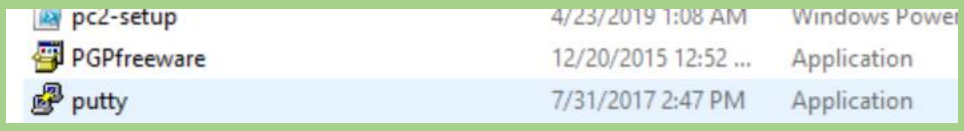


4. Select the prompt in the lower right corner of the desktop once the DVD has been loaded
5. Select **setup.exe** in the window. Select **Yes** when you are prompted with the **UAC**
6. Open the **Task Manager** and select **Processes**



Establish Connectivity Using the Backdoor

1. Switch to the **PT1-Kali VM**
2. Run **nmap 10.1.0.2 -p 4450**
3. Switch to **DC1**
4. From the desktop open the **LABFILES** folder, and then run **putty**



Disable the Malware

1. Switch to the **MS1 VM**
2. Use the Task Manager to end the **nc (32-bit process)**
3. Use **Windows Defender Firewall with Advanced Security** to disable the **Service port** inbound rule associated with the **nc** malware

Observations:

1) **Network Discovery:**

- Identified IP addresses of VMs using ip addr, ifconfig, ipconfig.
- Ran nmap on Kali VM to find open ports and operating systems.

2) **Web Server Information Gathering:**

- Used nslookup and cURL on Kali VM to find FQDN and web server details.

3) **Web Server Authentication Configuration:**

- Configured IIS on MS1 VM for basic authentication.
- Verified with Wireshark.

4) **Vulnerability Scanning:**

- Ran OpenVAS on Kali VM.
- Downloaded and analyzed scan reports.

5) **Malware Analysis:**

- Installed and disabled malware on MS1 VM using Task Manager and Windows Defender.

6) **Backdoor Connectivity:**

- Established and verified backdoor using nmap and other tools.

Results:

1) **Network Discovery:**

- Identified VMs' IP addresses, open ports, and OS details.

2) **Web Server Information Gathering:**

- Retrieved FQDN and web server version.

3) **Web Server Authentication Configuration:**

- Successfully enabled basic authentication.

4) **Vulnerability Scanning:**

- Identified vulnerabilities and affected hosts.

5) **Malware Analysis:**

- Successfully managed and disabled malware.

6) **Backdoor Connectivity:**

- Verified backdoor connectivity.

Conclusion:

This lab effectively demonstrated network reconnaissance, vulnerability scanning, and basic malware analysis. We identified and mitigated security issues, configured authentication, ran vulnerability scans, and handled malware. This emphasized the importance of regular security assessments and proactive defenses to maintain a secure network environment.

Future Work:

1. Enhance security measures and update systems regularly.
2. Implement advanced threat detection.
3. Conduct continuous monitoring and regular audits.
4. Provide ongoing security training for IT staff.