**Lab 7-01: Perform NetBIOS Enumeration using Windows Command-Line Utilities**

**Scenario**

FinanceSafe Inc., a financial services company, has hired SecureDES Consultants, a cybersecurity consulting firm, to do a comprehensive security evaluation of its internal and external network infrastructure. The engagement’s main goal is to evaluate the risk of unwanted access by locating sensitive data and weaknesses in the company’s Windows-based systems. The servers that store customer portals, employee management applications, and financial databases are part of FinanceSafe Inc.’s complex network, which has several subnets. Since many of the company’s systems have NetBIOS services enabled to enable file sharing and remote administration, one of their main concerns is the possible disclosure of sensitive data.

**Solution**

As a Certified Ethical Hacker or penetration tester, your task is to perform NetBIOS enumeration using Windows command-line utilities to gather critical information about the internal network. Using tools such as nbtstat and net view, you will explore the network to identify active systems, NetBIOS names, shared resources, and user account information that may be vulnerable to exploitation. This enumeration will help uncover potential entry points for further exploitation and provide insights into how attackers might leverage exposed NetBIOS services to compromise the security of FinanceSafe Inc.’s internal network. The gathered information will also serve as the foundation for additional penetration testing and security hardening recommendations.

Nbtstat can be helpful when troubleshooting NETBIOS name resolution issues. Several case-sensitive switches are used by the nbtstat command to eliminate and fix preloaded items. Information like NetBIOS over TCP/IP (NetBT) protocol statistics, NetBIOS name tables for local and remote computers, and the NetBIOS name cache may all be enumerated using nbtstat.

**Note:** In this lab, the target IP address we use is **192.168.56.106** of Windows Server 2025. Do not use this lab IP address. Use your virtual machine IP address at the time when you are performing this lab.

|  |
| --- |
| 1. Start your **Windows 10** and **Windows Server 25** virtual machines. Now, switch to the **Windows 10** virtual machine. Click on the **Windows Search** on the **Desktop**, search for **cmd** in the search field, and click on **Open**.    2. Execute the following command: **nbtstat -a [IP address of the remote machine].** In this command, **-a** shows the NetBIOS name table of a remote server or computer. The result shows the NetBIOS name table of a Windows Server 2025 virtual machine.    3. Execute the following command: **nbtstat -c.** In this command, **-c** lists the contents of the NetBIOS name cache of the remote server or computer.  The result shows the table of NetBIOS names, their resolved IP addresses, and the contents of the NetBIOS name cache. This data can be extracted without establishing a null or unauthenticated session.    4. Execute the following command: **net use**. The output shows details about the target, including network information, shared folders and drives, and connection status.    5. Depending on the available shares, the attackers can use this information to read or write to a remote computer system or even initiate a Denial-of-Service (DoS) attack. This concludes the example of utilizing Windows command-line tools like Nbtstat and Net use to do NetBIOS enumeration. |

**Lab 7-02: Perform SNMP Enumeration using SnmpWalk**

**Scenario**

TechCore Systems, a technology solutions provider, has hired SecureNet Assessments, a cybersecurity organization, to conduct a full security assessment of its network infrastructure. TechCore Systems relies extensively on networking devices, including routers, switches, and hubs, to run its operations. Many of these devices use the Simple Network Management Protocol (SNMP) for monitoring and administration functions. The organization fears improper SNMP settings might reveal important network information, exposing it to hackers.

**Solution**

As a Certified Ethical Hacker, you will utilize SnmpWalk, a powerful SNMP enumeration tool, to collect essential information about TechCore Systems' network. This involves detecting active hosts, user accounts, ARP tables, routing tables, device settings, and traffic data. SnmpWalk will allow you to connect with SNMP agents operating on networking devices to obtain data and inventory exposed network resources.

The information acquired will help to discover vulnerabilities such as weak SNMP community strings and excessive disclosure of device-specific data, which attackers might use to gain unwanted network access.

The command-line utility SnmpWalk quickly examines many SNMP nodes and finds a collection of variables that may be used to access the target network. It is sent to the root node to get the data from all sub-nodes, including switches and routers.

**Note:** In this lab, the target IP address we use is **192.168.56.105** of Windows Server 2025. Do not use this lab IP address. Use your virtual machine IP address at the time when you are performing this lab.

**Prerequisite:** Before starting this lab, install the SNMP service on Windows Server 2025. Use the documentation provided below to install SNMP on Windows Server 2025.

**Documentation:** <https://solarwindscore.my.site.com/SuccessCenter/s/article/Install-or-configure-SNMP-for-Windows?language=en_US>

|  |
| --- |
| 1. Turn on your **Windows Server 2025** and **PattotOS** virtual machines. Now, switch to the **ParrotOS** virtual machine. Open the **Terminal** and execute the following command: **sudo su** to run the programs as a root user. When prompted, enter your **root** password.    2. Execute the following command: **apt-get install snmp** to install SnmpWalk in the ParrotOS virtual machine.    3. Execute the following command: **snmpwalk -v1 -c public [target IP]**. The version number of SNMP (1, 2c, or 3) is specified by the **-v**. By using **-c**, a community string is set. The output shows all OIDs, variables, and other related information.    3. Execute the following command: **snmpwalk -v2c -c public [Target IP Address]** to enumerate SNMPv2 on the target system. The result shows the data transmitted from the SNMP agent to the SNMP server, encompassing server information, user credentials, and other parameters. This concludes the demonstration of SNMP enumeration with the SnmpWalk. |

**Lab 7-03: Perform LDAP Enumeration using Active Directory Explorer (AD Explorer)**

**Scenario**

A multinational organization, GlobalTech Solutions, has contracted a cybersecurity consultancy, SecureLink Assessments, to evaluate the security of its internal directory services. GlobalTech Solutions relies on Active Directory to manage its global branches’ user accounts, devices, and network resources. The organization is concerned that misconfigured LDAP settings could expose sensitive directory information, making it easier for attackers to map their network and launch targeted attacks.

**Solution**

As a Certified Ethical Hacker, your task is to perform LDAP enumeration using Active Directory Explorer (AD Explorer). The goal is to connect to the organization’s LDAP server and extract details such as usernames, email addresses, departmental information, server names, and group memberships. This information can help identify potential vulnerabilities within the directory services configuration, including overly permissive access, exposed organizational details, and weak authentication policies.

Active Directory Explorer (AD Explorer) is a robust Active Directory viewer and editor. It allows you to effortlessly explore an AD database, create preferred locations, see object properties and attributes without opening dialog boxes, update permissions, inspect an object’s structure, and do advanced searches that can be saved and re-executed.

Using AD Explorer, you will establish a connection to the LDAP server on TCP port 389 and explore the hierarchical structure of the directory. You will compile a detailed inventory of the organization’s network components by querying various objects and attributes within Active Directory. The information gathered will be analyzed to determine how attackers could use it to map the network, escalate privileges, or compromise sensitive systems.

Ensure that all activities are performed with proper authorization from GlobalTech Solutions’ management and in compliance with legal and organizational policies. The findings from this exercise will provide actionable insights to help the organization secure its LDAP implementation, reduce the attack surface, and safeguard its internal directory services.

**Note:** In this lab, the target IP address we use is **192.168.56.106** of Windows Server 2025. Do not use this lab IP address. Use your virtual machine IP address at the time when you are performing this lab.

**Prerequisites:** Before starting this lab, install the Active Directory Domain Services on Windows Server 2025. Use the documentation provided below to install Active Directory Domain Services on Windows Server 2025.

**Documentation:** <https://www.ibm.com/docs/en/storage-scale-bda?topic=support-install-configure-active-directory>

|  |
| --- |
| 1. Start your **Windows 11** and **Windows Server 25** virtual machines. Then switch to **Windows 11** virtual machine, open any browser, and type the following URL: [**https://learn.microsoft.com/en-us/sysinternals/downloads/adexplorer**](https://learn.microsoft.com/en-us/sysinternals/downloads/adexplorer). Click on the **Download AdExplorer** to download the ADExplorer executable file.    2. Go to the **Downloads** folder, unzip the **ADExplorer** folder, and then navigate inside the folder. Double-click on the **ADExplorer.exe**.    3. The Active Directory Explorer License Agreement window appears. Click on the **Agree** button.    4. The Connect to Active Directory window opens; type the **IP address** of the Windows Server 2025 in the **Connect to field**. Then, enter your Windows Server 2025 **User** and **Password**. Then click on the **OK** button.    5. The **Active Directory Explorer** shows the active directory structure in the left pane.    6. Click on the **+ icon** to expand **DC=CEH, DC=com.** Click on the **+ icon** to expand **CN=Users** to explore domain user details.    7. Click any **username** (here, John) from the left pane to display its properties in the right pane. Right-click on the **displayName** attribute in the right pane. Then, click on **Modify...** from the context menu to modify the user’s profile.    8. The Modify Attribute window opens. Select the **username** (here, John) under the **Value** section. Then click on the **Modify...** button.    9. The Edit Value pop-up window opens. Rename the **username** in the **Value data** field. Click on the **OK** button to save the changes. |

**Lab 7-04: Perform NFS Enumeration using RPCScan and SuperEnum**

**Scenario**

A software development company, CodeStream Innovations, has engaged a cybersecurity consultancy, SecureProbe Analysts, to conduct a detailed security assessment of its internal file-sharing infrastructure. The company relies heavily on a Network File System (NFS) server to facilitate file sharing and collaboration among its development teams. These servers store and manage sensitive data, including proprietary source code, project documentation, and team resources. CodeStream Innovations is concerned that misconfigured NFS settings may expose shared directories and client information, creating a potential entry point for attackers.

**Solution**

As a Certified Ethical Hacker or penetration tester, your task is to perform NFS enumeration using RPCScan and SuperEnum to extract critical details about the NFS server. RPCScan interacts with RPC (Remote Procedure Call) services to check for NFS share setup errors. It lists RPC services, mountpoints, and NFS-accessible folders. It is also capable of listing NFS shares in recursive mode. SuperEnum offers a script that enumerates all open ports, including the NFS port (2049).

The information gathered will allow you to assess whether the server is improperly exposing sensitive data or is vulnerable to spoofing attacks. By simulating a scenario where an attacker spoofs a client’s IP address to gain unauthorized access to shared files, you will evaluate the risk level and identify necessary mitigation measures.

**Note:** In this lab, the target IP address we use is **192.168.56.106** of Windows Server 2025. Do not use this lab IP address. Use your virtual machine IP address at the time when you are performing this lab.

|  |
| --- |
| 1. Turn on your **Windows Server 2025** and **PattotOS** virtual machines. Now, switch to the **Windows Server 2025** virtual machine at the bottom-left corner of the **Desktop** andclick on the **Start** button**.** Click on the **Server Manager** to open it. The **Server Manager** main window opens. By default, the **Dashboard** will be selected. Click on the **Add roles and features**.    2. Click on the **Next >** button.    3. Leave all the settings as default and click on the **Next >** button.    4. Click on the **Next >** button.    5. The **Server Roles section** appears. Expand **File and Storage Services.** Then select the **Server for NFS** checkbox inside the **File and iSCSI Services** option. Click the **Next >** button.    6. In the **Add features that are required for Server for NFS?** pop-up window. Click on the **Add Features** button.    7. Now, the **Serve for NFS** box checkbox is selected. Click on the **Next >** button.    8. Click on the **Next >** button.    9. Click on the **Install** button.    10. After the installation is finished. Click on the **Close** button.    11. Switch to the **ParrotOS** virtual machine. Execute the following command: **nmap -p 2049 [Target IP Address]**. The **-p** flag specifies port. The scan results reveal that port 2049 is open, indicating that the NFS service is active.    12. Execute the following command: **git clone** [**https://github.com/p4pentest/SuperEnum.git**](https://github.com/p4pentest/SuperEnum.git)to install the SuperEnum GitHub repository**.**    13. Execute the following command: **cd SuperEnum** to go to the SuperEnum directory. Then execute the following command: e**cho "192.168.56.106" >> Target.txt** to generate a file with the target machine's IP address. You can insert many IP addresses in the **Target.txt** file. However, we target only one virtual machine in this lab, the Windows Server 2025.    14. Execute the following command: **./superenum**. If an error occurs while executing the **./superenum** script, run the command **chmod +x superenum** to grant execute permissions, and then repeat Step 14.    15. Again, execute the following command: **./superenum.** Type **Target.txt** in the **Enter IP List filename with path,** and then press **Enter**.    16. The script scans the target IP address to identify open NFS and other services. The scanning process may take some time to complete. Once finished, scroll down to examine the results. Port 2049 is open, and the NFS service is operating on it.    17. First, execute the **cd ..** command to return to the previous directory. Execute the following command: **git clone** [**https://github.com/hegusung/RPCScan.git**](https://github.com/hegusung/RPCScan.git) to install the RPCScan GitHub repository. Then execute the **cd RPCScan** command to go inside the RPCScan directory.    18. Execute the following command: **python3 rpc-scan.py [Target IP address] --rpc**.The **--rpc** parameter lists the RPC (portmapper). The result indicates that port 2049 is open, and the NFS service is running on it. |

**Lab 7-05: Perform DNS Enumeration using Zone Transfer**

**Scenario**

A digital marketing agency, MarketEdge Solutions, has hired a cybersecurity firm, CyberPro Assessments, to evaluate its external network security posture. MarketEdge Solutions manages a range of web assets, including client portals, content delivery servers, and DNS servers, to support its global operations. The company is concerned that misconfigurations in its DNS servers may expose sensitive information such as hostnames, internal IP addresses, and usernames, making it easier for attackers to map their infrastructure and target critical systems.

**Solution**

As a Certified Ethical Hacker or penetration tester, your task is to perform DNS enumeration using the Zone Transfer technique. A DNS zone transfer involves replicating a copy of the DNS zone file from the primary DNS server to a secondary DNS server. The DNS server usually maintains a spare or secondary server for redundancy, which holds all information stored in the main server. If the DNS zone transfer setting is enabled on the target DNS server, it will provide the requested DNS information. Otherwise, it will return an error indicating that the zone transfer has failed or been refused.

Using tools like dig or nslookup, you will attempt to request a zone transfer from MarketEdge Solutions’ DNS servers. Consider a scenario where the server is misconfigured to permit zone transfers to unauthorized clients. It will provide detailed records of the domain’s structure in that case. This information will help identify potential entry points into the organization’s network and highlight critical misconfigurations that attackers could exploit.

Ensure all enumeration activities are conducted with explicit authorization from MarketEdge Solutions’ leadership and comply with relevant legal and ethical guidelines. The findings from this exercise will help the company strengthen its DNS server configurations and prevent unauthorized access to its sensitive DNS records.

**Note:** In this DNS enumeration lab, we use the [**https://www.certifiedhacker.com/**](https://www.certifiedhacker.com/) website. The target name server we are using is **ns1.bluehost.com**.

|  |
| --- |
| 1. Turn on your **Windows 11** and **PattotOS** virtual machines. Now, switch to the **ParrotOS** virtual machine. Launch the **Terminal** and enter the command **sudo su** to execute programs with root user privileges. When prompted, enter your **root** password.    2. Execute the following command: **dig ns [Target Domain]**. In this command, **ns** returns the name servers as a result. This command gets information about all DNS name servers for the target domain. This is demonstrated in the ANSWER SECTION of the screenshot below. On Linux-based systems, the **dig** command is used to query DNS name servers for information such as target host addresses, name servers, mail exchanges, etc.    3. Execute following command: **Run dig @[NameServer] [Target Domain] axfr**. The **axfr** command gets zone information. The result indicates that the server is available but that the transfer failed.    4. After gathering information about the DNS name servers, an attacker can probe one of the servers to verify whether zone transfers are permitted by the target DNS. Zone transfers are not permitted for the destination domain; hence, the command resulted in the message: The transfer has failed. A penetration tester should attempt DNS zone transfers across multiple domains within the target organization.5. Switch to **Windows 11** virtual machine. In the Desktop, click on the Windows **Search** icon. In the search bar, type **CMD**. Click on the **Open** to open the command prompt.    6. Execute the following command: **nslookup**.  In the nslookup interactive mode, execute the following command: **set querytype=soa**.  Enter the target domain **certifiedhacker.com** and press **Enter**. This resolves the target domain information.   * **set querytype=soa** retrieves administrative information about the target domain certifiedhacker.com DNS zone using the SOA (Start of Authority) record. * The result shows information about the target domain, including the principal name server and the responsible mail address. * In the nslookup interactive mode, execute the following command: **ls -d [Name Server]**. In this command, **ls -d** requests a zone transfer for the given name server. |

## Lab 7-06: Perform SMTP Enumeration using Nmap

**Scenario**

A technology services firm, DataLink Solutions, has engaged a cybersecurity consultancy, ProSecure Assessments, to evaluate the security of its email communication systems. DataLink Solutions relies on an internal SMTP server to transmit email across its departments and with external clients. The organization is concerned about the possibility of attackers enumerating valid user accounts or delivery addresses from its SMTP server, which could lead to phishing campaigns or unauthorized access attempts.

**Solution**

As a Certified Ethical Hacker or penetration tester, your task is to perform SMTP enumeration using Nmap to identify potential vulnerabilities in the SMTP server configuration. This process will involve probing the SMTP server to discover valid email addresses, usernames, and message recipients by leveraging Nmap’s scripting capabilities. Specifically, you will use scripts like smtp-enum-users to query the server for information about its users and determine whether it leaks sensitive data.

You will connect to the SMTP server via one of its standard ports (TCP 25, 2525, or 587) and execute enumeration commands to validate user accounts and delivery addresses. The information gathered will be analyzed to assess whether the server exposes critical data that attackers could exploit to target employees or compromise the email system.

The Nmap scripting engine may be used to enumerate the target system’s SMTP service and acquire information about all user accounts on the SMTP server.

**Note:** In this lab, the target IP address we use is **192.168.56.106** of Windows Server 2025. Do not use this lab IP address. Use your virtual machine IP address at the time when you are performing this lab.

**Prerequisites:** Before starting this lab, install the SMTP Services on Windows Server 2025. Use the documentation provided below to install SMTP Services on Windows Server 2025.

**Documentation:** <https://phoenixnap.com/kb/windows-smtp-server>

|  |
| --- |
| 1. Turn on your **Windows Server 2025** and **PattotOS** virtual machines. Now, switch to the **ParrotOS** virtual machine. Open the **Terminal** and execute the following command: **sudo su** to run the programs as a root user. When prompted, enter your **root** password.    2. Execute the following command: **nmap -p 25 --script=smtp-enum-users [Target IP Address]**. The **-p** defines the port, while the **--script** argument runs a provided script, **smtp-enum-users**. The output shows a list of all potential mail users on the target system.    3. Execute the following command: **nmap -p 25 --script=smtp-open-relay [Target IP Address]**. The script we are using in this command is **smtp-open-relay**. The output shows a list of open SMTP relays on the target machine.    4. Execute the following command: **nmap -p 25 --script=smtp-commands [Target IP Address]**. The script we are using in this command is **smtp-commands.** A list of all SMTP commands found in the Nmap directory is displayed. You can further investigate the commands to find out more about the target host.    5. Using this information, attackers can launch password spraying attacks to obtain unauthorized access to user accounts. This concludes the lab on SMTP enumeration using Nmap. |

**Lab 7-07: Enumerate Information using Global Network Inventory**

**Scenario**

A financial technology company, FinEdge Solutions, has partnered with a cybersecurity firm, InfoSecure Analysts, to perform a thorough security assessment of its corporate network infrastructure. The company has a complicated infrastructure that includes Windows and Linux computers, file servers, database servers, and Active Directory services. While early enumeration attempts have shown useful results, FinEdge Solutions is worried that major vulnerabilities or misconfigurations may still be ignored without an in-depth investigation. To achieve complete network visibility, the company has requested the use of advanced enumeration techniques.

**Solution**

As a Certified Ethical Hacker or penetration tester, your task is to perform enumeration using the Global Network Inventory to gather extensive information about the target network's infrastructure. Global Network Inventory is an audit scanner in zero deployment and agentless settings. It searches one or more computers by IP range or domain, as specified in the Global Network Inventory host file.

This enumeration exercise can help in identifying hidden vulnerabilities that attackers may exploit, such as exposed services, outdated software, and misconfigured settings. The complete network inventory will also help to identify security weaknesses and prioritize actions to address them.

**Note:** In this lab, the target IP address we use is **192.168.56.106** of Windows Server 2025. Do not use this lab IP address. Use your virtual machine IP address at the time when you are performing this lab.

|  |
| --- |
| 1. Start your **Windows 11** and **Windows Server 25** virtual machines. Switch to a **Windows 11** virtual machine. Open any browser and type the following URL:[**https://magnetosoft.com/products-downloads/**](https://magnetosoft.com/products-downloads/). Click on the **Download Global Network Inventory** to download the executable file of Global Network Inventory. Then, navigate to the Downloads folder. Double-click on the **gni\_setup.exe**.    2. Click on the **Next >** button.    3. Select **I accept the terms in the license agreement** radio button. Click on the **Next >** button.    4. Click on the **Next >** button.    5. Click on the **Next >** button.    6. Click on the **Next >** button.    7. Click on the **Install** button.    8. Click on the **Finish** button.    9. Click on the **I Agree** button.    10. Click on the **Close** button.    11. Click on the **Next >** button.    12. Under the **Audit Scan Mode** section. Click on the **Single address scan** radio button. Then click on the **Next >** button.    13. Enter the target machine **IP address**. In this lab, we are targeting **Windows Server 2025.** Click on the **Next >** button.    14. Enter your **User name** and **Password**. Click on the **Next >** button.    15. Click on the **Finish** button.    16. The scan process will start; it will take a few minutes to complete.    17. After the scan is completed. The Scan summary of the scanned target IP address **192.168.56.106** appears    18. Hover your mouse cursor over the **Computer** details under the **Scan summary** tab to view the scan summary.    19. Click on the **Operating System** tab and hover the mouse cursor over **Windows details** to view the complete details of the machine.    20. Click on the **BIOS** tab and hover the mouse cursor over **Default System BIOS** to display detailed BIOS settings information    21. Click on the **NetBIOS** tab and hover the mouse cursor over any **NetBIOS application** to display the detailed NetBIOS information about the target.    22. Click on the **User groups** tab and hover the mouse cursor over any **username** to display detailed user group information.    23. Click on the **Users** tab and hover the mouse cursor over any **username** to view login details for the target machine.    24. Click on the **Services** tab and hover the mouse cursor over any **service** to view its details.    25. Click on the **Installed software** tab and hover the mouse cursor over any **software** to view its details.    26. Click the **Shares** tab and hover the mouse cursor over any **shared folder** to view its details.    27. Similarly, you can click other tabs such as **Computer System**, **Processors**, **Main board**, **Memory**, **SNMP systems,** and **Hot fixes**. Hover the mouse cursor over elements under each tab to see more information. |

**Lab 7-08: Perform Vulnerability Analysis using OpenVAS**

**Scenario**

PrimeNova, a regional financial services company, has suffered a severe computer and system breach. A hacker exploited a vulnerability in its customer management software, compromising all sensitive customer data, including account details and transaction history. The company heavily depends on its compliance reporting and customer relationship management software, which makes it a critical asset. In response to the incident, the company initiated a thorough investigation to discover and fix vulnerabilities in its computers and systems to prevent this type of attack in the future.

**Solution**

The company hires you as a Certified Ethical Hacker to perform a vulnerability analysis using advanced assessment tools. As an ethical hacker, your task is to simulate a real-world attack scenario to identify weaknesses in the computer systems. To achieve this, you use OpenVAS, a highly regarded open-source vulnerability scanner.

In this lab, you will systematically scan the company’s systems to identify vulnerabilities such as unpatched software, open ports, insecure configurations, and outdated services.

OpenVAS is a robust framework comprising multiple services and tools designed to deliver comprehensive vulnerability scanning and management solutions. It supports both unauthenticated and authenticated testing, as well as a variety of high-level and low-level internet and industrial protocols, and it optimizes performance for large-scale scanning. Additionally, it incorporates a versatile internal programming language for implementing custom vulnerability tests. The security scanner is supplemented by an updated feed of over 50,000 Network Vulnerability Tests (NVTs), ensuring thorough and up-to-date assessments.

The findings from the assessment will help the company prioritize and remediate critical vulnerabilities, strengthening its overall security posture.

**Note:** In this lab, the target IP address we use is **192.168.56.106** of Windows Server 2025. Do not use this lab IP address. Use your virtual machine IP address at the time when you are performing this lab.

|  |
| --- |
| 1. Start your **PattotOS** and **Windows Server 2025** virtual machines. Switch to ParrotOS and open the **Terminal**. Then, execute the **sudo su** command to run programs with root user privileges.    2. Execute the following command: **apt-get update && apt-get upgrade -y** to automatically update the package index and upgrade all installed packages to their latest versions.    3. Execute the following command: **apt-get install docker.io -y** to install Docker in ParrotOS.    4. Execute the following command: **docker run -d -p 443:443 –-name openvas mikesplain/openvas** to launch OpenVAS.    5. Open any browser in ParrotOS. Type the following **https://127.0.0.1/** to go to the OpenVAS login page. Log in with username and password **admin**/**admin**. Click on the **Login** button. If a **Warning page** appears. Then Click on the **Advanced.** Click on **Accept the Risk.** Then Click on the **Continue**.    6. The **OpenVAS** page appears. Click on the **Scans**. Then, Click on the **Tasks**. If you see a **Welcome to scan task management!** pop-up window, close it.    7. Hover over the **wand** icon. Then, click on the **Task Wizard**.    8. The **Task Wizard** window opens; enter the target machine **IP address** in the **IP address or hostname** field. Then, click on the **Start Scan** button.    9. The task will appear under the **Tasks** section, and OpenVAS will begin scanning the target IP address. Wait until the status changes from **Requested** to **Done**.  10. Once the scan is complete, click the **Done** button under the **Status** column to view the vulnerabilities detected in the target system. The scanning process may take some time.    11. Click on the **Scans.** Then Click on the **Results**.    12. The Results section lists the detected vulnerabilities, their severity, and the port numbers on which they operate. The results may vary when performing this task. Click on any vulnerability in the **Vulnerability** column to obtain more information.    13. Detailed information about the selected vulnerability will be displayed.    14. Now compare the results of the vulnerability assessment report of Windows Server 2025 by enabling Windows Firewall. Switch back to the **Windows Server 2025**. Go to the **Control Panel** **→** **System and Security** **→** **Windows Defender Firewall** **→** **Turn Windows Defender Firewall on or off**, and enable **Windows Defender Firewall**. Then click on the **OK** button, and after that, close the **Control Panel** window.    15. Repeat steps 6 to 9 again. Click on the **Scans.** Then Click on the **Reports**. The target machine’s scan results remain unchanged before and after enabling the Windows Firewall, indicating that the target system is still vulnerable to attack even with the firewall enabled. |