**DHCP Starvation Attack using Yersinia tool**

A DHCP Starvation Attack is a type of Denial-of-Service (DoS) attack that targets the Dynamic Host Configuration Protocol (DHCP) service. The goal of this attack is to exhaust the available IP addresses in the DHCP pool, preventing legitimate users from obtaining an IP address and thereby disrupting network connectivity.

**How the Attack Works**

1. The attacker floods the DHCP server with numerous fake DHCP request packets, each using a unique MAC address.
2. The DHCP server assigns an IP address to each fake request until the entire pool of IP addresses is exhausted.
3. Legitimate users are unable to obtain an IP address, causing a network outage for new clients.

**Walkthrough**

In this walkthrough, we'll perform a DHCP Starvation Attack using the Yersinia tool on Kali Linux. This attack exhausts a DHCP server’s pool of IP addresses, preventing legitimate users from obtaining IP addresses and causing a Denial of Service (DoS) on the network.

Requirements

1. Kali Linux (as the attacker machine)
2. Yersinia tool
3. Wireshark to capture and observe network traffic
4. Windows Machine (to test IP allocation failure)

1.Open Wireshark on Kali Linux

A screen shot of a computer

Description automatically generated

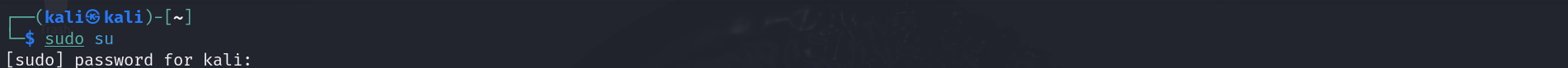
2.In Wireshark, select the primary network interface (here, eth0) to capture traffic.

A screenshot of a computer

Description automatically generated

3.. Open another Terminal Window on Kali.

4. Run as Root. Enter sudo su and provide the password **kali** if prompted, to switch to the root user.



5. Maximize the Terminal Window. Yersinia’s interactive mode works best in a maximized terminal.

6. Write the command to install yersinia.

**# yersinia**  
A screenshot of a computer

Description automatically generated  
If not install, press **Y** to install the tool.

7.To see the commands, write

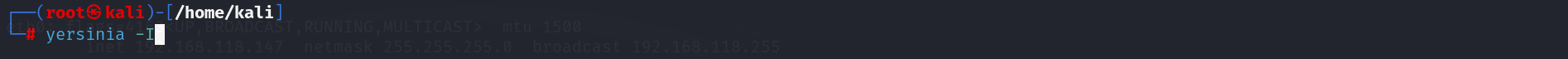
**# yersinia -h**

A black screen with white text

Description automatically generated

8. Launch Yersinia in Interactive Mode, see using help option,-I is responsibe for interactive mode.

**# yersinia -I**



9. Press any key to continue

A screenshot of a computer

Description automatically generated

10. Press F2. This switches Yersinia to DHCP mode. You’ll see DHCP options in the lower section of the terminal.

A screen shot of a computer

Description automatically generated

11.Press x to display the Attack Panel.

A screenshot of a computer screen

Description automatically generated

12.Press 1 to select the DHCP starvation attack.

A screenshot of a computer screen

Description automatically generated

13.Yersinia will now start sending a large number of DHCP requests to the network.

A screenshot of a computer screen

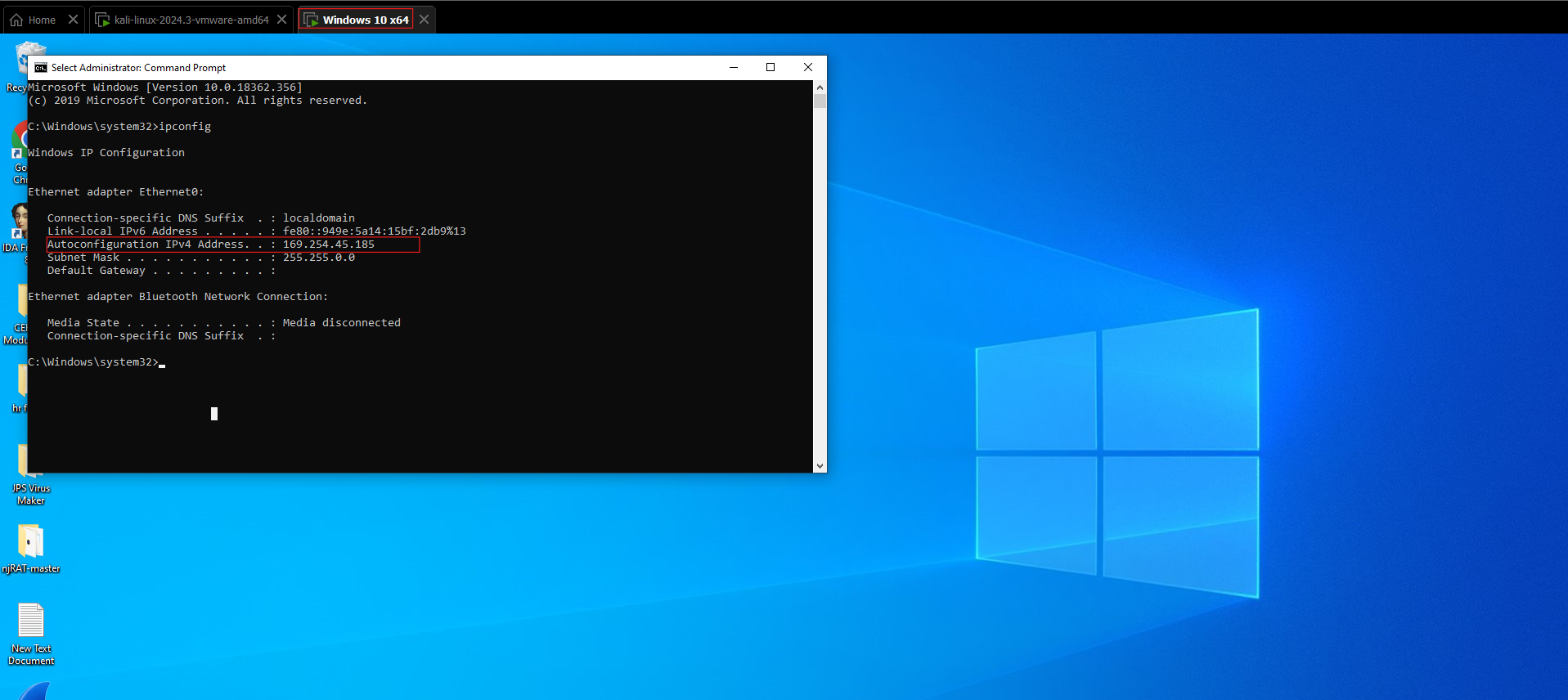
Description automatically generated

14. Switch to the Wireshark window. You should see a significant number of DHCP packets being captured, indicating that the attack is underway.

A screenshot of a computer

Description automatically generated

15. Stop the DHCP Starvation Attack. In Yersinia, press **q** to terminate the attack.  
  
16. Since the DHCP server’s IP address pool is exhausted, the Windows machine will be unable to obtain an IP address from the DHCP server. Instead, it will assign itself an APIPA (Automatic Private IP Addressing) address, such as 169.254.45.185.



This demonstrates a successful DHCP starvation attack.

**Summary Points**

1. **Goal**: To exhaust the DHCP server’s IP pool, preventing new devices from obtaining IP addresses.
2. **Tools Used**: Yersinia for DHCP starvation, Wireshark for traffic monitoring.
3. **Key Steps**:
   1. Start Wireshark to capture DHCP packets.
   2. Launch Yersinia in interactive mode on Kali.
   3. Select DHCP mode and initiate the DHCP starvation attack.
   4. Stop the attack and close Yersinia and Wireshark.
   5. Add a Windows machine to observe IP allocation failure due to APIPA assignment (e.g., 169.254.45.185).