Lab 2: Detect Session Hijacking

Lab Scenario

Session hijacking is very dangerous; it places the victim at risk of identity theft, fraud, and loss of sensitive information. All networks that use TCP/IP are vulnerable to different types of hijacking attacks. Moreover, these kinds of attacks are very difficult to detect, and often go unnoticed unless the attacker causes severe damage. However, following best practices can protect against session hijacking attacks.

As a professional ethical hacker or penetration tester, it is very important that you have the required knowledge to detect session hijacking attacks and protect your organization's system against them. Fortunately, there are various tools available that can help you to detect session hijacking attacks such as packet sniffers, IDSs, and SIEMs.

Lab Objectives

- Detect session hijacking using Wireshark

Overview of Detecting Session Hijacking

There are two primary methods that can be used to detect session hijacking:

- **Manual Method**: Involves using packet sniffing software such as Wireshark to monitor session hijacking attacks; the packet sniffer captures packets being transferred across the network, which are then analyzed using various filtering tools
- **Automatic Method**: Involves using Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to monitor incoming network traffic; if a packet matches any of the attack signatures in the internal database, the IDS generates an alert, and the IPS blocks the traffic from entering the database

Task 1: Detect Session Hijacking using Wireshark

Wireshark allows you to capture and interactively browse the traffic running on a network. The tool uses WinPcap to capture packets, and so is only able to capture packets on networks that are supported by WinPcap. It captures live network traffic from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, and FDDI networks. Security professionals can use Wireshark to monitor and detect session hijacking attempts.

Here, we will use the Wireshark tool to detect session hijacking attacks manually on the target system.

We will use the **Parrot Security** (**10.10.1.13**) machine to carry out a session hijacking attack on the **Windows 11** (**10.10.1.11**) machine.

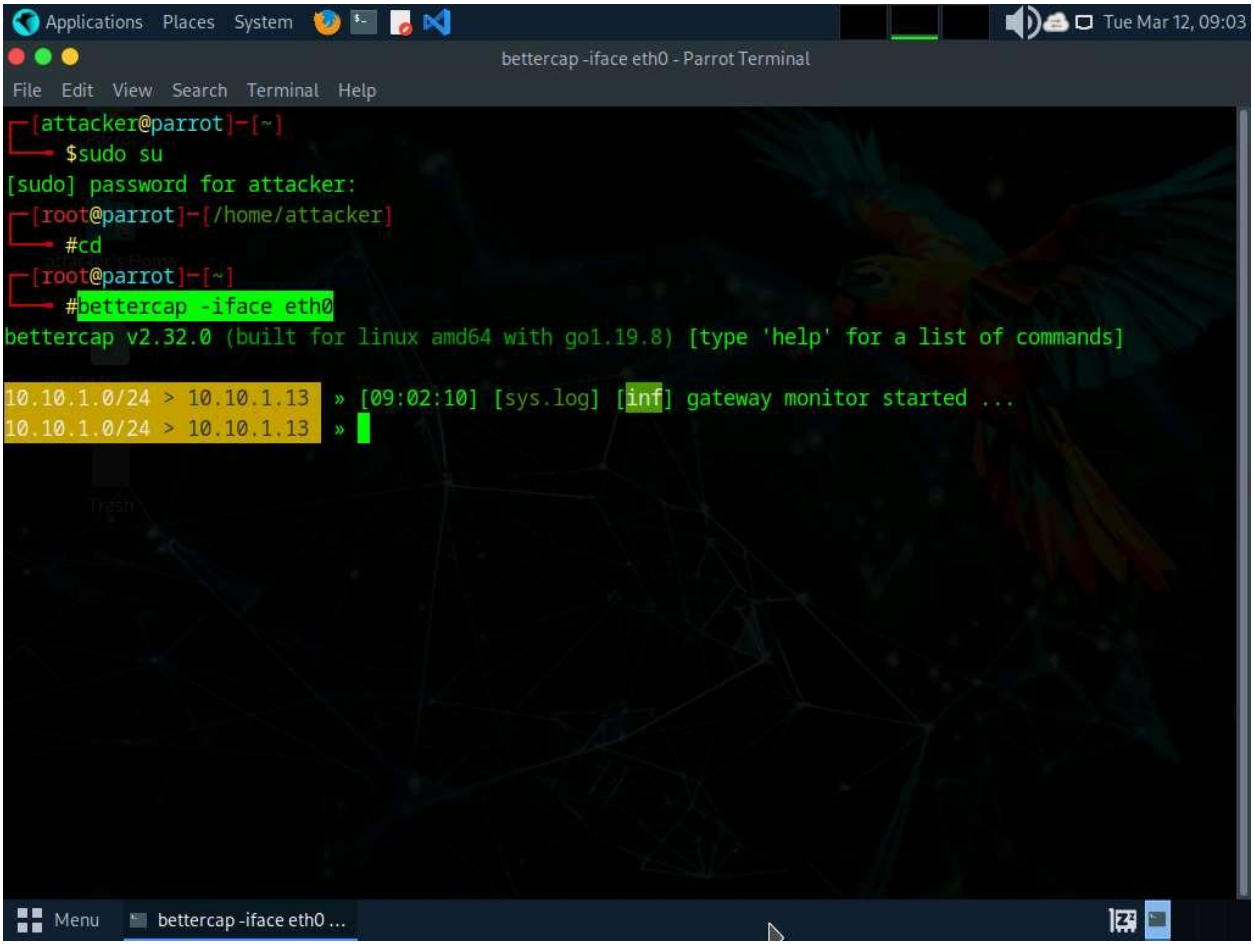
1. Click Windows 11 to switch to the **Windows 11** machine.
2. Click the windows **Search** icon on the **Desktop**, search for **Wireshark** in the search bar and launch it.
3. **The Wireshark Network Analyzer** window appears, start capturing the network traffic on the primary network interface (here, **Ethernet**).

4. Now, we shall launch a session hijacking attack on the target machine (**Windows 11**) using **bettercap**.

To do so, you may either follow Steps **8-11** below, or refer to Task 2 (Intercept HTTP Traffic using bettercap) in Lab 1.

5. Click Parrot Security to switch to the **Parrot Security** machine.
6. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**). Run **cd** to jump to the root directory.
7. Run **bettercap -iface eth0** to set the network interface.

-iface: specifies the interface to bind to (here, **eth0**).

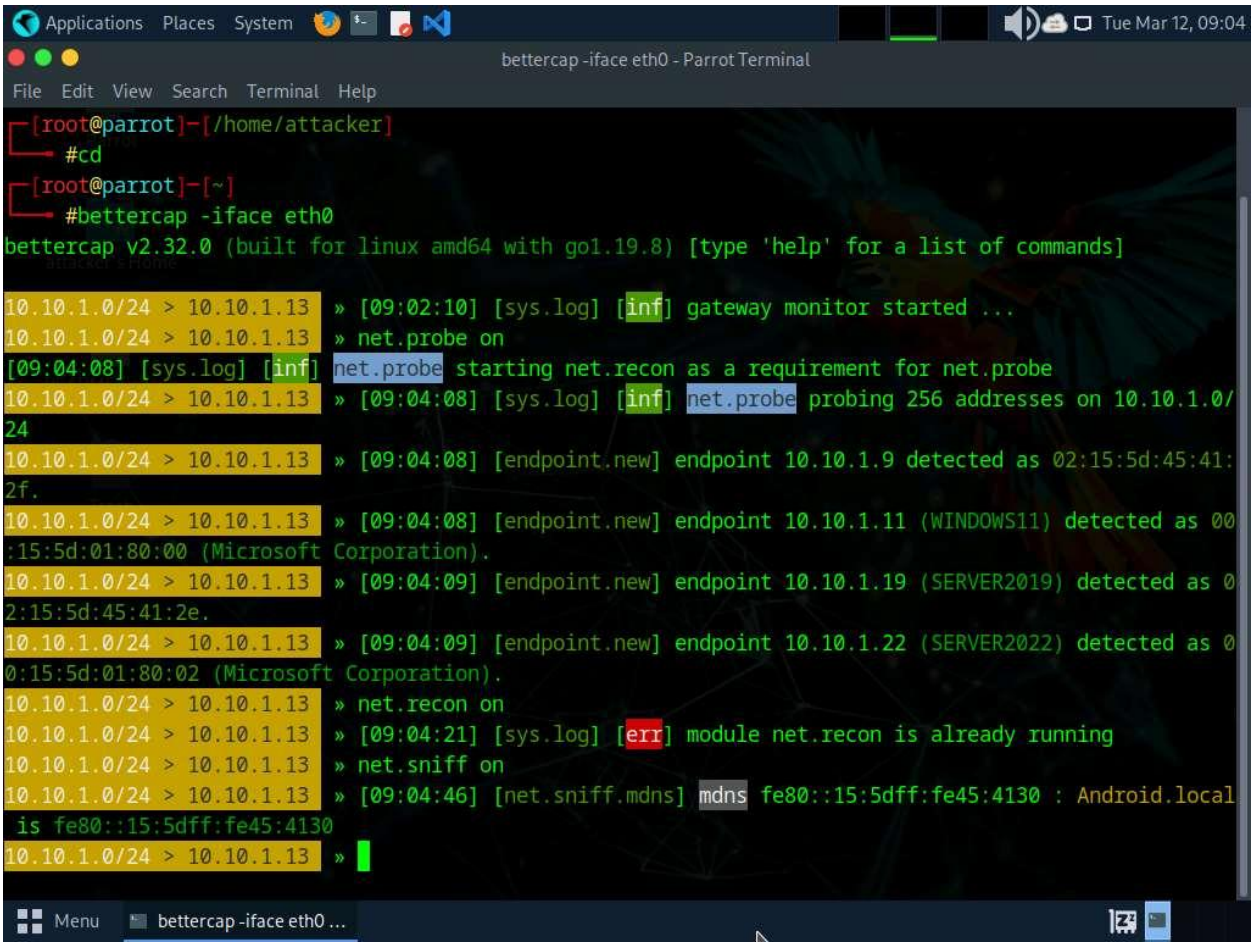


8. Type **net.probe on** and press **Enter**. This module will send different types of probe packets to each IP in the current subnet for the **net.recon** module to detect them.
9. Type **net.recon on** and press **Enter**. This module is responsible for periodically reading the system ARP table to detect new hosts on the network.

The net.recon module displays the detected active IP addresses in the network. In real-time, this module will start sniffing network packets.

10. Type **net.sniff on** and press **Enter**. This module is responsible for performing sniffing on the network.

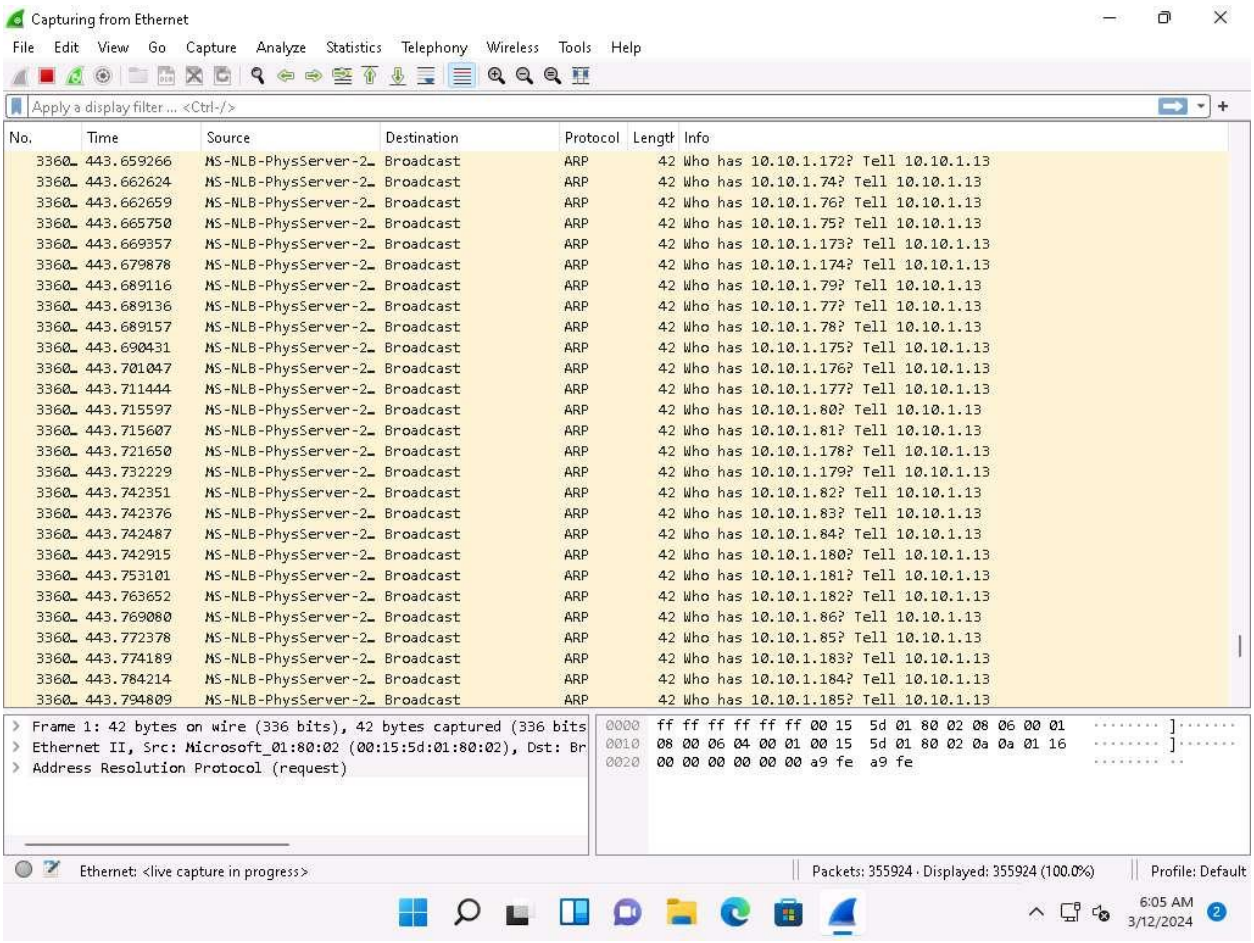
11. You can observe that bettercap starts sniffing network traffic on different machines in the network, as shown in the screenshot.



12. Click Windows 11 to switch back to the **Windows 11** machine and observe the huge number of **ARP packets** captured by the **Wireshark**, as shown in the screenshot.

bettercap sends several ARP broadcast requests to the hosts (or potentially active hosts). A high number of ARP requests indicates that the system at **10.10.1.13** (the attacker's system in this task) is acting as a client for all the IP addresses in the subnet, which means that all the packets from the victim node (in this case, **10.10.1.11**) will first go to the host system (**10.10.1.13**), and then the gateway. Similarly, any packet destined for the victim node is first forwarded from the gateway to the host system, and then from the host system to the victim node.

more...



13. This concludes the demonstration of how to detect a session hijacking attack using Wireshark.
14. Close all open windows and document all the acquired information.

Question 11.2.1.1

Use the bettercap tool (available in the Parrot Security machine) to sniff the traffic on the target system (10.10.1.11). Use the Wireshark tool on the target system (10.10.1.11) to detect the session hijacking attempt. Traffic on which protocol indicates the session hijacking attempt in Wireshark?