

—(kaliⓀkali)-[~/Desktop/project/project_SOC]

—\$ bash combined.sh

[!] This script must be run as root. Please switch to root and try again.

—(kaliⓀkali)-[~/Desktop/project/project_SOC]

—\$ █

```
(root@kali)-[/home/kali/Desktop/project/project_SOC]
# bash combined.sh
```

```
Welcome to the SOC Monitoring
and Attack Simulation Tool
```

```
A Comprehensive Security Operations
Center (SOC) Project
```

```
Monitor, Analyze, and Simulate Cyber Threats
to Strengthen Your Network
```

```
Author: Yechiel Said
Version: 1.0
Developed for: Advanced SOC Projects
```

```
Main Menu
```

1. main_attacks - Access the Attack Simulation Menu
 2. main_monitor - Access the Monitoring Menu
 3. Exit - Exit the Program
-
-

```
Enter your choice: █
```

Enter your choice: 1
Redirecting to Attack Simulation Menu ...

Multi-Attack Simulation Script

[+] Your machine's IP: 192.168.189.166

Installing Dependencies

[+] Your machine's IP: 192.168.189.166

Installing Dependencies

[+] nmap is already installed.

[+] hydra is already installed.

[+] masscan is already installed.

[+] msfconsole is already installed.

[+] hping3 is already installed.

[+] arpspoof is already installed.

[+] sslstrip is already installed.

[+] tor is already installed.

[+] macchanger is already installed.

[+] curl is already installed.

[#] Installing geoip-bin...

[+] geoip-bin installed.

[*] All dependencies are installed.

Attack Options

- 1 - DDoS Attack
- 2 - DNS Amplification
- 3 - MITM Attack
- 4 - Discover Network IPs
- 99 - Exit

[!] Choose an option:
Enter your choice:

Attack Options

- 1 - DDoS Attack
- 2 - DNS Amplification
- 3 - MITM Attack
- 4 - Discover Network IPs
- 99 - Exit

[!] Choose an option:
Enter your choice: 1

DDoS Attack

Enter target IP for DDoS:

DDoS Attack

Enter target IP for DDoS: 192.168.189.149
[+] Attack logged: DDoS on 192.168.189.149

hping in flood mode, no replies will be shown

Capturing from Ethernet0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help



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

No.	Time	Source	Destination	Protocol	Length	Info
2154...	49.286673	192.168.189.166	192.168.189.149	UDP	60	28382 → 80 Len=0
2154...	49.287037	192.168.189.166	192.168.189.149	UDP	60	28383 → 80 Len=0
2154...	49.287037	192.168.189.166	192.168.189.149	UDP	60	28384 → 80 Len=0
2154...	49.287037	192.168.189.166	192.168.189.149	UDP	60	28385 → 80 Len=0
2154...	49.287037	192.168.189.166	192.168.189.149	UDP	60	28386 → 80 Len=0
2154...	49.287468	192.168.189.166	192.168.189.149	UDP	60	28387 → 80 Len=0
2154...	49.287468	192.168.189.166	192.168.189.149	UDP	60	28388 → 80 Len=0
2154...	49.287468	192.168.189.166	192.168.189.149	UDP	60	28389 → 80 Len=0
2154...	49.287468	192.168.189.166	192.168.189.149	UDP	60	28390 → 80 Len=0
2154...	49.287468	192.168.189.166	192.168.189.149	UDP	60	28391 → 80 Len=0
2154...	49.287468	192.168.189.166	192.168.189.149	UDP	60	28392 → 80 Len=0
2154...	49.287566	192.168.189.166	192.168.189.149	UDP	60	28393 → 80 Len=0
2154...	49.287566	192.168.189.166	192.168.189.149	UDP	60	28394 → 80 Len=0
2154...	49.287651	192.168.189.166	192.168.189.149	UDP	60	28395 → 80 Len=0
2154...	49.287651	192.168.189.166	192.168.189.149	UDP	60	28396 → 80 Len=0
2154...	49.287736	192.168.189.166	192.168.189.149	UDP	60	28397 → 80 Len=0

> Frame 1: 125 bytes on wire (1000 bits), 125 bytes captured (1000 bits) on interface \Device\NPF_{0EF99F39-27B7-4329-B3...}

> Ethernet II, Src: VMware_c0:00:08 (00:50:56:c0:00:08), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

> Internet Protocol Version 4, Src: 192.168.189.1, Dst: 255.255.255.255

> User Datagram Protocol, Src Port: 10004, Dst Port: 10004

> Data (83 bytes)

```

0000  ff ff ff ff ff ff 00 50 56 c0 00 08 08 00 45 00  .....P V.....E
0010  00 6f c8 d2 00 00 80 11 f4 01 c0 a8 bd 01 ff ff  .o.....
0020  ff ff 27 14 27 14 00 5b 30 dc 3c 58 4d 4c 3e 3c  ..'..'..[ 0-<XML><
0030  50 61 63 6b 65 74 54 79 70 65 3e 52 65 71 75 65  PacketTy pe>Reque
0040  73 74 3c 2f 50 61 63 6b 65 74 54 79 70 65 3e 0a  st</Pack etType>-
0050  3c 50 72 6f 64 75 63 74 4e 61 6d 65 3e 41 50 47  <Product Name>APG
0060  20 41 74 77 6f 6f 64 3c 2f 50 72 6f 64 75 63 74  Atwood< /Product
0070  4e 61 6d 65 3e 0a 3c 2f 58 4d 4c 3e 0a  Name>-</ XML>-

```

Ethernet0: <live capture in progress>

Packets: 215464 · Displayed: 215464 (100.0%)

Profile: Default

- 1 - DDoS Attack
- 2 - DNS Amplification
- 3 - MITM Attack
- 4 - Discover Network IPs
- 99 - Exit

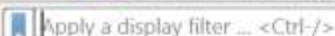
[!] Choose an option:
Enter your choice: 2

DNS Amplification Attack

Enter target DNS server IP: 192.168.189.149



[+] Attack logged: DNS Amplification on 192.168.189.149

[main] memlockall(): No such file or directory
Warning: can't disable memory paging!
ping in flood mode, no replies will be shown



```
0000 00 50 56 ed 0e f4 00 0c 29 c4 16 22 08 00 45 00 .PV....)..."E
0010 00 3f 5d d1 00 00 80 11 00 00 c0 a8 bd 95 c0 a8 .?].....
0020 bd 02 c5 9e 00 35 00 2b fc 25 63 67 01 00 00 01 .....5+.%cg...
0030 00 00 00 00 00 00 03 77 77 77 09 77 69 72 65 73 .....w ww-wires
0040 68 61 72 6b 03 6f 72 67 00 00 01 00 01 hark.org .....
```

Packets: 31427 · Displayed: 31427 (100.0%)

  Type here to search



9:11 PM
1/21/2025

MITM Attack

Enter victim IP: 192.168.189.149

Enter gateway IP: 192.168.189.2

[+] Attack logged: MITM on 192.168.189.149

[+] MITM attack in progress. Capturing traffic...

0:c:29:63:dc:c8 0:c:29:c4:16:22 0806 42: arp reply 192.168.189.2 is-at 0:c:29:63:dc:c8

tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes

0:c:29:63:dc:c8 0:c:29:c4:16:22 0806 42: arp reply 192.168.189.2 is-at 0:c:29:63:dc:c8



arp.duplicate-address-detected

No.	Time	Source	Destination	Protocol	Length	Info
174	79.418579	VMware_ed:0e:f4	Broadcast	ARP	60	Who has 192.168.189.166? Tell 192.168.189.2 (duplicate use of 192.168.189.2 detected!)
175	79.418579	VMware_63:dc:d2	VMware_ed:0e:f4	ARP	60	192.168.189.166 is at 00:0c:29:63:dc:d2 (duplicate use of 192.168.189.2 detected!)
177	79.419304	VMware_63:dc:c8	VMware_ed:0e:f4	ARP	60	192.168.189.166 is at 00:0c:29:63:dc:c8 (duplicate use of 192.168.189.2 detected!)

> Frame 177: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{0EF99F39-27B7-4329-B375-...} ...

> Ethernet II, Src: VMware_63:dc:c8 (00:0c:29:63:dc:c8), Dst: VMware_ed:0e:f4 (00:50:56:ed:0e:f4) ...

> Address Resolution Protocol (reply) ...

> [Duplicate IP address detected for 192.168.189.166 (00:0c:29:63:dc:c8) - also in use by 00:0c:29:63:dc:d2 (frame 175)] ...

> [Duplicate IP address detected for 192.168.189.2 (00:50:56:ed:0e:f4) - also in use by 00:0c:29:63:dc:c8 (frame 153)] ...

0000 00 50 56 ed 0e f4 00 0c 29 63 dc c8 08 06 00 01 -PV-....)c-....

0010 08 00 06 04 00 02 00 0c 29 63 dc c8 c0 a8 bd a6)c-....

0020 00 50 56 ed 0e f4 c0 a8 bd 02 00 00 00 00 00 00 -PV-....

0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

- 2 - DNS Amplification
- 3 - MITM Attack
- 4 - Discover Network IPs
- 99 - Exit

[!] Choose an option:
Enter your choice: 4

Network Discovery

[*] Scanning the network for live IPs ...

[+] Found IPs on the network:

- 192.168.189.1
- 192.168.189.2
- 192.168.189.149
- 192.168.189.254
- 192.168.189.145
- 192.168.189.166

Main Menu

1. main_attacks - Access the Attack Simulation Menu
 2. main_monitor - Access the Monitoring Menu
 3. Exit - Exit the Program
-
-

Enter your choice: 2

Redirecting to Monitoring Menu ...

Main Menu

1. Display IP Addresses
2. Attack Monitoring
3. Exit

Enter your choice: 1

Displaying IP Addresses

Select the action for displaying IP addresses:

1. Display IP addresses from auth.log
2. Display IP addresses from the local network
3. Exit

Enter your choice:

Displaying IP Addresses

Select the action for displaying IP addresses:

1. Display IP addresses from auth.log
2. Display IP addresses from the local network
3. Exit

Enter your choice: 1

192.168.1.100

192.168.1.101

192.168.1.102

192.168.1.103

192.168.1.104

192.168.1.105

192.168.1.106

192.168.1.107

192.168.1.108

Main Menu

1. Display IP Addresses
2. Attack Monitoring
3. Exit

Enter your choice: 2

Attack Monitoring Menu

1. SSH Attack Monitoring
2. SMB Attack Monitoring
3. FTP Attack Monitoring
4. HTTP Attack Monitoring
5. System Events Monitoring
6. Display All Possible Attacks with Descriptions
7. Choose a Target or Random IP
8. Exit

Enter your choice:

Attack Monitoring Menu

1. SSH Attack Monitoring
2. SMB Attack Monitoring
3. FTP Attack Monitoring
4. HTTP Attack Monitoring
5. System Events Monitoring
6. Display All Possible Attacks with Descriptions
7. Choose a Target or Random IP
8. Exit

Enter your choice: 6

List of Possible Attacks & Descriptions

1. SSH Login Attempts: Tracks accepted and failed login attempts for SSH.
2. SMB Login Events: Detects valid and invalid SMB session attempts.
3. FTP Login Events: Monitors FTP logins and errors.
4. HTTP Attacks: Identifies brute-force attacks and suspicious user agents.
5. System Events: Logs authentication failures and unauthorized access.

-
-
1. SSH Attack Monitoring
 2. SMB Attack Monitoring
 3. FTP Attack Monitoring
 4. HTTP Attack Monitoring
 5. System Events Monitoring
 6. Display All Possible Attacks with Descriptions
 7. Choose a Target or Random IP
 8. Exit

Enter your choice: 1

Monitoring SSH login events

No activity for 30 seconds. Stopping SSH login events monitoring ...

Attack Monitoring Menu

1. SSH Attack Monitoring
2. SMB Attack Monitoring
3. FTP Attack Monitoring
4. HTTP Attack Monitoring
5. System Events Monitoring
6. Display All Possible Attacks with Descriptions
7. Choose a Target or Random IP
8. Exit

Enter your choice: 2

Monitoring SMB login events

[SMB login events Event] Jan 16 12:41:30 server smbd[23457]: session closed for user1 from 192.168.1.103

[SMB login events Event] [SMB login events Event] Jan 16 12:41:30 server smbd[23457]: session closed for user1 from 192.168.1.103

No activity for 30 seconds. Stopping SMB login events monitoring...

Attack Monitoring Menu

1. SSH Attack Monitoring
2. SMB Attack Monitoring
3. FTP Attack Monitoring
4. HTTP Attack Monitoring
5. System Events Monitoring
6. Display All Possible Attacks with Descriptions
7. Choose a Target or Random IP
8. Exit

Enter your choice: 3

Monitoring FTP login events

```
[FTP login events Event] Jan 16 12:50:01 server ftpd[34567]: Failed login for user anonymous from 192.168.1.104
[FTP login events Event] [FTP login events Event] Jan 16 12:50:01 server ftpd[34567]: Failed login for user anonymous from 192.168.1.104
[FTP login events Event] Jan 16 12:52:15 server ftpd[34568]: Login successful for user admin from 192.168.1.105
[FTP login events Event] [FTP login events Event] Jan 16 12:52:15 server ftpd[34568]: Login successful for user admin from 192.168.1.105
```

No activity for 30 seconds. Stopping FTP login events monitoring...

```
Enter your choice: 4
```

```
Monitoring HTTP events install required tools
=====
DEPENDENCIES:

```

```
[HTTP events Event] Jan 16 13:00:42 server httpd[45678]: GET /admin HTTP/1.1 403 192.168.1.106
[HTTP events Event] [HTTP events Event] Jan 16 13:00:42 server httpd[45678]: GET /admin HTTP/1.1 403 192.168.1.106
[HTTP events Event] Jan 16 13:01:05 server httpd[45679]: User-Agent: suspicious-bot detected from 192.168.1.107
[HTTP events Event] [HTTP events Event] Jan 16 13:01:05 server httpd[45679]: User-Agent: suspicious-bot detected from 192.168.1.107
```


Attack Monitoring Menu

1. SSH Attack Monitoring
2. SMB Attack Monitoring
3. FTP Attack Monitoring
4. HTTP Attack Monitoring
5. System Events Monitoring
6. Display All Possible Attacks with Descriptions
7. Choose a Target or Random IP
8. Exit

Enter your choice: 5

Monitoring System events

```
[SMB login events Event] Jan 16 12:41:30 server smbd[23457]: session closed for user1 from 192.168.1.103
[System events Event] [SMB login events Event] Jan 16 12:41:30 server smbd[23457]: session closed for user1 from 192.168.1.103
[FTP login events Event] Jan 16 12:50:01 server ftpd[34567]: Failed login for user anonymous from 192.168.1.104
[System events Event] [FTP login events Event] Jan 16 12:50:01 server ftpd[34567]: Failed login for user anonymous from 192.168.1.104
[FTP login events Event] Jan 16 12:52:15 server ftpd[34568]: Login successful for user admin from 192.168.1.105
[System events Event] [FTP login events Event] Jan 16 12:52:15 server ftpd[34568]: Login successful for user admin from 192.168.1.105
[HTTP events Event] Jan 16 13:00:42 server httpd[45678]: GET /admin HTTP/1.1 403 192.168.1.106
[System events Event] [HTTP events Event] Jan 16 13:00:42 server httpd[45678]: GET /admin HTTP/1.1 403 192.168.1.106
[HTTP events Event] Jan 16 13:01:05 server httpd[45679]: User-Agent: suspicious-bot detected from 192.168.1.107
```


3. FIP Attack Monitoring
4. HTTP Attack Monitoring
5. System Events Monitoring
6. Display All Possible Attacks with Descriptions
7. Choose a Target or Random IP
8. Exit

Enter your choice: 7

Choose Target IP

Do you want to select from auth.log or local network? [auth/local]: auth

Available IPs:

192.168.1.100
192.168.1.101
192.168.1.102
192.168.1.103
192.168.1.104
192.168.1.105
192.168.1.106
192.168.1.107
192.168.1.108

Enter a target IP from the list or type 'random' to select a random IP:

Choose Target IP

Do you want to select from auth.log or local network? [auth/local]: auth

Available IPs:

192.168.1.100

192.168.1.101

192.168.1.102

192.168.1.103

192.168.1.104

192.168.1.105

192.168.1.106

192.168.1.107

192.168.1.108

Enter a target IP from the list or type 'random' to select a random IP: 192.168.1.103

Selected IP: 192.168.1.103

192.168.1.108

Randomly selected IP: 192.168.1.104

2025-01-18 14:53:46 - Attack detected for 192.168.1.104

2025-01-18 15:01:35 - Selected: Choose a Target or Random IP

2025-01-18 15:01:49 - SSH Attack - Target: 192.168.1.100 - Log Source: auth.log

2025-01-18 15:01:49 - SMB Attack - Target: 192.168.1.100 - Log Source: auth.log

2025-01-18 15:01:49 - FTP Attack - Target: 192.168.1.100 - Log Source: auth.log

2025-01-18 15:02:04 - Selected: Choose a Target or Random IP

2025-01-18 15:02:29 - Selected: SSH Attack Monitoring

2025-01-18 15:03:06 - Selected: SMB Attack Monitoring

2025-01-18 15:03:47 - Selected: FTP Attack Monitoring

2025-01-18 15:04:29 - Exiting program

2025-01-18 15:11:02 - Selected: HTTP Attack Monitoring

2025-01-18 15:11:40 - Selected: System Events Monitoring

2025-01-18 15:12:17 - Selected: Choose a Target or Random IP

2025-01-18 15:12:42 - SSH Attack - Target: 192.168.1.105 - Log Source: auth.log

2025-01-18 15:12:42 - SMB Attack - Target: 192.168.1.105 - Log Source: auth.log

2025-01-18 15:12:42 - FTP Attack - Target: 192.168.1.105 - Log Source: auth.log

2025-01-18 15:12:52 - Exiting program

2025-01-19 10:14:30 - Selected: Display All Possible Attacks with Descriptions

2025-01-19 10:14:53 - Selected: Choose a Target or Random IP

2025-01-19 10:15:05 - SSH Attack - Target: 192.168.1.101 - Log Source: auth.log

2025-01-19 10:15:05 - SMB Attack - Target: 192.168.1.101 - Log Source: auth.log

2025-01-19 10:15:05 - FTP Attack - Target: 192.168.1.101 - Log Source: auth.log

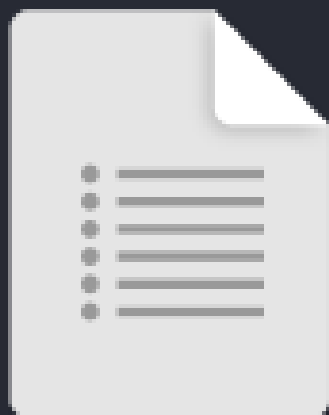
2025-01-19 10:16:04 - Exiting program

2025-01-19	10:56:31	- Attack: DDoS, Target: #!/bin/bash
2025-01-19	10:56:49	- Attack: DDoS, Target: 192.168.189.149
2025-01-19	10:57:51	- Attack: DNS Amplification, Target: 192.168.189.149
2025-01-19	10:59:32	- Attack: MITM, Target: 192.168.189.149
2025-01-19	11:22:22	- Attack: DDoS, Target: 192.168.189.149
2025-01-19	11:23:50	- Attack: DNS Amplification, Target: 192.168.189.149
2025-01-19	11:25:16	- Attack: MITM, Target: 192.168.189.149
2025-01-20	10:15:48	- Attack: MITM, Target: 192.168.189.149
2025-01-20	10:19:16	- Attack: DDoS, Target: 192.168.189.149
2025-01-20	10:20:07	- Attack: DNS Amplification, Target: 192.168.189.149
2025-01-20	15:10:25	- Attack: DDoS, Target: 192.168.189.149
2025-01-20	15:23:54	- Attack: DDoS, Target: 192.168.189.149
2025-01-20	15:24:36	- Attack: DNS Amplification, Target: 192.168.189.149
2025-01-20	15:25:11	- Attack: MITM, Target: 192.168.189.149
2025-01-21	15:07:59	- Attack: DDoS, Target: 192.168.189.149
2025-01-21	15:11:06	- Attack: DNS Amplification, Target: 192.168.189.149
2025-01-21	15:12:35	- Attack: MITM, Target: 192.168.189.149
2025-01-21	15:18:18	- Attack: MITM, Target: 192.168.189.149
2025-01-21	15:19:43	- Attack: MITM, Target: 192.168.189.149

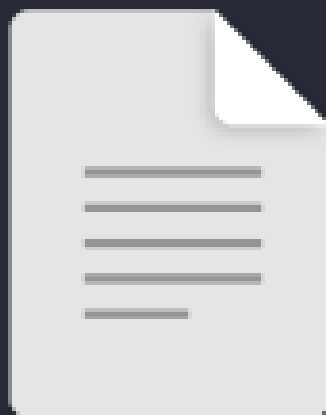




soc_results



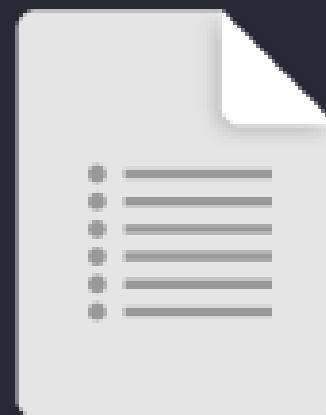
ftp_activity.log



report.txt



smb_activity.log



ssh_activity.log

noapis.sh ^

example.sh ^

alexem.sh ^

FT_vuln.sh ^

new.s

```
1 - FTP attack detected for 192.168.1.101
2 - FTP attack detected for 192.168.1.100
3 [FTP login events - FTP attack detected for 192.168.1.105
4 - FTP attack detected for 192.168.1.101
5 [FTP login events - FTP attack detected for 192.168.1.104
6
```

◀ exemple.sh × aiexem.sh × PT_Vuln.sh × new.sh ▶

```
1 - SMB attack detected for 192.168.1.101
2 - SMB attack detected for 192.168.1.100
3 - SMB attack detected for 192.168.1.105
4 - SMB attack detected for 192.168.1.101
5 - SMB attack detected for 192.168.1.104
6
```

PI_vuln.sn x new.sn x attack2.sn x combined.sn x combal.sn x

```
1 [SSH login events - SSH attack detected for 192.168.1.101
2 [SSH login events - SSH attack detected for 192.168.1.100
3   - SSH attack detected for 192.168.1.105
4 [SSH login events - SSH attack detected for 192.168.1.101
5   - SSH attack detected for 192.168.1.104
6
```



```
1 Main Menu:
2 1. Monitor Attacks
3 2. Display IP Addresses
4 3. Exit
5 Select the attack type to monitor:
6 1. SSH Attack Monitoring
7 2. SMB Attack Monitoring
8 3. FTP Attack Monitoring
9 4. Display All Possible Attacks with Descriptions
10 5. Choose a Target or Random IP
11 6. Exit
12 List of Possible Attacks with Descriptions from auth.log:
13 1. Failed SSH Login Attempts: Unauthorized attempts to access the system using SSH.
14 2. Accepted SSH Connections: Successful SSH logins indicating potential insider activity or legitimate access.
15 3. Invalid Usernames: Attempts to access the system using non-existent usernames.
16 4. Open and Close Sessions: Tracking session lifecycle for audit or anomaly detection.
17 5. IP Address Monitoring: Identifying suspicious or repeated IP addresses attempting access.
18 Main Menu:
19 1. Monitor Attacks
20 2. Display IP Addresses
21 3. Exit
22 Select the attack type to monitor:
23 1. SSH Attack Monitoring
24 2. SMB Attack Monitoring
25 3. FTP Attack Monitoring
26 4. Display All Possible Attacks with Descriptions
27 5. Choose a Target or Random IP
28 6. Exit
29 Monitoring SSH login events... Description: Detecting specific keywords like 'Failed', 'Accepted', or IP patterns in SSH logs.
30 Main Menu:
31 1. Monitor Attacks
32 2. Display IP Addresses
33 3. Exit
34 Select the attack type to monitor:
35 1. SSH Attack Monitoring
36 2. SMB Attack Monitoring
37 3. FTP Attack Monitoring
38 4. Display All Possible Attacks with Descriptions
39 5. Choose a Target or Random IP
40 6. Exit
```