Projeto 4 Diogo Antunes 2018016615

Ataque A: Arp Poisoning Attack

CVE-1999-0667

O CVE-1999-0667 descreve uma falha no protocolo ARP (Address Resolution Protocol), que pode ser explorada por invasores para manipular a comunicação dentro de uma rede. Essa vulnerabilidade permite que um atacante envie mensagens ARP falsas, enganando os dispositivos para que associem o endereço IP de um alvo ao seu próprio endereço MAC. Como resultado, o tráfego de rede pode ser interceptado, redirecionado ou até bloqueado, facilitando ataques como Man-in-the-Middle (MITM), roubo de informações e negação de serviço (DoS). Este CVE não possui CVSS Score, pois este fou«i registado em 1999 o CVSS apenas foi criado em 2005.

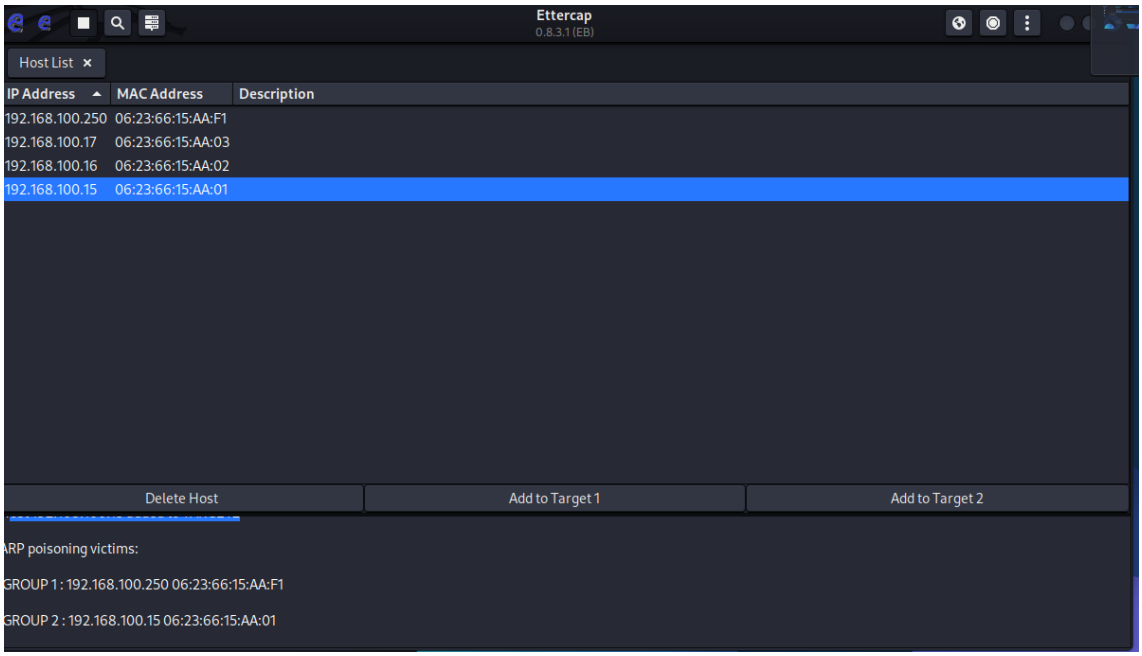
Ataque Arp Poisoning

É um ataque que explora vulnerabilidades no protocolo ARP (Address Resolution Protocol), permitindo que um invasor intercepte, modifique ou redirecione o tráfego de rede entre dispositivos em uma LAN (Local Area Network). Primeiramente o atacante monitora o tráfego ARP, para identificar os dispositivos da Rede, enviando para eles pacotes ARP “envenenados”, informando que o endereço MAC da sua máquina corresponde ao endereço IP do gateway da rede ou de outros dispositivos. As vitimas atualizam as suas tabelas ARP com as informações falsas e passam a enviar pacotes para o invasor.

Para realizar este ataque vou utilizar a ferramenta Ettercap.

```
root@TA1:~# arp -a
? (192.168.100.100) at 00:0c:29:cf:bd:d5 [ether] on eth0
? (192.168.100.250) at 06:23:66:15:aa:f1 [ether] on eth0
root@TA1:~#
```

```
R1-6615#sh arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.100.15           1   0623.6615.aa01  ARPA   Ethernet0/0
Internet  192.168.100.100          0   000c.29cf.bdd5  ARPA   Ethernet0/0
Internet  192.168.100.250          -   0623.6615.aaf1  ARPA   Ethernet0/0
Internet  192.168.200.251          -   0623.6615.bbf1  ARPA   Ethernet0/1
R1-6615#
```

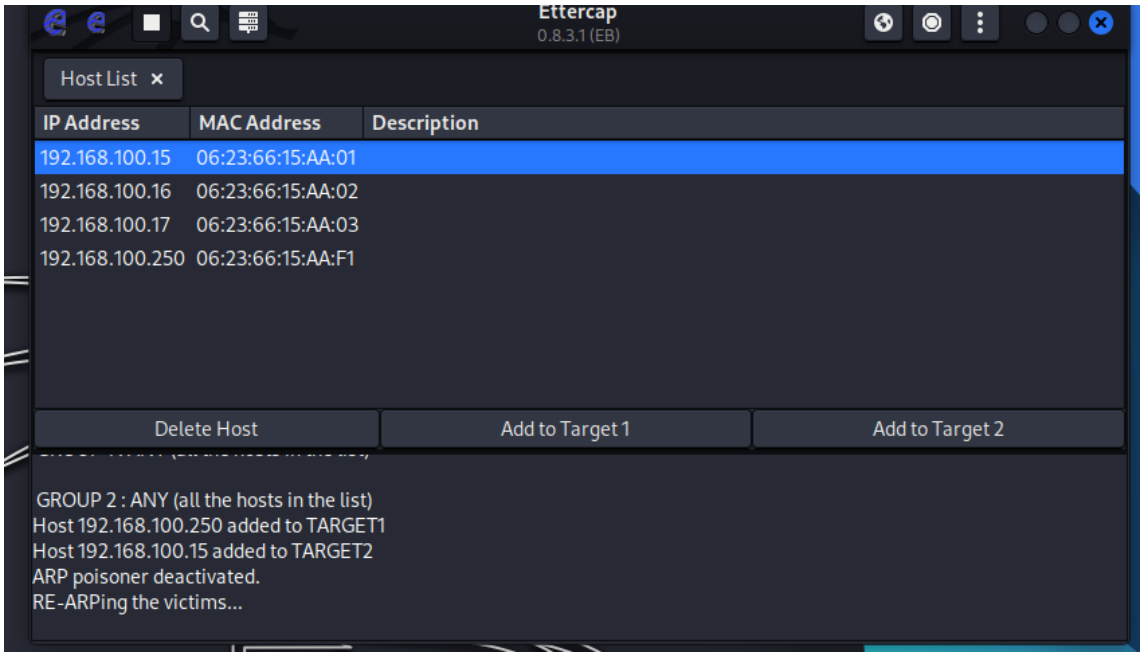


Primeiramente, identicamos no Ettercap os dispositivos presentes na rede, onde a ferramenta começa a enviar pacotes ARP para os dispositivos da rede. Sabendo agora as informações dos dispositivos inicia-se o ataque na tentativa de atualizar as tabelas ARP, associando o seu Mac-address aos endereços IP dos vários dispositivos da rede.

```
R1-6615#sh arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.100.15           0   000c.29cf.bdd5  ARPA   Ethernet0/0
Internet  192.168.100.16           0   000c.29cf.bdd5  ARPA   Ethernet0/0
Internet  192.168.100.17           0   000c.29cf.bdd5  ARPA   Ethernet0/0
Internet  192.168.100.100          0   000c.29cf.bdd5  ARPA   Ethernet0/0
Internet  192.168.100.250          -   0623.6615.aaf1  ARPA   Ethernet0/0
Internet  192.168.200.15           4   0623.6615.bb01  ARPA   Ethernet0/1
Internet  192.168.200.251          -   0623.6615.bbf1  ARPA   Ethernet0/1
R1-6615#
```

```
root@TA1:~# arp -a
? (192.168.100.16) at 00:0c:29:cf:bd:d5 [ether] on eth0
? (192.168.100.17) at 00:0c:29:cf:bd:d5 [ether] on eth0
? (192.168.100.250) at 00:0c:29:cf:bd:d5 [ether] on eth0
? (192.168.100.100) at 00:0c:29:cf:bd:d5 [ether] on eth0
root@TA1:~#
```

Aqui pode-se verificar que o terminal TA1 e o router atualizaram as suas tabelas ARP com os endereços dos vários dispositivos da rede com o Mac-adress da VM do kali.




```
root@TA1:~# arp -a
? (192.168.100.17) at 06:23:66:15:aa:03 [ether] on eth0
? (192.168.100.100) at 00:0c:29:cf:bd:d5 [ether] on eth0
? (192.168.100.250) at 06:23:66:15:aa:f1 [ether] on eth0
? (192.168.100.16) at 06:23:66:15:aa:02 [ether] on eth0
root@TA1:~#
```

Após, terminar o Ataque, o Ettercap volta a enviar pacotes Arp para os dispositivos da rede atualizarem as suas tabelas ARP com as informações corretas.

Mitigação do Ataque ARP Poisoning Attack

Para mitigar este ataque vamos utilizar o Dynamic ARP Inspection (DAI), que utiliza também o dhcp spnooping configurando-o no switch da rede, para impedir o rastreamento e contaminação das tabelas ARP. Para isso o switch tem de inspecinar os pacotes ARP, verificando a relação entre os os IPs e os endereços Mac, comparando-os ás informações dos dispositivos que receberam IPs por DHCP.

```
SW1(config)# ip dhcp snooping
SW1(config)#ip dhcp snooping vlan 1
SW1(config)#ip arp inspection vlan 1
SW1(config)#int e0/0
SW1(config-if)#ip arp inspection trust
SW1(config-if)#ip dhcp snooping trust
```

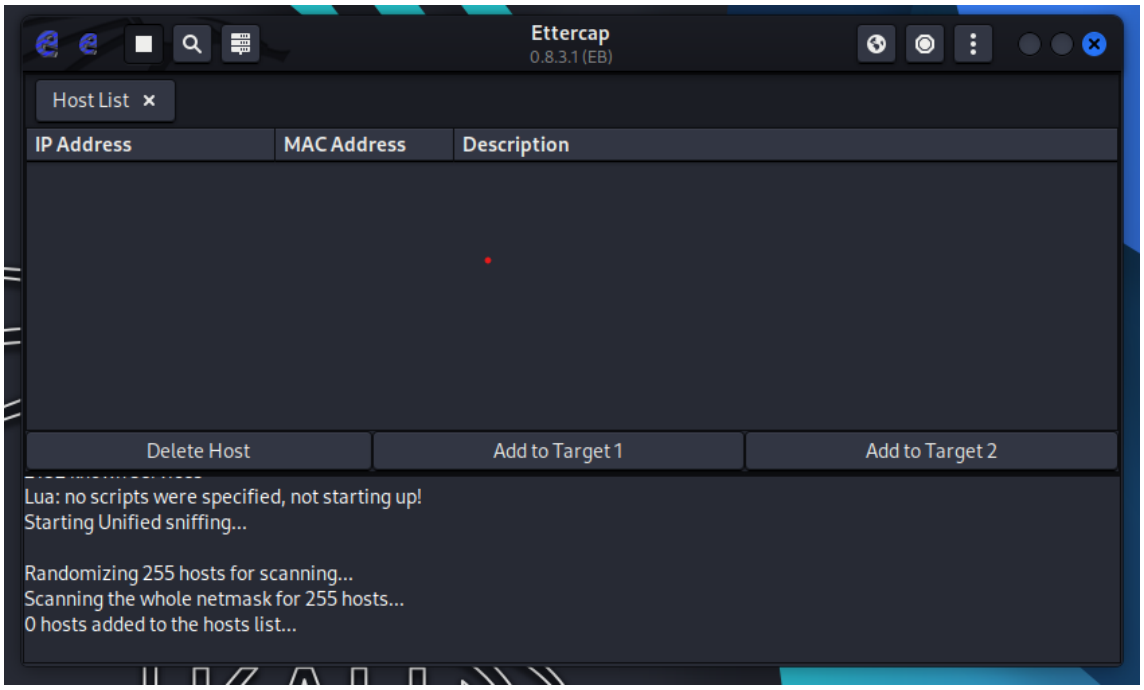
```
SW1(config)#int range e0/1-3
SW1(config-if-range)#ip dhcp snooping limit rate 20
SW1(config-if-range)#ip arp inspection limit rate 20
SW1(config-if-range)#int e1/0
SW1(config-if)#ip dhcp snooping limit rate 20
SW1(config-if)#ip arp inspection limit rate 20
SW1(config-if)#exit
SW1(config)#ip arp inspection validate src-mac dst-mac ip
```

```
SW1#sh ip dhcp snooping
Switch DHCP snooping is enabled
Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:
1
DHCP snooping is operational on following VLANs:
1
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
   remote-id: aabb.cc00.0300 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                Trusted    Allow option    Rate limit (pps)
-----------------------  -------    ------------    ----------------
Ethernet0/0              yes        yes             unlimited
  Custom circuit-ids:
Ethernet0/1              no         no              20
  Custom circuit-ids:
Ethernet0/2              no         no              20
  Custom circuit-ids:
Ethernet0/3              no         no              20
  Custom circuit-ids:
Ethernet1/0              no         no              20
  Custom circuit-ids:
```

```
SW1#sh ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
Total number of bindings: 0
```

```
SW1#sh ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
Total number of bindings: 0

SW1#sh ip arp inspection int

 Interface        Trust State     Rate (pps)     Burst Interval
 ---------------  -----------     ----------     --------------
 Et0/0            Trusted              None                N/A
 Et0/1            Untrusted              20                  1
 Et0/2            Untrusted              20                  1
 Et0/3            Untrusted              20                  1
 Et1/0            Untrusted              20                  1
 Et1/1            Untrusted              15                  1
 Et1/2            Untrusted              15                  1
```

```
SW1#sh ip arp inspection statistics

 Vlan      Forwarded        Dropped     DHCP Drops      ACL Drops
 ----      ---------        -------     ----------      ---------
    1              0              0              0              0

 Vlan   DHCP Permits    ACL Permits  Probe Permits   Source MAC Failures
 ----   ------------    -----------  -------------   -------------------
    1              0              0              0                     0

 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------
    1                  0                        0                      0
```




```
*Mar 31 10:46:04.645: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et1/0, vlan 1.(
[000c.29cf.bdd5/192.168.100.100/0000.0000.0000/192.168.100.196/10:46:01 UTC Mon Mar 31 2025
])
SW1#
*Mar 31 10:47:41.010: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et0/1, vlan 1.(
[0623.6615.aa01/192.168.100.15/0000.0000.0000/192.168.100.250/10:47:40 UTC Mon Mar 31 2025]
)
*Mar 31 10:47:42.012: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et0/1, vlan 1.(
[0623.6615.aa01/192.168.100.15/0000.0000.0000/192.168.100.250/10:47:41 UTC Mon Mar 31 2025]
)
```

Como se pode verificar, após a configuração do DAI e do DHCP snooping, a o atacante já não consegue registar as informações dos dispositivos da Rede. Na configuração tive algumas dificuldades, pois após a configuração do DHCP snooping, mesmo tendo um DHCP limit rate alto, o swtich bloqueia qualquer comunicação do lado dos terminais, pois as portas estão como “untrusted”. Tentei mesmo configurando as máquinas a receber ip por DHCP a partir de endereços da Vlan, configurarando uma Vlan 10 com sub-interface, e associando as portas do switch para o terminar à Vlan 10. No entanto quando configurava o comando DHCP snooping aos terminais da rede perdiam os IP que tinham recebido por DHCP e não conseguia ter comunicação com o router.

Ataque B1: DHCP Starvation / Exhaustion Attack

CVE-2024-3661 – Tunnel Vision

A CVE-2024-20259 é uma vulnerabilidade de negação de serviço grave no Cisco IOS XE que afeta o recurso de DHCP Snooping, podendo causar interrupção nos serviços DHCP e impactar a operação da rede. A aplicação de patches de segurança e boas práticas de configuração são fundamentais para mitigar os riscos dessa vulnerabilidade. Ainda não tem CVSS publicado.

Ataque DHCP Starvation / Exhaustion Attack

O DHCP Starvation Attack é um ataque de negação de serviço (DoS - Denial of Service) direcionado ao protocolo DHCP (Dynamic Host Configuration Protocol). O objetivo do ataque é esgotar todos os endereços IP disponíveis no servidor DHCP, impedindo que novos dispositivos legítimos obtenham um IP e, consequentemente, fiquem sem conexão de rede.

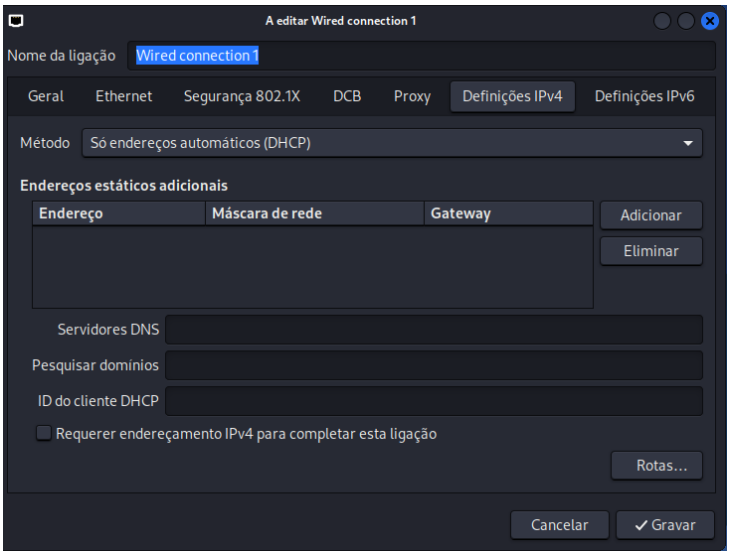
O atacante usa uma ferramenta automatizada para enviar inúmeras requisições DHCP DISCOVER ao servidor DHCP. Cada pedido apresenta um endereço MAC diferente. O objetivo é o servidor DHCP ficar com todos os endereços disponíveis alocados. Ou seja, com isto novas máquinas deixam de poder acessar à rede.

```
R1-6615(config)#ip dhcp excluded-address 192.168.100.1 192.168.100.14
R1-6615(config)#ip dhcp excluded-address 192.168.100.200 192.168.100.254
R1-6615(config)#ip dhcp pool REDE_A
R1-6615(dhcp-config)#network 192.168.100.0 255.255.255.0
R1-6615(dhcp-config)#default-router 192.168.100.250
R1-6615(dhcp-config)#dns-server 8.8.8.8
R1-6615(dhcp-config)#
```

```
TA1 console is now available... Press RETURN to get started.
udhcpc: started, v1.30.1
udhcpc: sending discover
udhcpc: sending select for 192.168.100.15
udhcpc: lease of 192.168.100.15 obtained, lease time 86400
root@TA1:~#
```

```
TA2 console is now available... Press RETURN to get started.
udhcpc: started, v1.30.1
udhcpc: sending discover
udhcpc: sending select for 192.168.100.16
udhcpc: lease of 192.168.100.16 obtained, lease time 86400
root@TA2:~#
```

```
TA3 console is now available... Press RETURN to get started.
udhcpc: started, v1.30.1
udhcpc: sending discover
udhcpc: sending select for 192.168.100.17
udhcpc: lease of 192.168.100.17 obtained, lease time 86400
root@TA3:~#
```

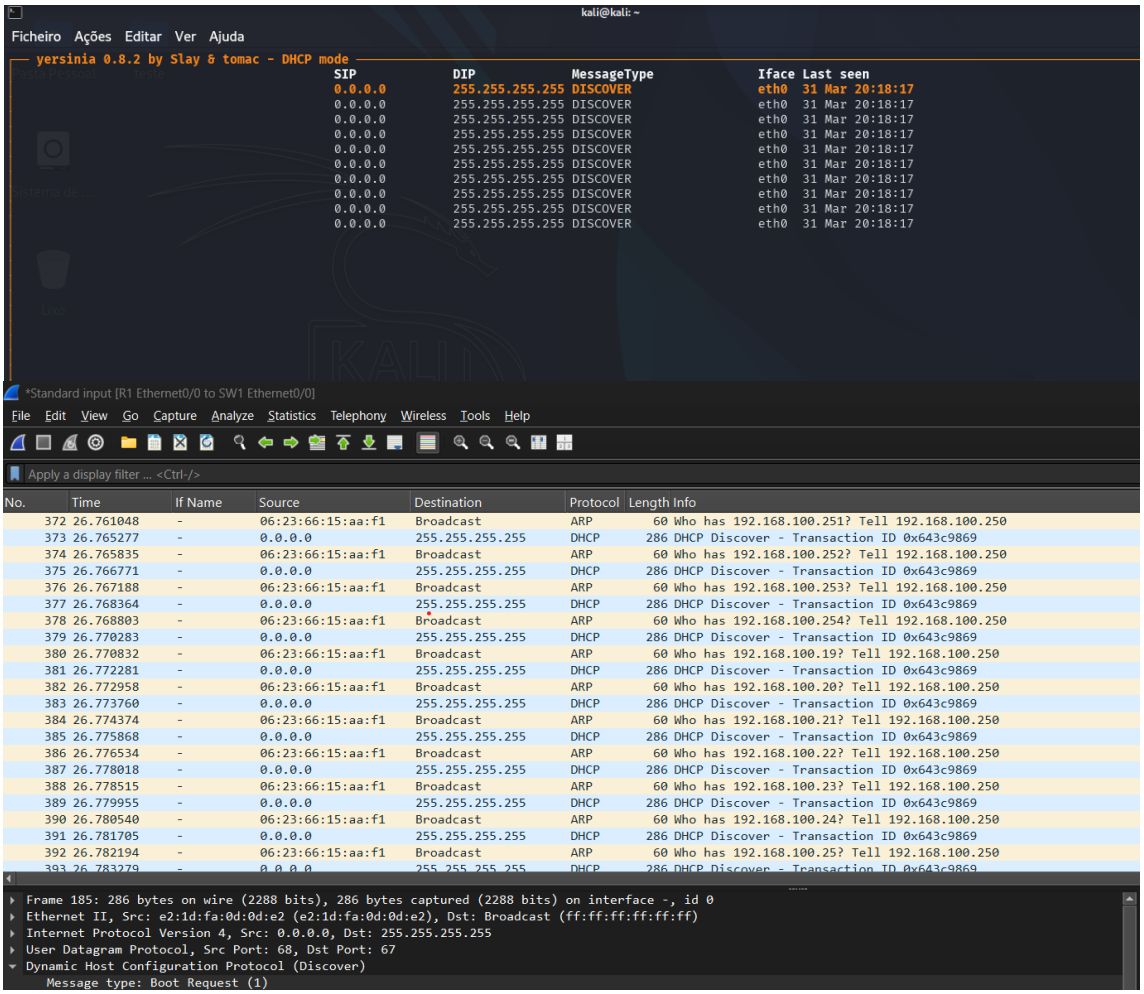


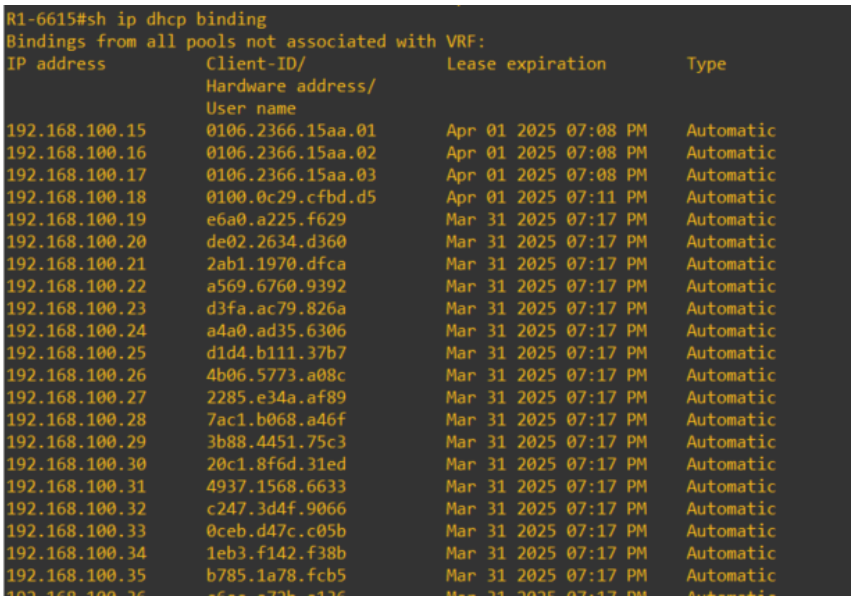
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.18  netmask 255.255.255.0  broadcast 192.168.100.255
        inet6 fe80::4970:8b6:7fbb:b73a  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:cf:bd:d5  txqueuelen 1000  (Ethernet)
        RX packets 1  bytes 342 (342.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 22  bytes 3000 (2.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
R1-6615#sh ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.168.100.15      0106.2366.15aa.01       Apr 01 2025 05:02 PM    Automatic
192.168.100.16      0106.2366.15aa.02       Apr 01 2025 05:02 PM    Automatic
192.168.100.17      0106.2366.15aa.03       Apr 01 2025 05:02 PM    Automatic
192.168.100.18      0100.0c29.cfbd.d5       Apr 01 2025 05:06 PM    Automatic
R1-6615#
```

Configurei o servidor DHCP, de modo a respeitar as regras de endereçamento do primeiro projeto.

Para realizar o ataque utilizei a ferramenta Yersinia. Pode-se verificar na imagem abaixo o atacante Kali a enviar os pacotes DHCP Discover para o Router.





```
R1-6615#sh ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.168.100.15      0106.2366.15aa.01       Apr 01 2025 07:08 PM    Automatic
192.168.100.16      0106.2366.15aa.02       Apr 01 2025 07:08 PM    Automatic
192.168.100.17      0106.2366.15aa.03       Apr 01 2025 07:08 PM    Automatic
192.168.100.18      0100.0c29.cfbd.d5       Apr 01 2025 07:11 PM    Automatic
192.168.100.19      e6a0.a225.f629          Mar 31 2025 07:17 PM    Automatic
192.168.100.20      de02.2634.d360          Mar 31 2025 07:17 PM    Automatic
192.168.100.21      2ab1.1970.dfca          Mar 31 2025 07:17 PM    Automatic
192.168.100.22      a569.6760.9392          Mar 31 2025 07:17 PM    Automatic
192.168.100.23      d3fa.ac79.826a          Mar 31 2025 07:17 PM    Automatic
192.168.100.24      a4a0.ad35.6306          Mar 31 2025 07:17 PM    Automatic
192.168.100.25      d1d4.b111.37b7          Mar 31 2025 07:17 PM    Automatic
192.168.100.26      4b06.5773.a08c          Mar 31 2025 07:17 PM    Automatic
192.168.100.27      2285.e34a.af89          Mar 31 2025 07:17 PM    Automatic
192.168.100.28      7ac1.b068.a46f          Mar 31 2025 07:17 PM    Automatic
192.168.100.29      3b88.4451.75c3          Mar 31 2025 07:17 PM    Automatic
192.168.100.30      20c1.8f6d.31ed          Mar 31 2025 07:17 PM    Automatic
192.168.100.31      4937.1568.6633          Mar 31 2025 07:17 PM    Automatic
192.168.100.32      c247.3d4f.9066          Mar 31 2025 07:17 PM    Automatic
192.168.100.33      0ceb.d47c.c05b          Mar 31 2025 07:17 PM    Automatic
192.168.100.34      1eb3.f142.f38b          Mar 31 2025 07:17 PM    Automatic
192.168.100.35      b785.1a78.fcb5          Mar 31 2025 07:17 PM    Automatic
```

Utilizando o comando “sh ip dhcp binding”, pode -se verificar os endereços da rede todos atribuídos.

DHCP Spoofing Attack

CVE-2020-13529

Uma vulnerabilidade notável relacionada a esse tipo de ataque é a CVE-2020-13529. Essa falha afeta o Systemd na versão 245 e permite que um invasor, por meio de pacotes DHCP FORCERENEW especialmente criados, induza um cliente DHCP a aceitar respostas DHCP ACK falsificadas. Isso possibilita a reconfiguração não autorizada das interfaces de rede do sistema afetado, potencialmente levando a uma negação de serviço ou permitindo ataques MITM.

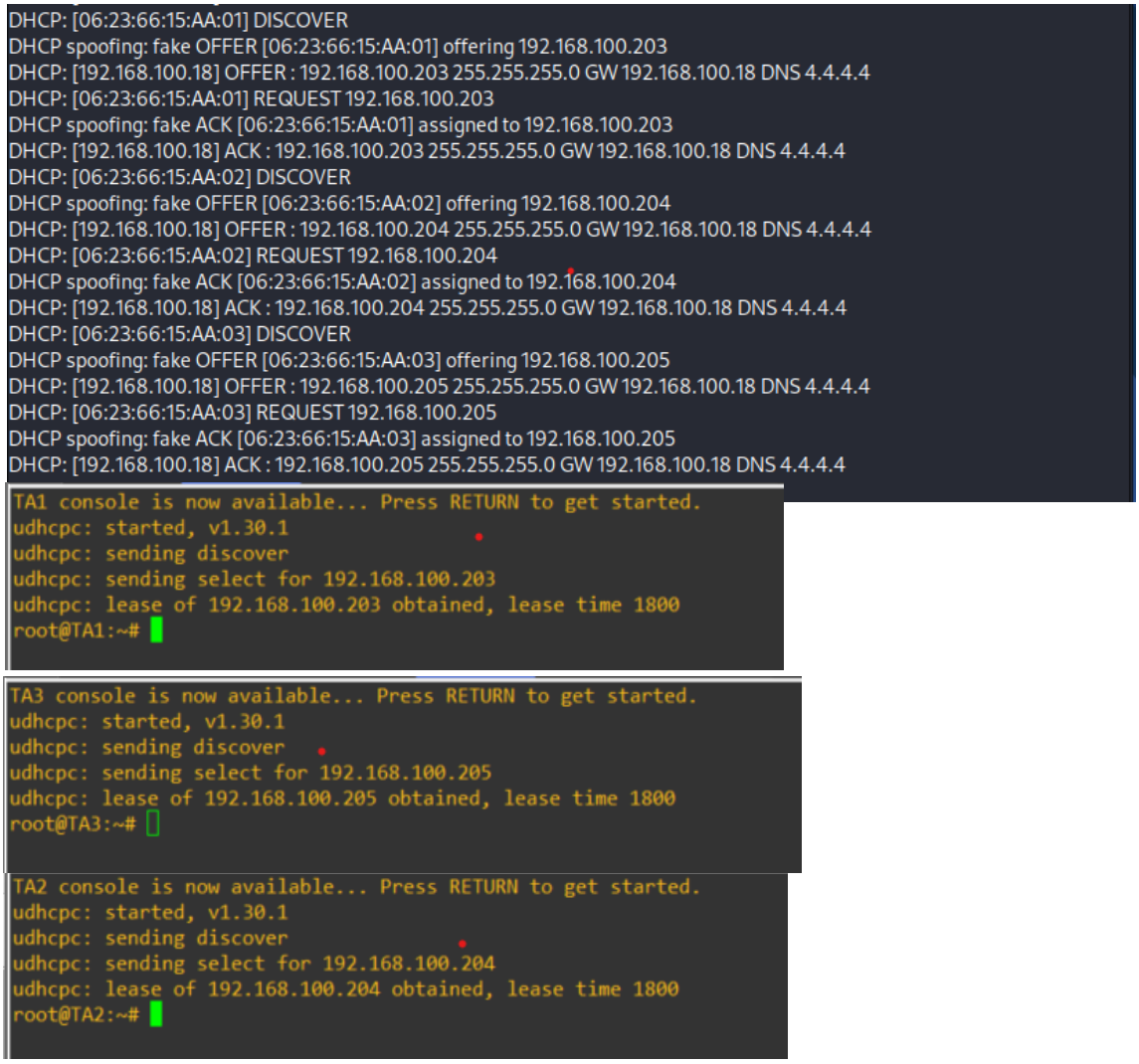
- **Pontuação CVSS v3.1**: 6.1
- **Ano de Divulgação**: 2021

Ataque DHCP Spoofing

O DHCP Spoofing Attack é um ataque em que um invasor configura um servidor DHCP falso dentro da rede para fornecer informações maliciosas a dispositivos que solicitam endereços IP. Isso permite ao atacante redirecionar o tráfego, realizar ataques Man-in-the-Middle (MITM) ou até causar uma negação de serviço (DoS).

Para realizar o ataque, o atacante configura um servidor DHCP falso, e quando um dispositivo solicita um endereço IP (pacote DHCP DISCOVER), o servidor falso responde com um DHCP OFFER com um endereço IP, gateway e dns falsos. Os dispositivos depois aceitam a primeira resposta DHCP que recebe.

Para realizar o ataque utilizei novamente o Ettercap. Coloquei para enviar IPs entre o endereço 192.168.100.200 e 192.168.250 com a mascara 255.255.255.0 e com o servidor dns 4.4.4.4.



Como se pode verificar os terminais atualizaram os seus endereços ip, para a gama envia pelo Servidor DHCP falso.

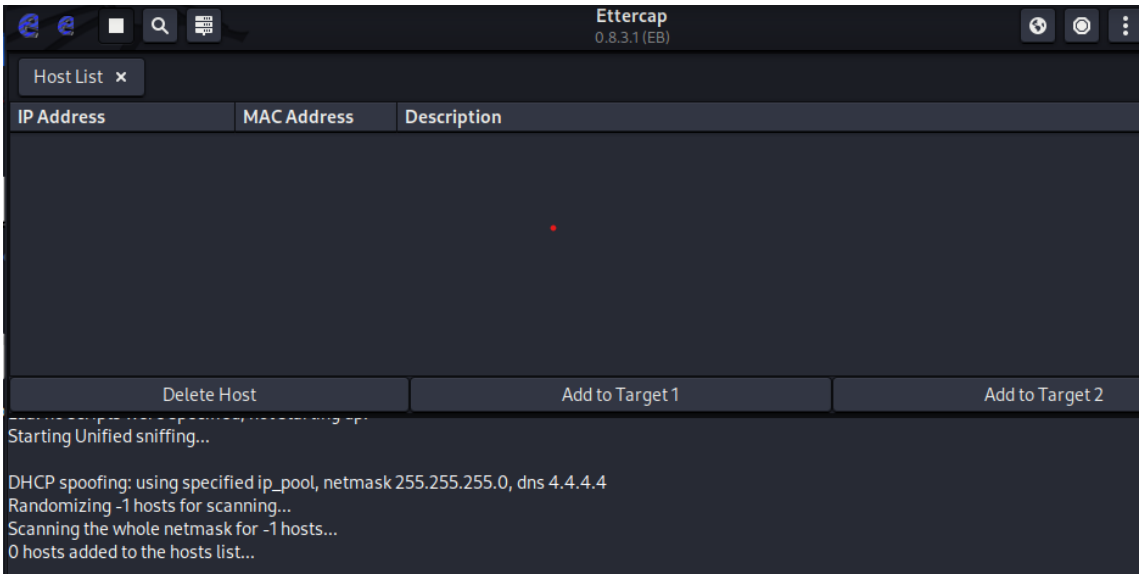
Mitigação de ataques DHCP

Para mitigar os ataques DHCP, utiliza-se novamente o DHCP Snooping. Configurando a porta que liga ao Router como confiável e o resto das portas ligadas aos terminais coloca-se como não confiáveis. No entanto, novamente quando faço a configuração do DHCP Snopping quando um pacote DHCP é enviado a partir de uma porta que estão como “untrusted”, este é bloqueado. Ou seja, os terminais não recebem os endereços IP.

```
TA1 console is now available... Press RETURN to get started.
udhcpc: started, v1.30.1
udhcpc: sending discover
udhcpc: sending discover
udhcpc: sending discover
udhcpc failed to get a DHCP lease
udhcpc: no lease, forking to background
root@TA1:~#
```

```
Ficheiro  Ações  Editar  Ver  Ajuda
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::4970:8b6:7fbb:b73a  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:cf:bd:d5  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 30  bytes 5503 (5.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Loopback Local)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Como não foi possível receber endereços IP por dhcp, o ettercap não consegue funcionar nas devidas condições. Como se pode verificar a ferramenta não encontrou nenhum dispositivo da rede.



No ataque B1, DHCP Starvation/Exhaustion, após a mitigação, o yersinia envia a partir da interface para a rede pacotes DHCP_OFFER para a rede, como se pode verificar. No entanto, não recebe nenhuma resposta, pois o Switch está a bloquear as solicitações falsas que foram enviadas por causa da configuração do dhcp snooping nas interfaces da Vlan.

```
yersinia 0.8.2 by Slay & tomac - DHCP mode
SIP              DIP             MessageType              Iface Last seen
0.0.0.0          255.255.255.255 DISCOVER                 eth0  01 Apr 01:09:07
0.0.0.0          255.255.255.255 DISCOVER                 eth0  01 Apr 01:09:07
0.0.0.0          255.255.255.255 DISCOVER                 eth0  01 Apr 01:09:07
0.0.0.0          255.255.255.255 DISCOVER                 eth0  01 Apr 01:09:07
0.0.0.0          255.255.255.255 DISCOVER                 eth0  01 Apr 01:09:07
0.0.0.0          255.255.255.255 DISCOVER                 eth0  01 Apr 01:09:07
0.0.0.0          255.255.255.255 DISCOVER                 eth0  01 Apr 01:09:07
0.0.0.0          255.255.255.255 DISCOVER                 eth0  01 Apr 01:09:07
0.0.0.0          255.255.255.255 DISCOVER                 eth0  01 Apr 01:09:07
0.0.0.0          255.255.255.255 DISCOVER                 eth0  01 Apr 01:09:07
```

```
SW1#
*Apr  1 00:07:37.787: %DHCP_SNOOPING-4-DHCP_SNOOPING_ERRDISABLE_WARNING: DHCP Snooping rece
ived 20 DHCP packets on interface Et1/0
*Apr  1 00:07:37.787: %DHCP_SNOOPING-4-DHCP_SNOOPING_RATE_LIMIT_EXCEEDED: The interface Et1
/0 is receiving more than the threshold set
*Apr  1 00:07:37.787: %PM-4-ERR_DISABLE: dhcp-rate-limit error detected on Et1/0, putting E
t1/0 in err-disable state
*Apr  1 00:07:38.787: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0, changed
state to down
SW1#
*Apr  1 00:07:39.787: %LINK-3-UPDOWN: Interface Ethernet1/0, changed state to down
SW1#
```