باسمه تعالی

درس: آزمایشگاه امنیت شبکه

نام و نام خانوادگی: هادی امینی

شماره دانشجویی: 9912762370

شماره آزمایش : 05

تاریخ تحویل: 1403/03/02

موضوع: **تست نفوذ شبکه**

✓ *تفاوت تست نفوذ و ارزیابی آسیب پذیری را بیان کنید.*

هدف:

- ***ارزیابی آسیب پذیری :***هدف یافتن نقاط ضعف و آسیب پذیری های بالقوه در یک سیستم یا شبکه است.
- ***تست نفوذ :***هدف سنجش توانایی یک مهاجم واقعی برای نفوذ به یک سیستم یا شبکه و سوء استفاده از آسیب پذیری های یافت شده است.

روش:

- ***ارزیابی آسیب پذیری :***معمولاً از اسکنرهای خودکار و ابزارهای دیگر برای شناسایی آسیب پذیری های شناخته شده استفاده می کند.
- ***تست نفوذ :***تست کنندگان نفوذ از تکنیک های مختلفی، از جمله مهندسی اجتماعی، اسکن دستی و حملات هک، برای یافتن آسیب پذیری ها و سوء استفاده از آنها استفاده می کنند.

محدودیت ها:

- ***ارزیابی آسیب پذیری :***ممکن است همه آسیب پذیری ها را پیدا نکند، به خصوص آسیب پذیری های ناشناخته یا پیچیده.
- ***تست نفوذ :***می تواند پرهزینه و زمان بر باشد و ممکن است همه مسیرهای حمله را پوشش ندهد.

مزایا:

- ***ارزیابی آسیب پذیری :***یک روش نسبتاً سریع و ارزان برای یافتن آسیب پذیری ها است.
- ***تست نفوذ :***می تواند اطلاعات دقیق تری در مورد اینکه چگونه یک مهاجم می تواند از آسیب پذیری ها سوء استفاده کند، ارائه دهد.

کاربرد:

- ***ارزیابی آسیب پذیری :***معمولاً در مراحل اولیه چرخه توسعه نرم افزار یا به عنوان بخشی از یک ارزیابی امنیتی منظم استفاده می شود.
- ***تست نفوذ :***معمولاً برای تأیید یافته های ارزیابی آسیب پذیری یا برای ارزیابی اثر اقدامات اصلاحی استفاده می شود.

به طور خلاصه ***ارزیابی آسیب پذیری*** می گوید که چه آسیب پذیری هایی وجود دارد، در حالی که ***تست نفوذ*** نشان می دهد که چگونه می توان از آنها سوء استفاده کرد.

✓ مکانیزمهای امنیتی برای مقابله با هر یک از حملات Flooding MAC ، Attack DHCP، Hopping VLANو ARP Spoofing را شرح دهید.

حمله Flooding MAC :

- **لیست های کنترل دسترسی** : ACL ها مجموعه ای از قوانین هستند که به شما امکان می دهند مشخص کنید چه ترافیکی مجاز به ورود و خروج از یک پورت یا VLAN است .می توانید از ACL ها برای مسدود کردن آدرس های MAC جعلی که سعی در ارسال ترافیک به پورت شما دارند استفاده کنید .برای مثال، می توانید یک ACL ایجاد کنید که فقط به آدرس های MAC شناخته شده در شبکه شما اجازه ورود به پورت را بدهد.
- ***پورت های امن :*** پورت های امن پورت های سوئیچ هستند که به طور پیش فرض خاموش هستند و باید به صورت دستی فعال شوند .هنگامی که یک پورت امن فعال می شود، فقط ترافیک مجاز از آدرس های MAC مجاز می تواند از آن عبور کند .این امر می تواند به محافظت از دستگاه های متصل به پورت امن در برابر حملات Flooding MAC کمک کند.

- **بازرسی آدرس MAC** : بازرسی آدرس MAC مکانیزمی است که آدرس MAC هر فریم ورودی را با آدرس های MAC موجود در یک پایگاه داده مقایسه می کند .اگر آدرس MAC مطابقت نداشته باشد، فریم دور انداخته می شود .این امر می تواند به جلوگیری از ورود آدرس های MAC جعلی به شبکه شما کمک کند.

حمله DHCP Spoofing :

- **سرور DHCP قابل اعتماد :**از یک سرور DHCP استفاده کنید که از ویژگی های امنیتی مانند احراز هویت و رمزگذاری پشتیبانی می کند .همچنین باید مطمئن شوید که سرور DHCP شما به روز است و هیچ آسیب پذیری شناخته شده ای ندارد.
- **بررسی IP DHCP:** ترافیک DHCP را برای آدرس های IP و سرورهای DHCP جعلی بررسی کنید . می توانید از ابزاری مانند DHCP Snooping یا DHCP Inspector برای این کار استفاده کنید . این ابزارها ترافیک DHCP را رصد می کنند و به دنبال ناهنجاری هایی مانند آدرس های IP تکراری یا سرورهای DHCP غیرمجاز هستند.
- **رزرو آدرس IP:** برای دستگاه های مهم مانند سرورها و روترها آدرس های IP رزرو کنید .این امر به جلوگیری از جعل آدرس های IP این دستگاه ها توسط مهاجمان کمک می کند.

حمله VLAN Hopping :

- **لیست های کنترل دسترسی (ACLs):** از ACL ها برای محدود کردن ترافیک بین VLAN ها استفاده کنید .می توانید برای هر VLAN یک ACL جداگانه ایجاد کنید و مشخص کنید که چه نوع ترافیکی مجاز به ورود و خروج از آن VLAN است.
- **پورت های Trunk :**پورت های Trunk پورت های سوئیچ هستند که می توانند ترافیک را بین چندین VLANحمل کنند .برای اتصال سوئیچ ها در VLAN های مختلف فقط از پورت های Trunk استفاده کنید .این امر به جلوگیری از ورود ترافیک غیرمجاز به VLAN ها کمک می کند.
- **شناسایی VLAN:** از پروتکل های شناسایی VLAN مانند 802.1Q یا 802.1p.برای تأیید اینکه ترافیک به VLAN صحیح ارسال می شود استفاده کنید .این پروتکل ها برچسب هایی را به فریم های اترنت اضافه می کنند که VLAN را که فریم به آن تعلق دارد، مشخص می کند.

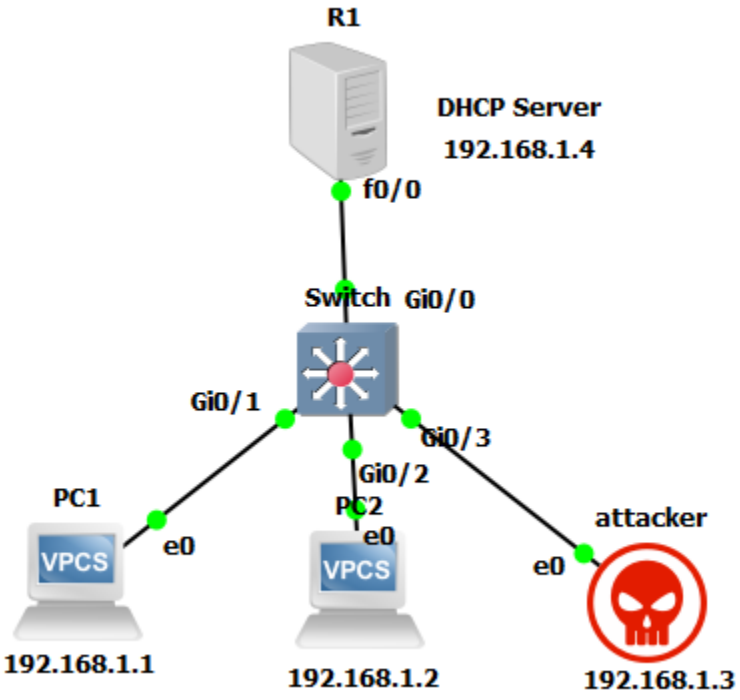
حمله ARP Spoofing :

- **بررسی IP ARP:** ترافیک ARP را برای آدرس های IP و MAC جعلی بررسی کنید .می توانید از ابزاری مانند ARP Spoofing Inspector برای این کار استفاده کنید .این ابزار ترافیک ARP را رصد می کند و به دنبال ناهنجاری هایی مانند آدرس های IP جعلی یا نگاشت های MAC نادرست است.

- **ARP Inspection:** از ARP Inspection برای تأیید اینکه آدرس های IP و MAC با یکدیگر مطابقت دارند استفاده کنید. ARP Inspection مکانیزمی است که در برخی از سوئیچ ها و روترها تعبیه شده است. هنگامی که یک دستگاه در شبکه یک درخواست ARP ارسال می کند، سوئیچ یا روتر قبل از ارسال پاسخ ARP به دستگاه مقصد، آدرس IP و MAC را تأیید می کند.
- **آدرس های IP ایستا:** برای دستگاه های مهم مانند سرورها و روترها از آدرس های IP ایستا استفاده کنید. این امر به جلوگیری از جعل آدرس های IP این دستگاه ها توسط مهاجمان کمک می کند.

پیاده سازی عملی

حمله DHCP Starvation :



دستورات کانفیگ روتر به عنوان DHCP Server :

```
enable
configure terminal
ip dhcp pool VLAN1
network 192.168.1.0 255.255.255.0
default-router 192.168.1.4
```

```
exit
```

دریافت آیپی از DHCPتوسط کلاینت ها:

```
PC2> ip dhcp
DDORA IP 192.168.1.2/24 GW 192.168.1.4

PC2> show

NAME   IP/MASK              GATEWAY         MAC                LPORT  RHOST:PORT
PC2    192.168.1.2/24       192.168.1.4     00:50:79:66:68:00  20011  127.0.0.1:20012
       fe80::250:79ff:fe66:6800/64
```

```
PC1> ip dhcp
DDORA IP 192.168.1.1/24 GW 192.168.1.4

PC1> sh

NAME   IP/MASK              GATEWAY         MAC                LPORT  RHOST:PORT
PC1    192.168.1.1/24       192.168.1.4     00:50:79:66:68:01  20009  127.0.0.1:20010
       fe80::250:79ff:fe66:6801/64
```

```
└─$ sudo ifup eth0
Internet Systems Consortium DHCP Client 4.4.3-P1
Copyright 2004-2022 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/00:0c:29:b6:7b:85
Sending on   LPF/eth0/00:0c:29:b6:7b:85
Sending on   Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 6
DHCPOFFER of 192.168.1.3 from 192.168.1.4
DHCPREQUEST for 192.168.1.3 on eth0 to 255.255.255.255 port 67
DHCPACK of 192.168.1.3 from 192.168.1.4
bound to 192.168.1.3 -- renewal in 41112 seconds.

┌──(hadi㉿hadi)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:b6:7b:85 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.3/24 brd 192.168.1.255 scope global dynamic eth0
       valid_lft 86396sec preferred_lft 86396sec
    inet6 fe80::20c:29ff:feb6:7b85/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
```

دستور اجرای حمله:

sudo yersinia dhcp -attack 1 -i eth0

```
┌──(hadi㉿hadi)-[~]
└─$ sudo yersinia dhcp -attack 1 -i eth0
Warning: Couldn't allocate kernel memory for filter: try increasing net.core.optmem_max with sysctl
<*> Starting DOS attack sending DISCOVER packet...
<*> Press any key to stop the attack <*>
```

بعد از اجرای حمله ، با دستور show ip dhcp pool میتوان آمار آیپی های تخصیص یافته را مشاهده کرد که تمامی آدرس ها استفاده شده است.

```
R1#show ip dhcp pool

Pool VLAN1 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 253
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses
 0.0.0.0              192.168.1.1      - 192.168.1.254     253
R1#
```

دستورات مقابله با حمله:

```
ip dhcp snooping limit rate 5
ip dhcp snooping verify mac-address
switchport mode access
switchport port-security mac-address sticky
switchport port-security violation shut
sh port-sec address
```

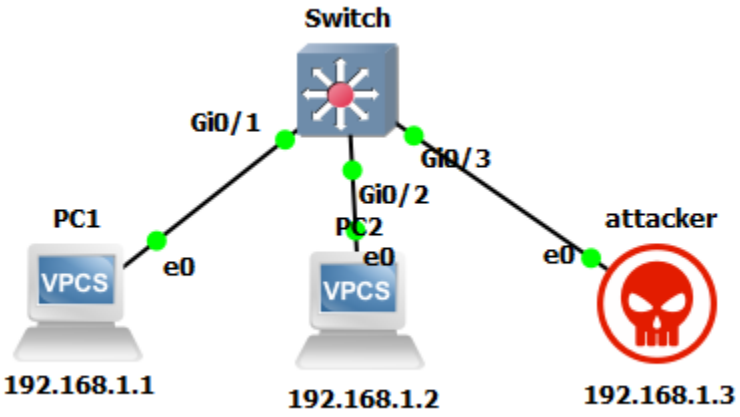
بعد از اجرای این دستورات، سوییچ با مهاجم مقابله میکند و دسترسی اینترفیس مربوطه قطع میشود:

```
*May 22 13:42:00.440: %DHCP_SNOOPING-4-DHCP_SNOOPING_ERRDISABLE_WARNING: DHCP Snooping received 5 DHCP packets on interface
Gi0/3
*May 22 13:42:00.441: %DHCP_SNOOPING-4-DHCP_SNOOPING_RATE_LIMIT_EXCEEDED: The interface Gi0/3 is receiving moret than the th
reshold set
*May 22 13:42:00.442: %PM-4-ERR_DISABLE: dhcp-rate-limit error detected on Gi0/3, putting Gi0/3 in err-disable state
*May 22 13:42:01.754: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/3, changed state to down
*May 22 13:42:03.077: %LINK-3-UPDOWN: Interface GigabitEthernet0/3, changed s
```

نمایش آمار آیپی های تخصیص یافته در روتر:

```
R1#show ip dhcp pool

Pool VLAN1 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 3
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses
 192.168.1.4          192.168.1.1      - 192.168.1.254     3
R1#
```

حمله MAC Flooding :



تنظیم آی‌پی در pc ها به صورت استاتیک:

```
PC2> ip 192.168.1.2/24
Checking for duplicate address...
PC2 : 192.168.1.2 255.255.255.0

PC2> sh

NAME   IP/MASK              GATEWAY           MAC                LPORT  RHOST:PORT
PC2    192.168.1.2/24       0.0.0.0           00:50:79:66:68:01  20002  127.0.0.1:20003
       fe80::250:79ff:fe66:6801/64
```

```
PC1> ip 192.168.1.1/24
Checking for duplicate address...
PC1 : 192.168.1.1 255.255.255.0

PC1> sh

NAME   IP/MASK              GATEWAY           MAC                LPORT  RHOST:PORT
PC1    192.168.1.1/24       0.0.0.0           00:50:79:66:68:00  20000  127.0.0.1:20001
       fe80::250:79ff:fe66:6800/64
```

```
┌──(hadi㉿hadi)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:b6:7b:85 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.3/24 brd 192.168.1.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:feb6:7b85/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
```

نمایش جدول مک آدرس ها در سوییچ:

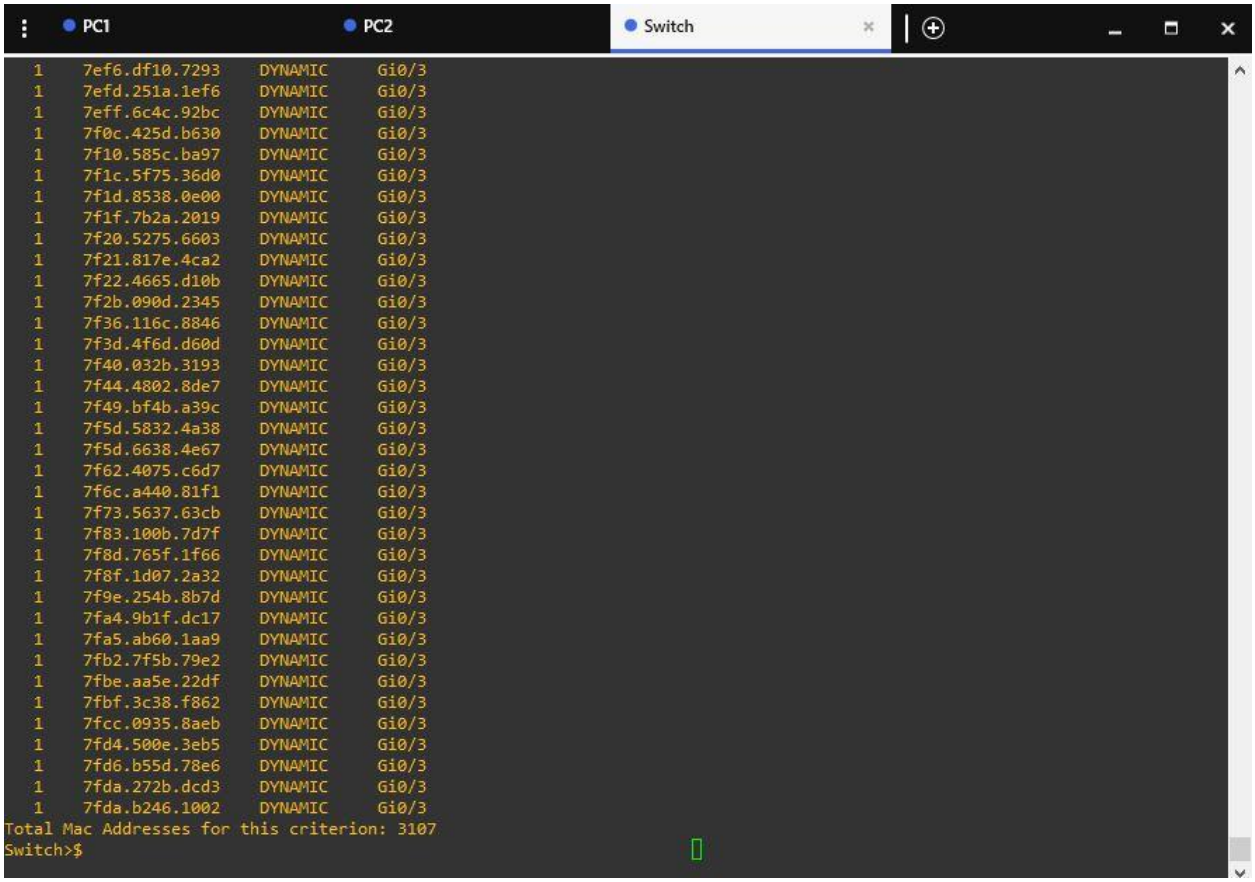
```
Switch>sh mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0050.7966.6800    DYNAMIC     Gi0/1
   1    0050.7966.6801    DYNAMIC     Gi0/2
Total Mac Addresses for this criterion: 2
Switch>
```

دستور اجرای حمله با استفاده از ابزار macof:

```
sudo macof -i eth0
```

```
hadi@hadi: ~
File  Actions  Edit  View  Help
95:82:d9:63:7b:75 43:86:35:2e:ba:30 0.0.0.0.64339 > 0.0.0.0.37996: S 511108796:511108796(0) win 512
e0:69:fe:20:1e:75 7d:25:7b:4f:43:74 0.0.0.0.11041 > 0.0.0.0.39972: S 124764875:124764875(0) win 512
5:3e:8f:50:5a:e2 af:69:a7:11:4a:e9 0.0.0.0.19321 > 0.0.0.0.31798: S 581270609:581270609(0) win 512
33:74:db:75:66:5 31:be:e6:5d:88:1e 0.0.0.0.29383 > 0.0.0.0.45428: S 416810420:416810420(0) win 512
c8:fa:8c:63:6a:a9 77:7b:a1:71:4d:53 0.0.0.0.57531 > 0.0.0.0.51407: S 1574860505:1574860505(0) win 512
a9:4f:3e:68:4b:e3 7e:1c:d4:70:3e:33 0.0.0.0.33236 > 0.0.0.0.38928: S 1152035113:1152035113(0) win 512
4f:b0:5c:e:e3:57 ea:9f:47:6:c3:da 0.0.0.0.25827 > 0.0.0.0.26930: S 1916279694:1916279694(0) win 512
50:8e:dc:52:1b:6c 8c:a1:4e:b:45:4e 0.0.0.0.34520 > 0.0.0.0.8229: S 1216793298:1216793298(0) win 512
a8:fa:73:50:40:4b e8:8f:f3:2e:6e:58 0.0.0.0.51724 > 0.0.0.0.83: S 1419988704:1419988704(0) win 512
88:99:96:7:30:62 a:83:b9:c:50:47 0.0.0.0.9123 > 0.0.0.0.41431: S 1959721618:1959721618(0) win 512
eb:cb:5b:59:8d:d0 4c:a:39:13:21:d2 0.0.0.0.7339 > 0.0.0.0.9644: S 82769955:82769955(0) win 512
e5:d1:56:2f:2e:48 9f:a9:a5:51:17:c0 0.0.0.0.52107 > 0.0.0.0.60073: S 69105145:69105145(0) win 512
23:2c:67:76:36:1b 52:ab:ec:25:4e:b2 0.0.0.0.47229 > 0.0.0.0.34346: S 2098442999:2098442999(0) win 512
50:15:43:22:51:d5 81:cd:eb:2a:18:55 0.0.0.0.45574 > 0.0.0.0.50206: S 1709594374:1709594374(0) win 512
cf:3f:54:34:28:3e 73:4b:d4:2b:68:ef 0.0.0.0.26924 > 0.0.0.0.18892: S 1723014107:1723014107(0) win 512
1d:94:bd:24:18:a5 5d:ec:1d:12:1a:8a 0.0.0.0.38989 > 0.0.0.0.36837: S 276846252:276846252(0) win 512
d8:85:ec:31:bf:9e 4c:8a:5d:13:31:b0 0.0.0.0.51058 > 0.0.0.0.9695: S 1642800978:1642800978(0) win 512
c4:44:33:10:60:7d 77:33:11:f:3e:cc 0.0.0.0.25635 > 0.0.0.0.54774: S 1684645419:1684645419(0) win 512
4e:94:ec:24:6f:43 76:49:54:42:b5:b7 0.0.0.0.6328 > 0.0.0.0.58838: S 1899725275:1899725275(0) win 512
95:dd:99:50:db:2a a5:78:ff:25:d9:cb 0.0.0.0.4343 > 0.0.0.0.8832: S 1208021083:1208021083(0) win 512
1d:19:c2:d:53:8d fc:6c:99:2a:67:69 0.0.0.0.10800 > 0.0.0.0.48565: S 1700164863:1700164863(0) win 512
6b:ac:fc:77:91:13 38:eb:fc:c:32:30 0.0.0.0.37731 > 0.0.0.0.25599: S 1954166556:1954166556(0) win 512
9e:4c:45:17:c5:59 12:c0:43:71:88:2 0.0.0.0.5381 > 0.0.0.0.46742: S 87173553:87173553(0) win 512
f6:60:d4:6f:c3:55 fc:ee:b8:6b:5f:e8 0.0.0.0.60607 > 0.0.0.0.59739: S 314007366:314007366(0) win 512
17:4b:9:53:65:16 cc:9:da:50:55:96 0.0.0.0.56340 > 0.0.0.0.23035: S 909169596:909169596(0) win 512
75:f0:0:70:d0:6d d:e7:62:7a:cc:11 0.0.0.0.7728 > 0.0.0.0.1374: S 2129182397:2129182397(0) win 512
fc:68:c3:69:70:8e 27:38:af:6a:74:ad 0.0.0.0.25020 > 0.0.0.0.58256: S 1772773811:1772773811(0) win 512
a3:79:2:31:7d:e9 43:77:dc:72:4c:85 0.0.0.0.11066 > 0.0.0.0.56296: S 1506193643:1506193643(0) win 512
b6:50:dd:12:27:eb 4c:b:ab:17:3:45 0.0.0.0.52242 > 0.0.0.0.39716: S 2024054794:2024054794(0) win 512
e7:12:50:55:6e:6b d5:79:54:1e:e:8b 0.0.0.0.27920 > 0.0.0.0.31390: S 300605600:300605600(0) win 512
da:d8:7d:75:30:9d 17:21:d4:0:77:b8 0.0.0.0.59694 > 0.0.0.0.19895: S 2065465995:2065465995(0) win 512
db:df:2:23:3a:e1 3f:
```

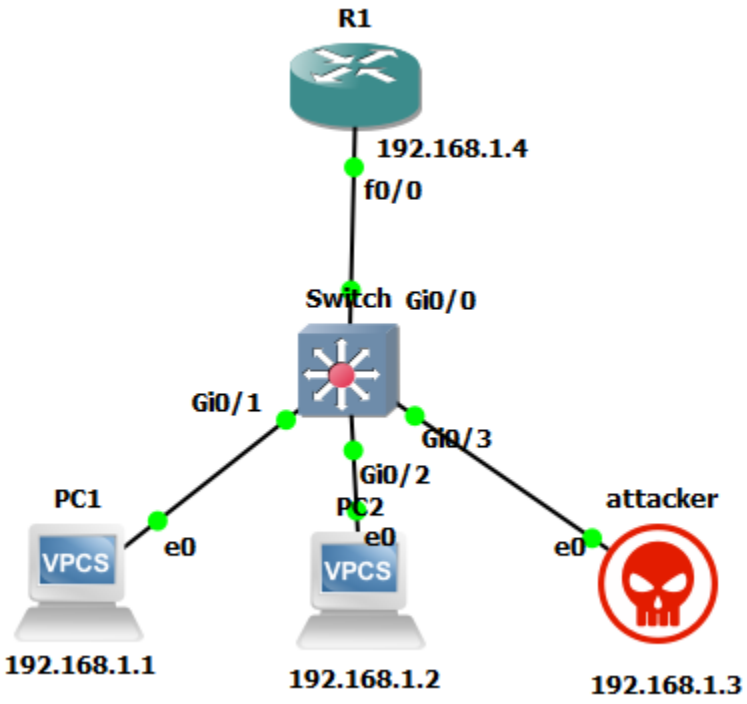
نتیجه اجرای حمله:



نحوه مقابله:

```
enable
conf t
int gi0/3
switchport mode access
switchport port-security mac-address sticky
switchport port-security violation shut
sh port-sec address
```

حمله Arp Spoofing:



pc1:

```
PC1> ip dhcp
DDORA IP 192.168.1.1/24 GW 192.168.1.4

PC1> arp

arp table is empty

PC1> ping 192.168.1.2

84 bytes from 192.168.1.2 icmp_seq=1 ttl=64 time=8.572 ms
84 bytes from 192.168.1.2 icmp_seq=2 ttl=64 time=7.943 ms
84 bytes from 192.168.1.2 icmp_seq=3 ttl=64 time=5.801 ms
84 bytes from 192.168.1.2 icmp_seq=4 ttl=64 time=10.324 ms
84 bytes from 192.168.1.2 icmp_seq=5 ttl=64 time=11.510 ms

PC1> arp

00:50:79:66:68:01  192.168.1.2 expires in 98 seconds

PC1> sh

NAME   IP/MASK              GATEWAY          MAC                LPORT  RHOST:PORT
PC1    192.168.1.1/24       192.168.1.4      00:50:79:66:68:00  20009  127.0.0.1:20010
       fe80::250:79ff:fe66:6800/64
```

Pc2:

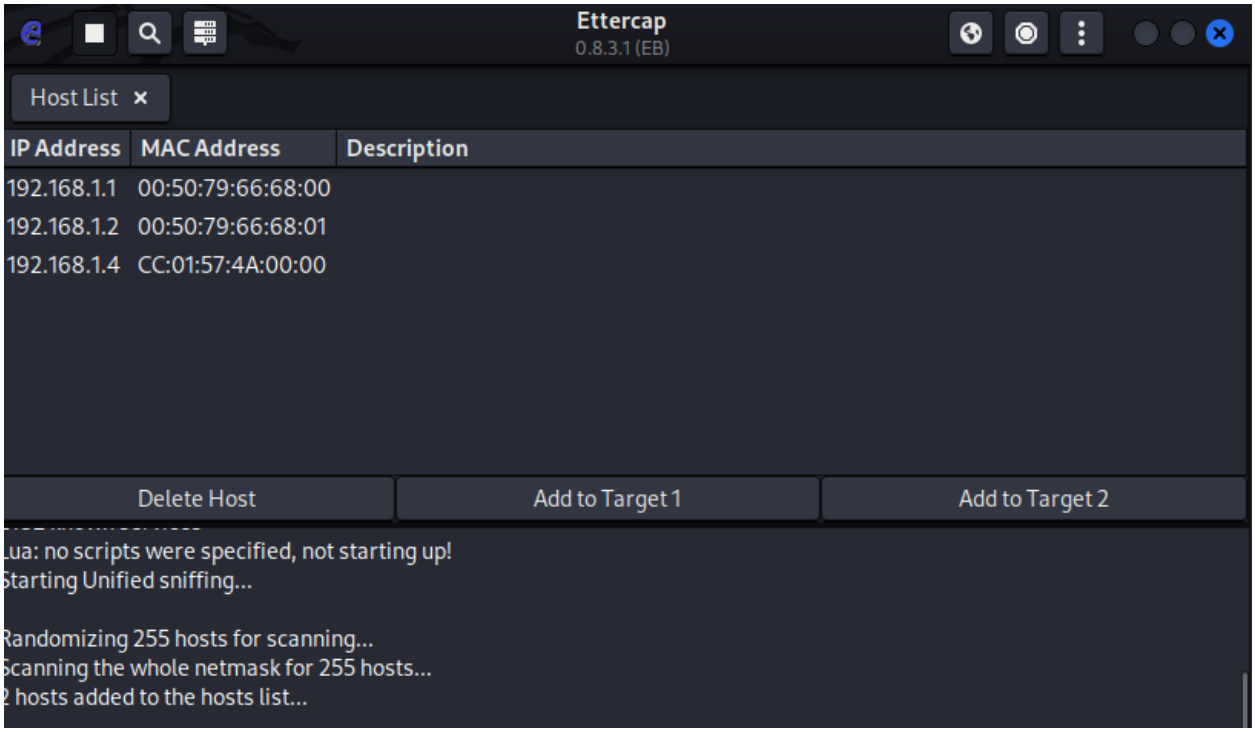
```
PC2> ping 192.168.1.1

84 bytes from 192.168.1.1 icmp_seq=1 ttl=64 time=29.150 ms
84 bytes from 192.168.1.1 icmp_seq=2 ttl=64 time=16.011 ms
^C
PC2> ping 192.168.1.3

84 bytes from 192.168.1.3 icmp_seq=1 ttl=64 time=9.719 ms
84 bytes from 192.168.1.3 icmp_seq=2 ttl=64 time=9.105 ms
84 bytes from 192.168.1.3 icmp_seq=3 ttl=64 time=7.376 ms
84 bytes from 192.168.1.3 icmp_seq=4 ttl=64 time=7.863 ms
^C
PC2> arp

00:0c:29:b6:7b:85  192.168.1.3 expires in 118 seconds
00:50:79:66:68:00  192.168.1.1 expires in 109 seconds

PC2>
PC2> sh

NAME   IP/MASK              GATEWAY          MAC                LPORT  RHOST:PORT
PC2    192.168.1.2/24       192.168.1.4      00:50:79:66:68:01  20011  127.0.0.1:20012
       fe80::250:79ff:fe66:6801/64
```

Attacker(kali):

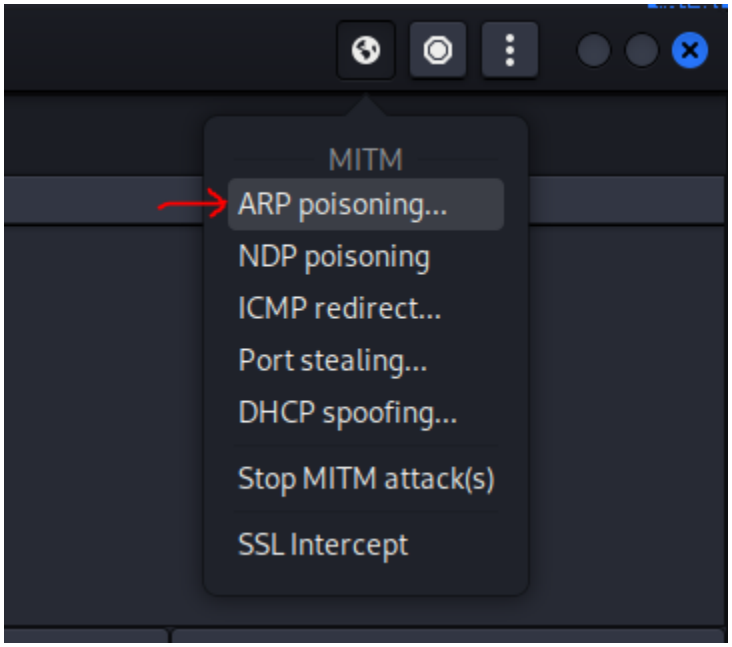
```
┌──(hadi㉿hadi)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:b6:7b:85 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.3/24 brd 192.168.1.255 scope global dynamic eth0
       valid_lft 86293sec preferred_lft 86293sec
    inet6 fe80::20c:29ff:feb6:7b85/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever

┌──(hadi㉿hadi)-[~]
└─$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=81.4 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=17.6 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=15.6 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=18.2 ms

── 192.168.1.1 ping statistics ──^C
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 15.608/33.184/81.376/27.839 ms
```

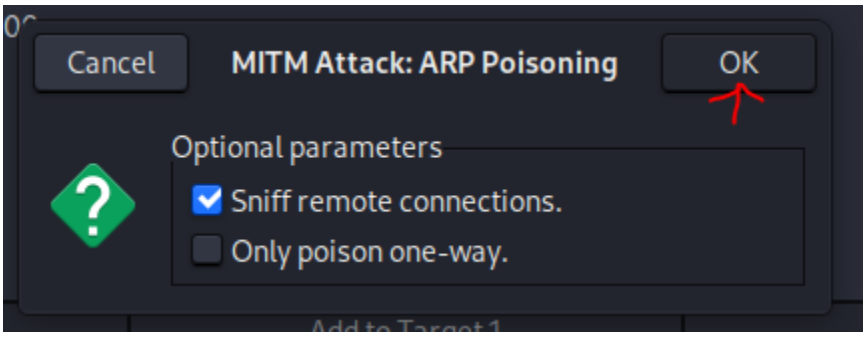
برای انجام حمله از ابزار EtterCap استفاده میکنیم. مراحل آن به شرح زیر است:

با استفاده از دکمه 1 میتوانیم شبکه را اسکن کنیم. سپس لیست هاست ها با استفاده از دکمه 2 قابل مشاهده است:

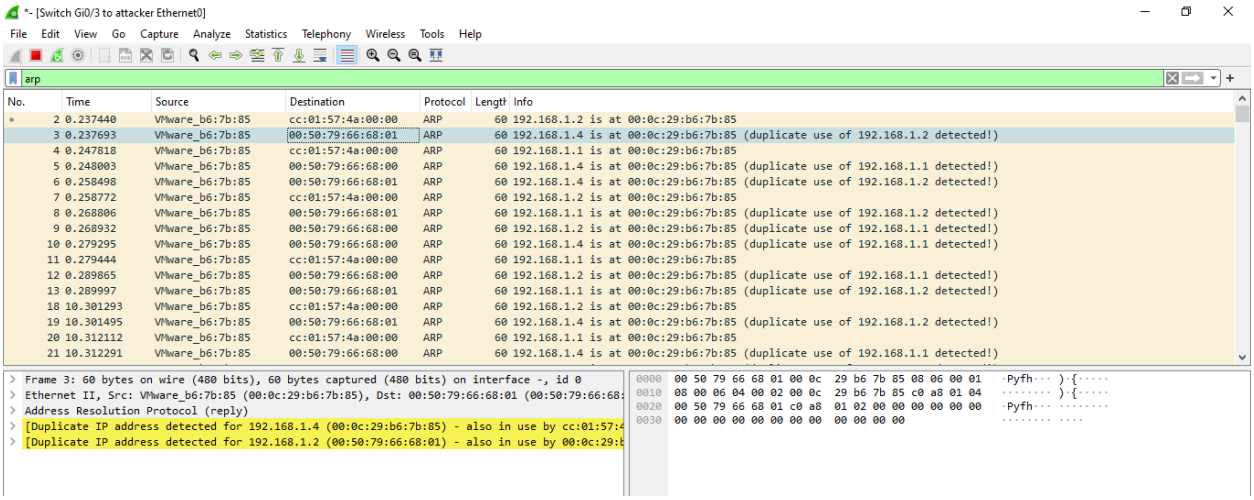


با کلیک روی دکمه شماره 3 و انتخاب گزینه arp poisioning میتوانیم حمله را انجام دهیم:





پس از شروع حمله، سیستم مهاجم پکت های arp را به صورت متوالی ارسال میکند:



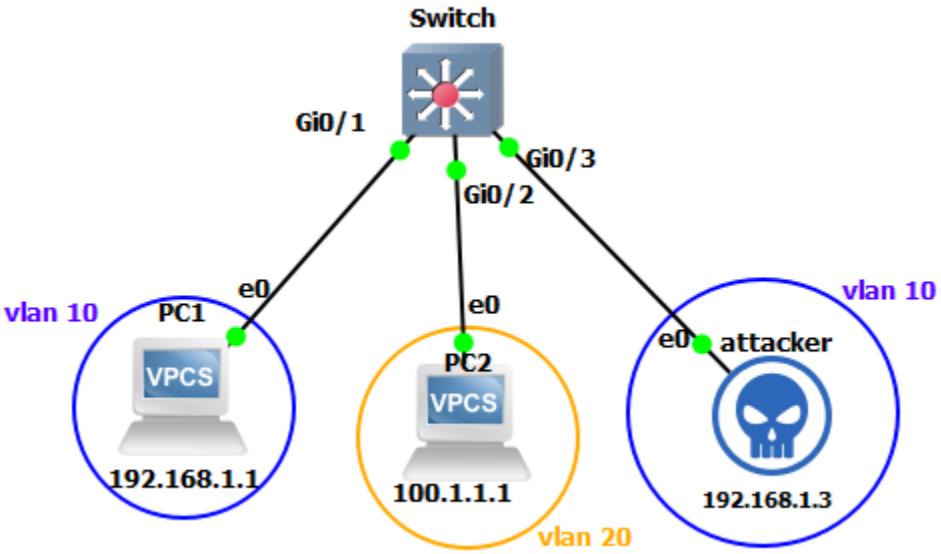
همانطور که مشاهده میشود برای آیپی های تکراری دو mac وجود دارد.

دستورات مقابله با حمله:

```
enable
configure terminal

! Enable DHCP Snooping
ip dhcp snooping
ip dhcp snooping vlan 1
ip dhcp snooping database flash:dhcp_snoop.txt

! Enable ARP Inspection
ip arp inspection vlan 1

! Trust the interface connected to the router
interface gigabitEthernet 0/0
 ip dhcp snooping trust
 ip arp inspection trust
 exit
```

عدم اعتبار پکت های ارسالی از اینترفیس مهاجم:

حمله VLAN Hopping:



دستورات ساخت vlan در سوییچ:

```
enable
configure terminal
vlan 10
exit
vlan 20
exit

int Gi0/2
switchport access vlan 20
exit

int Gi0/3
switchport access vlan 10
exit

int Gi0/1
switchport access vlan 10
exit
```

نمایش vlan های ساخته شده:

```
Switch#show vlan brief
*May 21 13:30:10.353: %SYS-5-CONFIG_I: Configured from console by console

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/0, Gi1/0, Gi1/1, Gi1/2
                                                Gi1/3, Gi2/0, Gi2/1, Gi2/2
                                                Gi2/3, Gi3/0, Gi3/1, Gi3/2
                                                Gi3/3
10   VLAN0010                         active    Gi0/1, Gi0/3
20   VLAN0020                         active    Gi0/2
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
Switch#
```

وضعیت اینترفیس ها قبل از حمله:

```
Switch#show interface status

Port      Name               Status       Vlan       Duplex  Speed Type
Gi0/0                        notconnect   1          a-full   auto RJ45
Gi0/1                        connected    1          a-full   auto RJ45
Gi0/2                        connected    1          a-full   auto RJ45
Gi0/3                        connected    1          a-full   auto RJ45
Gi1/0                        notconnect   1          a-full   auto RJ45
Gi1/1                        notconnect   1          a-full   auto RJ45
Gi1/2                        notconnect   1          a-full   auto RJ45
Gi1/3                        notconnect   1          a-full   auto RJ45
Gi2/0                        notconnect   1          a-full   auto RJ45
Gi2/1                        notconnect   1          a-full   auto RJ45
Gi2/2                        notconnect   1          a-full   auto RJ45
Gi2/3                        notconnect   1          a-full   auto RJ45
Gi3/0                        notconnect   1          a-full   auto RJ45
Gi3/1                        notconnect   1          a-full   auto RJ45
Gi3/2                        notconnect   1          a-full   auto RJ45
Gi3/3                        notconnect   1          a-full   auto RJ45
Switch#
```

اجرای حمله با استفاده از yersinia انجام می‌شود:

sudo yersinia dtp -attack 1 -i eth0

```
┌──(hadi㉿hadi)-[~]
└─$ sudo yersinia dtp -attack 1 -i eth0
[sudo] password for hadi:
Warning: Couldn't allocate kernel memory for filter: try increasing net.core.optmem_max with sysctl
<*> Starting NONDOS attack enabling trunking...
<*> Press any key to stop the attack <*>
```

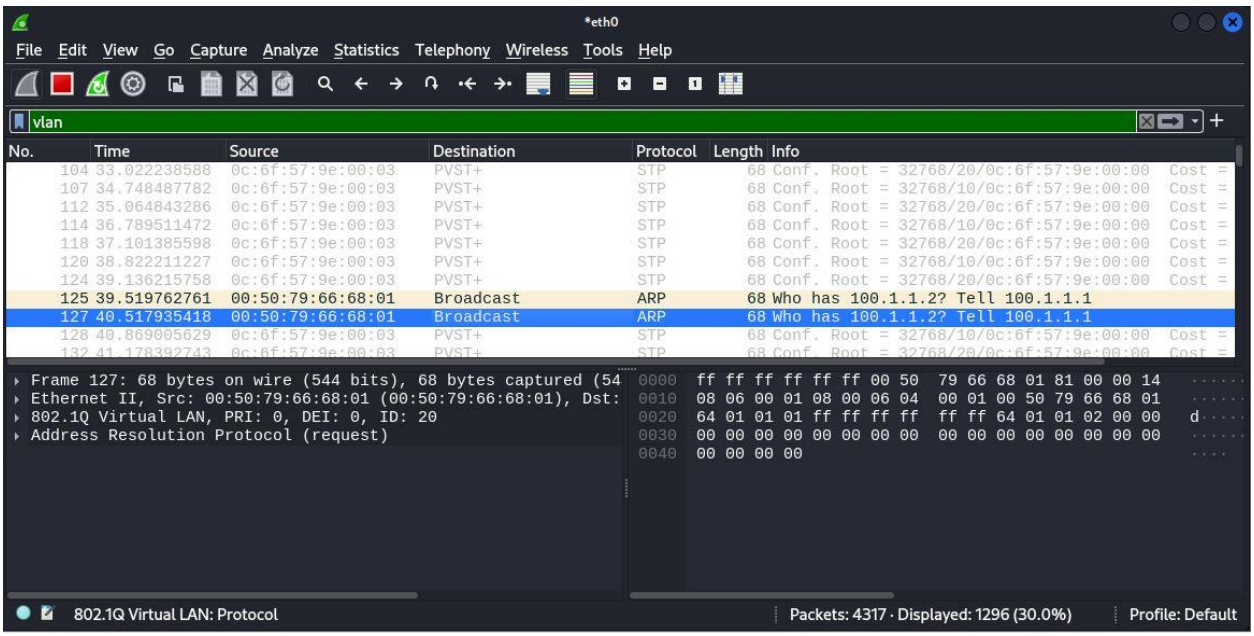
نمایش لاگ های DTP در سوییچ:

```
Switch#debug dtp events
DTP events debugging is on
Switch#
*May 22 15:30:37.542: DTP-event:Gi0/3:Received packet event ../dyntrk/dyntrk_process.c:2219
*May 22 15:30:38.510: DTP-event:Gi0/3:Received packet event ../dyntrk/dyntrk_process.c:2219
*May 22 15:30:39.547: DTP-event:Gi0/3:Received packet event ../dyntrk/dyntrk_process.c:2219
```

پس از آن، پورت مربوط به مهاجم با موفقیت در حالت trunk قرار میگیرد:

```
Switch#show interface status
*May 22 15:31:39.934: DTP-event:Gi0/3:Received packet event ../dyntrk/dyntrk_process.c:2219

Port      Name               Status       Vlan       Duplex  Speed Type
Gi0/0                        notconnect   1          a-full   auto RJ45
Gi0/1                        connected    1          a-full   auto RJ45
Gi0/2                        connected    1          a-full   auto RJ45
Gi0/3                        connected    trunk      a-full   auto RJ45
Gi1/0                        notconnect   1          a-full   auto RJ45
Gi1/1                        notconnect   1          a-full   auto RJ45
Gi1/2                        notconnect   1          a-full   auto RJ45
Gi1/3                        notconnect   1          a-full   auto RJ45
Gi2/0                        notconnect   1          a-full   auto RJ45
Gi2/1                        notconnect   1          a-full   auto RJ45
Gi2/2                        notconnect   1          a-full   auto RJ45
Gi2/3                        notconnect   1          a-full   auto RJ45
Gi3/0                        notconnect   1          a-full   auto RJ45
Gi3/1                        notconnect   1          a-full   auto RJ45
Gi3/2                        notconnect   1          a-full   auto RJ45
Gi3/3                        notconnect   1          a-full   auto RJ45
Switch#
```

حالا مهاجم میتواند پکت های مربوط به vlan دیگر را مشاهده کند:



دستورات مربوط به مقابله با حمله:

```
switchport mode access
switchport nonegotiate
```