

گزارش آزمایش پنجم

نظری

تفاوت تست نفوذ و ارزیابی آسیب پذیری

اسکن آسیب پذیری یا ارزیابی آسیب پذیری صرفاً به دنبال یافتن آسیب پذیری‌ها در یک برنامه کاربردی یا شبکه می‌باشد. این تکنیک برای تخمین میزان و حجم آسیب پذیری‌های مختلف مورد استفاده قرار می‌گیرد. ارزیابی آسیب پذیری شامل استفاده از ابزارهای خودکار (مانند Burp suite، nessus و ..) به منظور یافتن آسیب پذیری‌ها می‌باشد که نتایج آن در قالب یک گزارش (معمولاً خودکار تولید شده) به شما ارائه می‌شود. به طور خلاصه **ارزیابی آسیب پذیری بر شناسایی نقاط ضعف و آسیب پذیری‌های بالقوه در سیستم‌ها تمرکز دارد.**

تست نفوذ شبکه یک سرویس امنیتی است که آسیب پذیری‌های امنیتی در شبکه‌ها، سیستم‌ها، میزبان‌ها و دستگاه‌ها را با استفاده از تکنیک‌های مخرب برای آزمایش پاسخ‌های امنیتی شبکه شناسایی می‌کند. هدف از آزمایش نفوذ شبکه، شناسایی اکسپلویت (Exploits) های امنیتی است قبل از اینکه هکرها بتوانند آن‌ها را کشف و از آن‌ها بهره‌برداری کنند. این اکسپلویت‌ها می‌توانند باعث نقض داده‌ها و اطلاعات کسب و کار شوند. با انجام این کار، به هکرهای اخلاقی اجازه داده می‌شود تا با استفاده از هر وسیله‌ای که لازم است، سعی کنند به شبکه مورد نظر نفوذ کنند. به طور خاص، با استفاده از روش‌هایی که یک هکر واقعی استفاده می‌کند. به غیر از میزان امنیت سایبری، که باید قبل از تست نفوذ شبکه انجام شود، تست نفوذ شبکه یکی از بالاترین سطوح تضمین امنیتی یک کسب و کار را فراهم می‌کند. به طور خلاصه **هکرهاى اخلاقى از نقاط ضعف برای نفوذ به سیستم‌ها و شبکه‌ها استفاده می‌کنند.**

مکانیزم‌های امنیتی برای مقابله با حملات

نوع حمله

MAC Flooding:

در این نوع حمله، مهاجم با ارسال تعداد زیادی آدرس MAC جعلی، سوییچ شبکه را تحت فشار قرار داده و باعث اختلال در ترافیک مجاز می‌شوند. وقتی که جدول آدرس MAC در یک سوییچ پر شود، سوییچ دیگر نمی‌تواند آدرس‌های MAC مجاز را ذخیره کند. این امر سوییچ را دچار سردرگمی می‌کند و باعث می‌شود تمام بسته‌های داده ورودی را به هر پورت روی شبکه پخش کند. این کار ترافیک مجاز را مختل کرده و اطلاعات حساس را در معرض دید قرار می‌دهد.

مکانیزم مقابله با حمله

Port Security: سوییچ‌ها می‌توانند تعداد آدرس‌های مک مجاز در یک پورت خاص را محدود کنند. این کار از اتصال دستگاه‌های غیرمجاز و ایجاد ترافیک سیل آسا در شبکه جلوگیری می‌کند.

فیلترینگ مک آدرس (MAC Address Filtering): می‌توانیم سوییچ‌ها را طوری پیکربندی کنیم که فقط آدرس‌های مک خاصی را در هر پورت بپذیرند. این رویکرد Whitelist اطمینان می‌دهد که فقط دستگاه‌های مجاز می‌توانند متصل شوند و از ارسال آدرس‌های جعلی توسط افراد خارجی به منظور ایجاد ترافیک سیل آسا جلوگیری می‌کند.

تقسیم‌بندی شبکه (Network Segmentation): تقسیم شبکه به VLAN ها می‌تواند تأثیر حمله سیل آسا آدرس مک را محدود کند. اگر یک VLAN به خطر بیفتد، حمله در همان بخش محدود می‌شود و از سایر قسمت‌های شبکه محافظت می‌کند.

نوع حمله

DHCP Attack:

DHCP یک سرویس در شبکه است که به طور خودکار آدرس‌های IP را به دستگاه‌ها اختصاص می‌دهد. حملات سوءاستفاده از سرویس DHCP این پروتکل را هدف قرار می‌دهند تا عملکرد شبکه را مختل کنند.

DHCP Starvation Attack: این حمله به دنبال محروم کردن دستگاه‌های مجاز از دسترسی به شبکه با خالی کردن pool آدرس‌های IP موجودی است که توسط سرور DHCP ارائه می‌شود. در این صورت سرور قادر نخواهد بود به سیستم‌های مجاز IP تخصیص دهد.

DHCP Spoofing Attack: این حمله به دنبال فریب دادن دستگاه‌ها برای اتصال به یک سرور DHCP جعلی است که توسط مهاجم کنترل می‌شود.

مکانیزم مقابله با حمله

سرور DHCP:

فعال کردن DHCP snooping روی سوییچ‌ها: این ویژگی مجاز بودن پیام‌های DHCP را تأیید می‌کند و از دستگاه‌های غیرمجاز برای جعل آدرس‌های IP جلوگیری می‌کند.

کانفیگ رزرو سرور DHCP: آدرس‌های IP خاصی را برای دستگاه‌های حیاتی رزرو می‌کنیم تا اطمینان حاصل شود که همیشه به آنها دسترسی داشته باشیم.

محدود کردن pool آدرس IP: بهتر است کل استخر آدرس‌های IP را اختصاص داده نشوند و بخشی را برای دستگاه‌های حیاتی رزرو کنیم و اندازه کلی را برای جلوگیری از خالی شدن در طول حمله محدود کنیم.

امنیت سوئیچ شبکه:

DHCP Snooping: این ویژگی ترافیک DHCP را کنترل می‌کند و مجاز بودن پیام‌های DHCP را تأیید می‌کند. ردیابی DHCP می‌تواند سرورهای DHCP جعلی را شناسایی کرده و از جعل آدرس‌های IP توسط آنها جلوگیری کند.

Port Security: می‌توانیم با محدود کردن تعداد آدرس‌های مک مجاز در یک پورت سوئیچ از اتصال دستگاه‌های غیرمجاز و ایجاد ترافیک سیل آسا در شبکه با درخواست‌های DHCP جعلی جلوگیری کنیم.

نوع حمله

VLAN Hopping:

VLAN Hopping به سوءاستفاده از یک ضعف امنیتی شبکه برای دسترسی به منابع شبکه در یک VLAN اشاره دارد که یک دستگاه به طور معمول مجوز دسترسی به آن را ندارد. این روش به مهاجمان روی یک VLAN خاص این امکان را می‌دهد که از موانع امنیتی عبور کرده و به VLAN دیگری برسند.

Spoofing: مهاجم با ارسال پیام‌های جعلی سوئیچ‌های شبکه را دستکاری و فریب می‌دهد تا باور کند دستگاه مهاجم مجوز دسترسی به VLAN هدف را دارد. هنگامی که سوئیچ فریب خورد، به ترافیک مهاجم اجازه می‌دهد تا به VLAN هدف وارد شود.

Double Tagging: در این حمله مهاجم از قابلیت IEEE 802.1Q که برای تگ گذاری VLAN استفاده می‌شود، سوء استفاده می‌کند. این استاندارد به فریم‌ها اجازه می‌دهد تا تگی را حمل کنند که VLAN متعلق به آن را مشخص می‌کند. در Double Tagging، مهاجم فریمی را با دو تگ VLAN ارسال می‌کند. اولین تگ، عضویت واقعی VLAN مهاجم را مشخص می‌کند و تگ دوم، VLAN هدف را که مهاجم می‌خواهد به آن دسترسی پیدا کند، مشخص می‌کند. اولین سوئیچی که فریم با آن مواجه می‌شود، به طور معمول تگ بیرونی (VLAN مهاجم) را طبق انتظار حذف می‌کند. سوئیچ دوم که از این دستکاری بی‌خبر است، تگ داخلی باقی‌مانده (VLAN هدف) را می‌بیند و فریم را به گونه‌ای ارسال می‌کند که گویی از VLAN هدف نشأت گرفته است. این امر دسترسی غیرمجاز به VLAN هدف را اعطا می‌کند.

مکانیزم مقابله با حمله

Port Security: می توانیم با محدود کردن تعداد آدرس های مک مجاز در یک پورت سوئیچ از اتصال دستگاه های غیرمجاز و ایجاد ترافیک سیل آسا در شبکه با درخواست های DHCP جعلی جلوگیری کنیم.

همچنین می توانیم قابلیت هایی مانند احراز هویت MAC را فعال کنیم، که نیازمند آن است تا دستگاه ها قبل از دسترسی به شبکه، هویت خود را با استفاده از یک آدرس MAC از قبل کانفیگ شده ثابت کنند.

فهرست های کنترل دسترسی (ACL:VLAN (ACLs) ها را برای محدود کردن جریان ترافیک بین VLAN ها می توانیم کانفیگ کنیم و فقط ارتباط مجاز بین VLAN های خاص را مجاز تعریف می کنیم تا دسترسی غیرمجاز مسدود شود.

نوع حمله

:ARP Spoofing

در یک حمله جعلی ARP، مهاجم پیام های ARP مخرب را به LAN ارسال می کند. این پیام ها ادعا می کنند که دستگاه مهاجم دارای آدرس MAC مرتبط با آدرس IP گیرنده مورد نظر است از این طریق مهاجم می تواند داده ها را بخواند، تغییر دهد و یا ارتباط را با دور ریختن داده ها قطع کند.

مکانیزم مقابله با حمله

ورودی های استاتیک ARP: می توانیم ورودی های استاتیک ARP را روی دستگاه های حیاتی مانند روترها، پرینترها یا سرورها کانفیگ کنیم. این کار به دستگاه ما می گوید که همیشه یک آدرس IP خاص را با یک آدرس MAC خاص مرتبط کند، با این کار از نیاز به اتکا به درخواست های ARP عبور کرده و احتمال فریب خوردن توسط ورودی های جعلی را کاهش می دهد.

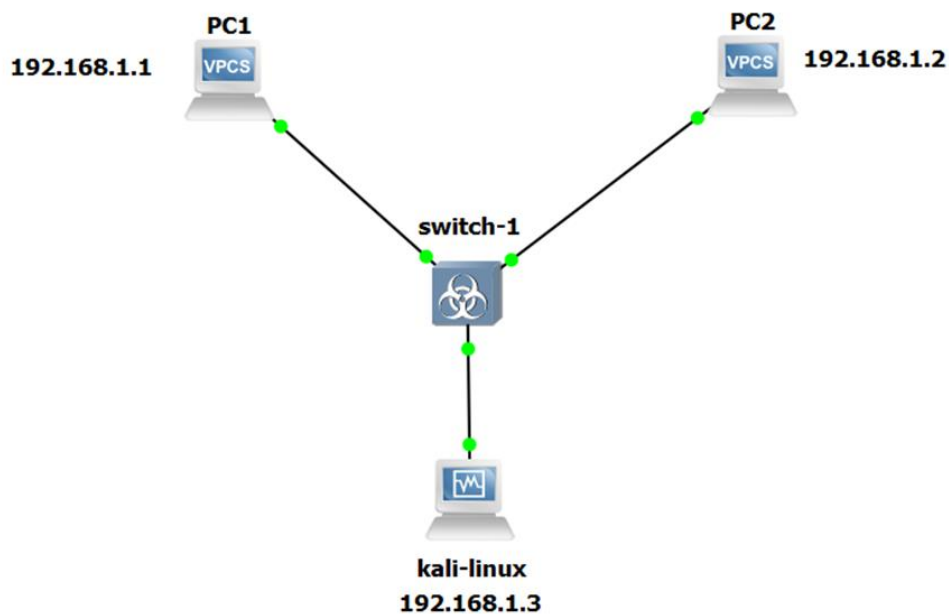
Port Security: می توانیم با محدود کردن تعداد آدرس های مک مجاز در یک پورت سوئیچ از اتصال دستگاه های غیرمجاز و ایجاد ترافیک سیل آسا در شبکه با درخواست های جعلی جلوگیری کنیم.

تقسیم بندی شبکه (Network Segmentation): تقسیم شبکه به VLAN ها می تواند تأثیر حمله جعلی ARP را محدود کند. اگر مهاجمی موفق به جعل یک ورودی ARP شود، تنها بر دستگاه های موجود در همان بخش VLAN تأثیر می گذارد، نه کل شبکه. محافظت می کند.

عملی

:MAC Flooding

توپولوژی در نظر گرفته شده برای این حمله به صورت زیر می باشد.



سپس ip ماشین ها را ست می کنیم.

```
switch PC1 PC2
PC1> ip 192.168.1.1 255.255.255.0 192.168.1.100
Checking for duplicate address...
PC1 : 192.168.1.1 255.255.255.0 gateway 192.168.1.100
PC1> show ip
NAME      : PC1[1]
IP/MASK    : 192.168.1.1/24
GATEWAY    : 192.168.1.100
DNS        :
MAC        : 00:50:79:66:68:00
LPORT     : 20005
RHOST:PORT : 127.0.0.1:20006
MTU        : 1500
```

```
switch PC1 PC2
Welcome to Virtual PC Simulator, version 0.8.3
Dedicated to Daling.
Build time: Sep 9 2023 11:15:00
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

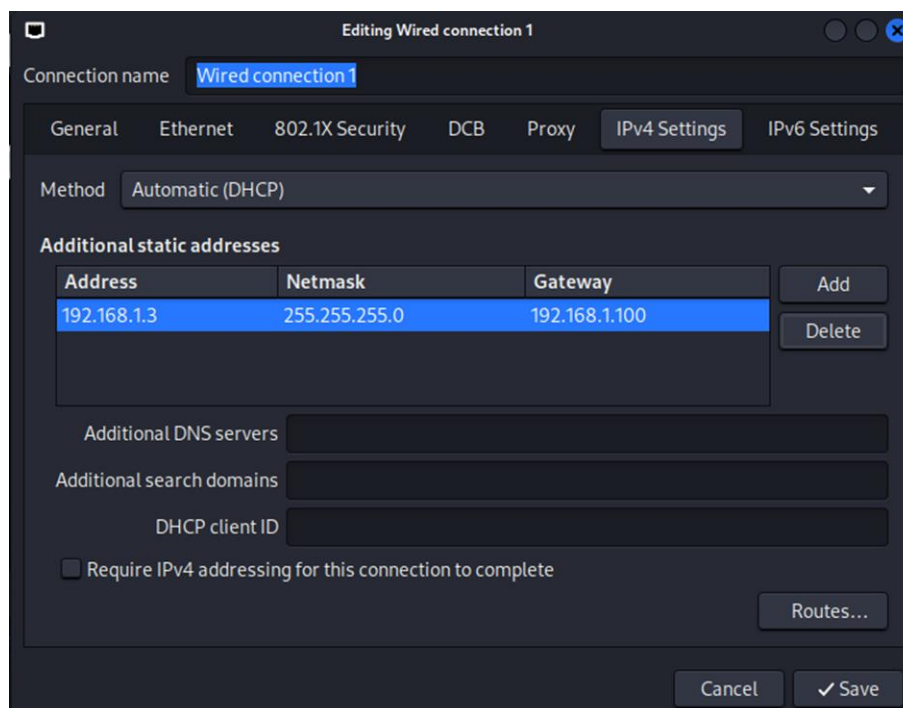
Executing the startup file

PC2> ip 192.168.1.2 255.255.255.0 192.168.1.100
Checking for duplicate address...
PC2 : 192.168.1.2 255.255.255.0 gateway 192.168.1.100

PC2> show ip

NAME      : PC2[1]
IP/MASK    : 192.168.1.2/24
GATEWAY    : 192.168.1.100
DNS        :
MAC        : 00:50:79:66:68:01
LPORT     : 20007
RHOST:PORT : 127.0.0.1:20008
MTU        : 1500
```

برای ماشین kali مطابق روش زیر با gui از طریق settings > Advanced Network Configurations ، ip را ست می کنیم یا از طریق command ، sudo nano /etc/network/interfaces فایل interfaces ها را باز کرده و ip مورد نظر را ست می کنیم.



```

(root@kali)-[~]
# sudo nano /etc/network/interfaces

(root@kali)-[~]
# sudo systemctl restart networking.service

(root@kali)-[~]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.3 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:fe1e:364a prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:1e:36:4a txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 31 bytes 3636 (3.5 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 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 20 bytes 1344 (1.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 20 bytes 1344 (1.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

سپس برای بررسی اینکه pc ها به درستی به هم متصل شده اند پینگ می گیریم.

```
PC1> ping 192.168.1.2
```

```

84 bytes from 192.168.1.2 icmp_seq=1 ttl=64 time=13.175 ms
84 bytes from 192.168.1.2 icmp_seq=2 ttl=64 time=35.055 ms
84 bytes from 192.168.1.2 icmp_seq=3 ttl=64 time=3.707 ms
84 bytes from 192.168.1.2 icmp_seq=4 ttl=64 time=10.903 ms
84 bytes from 192.168.1.2 icmp_seq=5 ttl=64 time=27.435 ms

```

```
PC2> ping 192.168.1.1
```

```

84 bytes from 192.168.1.1 icmp_seq=1 ttl=64 time=12.255 ms
84 bytes from 192.168.1.1 icmp_seq=2 ttl=64 time=55.889 ms
84 bytes from 192.168.1.1 icmp_seq=3 ttl=64 time=31.397 ms
84 bytes from 192.168.1.1 icmp_seq=4 ttl=64 time=66.400 ms
84 bytes from 192.168.1.1 icmp_seq=5 ttl=64 time=51.750 ms

```

```

root@kali: ~
File Actions Edit View Help

(root@kali)-[~]
# 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=21.7 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=11.4 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=23.7 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=12.9 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=5.19 ms
64 bytes from 192.168.1.1: icmp_seq=6 ttl=64 time=3.76 ms
64 bytes from 192.168.1.1: icmp_seq=7 ttl=64 time=2.64 ms
64 bytes from 192.168.1.1: icmp_seq=8 ttl=64 time=2.03 ms

```

برای شروع حمله، مهاجم (kali) دستور زیر را وارد می کند.

```
(root@kali)-[~]  
# sudo macof -i eth0
```

و با ارسال تعداد زیادی آدرس mac ، جدول آدرس mac سوییچ را پر می کند.

```
root@kali: ~  
File Actions Edit View Help  
in 512  
f0:e8:8:66:41:ce 10:61:92:1:a6:9a 0.0.0.0.9785 > 0.0.0.0.44164: S 748646674:748646674(0) win 5  
12  
60:5a:ca:72:4f:d8 63:ab:f8:66:e8:5a 0.0.0.0.7102 > 0.0.0.0.2012: S 788099689:788099689(0) win  
512  
cc:56:a:4f:f8:ab d4:99:77:7d:2:ae 0.0.0.0.59147 > 0.0.0.0.8308: S 1087651827:1087651827(0) win  
512  
76:42:fd:2b:c0:4f c8:c:26:46:16:d1 0.0.0.0.2597 > 0.0.0.0.4257: S 615464532:615464532(0) win 5  
12  
e2:54:e2:4f:2d:b0 21:35:6:4b:20:37 0.0.0.0.44966 > 0.0.0.0.42708: S 656253116:656253116(0) win  
512  
79:d3:7c:37:b0:6d a8:fe:59:7e:42:a2 0.0.0.0.46624 > 0.0.0.0.33470: S 2021010392:2021010392(0)  
win 512  
a9:b6:c2:50:c2:92 24:14:84:72:59:da 0.0.0.0.37081 > 0.0.0.0.28158: S 1967819877:1967819877(0)  
win 512  
3c:6a:98:2b:75:26 48:44:c3:5f:fc:15 0.0.0.0.22009 > 0.0.0.0.36155: S 684666151:684666151(0) wi  
n 512  
9d:1:a8:5c:ec:60 54:e9:2e:22:47:5b 0.0.0.0.57121 > 0.0.0.0.14671: S 1736000123:1736000123(0) w  
in 512  
7d:4:ba:6b:60:31 a1:16:91:7f:df:76 0.0.0.0.59374 > 0.0.0.0.40084: S 974269943:974269943(0) win  
512  
68:d5:8:3b:de:fd c8:53:4b:3c:7c:34 0.0.0.0.25502 > 0.0.0.0.59860: S 221146550:221146550(0) win  
512  
6e:7a:39:d:29:d9 ce:11:b3:8:2b:93 0.0.0.0.47713 > 0.0.0.0.5010: S 1040619769:1040619769(0) win  
512  
65:94:9d:2:36:c7 22:c5:94:50:34:ad 0.0.0.0.10049 > 0.0.0.0.42501: S 309898125:309898125(0) win  
512  
b3:e:f1:0:76:ce a9:99:7f:73:b8:9f 0.0.0.0.3426 > 0.0.0.0.59025: S 821778909:821778909(0) win 5  
12  
da:8f:4c:10:80:12 dc:74:94:6c:a7:ba 0.0.0.0.22615 > 0.0.0.0.57356: S 1491914887:1491914887(0)
```

پس از اجرای حمله جدول آدرس mac سوییچ با mac های جعلی به جای mac سیستم های مجاز و واقعی پر می شود.


```
Switch>show mac address-table
Mac Address Table
-----
Vlan    Mac Address      Type      Ports
-----
1       0030.e71e.f834    DYNAMIC   Gi0/0
1       004d.7b55.577b    DYNAMIC   Gi0/0
1       0050.7966.6800    DYNAMIC   Gi0/2
1       0050.7966.6801    DYNAMIC   Gi0/1
1       005e.9404.073c    DYNAMIC   Gi0/0
1       005f.a01c.0c73    DYNAMIC   Gi0/0
1       0063.7300.380b    DYNAMIC   Gi0/0
1       0066.9010.d1ae    DYNAMIC   Gi0/0
1       007b.507d.da0b    DYNAMIC   Gi0/0
1       0092.a03f.7ea1    DYNAMIC   Gi0/0
1       00a2.4627.d199    DYNAMIC   Gi0/0
1       00b2.403a.1936    DYNAMIC   Gi0/0
1       00be.cc46.b97e    DYNAMIC   Gi0/0
1       00df.c571.a25c    DYNAMIC   Gi0/0
1       00ef.4e2a.88d4    DYNAMIC   Gi0/0
1       00f3.8c47.8f3a    DYNAMIC   Gi0/0
1       0104.9c4c.1a91    DYNAMIC   Gi0/0
1       0117.6678.17b1    DYNAMIC   Gi0/0
1       0127.3b13.fcd8    DYNAMIC   Gi0/0
1       0128.1221.0aca    DYNAMIC   Gi0/0
1       0154.5111.0926    DYNAMIC   Gi0/0
1       0159.8c05.7362    DYNAMIC   Gi0/0
1       016a.4e2a.8405    DYNAMIC   Gi0/0
1       0172.2d60.db59    DYNAMIC   Gi0/0
1       0175.2c1d.cfa6    DYNAMIC   Gi0/0
1       017b.436c.371e    DYNAMIC   Gi0/0
1       017e.1602.87c5    DYNAMIC   Gi0/0
1       0180.8a13.79aa    DYNAMIC   Gi0/0
1       0181.1639.06f4    DYNAMIC   Gi0/0
1       0183.6a41.5d90    DYNAMIC   Gi0/0
```

solarwinds | Solar-PuTTY free tool © 2019-2023 SolarWinds Worldwide, LLC. All rights reserved.

برای جلوگیری از این حمله از مکانیزم Port Security استفاده کرده و ماکسیمم تعداد mac هایی را که یک interface می تواند دریافت کند را در این مثال به دو کاهش می دهیم. سپس سوییچ را طوری کانفیگ می کنیم که آدرس mac سیستم های متصل به آن را به صورت dynamic بشناسد تا از اتصال سیستم های غیرمجاز جلوگیری شود.

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int g0/0
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport host
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled

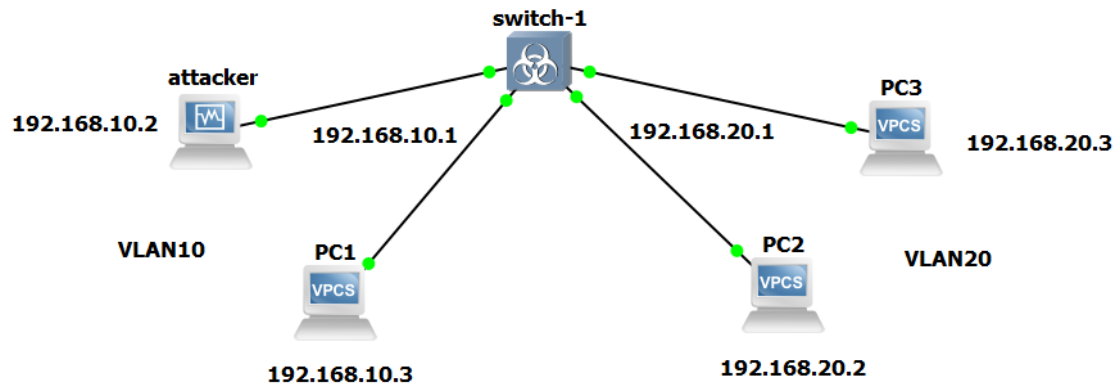
Switch(config-if)#switchport port-security maximum 2
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#exit
```

پس از انجام مجدد حمله در این حالت این interface، down می شود.

```
Switch(config)#  
Switch(config)#  
*May 22 13:06:57.747: %PM-4-ERR_DISABLE: psecure-violation error detected on Gi0/0, putting Gi0/0 in err-disable state  
*May 22 13:06:57.759: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 9021.6a57.0c  
9e on port GigabitEthernet0/0.  
*May 22 13:06:58.754: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to down  
*May 22 13:06:59.795: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to down
```

VLAN hopping

توپولوژی در نظر گرفته شده برای این حمله به صورت زیر می باشد.



ip ماشین ها را ست می کنیم

```
PC1> ip 192.168.10.3 255.255.255.0 192.168.10.1
Checking for duplicate address...
PC1 : 192.168.10.3 255.255.255.0 gateway 192.168.10.1
```

```
PC2> ip 192.168.20.2 255.255.255.0 192.168.20.1
Checking for duplicate address...
PC2 : 192.168.20.2 255.255.255.0 gateway 192.168.20.1
```

```
PC3> ip 192.168.20.3 255.255.255.0 192.168.20.1
Checking for duplicate address...
PC3 : 192.168.20.3 255.255.255.0 gateway 192.168.20.1
```

برای ست کردن ip ماشین ubuntu می توانیم از روش مشابه kali استفاده کنیم.

Editing Wired connection 1

Connection name: Wired connection 1

General Ethernet 802.1X Security DCB Proxy **IPv4 Settings** IPv6 Settings

Method: Manual

Addresses

| Address | Netmask | Gateway |
|--------------|---------------|--------------|
| 192.168.10.2 | 255.255.255.0 | 192.168.10.1 |

Add Delete

DNS servers

Search domains

DHCP client ID

☐ Require IPv4 addressing for this connection to complete

Routes...

Cancel Save

سپس vlan بندی می کنیم.

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name VLAN10
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name VLAN20
Switch(config-vlan)#end
```

```
Switch#show vlan
```

| VLAN | Name | Status | Ports |
|------|--------------------|-----------|--|
| 1 | default | active | Gi0/0, Gi0/1, Gi0/2, Gi0/3 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 | VLAN10 | active | |
| 20 | VLAN20 | active | |
| 1002 | fddi-default | act/unsup | |
| 1003 | token-ring-default | act/unsup | |
| 1004 | fddinet-default | act/unsup | |
| 1005 | trnet-default | act/unsup | |

| VLAN | Type | SAID | MTU | Parent | RingNo | BridgeNo | Stp | BrdgMode | Trans1 | Trans2 |
|------|-------|--------|------|--------|--------|----------|------|----------|--------|--------|
| 1 | enet | 100001 | 1500 | - | - | - | - | - | 0 | 0 |
| 10 | enet | 100010 | 1500 | - | - | - | - | - | 0 | 0 |
| 20 | enet | 100020 | 1500 | - | - | - | - | - | 0 | 0 |
| 1002 | fddi | 101002 | 1500 | - | - | - | - | - | 0 | 0 |
| 1003 | tr | 101003 | 1500 | - | - | - | - | - | 0 | 0 |
| 1004 | fdnet | 101004 | 1500 | - | - | - | ieee | - | 0 | 0 |
| 1005 | trnet | 101005 | 1500 | - | - | - | ibm | - | 0 | 0 |

--More--

سپس برای بررسی اینکه pc ها به درستی به هم متصل شده اند پینگ می گیریم. Pc های یک vlan یکدیگر را پینگ می کنند اما pc های vlan های دیگر را پینگ نمی کنند.

```
PC1> ping 192.168.20.2
host (192.168.10.1) not reachable
```

```
PC1> ping 192.168.10.2
84 bytes from 192.168.10.2 icmp_seq=1 ttl=64 time=4.287 ms
84 bytes from 192.168.10.2 icmp_seq=2 ttl=64 time=14.582 ms
84 bytes from 192.168.10.2 icmp_seq=3 ttl=64 time=4.923 ms
84 bytes from 192.168.10.2 icmp_seq=4 ttl=64 time=4.866 ms
84 bytes from 192.168.10.2 icmp_seq=5 ttl=64 time=4.851 ms
```

```
PC3> ping 192.168.10.2
host (192.168.20.1) not reachable
```

```
PC3> ping 192.168.20.2
84 bytes from 192.168.20.2 icmp_seq=1 ttl=64 time=4.269 ms
84 bytes from 192.168.20.2 icmp_seq=2 ttl=64 time=5.793 ms
84 bytes from 192.168.20.2 icmp_seq=3 ttl=64 time=6.112 ms
84 bytes from 192.168.20.2 icmp_seq=4 ttl=64 time=2.694 ms
84 bytes from 192.168.20.2 icmp_seq=5 ttl=64 time=3.524 ms
```

```
homa@homa-VirtualBox: ~  
homa@homa-VirtualBox:~$ 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  
        valid_lft forever preferred_lft forever  
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000  
    link/ether 08:00:27:38:3e:03 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.10.2/24 brd 192.168.10.255 scope global noprefixroute enp0s3  
        valid_lft forever preferred_lft forever  
    inet6 fe80::51ca:b8c5:5668:d3fa/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
homa@homa-VirtualBox:~$ ping 192.168.10.3  
PING 192.168.10.3 (192.168.10.3) 56(84) bytes of data.  
64 bytes from 192.168.10.3: icmp_seq=1 ttl=64 time=3.78 ms  
64 bytes from 192.168.10.3: icmp_seq=2 ttl=64 time=3.56 ms  
64 bytes from 192.168.10.3: icmp_seq=3 ttl=64 time=1.82 ms  
64 bytes from 192.168.10.3: icmp_seq=4 ttl=64 time=4.33 ms  
64 bytes from 192.168.10.3: icmp_seq=5 ttl=64 time=3.05 ms  
64 bytes from 192.168.10.3: icmp_seq=6 ttl=64 time=4.15 ms  
64 bytes from 192.168.10.3: icmp_seq=7 ttl=64 time=4.78 ms  
64 bytes from 192.168.10.3: icmp_seq=8 ttl=64 time=3.71 ms  
64 bytes from 192.168.10.3: icmp_seq=9 ttl=64 time=2.65 ms  
64 bytes from 192.168.10.3: icmp_seq=10 ttl=64 time=3.22 ms  
64 bytes from 192.168.10.3: icmp_seq=11 ttl=64 time=13.9 ms  
^C  
--- 192.168.10.3 ping statistics ---  
11 packets transmitted, 11 received, 0% packet loss, time 10014ms  
rtt min/avg/max/mdev = 1.820/4.451/13.913/3.091 ms  
homa@homa-VirtualBox:~$
```

وضعیت interface ها را قبل از حمله در سوییچ مشاهده می کنیم.

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

برای مشاهده جزئیات حمله در سوییچ دستور زیر را وارد می کنیم.

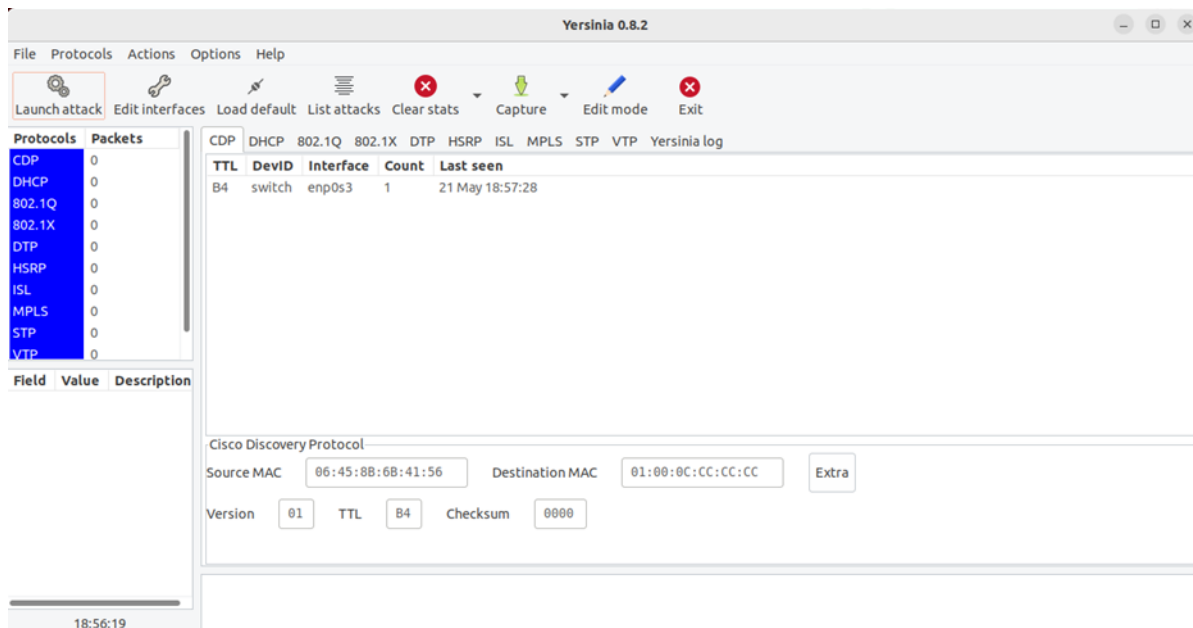
```
Switch>en
Switch#debug dtp event
DTP events debugging is on
```

برای شروع حمله، مهاجم دستور زیر را وارد کرده و ابزار yersinia را باز می کند.

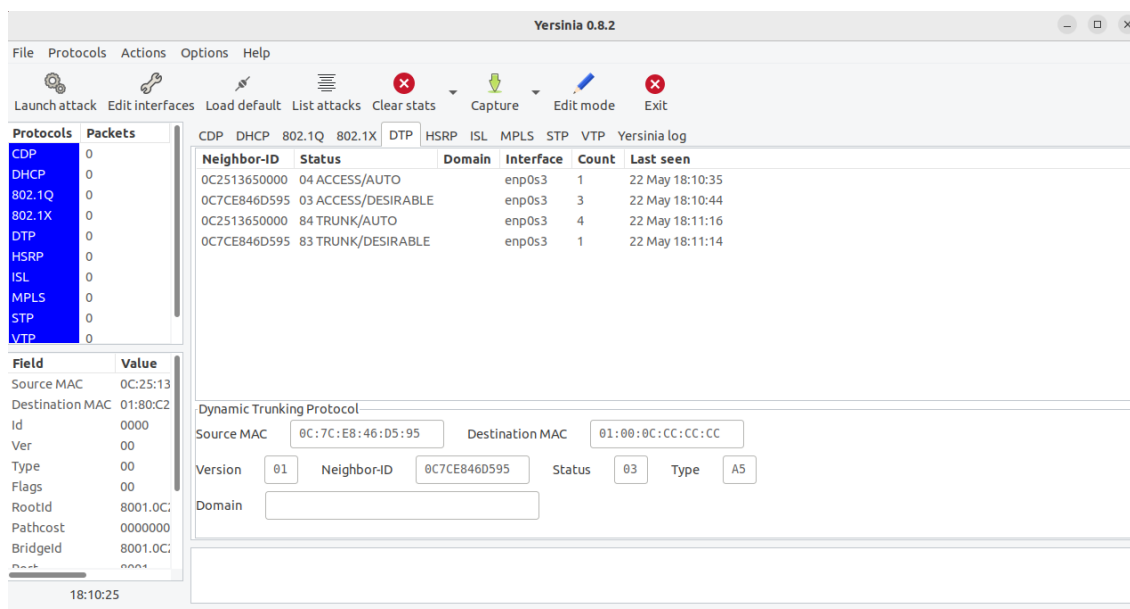
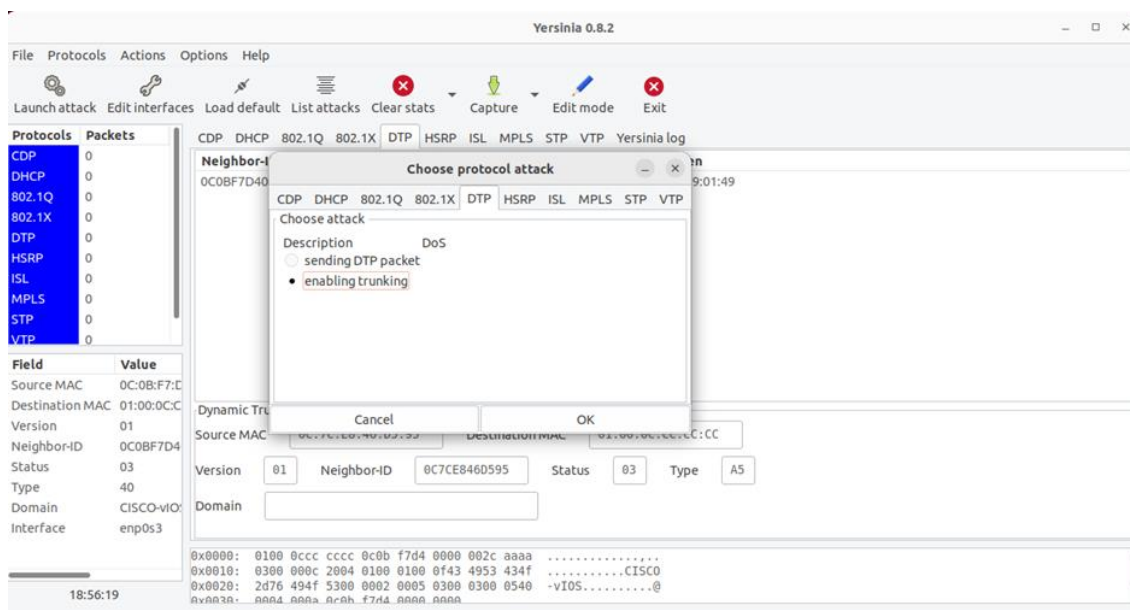
```
homa@homa-VirtualBox: ~
homa@homa-VirtualBox:~$ sudo yersinia -G
[sudo] password for homa:
Gtk-Message: 18:56:18.249: Failed to load module "canberra-gtk-module"

(yersinia:2500): Gtk-WARNING **: 18:56:18.329: gtk_menu_attach_to_widget(): menu already attached to GtkImageMenuItem
(yersinia:2500): Gtk-WARNING **: 18:56:18.330: gtk_menu_attach_to_widget(): menu already attached to GtkImageMenuItem
```

محیط گرافیکی این ابزار به صورت زیر می باشد.



از interface حمله را آغاز کرده و سعی می کنیم interface را به trunk mode ببریم.



پس از حمله interface متصل به مهاجم به trunk mode تغییر می کند.


```

*May 22 14:39:38.094: DTP-event:Gi0/0:Received packet event ../dyntrk/dyntrk_process.c:2219
*May 22 14:39:39.639: DTP-event:Gi0/0:Received packet event ../dyntrk/dyntrk_process.c:2219
*May 22 14:39:40.056: DTP-event:Gi0/0:Received packet event ../dyntrk/dyntrk_process.c:2219
*May 22 14:40:09.660: DTP-event:Gi0/0:Received packet event ../dyntrk/dyntrk_process.c:2219
*May 22 14:40:40.266: DTP-event:Gi0/0:Received packet event ../dyntrk/dyntrk_process.c:2219
Switch#show int status

Port      Name      Status      Vlan      Duplex  Speed  Type
Gi0/0      Name      connected   trunk     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

```

برای جلوگیری از این حمله از مکانیزم Port Security استفاده کرده و ماکسیمم تعداد mac هایی را که یک interface می تواند دریافت کند را در این مثال به دو کاهش می دهیم. سپس سوییچ را طوری کانفیگ می کنیم که آدرس mac سیستم های متصل به آن را به صورت dynamic بشناسد تا از اتصال سیستم های غیرمجاز جلوگیری شود.

```

Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int g0/0
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport host
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled

Switch(config-if)#switchport port-security maximum 2
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#exit

```

پس از اجرای مجدد حمله اگر وضعیت interface ها را چک کنیم مشاهده میکنیم که به trunk mode تغییر حالت نداده است.

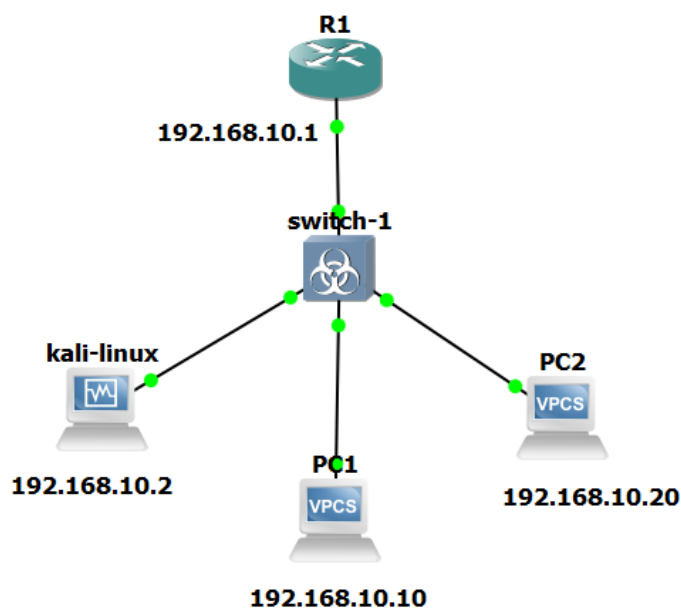
```
Switch#show int status
```

| Port | Name | Status | Vlan | Duplex | Speed | Type |
|-------|------|------------|------|--------|-------|------|
| Gi0/0 | | connected | 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#
```

: ARP Spoofing

توپولوژی در نظر گرفته شده برای این حمله به صورت زیر می باشد.



ابتدا به صورت زیر روتر را کانفیگ می کنیم.

```
R1#conf t
*Mar  1 00:25:43.411: %SYS-5-CONFIG_I: Configured from console by console
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int f0/0
R1(config-if)#ip addr 192.168.10.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#do show ip int brief
Interface                IP-Address      OK? Method Status              Protocol
FastEthernet0/0          192.168.10.1    YES manual up                  up
FastEthernet0/1          unassigned      YES unset  administratively down down
R1(config-if)#exit
```

سپس ip ماشین ها را ست می کنیم

```

PC1> ip 192.168.10.10 255.255.255.0 192.168.10.1
Checking for duplicate address...
PC1 : 192.168.10.10 255.255.255.0 gateway 192.168.10.1

PC1> show ip

NAME       : PC1[1]
IP/MASK    : 192.168.10.10/24
GATEWAY    : 192.168.10.1
DNS        :
MAC        : 00:50:79:66:68:00
LPORT      : 20002
RHOST:PORT : 127.0.0.1:20003
MTU        : 1500

```

```

PC2> ip 192.168.10.20 255.255.255.0 192.168.10.1
Checking for duplicate address...
PC2 : 192.168.10.20 255.255.255.0 gateway 192.168.10.1

PC2> show ip

NAME       : PC2[1]
IP/MASK    : 192.168.10.20/24
GATEWAY    : 192.168.10.1
DNS        :
MAC        : 00:50:79:66:68:01
LPORT      : 20004
RHOST:PORT : 127.0.0.1:20005
MTU        : 1500

```

```

root@kali: ~
File Actions Edit View Help
GNU nano 7.2 /etc/network/interfaces *
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.10.2
netmask 255.255.255.0
gateway 192.168.10.1

```

برای بررسی درستی کانکشن ها پینگ می گیریم.

```

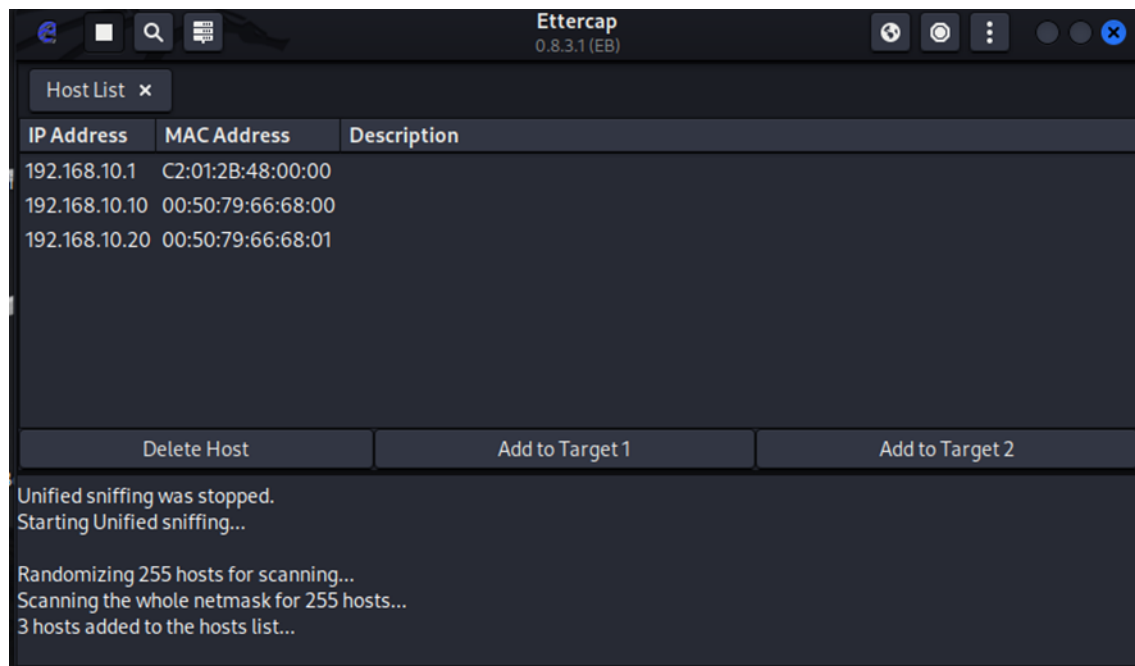
(root@kali)~[~]
# ping 192.168.10.1
PING 192.168.10.1 (192.168.10.1) 56(84) bytes of data:
64 bytes from 192.168.10.1: icmp_seq=2 ttl=255 time=23.7 ms
64 bytes from 192.168.10.1: icmp_seq=3 ttl=255 time=15.9 ms
64 bytes from 192.168.10.1: icmp_seq=4 ttl=255 time=12.9 ms
64 bytes from 192.168.10.1: icmp_seq=5 ttl=255 time=5.04 ms
^C
— 192.168.10.1 ping statistics —
5 packets transmitted, 4 received, 20% packet loss, time 4050ms
rtt min/avg/max/mdev = 5.035/14.397/23.722/6.692 ms

```

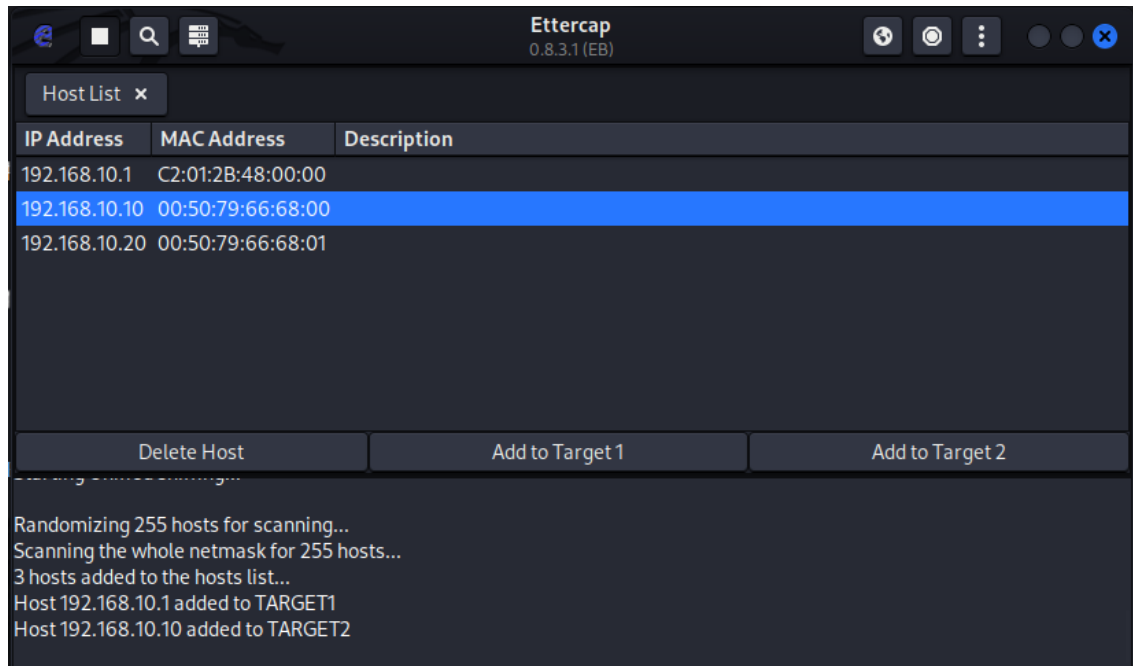
برای انجام این حمله از ابزار Ettercap استفاده می کنیم.



روی آیکن search در بالا سمت چپ کلیک می کنیم تا لیست ip آدرس ها و mac های متناظر در آن شبکه را نمایش دهد.



سیستم هدف (PC1) و روتر را انتخاب می کنیم.



قبل از شروع حمله arp table PC1 را مشاهده می کنیم.

```
PC1> ping 192.168.10.1
84 bytes from 192.168.10.1 icmp_seq=1 ttl=255 time=33.906 ms
84 bytes from 192.168.10.1 icmp_seq=2 ttl=255 time=12.876 ms
84 bytes from 192.168.10.1 icmp_seq=3 ttl=255 time=17.721 ms
84 bytes from 192.168.10.1 icmp_seq=4 ttl=255 time=10.110 ms
84 bytes from 192.168.10.1 icmp_seq=5 ttl=255 time=8.817 ms

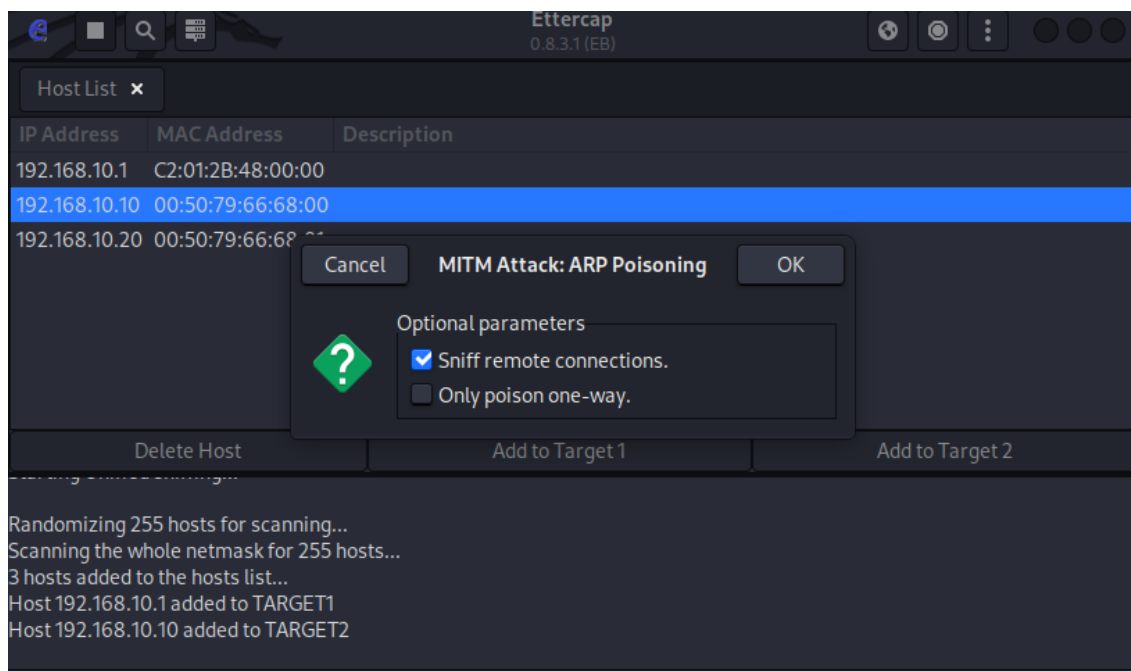
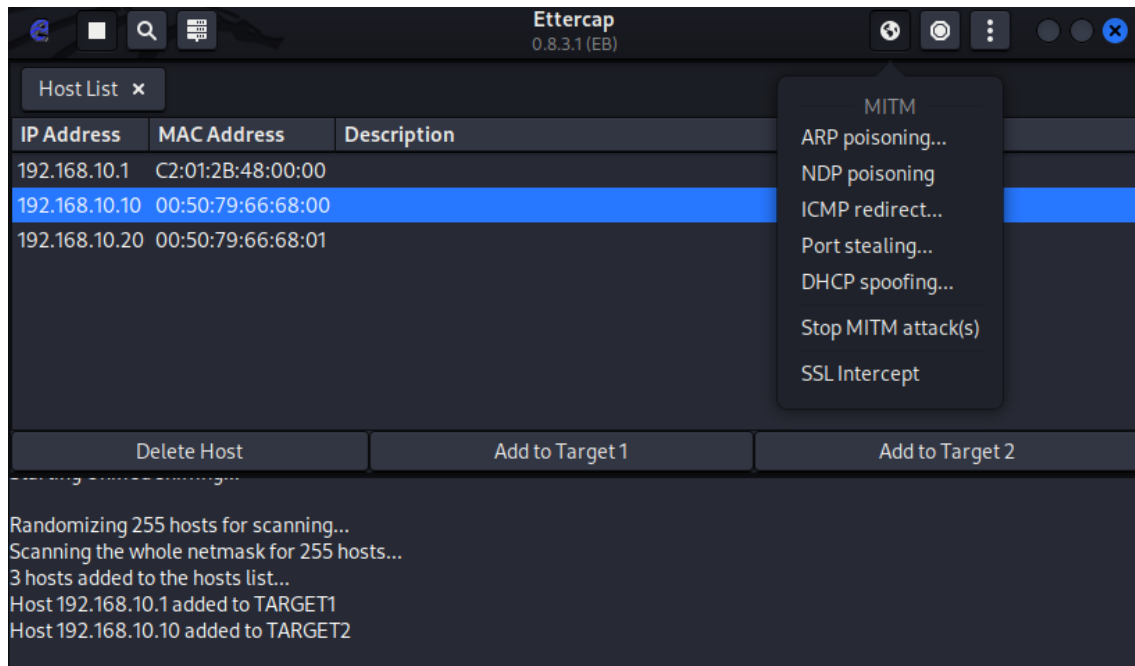
PC1> ping 192.168.10.2
84 bytes from 192.168.10.2 icmp_seq=1 ttl=64 time=11.924 ms
84 bytes from 192.168.10.2 icmp_seq=2 ttl=64 time=18.489 ms
84 bytes from 192.168.10.2 icmp_seq=3 ttl=64 time=13.245 ms
84 bytes from 192.168.10.2 icmp_seq=4 ttl=64 time=17.783 ms
84 bytes from 192.168.10.2 icmp_seq=5 ttl=64 time=15.865 ms

PC1> ping 192.168.10.20
84 bytes from 192.168.10.20 icmp_seq=1 ttl=64 time=15.217 ms
84 bytes from 192.168.10.20 icmp_seq=2 ttl=64 time=10.213 ms
84 bytes from 192.168.10.20 icmp_seq=3 ttl=64 time=7.259 ms
84 bytes from 192.168.10.20 icmp_seq=4 ttl=64 time=9.000 ms
84 bytes from 192.168.10.20 icmp_seq=5 ttl=64 time=5.016 ms

PC1> show arp

c2:01:2b:48:00:00 192.168.10.1 expires in 79 seconds
08:00:27:1e:36:4a 192.168.10.2 expires in 95 seconds
00:50:79:66:68:00 192.168.10.20 expires in 107 seconds
```


حمله arp posining بر روی سیستم قربانی را شروع می کنیم.



پس از حمله مشاهده می شود که آدرس mac مهاجم جایگزین آدرس mac روتر شده است.

```

PC1> show arp

c2:01:2b:48:00:00 192.168.10.1 expires in 79 seconds
08:00:27:1e:36:4a 192.168.10.2 expires in 95 seconds
00:50:79:66:68:00 192.168.10.20 expires in 107 seconds

PC1> ping 192.168.10.1

84 bytes from 192.168.10.1 icmp_seq=1 ttl=255 time=42.106 ms
84 bytes from 192.168.10.1 icmp_seq=2 ttl=255 time=46.708 ms
84 bytes from 192.168.10.1 icmp_seq=3 ttl=255 time=46.397 ms
84 bytes from 192.168.10.1 icmp_seq=4 ttl=255 time=42.520 ms
84 bytes from 192.168.10.1 icmp_seq=5 ttl=255 time=56.732 ms

PC1> show arp

08:00:27:1e:36:4a 192.168.10.2 expires in 118 seconds
08:00:27:1e:36:4a 192.168.10.1 expires in 116 seconds

```

محتویات پکت های ارسالی سیستم قربانی برای مهاجم قابل مشاهده است.

```

PC1> ping 8.8.8.8

*192.168.10.1 icmp_seq=1 ttl=255 time=33.008 ms (ICMP type:3, code:1, Destination host unreachable)
*192.168.10.1 icmp_seq=2 ttl=255 time=20.984 ms (ICMP type:3, code:1, Destination host unreachable)
*192.168.10.1 icmp_seq=3 ttl=255 time=22.724 ms (ICMP type:3, code:1, Destination host unreachable)
*192.168.10.1 icmp_seq=4 ttl=255 time=44.693 ms (ICMP type:3, code:1, Destination host unreachable)
*192.168.10.1 icmp_seq=5 ttl=255 time=22.015 ms (ICMP type:3, code:1, Destination host unreachable)

```

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

| Time | Source | Destination | Protocol | Length | Info |
|------|--------------|------------------------|------------------------|--------|---------------------|
| 40 | 67.341019813 | 0c:c3:99:c3:00:00 | Spanning-tree-(for-... | STP | 60 Conf. Root = 327 |
| 41 | 70.078674440 | PCSSystemtec_1e:36:... | c2:01:2b:48:00:00 | ARP | 42 192.168.10.10 is |
| 42 | 70.078703540 | PCSSystemtec_1e:36:... | 00:50:79:66:68:00 | ARP | 42 192.168.10.1 is |
| 43 | 70.666326177 | 0c:c3:99:c3:00:00 | 0c:c3:99:c3:00:00 | LOOP | 60 Reply |
| 44 | 70.943234488 | 0c:c3:99:c3:00:00 | Spanning-tree-(for-... | STP | 60 Conf. Root = 327 |
| 45 | 74.537885210 | 0c:c3:99:c3:00:00 | Spanning-tree-(for-... | STP | 60 Conf. Root = 327 |
| 46 | 77.207505414 | 192.168.10.10 | 8.8.8.8 | ICMP | 98 Echo (ping) requ |
| 47 | 77.211968945 | 192.168.10.10 | 8.8.8.8 | ICMP | 98 Echo (ping) requ |
| 48 | 77.225366353 | 192.168.10.1 | 192.168.10.10 | ICMP | 70 Destination unre |
| 49 | 77.227956715 | 192.168.10.1 | 192.168.10.10 | ICMP | 70 Destination unre |
| 50 | 78.193697188 | 0c:c3:99:c3:00:00 | Spanning-tree-(for-... | STP | 60 Conf. Root = 327 |

Frame 47: 98 bytes on wire (784 bits), 98 by
 Ethernet II, Src: PCSSystemtec_1e:36:4a (08:
 Internet Protocol Version 4, Src: 192.168.10.1
 Internet Control Message Protocol

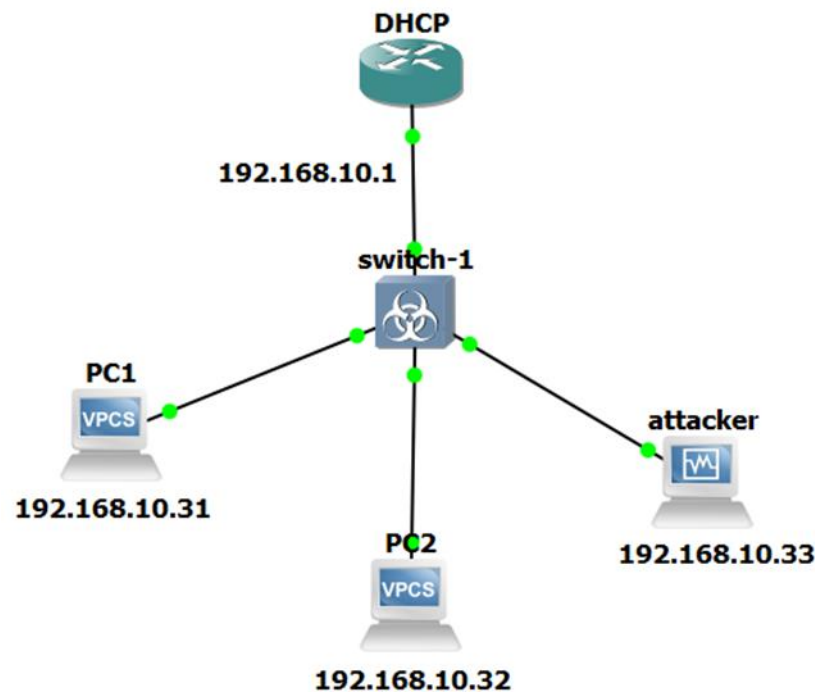
eth0: <live capture in progress> Packets: 81 · Displayed: 81 (100.0%) Profile: Default

برای پیشگیری از این حمله می توانیم جدول استاتیک arp برای سوییچ تعریف کنیم.

```
Switch(config)#arp 192.168.10.1 c2:01:2b:48:00:00 arpa
Switch(config)#arp 192.168.10.2 08:00:27:1e:36:4a arpa
Switch(config)#arp 192.168.10.10 00:50:79:66:68:01 arpa
Switch(config)#arp 192.168.10.20 00:50:79:66:68:00 arpa
```

:DHCP Attack

توپولوژی در نظر گرفته شده برای این حمله به صورت زیر می باشد.



ابتدا DHCP server را کانفیگ می کنیم.

```
DHCP#conf t
Enter configuration commands, one per line. End with CNTL/Z.
DHCP(config)#int fa0/0
DHCP(config-if)#ip add 192.168.10.1 255.255.255.0
DHCP(config-if)#no shut
DHCP(config-if)#exit
*Mar  1 00:06:53.595: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:06:54.595: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
DHCP(config-if)#exit
DHCP(config)#end
```

```
DHCP(config)#ip dhcp pool pool1
DHCP(dhcp-config)#network 192.168.10.0
DHCP(dhcp-config)#default-router 192.168.10.1
DHCP(dhcp-config)#exit
DHCP(config)#
DHCP(config)#
DHCP(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.30
```

و ip ها را از DHCP server دریافت می کنیم.

```
PC1> ip dhcp
DDORA IP 192.168.10.31/24 GW 192.168.1.1
```

```
PC2> ip dhcp
DDORA IP 192.168.10.32/24 GW 192.168.1.1
```

```
homa@homa-VirtualBox:~$ sudo dhclient -v
[sudo] password for homa:
Internet Systems Consortium DHCP Client 4.4.3
Copyright 2004-2022 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/enp0s3/08:00:27:38:3e:03
Sending on   LPF/enp0s3/08:00:27:38:3e:03
Sending on   Socket/fallback
xid: warning: no netdev with useable HWADDR found for seed's uniqueness enforcement
xid: rand init seed (0x6633fc4f) built using gethostid
DHCPDISCOVER on enp0s3 to 255.255.255.255 port 67 interval 3 (xid=0x20cc471f)
DHCPOFFER of 192.168.10.33 from 192.168.10.1
DHCPREQUEST for 192.168.10.33 on enp0s3 to 255.255.255.255 port 67 (xid=0x1f47cc20)
DHCPACK of 192.168.10.33 from 192.168.10.1 (xid=0x20cc471f)
bound to 192.168.10.33 -- renewal in 37019 seconds.
```

از طریق دستور زیر، ip هایی که به سیستم ها توسط این سرور بایند شده اند، قابل مشاهده اند.

```
DHCP#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/
                   Hardware address/
                   User name
192.168.10.31       0100.5079.6668.01    Mar 02 2002 12:46 AM    Automatic
192.168.10.32       0100.5079.6668.00    Mar 02 2002 12:47 AM    Automatic
192.168.10.33       0800.2738.3e03       Mar 02 2002 01:21 AM    Automatic
```

و مشاهده می شود که تعداد کل آدرس ip هایی که سرور می تواند تخصیص بدهد چندتا است و 3 آدرس ip تخصیص داده شده و سایر آدرس ها استفاده نشده اند.

```
DHCP#show ip dhcp pool
```

```
Pool pool1 :
```

```
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
```

```
192.168.10.57 192.168.10.1 - 192.168.10.254 3
```

برای انجام این حمله نیز از ابزار yersinia استفاده می کنیم.



homa@homa-VirtualBox: ~

```
homa@homa-VirtualBox:~$ sudo yersinia -G
```

```
[sudo] password for homa:
```

Yersinia 0.8.2

File Protocols Actions Options Help

Launch attack Edit interfaces Load default List attacks Clear stats Capture Edit mode Exit

| Protocols | Packets |
|-----------|---------|
| CDP | 0 |
| DHCP | 0 |
| 802.1Q | 0 |
| 802.1X | 0 |
| DTP | 0 |
| HSRP | 0 |
| ISL | 0 |
| MPLS | 0 |
| STP | 0 |
| VTP | 0 |

| SIP | DIP | MessageType | Interface | Count | Last seen |
|---------|-----------------|-------------|-----------|-------|-----------------|
| 0.0.0.0 | 255.255.255.255 | 01 DISCOVER | enp0s3 | 1 | 21 May 23:50:41 |
| 0.0.0.0 | 255.255.255.255 | 01 DISCOVER | enp0s3 | 1 | 21 May 23:50:41 |
| 0.0.0.0 | 255.255.255.255 | 01 DISCOVER | enp0s3 | 1 | 21 May 23:50:41 |
| 0.0.0.0 | 255.255.255.255 | 01 DISCOVER | enp0s3 | 1 | 21 May 23:50:41 |
| 0.0.0.0 | 255.255.255.255 | 01 DISCOVER | enp0s3 | 1 | 21 May 23:50:41 |
| 0.0.0.0 | 255.255.255.255 | 01 DISCOVER | enp0s3 | 1 | 21 May 23:50:41 |
| 0.0.0.0 | 255.255.255.255 | 01 DISCOVER | enp0s3 | 1 | 21 May 23:50:41 |
| 0.0.0.0 | 255.255.255.255 | 01 DISCOVER | enp0s3 | 1 | 21 May 23:50:41 |
| 0.0.0.0 | 255.255.255.255 | 01 DISCOVER | enp0s3 | 1 | 21 May 23:50:41 |
| 0.0.0.0 | 255.255.255.255 | 01 DISCOVER | enp0s3 | 1 | 21 May 23:50:41 |

Dynamic Host Configuration Protocol

Source MAC 02:48:33:66:02:51 Destination MAC FF:FF:FF:FF:FF:FF Extra

SIP 0.0.0.0 DIP 255.255.255.255 SPort 68 DPort 67

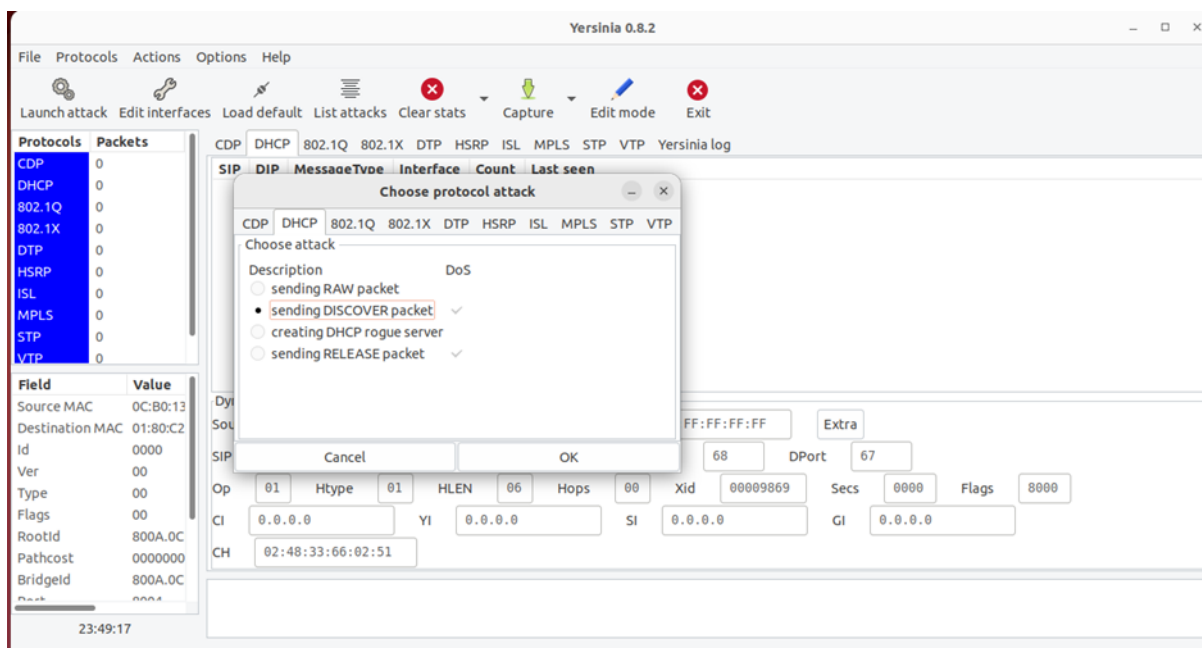
Op 01 Htype 01 HLEN 06 Hops 00 Xid 00009869 Secs 0000 Flags 8000

CI 0.0.0.0 YI 0.0.0.0 SI 0.0.0.0 GI 0.0.0.0

CH 02:48:33:66:02:51

23:49:17

برای انجام حمله DHCP Starvation از launch attack > DHCP > sending DISCOVER PACKET
حمله را شروع می کنیم و پکت های DISCOVER فراوان برای DHCP سرور ارسال می کنیم.



در این صورت اگر یک سیستم مجاز درخواست ip جدید از این سرور داشته باشد، سرور پاسخگو نخواهد بود.

```
PC1> ip dhcp  
DDD  
Can't find dhcp server
```

و mac table نیز به صورت زیر خواهد بود

DHCP

PC1

PC2

switch

Switch>show mac address-table

Mac Address Table

| Vlan | Mac Address | Type | Ports |
|------|----------------|---------|-------|
| 1 | 0004.b32e.9eaf | DYNAMIC | Gi0/2 |
| 1 | 000a.0611.fe75 | DYNAMIC | Gi0/2 |
| 1 | 001f.d226.e77c | DYNAMIC | Gi0/2 |
| 1 | 0026.2a1c.74a3 | DYNAMIC | Gi0/2 |
| 1 | 003f.204c.4b13 | DYNAMIC | Gi0/2 |
| 1 | 0050.7966.6800 | DYNAMIC | Gi0/0 |
| 1 | 0052.9311.a2d0 | DYNAMIC | Gi0/2 |
| 1 | 0057.ff21.dbf6 | DYNAMIC | Gi0/2 |
| 1 | 005e.f837.65c2 | DYNAMIC | Gi0/2 |
| 1 | 0060.c15f.1490 | DYNAMIC | Gi0/2 |
| 1 | 0061.b60b.e89d | DYNAMIC | Gi0/2 |
| 1 | 0062.a872.d9c8 | DYNAMIC | Gi0/2 |
| 1 | 006a.4276.3243 | DYNAMIC | Gi0/2 |
| 1 | 0073.0233.6a20 | DYNAMIC | Gi0/2 |
| 1 | 0076.a557.1910 | DYNAMIC | Gi0/2 |
| 1 | 007e.5e03.bdf3 | DYNAMIC | Gi0/2 |
| 1 | 0081.364d.327c | DYNAMIC | Gi0/2 |
| 1 | 0082.8159.a24c | DYNAMIC | Gi0/2 |
| 1 | 008a.270a.179c | DYNAMIC | Gi0/2 |
| 1 | 0094.d905.29ba | DYNAMIC | Gi0/2 |
| 1 | 0096.7c1b.b66d | DYNAMIC | Gi0/2 |
| 1 | 009b.c60f.d199 | DYNAMIC | Gi0/2 |
| 1 | 00a9.597c.5db7 | DYNAMIC | Gi0/2 |
| 1 | 00ab.5d77.b850 | DYNAMIC | Gi0/2 |
| 1 | 00b9.636c.43a9 | DYNAMIC | Gi0/2 |
| 1 | 00b9.7a59.978a | DYNAMIC | Gi0/2 |
| 1 | 00c1.b01e.df80 | DYNAMIC | Gi0/2 |
| 1 | 00c8.cb28.23dc | DYNAMIC | Gi0/2 |
| 1 | 00cc.3029.ffe4 | DYNAMIC | Gi0/2 |

--More--

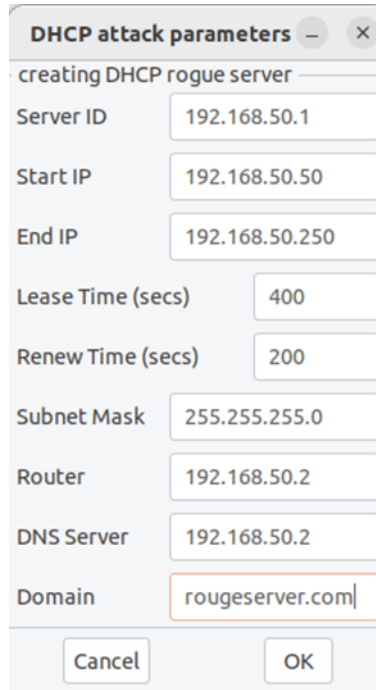
solarwinds

Solar-PuTTY free tool

© 2019-2023 SolarWinds Worldwide, LLC. All rights reserved.

همچنین برای انجام حمله DHCP Spoofing مطابق تصویر زیر عمل می کنیم.

و یک DHCP سرور جعلی می سازیم.



DHCP attack parameters

creating DHCP rogue server

Server ID: 192.168.50.1

Start IP: 192.168.50.50

End IP: 192.168.50.250

Lease Time (secs): 400

Renew Time (secs): 200

Subnet Mask: 255.255.255.0

Router: 192.168.50.2

DNS Server: 192.168.50.2

Domain: rougeserver.com

Cancel OK

و اگر کاربری درخواست ip به این سرور جعلی دهد ip فیک به او داده می شود و مهاجم قادر به مشاهده داده ها خواهد بود.

برای مقابله با این حمله نیز می توان از مکانیزم Port Security استفاده کرده و ماکسیمم تعداد mac هایی را که یک interface می تواند دریافت کند را در این مثال به دو کاهش می دهیم. سپس سوییچ را طوری کانفیگ می کنیم که آدرس mac سیستم های متصل به آن را به صورت dynamic بشناسد تا از اتصال سیستم های غیرمجاز جلوگیری شود.

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int g0/0
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport host
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled

Switch(config-if)#switchport port-security maximum 2
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#exit
```