بسمه تعالی

آزمایشگاه شبکه

دانشکده برق و کامپیوتر

دانشگاه صنعتی اصفهان

بهار ۱۴۰۲

دکتر حیدرپور، دکتر فانیان

پیش گزارش آشنایی و محافظت در برابر حملات جعل در سوئیچ

فهرست:

حمله‌ی جعل DHCP (DHCP Spoofing)

در جلسات قبل با سرور DHCP و نقش آن در شبکه آشنا شدید. همانطور که می‌دانید، سرور DHCP در پاسخ به یک درخواست DHCP از سمت یک کاربر، طی چندین پیام در نهایت آدرس IP اختصاص داده شده به کاربر، آدرس IP درگاه پیش‌فرض (Default Gateway) و آدرس سرور DNS را برای کاربر ارسال می‌کند. همچنین گفته شد که اگر چندین پاسخ DHCP به سمت کاربر ارسال شود، کاربر اولین پاسخ را قبول کرده و از باقی پاسخ‌ها صرف نظر خواهد کرد. در این حالت، اگر مهاجمی بتواند سریع‌تر از سرور DHCP، پاسخ جعلی خود را به دست کاربر برساند، امنیت کاربر به خطر خواهد افتاد. یکی از اقداماتی که مهاجم برای رسیدن به این هدف می‌تواند انجام دهد، ارسال تعداد زیادی درخواست DHCP به سمت سرور DHCP است به صورتی که سرور نتواند به درخواست‌های ارسال شده در زمان مطلوب پاسخ دهد. در این حالت، با مشغول نگه داشتن سرور DHCP، مهاجم قادر خواهد بود که پاسخ جعلی خود را به قربانی برساند.

مهاجم با جعل پاسخ DHCP می‌تواند آدرس درگاه پیش‌فرضی که برای قربانی ارسال می‌کند را برابر با آدرس IP خودش قرار دهد. در این صورت تمام بسته‌های ارسالی از سمت قربانی که به مقصد خارج از شبکه ارسال می‌شوند ابتدا به ماشین مهاجم می‌رسد.

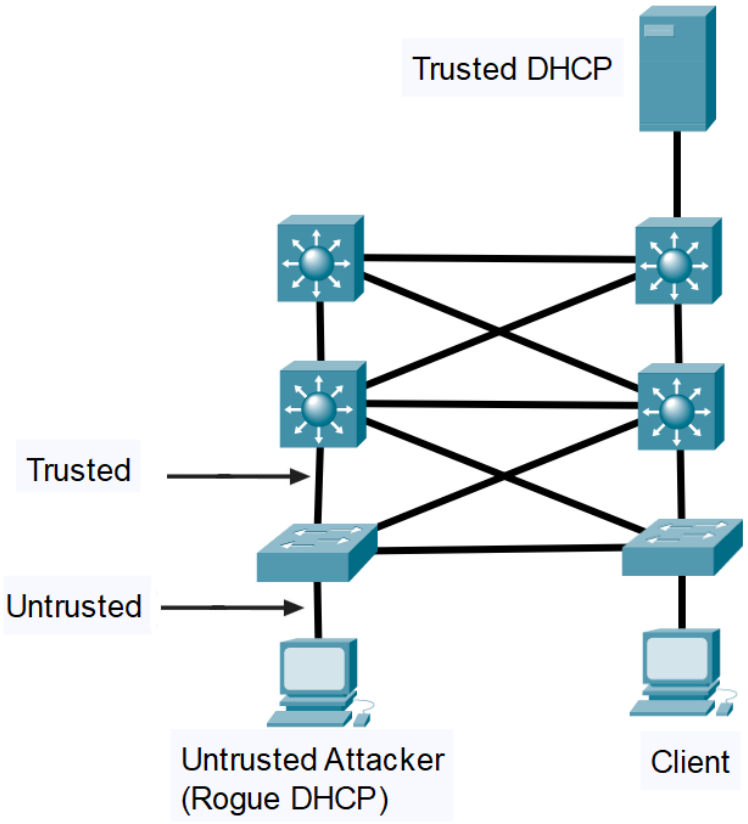
در حالتی دیگر، مهاجم می‌تواند آدرس سرور DNS ارسالی برای قربانی را برابر با آدرس یک سرور DNS تحت کنترل خود قرار دهد. در این حالت، پرسمان‌های DNS قربانی به سمت سرور DNS تحت کنترل مهاجم ارسال می‌شود که مهاجم می‌تواند در پاسخ به پرسمان ارسال شده، هر آدرس IP دلخواهی را به عنوان پاسخ ارسال کند. در این صورت، مهاجم می‌تواند قربانی را به سمت دامنه‌ای جعلی با ظاهری شبیه به دامنه مورد نظر قربانی هدایت کند.

دفاع در برابر حمله‌ی جعل DHCP (DHCP Snooping)

در این قسمت راهکارهای مقابله با حمله جعل DHCP که در قسمت قبل مطرح شد معرفی می‌شود.

برای مقابله با حمله جعل DHCP، دو راهکار معرفی می‌شود. یکی از راهکارها تقسیم پورت‌های سوئیچ به دو دسته‌ی قابل اعتماد (Trusted) و غیر قابل اعتماد (Untrusted) می‌باشد. به عبارت دقیق‌تر، پورت‌های دسترسی (Access) را به عنوان پورت‌های غیر قابل اعتماد تعریف می‌کنیم تا سوئیچ پیام‌هایی که از نوع پیام‌های پاسخ DHCP هستند را (همانند DHCP ACK، DHCP Offer و ...) از

روی این پورت‌ها عبور ندهد و از پیغام‌های DHCP فقط دو پیام DHCP Discovery و DHCP Recovery را مجاز در نظر بگیرد. با اعمال این راهکار، کاربرانی که از طریق این پورت‌ها به شبکه متصل می‌شوند، نمی‌توانند پاسخ‌های جعلی DHCP را به داخل شبکه ارسال کنند.



برای دفاع در برابر حمله‌ی منع خدمت علیه سرور DHCP، مدیر شبکه می‌تواند نرخ ارسال درخواست‌های DHCP روی پورت‌های دسترسی را محدود کند به صورتی که اگر تعداد درخواست‌های ارسالی از روی این پورت از نرخ مشخص شده فراتر رود، پورت مربوطه خاموش می‌شود.

در ادامه، دستورات مربوط به فعال‌سازی این دو راهکار دفاعی در سوئیچ‌ها معرفی می‌شود. به طور کلی، برای تعریف پورت‌های قابل اعتماد و غیر قابل اعتماد، ابتدا باید DHCP Snooping را به صورت سراسری یا روی یک شبکه‌ي محلی مجازی خاص فعال کنیم و سپس پورت‌های قابل اعتماد را مشخص کنیم. توجه داشته باشید که در حالت پیشفرض، پس از فعال‌سازی DHCP Snooping، همه‌ی پورت‌ها غیر قابل اعتماد هستند.

فعال‌سازی DHCP Snooping به صورت سراسری

```
Switch(config)# ip dhcp snooping
```

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ip dhcp snooping
Switch(config)#
```

فعال‌سازی DHCP Snooping روی شبکه‌های محلی مجازی خاص

```
Switch(config)# ip dhcp snooping vlan [vlan list]
```

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ip dhcp snooping vlan 123
Switch(config)#
```

در پیام‌های DHCP، می‌توان فیلدی به نام option-82 اضافه کرد که سرور DHCP به کمک آن می‌تواند اختصاص IP به کاربران را به صورت دقیق‌تر انجام دهد. فیلد option-82 یک فیلد شامل یک سری اطلاعات در مورد درخواست دهنده است که برای شناسایی مکان فیزیکی درخواست دهنده استفاده می‌شود. این فیلد حاوی اطلاعاتی مانند پورت سوئیچ یا VLAN محل اتصال کلاینت، آدرس MAC کلاینت و سایر جزئیات مرتبط است.

در حالت پیش‌فرض با فعال شدن DHCP Snooping، فیلد option-82 در پیام‌های DHCP فعال خواهد شد. با دستور زیر می‌توان این فیلد را فعال کرد.

```
Switch(config)# ip dhcp snooping information option
```

در حالت پیش‌فرض، برای قسمت‌های غیر قابل اعتماد شبکه (Untrusted)، فیلد option-82 غیر مجاز خواهد بود. به کمک دستور زیر می‌توان برای قسمت‌های غیر قابل اعتماد نیز فیلد option-82 را مجاز ساخت.

```
Switch(config)# ip dhcp snooping information option allow-untrusted
```

تعریف یک پورت به عنوان پورت قابل اعتماد

```
Switch(config-if)# ip dhcp snooping trust
```

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int fa0/1
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#
```

دقت کنید که روی هر دو سوئیچ و در هر دو طرف لینک باید این دستور اجرا شود تا اتصال به حالت قابل اعتماد تبدیل شود.

تنظیم تعداد بسته‌های DHCP مجاز به ارسال از روی پورت در ثانیه:

```
Switch(config-if)# ip dhcp snooping limit rate [number]
```

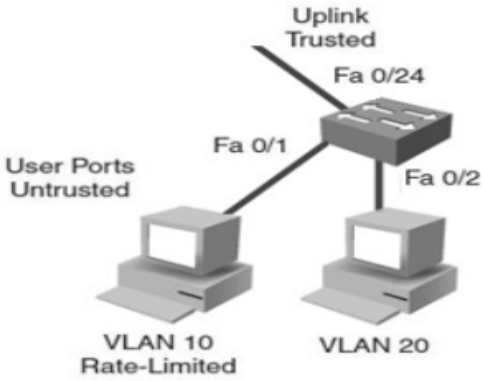
```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int fa0/1
Switch(config-if)#ip dhcp snooping limit rate 100
Switch(config-if)#
```

در حالت پیش‌فرض هیچ محدودیتی روی این نرخ وجود ندارد.

مشاهده تنظیمات DHCP Snooping

```
Switch# show ip dhcp snooping
```

برای مثال در شبکه‌ی شکل زیر دو VLAN 10 و VLAN 20 را داریم که برای هر دو DHCP Snooping فعال شده و خروجی دستور show ip dhcp snooping برای آن نمایش داده شده است.

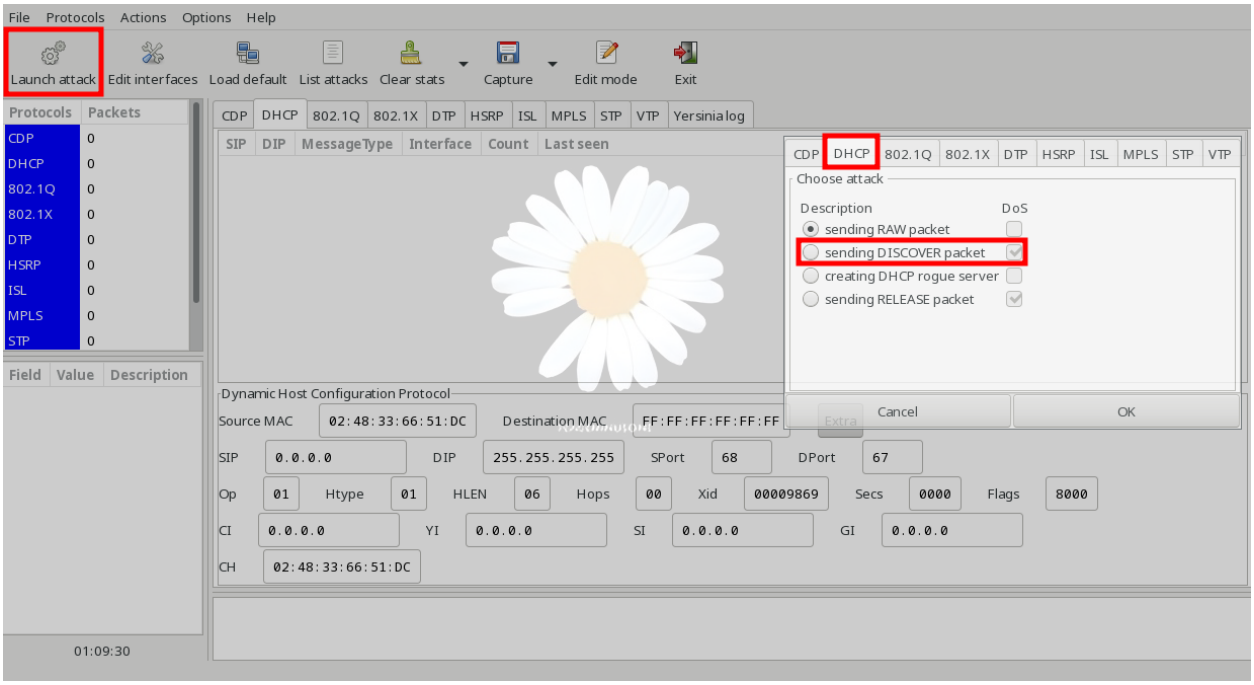



```
switch# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10,20
DHCP snooping is operational on following VLANs:
10,20
DHCP snooping is configured on the following L3 Interfaces:
Insertion of option 82 is enabled
circuit-id default format: vlan-mod-port
remote-id: 001a.e372.ab00 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                  Trusted    Allow option      Rate limit (pps)
  FastEthernet0/1          no         no                5
  FastEthernet0/24         yes        yes               unlimited
```

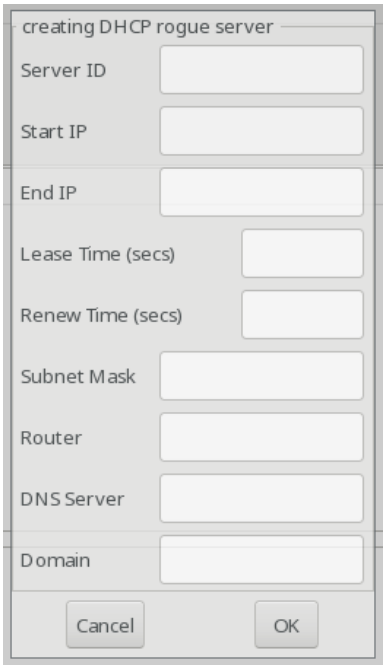
حمله DHCP spoofing با ابزار Yersinia

ابزار Yersinia برای جعل DHCP استفاده می‌شود؛ ناگفته نماند ابزار Ettercap، DHCPig Responder و ... هم هستند که می‌توانید مستندات آنها را مطالعه و با هر یک و ویژگی‌های متناسب آنها آشنا شوید. از Yersinia می‌توان برای انجام حملات مختلف بر روی این پروتکل ها مانند STP manipulation, VLAN hopping, DTP and CDP hijacking, MAC flooding, and ARP spoofing استفاده کرد.



هنگامی که برنامه‌ی Yersinia را توسط دستور Yersinia -G اجرا نمایید با تصویر بالا مواجه خواهید شد. پس از زدن بر روی دکمه‌ی Launch attack صفحه‌ای که در سمت راست تصویر بالا قرار دارد مواجه خواهید شد. می‌توانید برای پروتکل‌های مختلف انواع متفاوتی از حملات را انتخاب نموده و سپس بر روی دکمه‌ی ok کلیک فرمایید. در اینجا ما از منوی بالا DHCP را انتخاب و سپس نوع Sending DISCOVER packets را انتخاب می‌نماییم. در این حالت تعداد بسیار زیادی بسته‌ی DHCP DISCOVER ارسال خواهد شد که موجب می‌شود DHCP server از کار بیفتد.

همچنین می‌توانید با استفاده از گزینه‌ی DHCP rough server یک سرور جعلی DHCP راه بیندازید که این امر زمانی مورد استفاده قرار میگیرد که شما طی یک حمله ابتدا DHCP server اصلی را از کار بیندازید و سپس سرور جعلی خود را بجای سرور اصلی جا بزنید.

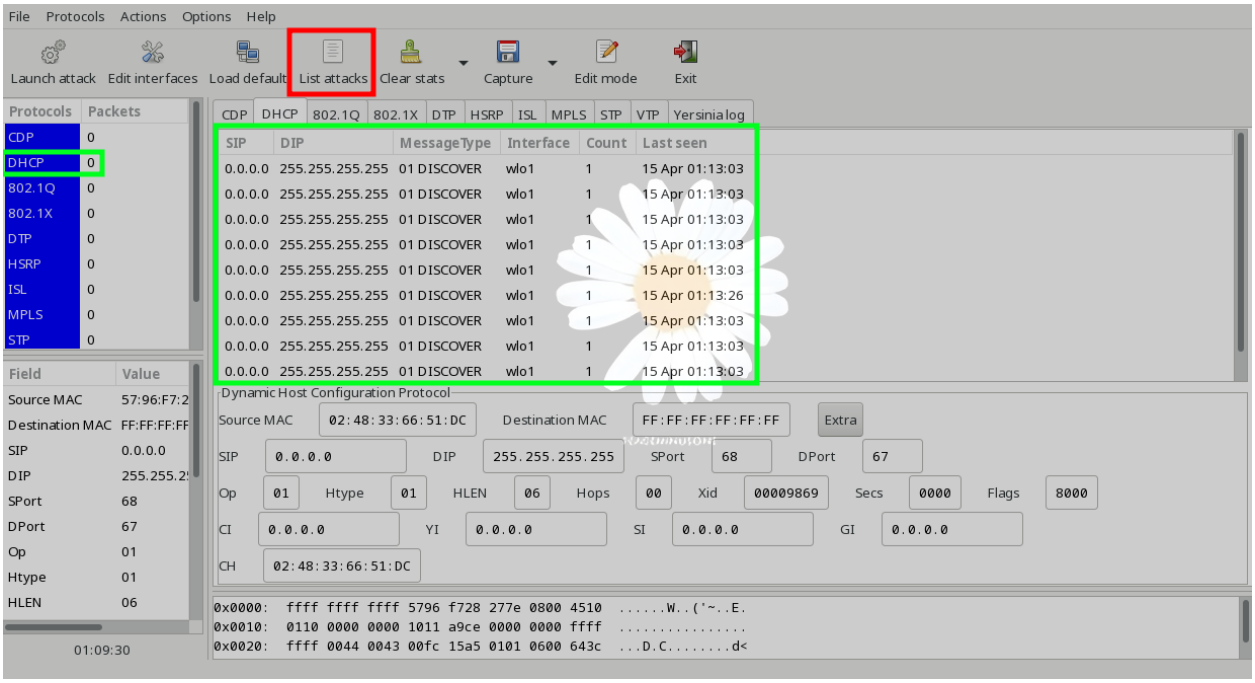


پس از انتخاب گزینه‌ی نام برده با صفحه‌ی روبرو مواجه خواهید شد که با توجه به نیاز خود باید فیلدهای مرتب را پر کنید.

برای server ID باید IP ماشین خود (ماشین مهاجم) را وارد نمایید، در فیلدهای Start IP و End IP رنج آیپی‌هایی که DHCP جعلی قرار است به دیگر ماشین‌ها منتسب نماید را مشخص می‌نمایید. Lease Time برای مشخص نمودن زمان تخصیص IP داده شده مورد استفاده قرار می‌گیرد؛ همچنین Renew Time مشخص می‌کند بعد از چه مدتی مجددا درخواست اختصاص IP داده شود که با این کار Lease Time آپدیت خواهد شد.

دیگر موارد را نیز می‌توانید با توجه به نیاز خود و تنظیمات شبکه‌ی خود تنظیم نمایید.

برای متوقف کردن حمله نیز مطابق با تصویر زیر کافی است بر روی List attacks کلیک فرموده و سپس حمله را متوقف سازید. لیست تمامی بسته‌های ارسالی نیز در پنجره‌ای که با رنگ سبز مشخص شده است نشان داده خواهد شد.

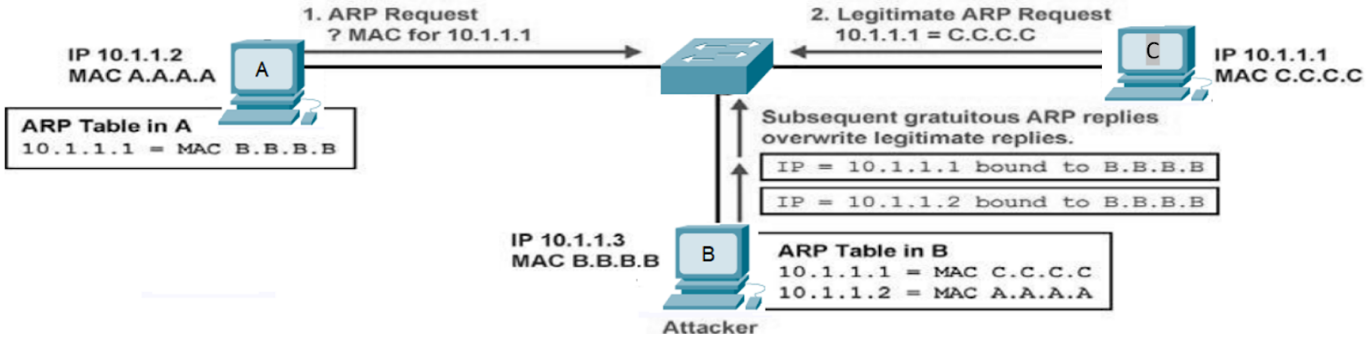


تذکر: معرفی این ابزار صرفا جنبه‌ی آموزشی دارد و اکیدا توصیه می‌شود در شبکه‌های واقعی به‌طور نا آگاهانه از آن استفاده نکنید :). زیاد عواقب خوبی نداره مثلا ادمین شبکه از حضورتون مطلع میشه...

حمله ARP Spoofing

همانطور که در جلسات قبل گفته شد، جدول ARP یا همان (ARP Table) شامل اطلاعات آدرس فیزیکی (MAC) دستگاه‌های متصل به شبکه است. این جدول توسط پروتکل ARP برای ترجمه آدرس‌های IP به آدرس‌های MAC استفاده می‌شود. هنگامی که دستگاهی در شبکه محلی بخواهد با یک دستگاه دیگر در شبکه‌ی محلی خودش ارتباط برقرار کند، از جدول ARP استفاده می‌کند تا آدرس MAC دستگاه مورد نظر را پیدا کند و بتواند اطلاعات را برای آن ارسال کند.

فرض کنید دو میزبان A و C در یک شبکه محلی داریم. در صورتی که A بخواهد پیامی برای C بفرستد، این ارتباط در لایه ۲ و به کمک آدرس فیزیکی انجام می‌شود. میزبان A آدرس IP میزبان C را در اختیار دارد ولی برای این ارتباط نیاز به آدرس مک میزبان C دارد. در این حالت، اگر در جدول ARP موجود در میزبان A، آدرس فیزیکی میزبان C وجود نداشته باشد، میزبان A یک درخواست ARP (یا همان ARP Request) با آدرس IP میزبان C را روی کل شبکه‌ی محلی ارسال می‌کند تا میزبانی که این آدرس IP را دارد، آدرس فیزیکی خود را برای A ارسال کند. این سناریو در شکل زیر نمایش داده شده است.



در حمله‌ی ARP Spoofing یا ARP Poisoning مهاجم خودش را به عنوان یک دستگاه دیگر در شبکه جا می‌زند. به طور دقیق‌تر، مهاجم در پاسخ به درخواست‌های ARP ارسال شده برای یک آدرس IP خاص در شبکه (که این IP متفاوت با IP مهاجم است)، آدرس فیزیکی خودش را به عنوان پاسخ برای درخواست کننده ارسال می‌کند. این حمله باعث می‌شود که ترافیک شبکه به سمت مهاجم هدایت شود و او قادر خواهد بود تا اطلاعاتی که قرار بود برای میزبان دیگری ارسال شود را بطور غیر مجاز دریافت کند.

دفاع در برابر ARP Spoofing (Dynamic ARP Inspection)

برای مقابله با حملات ARP Spoofing، از Dynamic ARP Inspection یا DAI استفاده می‌شود. DAI همانند ویژگی DHCP Snooping پورت‌های سوئیچ را به دو دسته‌ی پورت‌های قابل اعتماد و غیر قابل اعتماد تقسیم می‌کند. همچنین امکان محدود کردن نرخ ارسال بسته‌های ARP را نیز فراهم می‌کند.

DAI بسته‌های ARP ارسالی از پورت‌های قابل اعتماد را بدون بررسی کردن عبور می‌دهد و به سمت مقصد هدایت می‌کند، ولی برای پاسخ‌های ARP ارسال شده از پورت‌های غیر قابل اعتماد، اعتبار آدرس IP و آدرس فیزیکی ارسالی را بررسی می‌کند. به این منظور، DAI باید تناظر آدرس IP و آدرس فیزیکی را برای دستگاه‌های موجود در شبکه داشته باشد. این اطلاعات با فعال‌سازی DHCP Snooping در سوئیچ در یک جدول ذخیره می‌شود و DAI با استفاده از اطلاعات موجود در این جدول می‌تواند معتبر بودن جفت آدرس IP و آدرس فیزیکی موجود در بسته‌ی مربوط به پاسخ ARP ارسال شده از یک پورت غیر قابل اعتماد را بررسی کند.

فعال‌سازی DAI روی شبکه‌های محلی مجازی خاص

```
Switch(config)# ip arp inspection vlan [vlan_list]
```

با فعال‌سازی DAI، در حالت پیشفرض، همه‌ی پورت‌ها غیر قابل اعتماد هستند و محدودیت نرخ بسته‌های ARP ارسالی نیز برابر با ۱۵ بسته در ثانیه است.

تعریف پورت به عنوان پورت قابل اعتماد

```
Switch(config-if)# ip arp inspection trust
```

مشخص کردن نرخ مجاز عبور بسته‌های ARP

```
Switch(config-if)# ip arp inspection limit {rate pps [burst interval seconds] | none}
```

در این دستور، منظور از pps بسته بر ثانیه است و burst interval نیز حداکثر بازه‌ی زمانی که طی آن بسته‌ها را می توان با نرخی فراتر از حد نرخ تعیین شده ارسال کرد مشخص می‌کند. این بازه در حالت پیش‌فرض برابر ۱ ثانیه می‌باشد.

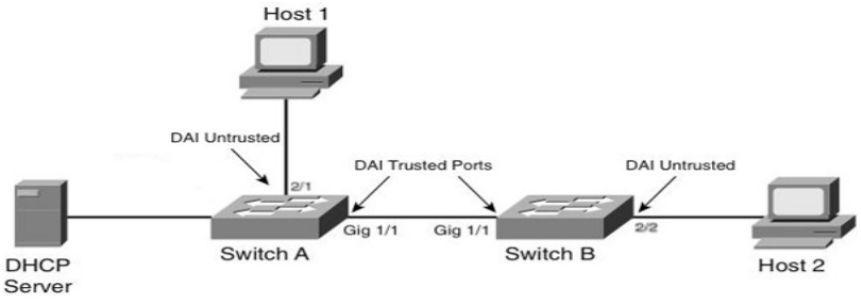
همانطور که گفته شد، DAI برای بسته‌های ARP ارسالی تناظر IP و آدرس MAC را بررسی می‌کند. با این حال به کمک دستور زیر می‌توانید سوئیچ را برای انجام بررسی‌های اضافه پیکربندی کنید.

```
Switch(config)# ip arp inspection validate {[src- mac] [dst-mac] [ip_address]}
```

- src-mac منجر می‌شود برای همه‌ی بسته‌های ARP آدرس MAC مبدا در سرآیند فریم با آدرس مک فرستنده در بدنه ARP بررسی شود.
- dst-mac برای همه‌ی بسته‌های ARP آدرس MAC مقصد در سرآیند فریم با آدرس مک گیرنده در بدنه ARP بررسی شود.
- IP، بدنه‌ی ARP را برای آدرس‌های IP نامعتبر و غیر منتظره بررسی می‌کند. آدرس IP فرستنده در همه‌ی بسته‌های ARP بررسی می‌شوند و آدرس‌های IP گیرنده فقط برای پاسخ‌های ARP بررسی می‌شوند.

مشاهده تنظیمات DAI به صورت سراسری

```
Switch# show ip arp inspection interfaces
```




```
SwitchA# show ip arp inspection interfaces
 Interface              Trust State       Rate (pps)     Burst Interval
 ---------------------  ----------------  -------------  --------------
 Gi1/1                  Trusted           None           N/A
 Gi1/2                  Untrusted         15             1
 Fa2/1                  Untrusted         15             1
 Fa2/2                  Untrusted         15             1
```

مشاهده تنظیمات DAI برای یک شبکه‌ی محلی مجازی خاص

```
Switch# show ip arp inspection vlan [vlan-id]
```

مشاهده جدول تناظر آدرس فیزیکی به آدرس IP

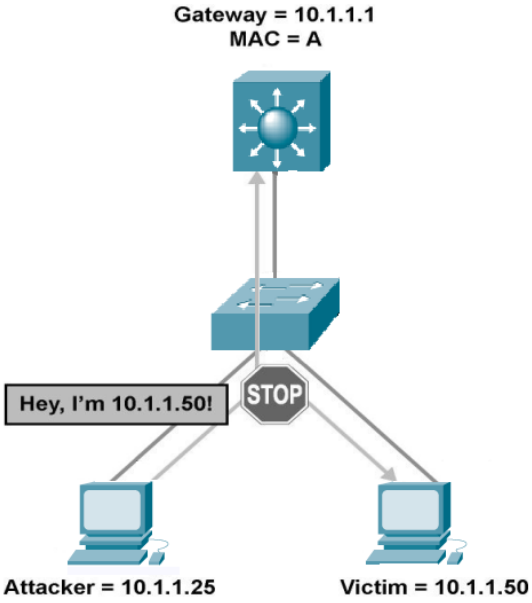
```
Switch# show ip dhcp snooping binding
```

```
SwitchA# show ip dhcp snooping binding

 MacAddress          IpAddress       Lease(sec)  Type            VLAN  Interface
 ------------------  --------------  ----------  --------------  ----  --------------------
 00:01:00:01:00:01   10.10.10.1      4995        dhcp-snooping   10    FastEthernet2/1
```

حمله جعل IP (IP Spoofing)

حمله‌ی جعل IP، حمله‌ای است که توسط مهاجمان برای ارسال بسته‌هایی با آدرس IP مبدا نادرست و جعلی به منظور مخفی کردن هویت مهاجمان و جعل هویت دستگاه دیگری در شبکه استفاده می‌شود. با جعل آدرس IP، مهاجم می‌تواند به صورتی جلوه دهد که گویی حمله از یک منبع قابل اعتماد انجام می‌شود و شناسایی و مسدود کردن حمله را برای مدیران شبکه دشوارتر می کند.



دفاع در برابر حمله‌ی جعل IP

برای مقابله با حملات جعل IP از IP Source Guard (یا IPSG) استفاده می‌شود. IPSG نیز اتصالات را به دو دسته‌ی قابل اعتماد و غیر قابل اعتماد تقسیم کرده و برای بسته‌هایی که از قسمت غیر قابل اعتماد دریافت می‌کند، اعتبار و مطابقت آدرس IP مبدا را با آدرس IP موجود در جدول تناظر آدرس‌های IP و MAC بررسی می‌کند. با فعال‌سازی IPSG، دستگاه‌های موجود در قسمت غیر قابل اعتماد، قادر نخواهند بود که با آدرس IP جعلی ترافیک روی شبکه ارسال کنند.

دستور فعال‌سازی IPSG

برای فعال‌سازی IPSG روی سوئیچ‌های لایه دو از دستور زیر استفاده می‌شود.

```
Switch(config-if)# ip verify source [port-security]
```

برای فعال‌سازی IPSG روی سوئیچ‌های لایه سه از دستور زیر استفاده می‌شود.

```
Switch(config-if)# ip verify source vlan dhcp-snooping [port-security]
```

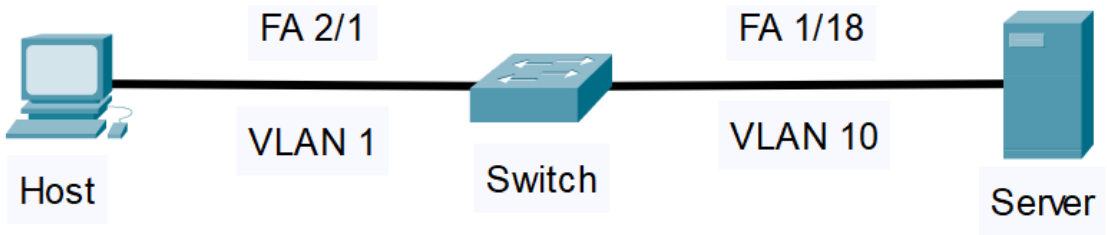
توجه فرمایید برای فعال‌سازی IPSG باید حتما DHCP Snooping و port-security فعال باشد.

دستور تعریف یک تناظر آدرس IP و آدرس مک به صورت دستی

```
Switch(config)# ip source binding mac-address vlan vlan-id
ip-address interface interface-id
```

دستور نمایش پیکربندی IPSG:

```
Switch# show ip verify source
```




```
Switch# show ip source binding
MacAddress          IpAddress       Lease(sec)  Type           VLAN  Interface
------------------  --------------  ----------  -------------  ----  ------------------
00:02:B3:3F:3B:99   10.1.1.11       6522        dhcp-snooping  1     FastEthernet2/1
00:00:00:0A:00:0B   10.1.10.1       infinite    static         10    FastEthernet2/18
Switch# show ip verify source
Interface  Filter-type  Filter-mode  IP-address     Mac-address        Vlan
---------  -----------  -----------  -------------  -----------------  ----
Fa2/1      ip-mac       active       10.1.1.11      00:02:B3:3F:3B:99  1
Fa2/18     ip-mac       active       10.1.10.11     00:00:00:0a:00:0b  10
```

ابزار hping3

با استفاده از hping3، کاربران می‌توانند بسته‌هایی با مقادیر مشخص برای فیلدهای مختلف، از جمله آدرس‌های IP مبدا و مقصد، انواع پروتکل، پرچم‌ها و بارهای ارسالی ایجاد کنند. علاوه بر این، hping3 از ویژگی‌های پیشرفته‌ای مانند فرگمنتیشن، TCP/IP options و raw mode پشتیبانی می‌کند که آن را به ابزاری قدرتمند برای عیب‌یابی شبکه و ابزاری امنیتی تبدیل می‌کند.

علاوه بر hping3 ابزارهایی نظیر spacy نیز وجود دارند که قابلیت‌های بیشتری نیز به شما خواهد داد و می‌توانید تمامی بیت‌های بسته‌های شبکه را متناظر با نیاز خود مقدار دهی فرمایید و بسته را ارسال کنید.

برای استفاده از دستور hping3 می‌توانید بر روی خط فرمان خود hping3 –help وارد نمایید. برای مثال به منظور IP spoofing می‌توان از دستور زیر استفاده نمود.

```
$ sudo hping3 -S -a 10.0.0.2 -c 1 -p 80 192.168.1.10
```

در دستور بالا از آپشن c- برای مشخص نمودن تعداد بسته‌های ارسالی استفاده کرده‌ایم که در این مثال ۱ در نظر گرفته شده است یعنی یک بسته‌ی ICMP فرستاده خواهد شد. همچنین با آپشن S- مشخص نموده‌ایم که می‌خواهیم یک بسته‌ی SYN ارسال کنیم (با A- برای ACK می‌توان مشخص کرد، F- برای بسته‌ی FIN و همینطور R- برای بسته‌ی RST. برای آشنایی با دیگر قابلیت‌ها نیز می‌توانید راهنمای این دستور را مطالعه فرمایید). با آپشن a- هم مشخص نموده‌ایم که این بسته با چه آدرس مبدا ای فرستاده شود. p- هم برای مشخص نمودن پورت مورد استفاده قرار می‌گیرد. نهایتا پس از اجرای دستور بالا یک بسته‌ی SYN برای آدرس 192.168.1.10 بر روی پورت مقصد 80 و با آدرس مبدا 10.0.0.2 ارسال خواهد شد.

گفتنی است با استفاده از این دستور می‌توانید اندازه‌ی پنجره، نوع پروتکل، seq number و بسیاری موارد دیگر را نیز مشخص نمایید؛ همچنین از حالت flood آن برای انجام حملات DOS استفاده می‌شود.

تذکر: معرفی این ابزار صرفا جنبه‌ی آموزشی دارد و اکیدا توصیه می‌شود در شبکه‌های واقعی به‌طور نا آگاهانه از آن استفاده نکنید :). زیاد عواقب خوبی نداره مثلا ممکنه ban بشین.

امنیت اتصال به تجهیزات شبکه

مدیر شبکه برای اتصال به تجهیزات شبکه، مانند سوئیچ‌ها، به منظور پیکربندی، عیب‌یابی و ... از پروتکل‌های اتصال از راه دور همانند Telnet و SSH استفاده می‌کند. به دلیل امنیت بیشتر پروتکل SSH، استفاده از این پروتکل برای اتصال به تجهیزات پیشنهاد می‌شود.

آسیب پذیری‌های telnet

- همه‌ی نام‌های کاربری، رمزعبور و داده‌های ارسال شده از طریق شبکه به صورت متن در دسترس و آسیب‌پذیر هستند.
- یک مهاجم از راه دور می‌تواند سرویس Telnet را از کار بیاندازد. توسط حمله DDoS، با باز کردن تعداد بسیار زیادی session telnet به صورت جعلی.
- یک مهاجم از راه دور می‌تواند یک حساب مهمان فعال پیدا کند و ممکن است توسط آن حساب مورد اعتماد به سیستم نفوذ کند.

پوسته امن (SSH)

- SSH یک پروتکل server, client است که برای ورود به کامپیوتر دیگر از طریق شبکه، برای اجرای دستورات در یک ماشین راه دور و انتقال فایل ها از یک ماشین به ماشین دیگر استفاده می شود.
- احراز هویت قوی و ارتباطات ایمن را از طریق کانال های ناامن فراهم می کند.
- هنگام استفاده از سیستم SSH (به جای Telnet)، کل جلسه ورود، از جمله رمز عبور و جلسه login رمزگذاری می‌شود. بنابراین، دسترسی به رمز عبور برای افراد خارجی تقریبا غیر ممکن است.
- پیاده سازی های نسخه SSH 1 در برابر خطرات امنیتی مختلف آسیب پذیر هستند. در صورت امکان از SSH نسخه 2 به جای SSH نسخه 1 استفاده کنید.

پیکربندی SSH در سوئیچ طی گام‌های زیر انجام می‌شود

۱. تعریف یک حساب کاربری

```
Switch(config)# username user_name secret password
```

با دستور بالا یک کاربر به نام user_name و رمز عبور password ساخته می‌شود. برای حساب کاربری همچنین می‌توان یک سطح دسترسی مشخص کرد که بین سطح 0 تا سطح 15 می‌تواند متغیر باشد (15 بیشترین سطح دسترسی است):

```
Switch(config)# username user_name privilege 15 secret password
```

۲. تعریف یک دامنه

```
Switch(config)# ip domain-name example.com
```

پس از اجرای دستور بالا یک دامنه با نام example.com برای سوئیچ در نظر گرفته می‌شود.

۳. برای اتصال SSH به استفاده از یک جفت کلید عمومی و خصوصی (رمز نامتقارن) نیاز است که با دستور زیر این جفت کلید ساخته می‌شود سپس طول کلید را باید مشخص نمایید (توصیه می‌شود ۲۰۴۸ وارد فرمایید).

```
Switch(config)# crypto key generate rsa
```

۴. (گام اختیاری) مشخص کردن نسخه SSH (نسخه پیش‌فرض ۱ است ولی پیشنهاد می‌شود از نسخه ۲ استفاده شود)

```
Switch(config)# ip ssh version 2
```

۵. (گام اختیاری) تنظیم موردی همچون زمان timeout و تعداد دفعات مجاز برای احراز هویت

```
Switch(config)# ip ssh timeout 90 authentication-retries 2
```

۶. تنظیم خطوط اتصال به کنسول. line vty 0 تا line vty 15 خطوطی هستند که هنگام اتصال به کنسول سوئیچ از آن‌ها استفاده می‌شود. به کمک دستور زیر می‌توان این خطوط را پیکربندی کرد

با دستور زیر وارد محیط پیکربندی برای خطوط 0 تا 15 می‌شویم

```
Switch(config)# line vty 0 15
```

با استفاده از دستور زیر، سوئیچ برای احراز هویت از حساب‌های کاربری محلی تعریف شده در سوئیچ استفاده می‌کند

```
Switch(config-line)# login local
```

با دستور زیر پروتکل انتخابی برای ارتباط بیرون به سوئیچ را انتخاب می‌کنیم

```
Switch(config-line)#  transport input [ssh | telnet | all | none]
```

در کنار پیکربندی اتصالات به صورت ذکر شده، می‌توان برای خطوط VTY لیست کنترل دسترسی نیز مشخص کرد. به عنوان مثال، با اجرای دستورات زیر، فقط میزبان‌هایی با آدرس IP در محدوده 10.1.1.0/24 می‌توانند به کنسول سوئیچ متصل شوند

```
Switch(config)# access-list 10 permit 10.1.1.0 0.0.0.255
Switch(config)# line vty 0 15
Switch(config-line)# access-class 10 in
```

علاوه بر SSH و Telnet می‌توان از HTTP یا HTTPS نیز برای اتصال به کنسول سوئیچ استفاده کرد. از بین HTTP و HTTPS، استفاده از HTTPS به خاطر امنیت بیشتر نسبت به HTTP پیشنهاد می‌شود.

برای غیر فعال کردن HTTP و HTTPS از دستورهای زیر استفاده می‌شود

```
Switch(config)# no ip http server
Switch(config)# no ip http secure-server
```

برای استفاده از HTTPS، دستورات زیر استفاده می‌شود

۱. ساخت حساب کاربری:

```
Switch(config)# username user_name privilege 15 secret password
```

۲. اختصاص دامنه:

```
Switch(config)# ip domain-name example.com
```

۳. تولید کلیدهای نامتقارن:

```
Switch(config)# crypto key generate rsa
```

۴. غیر فعال کردن HTTP:

```
Switch(config)# no ip http server
```

۵. فعال‌سازی HTTPS:

```
Switch(config)# ip http secure-server
```

همچنین با اجرای دستور زیر، سوئیچ برای احراز هویت از حساب‌های کاربری محلی تعریف شده در سوئیچ استفاده می‌کند

```
Switch(config)# http authentication local
```

در حالت استفاده از HTTPS نیز می‌توان لیست کنترل دسترسی برای اتصالات تعریف کرد. به عنوان مثال، با اجرای دستور زیر

```
Switch(config)# access-list 10 permit 10.1.9.0 0.0.0.255
```

برای اعمال لیست ۱۰ روی اتصالات از دستور زیر استفاده می‌شود

```
Switch(config)# http access-class 10
```

در این حالت، فقط کاربران موجود در 10.1.9.0/24 قادر به اتصال به سوئیچ خواهند بود.

پایدار باشید