دانشگاه صنعتی اصفهان

دانشکده مهندسی برق و کامپیوتر

مقطع: کارشناسی

DHCP Spoofing | Snooping

نگارش

امیررضا نظری‌زاده

اردیبهشت ۱۳۹۹

فهرست مطالب

صفحه

بخش اول:

آشنایی با پروتکل ARP

۱-۱-آشنایی با ARP

هر دستگاهی که درون یک شبکه قرار دارد صاحب یک رکورد اطلاعاتی در جدول ARP[۱] در این جدول مشخص می‌شود که به هر مک آدرس درون شبکه چه IP تخصیص داده شده است. در این صورت، وقتی شما می‌خواهید به یک سیستم داده‌ای ارسال کنید، سیستم شما متوجه می‌شود سیستمی که IP مورد نظر را دارد، چه آدرس فیزیکی دارد. این جدول در سیستم عامل لینوکس برای سیستم‌های درون شبکه از طریق دستور زیر قابل مشاهده است:

Sudo arp –a

ARP Spoofing نوعی از حمله می‌باشد که در آن فرد نفوذگر به ارسال پیام ARP جعل شده در یک شبکه محلی، می‌پردازد. این عملیات منجر به اتصال آدرس فیزیکی (آدرس مک[۲]) نفوذگر به IP کامپیوترهای معتبر[۳] شبکه در جدولARP می‌شود. وقتی آدرس فیزیکی نفوذگر به IP یکی از دستگاه‌های معتبر شبکه وصل شود، نفوذگر می‌تواند تمام داده‌هایی که قرار بود به صاحب اصلی IP ارسال شود را دریافت کند. حمله ARP Spoofing می‌تواند به نفوذگر این امکان را بدهد که داده‌های در حال انتقال را تغییر دهد و یا جلوی آن‌ها را بگیرد. این حمله تنها برروی شبکه‌های محلی[۴] که پروتکل ARP در آن‌ها مورد استفاده قرار می‌گیرد قابل انجام است.

نتیجه حملات ARP Spoofing می‌تواند تاثیرات بسیار منفی برروی شرکت‌های تجاری بگزارد. به عنوان یک نمونه اولیه از این اثرات می‌توان به ربوده شدن اطلاعات حساس توسط مهاجم اشاره کرد. فراتر از آن، ARP Spoofing می‌تواند منجر به آماده‌سازی جملات دیگری همانند حملات زیر بشود:

- حملات DoS: این دسته از حملات به این صورت از اسپوفینگ آرپ بهره می‌برند که چندین آدرس IP را به یک آدرس فیزیکی (MAC) لینک می‌کنند، که در این حالت آدرس فیزیکی، همان آدرس قربانی می‌باشد. سپس، ترافیکی که قرار بود برای چندین آدرس IP متفاوت ارسال

---

۱ Address Resolution Protocol

۲ Mac Address

۳ Valid/Legitimare

۴ Local

شـــود، به ســـمت قربانی جهت داده می‌شـــود و باعث درگیری قربانی با حجم زیادی ترافیک ناخواسته می‌شود.

- Session Hijacking: مهاجم با Intercept کردن داده‌هایی که در حال رد و بدل شـــدن بین سیستم قربانی و دیگر سیستم ها است، می‌تواند به SessionID قربانی دست پیدا کند و با تغییر Session خود به Session قربانی، به اطلاعات حساس او دست پیدا کند.
- حملات MitM: این نوع از جملات نیز با استفاده از قابلیت اصلی اسپوفینگ آرپ یعنی دریافت و تغییر/قطع ترافیک، می‌تواند صورت بگیرند.

۱-۲-حملات ARP Spoofing

برای انجام عملیات جعل ARP یا همان اسپوفینگ، ابتدا به وسیله دستور زیر اطلاعات شبکه‌ای که در آن قرار داریم را دریافت می‌کنیم:

```
kali@kali:~$ sudo ip route
[sudo] password for kali:
default via 192.168.1.1 dev eth0 onlink
192.168.1.0/24 dev eth0 proto kernel scope link src 192.168.1.136
```

بنابراین در مثال بالا سیستم در شبکه‌ای با NetID نمایش داده شده یعنی ۱۹۲,۱۶۸,۱,۰ قرار دارد.
پس از متوجه شدن محدوده آدرس شبکه‌ای که در آن قرار داریم، با استفاده از دستور زیر می‌توانیم دستگاه‌هایی را که در شبکه فعلی حضور دارند مشاهده کنیم:

sudo netdiscover –r <range of IP>

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

98 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 5880
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.1.1     74:da:da:6a:27:91     72    4320  D-Link International
192.168.1.34    80:19:34:a3:e6:9d     22    1320  Intel Corporate
192.168.1.36    e0:19:1d:5b:aa:eb      3     180  HUAWEI TECHNOLOGIES CO.,LTD
192.168.1.33    c0:bd:d1:d3:61:22      1      60  SAMSUNG ELECTRO-MECHANICS(THAILAND
```

یکی از IPهای موجود را به عنوان هدف انتخاب می‌کنیم. (برای آزمایش می‌توان یک ماشین مجازی بارگزاری کرد و سپس عملیات را برروی آن انجام داد)

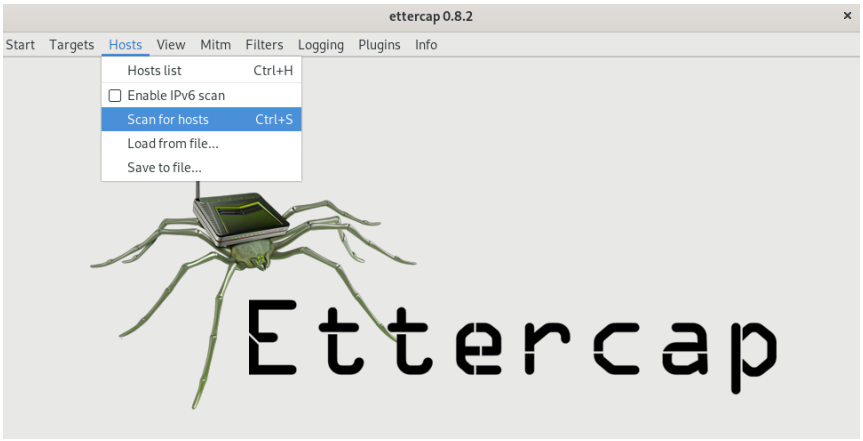
ابزاری که در اینجا می‌خواهیم به وسیله آن اسپوفینگ انجام بدهیم، Ettercap نام دارد. این ابزار به صورت پیش‌فرض برروی سیستم‌عامل‌هایی همانند Kali و یا ParrotOS نصب می‌باشد. در صورتی که این ابزار بر روی سیستم شما نصب نیست با استفاده از دستور زیر آن را نصب کنید (بر روی سیستم‌های مبتنی بر apt):

Sudo apt-get install ettercap-grapgical

سپس برنامه را در حالت سوپریوزر باز کنید:

Sudo ettercap –G

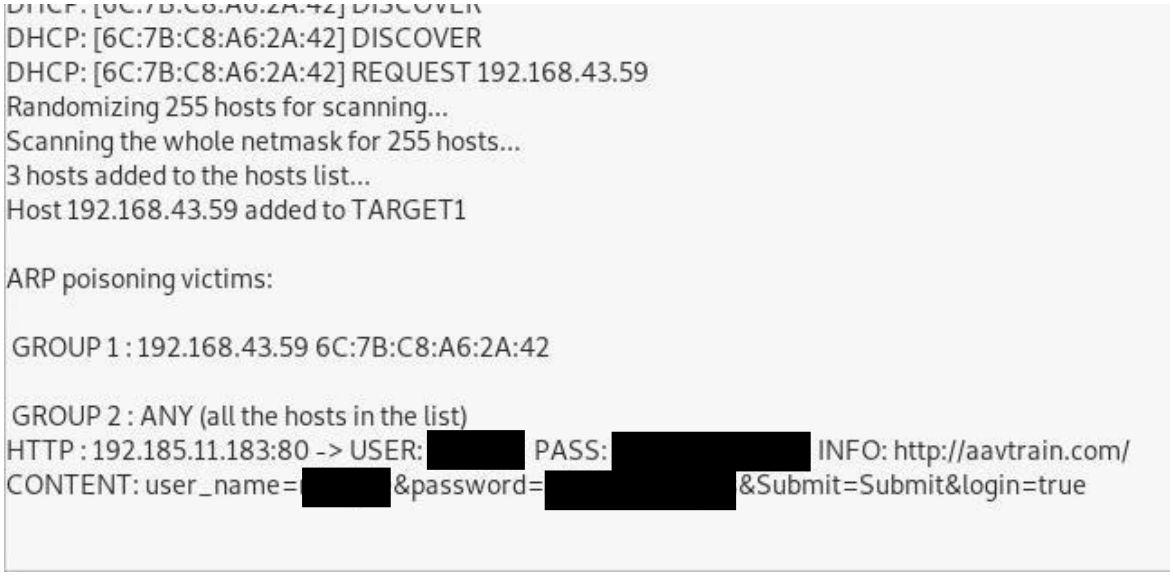
فلگ G به معنای باز کردن برنامه در حالت گرافیکی می‌باشد. بعد از باز شدن برنامه از نوار بالایی گزینه Sniff را انتخاب کرده بر روی Unified Sniffing کلیک کرده و کارت شبکه مورد نظر را انتخاب کنید.



در مرحله بعدی می‌بایست host و یا همان دستگاه‌های درون شبکه را اسکن کنیم. از نوار بالایی برنامه، گزینه Hosts را انتخاب کرده بر روی Scan for hosts کلیک کنید. بعد از اتمام اسکن، این بار از نواربالایی و گزینه Hosts ، آیتم Hosts List را انتخاب کنید تا هاست‌های اسکن شده را مشاهده کنید. بر روی Hostهای مورد نظر کلیک راست کرده و با زدن گزینه‌های Add هاست مورد نظر را در گروه‌های مجزا (گروه۱ و ۲) قرار دهید. این دو هاست برای مثال می‌تواند روتر خانگی شما و یک ماشین مجازی باشد.

بعد از انتخاب اهداف، نوبت به شروع حمله می‌رسد. این بار از نوار بالایی گزینه Mitm را انتخاب کرده، بر روی arp poisoning کلیک کنید. گزینه اول به معنای شنود ارتباطات ریموت می‌باشد بنابراین آن را انتخاب کنید. اگر می‌خواهید حمله یک طرفه (تنها پکت‌هایی که از گروه ۱ به گروه۲ می‌روند) انجام شود تیک گزینه دوم را بزنید. پس انجام تنظیمات، از منوی بالا، گزینه Start و سپس Start Sniffing

را بزنید. جزییات حمله از طریق خروجی پایین برنامه قابل مشاهده است. اگر تنظیمات درست انجام شده باشد، یکی از کارهایی که مهاجم می‌تواند انجام دهد این است که اگر قربانی در یک سایت که از SSL استفاده نمی‌کند، نام کاربری و رمز عبور خود را وارد کند، توسط مهاجم Intercept شده و مهاجم می‌تواند از آن سواستفاده کند:



همانطور که قابل مشاهده است، فیلدهای User و Password توسط مهاجم قابل رویت است.

بخش دوم:

آشنایی با پروتکل DHCP

۲-۱-آشنایی با DHCP

DHCP [۵] یک پروتکل مدیریت شبکه[۶] است که در شبکه‌های مبتنی بر IP مورد استفاده قرار می‌گیرد که به واسطه آن یک سرور DHCP به صورت پویا به تخصیص آدرس‌های IP و دیگر پارامترهای شبکه به دستگاه‌های درون شبکه می‌پردازد. در نتیجه این عملیات، دستگاه‌ها در شبکه شناسایی شده و می‌توانند با یکدیگر ارتباط برقرار کنند.

بسیاری از Access Pointها نظیر روترهای[۷] خانگی برای احراز دستگاه‌ها در شبکه خود، از پروتکل DHCP استفاده می‌کنند. ما نیز دراین گزارش در تلاش هستیم یک سرور DHCP را نصب و راه‌اندازی کنیم. بدین منظور، از یک سیستم لینوکسی متصل به شبکه استفاده می‌کنیم. مطالب مطرح شده در این گزارش بر روی سیستم‌عامل ویندوز نیز قابل انجام است، در صورت تمایل به راه‌اندازی این سرور مطرح شده بر روی سیستم‌عامل ویندوز به راحتی و از طریق جستجو در اینترنت و سایت رسمی مایکروسافت، اقدام کنید.

۲-۲-نصب DHCP

سرورهای DHCP زیادی برای لینوکس موجود می‌باشد. سرور ISC یکی از قدرتمندترین و معروف‌ترین سرورهای DHCP می‌باشد و در عین حال به سادگی قابل تنظیم است. ما نیز در این گزارش از ISC استفاده می‌کنیم.

در گام اول، به یک سیستم مبتنی بر لینوکس نیاز داریم. برای این کار از یک ماشین مجازی استفاده کنیم. لینوکس مورد استفاده در این گزارش مبتنی بر Debian می‌باشد، در عین حال اجرای عملیات این گزارش بر روی دیگر نسخ لینوکس تفاوت چندانی نمی‌کند. برای شروع، پس اطمینان از اتصال به اینترنت، سرور DHCP را از طریق وارد کردن دستور زیر در ترمینال لینوکس، نصب می‌کنیم:

```
sudo apt-get install isc-dhcp-server
```

---

[۵] Dynamic Host Configuration Protocol

[۶] Network Management Protocol

[۷] Router

پس از اتمام نصب، باید مشخص کنیم که سرور DHCP برای کدام یک از آداپتورهای موجود بر روی سیستم می‌بایست کار کند. برای مثال، ما قصد داریم از آداپتور wlan0 برای راه‌اندازی این سرور استفاده کنیم. به همین منظوراز طریق دستور زیر فایل مربوطه را به وسیله ویرایشگر nano باز کرده:

Sudo nano /etc/default/isc-dhcp-server

و نام آداپتور مورد نظر به عنوان مقدار متغیر INTERFACESv4 وارد می‌کنیم:

INTERFACESv4=”wlan0”

۲-۳-پیکربندی DHCP

در این مرحله ابتدا به سیستمی که سرور بر روی آن قرار است راه‌اندازی شود یک IP ایستا[۸] اختصاص می‌دهیم. بدین منظور فایل مربوطه را از طریق وایرایشگر nano و با دسترسی سوپریوزر Sudo باز می‌کنیم:

Sudo nano /etc/network/interfaces

خطوط زیر را به منظور تنظیم IP ایستا وارد می‌کنیم:

auto wlan0

iface wlan0 inet static

address 192.168.1.36

netmask 255.255.255.0

network 192.168.1.0

broadcast 192.168.1.255

gateway 192.168.1.1

---

[۸] Static Local IP

نام هر فیلد بیانگر نقش آن می‌باشـــد. برای مثال فیلد Address بیانگر IP می‌باشـــد که می‌خواهیم به صورت ایستا به سرور اختصاص داده شود. هم‌چنین فیلد Network بیانگر محدوده IPهای شبکه‌ای است که در آن قرار دارد.

پس از تنظیم IP ایستا برای سرور خود، حال نوبت به تنظیم سرور DHCP می‌رسد. برای اینکار فایل /etc/dhcp/dhcpd.conf را به صورت زیر تغییر می‌دهیم:

Sudo nano /etc/dhcp/dhcpd.conf

```
authoritative;
default-lease-time 86400;
max-lease-time 86400;
subnet 192.168.1.0 netmask 255.255.255.0}
  range 192.168.1.100 192.168.1.150;
  option routers 192.168.1.1;
  option domain-name-servers 192.168.1.1;
  option domain-name “local”;
}
```

بقیه خطوط این فایل را یا پاک کنید و یا به حالت کامنت در بیاورید. توجه کنید که در انتهای هر خط می‌بایست یک ; وجود داشته باشد. در اینجا خط اول یعنی authoritative به این معنی است که اگر DHCP سرور دیگری موجود نباشد، سروری که ما ساخته‌ایم وارد عمل شده و عملیات DHCP را انجام می‌دهد. دیگر پارامترها نیز پارامترهای مر سوم DHCP می‌باشند. فیلدهای بالا را مطابق با شبکه‌ای که در آن قرار دارید و با توجه به نیاز خود پر کنید.

حال نوبت به آن می‌رسد که سیستم را فعال کنیم. برا این کار سرویس DHCP را به وسیله دستور زیر فعال می‌کنیم:

Sudo systemctl start isc-dhcp-server

برای مشاهده وضعیت سرور می‌توانید از دستور زیر استفاده کنید:

```
Sudo systemctl status isc-dhcp-server
```

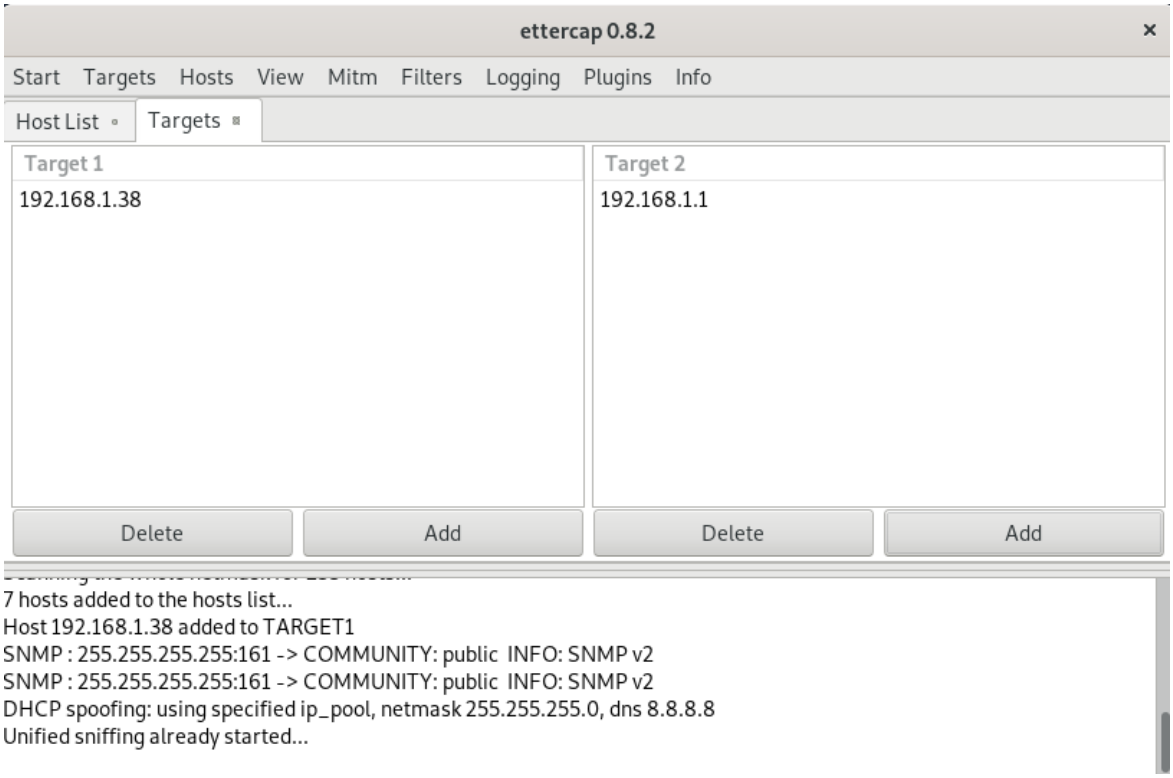
در اینجا پیکربندی سرور به اتمام میرسد. برای آزمایش سرور خود، یک دستگاه همانند تلفن همراه خود را برداشته و Wi-Fi آن را روشن کرده تا به شبکه متصل شود. توجه داشته باشید، برای راحتی آزمایش سرور می‌توانید از تنظیمات روتر خود، گزینه DHCP را غیر فعال کنید. این گزینه عموما در منوی local network روترها موجود است. برای پیدا کردن محل دقیق آن از سایت سازنده روتر استفاده کنید. پس از اتصال تلفن همراه، برای ارزیابی صحت عملکرد سرور، به قسمت تنظیمات تلفن رفته، IP محلی آن را بررسی می‌کنیم. این IP می‌بایست از بازه‌ای باشد که در تنظیمات DHCP روبروی کلمه کلیدی Range زدیم. روش دیگر، بررسی دستگاه‌های متصل از طریق وارد کردن دستور زیر در ترمینال سرور می‌باشد:

```
cat /var/lib/dhcp/dhcpd.leases
```

۲-۴-آشنایی با DHCP Spooping

همانطور که پیش‌تر اشاره کردیم، به هنگام ورود یک دستگاه به یک شبکه محلی، سرور DHCP یک IP محلی به آن دستگاه اختصاص می‌دهد. درخواست‌های DHCP به صورت Broadcast منتشر می‌شوند؛ فلذا در DHCP Spoofing هدف این است که جواب این درخواست از سمت نفوذگر و قبل از پاسخ واقعی از سمت سرور معتبر باشد. در این‌صورت می‌توانیم Default Gateway و دیگر المان‌های شبکه را طبق خواسته خود به درخواست کننده ارسال کنیم. برای مثال معرفی خود به عنوان GW شبکه به کاربر جدید، می‌توانیم ترافیک مدنظر را از سیستم خود مسیردهی کنیم.

برای انجام این حمله نیز، از ابزار Ettercap استفاده می‌کنیم. بدین منظور همانند حمله ARP Spoof که در ابتدای گزارش به آن پرداخته شد، پارامترهای مورد نیاز را در ابزار وارد می‌کنیم. در مرحله بعد بر روی گزینه Mitm کلیک کرده و گزینه DHCP Spoofing را انتخاب می‌کنیم. در فیلدهای پیش رو، در قسمت Netmask آدرس Subnet فعلی و در قسمت DNS Server یک DNS همانند ۸,۸,۸,۸ می‌دهیم. سپس از نوار Start، حمله را شروع می‌کنیم.



در شکل بالا، دستگاه‌های با آدرس ۱۹۲,۱۶۸,۱,۳۸ و ۱۹۲,۱۶۸,۱,۱ به عنوان اهداف انتخاب شده‌اند. در این حالت سیستم نفوذگر پس از انجام عملیات اسپوفینگ، می‌تواند خود را به عنوان GW شبکه به کاربر جدید با آدرس ۱۹۲,۱۶۸,۱,۳۸ معرفی کند.

۲-۵-آشنایی با DHCP Snooping

حملات DHCP Starvation یکی از حملات مر سوم شبکه‌های کامپیوتری می‌با شد که در آن عملکرد سرور DHCP مورد هدف قرار می‌گیرد. هدف اصلی این نوع از حملات این است که سرور DHCP شبکه مورد هجوم حجم زیادی از درخوا ست‌های DHCP یا DHCP Request Message به وسیله مک آدرس‌های مبدا جعل شده، قرار بگیرد. پس از رسیدن این حجم از درخواست‌ها به سرور DHCP، سرور به آن‌ها پا سخ می‌دهد بدون اینکه متوجه با شد که این یک حمله DHCP Starvation ا ست. مهاجم نیز تا تخلیه شدن تمامی محتوای DHCP Pool (مخزنی که در آن IPهای ممکن و قابل تخصیص به کاربران، درون آن نگه دا شته می شود) به ار سال این درخوا ست‌ها ادامه خواهد داد. حال که مهاجم اختیار آدرس‌های ممکن برای شبکه فعلی را دارد، می‌تواند کارهای مختلفی انجام دهد که نتیجه آن اختلال در شبکه خواهد بود. برای مثال می‌تواند به کاربران آدرس تجهیزات و زیرساخت‌های شبکه را اختصاص دهد که این باعث بوجود آمدن اختلالات جدی در شبکه می‌شود.

مکانیزم‌های مربوط به اسنوپینگ DHCP، برروی سوییچ‌های موجود در شبکه اعمال می شوند. برای مثال سوییچ‌های سیسکو و هواوی ارائه دهنده این خدمت برروی تجهیزات خود هستند. برای مثال سوییچ‌های Cisco ۳۷۵۰، Cisco ۲۹۶۰ و Cisco ۳۸۵۰ که جزو سوییچ‌های پرکاربرد چه در زمینه آموزش و چه در شرکت‌های تجاری هستند، قابلیت‌هایی را بدین منظور مهیا می‌کنند.

اسنوپینگ DHCP یک قابلیت لایه۲ در سوییچ می‌باشد که سرور DHCP نامعتبری که اقدام به آدرس‌دهی به کاربران می‌کند را مسدود می‌کند. روش کار اسنوپینگ DHCP مشخص و ساده است. این سازوکار پورت‌های سوییچ را به دو دسته تقسیم می‌کند:

- پورت‌های Trusted
- پورت‌های Untrusted

پورت مورد اعتماد که با نام‌های Trusted Source و هم‌چنین Trusted Interface نیز شناخته می‌شود، به پورت یا سورسی گفته می‌شود که پیام‌های DHCP آن مورد اعتماد است چراکه تحت نظارت ادمین سیستم می‌باشد. پس بنابراین در یک شبکه پورتی که به سرور DHCP متصل است Trusted نامیده می شود و دیگر پورت‌ها که به سیستم‌ها و یا تجهیزات دیگه متصل هستند، Untrusted نامیده می‌شوند.

اما سازوکار عملی اسنوپینگ DHCP به این صورت است که وقتی آن را فعال می‌کنیم، سوییچ شروع به جلوگیری از یک سری ترافیک مربوط به DHCP می‌کند تا بتواند در مقابل سرورهای DHCP جعلی از سیستم محافظت کند. برخی از این ترافیک‌ها عبارتند از:

- پیام‌های DHCP زیر را که از یک سرورDHCP که مورد اعتماد نیست را متوقف می‌کند:
  - DHCPACK
  - DHCPNACK
  - DHCPOFFER
- اگر پیام‌های DHCP که یک offer را reject و یا release می‌کنند از طرف ارتباط اصلی DHCP نباشند، توسط این مکانیزم مسدود می‌شوند.

و همچنین دیگر مواردی که به وسیله آن‌ها مکانیزم DHCP Snooping عملیاتی می‌شود.

برای تنظیم این کانیزم برروی سوییچ سیسکو پس از وارد شدن به مود Configure دستور زیر را وارد می‌کنیم تا سرویس بصورت Global برروی سوییچ فعال شود:

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

پس از فعال‌سازی، به وسیله دستور زیر VLAN ای که می‌خواهید این امکان برای آن فعال شود را وارد کنید:

```
switch(config)#ip dhcp snoop vlan 99,999
```

برای مثال این سرویس را برای vlan شماره ۹۹۹۹۹ فعال کردیم. حال همانطور که گفتیم، باید پورت متصل به سرورDHCP که می‌دانیم معتبر است را باید به عنوان اینترفیس مورد اعتماد تعریف کنیم. بدین منظور در مود Configure ابتدا وارد اینترفیس مربوطه می‌شویم و سپس آن را به عنوان یک اینترفیس مورد اعتماد معرفی می‌کنیم:

```
switch(config)#int g0/22
switch(config-if)#ip dhcp snooping trust
```

بنابراین سرور DHCP که برروی پورت g۰/۲۲ می‌باشد، به عنوان سرور معتبر شناخته می شود و دیگر کاربران و تجهیزات نمی‌توانند به عنوان سرور شروع به کار کنند چراکه طبق عملیات کنترل ترافیک DHCP که پیش‌تر گفتیم، فعالیت آن‌ها در این باره مسدود می‌شود.