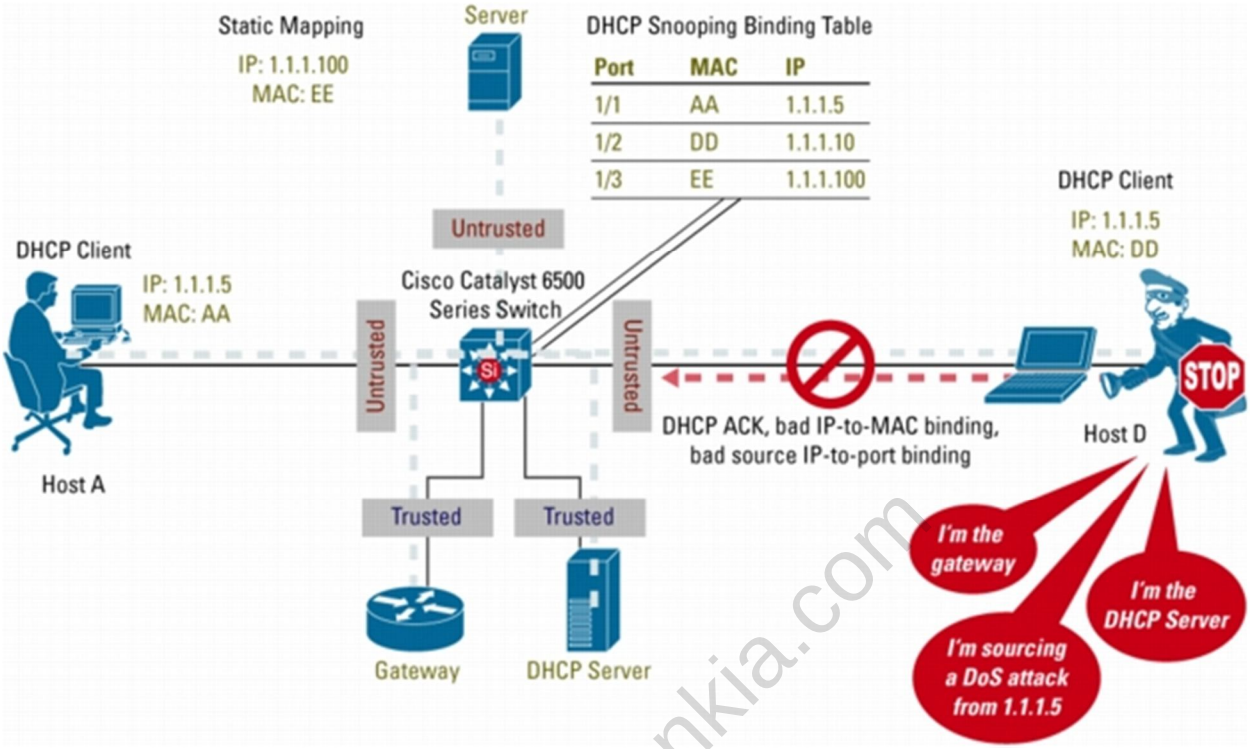
DHCP Snooping



یکی از پر مخاطره ترین حملات DOS یا همان حملاتی که با هدف از کار اندازی سرویس شبکه در شبکه های بزرک سازمانی به راحتی قابل اجرا می باشند، راه اندازی یک DHCP سرور جعلی است که در حالت ساخت یافته و پیشرفته می تواند منجر به حملات سطح بالاتری با اهداف مخربتر گردد.

علی رغم ادعا های ماکروسافت بر غیر قابل نفوذ بودن شبکه های مبتنی بر دامنه های تحت مدیریت سرور دامین کنترلر Windows server 2008 ، در عمل باز هم شاهد هستیم که کلاینت های عضو دامین به راحتی تحت تأثیر یک DHCP سرور Authorize نشده قرار می گیرند. به عنوان مثال کافی است یک مودم ADSL با تنظیمات پیش فرض که معمولا به حالت DHCP Enable می باشد را بصورت اتفاقی به شبکه متصل کنید. در این وضعیت درخواست های مبتنی بر دریافت IP Address کلاینت ها از طریق این مودم پاسخ داده شده و این دسته از کلاینت های شبکه بصورت خودکار دسترسی خود از سایر سرویس های مجاز شبکه را ازدست خواهند داد.

نقطه آسیب پذیری :

آسیب پذیری موجود زمانی مخاطره انگیز است که DHCP سرور جعلی با هدف تغییر جریان ترافیک شبکه به نقطه ای خاص طراحی و پیاده سازی شده باشد. به عنوان مثال در این حالت کوچکترین هدف می تواند دزدی نام های کاربری و کلمات عبور سیستم اتوماسیون اداری مربوط به یک سازمان باشد که از طریق تزریق اطلاعات جعلی DNS سرور به همراه اعطای IP Address عملیاتی خواهد شد.

راه حل :

یکی از موثر ترین روش های مهار این آسیب پذیری استفاده از مکانیزم DHSP SNOOPING یا به زبان ساده رجیستر کردن تنها DHCP سرور مجاز موجود در شبکه بر روی بستر شبکه Switching خواهد بود.

پس از اجرای این پیکربندی بر روی تجهیزات سوئیچ Cisco موجود در شبکه ، تنها پورت شبکه ای که مجاز به عبور بسته های حاوی پاسخ به DHCP Req خواهد بود همان پورت شبکه متصل به DHCP Server رسمی راه اندازی شده توسط مدیر شبکه خواهد بود.

برای پیکربندی DHCP Snooping بر روی سوئیچ های Cisco بصورت زیر عمل کنید:

1- ابتدا وارد محیط پیکربندی سوئیچ شده و دستور زیر را برای فعال کردن این قابلیت وارد نمایید.

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

با وارد کردن این دستور ، DHCP Snooping بصورت Globally بر روی سوئیچ فعال می شود ولی در صورت لزوم می توانید این قابلیت از طریق دستور زیر تنها بر روی یک VLAN خواص فعال نمایید.

```
Switch(config)#ip dhcp snooping vlan 20,30,35
```

در مثال فوق DHCP Snooping بر روی سه VLAN فعال شده است.

2- حالا نوبت مشخص کردن پورت شبکه متصل به DHCP Server واقعی و مجاز شبکه است.

برای این منظور وارد اینترفیس مورد نظر شده و دستورات لازم را بصورت زیر وارد می کنیم.

```
Switch(config)#interface fastethernet 0/1
Switch(config-if)#ip dhcp snooping trust
```

دستورات اخیر باید بر روی پورت شبکه متصل به DHCP Server و همه پورت های uplink اجرا شود.

محافظت از DHCP Server در برابر حملات DOS:

یکی از حملات رایج در رابطه با از کاراندازی سرویس DHCP موجود در شبکه، ارسال درخواست های جعلی درخواست IP Address است که با توجه به تعداد IP Address های محدود قابل ارائه در pool IP تعریف شده در DHCP سرور (مثلا 250 عدد) می تواند باعث ایجاد اختلال در شبکه گردد. در این حالت هکر با ارسال در خواست های جعلی به سرور DHCP سرور باعث سرریز شدن بافر مربوطه و یا اتمام IP Address های قابل ارائه در داخل یک Zone شبکه گردد.

به منظور تکمیل اقدامات امنیتی مربوط به سرویس DHCP سرور ، می توانید از دو دستور زیر نیز استفاده نمایید :

3 - جهت محدود کردن نرخ ارسال درخواست های DHCP از دستور زیر استفاده نمایید:

```
Switch(config-if)#ip dhcp snooping limit rate 75
```

شرکت سیسکو نرخ 100 بسته در ثانیه را به عنوان آستانه مجاز پیشنهاد می کند.

4- به منظور جلوگیری از ارسال بسته های جعلی درخواست DHCP هم می توانید دستور زیر را وارد نمایید:

Switch(config-if)#ip dhcp snooping verify mac-address

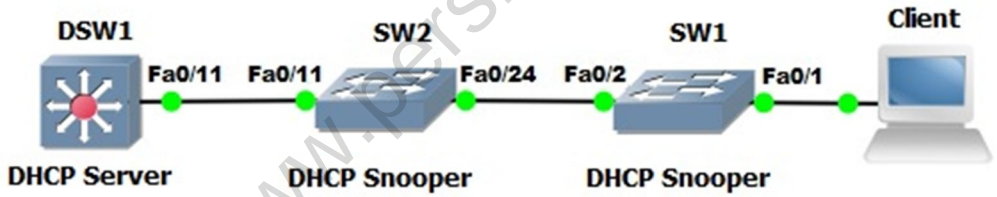
با این پیکربندی سوئیچ های سیسکو وضعیت یکسان بودن Source MAC address موجود در پکت DHCP را با Source MAC address واقعی یا همان آدرس فیزیکی کارت شبکه کلاینت چک می کند تا کلاینت متصل به یک اینترفیس untrusted با ارسال بسته های حاوی MAC Address جعلی باعث پر شدن ظرفیت IP pool مربوطه بر روی سرور DHCP نشود.

پیکربندی DHCP Snooping و مشکلات Option 82

در سطح یک سوئیچ بخوبی کار میکنه و مشکلی هم نداره اما وقتی فاصله کلاینت از DHCP Relay و DHCP سرور بیشتر از یک سوئیچ باشه اونوقت ماجرا تفاوت خواهد کرد. اولین موضوع قابل تامل، بروز اخلال کامل در عملکرد سرور DHCP و عدم موفقیت کلاین ها در دریافت آدرس IP از DHCP سرور و به دنبال آن احساس قطع ارتباط شبکه از سمت کلاینت ها می باشد.

شرح مشکل:

در سناریوی زیر بعد از اتمام پیکربندی DHCP Snooping ، سیستم کلاینت قادر به دریافت آدرس از DHCP نیست.



علت بروز مشکل:

هنگامی که DHCP Snooping بر روی سوئیچ ها فعال می شود، Option 82 بصورت خودکار بر روی بسته های DHCP اضافه شده و سپس از ترانک پورت سوئیچ SW1 خارج و به سوئیچ SW2 وارد می شوند. در سناریوی فوق ، پورت fa0/2 از SW1 و fa0/11 از sw2 در مود trust پیکربندی شده اند.در این حالت سوئیچ sw2 بسته های DHCP وارد شده از پورت شماره fa0/24 را Drop می کند زیرا سوئیچ امن شده با مکانیزم Snooping، از پذیرش بسته های DHCP حاوی Option 82 از روی پورت Untrusted ممانعت خواهد کرد. به همین سادگی ...

رویکرد های مواجهه با این مشکل:

1- تراست کردن بسته های DHCP با Option 82 از روی پورت های Untrust :

SW2(config)#ip dhcp snooping information option allow-untrusted

```
DSW1(config)#ip dhcp relay information trust-all
```

2- راه بعدی تراست کردن پورت شماره fa0/24 بر روی سوئیچ SW2 است که روش ایمنی نیست و توصیه هم نمی شود.