آسیب پذیری های سرور DHCP و روش مقابله با آن ها

سرویس DHCP یکی از مهمترین سرویس هایی است که در یک شبکه ارائه میشود، از این رو برقراری امنیت این سرویس از اهمیت ویژه ای برخوردار است. در این مقاله به بررسی حملات و روش های جلوگیری از Starvation DHCP(Dynamic Host Configuration Protocol)، راه اندازی Rough DHCP و حمله Middle Man in the به وجود آمده از طریق DHCP Starvatiom می‌پردازیم.

سرویس DHCP بیان کننده نحوه اختصاص دادن IP به سیستم هایی که برای متصل شدن به شبکه درخواست IP می کنند، است. سروری را که سرویس DHCP بر روی آن فعال شده باشد را سرور DHCP گویند.

هر سرور DHCP دارای یک سری رنج IPاست که با توجه به توپولوژی شبکه توسط مدیر سرور مشخص می شود. نحوه تخصیص دادن یک IP به یک سیستم کامپیوتری به این گونه است که در ابتدا هنگامی که یک سیستم (کامپیوتر رومیزی، سرور، پرینتر، روتر و ...) از لحاظ فیزیکی به شبکه متصل باشد، یک درخواست DHCP Discover را به صورت Broadcast از پورت UDP 67 به شبکه می‌فرستد.

در مرحله ۲ سرور DHCP با دریافت پیغام DHCP Discover یک IPبه دستگاه مورد نظر پیشنهاد می-دهد. این پیشنهاد تحت پیغام DHCP Offer به وسیله پورت ۶۸ UDP به صورت Unicast به دستگاه مورد نظر فرستاده می‌شود.

در مرحله سوم که سرور DHCP و دستگاهی که درخواست IP کرده است ارتباطی نظیر به نظیر (Point to Point) ایجاد کرده‌اند، دستگاه مورد نظر درصورت تمایل به تخصیص IP پیشنهاد شده، پیغام DHCP Request را به صورت Unicast به سرور DHCP اعلام می‌کند.

نهایتا در مرحله چهارم پیغام DHCP ACK از طرف سرور DHCP به دستگاه داده می‌شود که مبنی بر این است که IP به آن سیستم تخصیص داده شده و در پایگاه داده DHCP ذخیره می‌شود.

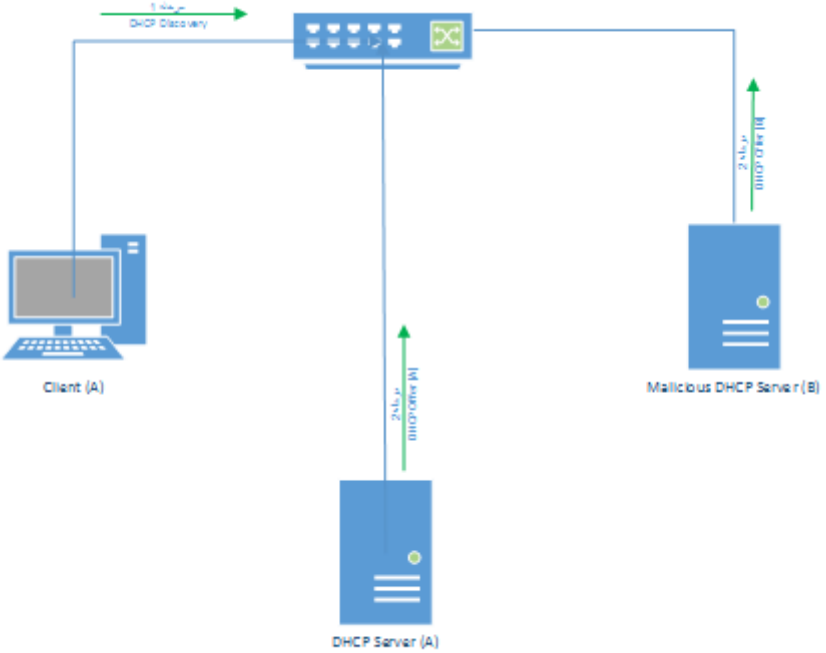
چالش‌های پیش روی پروتکل DHCP:

در مورد نحوه کار پروتکل DHCP و مراحل پاسخ دادن به درخواست یک سیستم خاص در قسمت قبلی توضیح داده شد. در این بخش تمرکز این مقاله را بر روی چالش‌های امنیتی که پیش روی این پروتکل است می‌گزاریم.

همانطور که گفته شد پیغام DHCP Discovery یک پیغام Broadcast است، از این رو در صورتی که

بیش از یک سرور DHCP در شبکه موجود باشند، هرکدام از آن سرورها به صورت مجزا به سیستم درخواست کننده پاسخ می‌دهند.

در این حالت، سیستمی که پیغام DHCP Discovery را فرستاده است با آن سروری عملیات را ادامه می‌دهد که پیغام DHCP Offer آن زودتر به دستش رسیده باشد. از این رو در صورتی که یک سرور DHCP تقلبی یا به اصطلاح Rogue DHCP در شبکه وجود داشته باشد درخواست DHCP Discovery به آن می‌رسد و شروع به ادامه دادن مراحل سرویس DHCP می‌کند.



در صورتی که DHCP Offer پیشنهاد شده از سمت سرور تقلبی، زودتر از پیغام DHCP Offer پیشنهاد شده از سمت سرور اصلی DHCP برسد، سیستمی که در ابتدا درخواست IP کرده بوده است از یک سرور DHCP مخرب IP را دریافت کرده است.

دریافت IP از سمت سرور تقلبی به خودی خود مشکلی را ایجاد نمی‌کند، اما حالتی را در نظر بگیریم که حمله کننده تغییراتی را در رنج IP که می‌خواهد به کاربران پیشنهاد بدهد ایجاد کند. تغییرات می تواند به یکی از حالت های زیر به وجود آید:

۱. پیشنهاد کردن رنج شبکه اشتباه

در این نوع حمله رنج شبکه اشتباهی به کاربر داده می‌شود. به طور مثال در صورتی که رنج شبکه ما 10.10.1.0/24 است، حمله کننده یک IP از رنج 172.16.32.0/26 به آن می‌دهد.
با به وجود آوردن این تغییر این سیستم خاص امکان برقراری ارتباط با شبکه داخلی خود را ندارد و کار کردن با آن مختل می‌شود.

۲. تغییر در تنظیمات default gateway

این حمله یکی از انواع حمله های ترکیبی به حساب می‌آید. نحوه کار شخص حمله کننده در این روش به این گونه است که در IP پیشنهاد شده به کاربر، IP خودش را به عنوان Default Gateway قرار می‌دهد. در مرحله بعدی حمله کننده با نصب کردن نرم افزارهای جاسوسی شبکه (Wireshark و ...) می تواند تمامی ارتباطات آن سیستم را مانیتور کند و از اطلاعات مورد نظر در راستای اهداف غیر قانونی خود استفاده کند.

۳. تغییر در DNS سرور

این روش حمله کردن را می‌توان خطرناک ترین نوع حمله در بین این دسته از حملات به شمار آورد. ماهیت حمله به این صورت است که حمله کننده در مرحله اول حمله یک Website تقلبی مالی، اجتماعی، ایمیل و ... همانند وب سایت های دیگر را طراحی کرده است. مرحله بعد راه اندازی یک DNS سرور تقلبی است بدین صورت که به جای برگرداندن IP واقعی سایت مورد نظر کاربر (مثل Gmail.com، bank.com و ...) IP وبسایت خود را به کاربر انتقال می‌دهد. در این صورت تمامی اطلاعات اکانت کاربر به دست حمله کننده می‌رسد.

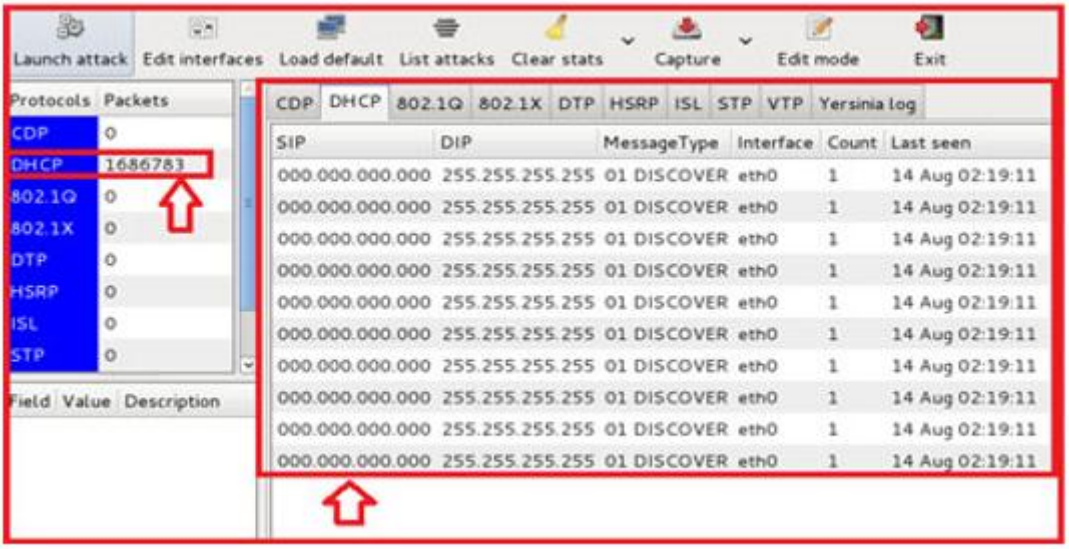
روش دیگر مورد استفاده حمله کننده برای تخریب سرویس DHCP:

در روش‌های حمله‌ای که در مرحله قبل صحبت شد، فرض بر وجود داشتن همزمان هر دو سرور مخرب و اصلی در شبکه داخلی بود. در این حالت با توجه به زودتر رسیدن یا نرسیدن پیغام DHCP Offer سرور مخرب به کاربران، اطلاعات آن کاربران خاص توسط حمله کننده

جاسوسی (Sniff) می‌شود.

آیا از دید حمله کننده این روش یک روش بهینه است؟ آیا راه حلی برای sniff تمامی سیستم ها وجود دارد؟ پاسخ این جاست که در صورتی که سرور اصلی DHCP به گونه‌ای مورد حمله قرار گیرد که قادر به سرویس دهی نباشد، تمامی سیستم های درون شبکه را می‌توان تحت کنترل خود داشت.

از این رو از روشی به نام Flooding برای از کار انداختن سرویس DHCP استفاده می‌شود. روش کار به این گونه است که حمله کننده با فرستادن درخواست‌های DHCP Discovery متوالی با MAC Address های تولید شده به صورت تصادفی پایگاه داده IPهای سرور DHCP را خالی می کند. حالا هنگامی که یک کاربر عادی DHCP Discovery را Broadcast می کند، دیگر سرور DHCP اصلی به دلیل موجود نداشتن IP پیغام DHCP Offer را نمی فرستد و تنها جواب از سمت سرویس DHCP راه اندازی شده توسط حمله کننده به دست کاربر می رسد.



نحوه دفاع در برابر حملات به سرور DHCP:

حال که از دید حمله کننده با نحوه حمله به سرور DHCP آشنا شدیم، نوبت به بررسی راه حل های دفع حمله است. بدین منظور از دو روش Port-security و DHCP Snooping استفاده می‌شود.

1. **Port-Security**

از Port-security به منظور جلوگیری از حمله Flooding به سرور DHCP استفاده می شود. روش کار به این گونه است که تعداد MAC-Address محدودی اجازه دسترسی به شبکه بر روی یک پورت خاص سوئیچ ازتباطی را خواهند داشت. بدین ترتیب دیگر حمله کننده توانایی فرستادن DHCP Discovery با چندین MAC-Address را نخواهد داشت.

روش کانفیگ کردن Port-security بر روی سوئیچ های Cisco به شرح زیر است:

توضیحات	دستورها
جهت وارد شدن به مد کانفیگ	Switch# configure terminal
با توجه به توپولوژی تمامی پورت ها غیر از پورت ۲۴ انتخاب می شود	Switch(config)# int r f 0/1-23
حالت کاری این پورت ها را user می گزاریم	Switch(Config-if-range)# switchport mode access
Port-security را بر روی پورت ها فعال می کنیم	Swiith(config-if-range)# switchport port-security
حالت violation را بر روی protected می گزاریم	Swiith(config-if-range)# switchport port-security protected violation
Mac-address هایی که اجازه ارتباط در شبکه را دارند را بر اساس MAC-Address های فعلی تعریف می کنیم	Swiith(config-if-range)# switchport port-security sticky mac-address

۲. DHCP Snooping:

DHCP Snooping همچون فایروالی بین هاست های غیر مطمئن و سرور DHCP عمل می‌کند.

کارهایی که این تکنولوژی انجام می دهد شامل موارد زیر است:

۲.۱. اعتبار سنجی (Validation) پیام های DHCP که از سمت منابع غیر مطمئن ایجاد می شود و فیلتر کردن پیام های نامعتبر

۲.۲. ساخت و نگهداری پایگاه داده DHCP Snooping که شامل اطلاعاتی راجع به هاست های غیر مطمئن و IP های تخصیص داده شده به آن ها است.

۲.۳.استفاده از پایگاه داده DHCP Snooping به منظور درخواست های بعدی که از سمت هاست های غیر مطمئن می‌رسد.

DHCP Snooping به صورت پیش فرض در همه Vlan ها غیر فعال است و Per vlan فعال می شود. این تکنولوژی پایگاه داده خود را به هنگام دریافت بسته های DHCP و تخصیص ip به سیستم ها به روز می کند.

Trust و Untrust: هاست های Trust هاست هایی هستند که اجازه فرستادن DHCP Offer را دارند. این پورت ها، پورت های متصل به سرورهای DHCP و پورت های (Uplink) Trunk هستند. لذا تمامی پورت های Trunk و آن هایی که سرور DHCP به آن ها متصل هستند به صورت Trust پیکربندی می‌شوند.

Limit rate: به منظور جلوگیری از حمله Flooding به سرور DHCP تعداد درخواست هایی که در بازه زمانی خاص به یک پورت فرستاده می‌شود با این پارامتر محدود می‌شود

نحوه پیکربندی سوئیچ های Cisco به منظور راه اندازی DHCP Snooping به شرح زیر است.

توضیحات	دستورات
فعال سازی DHCP Snoping بر روی Vlan 1	Switch(config)#ip dhcp snooping vlan 1
انتخاب پورت های متصل به دستگاه کاربران	Switch(config)#interface r f 0/1 - 22
Untrust کردن پورت های مورد نظر	Switch(config-range-if)#ip dhcp snooping untrust
انتخاب پورت های Trunk و متصل به DHCP	Switch(config-range-if)#int r f 0/23-24
Trust کردن پورت ها	Switch(config-range-if)#ip dhcp snooping trust
محدود کردن تعداد درخواست ها به ۱۰ عدد در ثانیه	Switch(config-range-if)#Ip dhcp snooping limit rate 10