به نام خدا

اسماعیل زارع

انواع حملات DHCP

DHCP یکی از پر استفاده ترین پروتکل های شبکه است Dynamic Host Configuration Protocol .پروتکلی است که توسط دستگاه‌های شبکه‌ای بکار می‌رود تا پارامترهای مختلف را که برای عملکرد برنامه‌های منابع گیر در IP ضروری می‌باشند، بدست آورد. با بکارگیری این پروتکل، حجم کار مدیریت سیستم به شدت کاهش می‌یابد و دستگاه‌ها می‌توانند با حداقل تنظیمات یا بدون تنظیمات دستی به شبکه افزوده شوند. پروتکل DHCP طبق RFC2131متشکل از ٤ مرحله رفت و برگشتی زیر است:

- DHCP Discover — broadcast from the client
- DHCP Offer — broadcast from the server
- DHCP Request — unicast from client
- DHCP ACK — unicast from server

انواع حملاتDHCP

مشابه پروتکل ARP به علت عدم وجود مکانیزم احراز هویت در زمان ورود کاربران به شبکه، حملات مختلفی می توان انجام داد که دو مورد زیر یکی از رایج ترین آنها می باشند:

DHCP Snooping : در این حمله یک Client خود را به جای سرور DHCP جا زده و اقدام به سرویس دهی به کاربران در هنگام ورود به شبکه می کند. این کلاینت می تواند با ارسال یک درگاه (Gateway) و DNS سرور اختصاصی حمله Man In the Middleرا انجام دهد و اقدام به DNS poisoning نماید.

DHCP Starvation : در این حمله یک Client چند درخواست ارسال کرده و تمام IP های حاظر را در DHCP Pool نگه می دارد. وقتی کاربران جدید به شبکه متصل می شوند دیگر IP ای وجود ندارد و در نتیجه Denial of Service رخ می دهد.

DHCP Spoofing چیست؟

حمله ای است که در آن هکرها سرور DHCP را نصب می کنند و از آن برای ارسال پاسخ های جعلی DHCP به دستگاه های یک شبکه استفاده می کنند.

هکرها اغلب از این حمله برای جایگزینی آدرس های IP سرورهای Default Gateway و DNS استفاده می کنند و از این طریق ترافیک را به سمت سرورهای مخرب منحرف می کنند.

فرض کنید شما در شبکه یک کامپیوتر رومیزی دارید که طبیعتا یک Client است.

برای برقراری ارتباط میان این کامپیوتر با دیگر اجزای شبکه و همچنین شبکه های دیگر به یک IP نیاز دارید.

شما می توانید این IP را از طریق) DHCP تخصیص IP به صورت خودکار (دریافت کنید.

به هر سیستمی که پروتکل DHCP بر روی آن راه اندازی شده باشد، DHCPسرور می گویند.

این Client برای دریافت IP ابتدا یک درخواست به سمت DHCP Server برای گرفتن IP ارسال می کند؛ سپس DHCP Server یک Packet که حاوی یک IP خاص، DNS، Subnetشبکه و default gateway می باشد را به Client به مورد نظر ارسال می کند و آن Client می تواند به این صورت با دیگر اجزای شبکه ارتباط برقرار کند.

اما در این میان افرادی سودجو هستند که می خواهند اطلاعات مربوط به آن شبکه یا آن Client را به دست آورده و یا شبکه ی مورد نظر را دچار اختلال کنند.

آنها با قرار دادن DHCP سرور های تقلبی می توانند به Client ها دسترسی داشته باشند.

زمانی که Client ها از سرورهای اصلی درخواست IPمی کنند، ممکن است در واقع به DHCP Server تقلبی این درخواست را ارسال کرده باشند؛ بنابراین Server تقلبی یک IP به Client می دهد که با دستکاری هایی که بر روی این IP می کند، قصد اختلال و از کار انداختن شبکه را دارد.

روش های جلوگیری از حملاتDHCP Spoofing

اما چگونه می توان جلوی DHCP Spoofing در شبکه را گرفت؟

1- Port Security

از این روش می توان برای رفع حملاتی که برای از کار انداختن DHCP Server صورت می گیرد، استفاده کرد.

با استفاده از این روش، Mac Addressهای مشخصی در یک پورت خاص در شبکه اجازه دسترسی دارند. در این صورت دیگر فرد مهاجم قادر به ارسال بسته های حاوی در خواست IP با چند Mac Address را نخواهد بود.

2- DHCP Snooping

به طور خلاصه می توان **DHCP Snooping** را به این گونه شرح داد که مانند فایروالی میان DHCP Sever و Host های نا معتبر و غیرقابل اطمینان است و روش کار آن به این گونه است که:

- DHCP Snooping پیام های که از طرف Host های نامعتبر و دستگاهای نا معتبر (دستگاهای که به عنوان مثال در یک سازمان وجود ندارند و بیرون از سازمان قرار دارند) به DHCP Serverارسال می شود را فیلتر می کند.
- کار **DHCP Snooping** ساخت یک جدول و یا یک پایگاه داده است که اطلاعات این جدول شامل IP ها، DNSها و... تخصیص داده شده به Host ها است.
- استفاده از همان جدول به منظور شناسایی پیام های بعدی که از سمت Host های نامعتبر در دفعات بعدی می رسد.

3- Trust – Untrust

حالت Trust به حالتی می گویند که Host های معتبر اجازه دسترسی و ارسال بسته به DHCP Server را دارند.

در واقع به پورت هایی که به DHCP Server اجازه دسترسی دارند را پورت Trust و به پورت ها و Host هایی که اجازه دسترسی به DHCP Server را ندارند Untrust می گویند.

4- Limit Rate

این روش به این گونه است که در بازه زمانی مشخصی تنها می توان تعداد خاصی درخواست به DHCP Server ارسال کرد و به این ترتیب از حمله به DHCP Server و خالی کردن لیست IP آن جلوگیری کرد.

قابلیت DHCP Snooping در سوئیچ های لایه ۲ موجود می باشد که می توان آن را فعال کرد.

مشکلات DHCP اسپوفینگ برای شبکه

۱- تغییر دادن: IP

فرض کنید شما یک Client هستید و یک درخواست برای گرفتن IP از DHCP Server می دهید.

در اینجا DHCP server تقلبی وارد عمل می شود و با دادن یک IP تقلبی به جای IP اصلی آن Client را دچار مشکل می کند؛ به عنوان مثال به جای دادن آدرس ۲٤/۱۹۲.۱٦۸.۱.۰ به شما آدرس 172.168.16.0/30را می دهد و باعث تداخل آن Client شده و در واقع آن Client را در شبکه از کار می اندازند.

۲- تغییر: default gateway

در اینجا فرد مهاجم IP خود را به عنوان default gateway به Client می دهد.

بنابراین هر بسته ای که از طرف آن Client بخواهد به خارج از شبکه برود، ابتدا به سمت سیستم تقلبی ارسال می شود و شخص مهاجم اطلاعات مورد نیاز خود را بدست می اورد.

سپس آن بسته را به سمت مقصد اصلی خود ارسال می کند؛ بدون آن که کسی در بین از این اتفاقات با خبر شود.

۳- تغییر در: DNS

یکی دیگر از اطلاعاتی که به همراه IP و ... به یک Client داده می شود، آدرس DNS Server آن شبکه است تا شخص بتواند به سایت های مختلف دسترسی داشته باشد.

در اینجا فرد مهاجم ابتدا با طراحی سایتی تقلبی، به عنوان مثال پرداخت آنلاین یک بانک، اولین قدم خود را بر می دارد سپس در مرحله دوم اقدام به ساخت یک DNS Server تقلبی می کند.

بدین صورت فرد آدرس IP خود را به جای آدرس IPسایت واقعی مانند GOOGLE و یا .... بر می گرداند و وبسایت خود را به کاربر انتقال می دهد. با این روش می توان تمامی اطلاعات مهم یک فرد را بدست آورد.

۴- از بین بردن DHCP Server اصلی:

در اینجا فرد حمله کننده قلب سرویس DHCP را مورد حمله قرار می دهد.

به این صورت که فرد مهاجم درخواست هایی را به صورت متوالی با Mac Address های تصادفی که تولید می کند، به Serverاصلی می فرستد.

در این زمان هم DHCP به تمام آن ها پاسخ داده و به هر کدام یک IP بخصوص می دهد.

تا اینجا کار به نظر مشکلی وجود ندارد؛ اما زمانی شبکه دچار مشکل می شود که پایگاه داده IP های DHCP Server اصلی خالی شده و دیگر IP برای تخصیص به Client ها وجود ندارد.

از اینجا به بعد هر Client که در شبکه درخواستی برای گرفتن IP می کند در واقع تمامی آن ها را به Server تقلبی ارسال می کند و بنابراین آدرس هایی که به آن ها داده می شود دستخوش تغییراتی است که در مراحل قبل درباره آن ها صحبت کردیم.

DHCP Starvation چیست؟

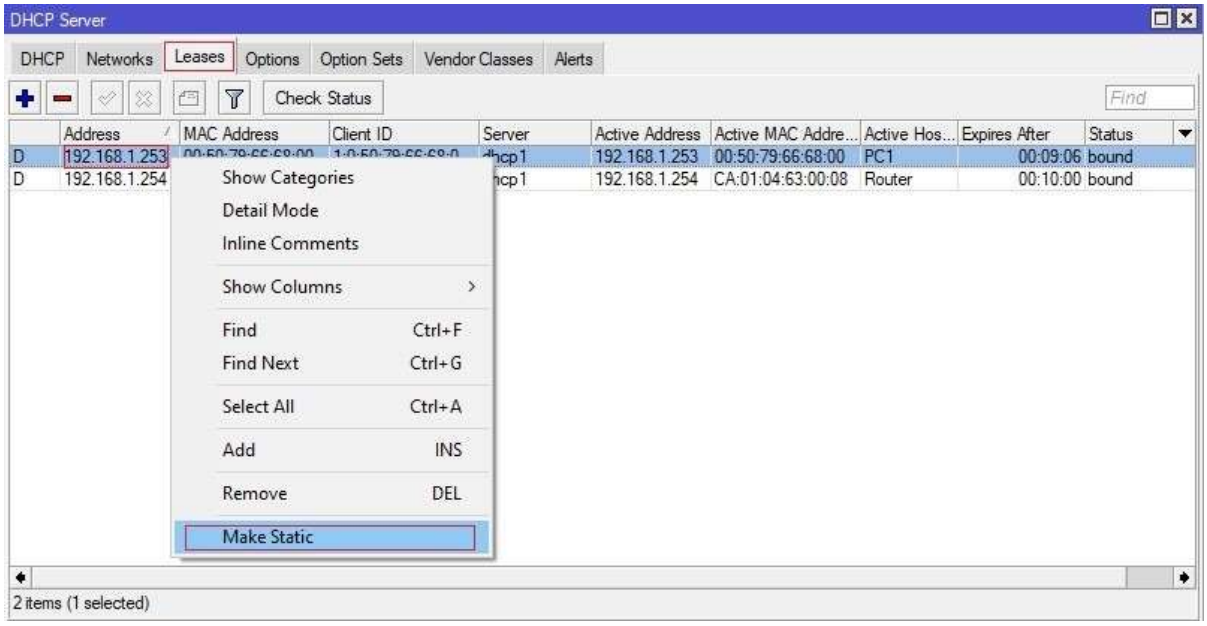
یک مدل حمله با نام DHCP Starvation وجود دارد که یکی از حملات رایج در شبکه محسوب می گردد Starvation .در لغت به معنای قحطی می باشد و در این جا به تمام شدن و خالی شدن Pool آدرس های IP اشاره دارد. به واسطه حملات DHCP Starvation به راحتی می توان یک شبکه را مختل نمود. این حمله به این صورت شکل می گیرد که مهاجم در عرض چند ثانیه تعداد زیادی آدرس MAC جعلی ایجاد و سپس با استفاده از این آدرس های MAC جعلی به سمت DHCP Server درخواست ارسال می نماید.

در مقابل DHCP Server بدون اطلاع از حمله انجام شده به ازای هر درخواست یک آدرس IP به آن اختصاص می دهد. بنابراین در مدت زمان کوتاهی تمام آدرس های موجود در Pool به آدرس های MAC جعلی اختصاص داده می شود و Pool به کلی

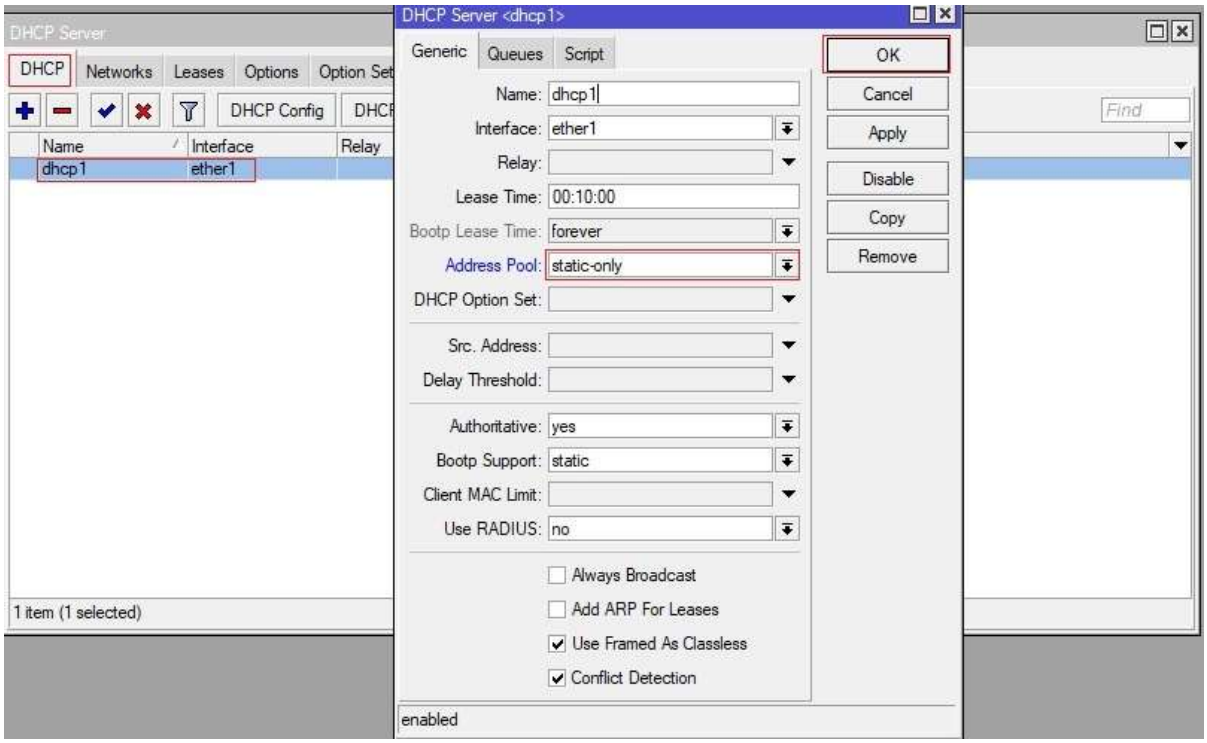
خالی می شود و دیگر آدرسی برای تخصیص به دستگاه های واقعی و مجاز در شبکه وجود نخواهد داشت. حالا دستگاه های مجاز در شبکه امکان دریافت آدرس IP را نخواهند داشت و ارتباط تمام تجهیزات و کامپیوتر ها در شبکه با یکدیگر قطع خواهد شد.

راهکار جلوگیری از DHCP Starvation

برای مقابله با این حمله راهکاری در میکروتیک وجود دارد که با تنظیمات مربوطه می توان از وقوع چنین حملاتی جلوگیری نمود. جهت پیشگیری از این حملات می بایست ابتدا کلاینت های مجاز در شبکه آدرس IP را دریافت نمایند. برای مثال ما قصد داریم PC1 و Router در شبکه ما حتما آدرس IP داشته باشند. پس از این که دستگاه های مد نظر ما در شبکه آدرس های خود را دریافت نمودند ما از طریق تب Leases می توانیم مشاهده کنیم که هر دستگاه با چه آدرس MAC چه آدرس IP دریافت کرده اند. حال ما با کلیک بر روی IP تخصیص یافته به دستگاه مورد نظر خود گزینه Make Static را انتخاب می نماییم.



بعد از اینکه دستگاه های مد نظر خود را در حالت Make Static قرار دادیم روی تب DHCP کلیک نموده و روی DHCP ساخته شد خود دوبار کلیک می کنیم. در پنجره باز شده یک قسمت با نام Address Pool وجود دارد این قسمت را روی Static-only قرار می دهیم و بر روی OK کلیک می نماییم.



با انجام این کار به غیر از دستگاه ها و تجهیزاتی که Make Static شده اند، هیچ دستگاه دیگری قادر به ارسال درخواست به DHCP Serverو دریافت آدرس IPانخواهد بود و نکته قابل ذکر این است که دستگاه هایی که IP دریافت نموده اند و در حالت Make Staticقرار گرفته اند برای همیشه همان آدرس را دریافت خواهند کرد و آدرس IP آن ها دیگر تغییر نخواهد نمود.