حمله ها و چگونگی آنها در لایه ۲:

Spanning Tree Protocol (STP) Attacks

پروتکل STP در شبکه های LAN-Switched به کار می رود. عملکرد اصلی آن از بین بردن Loop در شبکه می باشد. بدون این پروتکل شبکه های لایه ۲ از کار می ایستند. زیرا Loop های ایجاد شده در شبکه باعث ایجاد Flood و توقف آن می شوند. عملکرد و برنامه ریزی صحیح STP یک شبکه امن و باثبات را بوجود آورده و از گردش روان اطلاعات در شبکه اطمینان حاصل می کند. اگر یک هکر یک دستگاه STP جدید به شبکه اضافه کند و باعث ایجاد اختلال در عملکرد STP شود، میتواند چگونگی گردش اطلاعات را تحت تأثیر قرار داده و امنیت و قابل استفاده بودن ترافیک شبکه را به خطر اندازد.

Address Resolution Protocol (ARP) Attacks

پروتکل ARP توسط همه سیستم هایی که به یک شبکه اِترنت متصل هستند استفاده می شود. دستگاه ها از ARP برای پیدا کردن آدرس MAC لایه ۲ دستگاه مقصد و با استفاده از آدرس IP آنها استفاده می کنند. ARP به خودی خود نا‌امن است، زیرا دستگاه ها باید به جواب هایی که دریافت می کنند اطمینان کنند. بنابراین اگر دستگاه A، آدرس MAC دستگاه B را درخواست نماید و دستگاه C به جای B جواب دستگاه A را بدهد، دستگاه A اطلاعات را که مقصد آنها دستگاه B بوده به دستگاه C می فرستد. اگر دستگاه C در حال تلاش برای حمله (اختلال) باشد، ترافیک مخرب را به دستگاه B می فرستد. به این حملات Man in the Middle گفته می شود.

Media Access Control (MAC) Spoofing

در حمله جعل MAC یا MAC Spoofing، یک دستگاه در شبکه از آدرس MAC دستگاهی دیگر در شبکه استفاده می کند. هدف هکر عوض کردن مسیر ترافیکی می باشد که باید به دستگاه مقصد برسد و توسط دستگاه هکر (مخرب) دریافت می شود (اسپوفینگ چیست انواع حملات اسپوفینگ). اگر به شبکه تلفن فکر کنید، درست مانند اینست کسی کنترل تلفن شما را بدست آورد و زنگ هایی که قرار است به شما برسد پاسخ دهد. این مسیردهی مجدد می تواند برای مقاصد مختلفی از جمله تغییر مقصد یا حملات DoS استفاده شود.

Content Addressable Memory (CAM) Table overflows

جداول CAM یا جداول آدرس MAC در سوئیچ ها برای ردیابی مقصد به منظور فرستادن ترافیک استفاده می شوند. برای درک بهتر این حمله، شما نیاز دارید عملیات اولیه جداول CAM و اینکه چگونه باعث بهینه شدن نقل و انتقال اطلاعات در سوئیچ می شوند را بهتر درک کنید.

وقتی سوییچ روشن می شود، جدول CAM سوئیچ خالی است. سوییچ نمی داند کدام دستگاه به کدام اینترفیس متصل است و در نتیجه اطلاعات ارسالی اولیه را به همه اینترفیس ها ارسال میکند (Flooding). همانطور که جدول CAM اطلاعات را در اینترفیس مقصد دریافت میکند، اطلاعات آدرس های MAC دریافتی را در جدول وارد می کند و در نتیجه هر آدرس MAC را با همان اینترفیس ثبت میکند. وقتی سوئیچ آدرس MAC همه دستگاه های مقصد را داشته باشد دیگر ترافیکی Flood نمی شود و هر ترافیکی به آدرس مشخص مقصد فرستاده می شود و بنابراین پهنای باند سوییچ اضافه می شود.

هر سوئیچ تعداد مشخصی آدرس MAC را میتواند ثبت کند. بنابراین اگر جدول پر شود، ترافیک آدرس MAC ناشناخته Flood می شود. حمله CAM Table overflow اینگونه انجام می شود که یک یا چند دستگاه تعداد زیادی آدرس MAC را جعل می کنند و ترافیک را در سوئیچ پخش می کنند. جدول CAM سوییچ پر شده و همه ترافیک Flood می شود که باعث اشغال پهنای باند سوئیچ شده، انتقال اطلاعات را کند کرده و شبکه را مختل و غیر قابل استفاده می کند.

Cisco Discovery Protocol (CDP)/Link Layer Discovery Protocol (LLDP) Reconnaissance

پروتکل های CDP و LLDP برای مقاصد مشابهی استفاده می شوند. هر دو برای تشخیص نوع و اطلاعات مربوطه به دستگاه متصل به شبکه است. معمولاً این اطلاعات توسط ادمین های شبکه برای بهبود راهکارهای رفع مشکل در شبکه های بزرگ استفاده می شوند. همچنین این اطلاعات معمولاً قابل دسترس همه افراد هستند که این بدان معناست که یک هکر با Listen کردن یک لینک می تواند اطلاعات زیادی درباره دستگاه های متصل بدست آورد.

Virtual LAN Hopping

دو نمونه از حملات VLAN Hopping با یک هدف واحد (ارسال ترافیک به یک VLAN دیگر) وجود دارد.

Switch Spoofing

در این حمله هکر تلاش می کند یک سوئیچ اشتباه را به شبکه اضافه کرده و یک Trunk ایجاد کند. اگر حمله موفق باشد ترافیک VLAN های مختلف از این سوییچ عبور خواهد کرد و امکان بازبینی و تغییرات اطلاعات را برای هکر ایجاد می کند. این حمله بر اساس خصوصیات دینامیک Trunk ها در سوئیچ می باشد. اگر Trunking دینامیک غیر فعال شود و اینترفیس های غیر Trunk برای Trunk شدن برنامه ریزی نشوند این حمله بی اثر می شود.

Double Tagging

مشابه حملات جعل (Spoofing) دیگر، در جعل DHCP هکر سعی در جازدن خود به جای دیگریست. در اینصورت باید بعنوان سرور DHCP قانونی خود را جا بزند. بدلیل اینکه DHCP در بیشتر شبکه ها برای تخصیص آدرس ها و دیگر اطلاعات به کاربرها استفاده می شود از دست دادن کنترل این بخش از شبکه می تواند بسیار خطرناک باشد.

در حملات جعل DHCP یا DHCP Spoofing، هکر یک سرور DHCP جعلی را جاگذاری می کند. هنگامیکه کاربران درخواست تخصیص IP به سرور می دهند، سروری که سریعترین جواب را بدهد استفاده می شود. اگر کاربر از سرور جعلی که هکر جاگذاری کرده است جواب بگیرد، سرور جعلی می تواند هر آدرسی به آن تخصیص دهد و همینطور اینکه چه دستگاهی به عنوان Gateway استفاده می شود را کنترل کند .یک حمله خوب طراحی شده میتواند ترافیک کاربران را به سمت سرور جعلی هدایت کرده و به سمت Gateway دلخواه بفرستد. این حمله بسیار پنهان است بدین معنی که هکر به راحتی و بصورت پنهان میتواند به سرقت اطلاعات ادامه دهد.