**به نام خدا**

**نام و نام خانوادگی: بیتا بهروان**

**انواع حملات DNS و نحوه جلوگیری از آن‌ها**

منظور از حملات DNS هر نوع حمله‌ای است که سیستم نام دامنه (DNS) را درگیر کند. روش‌های مختلفی وجود دارد که مهاجمان می‌توانند از نقاط ضعف DNS استفاده کنند برای مثال بیشتر این حملات سواستفاده از DNS برای جلوگیری از دسترسی کاربران اینترنت به وب‌سایت‌های خاص است، این حملات DNS همچنین می‌تواند با هدایت بازدیدکنندگان سایت به صفحات (DNS hijacking) همراه باشد. مهاجمان همچنین می‌توانند از پروتکل DNS برای دزدیدن اطلاعات حساس از سازمان‌ها یا (DNS tunneling) استفاده کنند.

**انواع حملات DNS**

سیستم DNS پیچیده است و مهاجمان می‌توانند با در نظر گرفتن اهداف نهایی مختلف، از روش‌های مختلفی استفاده کنند. هدف بسیاری از این حملات این است که با ایجاد ترافیک جعلی، از دسترسی به سایت‌ها و  شبکه‌ها جلوگیری کنند.

به معنای کلی، این حملات با نام Denial-of-Service (DoS) شناخته می‌شوند که در امنیت سایبری رایج است. رایج ترین شکل حمله DoS، حمله Distributed Denial-of-Service یا DDoS است که اساساً بدان معنی است که ترافیک مهاجم از یک منبع نیست. در عوض، سرور از هزاران آدرس IP مختلف، که معمولاً بخشی از یک botnet هستند ، مورد حمله قرار می‌گیرد. این امر باعث می‌شود که حملات DDoS در مقایسه با حملات DoS بسیار دشوارتر باشد.

**Domain hijacking**

این نوع حمله می‌تواند تغییراتی در سرورهای DNS و ثبت دامنه شما ایجاد کند و ترافیک شما را از سرورهای اصلی به مقصد جدید هدایت کند. هنگامی که هکری نام دامنه‌ای را می‌رباید، کاربران را به سایت‌های مخرب و جعلی هدایت می‌کند. این وب‌سایت‌های جعلی اغلب به گونه‌ای طراحی شده‌اند که مانند یک سایت قانونی به نظر می‌رسند و هدف آنها فریب قربانیان برای وارد کردن اطلاعات ورود به سیستم یا جزئیات کارت اعتباری آنها است. سپس هکرها از این اطلاعات برای دسترسی به حساب‌های بانکی یا کلاهبرداری و ارتکاب جرایم دیگر استفاده می‌کنند.

هکرها با استفاده از Domain hijacking همچنین می‌توانند کاربران را به وبسایت‌هایی که شامل بدافزار هستند، هدایت کنند. این بدافزارها می‌تواند شامل باج‌افزارها (مسدود کردن دسترسی به سیستم و درخواست پول برای رفع این مشکل)، نرم‌افزارهای جاسوسی، نرم‌افزارهای تبلیغاتی و طیف وسیعی از برنامه‌های مخرب دیگر باشد. همچنین می‌توانند با هدایت کاربران به سایت‌هایی مملو از تبلیغات، بر حسب هر بازدید یا کلیک درآمد کسب کنند.

**DNS Flooding**

این نوع یکی از اساسی‌ترین انواع حمله DNS است. در این سرویس توزیع‌نشده (DDoS)، مهاجم سرورهای DNS شما را مورد حمله قرار می‌دهد. هدف از این نوع حمله این است که با ارسال درخواست‌های بیش از ظرفیت، سرور شما را از کار بیندازند و پاسخگویی به درخواست‌ها با مشکل روبرو می‌شود.

حملات DDoS نه تنها می‌تواند سرورها را با ترافیک جعلی خود غرق کند و از کار بیندازد، بلکه باعث می‌شود کاربرانی که نمی‌توانند به وب سایت متصل شوند، مروگر خود را به‌طور مداوم رفرش کنند که در نتیجه تعداد درخواست‌ها بیشتر شده و حمله را بدتر می‌کند.

**NXDOMAIN**

حمله NXDOMAIN نوع خاصی از DNS flooding است که در آن هکر تعداد زیادی درخواست بی‌اعتبار را به یک سرور DNS مشخص ارسال می‌کند. در پی این درخواست‌ها سرور به شناسایی و احراز هویت این IP های جعلی می‌پردازد و هر چه تعداد این درخواست‌های جعلی بیشتر باشد، سرور به‌گونه‌ای توسط آن‌ها اشغال می‌شود که پاسخ‌دهی به درخواست‌های واقعی مختل می‌شود. هدف اصلی این حمله این است که سرور DNS شما وقت، نرم‌افزار و منابع سخت‌افزاری خود را صرف درخواست‌های غیرمعتبر کند که باعث خرابی سرویس می‌شود، زیرا حافظه پنهان DNS کاملاً با نتایج خرابی NXDOMAIN پر می‌شود.

از نظر عملی، به این معنی است که وقتی کاربران سعی می‌کنند از وب‌سایتی بازدید کنند که سرور آن مورد حمله DNS قرار گرفته است، اگر آدرس IP را در حافظه پنهان (Cache) نداشته باشند، تأخیرهایی را در لود شدن وبسایت تجربه می‌کنند یا اصلا نمی‌توانند به آن دسترسی پیدا کنند.

شناسایی حملات NXDOMAIN برای مدیران سرور DNS دشوار است، زیرا ممکن است فکر کنند سرور دچار مشکل عملکردی شده است و متوجه درخواست‌های نامعتبر بیشمار ارسالی به سرور فرستاده نشوند.

**DNS Tunneling**

DNS tunneling یک تکنیک حمله است که از پروتکل DNS برای انتقال داده‌های رمزگذاری شده استفاده می‌کند. هکرها به طور مکرر از آن برای پراکنده کردن اطلاعات حساس سازمان‌های موردهدف استفاده می‌کنند. آنها همچنین می‌توانند از طریق DNS tunneling برای برقراری ارتباط و کنترل سرور از داخل شبکه مورد نظر استفاده کنند، سپس بدافزارهایی را در فایروال سازمان بارگیری کنند.

در حالی که این روش در ابتدا برای حمله به میزبان ایجاد نشده است و برای دور زدن کنترل‌های شبکه است، امروزه بیشتر از آن برای انجام حملات از راه دور استفاده می‌شود.

قبل از اینکه هکرها از تونل‌سازی DNS برای سرقت اطلاعات از شبکه یک سازمان استفاده کنند، ابتدا نیاز به دسترسی به شبکه سازمان دارند که این امر اغلب با فیشینگ یا شکل دیگری از بدافزارها حاصل می‌شود.

از آنجا که پروتکل DNS اغلب دقیق بررسی نمی‌شود، اجازه می‌دهد تا داده‌های رمزگذاری‌شده بدون شناسایی پخش شوند. تا زمانی که سازمان مورد هدف با دقت پروتکل DNS را بررسی نکند، هکر می‌تواند داده‌های حساس را به عنوان آنچه که به نظر می‌رسد فقط یک جستجوی DNS بی ضرر است از بین ببرد. در طول فرآیند، سرور DNS مهاجم پاسخ‌هایی را برای قانونی جلوه دادن درخواست‌ها ارسال می‌کند.

**DNS Poisoning**

DNS Poisoning معروف به کلاهبرداری DNS، یکی از رایج ترین حملات DNS است که هر روز اتفاق می‌افتد. مهاجمان با بهره‌برداری از آسیب‌پذیری‌های سیستم سعی می‌کنند داده‌های مخربی را به حافظه پنهان DNS سیستم بریزند. این یک روش حمله است که اغلب برای هدایت قربانیان به یک سرور دیگر استفاده می‌شود.

این نوع حمله بیشتر اوقات توسط سیستم‌های آسیب‌پذیر ایجاد می‌شود. باز کردن ایمیل‌های spam حاوی لینک‌های مخرب می‌تواند حافظه پنهان DNS را در معرض خطر قرار دهد و در نهایت به منظور سرقت اطلاعات شخصی یا آلوده کردن سیستم به جاسوس‌افزارها، تبلیغات مخرب ، ویروس ها و غیره، شما را به سمت وب‌سایت‌های مخرب هدایت می‌کند.

**روش‌های جلوگیری از حملات DNS**

از آنجایی که طیف گسترده‌ای از حملات DNS وجود دارد، برخی از آن‌ها از کنترل فرد یا سازمان خارج است. با این حال، هنوز راهکارهای زیادی وجود دارد که سازمان شما می‌تواند برای جلوگیری از حملات DNS انجام دهد:

**بازرسی DNS**: ممیزی و بازنگری DNS در کشف آسیب‌پذیری‌های مربوط به DNS به شما کمک می‌کند تا مشکلات مربوط به DNS های قدیمی و نرم‌افزارهای منسوخ شده را شناسایی کنید و از دسترسی مهاجمان به سرور سازمان جلوگیری کنید.

**استفاده از سرور اختصاصی DNS:** بسیاری از شرکت‌های کوچک ممکن است سرور DNS خود را در کنار سرورهای برنامه خود میزبانی کنند. این موضوع می‌تواند خطرات حملات برنامه‌های وب را افزایش دهد. به همین دلیل بهتر است سرویس‌های DNS را روی یک سرور جداگانه اجرا کنید.

**محدود کردن منطقه انتقال:** اگر محدوده انتقال DNS شما به دست یک مهاجم بیفتد، درک بهتری از ساختار شبکه شما را در اختیار او قرار خواهد داد. با رفتن به فایل پیکربندی نرم افزار DNS خود و محدود کردن منطقه انتقال به آدرس‌های خاص IP، می‌توانید از حملات منطقه‌ای مهاجمان جلوگیری کنید.

**به‌روزرسانی سرورهای DNS:** مجرمان اینترنتی به استفاده از آسیب‌پذیری‌های نرم‌افزارهای قدیمی علاقه‌مند هستند، بنابراین اجرای آپدیت در اسرع وقت ضروری است. آخرین نسخه نرم‌افزارهایی مانند Microsoft DNS و BIND از مشخصات امنیتی مانند DNSSEC پشتیبانی می‌کنند که اقدامات احراز هویت و یکپارچگی داده‌ها را ارائه می‌دهد.

**استفاده از سرویس کاهش DDoS:** اگر سرورهای DNS شما در یک حمله بزرگ DDoS هدف قرار گرفته باشند، این حملات می‌تواند سرویس‌های شما را غیرقابل دسترسی کنند و باعث اختلال در تجارت شما شوند.در نتیجه بهتر است از یک کاهش‌دهنده DNS مانند Cloudflare یا Akamai استفاده کنید که منابع آن می‌توانند به شما در حفظ آنلاین بودن سرورهای DNS کمک کنند.

همانطور که گفتیم، طیف گسترده‌ای از حملات DNS وجود دارد و مکانیزم دفاعی، زیرساخت، نرم‌افزارها و نیازهای هر سازمانی متفاوت است و در نتیجه ارائه راهکاری قطعی متناسب با هر شرایطی دشوار است.

نکته مهمی که باید درک شود این است که پروتکل DNS چگونه کار می‌کند و چگونه می‌توان از آن به روش‌های مختلف استفاده کرد. سازمان‌ها تنها در صورت درک خطرات پیش‌روی خود می‌توانند از سازمان محافظت کنند و در دفاع از خود رویکرد فعالی داشته باشند. در غیر این صورت ممکن است با عواقب جدی اخلال در تجارت، سرقت داده یا بدتر از آن مواجه شوند.