دانشکده علوم پزشکی و خدمات بهداشتی درمانی خلخال

موضوع:

امنیت در فضای سایبری

تهیه و تنظیم :

واحد IT بیمارستان

زمستان ۱۴۰۰


بسم الله الرحمن الرحیم

فضای سایبری

برای اولین بار توسط داستان نویسی به نام ویلیام گیبسون 1984 در یک داستان علمی-تخیلی و با عنوان بکار گرفته شد. در واقع به هر آنچه که مرتبط با شبکه های کامپیوتری و Cyber Space فضای سایبر اینترنت و فعالیت های کامپیوتری و مجازی باشد سایبر اطلاق می شود. بعلاوه برای معرفی گونه ی برخط، مجازی یا کامپیوتری هر چیزی نیز می تواند بکار رود. به دنیای کامپیوترها و جامعه ای که از آنها استفاده می نماید کلیه منابع اطلاعاتی موجود در شبکه های کامپیوتری و دارای فرهنگ خاصی مبتنی بر شبکه های ارتباطی الکترونیکی هستند، فضای سایبر یا دنیای مجازی گفته می شود.
فضای سایبر مجموعه ای از شبکه های ارتباطی کامپیوتری شامل وسایل ارتباطی، انتقالی، کنترلی و سیستمهای مدیریتی با یکسری اهداف ارزشمند برای پردازشها و زیرساختها میباشد. اینترنت بزرگترین مؤلفه از فضای سایبر میباشد.

ویژگی های فضای سایبر

۱.جهانی و فرامرزی بودن

از ویژگی‌های منحصر به فردی که فضای سایبر را از دیگر رسانه‌ها ممتاز می‌سازد، جهانی بودن آن است. هر فردی در هر نقطه از جهان می‌تواند از طریق آن به¬آسانی، به جدیدترین اطلاعات دست یابد.
مرزهای جغرافیایی تا کنون نتوانسته از گسترش روزافزون فضای سایبر جلوگیری کند. از این رو، هر نوع فیلتر و مرزبندی در برابر آن بسیار دشوار می‌نماید.

۲.دستیابی آسان به آخرین اطلاعات

چنانچه بخواهید به آخرین مقاله، کتاب و یا خبری که در زمینه تخصصی، در سطح جهان منتشر شده، دست یابید، ساده ترین و سریع ترین راه، استفاده از فضای سایبر است.

۳.جذابیت و تنوع

رسانه ها از فیلم، عکس، متن و یا هر هنر دیگری برای جذاب کردن خویش به کار می‌گیرند و این ابزارها در فضای سایبر قابل دستیابی است؛ به ویژه آن گاه که هیچ نظارت و فیلتری توان محدود کردنش را نداشته باشد. از ویژگی‌های منحصر به فردی که در تنوع و جذابیت فضای سایبر تأثیر بسزایی دارد، مشتری محوری محض است. در متون نوشتاری ارتباطی تنگاتنگ میان خوانندگان و نویسندگان وجود دارد که خواننده به راحتی می‌تواند نظر خود را با شخص نویسنده در میان بگذارد. از سوی دیگر، امکان نظر سنجی و ارزیابی در این فضا بسیار آسان تر و روزآمد تر است و این توانایی را به داده پردازان، فروشندگان و عرضه کنندگان محصولات اینترنتی می‌دهد که از آخرین خواسته‌های مشتریان و مخاطبان خود مطلع گردند.

حمله سایبری چیست و چرا انجام می‌شود؟

این نوع حملات توسط مجرمان سایبری و با استفاده از یک یا چند کامپیوتر انجام می‌شوند. هدف این حملات ممکن است یک دستگاه یا حتی چند دستگاه از یک مجموعه باشد. حملات سایبری ماهیت پلیدی دارند **و** می‌توانند یک کامپیوتر را کاملاً از کار بیندازند .همچنین از دیگر اهداف این حملات می‌توان به **سرقت** اطلاعات **و** زمینه‌سازی برای یک حمله بزرگ‌تر اشاره کرد .اگر برایتان سوال است که خوب چرا چنین حملاتی توسط هکرها انجام می‌شود، این سوال را پاسخ دهید: چرا دزدها دزدی می‌کنند؟! نیاز مالی، مشکل روانی، ذات پلید و . . . . هکرها هم به دلایل مختلفی دست به چنین کارهای خرابکارانه‌ای می‌زنند و هرروزه تعداد این حملات بیشتر از روز قبل می‌شوند.

انواع حملات از دیدگاه کلی

حملاتی که منابع یه شبکه رخ میده از دیدگاه کلی به دو بخش حملات فعال و حملات غیر فعال تقسیم میشن.

حملات فعال Active Attack

به حملاتی که از همون لحظه اول شروع حمله علائم اشکاری از خودشون بروز میدن و کشف اونها امکان پذیره حملات فعال گفته میشه .به عنوان مثال حمله نوع وقفه با از کار انداختن شبکه خودشو نشون میده و در دسته حملات اکتیو دسته بندی میشه

حملات غیر فعال Passive Attack

حملات غیر فعال هیچ علامت اشکاری در شبکه از خودشون نشون نمیدن و ممکنه برای ساعتها و هفته ها مخفی بمونن .حمله استراق سمع از این دسته از حملات محسوب میشه. حملات غیر فعال بسیار خطرناک و موجب آسیب بسیار زیاد به موجودیت های شبکه میشن.

مثلث امنیت یا CIA چیست؟

سازمانهای امروزی برای محافظت از اطلاعات و سیستمهای اطلاعاتی از دسترسی های غیر مجاز و جلوگیری از ایجاد تغییر، از بین رفتن یا دزدی داده ها بجز در مواردی که از سوی سازمان مجوز صادر شود اهمیت دارد. این کار را در یک کلام میتوان امنیت اطلاعات معنی کرد.
کامپیوترها می توانند قربانی عملیات های نهان باشند که متخصصین امنیت برای دفاع در برابر بدترین آنها، ۳ مفهوم اساسی امنیت اطلاعات را مطرح کرده اند.

- محرمانگی Confidentiality

- یکپارچگی Integrity
- در دسترس بودنAvailability

این ۳ مفهوم تحت عنوان CIA شناخته می شوند که در شکل زیر مشخص شده است:

برای بکارگیری مفاهیم محرمانگی، یکپارچگی و در دسترس بودن داده شما، سخت افزار، نرم افزار و ارتباطات سازمان می تواند ایمن شود.

مفهوم محرمانگی

جلوگیری از افشاء اطلاعات برای افراد غیرمجاز. به طور عموم این موضوع بر امنیت اجتماعی یا شناسایی خاصی دلالت دارد، اطلاعات مجوز درایور، حساب های بانکی و کلمات عبور و غیره از آن جمله است. برای سازمان ها می تواند شامل اطلاعات قبلی باشد اما در واقع نشان دهنده محرمانگی داده ها می باشد. برای ایجاد داده های محرمانه، سازمان باید سخت کار کند تا مطمئن شود که داده ها می توانند تنها توسط افراد مجاز دسترسی یابند.

مفهوم Integrity یکپارچگی

یکپارچگی بدین معناست که داده ها دستکاری نشده اند. اعتبار بخش پیش از تغییر داده ها در هر روشی که به صورت یکپارچه نگهداری کند لازم و ضروری می باشد. به عنوان مثال، اگر شخصی بخواهد فایل های مورد نیاز را حذف کند، حتی از روی عمد یا سهو، یکپارچگی آن فایل به خطر می افتد.

مفهوم در دسترس بود

در دسترس بودن بدین معناست که داده ها به منظور ذخیره سازی، پذیرش یا محافظت در دسترس باشند. این همچنین به این معناست که داده ها در برابر حملات ویروس ها نیز در دسترس هستند.
این ۳مفهوم باید همراه با امنیت سخت افزار، نرم افزار یا ارتباطات تأمین شوند. اصطلاح رایج دیگر AAA امنیت کامپیوتر می باشد. یعنی:

- (Authentication)تأیید هویت
- (Authorization)اختیار
- (Accounting)حساب کاربری

تأیید هویت (Authentication) : هنگامی که هویت شخص اثبات و توسط سیستم تأیید می شود. عموماً، این نیازمند یک شناسایی دیجیتالی برخی ترتیب ها، نام کاربری/کلمه عبور، یا سایر مفاهیم هویت سنجیمی باشد.

اختیار (Authorization) :هنگامی که یک کاربر به داده های معینی یا نواحی ساختمان قابل دسترس است اختیار پس از تأیید هویت اتفاق می افتد و می تواند به روش های متعددی شامل مجوزها، لیست های کنترل دسترس، زمان، روز و سایر محدودیت های لاگین و فیزیکی تعیین شود.

حساب کاربری (Accounting) :برای ردیابی داده ها، استفاده از کامپیوتر و منابع شبکه می باشد. اغلب به معنای لاگین کردن، حسابرسی و مانیتور کردن داده ها و منابع است، دارای حساب کاربری کردن امروزه به سرعت به یکی از مهمترین مفاهیم امنیت شبکه تبدیل شده است.

تعریف مهندسی اجتماعی

مهندسی اجتماعی چیست؟ شاید اگر این سوال از علاقمندان به مبحث امنیت پرسیده شود، هر بار و از هر شخصی جوابهایی متفاوت و شاید غیرمرتبط شنیده شود .کریستوفر هدنگی در کتاب « مهندسی اجتماعی؛ هنر هک کردن انسان »اورده است: مهندسی اجتماعی عمل دستکاری و اداره یک شخص است تا عملی انجام شود .ممکن است عمل انجام شده مورد علاقه شخص اداره شده باشد یا نباشد .هدف از اداره کردن نیز ممکن است بهدست آوردن اطلاعات، دسترسی پیدا کردن به اختیارات شخص یا انجام کاری توسط شخص اداره شده باشد.

تعریفهای دیگری نیز برای مهندسی اجتماعی ارائه شده است .چند مورد از تعریف های جالب در ادامه آورده شده است: مهندسی اجتماعی مهارتی است که به وسیله شخصی مجهول برای به دست آوردن اعتماد افراد درون سازمان و تشویق آنها برای ایجاد تغییرات دلخواه در سیستمهای کامپیوتری ودر جهت دستیابی به حق دسترسی، استفاده میشود. مهندسی اجتماعی انسانها را با روشهای مختلف فریب داده و با متقاعد نمودنشان از آنها برای دستیابی به اطلاعات، سوء استفاده میکند.

مهندسی اجتماعی سواستفاده زیرکانه از تمایل طبیعی انسانها به اعتماد کردن است . با اعتمادی که مهندسی اجتماعی به دست می آورد به همراه مجموع هایی از تکنیک ها، فرد را برای فاش کردن اطلاعات یا انجام کارهایی خاص متقاعد می نماید.

مهندسی اجتماعی مشتق شده از دو کلمه «مهندسی »و «اجتماعی »است . مهندسی آمیزهایی از سعی و خطاهای آزموده شده ومبتنی بر مستندسازی است؛ که بر مبنای آن میتوان شرایط جدید را با دقت قابل قبولی پیشبینی نمود و قبل از انجام آزمایش جدید، بر اساس تحلیل نتایج را مشخص نمود .اجتماعی به

زندگی روزمره ی مردم اشاره دارد که شامل زندگی حرفهایی و شخصی است .رفتارهای انسان نیز در قالب اجتماع قابل تعریف است

انواع مختلف حملات سایبری

همان طور که جرم و جنایت در دنیای واقعی انواع مختلفی اعم از کیف‌قاپی، جیب‌بری، زورگیری و ... دارد، حملات سایبری هم انواع بسیار گوناگونی دارند. در ادامه مدل‌های مختلف این کار ناشایست را بررسی می‌کنیم.

حملات فیشینگ(Phishing)

اگر بخواهیم هوش و ذکاوت هکرها را نادیده بگیریم، فقط خودمان را گول زده‌ایم .**فیشینگ** یکی از رایج‌ترین انواع حملات سایبری است که دولت کشور ما هم تلاش زیادی برای مقابله با آن کرده است. مثل اجرای طرح رمز پویا اجازه دهید این روش را با یک مثال برایتان توضیح دهم.

فرض کنید می‌خواهید از یک فروشگاه اینترنتی خرید داشته باشید و پس از انتخاب محصول به درگاه بانکی هدایت می‌شوید. این درگا ممکن است ساخته دست هکر باشد؛ یعنی شما به یک آدرس جعلی هدایت می‌شوید که ظاهرش کاملاً شبیه به سایت بانک مربوطه است.

سپس با خیال اینکه پس از پرداخت پول جنس‌تان آماده ارسال می‌شود، اطلاعات حساب بانکی‌تان را وارد می‌کنید؛ غافل از اینکه پولتان قرار است به جیب آدم بدهای داستان برود .فیشینگ به این صورت انجام می‌شود.

این نوع حملات به دو صورت انجام می‌شوند Spear Phishing Attacks .به‌معنای حملات **فیشینگ نیزه‌ای** و Whale Phishing Attacks به‌معنای حملات **فیشینگ وال** !تفاوت اصلی این دو نوع حمله میزان بزرگی آن‌ها است. همان طور که از نام‌ها مشخص است، نوع دوم لقمه‌های بزرگ‌تری برمی‌دارد.

اگر بخواهیم این نوع حملات را به‌زبان ساده بیان کنیم، باید بگوییم هکر در بین مسیر ارتباط دو نفر قرار می‌گیرد و اطلاعاتی که ردوبدل می‌کنند را به‌شکل ناشناس و بدون اینکه طرفین بفهمند سرقت می‌کند. در واقع هکر مثل یک واسطه در تمام درخواست هایی که از سمت کاربر به سرور ارسال می گردد، دخالت و جاسوسی می کند

حمله به‌کمک بدافزارها(Malwares)

بدافزارها کدهایی هستند که به‌صورت مخفیانه توسط هکر در سیستم‌های شخصی و ارگانی مخفی می‌شوند تا بتوانند او را به هدفش برسانند. بدافزارها انواع مختلفی دارند که از میان آن‌ها می‌توان به بدافزارهای جاسوسی و باج‌افزارها اشاره کرد.

هرساله تعداد زیادی از کسب‌وکارهای مطرح و مجرمان سایبری درگیر چنین حملاتی هستند و تعداد پرونده‌های این‌چنینی همیشه در حال افزایش است.

بدافزارها می‌توانند تا مدت خیلی زیادی **مخفی** باقی بمانند و به فعالیت‌های خرابکارانه‌شان ادامه دهند. تاثیرات مخرب آن‌ها می‌تواند ایجاد تغییرات و صدمه رساندن به انواع مختلف کامپیوترها باشد. این کدهای سمی می‌توانند یک شبکه را به‌طور کل مختل کنند و عملکرد یک ماشین را به صفر برسانند! معروف‌ترین نوع این حملات **تروجان** هستند.

ویروس‌ها

ویروس نوعی بدافزار است که با جای دادن یک کپی از خود در برنامه ای دیگر به آن پیوند می خورد و خودش را عضوی از آن برنامه می سازد. این بدافزار از رایانه ای به رایانه دیگر گسترش می یابد و آلودگی هایش را منتشر می کند. اثرات ویروس ها از عوارض آزار دهنده خفیف تا تخریبِ داده ها و یا تخریب خود نرم افزارها باهم متفاوت اند و حتی برخی از آنها می توانند موجب غیرفعال سازی و عدم سرویس دهی شوند. تقریباً همه ی ویروسها متکی به یک فایل اجرایی می‌باشند، از این رو اگر بر روی سیستمی ویروس وجود داشته باشد تنها زمانی فعال خواهد شد که کاربر، میزبان مخرب آن را باز یا اجرا کرده باشد. همزمان با اجرا شدن کد میزبان، کد ویروس نیز به همراه آن اجرا خواهد شد. معمولاً برنامه ی میزبان پس از آلوده شدن با ویروس نیز همچنان عملکردی طبیعی دارد اما در مواقعی ویروس طوری طراحی شده است تا با تکثیر و کپی کردن مکرر از خودش بر روی برنامه ی میزبان آن را کاملاً از میان بردارد و برنامه ی میزبان را به طور کل نابود سازد. ویروس ها می‌توانند به همراه یک سند یا نرم افزاری که به آن ضمیمه شده اند در حین ارسال از رایانه ای به رایانه ی دیگر توسط انواع حافظه های همراه، دیسک ها، استفاده کردن از شبکه، اشتراک گذاری فایل یا ضمیمه شدن به یک ایمیل گسترش یابند.

کرم کامپیوتری

کرم ها نیز مانند ویروس ها نمونه های تخریبگری را از روی خودشان تکثیر می کنند و می توانند خسارت هایی مشابه ویروس ها را ایجاد کنند. اما برخلاف ویروس ها، کرم ها برای گسترش یافتن نیازمند همراه شدن با فایل های میزبان نیستند و نرم افزارهای مستقلی می باشند. کرم ها برای پراکنده شدن حتی از انسان هم کمک نمی گیرند. برای انتشار و اجرا شدن کرم ها از نوعی مهندسی اجتماعی و فریب دادن کاربران استفاده می شود. یک کرم ابتدا از قسمت آسیب پذیر موجود در یک سیستم نفوذ می کند و سپس

با سوء استفاده از مزیت جابجایی فایل یا جابجایی داده اقدام به گسترش خود می کند و به همین ترتیب کرم های تکثیر شده مهاجرت خود را به مکان های جدیدتر ادامه میدهند. کرم به برنامه ای گفته می شود که می تواند خود را باز تولید کند. این برنامه با استفاده از شبکه، کپی های خود را از گره ای به گره های دیگر آن می فرستد. برخلاف ویروس، کرم ها خود را به برنامه های دیگر نمی چسبانند. عموما کرم ها با اشغال پهنای باند به شبکه آسیب می رسانند، در حالی که ویروس ها اغلب باعث خرابی برنامه های موجود .در کامپیوتر آلوده و از دست رفتن اطلاعات موجود در آن می شوند

تروجان ها

تروجان نیز یک بدافزار آسیب رسان می باشد که نام اش را از اسب چوبی بزرگی به نام اسب تروجان گرفته است. گفته می شود سربازان یونانی برای نفوذ به تروا درون اسب چوبی عظیمی پنهان می شوند و آن را در ساحل رها می کنند. مردمِ تروا با مشاهده ی اسب عظیم چوبی آن را نشانه ی پیروزی در جنگ و هدیه ای از طرف یونانی ها می پندارند و سرانجام غافل از اینکه جنگجویان یونانی در آن پنهان شده اند اسب چوبی عظیم را با خود به داخل شهرشان حمل می کنند. به زبانی عامیانه تروجان یک برنامه نرم ا دهد. کاربران نیز معمولاً فریب می خورند و تروجان را بر روی سیستم شان بار کرده یا اجرا می کنند. تروجان به محض فعال شدن قادر است تعداد زیادی از حملات را انجام دهد. این بد افزار با آزار کاربر همچون ظاهر کردن بی دلیل پنجره ها و تغییر دادن میز کار یا همان دسکتاپ همچنین تخریبِ میزبانِ خود مثل حذف کردن فایل ها، سرقت داده ها یا فعال کردن و تکثیر بدافزارهای دیگر اختلال ایجاد میکند، البته تروجان ها به عنوان ایجاد کننده گان درب مخفی نیز شناخته می شوند و از این طریق دستیابی نفوذگران بد اندیش را به سیستم فراهم می سازند. برخلاف ویروس ها و کرم ها، تروجان با تکثیر کردن خودش و همچنین با سرایت کردن به فایل ها گسترده نمی شود و مجبور است از راه تعامل با کاربران گسترش یابد که برای مثال هنگام بازکردن ضمیمه ی یک ایمیل به ظاهر عادی و یا پس از دانلود کردن و راه اندازی یک فایل از اینترنت این بد افزار شروع به کار میکند

حملات با استفاده از باج‌افزارها(Ransomware)

در این روش هکر با قرار دادن باج‌افزار روی دستگاه قربانی او را تهدید می‌کند که اگر خواسته‌اش را که معمولاً پرداخت پول است برآورده نکند، اطلاعات ارزشمندش را پاک می‌کند. البته هیچ تضمینی هم وجود ندارد که با پرداخت باج سبیل هکر به قولش وفادار بماند .اعتماد کردن به دزد جماعت کار راحتی نیست!

حملات استراق سمع(Eavesdropping Attacks)

این نوع حملات با رهگیری ترافیک ردوبدل شده در اینترنت انجام می‌شود و هدف آن سرقت اطلاعاتی است که تلفن‌های هوشمند یا کامپیوترها ارسال و دریافت می‌کنند. هدف ایدئال هکرها برای طرح‌ریزی این نوع حملات شبکه‌های ضعیف هستند که انتقال اطلاعات بین کاربر و سرور به‌سختی انجام می‌شود و فرصت

مناسب را برای نفوذ آن‌ها فراهم می‌کند. یکی از راه‌های پیشگیری از حملات استراق سمع آگاهی از دستگاه‌هایی است که به یک شبکه متصل هستند. می‌دانید چه دستگاه‌هایی به **وای‌فای** شما متصل هستند؟

سرقت کوکی‌ها(Cookie Stealing)

کوکی‌ها تقریبا در تمام وب‌سایت‌های اینترنت مورد استفاده قرار می گیرند. شاید با مفهوم کوکی آشنا نباشید.

کوکی چیست و چرا همه وب سایت ها از آن استفاده می کنند؟ وب‌سایت‌ها از کوکی برای شناسایی، به خاطر نگه داشتن و اعطای مجوزهای مناسب به یک کاربر خاص در بین میلیون‌ها کاربری که روی وب‌سایت هستند استفاده می‌کنند.
در روش**Cookie Stealing** ، هکر به کوکی‌ها روی کامپیوتر شما دسترسی پیدا می‌کند و آن‌هارا به مرورگر خودش ارسال می‌فرستد. به همین سادگی اطلاعاتی که کاربر قبول کرده در اختیار سایت شما قرار دهد، در اختیار افرادی قرار می‌گیرد که مجاز به داشتن آن نیستند.

تهدیدات داخلی(Insider Threats)

همیشه قرار نیست خراب‌کاری از بیرون انجام شود. گاهی ممکن است یکی از اعضای داخل مجموعه بنا به دلایل مختلف در سیستم اختلال ایجاد کند. اتفاقاً این نوع تهدیدات می‌توانند از انواع خارجی خطرناک‌تر باشند.

فردی که درون یک مجموعه قرار دارد به‌شکل قانونی مجوز بسیاری از دسترسی‌ها را دارد و همین موضوع کار را برای او راحت‌تر می‌کند. همچنین داشتن شناخت کامل از مجموعه و ساختارها دست او را برای انجام اقدامات خراب‌کارانه بازتر هم می‌کند. درضمن از آنجایی که تیم‌های امنیتی بیشتر بر عوامل خارجی تمرکز دارند، احتمال اینکه به او مشکوک شوند، بسیار کم است.

طرز اجرای حمله DoS چگونه است؟

تمرکز اصلی حمله DoS روی اشغال کردن کامل ظرفیت دستگاه هدف و در نتیجه انکار قابلیت سرویس‌دهی به درخواست‌های اضافی است. چندین بردار مختلف حمله در عملیات DoS را می‌توان بر اساس مشابهت‌هایشان گروه‌بندی کرد. حملات DoS عموماً در دو دسته طبقه‌بندی می‌شوند: حمله‌های سرریز بافر و حمله‌های سیل‌آسا.

حملات سرریز بافر(Buffer Overflow)

در این نوع از حمله یک سرریز بافر حافظه موجب می‌شود که دستگاه همه فضای هارددیسک، حافظه یا زمان پردازنده را مورد استفاده قرار دهد. این نوع از اکسپلویت غالباً منجر به بروز رفتار کند شدن سرور، کرش کردن سیستم و یا دیگر رفتارهای ناهنجار در سرور می‌شود که در نهایت انکار سرویس را موجب می‌گردد.

حمله‌های سیل‌آسا

در این روش یک مهاجم خرابکار با اشباع کردن سرور هدف‌گیری شده با تعداد زیادی بسته‌های داده، می‌تواند ظرفیت سرور را اشغال کند که در نهایت منجر به بروز وضعیت انکار سرویس می‌شود. برای این که اغلب حمله‌های DoS موفق باشند، مهاجم خرابکار باید پهنای باند بیشتری نسبت به هدف خود داشته باشد.

انواع حملات DoS کدام هستند؟

از نظر تاریخی، حمله‌های DoS به طور معمول از آسیب‌پذیری‌های **امنیتی** موجود در طراحی شبکه، نرم‌افزار و سخت‌افزار سوءاستفاده کرده‌اند. این حمله‌ها امروزه شیوع کمتری یافته‌اند، زیرا حمله‌های DDoS ظرفیت مخرب بیشتری دارند و با توجه به ابزارهای موجود، اجرایشان آسان‌تر است. در واقعیت، اغلب حمله‌های DoS می‌توانند به حمله‌های DDoS تبدیل شوند. برخی از نمونه‌های تاریخی برجسته حمله‌های DoS شامل موارد فهرست زیر هستند:

حمله Smurf

در این حمله قدیمی DoS یک مهاجم خرابکار ازنشانی برادکست شبکه دارای آسیب به واسطه ارسال پاکت‌های جعل شده سوءاستفاده می‌کرد تا نشانی IP مقصد را غرق کند.

Ping flood

این حمله انکار سرویس ساده بر مبنای اشغال کردن هدف با بسته‌های پینگ ICMP اجرا می‌شود. به این ترتیب با حمله کردن به یک سرور با تعداد پینگ زیاد که پردازش آن در توان سرور نیست، امکان پاسخ‌دهی مؤثر از آن سلب می‌شود و وضعیت انکار سرویس رخ می‌دهد. این حمله نیز می‌تواند به صورت DDoS اجرا شود.

چطور می‌توان گفت رایانه‌ای تحت حمله DoS است؟

با این که جداسازی یک حمله از دیگر خطاهای اتصال‌پذیری شبکه یا مصرف بالای پهنای باند کار آسانی نیست، اما برخی نشانه‌ها وجود دارند که توجه کردن به آن‌ها می‌تواند نشان دهد که سیستم تحت حمله قرار گرفته است. نشانه‌های حمله DoS شامل موارد زیر هستند:

- عملکرد کندی شبکه به طور نامعمول، مثلاً زمان زیاد بارگذاری فایل‌ها یا وب‌سایت.
- ناتوانی از بارگذاری یک وب‌سایت خاص مانند فایل‌های وب.
- فقدان ناگهانی اتصال‌پذیری برای دستگاه‌های روی شبکه واحد.

تفاوت بین حمله DoS و DDoS چیست؟

تمایز بین DDoS و DoS تعداد اتصال‌هایی است که در حمله مورد استفاده قرار می‌گیرد. برخی حمله‌های DDoSمانند حمله‌های کند و آرام از قبیل Slowloris توان خود را از سادگی و الزامات اندک مورد نیاز برای اثربخشی حمله می‌گیرند.

DoSاز یک اتصال منفرد استفاده می‌کند، در حالی که حمله DDoS از منابع زیادی از ترافیک حمله غالباً به شکل بات‌نت استفاده می‌کند. به طور کلی بسیاری از حمله‌ها به طور بنیادی مشابه هستند و می‌توانند با استفاده از یک یا چند منبع ترافیک خرابکارانه انجام شوند.

انواع حملاتDDoS

حمله‌های قطره اشک (Teardrop) یا تفکیکIP

در این نوع حمله، هکر یک بسته که به طور خاصی جعل شده به قربانی ارسال می‌کند. برای درک این نوع حمله، فرد باید درکی از پروتکل TCP/IP داشته باشد. برای ارسال داده‌ها روی شبکه، بسته‌های IP به بسته‌های کوچک‌تری تقسیم می‌شوند که این کار تفکیک آی‌پی (IP fragmentation) نامیده می‌شود.

هنگامی که بسته‌ها در نهایت به مقصدشان برسند، دوباره با همدیگر تجمیع می‌شوند تا داده‌های اصلی بازسازی شوند. در فرایند تفکیک، برخی فیلدها به بسته‌های تفکیکی اضافه می‌شوند تا بتوان در زمان تجمیع مجدد در مقصد، آن‌ها را شناسایی کرد. در حملهTeardrop ، مهاجم برخی بسته‌های جعلی می‌سازد که با یکدیگر همپوشانی دارند. در نتیجه سیستم عامل مقصد در مورد چگونگی تجمیع مجدد بسته‌ها دچار سردرگمی می‌شود و از کار می‌افتد.

حمله پینگ مرگ

در زمان مخابره داده‌ها روی اینترنت، داده‌ها به دسته‌های کوچکی از بسته‌های داده‌ای تقسیم می‌شوند. دریافت و بازسازی این بسته‌های خرد شده در کنار هم موجب می‌شود که بتوان پیام را بازسازی کرد. در حمله پینگ مرگ (Ping of death) مهاجم یک بسته بزرگ‌تر از ۶۵،۵۳۶ بایت ارسال می‌کند که بیشینه اندازه مجاز برای بسته‌های پروتکل IP است. بسته‌ها افراز شده و روی اینترنت ارسال می‌شوند. اما زمانی که بسته‌ها در زمان دریافت در مقصد کنار یکدیگر قرار می‌گیرند، سیستم عامل نمی‌تواند این بسته‌های بزرگ‌تر را مدیریت کند و از این رو کرش می‌کند.

اکسپلویت‌ها

اکسپلویت (Exploit) کردن سرورها نیز می‌تواند منجر به آسیب‌پذیری DDoS شود. بسیاری از وب‌اپلیکیشن‌ها روی وب‌سرورهایی مانند آپاچی و تامکت میزبانی می‌شوند. اگر یک آسیب‌پذیری در این وب‌سرورها وجود داشته باشد، مهاجم می‌تواند یک اکسپلویت را برای بهره‌برداری از این آسیب‌پذیری اجرا نماید. اکسپلویت لزوماً نباید کنترل را به دست بگیرد، بلکه همین مقدار که موجب از کار افتادن وب‌سرور

شود کفایت می‌کند. این وضعیت منجر به حمله انکار سرویس می‌شود. در صورتی که وب‌سرورها از پیکربندی پیش‌فرض استفاده کنند، هکرها با روش‌های آسانی می‌توانند وب‌سرور و نوع نسخه آن را شناسایی کنند. مهاجم آسیب‌پذیری‌ها و اکسپلویت‌های این نوع وب‌سرور را پیدا می‌کند و در صورتی که وب‌سرور پچ نشده باشد، می‌تواند با ارسال یک اکسپلویت آن را از کار بیندازد.

سامانه تشخیص نفوذ IDS و جلوگیری از نفوذ IPS

سامانه تشخیص نفوذ (Intrusion Detection System – IDS) با زیرنظر گرفتن ترافیک عبوری از شبکه، در صورت مشاهده هر نوع عملکرد مشکوک به نفوذ، آن را گزارش می‌کند. دقیقا مانند یک نگهبان در یک سازمان که با مشاهده تردد افراد و فعالیت هایی که انجام می دهند، رفتارهای مشکوک را گزارش می کند تا سازمان در صورت لزوم مانع آن رفتار مجرمانه بشود. اگر به مرور زمان متوجه وجود نقاط آسیب‌پذیر برای نفوذ در سامانه‌های نرم‌افزاری شویم، تا زمان رفع این مشکل نیاز داریم تا با استفاده از سامانه‌های جلوگیری از نفوذ (Intrusion Prevention System – IPS) مانع سوءاستفاده از آن ضعف امنیتی بشویم. البته سامانه‌های جلوگیری از نفوذ طبعاً باید امکان تشخیص نفوذ را داشته باشند؛ به همین دلیل گاهی به آن‌ها سامانه‌های تشخیص و جلوگیری از نفوذ (Intrusion Detection and Prevention System – IDPS)نیز گفته می‌شود. به دلیل وجود طیف گسترده ای از سامانه‌های نرم افزاری، ظهور حملات جدید، وجود پیکربندی‌های ناامن، عدم استفاده از یک سامانه تشخیص و جلوگیری از نفوذ و به‌روزرسانی امنیتی دیرهنگام در سامانه‌هایIT ، تا زمان رفع مشکلات امنیتی، به افرادی که درحال رصد و بهره‌برداری از آسیب‌پذیری شبکه‌های کامپیوتری هستند، فرصت کافی برای سوءاستفاده می‌دهد.