انواع حملات در فضای سایبر

فهرست

بطور کلی حمله علیه یک سامانه، به هر عمل با سوء نیت و بدخواهی علیه یک یا مجموعه‌ای از سامانه‌ها اطلاق می‌شود. در این تعریف دو مفهوم بسیار مهم و قابل توجه وجود دارد. اولاً عمل حتماً با سوء نیت حتی بدون تعیین هدف یا مقصود مشخصی انجام می‌شود. ثانیاً حملات بر روی یک سامانه خاص انجام می شوند در حالیکه سایر سامانه‌ها هدف یا قربانی حملات نیستند.

در این کتابچه ضمن تشریح مفاهیم هدف، فعالیت، اتفاق، پیامد و تأثیر حملات سعی شده است به بررسی حملات سایبری در سطوح مختلف معماری و طراحی، پیاده‌سازی و بهره‌برداری و همچنین عوامل مقابل امنیت پرداخته شود و در انتها تأثیر حملات در فضای تبادل اطلاعات بر افراد، سازمان‌ها و جامعه مورد بررسی قرار گیرد.

آغاز

حملات فضای تبادل اطلاعات چیست؟

بطور کلی حمله علیه یک سامانه، به هر عمل با سوء نیت و بدخواهی علیه یک یا مجموعه‌ای از سامانه ها اطلاق می شود. در این تعریف دو مفهوم بسیار مهم و قابل توجه وجود دارد. اول اینکه عمل حتماً با سوء نیت حتی بدون تعیین هدف یا مقصود مشخصی انجام می شود. دوم، حملات بر روی یک سامانه خاص انجام می‌شوند در حالیکه سایر سامانه‌ها هدف یا قربانی حملات نیستند.

در این قسمت به تشریح برخی از مفاهیم مرتبط می‌پردازیم.

- اهداف

تشخیص یک حمله و پی‌آمدهای آن بسیار مهم است. پیامدهای یک حمله بیشتر از فعالیت های خاص حمله، به نقش سامانه آسیب دیده بستگی دارد. ممکن است نیل به یک یا چند هدف، نیازمند دستیابی به هدف‌های جزئی‌تر از قبیل دست یافتن به مجوزهای دسترسی به سامانه باشد.

- فعالیت‌ها

فعالیت‌ها در واقع اقداماتی هستند که به مهاجم کمک می کنند تا به یک یا چند هدف جزئی دست یابد. این فعالیت‌ها می‌توانند شامل استفاده از مجوزهای ورود دزدیده شده (مثل نام کاربری و رمزعبور)، طغیان در یک شبکه با بسته های ناهنجار و غیره باشند.

- اتفاق‌ها

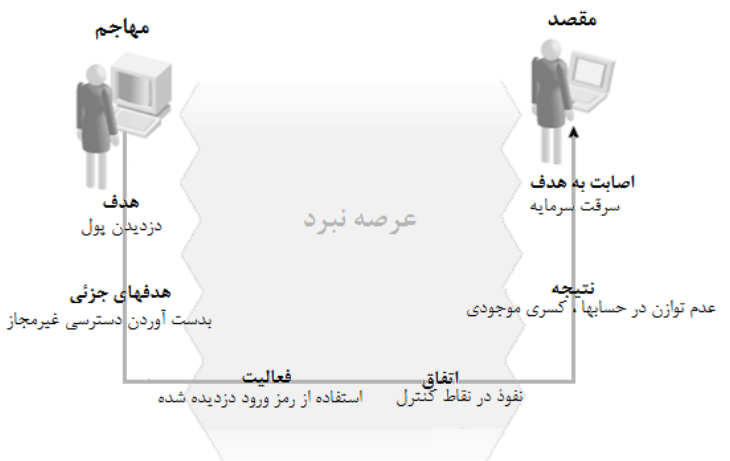
فعالیت‌های ذکر شده در بالا ممکن است منجر به اتفاق افتادن یک حمله شود. به عنوان مثال دسترسی نادرست امکان‌پذیر شده، پردازش تقاضاها معلق شده، فضای ذخیره اطلاعات خالی شده یا یک سامانه یا برنامه متوقف شود.

- پیامدها

یکی دیگر از مفاهیمی که اغلب با اتفاق یک حمله اشتباه گرفته می شود، پیامدهای حمله است. منظور از این واژه تأثیرهای مستقیم اتفاق‌ها، از قبیل ارائه ترازنامه مالی نادرست یا عدم امکان دسترسی به برنامه‌های رایانه‌ای برای یک فرآیند تجاری خاص می‌باشد.

- تأثیرات

در نهایت تأثیر حملات می‌تواند شامل مواردی از قبیل خدشه‌دارکردن اعتبار یک سازمان و فرصت‌ها و منافع از دست‌رفته باشد.



شکل ۱: فعالیت‌ها ، اتفاق‌ها ، اهداف و پیامدهای تجاری یک حمله

حملات و راه های دفاع در مقابل آن‌ها

چگونگی حمله مهاجمان به دلیل حملات بستگی دارد. برخی افراد به دنبال جستجو و کاوش بدون هیچ آسیبی هستند و برخی قصد دزدی داشته و بعضی نیز به دنبال آشفته کردن فضا هستند. افرادی هم در پی تخریب یا خودنمایی هستند. از آنجا که نمی توان تمام انگیزه ها راپیش بینی کرد، تلاش خواهیم کرد تا روش‌هایی را بررسی کنیم که یک فرد با ضریب هوش معمولی می تواند امنیت سامانه را به خطر بیاندازد. در زیر لیست تعدادی از انواع حملاتی که سامانه‌ها باید در برابر آن‌ها مقاوم باشند آورده شده است. با توجه به اینکه در کدام مرحله توسعه سامانه باشیم، آسیب پذیری‌ها در سه طبقه دسته‌بندی می‌شوند:

۱. حملات سطح معماری و طراحی

این مرحله زمانی است که در مورد سامانه، اجزا و طراحی آن فکر می‌شود. به عنوان یک قاعده عمومی، اصلاح و ترمیم آسیب هایی که ناشی از تصمیم‌های مرحله معماری و طراحی باشند سخت‌ترین نوع اصلاح است. این یک واقعیت است که اصول و قواعد مناسب و کافی برای دفاع برابر یک حمله نمی تواند مانع مسئولیت توسعه دهنده سامانه در زمینه فکر، برنامه ریزی و توجه به چگونگی حداقل رساندن چنین آسیب هایی باشد. برخی از حملات اصلی که در این مرحله مشاهده شده در زیر آورده شده است.

- حمله استراق سمع[۱]

این نوع حمله (استراق سمع) زمانی اتفاق می‌افتد که مهاجم در مسیر بین

[۱] Man-in-the-middle attack

دو هاست[1] در نقل و انتقالات شبکه قرار می‌گیرد و خود را در قالب یکی از افراد درگیر در انتقالات در شبکه جا میزند و ممکن است دستورات اضافی را وارد دستورات رد و بدل شده نماید.

روش مقابله: استفاده گسترده‌تر از پنهان‌سازی و کدکردن اطلاعات و همچنین استفاده از روش کنترل مجموع در نشست‌ها و رمزهای مشترک مثل کوکی‌ها.

- حمله وضعیت مسابقه[2]

معمولاً از دیدگاه رایانه ای، عملیات نرم افزارها شامل گام‌های مجزا هستند. بعنوان مثال مطمئن بودن دستورات موجود در یک فایل دسته‌ای، کنترل شده و در صورت اطمینان، دستور اجرای آن صادر می گردد. گاهی زمان مورد نیاز برای انجام این گام ها فضایی را برای مهاجمان باز می کند تا بتوانند امنیت را مورد هدف قرار دهند. در این مثال ممکن است شانس مختصری برای یک مهاجم بوجود آید تا یک فایل جدید حاوی کد مخرب را جایگزین فایلی که قبلا کنترل شده نماید. این جایگزینی می‌تواند برنامه را در راستای اجرای برنامه‌های موردنظر مهاجم، منحرف نماید. حتی اگر از دیدگاه انسان، زمان ایجاد شده برای انجام اعمال مخرب و سوءاستفاده خیلی کوتاه باشد، ولی یک برنامه می تواند مکررا آزمون نموده و در زمان مناسب بلافاصله برنامه مخرب را اجرا نماید. از آنجایی که غالباً نتیجه این حمله به ترتیب تکمیل دو یا چند پردازش موازی بستگی دارد، این مسئله با عنوان "وضعیت مسابقه" شناخته شده است.

---

[1] Host

[2] Race condition attack

روش مقابله: توجه به تفاوت بین عملیات اتمیک (غیرقابل تقسیم) و غیراتمیک و اجتناب از عملیات غیراتمیک بجز در مواردی که مطمئن باشیم که امنیت در معرض خطر نیست.

- حمله پاسخ[۱]

اگر مهاجم بتواند یک رکورد از تراکنش‌های داخلی بین برنامه‌های سامانه سرویس‌گیرنده و سرویس‌دهنده را در اختیار بگیرد، این احتمال وجود دارد که به قسمتی از محاورات با مقاصد خرابکارانه پاسخ دهد. جعل هویت سرویس‌گیرنده یا سرویس‌دهنده می‌تواند امنیت را بطور جدی تحت تاثیر قرار دهد.

روش مقابله: مشابه حملات استراق سمع، به علاوه ، توجه به معرفی در هر محاوره بین اجزای برنامه از طریق اعلام یک کد هویتی، بطوریکه در هر نشست کد هویت جدید ارائه شود.

- حمله شنود [۲]

اسنیفر به برنامه‌ای گفته می‌شود که تمام ارتباطات و روابط در یک شبکه محلی را به آرامی ضبط کند. اسنیفرها معمولاً ابزارهای تشخیص قانونی هستند که توسط مهاجمانی که می‌خواهند نام کاربری یا رمز عبور در یک شبکه را ضبط کنند مورد سوء استفاده قرار می‌گیرد.

روش مقابله: این نوع حمله بیشتر در سطح شبکه دیده می‌شود. جایی که تاثیر آن می تواند با پیکربندی دقیق و استفاده از روترهای شبکه

---

[۱] Replay attack

[۲] Sniffer attack

سوئیچ شده کاهش یابد (ولی حذف نمی‌شود). همچنین می‌توان با استفاده حداکثری و موثر از پنهان‌سازی اسنیفرها را بی‌خطر نمود.

- حمله دزدی نشست[۱]

با استفاده از ضعف موجود در پروتکل TCP/IP، یک مهاجم ممکن است قادر باشد تا کل اطلاعات یک شبکه را برباید یا یک اتصال برقرار شده را قطع کند. ابزارهای زیادی در سطح اینترنت برای پیاده‌سازی این نوع حمله نسبتاً ماهرانه و فنی پخش شده است.

روش مقابله: دفاع در برابر این حمله سطح شبکه، از طریق برنامه بسیار مشکل است ولی پنهان‌سازی علیرغم محدودیت‌هایی که دارد می تواند مؤثر باشد. همچنین برخی پردازش‌های عملیاتی می‌تواند به تشخیص یک دزدی نشست در شبکه بعد از اتفاق افتادن آن کمک کند. این درصورتی است که ورود به شبکه دقیق بوده و اطلاعات کافی در مورد نشست‌ها را ارائه دهد.

- حمله از بین بردن نشست[۲]

نشست‌های قانونی TCP/IP با ارسال یک بسته راه‌اندازی مجدد **TCP** از جانب یکی از طرفین خاتمه می یابد. یک مهاجم درون شبکه می تواند آدرس فرستنده بر روی چنین بسته‌ای را جعل کرده و اتصال را پیش از موعد قطع کند. همچنین می تواند اتصالات را به هم ریخته یا برای تخریب قسمتی از تراکنش‌ها تلاش نماید.

---

[۱] Session hijacking attack

[۲] Session killing attack

روش مقابله : مثل حملات دزدی نشست، باید اذعان داشت که ممانعت از این حملات از طریق برنامه امکان پذیر نیست ولی برنامه ها ممکن است قادر باشند بعد از انجام حمله با تثبیت اتصال یا راه اندازی مجدد تراکنش متوقف شده، مسئله را جبران نمایند.

۲. حملات سطح پیاده‌سازی

این حملات معمولاً در زمان تولید برنامه ها اتفاق می افتد. تشخیص و ترمیم حملات این سطح راحت‌تر از حملات سطح طراحی است. در زیر سه نمونه از حملات رایج این سطح آورده شده است.

- حمله سرریز بافر [۱]

بسیاری از زبان‌های برنامه‌نویسی این امکان را به برنامه نویسان می‌دهد تا فضای بافر با اندازه ثابت را برای رشته حروف دریافتی از کاربر در نظر بگیرند. وضعیت سرریز بافر زمانی اتفاق می‌افتدکه برنامه محدوده داده‌ها را کنترل نکرده و رشته حروف بیشتر از سایز درنظر گرفته شده برای بافر را دریافت کرده و منجر به سرریز بافر شود. در بسیاری از موارد یک مهاجم باهوش می‌تواند باعث شود تا بافر از طریق اجرای دستورات غیرمجاز سرریز شود.

روش مقابله : نوشتن کدها به زبان‌هایی که مانع سرریز بافر می‌شوند. همچنین اجتناب از خواندن و ذخیره رشته های متنی با طول متغیر در بافرهای با طول ثابت

[۱] *Buffer overflow attack*

- حمله درپشتی[1]

آسیب بسیاری از برنامه‌ها در اثر حملاتی است که در زمان نوشتن نرم‌افزار انجام شده‌اند. ممکن است مواردی را شنیده باشید که برخی برنامه‌نویسان کدهای مخصوصی را در برنامه قرارمی‌دهند که اجازه دور زدن کنترل دسترسی را می‌دهد.

روش مقابله :بکارگیری پردازه‌های تضمین کیفیت که تمام کدها را از نظر وجود درپشتی کنترل می‌کند.

- حمله تحلیل خطا[2]

برنامه‌ها معمولاً ورودی‌ها را بدون کنترل دقیق از منظر محتوای مخرب، دریافت می‌نمایند. تحلیل و کنترل مطمئن بودن داده‌های ورودی برای محدودکردن حملات بسیار مهم است.

روش مقابله: بکارگیری کدهای موجود که بوسیله متخصصان مورد اعتماد نوشته شده و با دقت بررسی، ارزیابی و نگهداری شده است، توصیه می شود.

۳. حملات مرحله بهره برداری

این حملات معمولا در زمان استفاده از برنامه‌ها و بعد از انتشار برنامه اتفاق می‌افتد. این دسته حملات، می‌تواند ناشی از تصمیم های اتخاذ شده بعد از توسعه و در زمان بهره‌برداری از برنامه باشد.

- حمله نفی سرویس[3]

---

[1] *Back door attack*

[2] Parsing error attack

[3] Denial-of-service attack

یک برنامه کاربردی، یک فضای میزبان یا حتی یک شبکه می‌تواند از طریق تقاضای سرویس های آبشاری یا هجوم ورودی‌های با تناوب بالا، برای کاربران قانونی خود غیرقابل استفاده گردد. وقتی این اتفاق بیفتد گفته می‌شود مهاجمان برای کاربران مجاز، نفی سرویس انجام داده‌اند.

روش مقابله: برنامه ریزی و تخصیص منابع و طراحی برنامه بطوریکه برنامه تقاضای متعادلی را بر روی منابع سامانه از قبیل فضای حافظه یا تعداد فایل های باز شده داشته باشد. برنامه نباید در زمان اتمام منابع، تنها شاکی بوده و اجرای آن متوقف شود.

- حمله کاربری پیش فرض [۱]

بسیاری از سامانه‌های عامل و برنامه‌ها بصورت پیش فرض با نام کاربری و رمز استاندارد تنظیم می شوند که این موضوع ورود راحت مهاجمانی که این رمزها را می‌دانند یا حدس می‌زنند امکان‌پذیر می‌کند.

روش مقابله: حذف تمام کاربری های پیش فرض یا اطمینان از تغییر آن‌ها توسط مدیر سامانه و بانک اطلاعاتی. همچنین کنترل مجدد بعد از نصب برنامه جدید یا نسخه جدید برنامه موجود.

[۱] Default accounts attack

- حمله شکستن رمز عبور [1]

مهاجمان بطور مرتب رمز عبور های ضعیف را به کمک برنامه‌های ویژه شکستن رمز حدس می‌زنند. این برنامه‌ها با استفاده از الگوریتم های خاص و لغت نامه کلمات رایج، صدها یا هزاران رمز عبور را حدس می‌زنند. رمز عبورهای ضعیف مثل اسامی رایج، تاریخ تولد یا کلمات خاص به راحتی حدس زده می‌شوند.

روش مقابله: به عنوان یک کاربر، انتخاب رمز عبور هوشمندانه و به عنوان یک برنامه‌نویس استفاده از ابزارهای موجود برای ساخت رمزعبورهای قوی و همچنین استفاده از روش های شناسایی موجود مثل ابزارهای زیستی یا کارت های هوشمند.

- عوامل مقابل امنیت

سه دسته عوامل زیر در مقابل امنیت قرار دارند:

عوامل تکنیکی : مواردی از قبیل اثرات متقابل پیش بینی نشده اجزا سامانه که هر یک به تنهایی مخرب نیستند، ترکیب اجزاء مستقل که به تنهایی مخرب نباشند و پیچیدگی‌های بیش از حد برنامه امنیت را قربانی می‌کنند.

عوامل فیزیولوژیکی : مسائل مربوط به ارزیابی ریسک، مدل ذهنی و شیوه تفکر در مورد برنامه، معمولا طراحی و پیاده سازی برنامه امن را برای انسان سخت می‌کند.

---

[1] Password cracking attack

عوامل دنیای واقعی : رایج شدن برنامه نویسی توسط افراد تازه‌کار و ناآشنا به مسائل امنیتی، فشارهای تولید برنامه، عوامل اقتصادی و سایر عوامل اجتماعی که در برابر کیفیت امنیت قرار دارند.

تأثیر فردی حملات فضای تبادل اطلاعات

حملات سایبری می توانند شهروندان را نیز تحت فشار قرار دهند. آن ها نیز به اندازه سازمان های بزرگ از حملات مهاجمین سایبری و کدهای مخربی که از طریق اینترنت اجرا می‌شوند آسیب می‌بینند و ناگزیرند برای ترمیم خسارت ها و یا بازیابی سامانه های کامپیوتری آسیب دیده هزینه هایی را متحمل شوند. برخی تأثیرات بالقوه این حملات بر شهروندان به شرح زیر است.

۱. آسیب رسانی مستقیم بر سامانه‌های رایانه‌ای
۲. هزینه های مورد نیاز برای ترمیم و فعال‌سازی سامانه های رایانه‌ای آسیب‌دیده
۳. کاهش بهره‌وری
۴. ازدست دادن همکاری با کارفرما،خانواده،گروه های اجتماعی و انجمن ها
۵. کاهش مشارکت‌های اقتصادی در انجمن‌های محلی و منطقه‌ای
۶. کاهش مشارکت کوتاه مدت و بلند مدت در تجارت الکترونیکی

تأثیر سازمانی حملات فضای تبادل اطلاعات

تأثیر بالقوه حملات سایبری بر سازمان‌ها به شرح زیر است.

۱. آسیب رسانی مستقیم بر سامانه‌های رایانه ای

۲. هزینه های مورد نیاز برای ترمیم و فعال سازی سامانه های رایانه‌ای آسیب‌دیده
۳. کاهش بهره‌وری کارکنان
۴. تأخیر در انجام سفارش‌ها یا خدمات مشتریان
۵. کاهش بهره‌وری مشتریان سازمان به دلیل تأخیر ایجاد شده
۶. تأخیر در تجارت مشتریان سازمان به دلیل تأخیر ایجاد شده
۷. تأثیر منفی بر اقتصاد محلی و ملی در محل استقرار سازمان و مشتریان یا سرمایه‌گذاران
۸. تأثیر منفی بر ارزش سرمایه گذاری افراد و صندوق های حمایتی مالی

جمع آوری اطلاعات مربوط به تاثیرات یک حمله سایبری قطعا امکان پذیر است ولی هزینه و زحمت زیادی خواهد داشت. زمانی که یک حمله سایبری فقط یک سازمان را مورد هدف قرار دهد پیچیدگی جمع آوری اطلاعات به گستردگی تخریب و مدت زمان قطعی سامانه بستگی دارد.

"خسارت واقعی" به معنی صدمات پیش بینی شده مستند ناشی از حمله است. در بیشتر جرایم سایبری، خسارت واقعی شامل صدمات زیر می شود:

۱. هزینه‌های منطقی جهت تشخیص آسیب‌ها
۲. هزینه‌های بازیابی سامانه‌ها و اطلاعات به حالت قبل از حمله
۳. تمامی منافع از دست رفته در اثر قطع سرویس

تأثیر حملات فضای تبادل اطلاعات بر جامعه

حملات سایبری می توانند از منظر بازخوردهای اجتماعی نیز مورد بررسی قرار گیرند. حملاتی که سامانه رایانه‌ای را فلج می کنند منجر به مصرف منابعی

می‌شوند که می توانستد در جاهای مناسب تر و برای مقاصد بهتر مورد استفاده قرار گیرند. برخی از تاثیرات حملات کدهای مخرب بر افراد و سازمان‌ها که در جامعه انعکاس دارد به شرح ذیل است.

۱. اختلال در زیرساختارهای حیاتی از قبیل آب، بهداشت عمومی، سرویس های اضطراری، صنایع دفاعی، مخابرات و ارتباطات، پست، انرژی، حمل و نقل و ترابری، بانکداری، صنایع شیمیایی و مواد پرخطر
۲. اختلال در فعالیت‌های فردی و خانوادگی
۳. اختلال در مشارکت‌های علمی
۴. اختلال در فعالیت‌های گروه‌های اجتماعی و انجمن‌ها
۵. اختلال در تجارت‌های محلی، ملی و الکترونیکی
۶. اختلال در فعالیت‌ها و عملیات دولتی