تیم قرمز حرفه‌ای

انجام تعاملات امنیت سایبری موفقیت‌آمیز

فصل دوم: چرا هکرهای انسانی؟

مهدی لقایی
سهیل هاشمی

۲

فصل دوم: چرا هکرهای انسانی؟

چرا باید از هکرهای انسانی استفاده کنیم؟ در فصل قبل با مزایای استفاده از تیم قرمز آشنا شدید اما در آن فصل دلیل قانع کننده‌ای برای استفاده از هکرهای انسانی مطرح نشد. همانطور که اشاره شد، مانور تیم قرمز یک فرایند چالش برانگیز و اغلب پرهزینه است. بخش صنعت و دانشگاه هر دو تلاش کرده‌اند که با استفاده از فناوری‌ها و ابزارهای مختلف، کار هکرهای انسانی را اتوماسیون یا جایگزین کنند. همچنین خدمات جدیدی با الزاماتی متفاوت از نظر انتخاب و به کارگیری پرسنل وجود دارند که به دنبال جایگزین کردن خدمات تیم قرمز هستند. پس از خواندن این فصل نباید تردیدی درباره برتری هکرهای انسانی نسبت به راهکارهای اتوماسیون برای تیم قرمز داشته باشید و اینکه پیدا کردن و استفاده از انواع پرسنل امنیتی، نمی‌تواند جایگزین خدمات تیم قرمز باشد.

ابتکار و اتوماسیون

انگیزه ایجاد نوآوری در فرایندهای کاری تیم قرمز بدون استفاده از هکرهای انسانی چندین دلیل دارد. این گرایشات با هدف تسریع ارزیابی، دسترسی آسان‌تر به ارزیابی‌ها یا جایگزینی تیم قرمز با خدماتی که پیاده‌سازی آنها راحت‌تر است، شکل گرفته‌اند. به نظر من هیچ یک از این روش‌ها قابلیت جایگزینی کارکنان حرفه‌ای تیم قرمز را به صورت امن یا واقع گرایانه ندارند. در ادامه مطلب تحلیلی از پیشنهادات صنعتی و دانشگاهی را برای جایگزین کردن هکرهای اخلاقی بررسی می‌کنیم. درک چنین راهکارهایی نشان می‌دهد که چرا وجود هکرهای اخلاقی اهمیت زیادی دارد و قرار نیست جایگزین شوند.

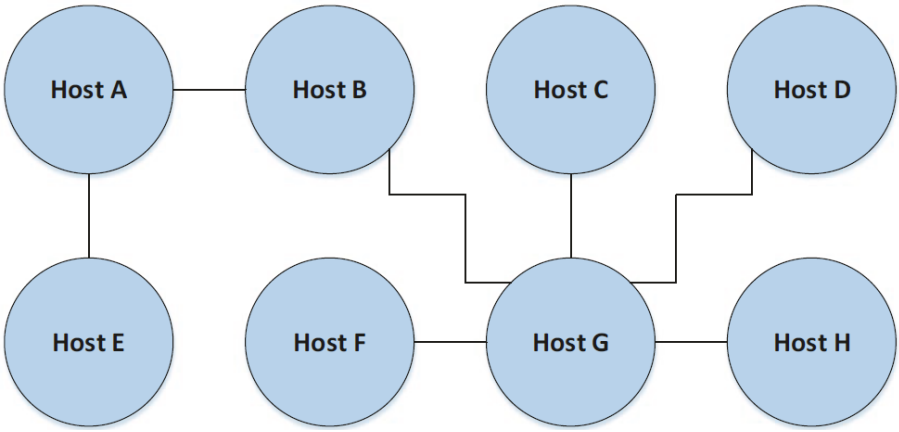
بخش عمده‌ای از تحقیقات صورت گرفته در زمینه ابتکار و نوآوری برای تیم‌های قرمز، توسط بخش دانشگاهی انجام شده‌اند. برخی از این مطالعات با عنوان تست نفوذ و برخی موارد با عنوان تیم قرمز معرفی می‌شوند. باز هم برای موضوع و هدف این کتاب، همه این قابلیت‌های امنیتی تهاجمی معادل هم محسوب می‌شوند. در انجمن‌های دانشگاهی مثل مقالات و مجلات علمی، بخش عمده‌ای از مطالعات به طور ویژه متمرکز بر اتوماسیون حمله تیم قرمز با استفاده از فناوری هستند نه ابتکار در زمینه فرایندهای امنیتی دفاعی که توسط انسان‌ها انجام می‌شود. احتمالاً دلیل این موضوع این است که عده بسیار کمی از محققان کارشناس مجرب امنیت تهاجمی هستند یا شاید دقیق‌تر اینکه، بیشتر کارشناسان مجرب حوزه امنیت تهاجمی، به دنبال انجام مطالعات آکادمیک نیستند. این یعنی احتمالاً نویسندگان و محققان دانشگاهی درباره چالش‌ها و مشکلات تیم قرمز از منظر اجراکننده آن تجربه عملی ندارند یا با کارهای واقع گرایانه‌ای که

می‌توان برای بهبود روش‌ها و فرایندها انجام داد، آشنا نیستند. به غیر از پیچیده‌تر کردن ابتکار و نوآوری در زمینه تجارت هکرهای اخلاقی، کارهای دانشگاهی باید قابل دفاع هم باشند. پیدا کردن روش‌هایی قابل دفاع برای کاری مثل مانور تیم قرمز، ارزیابی و محیط‌ها که به شدت تحت تأثیر اقدامات انسان قرار دارد می‌تواند بسیار دشوار باشد. بنابراین، تمرکز مطالعات آکادمیک تیم قرمز عمدتاً فناوری اتوماسیون و مدل‌های حمله‌ای است که امکان آزمایش مکرر آنها وجود دارد و می‌توان بدون دخالت کارشناسان حرفه‌ای تیم قرمز و اجرای واقعی این عملیات، آنها را امتحان کرد.

فناوری‌های حاصل از این تلاش‌ها به طور کلی در یکی از این سه دسته‌بندی قرار می‌گیرند: آنهایی که بهره برداری یا جابجایی بین سیستم‌ها را انجام نمی‌دهند، آنهایی که بهره برداری انجام می‌دهند اما جابجایی را انجام نمی‌دهند و آنهایی که هر دو کار را انجام می‌دهند. هر روش مزایا و معایب خاص خود را دارد همانطور که اتوماسیون به طور کلی این ویژگی را دارد. این به معنای بی‌استفاده بودن چنین راهکارهایی نیست و از طرفی به این معنا نیست که این راهکارها می‌توانند به خوبی جایگزین هکرهای اخلاقی شوند.

فناوری مدل‌سازی

شاید فناوری که از آسیب‌پذیری‌ها بهره برداری نمی‌کند یا از یک هدف به هدف دیگر منتقل نمی‌شود، به ظاهر شباهتی به تیم قرمز نداشته باشد اما به باور من، بین فناوری‌های اتوماسیونی که به روش آکادمیک مطرح شده‌اند، احتمال اینکه این روش‌ها تأثیر مثبتی بر فعالیت‌های تیم قرمز داشته باشند بیشتر است. کلید درک کاری که قرار است با کمک این فناوری‌ها انجام شود، کلمه "مدل سازی" است. فناوری و تکنیک‌هایی که روابط بین اهداف بالقوه در یک سازمان را مدل سازی می‌کنند قطعاً می‌توانند برای دستیابی به اهداف در یک مانور تیم قرمز بسیار مفید باشند. شکل ۲-۱ نمونه‌ای از چنین روابطی را نشان می‌دهد که در آن میزبان A آلوده کننده اولیه است و میزبان G بیشترین انتشار را انجام می‌دهد.



شکل ۲-۱ نمونه‌ای ساده سازی شده از نتایج مدل سازی

تیم‌های قرمز غیرسایبری در اصل حملات نظامی را شبیه سازی می‌کردند اما مدل سازی‌های مورد نظر ما، مانورهای دنیای سایبری هستند. مثلاً در یکی از این روش‌ها، اطلاعات به دست آمده از اهداف درون سازمان مثل پورت‌های باز، آدرس‌ها، طرح شبکه، نرم‌افزارهای نصب شده و غیره به یک مدل خودکار داده می‌شوند. سپس مدل اجرا می‌شود تا بر اساس مقایسه داده‌های ورودی با یک پایگاه داده حاوی اکسپلویت‌های شناخته شده، راه‌های ممکن یا بالقوه حمله و حرکت را مشخص کند.

محققان دانشگاهی مختلف با استفاده از الگوریتم‌ها یا منطق خاص خودشان درباره شیوه رخ دادن اکسپلویت و مسیرهای مختلف حمله و اینکه چه میزبان‌ها یا سیستم‌هایی در معرض یک خطر خاص قرار دارند، تکنیک‌ها و مطالعات مختلفی را مطرح کرده و انجام داده‌اند. یکی از ویژگی‌های مشترک همه این ایده‌ها این است که متکی بر نوعی ورودی هستند که بر اساس روش‌های مختلف روی آنها کار می‌شود تا یک ماتریس از ارتباطات بالقوه تشکیل دهند که تیم‌های امنیت سایبری متمرکز بر آن شوند.

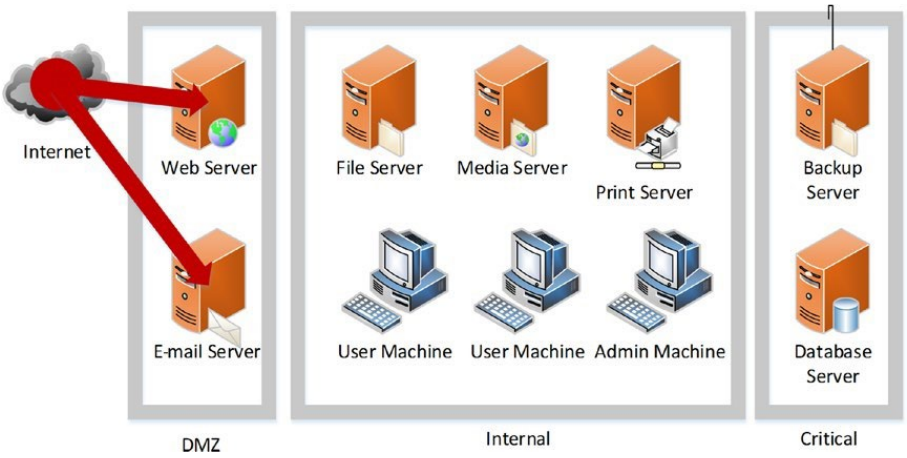
همانطور که نویسندگان مطالعات اشاره می‌کنند، استفاده از این فناوری‌ها به جای تیم قرمزی که توسط انسان اجرا می‌شود چند مشکل مهم دارد. این روش‌ها به خودی خود بسیار عالی هستند. در صورت استفاده از داده‌هایی با ساختار مشابه و اجرای این روش‌ها بر اساس داده‌های به روز آسیب‌پذیری‌ها، می‌توان به نقاط ریسک و مسیرهای اکسپلویت عملی رسید اما فقط برای اسنپ شاتی از زمان که داده‌های مورد استفاده، نمایانگر وضعیت آن لحظه خاص هستند. این اسنپ شات بستگی به این دارد که داده‌ها چه زمانی از اهداف جمع آوری شدند و پایگاه داده

آسیب‌پذیری‌ها آخرین بار چه زمانی به‌روزرسانی شده است. اگر پس از اجرای الگوریتم، یک پورت در یک میزبان تغییر کند، روش مورد نظر به شدت ناقص خواهد شد و یک آسیب‌پذیری که تازه مسلح شده می‌تواند نتایج مدل را کاملاً تغییر دهد.

نمی‌توان یک کاربرد برای دنیای واقعی را متصور شد که در آن اطلاعاتی که به چنین الگوریتمی تزریق می‌شود، یک بازنمایی کامل و دقیق از کل سازمان باشند. حالا کاربران و مدیران انسانی را به این ترکیب اضافه کنید که دائماً متغیرها را تغییر می‌دهند. در این صورت استفاده از داده‌ها در محیطی به غیر از آزمایشگاه یا شرایطی مشابه آن، غیرممکن خواهد بود. گرچه این فناوری نمی‌تواند جایگزین کامل مهارت و نیروی انسانی باشد، اما بدون شک یکی از راه‌های سریع تحلیل هدف گیری مهاجمان است.

فناوری غیرانتقالی

فناوری غیرانتقالی- شناسایی و بهره برداری از آسیب‌پذیری - بر خلاف فناوری مدل سازی خودکار، برای دنیای امنیت تهاجمی آشناتر است اما پس از نفوذ، درون یک سیستم یا سازمان شروع به حرکت و انتقال نمی‌کند (شکل ۲-۲).



شکل ۲-۲ روش غیرانتقالی و بدون بهره برداری

این نوع مطالعات در حوزه آکادمیک طیف وسیعی دارند. از جمله فناوری‌هایی که به طور اختصاصی روی یک نوع نرم‌افزار خاص (مثل صفحات وب یا پایگاه‌های داده) کار می‌کنند و روش‌های خودکار ارزیابی آسیب‌پذیری در کل شبکه به صورت سطحی.

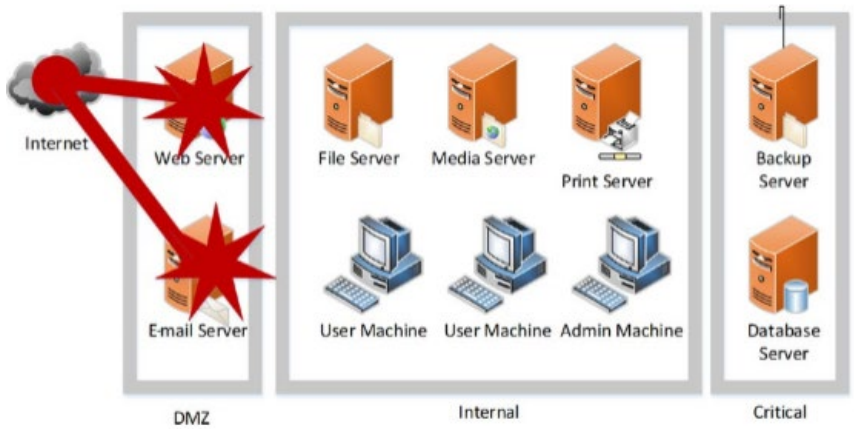
این فناوری‌ها از جمله راهکارهایی هستند که تنها یک بار فعال و استفاده می‌شوند و نیازی به کمک گرفتن از هکرهای اخلاقی ندارند. انتظار می‌رود که افراد آشنا با حیطه فناوری اطلاعات توانایی دانلود این ابزارها و استفاده از آنها برای هدف مورد نظرشان را داشته باشند. در این گروه، ابزارهایی وجود دارند که سعی دارند به صورت مکرر سازوکارهای امنیتی را دور بزنند و از صفحات وب یا پایگاه‌های داده بهره برداری کنند و سپس آسیب‌پذیری‌های شناسایی شده را به شخصی که از ابزار استفاده می‌کند، گزارش دهند. سایر ابزارهای این گروه شامل فناوری‌های اسکنی هستند که توانایی ارزیابی هر چیزی در محدوده محیط اجرا را دارند.

لازم به ذکر است که این گروه از ابزارهای جایگزین تیم قرمز، شامل اسکنرهای آسیب‌پذیری هستند که در خیلی از محافل آکادمیک از آنها به عنوان فناوری‌های خودکار سازی تیم قرمز یاد می‌شود. اجرای اسکن آسیب‌پذیری به عنوان تنها راهکار، دو مشکل ایجاد می‌کند. اول اینکه این روش نشان دهنده یک حمله واقعی برضد سازمان نیست و حتی توانایی شبیه سازی تأثیرات حمله واقعی را ندارد. دوم اینکه، این روش فقط آسیب‌پذیری‌های اهدافی را ارزیابی می‌کند که از نقطه اجرا قابل دسترس هستند بنابراین باعث می‌شود که بخش‌های بزرگ و خطرناکی از سازمان، بدون ارزیابی باقی بمانند.

بهترین راهکارها در این گروه، آنهایی هستند که روی تعداد زیادی از نقاط پایانی شبکه یا همه آنها توزیع می‌شوند. این روش یک بازنمایی دقیق از حمله یا پیامدهای آن نیست اما این راهکارها متناسب با محدوده استقرارشان، یک ارزیابی عمیق از محیط فراهم می‌کنند. برخی از این فناوری‌ها، سیستم عامل‌های کوچکی هستند که روی درایوهای **USB** یا سی‌دی‌ها نصب می‌شوند و می‌توان آنها را به صورت فیزیکی در سطح شبکه جابجا کرده و اطلاعات آسیب‌پذیری‌ها را از زوایای مختلف جمع آوری کرد. برخی از آنها بیشتر شبیه به محصولات امنیتی توزیع شده برای نقاط پایانی هستند که روی سیستم‌های زیادی نصب می‌شوند. حتی این سیستم‌ها هم معمولاً بهره برداری واقعی را انجام نمی‌دهند و هیچ یک بر خلاف حملات واقعی، به دنبال استفاده از سیستم یا اپلیکیشن تحت نفوذ برای گسترش بیشتر نیستند.

علاوه بر تلاش‌های آکادمیک صورت گرفته برای پیاده‌سازی چنین روش‌هایی، چندین نمونه صنعتی هم از این دسته‌بندی وجود دارد. گاهی اوقات شاهد استفاده از ابزار بهره برداری خودکار **db-autopwn** در سیستم عامل‌های مورد استفاده برای امنیت تهاجمی بودیم. به همین ترتیب، سایر فریم ورک‌های امنیتی غیررایگان هم گزینه‌هایی برای بهره برداری خودکار دارند که عمدتاً از **db-autopwn** استفاده کرده یا تقلیدی از آن بوده و بر اساس آن ساخته می‌شوند. این ابزارها

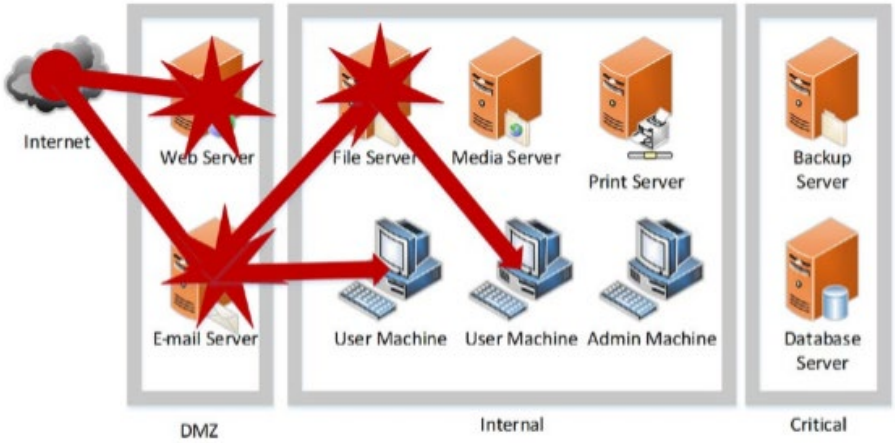
قابلیت بهره برداری از میزبان‌ها پس از اسکن آنها را دارند اما قابلیت چرخش پس از نفوذ را ندارند (شکل ۲-۳).



شکل ۲-۳ مدل غیرانتقالی با بهره برداری

فناوری‌های انتقالی با بهره‌برداری

در این قسمت بدافزارها وارد عمل می‌شوند. فناوری‌های این دسته سعی دارند پس از بهره برداری، از دسترسی‌های به دست آمده برای اسکن خودکار و انتقال به ماشین‌های دیگر استفاده کنند. در واقع در این بخش با موضوعاتی روبرو هستیم که شبیه موضوعات موجود در فریم ورک‌های صنعتی هستند و ابزارهایی که مثل کرم‌های کامپیوتری عمل می‌کنند. این فناوری متمرکز بر مفاهیمی از دو گروه قبلیِ ابزارهای جایگزین توصیه شده توسط جوامع آکادمیک است. این ابزارها نیاز به قابلیت‌های ارزیابی آسیب‌پذیری و همچنین مدل سازی روابط دارند. ترکیب این مفاهیم امکان دسترسی به یک سیستم و ادامه ارزیابی آسیب‌پذیری از چشم‌انداز تازه به دست آمده را فراهم می‌کنند - به روشی خودکار که با منطق هدفگیری رابطه‌ای بر اساس مدل سازی انتخابی حمله کار می‌کند (شکل ۲-۴).



شکل ۲-۴ انتقال و بهره برداری

عملکرد این گروه از ابزارها به شدت وابسته به الگوریتم‌های مورد استفاده برای شناسایی اکسپلولیت‌های مورد بهره برداری و همچنین روش انتشار در شبکه است. خطر این ابزارها این است که مثل یک کرم خودکار عمل می‌کنند و اگر به درستی پیکربندی یا نظارت نشوند، می‌توانند منجر به آسیب رسیدن و افت عملکرد سیستم‌های تحت ارزیابی شوند. میلیون‌ها روش و حالت مختلف برای از کنترل خارج شدن شرایط وجود دارد که احتمالاً تعداد آنها به اندازه تعداد راهکارهای قابل استفاده برای اجتناب از آنها با استفاده از منطق است. اما هر چقدر در ماتریس تصمیم گیری یک فریم ورک بهره برداری خودکار از منطق بیشتری استفاده کنید، پیچیدگی کار و نیاز به مداخله انسان بیشتر می‌شود. وابستگی به این فناوری‌ها باعث ایجاد نیاز به مراقبت از آنها یا استفاده از منابع رایانشی بسیار زیاد می‌شود در نتیجه مزایای آنها را از بین برده و نمی‌توانند جایگزینی مقرون به صرفه برای هکرهای اخلاقی محسوب شوند.

از نظر ابتکار و نوآوری، این گروه سوم از ابزارها - که برای بهره برداری و انتقال درون سازمان استفاده می‌شوند - باعث پیشی گرفتن تیم‌های قرمز در رقابت بین هکرهای انسانی و اتوماسیون می‌شوند. برای توضیح دلیل نیاز به استفاده از هکرهای انسانی اخلاقی، متمرکز بر همین قابلیت خواهم بود.

مزایا و معایب اتوماسیون

اما اتوماسیون چه معایبی دارد؟ چرا از یک ابزار رایگان برای شناسایی انواع آسیب‌پذیری‌های موجود در شبکه و رفع آنها استفاده نکنیم؟ آیا این روش به اندازه کافی خوب نیست؟ این‌ها سوالاتی هستند که باید برای کنار زدن گزینه استفاده از ابزارهای بهره برداری و انتقال خودکار اول به آنها پاسخ دهیم. گرچه چنین ابزارهایی مزایای خاص خودشان را دارند اما در زمینه ارزیابی امنیتی تهاجمی، معایب و نقطه ضعف‌های آنها بیشتر از مزایا است.

مزایای اتوماسیون

همانطور که پیش از این اشاره شد، مزایای راهکارهای بهره برداری و انتقال خودکار نسبتاً مشخص و بیشتر آنها مربوط به مسئله دسترسی پذیری هستند. قابلیت دسترسی آسان به ارزیابی‌هایی که توسط این فناوری انجام می‌شود دلیل اصلی وجود خریدار برای آنها و ادامه پیاده‌سازی چنین قابلیت‌هایی در فریم ورک‌های اکسپلویت است. شرکت‌هایی که منابع مالی لازم برای استخدام هکرهای اخلاقی جهت اجرای ارزیابی‌ها را ندارند، معمولاً راحت‌تر به این فناوری‌ها دسترسی دارند. برخی از این ابزارها به صورت رایگان قابل تهیه و استفاده هستند. خود سازمان به راحتی می‌تواند این ابزارها را اجرا کند و برخلاف تیم‌های قرمز درون سازمانی یا خدمات تست نفوذ خارجی، نیازی به انتظار و زمانبندی برای اجرای آنها ندارد. به غیر از مسئله زمانبندی، چنین فناوری‌هایی از نظر مدت زمان ارزیابی هم مزایای خاص خود را دارند. می‌توان فناوری‌های خودکار را در یک بازه چند ساعته روی سیستم‌های سازمانی اجرا کرد در حالی که ممکن است کار هکرهای اخلاقی چند روز یا چند هفته زمان ببرد. طبق تعریف، این فناوری‌ها به صرفه جویی در وقت و هزینه‌ها صرفه جویی می‌کنند. اما بررسی عمیق‌تر از این مزایای سطحی و واقع گرایانه نبودن آنها، نشان می‌دهد که چرا استقبال وسیعی از آنها صورت نگرفته و همچنان تقاضای زیادی برای هکرهای اخلاقی وجود دارد.

معایب اتوماسیون

مهم‌ترین ایراد فناوری‌های اکسپلویت و انتقال خودکار، بیشتر بودن زمان و هزینه پیاده‌سازی آنها نسبت به روش استفاده از هکرهای انسانی است که اهمیت بسیار زیادی دارد. بزرگترین مزایای نظری این ابزارها در عمل تبدیل به مهم‌ترین معایب آنها می‌شود. این ابزارها می‌توانند هزینه‌ها یا ریسک بیشتری را به سازمان‌ها تحمیل کنند که این هزینه‌ها و ریسک‌ها دو جنبه فعال و منفعل دارند که در ادامه به بررسی آنها می‌پردازیم.

ریسک‌های فعال

ریسک‌های فعال ذاتی موجود در راهکارهای تیم قرمز خودکار، می‌توانند حین ارزیابی سیستم‌ها نمایان شوند. بهره برداری یا هک، در اصل به سوء استفاده از یک سیستم به روش غیرمعمول به منظور دستیابی به نتایجی غیرمعمول گفته می‌شود. هر تلاشی برای بهره برداری از سیستم‌ها، با احتمال ایجاد پیامدهای منفی در سیستم همراه خواهد بود. ممکن است این پیامدها مثل کند شدن سرعت پردازش سیستم کم خطر یا مثل وارد شدن آسیب فیزیکی دائم به سیستم‌های تحت حمله، بسیار فاجعه بار باشند.

حتی با وجود پیاده‌سازی بررسی‌های امنیتی در این نرم‌افزارها، در روش اتوماسیون بهره برداری و انتقال بین سیستم‌ها قدرت تشخیصی که یک مهاجم انسانی دارد، وجود ندارد. بنابراین، ممکن است سرعت بالای اتوماسیون، باعث آسیب رسیدن به سیستم‌ها، دستگاه‌ها یا سرویس‌های ارزشمند با سرعتی بالا شود. ممکن است یک انسان با استفاده از یک اکسپلویت خطرناک باعث ایجاد نقص در عملکرد یک سیستم شود اما یک اسکریپت خودکار می‌تواند همان اکسپلویت را روی صد سیستم اجرا کند. این ریسک می‌تواند مزایای این فناوری‌ها از نظر مقرون به صرفه بودن را هم خنثی کند. ممکن است مبلغ صرفه جویی شده با خودداری از استخدام هکرهای اخلاقی - یا حتی مبلغی بیشتر از آن - صرف رسیدگی به هزینه‌های ناشی از بروز اختلال در خدمات، رسیدگی به مشکلات، جایگزینی سیستم‌های آسیب دیده یا حتی آسیب رسیدن به اعتبار سازمان و از دست رفتن مشتریان شود.

ریسک‌های منفعل

هزینه‌ها و ریسک‌های منفعل فناوری‌های بهره برداری خودکار، می‌تواند بیشتر از نوع فعال آنها باشد. در مجموع، فروشندگان فناوری‌های خودکار از جمله نرم‌افزارهای امنیتی و فریم ورک‌های اکسپلویت، به مقرون بودن محصولاتشان اشاره می‌کنند. دیدگاه آنها این است که چنین فناوری‌هایی با جایگزین کردن برخی از پرسنل به صرفه جویی در هزینه‌ها کمک می‌کنند. اما معمولاً هزینه‌های کسب مجوز و تهیه اشتراک این نرم‌افزارها برای به روز نگه داشتن اطلاعات آنها بسیار زیاد است. علاوه بر این، استفاده از این نرم‌افزارها به صورتی که منجر به ارتقای وضعیت امنیت سازمان شود، نیاز به تخصص کار با ابزارهایی خاص دارد. ممکن است در چنین شرایطی سازمان نیاز به صرف هزینه‌ای بیشتر برای آموزش کارمندان یا استخدام افرادی با گواهینامه یا تخصص استفاده از ابزار مورد نظر، داشته باشد. در این مرحله، بعید است که صرفه جویی ناشی

از به کار بردن ابزارهای بهره برداری خودکار، بیشتر از معایب استفاده نکردن از خدمات یا پرسنل امنیتی تهاجمی باشد.

به باور من، بین همه معایب استفاده از اتوماسیون، ریسک منفعل آن بیشترین خطر را برای سازمان ایجاد می‌کند چون استفاده از این ابزارها باعث ایجاد حس امنیت کاذب خواهد شد. همانطور که پیش از این اشاره شد، این احتمال وجود دارد که مدیران سازمان‌ها برای کاهش هزینه‌ها از فناوری‌های بهره برداری خودکار جهت ارزیابی وضعیت امنیتی خودشان استفاده کنند. مشکل اینجاست که این ارزیابی، شرایط یک حمله واقعی را به خوبی به تصویر نمی‌کشد.

فرض کنید که چنین نرم‌افزاری به قدری قوی و خوب است که همه حفره‌های امنیتی موجود در همه سیستم‌های شبکه را شناسایی می‌کند. سپس تیم امنیت سایبری به خوبی همه این تهدیدات را برکنار می‌کند. بدون تردید، این کار منجر به ایجاد حس اطمینان در مدیران سازمان و کارمندان امنیتی شده و تصور می‌کنند که در برابر تهدیدات سایبری ایمن هستند. اما طی چند هفته بعد، چند اکسپلویت جدید شناسایی شده یا دستگاه‌های جدیدی که در برابر اکسپلویت‌های قدیمی آسیب‌پذیر هستند به سازمان اضافه می‌شوند. یک مهاجم از این حفره‌ها استفاده کرده و بدون اینکه شناسایی شود، به کل سیستم نفوذ می‌کند. در این شرایط چه اتفاقی رخ می‌دهد؟

سازمان همه حفره‌های شناسایی شده در زمان اسکن را رفع کرده اما بهره برداری خودکار از سیستم‌ها با روش اجرای حمله توسط یک مهاجم و پیشرفت و پافشاری این مهاجمان تفاوت دارد. به دلیل وجود این تفاوت‌ها، پرسنل امنیت سایبری سازمان در جریان نیستند که چطور نظارت بر تهدیدات واقعی را انجام داده یا به فعالیت مهاجمان واکنش نشان دهند. بدتر اینکه، هیچ وقت فرایند واکنش به حادثه را در مقابل یک تهدید واقعی که به دنبال تثبیت جایگاه خودش در سازمان است، تجربه نکرده‌اند. همواره تهدیدات و اکسپلویت‌های جدیدی در یک سازمان شکل می‌گیرند. شناسایی و بهره برداری از حفره‌های تکنولوژیکی در سیستم‌ها فقط منجر به تقویت بخش محدودی از دستگاه امنیتی سازمان و مسئولیت‌های مربوط به آن می‌شود.

اجرای مانور تیم قرمز به همراه هکرهای اخلاقی به سازمان‌ها کمک می‌کند تا کاستی‌های موجود در همه جنبه‌های امنیتی خودشان را شناسایی کنند از جمله مشکلات مربوط به فناوری، کارمندان و رویه‌ها. همچنین این مانورها علاوه بر تشخیص مشکلات فناوری‌ها، به درک مشکلات موجود در شیوه پیاده‌سازی فناوری، روش‌ها و سیاست‌های امنیتی در سازمان کمک می‌کنند. بعلاوه، هکرهای اخلاقی واکنش کاربران و مدیران به یک حمله در سازمان را ارزیابی می‌کنند که این واکنش بخش بسیار مهمی از ارزیابی امنیت تهاجمی است.

بررسی چند سناریوی نمونه

در ادامه چند سناریو را بررسی می‌کنیم که هنگام اجرای تست نفوذ در سازمان‌ها با آنها روبرو شده‌ام. این مثال‌ها، برتری استفاده از هکرهای انسانی را بهتر مشخص می‌کنند. برای حفاظت از هویت افراد برخی از جزئیات این سناریوها تغییر کرده‌اند.

سناریوی اول

یک ارزیاب، هنگام بررسی یک سیستم لینوکسی پس از نفوذ به آن، متوجه وجود نام‌های مستعاری مثل **us-west** و **us-east** می‌شود. این سبک نام گذاری در زیرساخت‌های میزبانی ابر وب‌سرویس آمازون (**AWS1**) متداول است. ارزیاب، فهرست فرمان‌های اجرا شده توسط این نام‌های مستعار را ارزیابی کرده و نشانی جامپ باکس‌های[۲] **AWS** سازمان را پیدا می‌کند؛ همچنین موفق به پیدا کردن محل ذخیره اطلاعات ورود به دستگاه‌های ابر از راه دور در کامپیوتر تحت نفوذ می‌شود. سپس ارزیاب با استفاده از این اطلاعات، به یکی از جامپ باکس‌های سازمان در محیط **AWS** دسترسی پیدا می‌کند. بررسی محلی این سیستم نشان می‌دهد که سازمان برای راحت‌تر شدن کارها یا از سر غفلت، رمزهای **AWS** و اطلاعات ورود به کنسول مدیریت را از سیستم جامپ باکس پاکسازی نکرده است. به این ترتیب، ارزیاب توانست از اطلاعات ورود به حساب برای ساختن یک حساب کاربری جدید در کنسول مدیریت حساب **AWS** سازمان استفاده کرده و با استفاده از یک مرورگر اینترنتی وارد آن شود. به محض ورود به این کنسول، ارزیاب امکان حذف، خاموش کردن یا ایجاد ماشین‌های جدید را پیدا کرد.

فناوری‌های خودکار توانایی شناسایی این نام‌های مستعار و استفاده از اعتبارنامه‌های کاربری[۳] را برای حرکت و جابجایی در زیرساخت ابر سازمان ندارند. غریزه انسانی باعث شد که این ارزیابی بسیار عمیق‌تر از آنچه یک نرم‌افزار کامپیوتری انجام می‌دهد، اجرا شود. بررسی دستگاه‌های ثبت شده در حساب ابر **AWS** به ارزیاب کمک کرد تا بر اساس نام‌ها، سرویس‌ها و نرم‌افزارهای مورد استفاده تشخیص دهد که راهکارهای مورد استفاده برای مراحل پیش تولید و توسعه، در یک حساب **AWS** میزبانی می‌شوند. همچنین ارزیاب متوجه وجود چند ماشین مجازی خاموش

---

[1] Amazon Web Service

[۲] مترجم: سروری که در محیط‌های ابر استفاده می‌شود و با عمل کردن مثل یک سرور پروکسی، به کلاینت‌ها امکان می‌دهد که از راه دور به سرور متصل شوند.

[۳] نام کاربری و رمز عبور

شد که با اسم افراد نامگذاری شده بودند مثل کتی[4]. حداقل یکی از این نام‌ها شبیه نام یک حساب مدیریتی به نظر می‌رسد که در یکی از دستگاه‌های مورد نفوذ در مراحل اولیه ارزیابی، فعال بود.

ارزیاب اطلاعات لازم برای ورود به این سیستم‌ها را در اختیار ندارد چون همه اعتبارنامه‌های جمع آوری شده در مرحله ارزیابی تا به اینجا، مربوط به سیستم‌های لینوکسی بودند و این دستگاه‌های جدید وقتی روشن شوند، با سیستم عامل مایکروسافت ویندوز کار می‌کنند. ارزیاب، سیستم را خاموش کرده و هارددرایو دستگاه ویندوزی را به یکی از ماشین‌های مجازی لینوکسی که از قبل به آن نفوذ کرده بود وصل می‌کند. به این ترتیب، مهاجم می‌تواند از طریق فایل‌های سیستم عامل به اعتبارنامه‌های کاربری دست پیدا کند. سپس، ارزیاب دستگاه کتی را روشن کرده و با استفاده از اعتبارنامه‌های به دست آمده از هارددرایو، وارد آن می‌شود. این اعتبارنامه‌ها به ارزیاب امکان می‌دهند که به سایر دستگاه‌های ویندوزی هم دسترسی پیدا کند چون اعتبارنامه‌های کتی، در حوزه مدیریتی قرار داشتند. همچنین، اطلاعات جمع آوری شده از هارددرایو به شناسایی کنسول ورود به حساب AWS و اعتبارنامه‌های آن هم کمک می‌کند. در این مرحله، ارزیاب می‌تواند به همه دستگاه‌های متعلق به سازمان وارد شود و کل زیرساخت ابر سازمان را خاموش و حذف کند. وحشتناک است که مسئله ساده‌ای مثل استفاده از یک نام مستعار می‌تواند به حذف کل داده‌ها و دستگاه‌های سازمان با چند کلیک منجر شود. همچنین، کاملاً واضح است که فناوری اتوماسیون قابلیت اجرای فرایندها و ریزه کاری‌هایی که در این زنجیره نفوذ وجود داشت را ندارد. بعلاوه، هیچ فناوری اتوماسیونی که قرار باشد برای رسیدن به این سطح از نفوذ، به همه جنبه‌های سازمان نفوذ کند، قادر نیست این کار را با احتیاط و درایتی انجام دهد که از آسیب رسیدن به سازمان پیشگیری کند.

سناریوی دوم

یک ارزیاب هنگام بررسی یک سیستم میزبانی شده در محیط AWS، پس از نفوذ به آن - از طریق تاریخچه فرمان‌های دستگاه - متوجه اجرای فرمان‌های مدیریتی AWS توسط ادمین مدیر سیستم بدون وارد کردن اعتبارنامه‌های کاربری می‌شود. معمولاً برای اجرای این فرایند نیاز به ورود یک کلید یا رمز وجود دارد. ارزیاب سعی می‌کند همان فرمان را با یک حساب کاربری سطح پایین‌تر اجرا کند و مشخص می‌شود که می‌توان کارهای مدیریتی را روی کل حساب AWS انجام

[4] Kathy

داد. ارزیاب متوجه می‌شود که خود سیستم، مجوز اجرای فرمان‌های کنسول مدیریت **AWS** را دارد. به این ترتیب، ارزیاب می‌تواند به کل مرکز داده میزبانی شده در **AWS** نفوذ کرده و دستگاه‌های جدیدی به محیط ابر سازمان اضافه، حذف یا آنها را خاموش کند. سپس ارزیاب به این نتیجه می‌رسد که چون هیچ کلید یا اعتبارنامه **AWS** روی سیستم پیدا نشده، سایر سیستم‌ها هم مجوز و دسترسی اجرای فرمان‌های **AWS** روی این دستگاه را دارند. پس از این نتیجه گیری ارزیاب سعی می‌کند فرمان‌های قابل مشاهده در تاریخچه فرامین را اجرا کند. پس از اینکه مشخص شد این کار قابل انجام است، ارزیاب متوجه نقش این سیستم به عنوان یک مرکز مدیریت برای کل فضای ابر سازمان می‌شود.

برخلاف مورد قبل، می‌توان مطمئن بود که این تنظیمات و روش کار فقط برای راحتی انتخاب شده نه از سر غفلت مدیران سازمان. ممکن است حامیان فناوری‌های اتوماسیون این استدلال را مطرح کنند که نرم‌افزار تست نفوذ، قابلیت امتحان کردن همه فرمان‌های موجود در تاریخچه فرامین یا اسکریپت‌های دستگاه‌های تحت نفوذ را دارد. این نمونه و سایر قابلیت‌ها و کارهایی که یک ارزیاب می‌تواند انجام دهد، در صورتی که برای انجام آنها از تجربه و مهارت استفاده نشود می‌توانند بسیار ترسناک باشند. مثلاً فرض کنید که قبلاً مدیر سیستم، فایل‌ها را با استفاده از کاراکترهای جانشین حذف کرده یا کل درایوهای حاوی داده را پیش از پشتیبان گیری از سیستم فایل‌های جدید، پاکسازی کرده باشد در این صورت اتوماسیون نرم‌افزار تیم قرمز می‌تواند به نابودی داده‌های سازمان منجر شود.

سناریوی سوم

یک ارزیاب هنگام بررسی سیستمی پس از نفوذ، متوجه وجود یک سرویس فوروارد کننده اسپلانک[5] روی پورت ۸۰۸۹ با حالت شنود محلی می‌شود. این سرویس در اسکن‌های بیرونی قابل مشاهده نبوده چون شنود را به این روش انجام می‌دهد و از راه دور قابل دسترس نیست.

ارزیاب، اعتبارنامه‌های پیش فرض برای این سرویس را بررسی کرده و آنها را با استفاده از یک فرمان کرل[6] روی پورت محلی امتحان می‌کند. اعتبارنامه‌ها کار می‌کنند و سرویس با دسترسی‌های کاربر ارشد اجرا می‌شود بنابراین آزمونگر می‌تواند دسترسی‌ها را افزایش داده و یک کلید مدیریتی پیدا کند که امکان استفاده از آن برای نفوذ به کل شبکه محلی وجود دارد. توانایی ارزیاب برای شناسایی سرویسی که به صورت محلی اجرا می‌شود، بررسی اعتبارنامه‌های پیش

[5] Splunk forwarder
[6] curl

فرض این سرویس و سپس استفاده از سرویس برای تشدید حمله کارهایی است که هر فناوری اتوماسیونی در انجام آنها با چالش روبرو می‌شود. اسکن خودکار از راه دور هیچ آسیب‌پذیری را شناسایی نمی‌کند و استفاده از یک فناوری خودکار بهره برداری و انتقال که همه اجزاء را به صورت محلی ارزیابی می‌کند کارها را به شدت سخت‌تر می‌کند به خصوص اگر قرار باشد فهرست اعتبارنامه‌های کاربری را ذخیره کرده و از همه آنها استفاده کند.

سناریوی چهارم

یک ارزیاب هنگام بررسی سیستمی پس از نفوذ به آن، متوجه وجود فرمان‌های گیت[۷] در تاریخچه فرمان‌های اجرا شده توسط مدیر می‌شود. لازم به ذکر است که گیت یک مخزن کد است. سپس ارزیاب به مخزن گیت که محلی نیست دسترسی پیدا می‌کند و می‌تواند همه فایل‌های درون آن را بدون نیاز به احرازهویت استخراج کند. این فایل‌ها حاوی اعتبارنامه‌هایی هستند که در قالب متن ساده ذخیره شده‌اند همچنین پیکربندی‌های شبکه که منجر به نفوذ به کل سازمان می‌شوند. برخلاف یک هکر اخلاقی، فناوری‌های اتوماسیونی که پیش از این مورد بررسی قرار گرفتند، منطق استنتاجی لازم برای تشخیص ارتباط داشتن فرمان‌ها با گیت، هدف گیری مخزن، بررسی مخزن جهت شناسایی فایل‌هایی با نام‌های مورد توجه و استخراج، بیرون آوردن فایل‌ها از حالت فشرده و پیدا کردن اعتبارنامه‌های کاربری را ندارند.

فناوری‌های اتوماسیون بررسی شده در این فصل همگی ارزش بررسی توسط جامعه امنیت سایبری چه در بخش دانشگاه و چه در بخش صنعت را دارند به خصوص وقتی از آنها برای تقویت ارزیابی‌های انسانی استفاده شود. اما این باعث نمی‌شود که این فناوری جایگزین توانمند و امنی برای تیم‌های قرمز درون سازمانی یا سایر خدمات امنیت تهاجمی محسوب شود. در بسیاری از شرایط، شهود، منطق و احتیاط هکرهای اخلاقی از همه مزایای یک فناوری اتوماسیون برای سازمان پیشی می‌گیرند.

شکار تهدید

این فصل را با یک بررسی کلی از شکار تهدید و برخی از مشکلاتی که با افزایش محبوبیت این ایده، در صنعت امنیت تهاجمی شاهد آنها بودم، به پایان می‌رسانیم. شکار تهدید یعنی تلاش فعالانه برای شناسایی علائم نفوذ و استفاده از آنها جهت ارزیابی شبکه به منظور تشخیص

[7] Git

نفوذهایی که قبلاً صورت گرفته و احتمالاً هنوز ادامه دارند. انجام این کار به عنوان یک فعالیت امنیتی خوب است و اگر زیرساخت‌های امنیت سازمان از آن به عنوان یکی از استراتژی‌های دفاعی و نظارتی پشتیبانی کنند، می‌توان آن را پیاده‌سازی کرده یا در قالب خدمات تهیه کرد.

گسترش استفاده از اصطلاح شکار تهدید و افزایش فروش ابزارهای شکار تهدید به عنوان روشی جدید و نه به عنوان راهکاری برای تقویت روش‌های نظارتی موجود، با عوارض ناخوشایندی همراه است. فروش و استفاده از شکار تهدید به عنوان یک راهکار مقابله با تهدیدات پایدار پیشرفته (APT[8]) کار خطرناکی است. برخی از سازمان‌ها این ابزارها را جایگزین ارزیابی و بهره برداری فعال در نظر می‌گیرند. من به شخصه، تجربه همکاری با سازمان‌هایی را داشتم که درخواست می‌کردند درصد زیادی از کار تست نفوذ را با ابزارهای شکار تهدید جایگزین کنند. شکار تهدید ارزان‌تر است، راحت‌تر با ابزارهای نظارتی پرکاربرد ادغام می‌شود و از نظر کارمندان بخش امنیتی سازمان، خطرناک یا متخصام در نظر گرفته نمی‌شود بنابراین مزایای خاص خود را دارد. اما باید این مزایا را متناسب با کاربرد مورد نظر ارزیابی کرد.

همانطور که در فصل اول اشاره شد، شکار تهدید - با وجود تبلیغاتی که برای آن می‌شود - همچنان یک روش واکنشی برای برخورد با تهدیدات پیشرفته محسوب می‌شود. لازم است که مزایای پیاده‌سازی شکار تهدید به جای تیم قرمز یا تست نفوذ، با قابلیت‌های تیم قرمز که واقعاً یک روش پیشگیرانه است، مقایسه شود. علائم نفوذ تنها در صورتی مشهود خواهند بود که سازمان از قبل مورد نفوذ یا حمله قرار گرفته باشد. تمرکز بر شناسایی علائم فعالیت تهدیدات پیشرفته، یک فعالیت ارزشمند است اما نمی‌تواند جایگزین تست نفوذ یا تیم قرمز شود. صحبت من این نیست که این مسئله یک مشکل بزرگ در سطح کل صنعت امنیت سایبری است که باعث شده هکرهای انسانی و امنیت دفاعی به نفع شکار تهدید کنار زده شوند. قصد من صرفاً هشدار دادن درباره احتمال ایجاد چنین مشکلاتی با توجه به هیاهوی ایجاد شده درباره اصطلاح شکار تهدید و شیوه تبلیغ و بازاریابی آن بود.

خلاصه فصل دوم

در این فصل به بررسی انواع پیشرفت‌های تکنولوژیکی به دست آمده توسط صنعت و دانشگاه برای جایگزین کردن هکرهای اخلاقی با فناوری‌های اتوماسیون پرداختیم و اینکه چرا این راهکارها نمی‌توانند جایگزین تیم‌های قرمز انسانی باشند. همچنین در این فصل مفهوم شکار تهدید، مزایای

[8] advanced persistent threats

آن و احتمال از دست دادن قابلیت‌های دفاعی پیشگیرانه تیم قرمز و مزایای آن در صورت استفاده از شکار تهدید بررسی شد.

• تیم قرمز حرفه‌ای • مهدی لقایی • سهیل هاشمی

این کتاب به عنوان یک منبع برای افرادی نوشته شده که قصد اجرای مانورهای حرفه‌ای تیم قرمز را دارند؛ همچنین افرادی که از خدمات آنها استفاده می‌کنند. قرار نیست متن این کتاب هک کامپیوتر یا سازمان‌ها را به شما آموزش دهد بلکه به شما آموزش می‌دهد که چطور این کار را به روشی بهتر و طوری که منجر به ارتقای امنیت سازمان شود انجام دهید. این کار مستلزم کسب مهارت‌هایی فراتر از مهارت‌های شیرین هک برای اجرای ارزیابی های امنیتی تهاجمی است. چه به دنبال استخدام هکرهای اخلاقی باشید و چه به دنبال همکاری با آنها و چه خودتان یک هکر اخلاقی باشید، پس از مطالعه این کتاب باید درک بهتری از مهارت‌های لازم برای استفاده از شبیه‌سازی تهدیدات سایبری جهت کاهش ریسک پیدا کنید.