تیم قرمز حرفه‌ای

- مهدی لقایی
- سهیل هاشمی

فصل سوم: امنیت تهاجمی مدرن

فهرست مطالب

فهرست مطالب

۳

فصل سوم: امنیت تهاجمی مدرن

در فصل‌های قبلی به بررسی مزایای پیاده سازی تیم قرمز و سایر خدمات مشابه در یک سازمان با کمک هکرهای اخلاقی پرداختیم. حالا در این فصل، به مرور چالش‌ها و موانع کنونی برای دستیابی به قابلیت‌های امنیت تهاجمی می‌پردازیم. مشکلات این صنعت بی‌شمار هستند اما من به این نتیجه رسیدم که فراگیرترین این مشکلات مربوط به چند حوزه خاص هستند. تیم‌های قرمز همواره در نبردی بی‌پایان با مهاجمانی هستند که قرار است رفتار آنها را شبیه‌سازی کنند. استانداردهای مربوط به صنعت امنیت تهاجمی معمولاً مانع ارزیابی درست شده یا برای این کار مناسب نیستند. ماهیت خدمات ارایه شده به گونه‌ای است که باعث خصمانه شدن روابط با مشتریان می‌شود - واقعیتی که معمولاً منجر به ایجاد مشکلاتی واقعی برای ارزیابان و مشتریان آنها می‌شود. با فرض اینکه امکان رسیدگی به همه این محدودیت‌های ارزیابی وجود داشته باشد، باز هم برای تشکیل یک تیم قرمز موفق و کارآمد، باید به مسائل و چالش‌های مربوط به پرسنل رسیدگی کرد. در این فصل وضعیت محصولات امنیت دفاعی مدرن را از منظر این چالش‌ها بررسی می‌کنیم.

چالش تهدیدات پیشرفته مستمر (APT[1])

هدف و قصد تیم قرمز، شبیه‌سازی رفتار یک یا چند تهدید برای یک سازمان است به صورتی که سازمان آمادگی لازم را برای روبرو شدن با تهدیدات واقعی پیدا کند. انبوه حملات بالقوه و تهدیدات بسیار خطرناک - مثل APTها - چالش‌های زیادی برای اعضای تیم قرمز یا فروشنده‌های ابزارهای تست نفوذ ایجاد می‌کنند.

تعریف دقیق APT سخت و زمان‌بر است چون تعاریف و کاربردهای مختلفی برای آن ارایه شده است. برای هدف و موضوع این مطلب، ما فرض می‌کنیم که APTها عوامل مخربی در فضای سایبری هستند که منابع خوبی در اختیار دارند، دارای اهدافی مشخص هستند و با تلاش‌هایی سازمان یافته سعی به رسیدن به این اهداف دارند. این تعریف، مؤسسات و نهادهایی که توسط دولت‌ها پشتیبانی می‌شوند و گروه‌های مجرم سازمان یافته را هم پوشش می‌دهد. از جمله APTهای دولتی می‌توان به سازمان‌های سایبری مثل NSA در آمریکا، ستاد ارتباطات ویژه روسیه یا وزارت امنیت کشور چین اشاره کرد. همچنین، فعالیت‌های زیادی با پشتیبانی دولت‌ها وجود دارند که APT در نظر گرفته می‌شوند و در واقع شامل همه سازمان‌هایی هستند که از دولت بودجه دریافت می‌کنند تا حملات سایبری سازگار با اهداف آن سازمان اجرا کنند. اصطلاح APT

[1] Advanced Persistent Threats

در قالب جرایم سازمان یافته، دو کاربرد دارد. این اصطلاح می‌تواند اشاره به جرایم سازمان یافته سنتی مثل گروه‌های مافیا یا کارتل‌هایی داشته باشد که برای رسیدن به اهدافی خاص از حملات سایبری استفاده می‌کنند اما از این اصطلاح برای توصیف هر گروه هکری که با انگیزه‌های مشترک، اقدامات مجرمانه سازمان یافته انجام می‌دهد هم استفاده می‌شود مثل هکتیویست‌ها و خیلی دیگر از گروه‌های سازمان یافته مثل لازاروس[۲].

توانمندی بیشتر

صرف نظر از انگیزه گروه‌های **APT**، این افراد برای نفوذ به سازمان‌ها نسبت به تیم‌های قرمز روزبروز توانمندتر می‌شوند. توانمندی به خطر انداختن اهداف بالقوه در حملات سایبری، به در اختیار داشتن منابع بستگی دارد. یک **APT** نسبت به یک تیم قرمز به پول و منابع بیشتری دسترسی دارد. پرسنل، یکی از اجزای این توانمندی هستند. بسیاری از گروه‌های **APT** قابلیت پیشی گرفتن از پرسنل هر تیم قرمزی را دارند چه با در اختیار داشتن تعداد زیادی دارایی سایبری و چه با پرداخت هزینه‌های زیاد برای استخدام هکرهای بااستعداد.

یک **APT** بسته به نوع هدفش ممکن است چه برای استخدام افراد و چه خرید جدیدترین و بهترین ابزارها، میلیون‌ها دلار یا بیشتر هزینه کند. بنابراین این گروه‌ها، توانایی خرید ابزارهایی که ممکن است یک تیم قرمز به آنها دسترسی نداشته باشد را دارند مثل ابزارهای بسیار قدرتمند برای کرک کردن رمزهای عبور، نرم‌افزار فازینگ[۳] و فریم ورک‌های بهره برداری بسیار پیشرفته. همچنین گروه‌های **APT** برای خرید محصولات و خدمات به قوانین پایبند نیستند بنابراین ممکن است ابزارها را از منابع غیرمجازی بخرند که یک تیم قرمز امکان دسترسی و خرید قانونی از آنها را ندارد. از جمله این ابزارها و منابع می‌توان به اطلاعات شخصی اشاره کرد که به اجرای حملات مهندسی اجتماعی کمک می‌کنند مثل شماره ملی، شماره کارت بانکی و اطلاعات دیگر؛ همچنین ابزارهایی که از سازمان‌های دولتی یا سازمان‌های دیگری خریداری می‌شوند که یک تیم قرمز طبق قانون اجازه خرید یا استفاده از آنها را ندارد.

منابع دیگری که برخی از **APT**ها به آنها دسترسی دارند هم یکی دیگر از ویژگی‌های آنها است که ممکن است یک تیم قرمز امکان دسترسی به آنها را نداشته باشد. در مقایسه با **APT**ها - به خصوص گروه‌های دولتی که ممکن است یک سازمان را هدف بگیرند - تیم‌های قرمز به امکاناتی مثل دستگاه جمع آوری اطلاعات از دولت‌های خارجی دسترسی ندارند. منابع دیگری هم هستند

---

[2] Lazarus
[3] fuzzing

که APTهای دولتی با بودجه زیاد به آنها دسترسی دارند مثل نفوذ در شرکت‌های همان کشور یا حتی کشورهای دیگر. حتی برخی از گروه‌های APT این قدرت را دارند که از تولیدکننده‌ها درخواست کنند در سیستم‌ها یا اپلیکیشن‌هایی که قرار است به دست سازمان‌های هدف برسند، درهای پشتی نرم‌افزاری یا سخت‌افزاری ایجاد کنند. ممکن است برخی از این گروه‌ها امکان مداخله در زنجیره تأمین را داشته باشند و به محصولاتی که قرار است به دست سازمان هدف برسند، نفوذ کرده و آنها را برای رسیدن به اهدافشان دستکاری کنند.

زمان بیشتر

معمولاً تعاملات تیم قرمز در یک بازه زمانی خاص انجام می‌شوند. حتی در شرایطی که سازمانی یک تیم قرمز داخلی قوی دارد، باز هم ممکن است این تیم در زمان‌های مختلف روی گزینه‌های متفاوتی برای سازمان متمرکز شده و برای همیشه یک زیرمجموعه خاص را هدف نگیرد. در بسیاری از مواقع، ارزیابی‌های امنیت تهاجمی در بازه‌های زمانی دو هفته الی یک ماه انجام می‌شود تا کل سازمان ارزیابی شود. وقتی این کار توسط سازمان‌های دیگر انجام می‌شود، یک قرارداد برای آن در نظر گرفته می‌شود که زمانبندی دقیق ارزیابی را مشخص کرده و انعطاف پذیری زمانی را برای هکرهای اخلاقی از بین می‌برد. همچنین بعید است که یک سازمان محض احتیاط تصمیم بگیرد که تلاش‌های تیم قرمز جهت نفوذ به سیستم‌ها در آخر هفته‌ها یا پس از ساعات کاری انجام شوند که کارمندان در سازمان حضور ندارند.

وقتی چنین زمانبندی‌هایی را با برنامه کار APTها مقایسه کنید، متوجه برتری‌های آنها می‌شوید. حتی در صورت برابر بودن منابع، یک APT برای یک دلیل و هدف خاص یک سازمان را هدف می‌گیرد. به همین دلیل، این انگیزه احتمالاً باعث می‌شود که حمله سایبری تا زمان رسیدن به آن هدف ادامه پیدا کند و هیچ بازه زمانی مشخصی برای آن وجود نداشته باشد. در صورت مهم بودن هدف ممکن است یک APT برای چند سال روزها، شب‌ها و حتی آخر هفته‌ها کار کند اما تیم‌های قرمز قادر به شبیه‌سازی این ویژگی نیستند.

نامحدود بودن قلمروی فعالیت

محدوده فعالیت یک تیم قرمز یا اجراکننده تست نفوذ، شامل زیرمجموعه‌ای از سازمان است که با ارزیابی آن موافقت می‌شود. این محدوده در اصل یک توافقنامه است که مشخص می‌کند حمله به چه اشخاص یا چه چیزهایی مجاز است. متأسفانه، گروه‌های APT هنگام اجرای حملات سایبری، خودشان را به یک محدوده و قلمروی خاص محدود نمی‌کنند. گروه‌های APT می‌توانند کارهایی مثل هدف گیری افراد یا مدیران خاص را انجام دهند تا به دستگاه‌های کارمندان نفوذ

کرده و امکان اجرای حمله بر علیه سازمان را فراهم کنند. قطعاً چنین فعالیتی خارج از محدوده کار و اختیارات قانونی تیم قرمز قرار دارد. در همین راستا، گروه‌های **APT** می‌توانند از منابع خودشان برای اخاذی از افراد استفاده کنند تا اطلاعات یا دسترسی‌هایی را در اختیارشان قرار دهند که برای نفوذ به سازمان مورد نظر مفید هستند.

همچنین، تیم قرمز و سازمان مشتری آن هم با استفاده از این محدوده‌ها اطمینان حاصل می‌کنند که حین ارزیابی، نفوذی در دستگاه‌های بسیار مهم یا ناپایدار انجام نمی‌شود. بعلاوه، گروه‌های **APT** چنین توافقنامه‌هایی را امضا نمی‌کنند و می‌توانند اکسپلویت‌ها را با وجود احتمال از کار افتادن سیستم‌ها اجرا کنند و حتی سعی کنند به اهداف بسیار ناپایدار نفوذ کنند بدون اینکه نیاز به نگرانی درباره از کار افتادن یا آسیب دیدن سیستم‌ها داشته باشند. در واقع، **APT**ها می‌توانند کارهایی مثل حذف داده‌ها یا حساب‌های کاربری، از کار انداختن دستگاه‌ها یا سرویس‌ها را انجام دهند تا منجر به ایجاد واکنش‌هایی از سمت سازمان هدف شوند که به اجرای حمله سایبری کمک می‌کنند. می‌توان از این کارها برای اجرای موفقیت آمیز مهندسی اجتماعی، دور کردن تمرکز سازمان از فعالیت‌های دیگر یا وادار کردن سازمان به رفتارهایی که امکان نفوذ به اهداف اصلی را فراهم می‌کنند، استفاده کرد. معمولاً چنین رفتارها و امکاناتی در تیم‌های قرمز مشاهده نمی‌شود.

نداشتن قوانین تعامل

محدوده حمله مشخص می‌کند که امکان حمله به چه چیزهایی وجود دارد اما قوانین تعامل (**ROE**[4]) مشخص می‌کنند که تیم قرمز چطور می‌تواند به اهداف مشخص شده حمله کند. این توافقنامه بین سازمان و تیم قرمز یا اجرا کننده تست نفوذ، مشروعیت ارزیابی را مشخص کرده و می‌تواند از سازمان در برابر سهل انگاری‌های فاحش تیم قرمز حفاظت کند. هک کامپیوتر یک فعالیت غیرقانونی است و **ROE** شرایط ارزیابی، مجوزها، دسترسی‌ها و فرایندهای مورد نیاز را برای ارزیابان فراهم می‌کند.

در مقابل، گروه‌های **APT** در حملات سایبری خودشان همواره قانون شکنی می‌کنند و نگران پایبند ماندن به یک **ROE** خاص نیستند. یک گروه **APT**، از هر آنچه برای رسیدن به هدف مفید باشد استفاده می‌کند. قطعاً این کار احتمال موفقیت گروه‌های **APT** را نسبت به تیم قرمز برای نفوذ به سیستم‌ها افزایش می‌دهد چون گروه‌های **APT** محدودیت‌های مشخصی ندارند که

[4] rules of engagement

مشتری‌ها برای آنها تعیین کرده باشند. مهاجمان ATP در مقایسه با تیم‌های قرمز می‌توانند در حملاتشان بر ضد سازمان هدف خلاقانه‌تر و بی‌پرواتر اقدام کنند و استفاده از این واقعیت توسط آنها می‌تواند پیامدهای ویرانگری داشته باشد.

چالش‌های محیطی

صنعت امنیت سایبری و محیط کلی دنیای مدرن که تیم‌های قرمز در آنها فعالیت دارند، موانع جدی و متنوعی برای اجرای موفقیت آمیز تعاملات امنیت تهاجمی ایجاد می‌کنند. این موانع بسیار متنوع و مختلف هستند از فقدان ابتکار و نوآوری گرفته تا تصورات کلی اشتباه این صنعت درباره تیم قرمز.

استانداردهای مقرراتی

استانداردهای مقرراتی می‌توانند به دلیل سختگیری‌هایی که برای فعالیت تیم قرمز در نظر می‌گیرند، مشکل آفرین باشند. بعلاوه، وقتی استانداردی وجود ندارد یا استانداردهای موجود بسیار مبهم و کلی هستند هم امکان ایجاد مشکل وجود دارد. سازمان‌هایی که به دنبال ساختن یک تیم قرمز یا استفاده از امنیت تهاجمی هستند اغلب سیاست‌های سختگیرانه‌ای برای استفاده از داده‌ها دارند و باید حین تعیین چارچوب کلی توافقنامه تعاملات تیم قرمز، به صورت مورد به مورد آنها پرداخت. علاوه بر این، برای کار با برخی از انواع داده‌ها، قوانین صنعتی و کشوری وجود دارند که سازمان‌ها باید آنها را رعایت کنند. به همین دلیل، همه فعالیت‌های تیم قرمز در چنین سازمان‌هایی باید مطابق با سیاست‌ها و قوانین مربوطه انجام شوند. از جمله این داده‌ها می‌توان به اطلاعات سلامت اشاره کرد که توسط قانون HIPAA از آنها حفاظت می‌شود همچنین اطلاعات طبقه بندی شده و هویتی. فعالیت در شبکه‌هایی که داده‌های حفاظت شده خاصی را ذخیره یا جابجا می‌کنند هم می‌تواند برای تیم قرمز محدودیت ایجاد کند چون تیم قرمز باید علاوه بر اجرای درست مأموریت اصلی خودش، به استانداردهای موجود برای حفاظت از این داده‌ها پایبند باشد.

برای مثال فرض کنید - هنگام نفوذ به یکی از میزبان‌های شبکه که حاوی داده‌های HIPAA است - ارزیاب تیم قرمز اطلاعات سلامت افرادی خاص یا حتی افراد مافوق خودش در شرکت را مشاهده می‌کند. از منظر مقرراتی این یک اتفاق وحشتناک است و می‌تواند از نظر روابط محیط کار و تضاد منافع هم مشکل آفرین شود. به ویژه هنگام ارزیابی شبکه‌های طبقه بندی شده، ممکن است ارزیاب‌ها حین اجرای تست اطلاعاتی را جمع آوری کنند که سرجمع کردن آنها

قابلیت طبقه بندی را افزایش دهد یا حتی ممکن است ارزیاب‌ها با مشکلاتی مثل اشتباه در طبقه بندی داده‌ها روبرو شوند که همه این شرایط می‌توانند منجر به بروز یک حادثه امنیتی شوند که حالا باید علاوه بر تعاملات تیم قرمز به این حادثه هم رسیدگی کرد. می‌توان درک کرد که از نظر پایبندی به قوانین چنین استانداردهایی چطور می‌توانند باعث سخت‌تر شدن کار تیم‌های قرمز شوند اما ممکن است این استانداردها نیاز به صدور مجوز یا گواهینامه‌های خاصی را برای اجرای ارزیابی ایجاد کنند. ایجاد چنین محدودیت‌هایی برای حوزه فعالیت تیم قرمز که همین حالا هم از نظر جذب استعداد با چالش روبرو است می‌تواند برای اجرای موفقیت آمیز تعاملات امنیت تهاجمی در یک سازمان محدودیت‌های چشمگیری ایجاد کند.

محدودیت نوآوری

احتمالاً از نظر خیلی از مخاطبان این مطلب، "محدودیت نوآوری" جزء موانع کلی برای تیم قرمز نیست. شاید شما هم این استدلال را مطرح کنید که سازمان یا شرکت شما یک سیستم اختصاصی برای فرایندهای امنیت تهاجمی داشته و همواره در حال ابتکار و نوآوری است. این دیدگاه برای بسیاری از مواقع درست است اما بهتر است کمی بیشتر این موضوع را شفاف سازی کنیم. در این حوزه دائماً شاهد ابتکار و نوآوری هستیم؛ بسیاری از باهوش‌ترین و مستعدترین کارشناسان امنیت در این صنعت فعالیت دارند و هکرها هم - طبق ماهیت کارشان - خلاقانه عمل می‌کنند. با این حال، تعداد شرکت‌ها یا سازمان‌هایی که استراتژی‌های تیم قرمز یا تنظیمات خاص تست نفوذشان را در اختیار دیگران قرار دهند، زیاد نیست. اما این رویکرد قابل درک است چون ممکن است خیلی از شرکت‌ها چنین ابتکاراتی را جزء اسرار تجاری در نظر بگیرند و تیم‌های قرمز درون سازمانی هم آنها را جزء اطلاعات امنیتی مهم تلقی کنند. بنابراین جای تعجب نیست که در رابطه با ارتقای عملکرد تیم قرمز از منظر تجاری و فرایندی، اطلاعات زیادی موجود است. فروشنده‌ها از فروش نسخه‌های جدید ابزارهای امنیتی خودشان راضی هستند اما توضیح نمی‌دهند که هکرهای اخلاقی خودشان چطور شبکه‌ها را هک می‌کنند چون این کار قدرت رقابت آنها را کاهش می‌دهد.

دشواری ارایه ابتکارات آکادمیک واقعی هم نوآوری را محدودتر می‌کند. ما بسیاری از فناوری‌های ارایه شده توسط بخش دانشگاهی برای اتوماسیون یا امنیت تهاجمی را امتحان کرده‌ایم اما هیچ مطالعه‌ای پیدا نشد که توضیح دهد چطور می‌توان مانور تیم قرمز را ارتقاء داد تا به چالش‌هایی که در حال حاضر درباره آنها بحث می‌کنیم، رسیدگی شود. پس از سال‌ها تحقیق و مطالعه برای مقطع دکتری، هیچ نوآوری در زمینه تست نفوذ یا تیم قرمز پیدا نکردم که متمرکز

بر یک ابزار یا یک مدل تحلیل و هدف گیری خاص نباشد. نوشته‌های محدودی درباره یکسری اصلاحات نوآورانه برای مانورهای تیم قرمز نظامی وجود دارد اما نمی‌توان آنها را برای حوزه سایبری به کار بست. همانطور که در فصل دوم هم اشاره شد، دو دلیل وجود دارد. اول اینکه اکثر دانشگاهیانی که پایان نامه منتشر می‌کنند، تجربه امنیت تهاجمی ندارند و اکثر کارشناسان امنیت تهاجمی هم بیشتر نگران پیشرفت حرفه‌ای هستند تا اخذ مدارک رده بالا. دوماً ارزیابی موفقیت یا شکست یک فرضیه در حوزه امنیت تهاجمی به صورت قابل دفاع کار بسیار سختی است چون نیاز به مهارت‌های فنی بسیار بالا و همچنین مشارکت زیاد انسان در فرایند ارزیابی دارد.

این حقایق باعث شده‌اند که اطلاعات کمی درباره نوآوری در فرایندهای تیم قرمز در دسترس باشد. انجمن‌های دانشگاهی هنوز یک مجموعه علمی کامل در این زمینه ندارند و بیشتر افرادی که در این حوزه شاغل هستند، به دلایلی قابل درک تمایلی به انتشار نتایج و اطلاعات کارشان ندارند. این یعنی برای شروع یک عملیات تیم قرمز در سازمان‌ها، باید دانش این کار از افراد مجرب یا از طریق ارزیابی‌های خطرناکی که توسط کارمندان بی‌تجربه انجام می‌شود، جمع آوری شود. حتی اگر موضوع ابتکار و نوآوری را نادیده بگیریم، باز هم عملیات تیم قرمز فعالیتی است که به مرور زمان با شرایط سازمان تطبیق داده می‌شود و حتی افراد مجرب و واجد شرایط هم در طول مراحل ارزیابی و تست درباره سازمان هدف به نکات جدیدی دست پیدا می‌کنند. می‌توان گفت که اجرای یک ارزیابی بهینه توسط تیم قرمز، حاصل ترکیبی کامل از مجموعه مهارت‌های پرسنل، تجربه، تکنیک‌های اطلاعاتی، ابتکارات داخلی و همچنین آشنایی کاری با مجموعه هدف است.

باورهای غلط

در رابطه با عملیات تیم قرمز دیدگاه‌ها و تصورات غلط زیادی وجود دارد اما چند مورد از آنها بر عملکرد کلی امنیت تهاجمی چه توسط یک تیم درون سازمانی و چه توسط فروشنده این راهکارها تأثیر بیشتری دارند. اولین مورد، نبود یک تعریف واضح و درست از ارزیابی تیم قرمز یا تست نفوذ است. همچنین بین ارایه دهندگان این خدمات و مشتریان آنها دیدگاه‌های خطرناک غلطی درباره چنین تعاملاتی وجود دارد.

ممکن است تعریف تیم قرمز یا تست نفوذ کم اهمیت یا بدیهی به نظر برسد اما مشکل اینجاست که دائماً شاهد تغییر و پیچیده‌تر شدن تعریف و تعیین آنچه باید در یک تست انجام شود هستیم. این شرایط از چند جنبه بر امنیت سازمانی و همچنین بر خود این صنعت (به عنوان یک مشکل در اصول کسب و کار) تأثیرگذار است. من با سازمان‌هایی گفتگو کردم که بر اساس

الزامات سیاست امنیتی خودشان نیاز به اجرای ارزیابی در یک بازه زمانی معین داشتند. هر از گاهی مشاهده کردم که چنین سازمان‌هایی درخواست یک اسکن آسیب‌پذیری خودکار را دارند که می‌توان به آن "تست نفوذ" گفت تا بتوانند همزمان با صرفه جویی در منابع و زمان، الزامات تعیین شده در سیاست‌ها را برآورده کنند. همچنین مشاهده شده که برای پیشگیری از تأثیرگذاشتن تست‌های اجباری بر تجهیزات عملیاتی، یک تست نفوذ یا عملیات تیم قرمز غیرتهاجمی (مثل اسکن) انجام می‌شود فقط با این هدف که الزامات قانونی و استانداردها رعایت شده باشند. به غیر از اینکه چنین برچسب گذاری نامناسب است و این روش یک استفاده ضعیف از منابع هک اخلاقی محسوب می‌شود، این احتمال خطرناک را هم به همراه دارد که باعث ایجاد حس امنیت کاذب در سازمان می‌شود. بعلاوه، مشاهده می‌شود که در اثر افزایش تقاضا برای امنیت تهاجمی، ارایه دهندگان این خدمات از افراد کم مهارت‌تر استفاده می‌کنند تا اسکن آسیب‌پذیری را انجام دهند و این خدمات را به عنوان تست نفوذ تبلیغ می‌کنند. این رویکرد هم منجر به ایجاد همان مشکلات و تضعیف وضعیت امنیتی می‌شود.

در این قسمت به بررسی برخی دیدگاه‌های غلط موجود در خود این صنعت می‌پردازیم که کاملاً غیرمنطقی هستند و می‌توانند ماهرترین تیم‌های قرمز را هم با چالش روبرو کنند. اولین دیدگاه نادرست، انتظارات غیرواقع گرایانه است. من در مذاکرات قراردادی مختلفی حضور داشته‌ام که مشتریان در آنها ادعا می‌کنند که خواستار یک چرخه تست نفوذ دو هفته‌ای هستند. همچنین، اغلب این مشتریان انتظار دارند که حمله کوتاه از بیرون سازمان آغاز شود. یک دیدگاه غلط درباره امنیت تهاجمی این است که برای اینکه یک تست نفوذ اطلاعات مفیدی درباره دستگاه امنیتی سازمان ارایه دهد، این فرایند باید از بیرون سازمان شروع شود تا شبیه یک حمله واقعی باشد. من به شخصه شاهد بوده‌ام که برخی همکاران احساس می‌کنند اگر حملات را از بیرون سازمان انجام ندهند، شبیه هکرهای واقعی نیستند. گاهی اوقات در نظر گرفتن این قید برای یک ارزیابی یا حداقل برای بخشی از آن خوب است اما تلاش برای انجام ارزیابی در یک بازه زمانی محدود با در نظر گرفتن این شرط که حمله باید از بیرون سازمان آغاز شود، تأثیری جز افزایش هزینه‌ها ندارد. در بسیاری از مواقع، نفوذ به سازمان از بیرون می‌تواند هفته‌ها یا ماه‌ها زمان ببرد و پس از به دست آمدن این دسترسی‌ها، ارتقای سطح دسترسی و حرکت عرضی درون سازمان با سرعت چشمگیری انجام می‌شود. من به شخصه ترجیح می‌دهم که برای حفاظت از سازمان خودم، آسیب‌پذیری‌های بسیار خطرناک ارتقای سطح دسترسی و حرکت عرضی را شناسایی کنم تا

شناسایی آسیب‌پذیری‌های خارجی محدودی که امکان تشخیص آنها با روش‌های اسکن مناسب وجود دارد.

دیدگاه غلط بعدی این است که شکست جزء گزینه‌ها نیست. واقعیت این است که احتمال شکست خوردن وجود دارد چون ممکن است در بازه زمانی کوتاه تعیین شده برای این کار، کارزارهای مهندسی اجتماعی یا اجرای کد از راه دور با موفقیت انجام نشوند تا هکرهای اخلاقی بتوانند به سازمان نفوذ کنند. در نتیجه، ممکن است گزارش ارزیابی بسیار مختصر و فقط حاوی آسیب‌پذیری‌های کوچک یا اثبات نشده و توضیح تلاش‌های تیم برای به دست آوردن دسترسی‌ها باشد تا حداقل مدیریت سازمان مطلع باشد که قرار است در برابر چه چیزهایی از خود دفاع کند. دیدگاه غلط این است که چنین نتایجی قابل قبول نیستند. این شرایط ناشی از روش طی کردن فرایند ارزیابی است و می‌توان با ابتکار و نوآوری در این فرایندها، آن را تغییر داد.

مشتریان متخاصم

در این قسمت به یکی از چالش‌های واقعی اجرای موفقیت آمیز تعاملات تیم قرمز می‌پردازیم. کار ما به عنوان کارشناس امنیت تهاجمی، با تلاش برای فریب دادن دیگران، پیشی گرفتن از آنها یا شناسایی نقطه ضعف‌های سازمان‌های مشتری خودمان انجام می‌شود و امیدواریم که آنها پس از این کارها و خجالت زده شدن‌شان، همچنان مایل به ادامه همکاری با ما باشند. بعلاوه، ناکامی در گول زدن، دور زدن یا سوء استفاده از مشتریان می‌تواند باعث ایجاد این دیدگاه شود که خدمات ارایه شده کیفیت لازم را نداشته و نباید در آینده باز هم از آن استفاده کرد. از منظر امنیت تهاجمی، در سازمان‌های مشتری سه گروه از افراد وجود دارند که عبارتند از: پرسنل فنی که کار مدیریت و حفظ امنیت سازمان را برعهده دارند، پرسنل مدیریتی که مسئول حفظ رفاه و عملیات سازمانی هستند و پرسنل کاربری.

پرسنل فنی

پرسنل فنی کاربرانی هستند که اختیاراتی فراتر از ایجاد ورودی‌های معمولی برای وضعیت امنیتی سازمان دارند. این گروه شامل مدیران، پرسنل زیرساخت، پرسنل امنیتی و افراد مختلف دیگری است که ارتباط مستقیمی با وضعیت امنیتی کلی سازمان دارند از جمله اشخاصی که در

بخش تضمین اطلاعات[۵] کار می‌کنند. این گروه سه نوع مشکل اساسی برای اجرای موفقیت آمیز مأموریت تیم قرمز ایجاد می‌کنند که همگی مربوط به مسائل خجالت زده شدن و غیرحرفه‌ای بودن هستند که در قالب ترس از دست دادن شغل یا اعتبارشان نمایان می‌شوند. هر سه مثال زیر در ارزیابی‌هایی که من در آنها مشارکت داشته‌ام رخ داده‌اند و البته از خیلی از همکاران هم داستان‌های مشابهی را شنیده‌ام.

هنگام شروع ارزیابی، برخی از پرسنل فنی سعی داشتند مواردی را که واقعاً نیاز به ارزیابی داشتند، از حوزه ارزیابی خارج کنند. این کار معمولاً به این دلیل انجام می‌شود که پرسنل فنی از وجود حفره‌هایی اطلاع دارند که احتمال پیدا شدن آنها وجود دارد یا به این دلیل که رسیدگی به این اهداف جزء مسئولیت‌های مستقیم این پرسنل است و مایل نیستند که روی آنها ارزیابی انجام شود. وقتی چنین اتفاقی رخ می‌دهد، می‌تواند باعث ایجاد یک تقابل در فرایند محدوده بندی شود و در بسیاری از مواقع شخص فنی همان شخصی است که قرار است تعیین محدوده را تأیید کند یا رابطه کاری مستقیمی با تأیید کننده دارد. بنابراین، می‌توان انتظار داشت که در بیشتر مواقع مسئولان ارزیابی در این تقابل شکست بخورند.

حین اجرای فعالیت ارزیابی، مشخص شد که پرسنل فنی ارزیاب‌ها را هدف می‌گیرند. من هم شاهد رخ دادن این اتفاق بودم. یک آدرس منبع به سازمان داده شده بود تا مشخص باشد که فعالیت ارزیابی از کجا منشأ می‌گیرد و پرسنل امنیتی هم از این داده‌ها استفاده کردند تا فعالیت‌های ارزیاب‌ها را در شبکه شناسایی و مهار کنند. چنین مداخله‌هایی می‌تواند باعث ایجاد تردید نسبت به مشروعیت کار مسئولان ارزیابی در مرحله اجرای ارزیابی و گزارش دهی شود چون باعث ایجاد این دیدگاه می‌شود که اگر ارزیابان حین اجرای تست شناسایی شده‌اند، پس مهارت لازم را ندارند. مشاهده شده که گاهی اوقات کارمندان نظارت امنیتی بر اساس امضای ابزارهای مورد استفاده تیم قرمز، تکنیک‌هایی را پیاده سازی می‌کنند که فقط برای گیر انداختن این تیم طراحی شده‌اند - نه تهدیدات امنیتی واقعی. این کار باعث هدر رفتن وقت کارمندان نظارت امنیت و سخت‌تر شدن ارزیابی شبکه خواهد شد. با وجود چنین تعاملاتی، لازم است به مزایای تعاملات تیم بنفش هم توجه داشته باشیم.

ایجاد چنین موانع خصمانه و غیرواقع گرایانه‌ای برای ارزیابی‌های تیم قرمز به نفع هیچ شخصی نیست اما مقابله با چنین شرایطی آسان‌تر است چون تحلیل تنظیمات طراحی شده برای

---

[۵] مترجم: تضمین اطلاعات عمل تضمین اطلاعات و مدیریت ریسک‌های مربوط به استفاده، پردازش، ذخیره و انتقال اطلاعات است.

گیر انداختن تیم قرمز مشخص می‌کند که آیا این قانون به طور ویژه برای گیر انداختن این تیم طراحی شده یا به عنوان یک روش امنیتی واقعی و کلی پیاده سازی شده است.

آخرین و شاید مضرترین شرایط برای اجرای کارآمد ارزیابی‌ها، زمانی است که کارمندان فنی سعی دارند نتایج به دست آمده از یک ارزیابی را کم اهمیت جلوه دهند. بارها مشاهده کردم که پرسنل فنی با تمام تلاش سعی داشتند نشان دهند که یکی از سیستم‌هایی که به آن نفوذ کردیم هیچ اهمیتی نداشته حتی وقتی این سیستم تبدیل به نقطه‌ای برای نفوذ به سایر سیستم‌ها شده است. همچنین گاهی اوقات پرسنل فنی درخواست داشتند که برخی از آسیب‌پذیری‌های شناسایی شده کمتر مورد تحلیل و بررسی قرار بگیرند یا پیش از رسیدن گزارش به دست رئیس، تحلیل و تفسیر آن را تغییر داده‌اند. حتی بعضی از کارمندان گزارش را ویرایش کرده و بعد نتایج را به مدیریت سطح بالاتر ارایه می‌دهند. این اقدامات تأثیری به غیر از کاهش مزایای عملیات تیم قرمز برای سازمان و تحت تأثیر قرار دادن روابط حرفه‌ای ندارند.

پرسنل مدیریتی

مداخله‌های پرسنل مدیریتی شباهت زیادی به مداخله‌های پرسنل فنی دارد و در همان مراحل ارزیابی انجام می‌شود اما با دلایل کمی متفاوت.

بارها مشاهده شده که هنگام تعیین محدوده عملیات تیم قرمز، مدیریت سطح بالاتر سازمان وارد بحث شده و سعی دارند محدوده عملیات و زمان اجرای آن را تا حد ممکن کاهش دهند. معمولاً این کار به این دلیل انجام می‌شود که مثلاً طبق یک استاندارد مقرراتی خاص، باید تعداد مشخصی تست نفوذ در یک بازه زمانی مشخص انجام شود. در چنین شرایطی مدیران سعی دارند در هزینه‌ها صرفه جویی کنند و همزمان الزامات و قوانین را برآورده کنند. من کمتر به این مشکل برخورد کردم تا مشکلات دیگر اما قطعاً باید از این مشکل آگاه بوده و به آن توجه داشت.

روش بعدی مداخله مدیران سازمان در یک تداخل هم به مسئله تعیین محدوده ارتباط دارد. شناسایی یک مجموعه حفره امنیتی در یک سازمان راه خوبی برای جذب سرمایه جهت اصلاح این نواقص است. دیده شده که مدیران محدوده ارزیابی را به سمت بخش‌های خاصی هدایت می‌کنند که نیاز به جذب سرمایه برای آنها دارند به این امید که تیم قرمز یک مجموعه مشکل را پیدا کرده و آنها یافته‌ها را به مدیریت سطح بعدی سازمان گزارش داده و برای رسیدگی به این یافته‌ها بودجه دریافت کنند. این رویکرد تأثیر وحشتناکی بر تعاملات تیم قرمز ندارد اما خوب است که در جریان باشیم این هم جزء دیدگاه‌های رایج مدیرانی است که از منابع تیم قرمز

استفاده می‌کنند. با در نظر گرفتن این نکات، می‌توانید تلاش‌های خودتان را برای انتخاب محدوده عملیات هدفمندتر کنید.

آخرین و شاید جدی‌ترین تأثیر پرسنل مدیریتی بر تعاملات تیم قرمز، در مرحله گزارش دهی مشاهده می‌شود. برخی مواقع، مدیر ارشد سازمان گزارش را دریافت می‌کند اما آن را نادیده می‌گیرد. این اتفاق به دلایل مختلف رخ می‌دهد. اولین دلیل این است که مدیران با اجرای عملیات تیم قرمز وظایف مقرراتی خودشان را انجام داده‌اند و مایل نیستند که برای رعایت توصیه‌های مطرح شده در گزارش‌ها وقت و هزینه صرف کنند. دلیل دوم این است که گزارشات حاصل از تعاملات حوزه امنیت تهاجمی می‌توانند مسئولیت بزرگی برای سازمان داشته باشند.

سناریویی را تصور کنید که در آن تیم قرمز، یک بیمارستان را ارزیابی کرده و ۱۰ آسیب‌پذیری پیدا می‌کند. تیم قرمز با همکاری کارمندان امنیتی سازمان شدت آسیب‌پذیری‌ها و اولویت رسیدگی به آنها را مشخص می‌کند چون کارمندان بیمارستان برای رسیدگی به این مسائل محدود هستند و هر بار فقط می‌توانند روی یک موضوع کار کنند. حالا فرض کنید قرار است ششمین آسیب‌پذیری این فهرست چند ماه بعد رفع شود اما یک مهاجم با استفاده از آن باعث افشای داده‌هایی می‌شود که تحت قانون **HIPAA** حفاظت می‌شوند. یکی از اشخاصی که اطلاعاتش فاش شده شکایت کرده و از دادگاه درخواست می‌کند که بررسی کند آیا بیمارستان ارزیابی‌های امنیتی را انجام داده یا خیر. حالا بیمارستان باید اعلام کند که از چند ماه قبل از وجود این آسیب‌پذیری اطلاع داشته است. از نظر قانون مهم نیست که این آسیب‌پذیری جزء تهدیدات کم اهمیت‌تر برای سازمان در نظر گرفته شده و وجود اسناد گزارش این ارزیابی و داده‌های آن یک مسئولیت بزرگ برای سازمان محسوب می‌شود. صرف نظر از پیامدهای اخلاقی و قانونی، این مثال به خوبی نشان می‌دهد که چرا برخی از مدیران تمام تلاش خودشان را می‌کنند که نتایج تست را نادیده گرفته یا از آن خلاص شوند.

پرسنل کاربری

کاربران معمولی سازمان لزوماً بر فرایند تست تأثیری ندارند اما ممکن است وقتی با نتایج فعالیت یک تیم قرمز روبرو می‌شوند، رفتاری به شدت خصمانه داشته باشند. بنابراین، درک پیامدهای جامعه شناختی تعاملات امنیت تهاجمی ضروری است به خصوص در شرایطی که تیم قرمز از کارمندان درون سازمانی تشکیل شده و احتمالاً اعضای آن با کاربران همکار هستند. در این زمینه مشکلات مربوط به شرمسار شدن کاربران هستند. ممکن است این کاربران اشخاصی باشند که در یک کارزار مهندسی اجتماعی فریب خورده‌اند تا روی لینک‌ها کار کنند یا ایمیل‌های

مخرب را باز کنند و این کار باعث شروع نفوذ تیم قرمز شده باشد. همچنین ممکن است حین اجرای ارزیابی‌ها مشخص شود که یک کاربر خاص هنگام استفاده از سیستم‌های سازمانی برخی از فرایندها یا سیاست‌ها را نقض می‌کند یا اقداماتی غیرقانونی یا نامشروع انجام می‌دهد. یک نمونه از این تخلف‌ها وقتی است که یک تیم قرمز متوجه وجود یک منبع به اشتراک گذاشته شده می‌شود که حاوی فایل‌های صوتی و ویدیویی است که این کار بر خلاف سیاست‌های آن سازمان است و از همین منبع برای نفوذ به سازمان استفاده می‌کند. در این صورت ممکن است پرسنل مسئول این شرایط توبیخ یا حتی اخراج شوند که این اقدامات باعث تشدید روابط خصمانه خواهد شد.

نتیجه‌گیری چالش‌های پرسنل

واضح است که در هر سازمانی، اجرای تعاملات تیم قرمز با مشکلات زیادی در رابطه با افراد همراه است. این مشکلات می‌توانند پیچیده‌تر از یک رابطه فروشنده - مشتری باشند که ایجاد تعامل موفقیت آمیز در آن کار بسیار دشواری است. خوشبختانه، با شناسایی انواع مشکلاتی که احتمالاً پیش رو دارید، داشتن رفتار حرفه‌ای در طول دوره تعامل و قابلیت به تصویر کشیدن شرایط ترسناک، می‌توانید بیشتر این مشکلات را حل کنید بدون اینکه بر کارمندان یا تعاملات تیم قرمز تأثیرگذار شوند. منظور از "به تصویر کشیدن شرایط ترسناک" این است که بتوانیم به یک مدیر یا مسئول نشان دهیم که چطور ممکن است هدف یا آسیب‌پذیری که از نظر پرسنلی با دانش فنی محدودتر، کم اهمیت به نظر می‌رسد منجر به نفوذ به کل سازمان شود. این قابلیت یک مهارت بسیار ارزشمند است که می‌تواند به ارزیابان تیم قرمز برای غلبه بر موانعی که پرسنل سازمانی پیش رویشان قرار می‌دهند، کمک کند. اگر به عقب برگشته و نگاهی به آنچه قبلاً درباره بصیرت هکرهای اخلاقی گفته شد داشته باشید، راحت‌تر درک می‌کنید که چطور ممکن است مشکلات بسیار کوچک بر بخش‌های بزرگی از سازمان هدف تأثیرگذار شوند.

گزینش مؤثر نیرو برای تیم قرمز

بدون شک قبل از روبرو شدن به مشکلات مطرح شده در این فصل، اول باید خود تیم قرمز را تشکیل داد و گزینش نیرو برای تیم قرمز می‌تواند چالش سختی باشد حتی برای سازمان‌هایی که ابزار و هزینه‌های لازم برای استخدام پرسنل مورد نیاز را در اختیار دارند. بنابراین، در ادامه به بررسی مشکلاتی می‌پردازیم که من به عنوان معاون رئیس و اجرا کننده تست نفوذ اصلی یک

شرکت با آنها روبرو شدم. من در این شرکت مسئول تصمیم گیری برای استخدام سایر اعضای تیم تست نفوذ جهت رفع نیازهای مختلف امنیت تهاجمی و تیم قرمز بودم.

رشد سریع و چشمگیر اصطلاح "سایبری" یا "امنیت سایبری" و استفاده از آن توسط افراد مختلف برای رفع نیازهای خودشان در یک سازمان، تأثیر چشمگیری بر صنعت امنیت تهاجمی داشته است. اگر از ۱۰ شخص مختلف بپرسید که امنیت سایبری چه معنایی دارد با ۱۰ پاسخ مختلف روبرو خواهید شد. تنها واقعیت اثبات شده این است که بسیاری از اشخاصی که سابقه مهندسی امنیت، نظارت، تضمین اطلاعات یا مدیریت سیستم‌ها را دارند لقب "کارشناس امنیت سایبری" را دریافت می‌کنند و معمولاً همه سال‌هایی که در حوزه تضمین اطلاعات یا فناوری اطلاعات فعالیت داشته‌اند را جزء سابقه امنیت سایبری خودشان محسوب می‌کنند. این شرایط باعث می‌شود که انتخاب داوطلبان مناسب برای مصاحبه کار سختی باشد. من به شخصه شاهد استفاده از برچسب امنیت سایبری برای اشخاصی با سابقه کار در حوزه تشخیص آسیب‌پذیری و بهره برداری از سیستم‌ها بودم. در کنار این دشواری‌های استخدام کارشناس امنیت سایبری، این واقعیت هم وجود دارد که بسیاری از سازمان‌ها وقتی در اصل به دنبال استخدام یک مهندس امنیت سایبری هستند تا کارهای نظارتی را انجام دهد یا وقتی به دنبال یک تحلیلگر تضمین اطلاعات هستند، مهندس امنیت سایبری را جستجو و استخدام می‌کنند. این ابهام مجموعه مهارت‌ها و نیازها که در صنعت امنیت مدرن و همچنین در صنعت امنیت تهاجمی مشاهده می‌شود، می‌تواند برای تشکیل یک تیم قرمز توانمند مشکل آفرین باشد.

با این فرض که ما درباره پرسنل امنیت سایبری با تجربه کار در حوزه تشخیص و بهره برداری از آسیب‌پذیری‌ها صحبت می‌کنیم، باز هم یک معضل دیگر وجود دارد که باید با آن روبرو شویم. خیلی از سازمان‌ها با نیاز به استفاده از خدمات تیم‌های قرمز آشنایی دارند اما تعداد گزینه‌های واجد شرایط، با صلاحیت، دارای مجوز و مجرب بسیار کمتر از حد مورد نیاز است. معمولاً سازمان‌ها برای پیدا کردن گزینه‌های واجد شرایط با چالش روبرو هستند و پس از پیدا کردن این گزینه‌ها، نگه داشتن و حفظ آنها هم یک چالش دیگر است. احتمالاً برای هر اجراکننده تست نفوذ یا عضو تیم قرمزی فرصت‌های شغلی و دعوتنامه‌های زیادی وجود دارد. کارشناسان مجرب و باصلاحیت حوزه امنیت تهاجمی، در جایگاهی قرار دارند که می‌توانند به سرعت بین شرکت‌ها و مشاغل مختلف جابجا شوند چون این کار تقاضای زیاد و متقاضی کمی دارد. بنابراین حتی اگر سازمانی با موفقیت تیم قرمز را تشکیل دهد، حفظ این نیروها کار چالش برانگیزی است.

مشکل دیگری هم برای پیدا کردن پرسنل مورد نیاز جهت ساختن تیم قرمز وجود دارد که بیشتر مربوط به مسائل قانونی است. هک کردن بدون کسب مجوزهای قانونی لازم یک جرم مهم محسوب می‌شود و بعید است که افراد تجربیات هک معمولی و بدون مجوز خودشان را در رزومه ذکر کنند و این تجربیات جدی گرفته شوند. بنابراین، تنها راه به دست آوردن تجربه واقعی در این حوزه، عضویت در تیم‌های قرمز یا فعالیت به عنوان اجرا کننده تست نفوذ است. معمولاً من برای استخدام افرادی را در نظر می‌گیرم که تجربه کافی در حوزه امنیت یا فناوری اطلاعات داشته باشند و حداقل گواهینامه‌های امنیت تهاجمی را کسب کرده باشند اما این انتخاب همراه با ریسک بود چون کاندیدها، ارزیابی‌های لازم را به شکل حرفه‌ای انجام نداده بودند.

بعلاوه، انتخاب افرادی با تجربه بیشتر منجر به افزایش هزینه‌های استخدام می‌شود. افراد باتجربه در حوزه تست نفوذ یا تیم قرمز، احتمالاً جزء کارمندان ارشد بخش فناور اطلاعات یا سایر صنایع امنیتی هستند و انتظار دریافت دستمزد بیشتری دارند. به همین دلیل، جلب نظر و رضایت سازمانی اهمیت زیادی دارد چون پیدا کردن این افراد سخت و پرهزینه است و معمولاً به راحتی از دست می‌روند.

خلاصه فصل سوم

در این فصل به بررسی وضعیت امروزی امنیت تهاجمی پرداختیم. همچنین در این فصل بسیاری از چالش‌ها و موانع پیاده سازی و استفاده موفقیت آمیز از منابع تیم قرمز بررسی شدند.

• 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.