تیم قرمز حرفه‌ای

انجام تعاملات امنیت سایبری موفقیت‌آمیز

مهدی لقایی
سهیل هاشمی

تیم قرمز حرفه‌ای

- مهدی لقایی
- سهیل هاشمی

تیم قرمز حرفه‌ای

مهدی لقایی
سهیل هاشمی

نام کتاب: تیم قرمز حرفه‌ای

مترجمین: مهدی لقایی، سهیل هاشمی

مشخصات نشر: تهران، انتشارات شیل، ۱۴۰۲

شابک: ۶-۸۰-۵۳۲۲-۶۲۲-۹۷۸

مشخصات ظاهری: ۲۳۱ص

وضعیت فهرست نویسی: فیپا

عنوان اصلی: Professional Red Teaming

مولف: Oakley, Jacob G.

موضوع: computer security

کامپیوتر - ایمنی اطلاعات

data protection

حفاظت داده‌ها

رده بندی کنگره: UB250

رده بندی دیویی: ۳۵۵/۳۴۳۲

شماره کتابشناسی ملی: ۹۳۴۸۴۱۳

سال چاپ: ۱۴۰۲

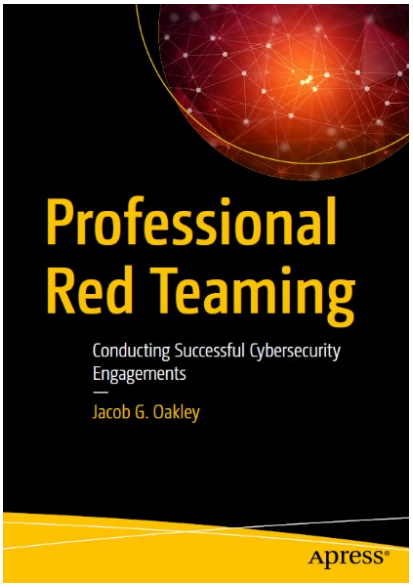
نوبت چاپ: اول

شمارگان: ۳۰۰

تلفن: ۰۹۰۲۱۰۰۱۱۳۱

وب‌سایت: peneter.com

ایمیل: info@peneter.com



سخنی با خوانندگان

از وقتی که یادمان می‌آید، علاقه‌مند به رایانه و بازی‌های رایانه‌ای بودیم. هرچه بزرگ‌تر شدیم، نه تنها که چیزی از این علاقه کاسته نشد، بلکه حل معما برای ما تبدیل به چاشنی پر رنگ آن شد. وارد دنیای بی‌انتهای امنیت شبکه شدیم و اکثر زمان خود را در راستای یادگیری مفاهیم و دست و پنجه نرم کردن با چالش‌های آن گذراندیم. پس از سال‌ها فعالیت و مشاوره‌های خصوصی در زمینه‌ی امنیت شبکه، اکنون که فرصتی برای ادای دین به همگان پیش آمده است، امیدواریم که ماحصل این کتاب برای علاقه‌مندان و دوست‌داران مفید واقع شود و به روشن شدن مسیر در حال پیمودن، کمکی هر چند ناچیز نماید.

ارادتمند شما،

مهدی لقایی

سهیل هاشمی

مقدمه

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 ارزیابی‌های 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.

فهرست مطالب

فهرست مطالب

فهرست مطالب

فهرست مطالب

فهرست مطالب

فهرست مطالب

۱

فصل اول: تیم‌های قرمز در فضای سایبری

مطالب دیجیتال و چاپی بی‌شماری وجود دارند که با توضیح و معرفی ابزارها یا اکسپلویت[1]های جدید، برای نفوذ به سیستم‌های دیجیتال کمک می‌کنند. این متون می‌توانند برای فعالان حوزه امنیت تهاجمی بسیار ارزشمند باشند و به آنها برای ایفای نقش خودشان کمک کنند. بدون شک نشریات شاخصی هستند که به هک اخلاقی کمک می‌کنند اما خیلی از آنها مناسب یک زمان خاص هستند. در واقع یکی از مهم‌ترین دلایل وسعت این مطالعات و کارها این است که هر روزه ابزارها یا کدهای جدیدی نوشته می‌شوند و آسیب‌پذیری‌ها و اکسپلویت‌های تازه‌ای برای بهره برداری شناسایی شده و باعث منسوخ شدن کارهای قدیمی می‌شوند.

سرعت سرسام آور پیشرفت فناوری‌های دفاعی و تهاجمی، منجر به شکل گیری یک نبرد تسلیحاتی شده است. ممکن است بهبود وضعیت امنیتی توسط ابزارهای دفاعی جدیدتر منجر به منسوخ شدن برخی از ابزارهای تهاجمی شود یا اینکه تولید ابزارهای تهاجمی بهتر و کارآمدتر آنها را از رده خارج کنند. ممکن است آسیب‌پذیری‌های مسلح شده با استفاده از تدابیر ابتکاری یا وصله‌های امنیتی خنثی شوند و یا اکسپولیت‌های جدیدتر با احتمال موفقیت بیشتر جای آنها را بگیرند.

با وجود تلاش و توجه بسیار زیادی که برای نوسازی پیوسته ابزارهای امنیت تهاجمی و توضیح جزئیات نحوه استفاده از آنها وجود دارد، باز هم به خود این فرایند حرفه‌ای کمتر توجه می‌شود. ممکن است فردی که به دنبال تبدیل شدن به یک کارشناس امنیت تهاجمی است بلافاصله ده‌ها کتاب مختلف را پیدا کند که شیوه هک سیستم‌ها با استفاده از کد، اکسپلویت و ابزارهای مختلف را آموزش می‌دهند. در مقابل، پیدا کردن مطالبی که نحوه استفاده موفقیت آمیز از این ابزارها و توانایی‌ها را برای بهبود وضعیت امنیت یک مشتری به روشی مثبت و از طریق فرایندهای حرفه‌ای آموزش دهند، کار چالش برانگیزی است.

معمولاً مهم‌ترین چالش‌های هر تعاملی، پیدا کردن و بهره برداری از آسیب‌پذیری‌ها نیستند بلکه چالش‌هایی هستند که در طی چرخه تعامل نمود پیدا می‌کنند. از جمله این موانع می‌توان به مشتریان سخت گیر، قوانین تعامل نامناسب یا محدوده بندی غیر دقیق اشاره کرد. تکنیک‌های امنیتی تهاجمی مثل تست نفوذ یا تیم قرمز منعکس کننده برخی از بهترین ابزارهایی هستند که برای ایمن سازی سیستم‌های اطلاعاتی به کار می‌روند. بنابراین، از نظر من بسیار مهم بود که در حوزه امنیت تهاجمی با ارایه توضیحاتی روایتی و تعیین بهترین اصول قابل استفاده برای تعاملات

[1] exploit

امنیتی تهاجمی حرفه‌ای، مشارکت داشته باشم. این کتاب منبعی برای اشخاصی است که مایل به ورود به این حوزه هستند یا اینکه در این حوزه فعالیت دارند.

برای موضوع و هدف این کتاب، اصطلاح "تیم قرمز" نقش یک عبارت کلی را دارد که به روش‌های امنیتی تهاجمی تیم قرمز و تست نفوذ اشاره می‌کند. از نظر بسیاری از شاغلان این حوزه، تفاوت‌های بین این دو حوزه اهمیت زیادی دارد اما در مجموع اطلاعاتی که در این کتاب ارایه می‌شود برای همه مفید خواهد بود. در این فصل توضیح می‌دهم که تیم قرمز چیست، چطور از آن برای امنیت سایبری استفاده می‌شود، هدف تیم قرمز و مزایا و معایب آن چیست.

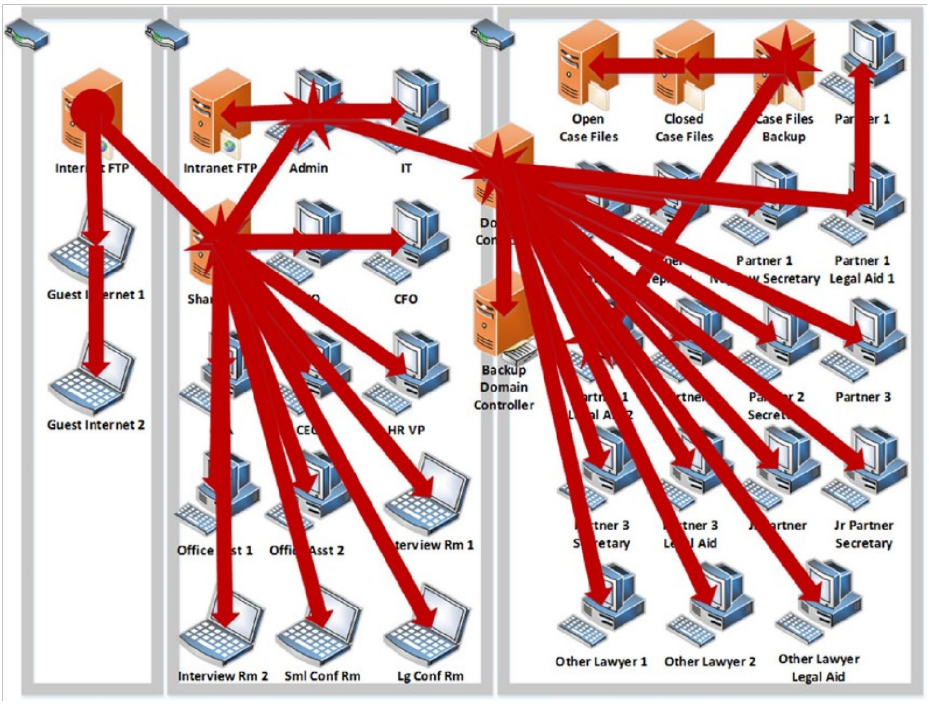
گفته می‌شود که اصطلاح تیم قرمز با جنگ سرد ارتباط دارد؛ زمانی که در حملات آزمایشی بر علیه سازمان‌های تحت حمله شوروی، از یک نیروی "قرمز" استفاده می‌شد که نشان دهنده دشمن بودند. مفهوم شبیه‌سازی حملات برای ارزیابی سازوکارهای دفاعی و واکنشی، مفهومی بسیار قدیمی‌تر است. ممکن است اصطلاح تیم قرمز به حملاتی با ماهیت نظامی اشاره داشته باشد اما این کتاب متمرکز بر به کار بستن این مفهوم شبیه‌سازی حمله در حوزه سایبری است. به غیر از مواردی که به شکل صریح اعلام شده، در این کتاب، تیم قرمز اشاره به تیم قرمز سایبری - یا در کل، تعاملات امنیتی تهاجمی - دارد نه آنهایی که ماهیتی نظامی داشته باشند.

اهداف تیم قرمز

هدف یک تیم قرمز سایبری، شبیه‌سازی حمله بر علیه یک سازمان به منظور ارزیابی سیستم‌های امنیتی و تسهیلات مربوط به آنها است. این تعریف به شدت کلی است و معمولاً اصطلاح "حمله" برای توصیف رفتار تیم‌های قرمز و مهاجمان مخربی که عملکردشان را تقلید می‌کنند بیش از حد تهاجمی و نامناسب است. در خیلی از مواقع، هدف اصلی یک مهاجم دستیابی به اطلاعات یا سرقت آن است. اقدامات مربوط به حمله تهاجمی، بر چنین اهدافی تأثیراتی منفی دارد چون در این سناریوها ممکن است مهاجم سعی کند تا حداکثر زمان ممکن شناسایی نشود. شاید دقیق‌ترین و مناسب‌ترین توصیف برای فعالیت تیم‌های قرمز «شبیه‌سازی دشمن» باشد. هدف این شبیه‌سازی، درک بیشتر قابلیت‌ها و ضعف‌های سازوکارهای دفاع، تشخیص و واکنش در مقابل مهاجمان است.

شبیه‌سازی دشمن توسط تیم‌های قرمز به اشکال مختلف انجام می‌شود و می‌توان آنها را در قالب تلاش برای نفوذ کلی، تلاش برای یک نفوذ خاص یا فرض نفوذ دسته بندی کرد. در نفوذ

کلی، تیم قرمز تمام سطح حمله سازمان هدف را ارزیابی می‌کند با این هدف که تا حداکثر میزان ممکن به آن نفوذ کند (شکل ۱-۱). تلاش برای نفوذ خاص، شامل اقداماتی است که در آنها ارزیابی یک زیرمجموعه خاص از سطح حمله اولویت دارد و سایر بخش‌های سازمان خارج از محدوده تلقی می‌شوند. فرض نفوذ یکی از تعاملات تیم قرمز است که در آن ارزیابی با فراهم کردن امکان دسترسی برای اجرا کننده تست شروع می‌شود با این فرض که مهاجم موفق به نفوذ شده است. هر یک از این انواع تعاملات تیم قرمز چالش‌ها، پیچیدگی‌ها و زیرمجموعه‌های خاص خودشان را دارند و برای سناریوهای خاصی مناسب هستند.



شکل ۱-۱ نفوذ جامع

می‌توان گفت که نفوذ جامع، دقیق‌ترین شکل از شبیه‌سازی طرف متخاصم است چون در این روش هدف نفوذ کامل است و احتمالاً نقطه شروع برای ارزیابان، اینترنت خواهد بود. در این شرایط سازمان واقع گرایانه‌ترین شبیه‌سازی را برای ارزیابی سازوکارهای دفاعی خودش خواهد داشت یعنی ارزیابی تشخیص و واکنش. اما از طرفی این نوع ارزیابی کمترین کارایی دارد و ممکن است منجر به ایجاد نتایجی ناقص شود. اگر در ارزیابی امکان نفوذ به یک بخش خاص از سازمان

به دلیل محدودیت‌های زمانی یا کمبود مهارت وجود نداشته باشد، ممکن است نتایج این تعامل منجر به ایجاد حس امنیت کاذب شود.

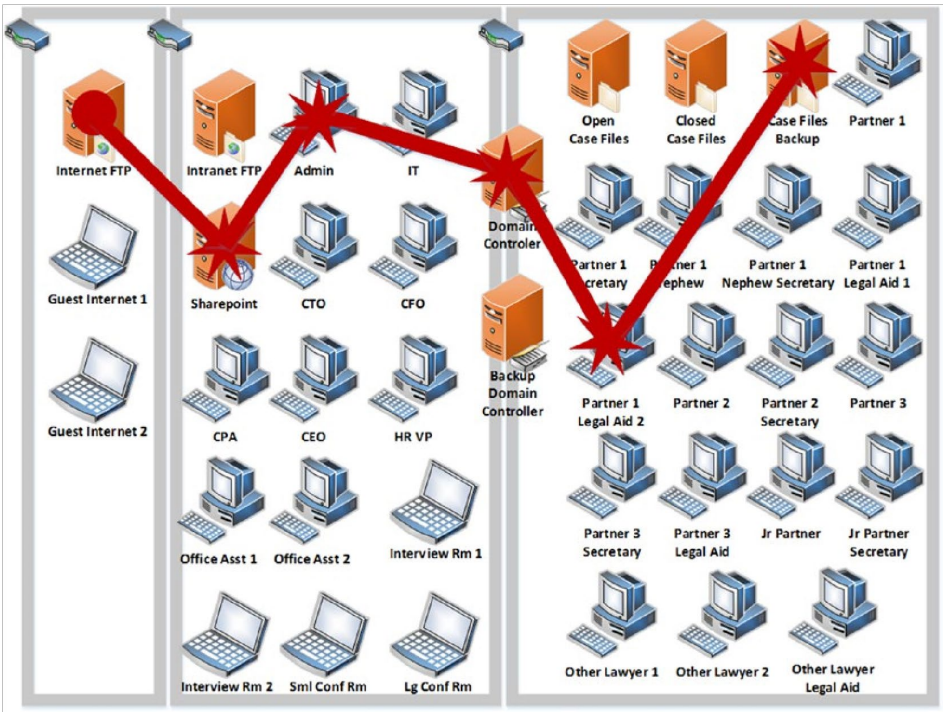
تلاش برای نفوذ جامع را می‌توان به چند زیرمجموعه تقسیم کرد. گرچه در این روش کلیت هدف خود سازمان است، اما معمولاً می‌توان روش‌های انجام حمله را تعیین کرد. مثلاً یک حمله کاملاً جامع حمله‌ای است که در آن هر نوع مسیر حمله‌ای مناسب تلقی می‌شود. ممکن است این مسیرها شامل اتصالات اینترنت، تلاش‌های فیزیکی برای ورود به تشکیلات سازمانی با هدف اجرای حملات سایبری، ایجاد اختلال در زنجیره تأمین و یا بهره برداری از مسیرهای ارتباطی مثل کابل‌های فیزیکی یا شبکه‌های بی‌سیم مورد استفاده سازمان باشند. در بیشتر مواقع، حمله جامع تیم قرمز از طریق یک زیرمجموعه یا یکی از این مسیرها انجام می‌شود. رایج‌ترین روش انجام نفوذ جامع توسط تیم قرمز، هدف گرفتن سازمان فقط با استفاده از مسیرهای متصل به اینترنت است.

تعاملاتی که با هدف ایجاد نفوذ به صورت خاص انجام می‌شوند، روشی کارآمدتر و اختصاصی‌تر برای ارزیابی یک سازمان هستند (شکل ۱-۲). این تعاملات بر خلاف نفوذ جامع، تصویر کلی بالقوه وضعیت امنیتی سازمان را مشخص نمی‌کنند اما می‌توانند منجر به ایجاد اکتشافاتی موفق و - مقابله با - آسیب‌پذیری‌های موجود در زیرمجموعه‌ای از سازمان شوند. مادامی که این زیرمجموعه شامل اولویت بندی مناسب دارایی‌ها[۲] باشد، می‌توان آن را روشی بسیار کارآمد و مؤثر برای اجرای مانورهای تیم قرمز دانست.

برای ارزیابی اهداف مختلف، از زیرمجموعه‌های متفاوتی از نفوذ اختصاصی استفاده می‌شود. می‌توان نفوذ به روش اختصاصی را محدود به یک اپلیکیشن خاص کرد که روی یک دستگاه خاص با سطح دسترسی تعیین شده اجرا می‌شود. اجرای چنین تست‌هایی هنگام انتشار نرم‌افزارهای جدید و مهم در یک سازمان امری رایج است. گرچه این سطح حمله کوچک است اما می‌تواند شامل برخی از بزرگترین ریسک‌هایی باشد که یک سازمان ممکن است با آنها روبرو شود. نفوذ خاص می‌تواند زیرمجموعه‌ای از کاربران، سیستم‌ها یا اپلیکیشن‌های درون سازمان را که اولویت بالایی دارند، شامل شود. انواع و اهداف امنیتی خاص (یا ترکیبی از آنها) که اقدامات تیم قرمز بر آنها تمرکز دارد، فرایند ارزیابی را هدایت می‌کنند.

---

[۲] مترجم: داشته‌های سخت‌افزاری و نرم‌افزاری سازمان



شکل ۱-۲. نفوذ به صورت خاص

تعاملاتی با فرض نفوذ، معمولاً کارایی بیشتری داشته و در عین حال ممکن است تصویری کمتر واقع گرایانه درباره طرف متخاصم ایجاد کنند. اما اگر اجرا و تعیین محدوده چنین تعاملاتی به خوبی انجام شود، می‌توانند مقرون به صرفه‌ترین روش (از نظر هزینه) برای تقویت وضعیت امنیتی باشند.

می‌توان فرض نفوذ را بر اساس انواع دسترسی که ارزیابی از آنها شروع می‌شود و محل آنها درون سازمان دسته بندی کرد. در تلاش برای نفوذ به صورت جامع و یا خاص از روش انتشار بدافزار در سازمان از طریق ایمیل استفاده می‌شود، اما ارزیابی بر اساس فرض نفوذ، با بررسی نوع دسترسی‌های به دست آمده در چنین حمله‌ای، در صورت موفقیت آمیز بودن آن انجام می‌شود. در این حالت، ارزیابی‌های نفوذ می‌توانند نیاز به هفته‌ها انتظار برای باز شدن ایمیلی حاوی یک بدافزار توسط کاربر را از بین ببرند و ریسک‌های حقوقی و اخلاقی بالقوه چنین عملیاتی را دور بزنند. چه در این روش دسترسی برای یک کاربر خاص و چه یک ماشین جدید به سازمان اضافه شود، در هر صورت این روش برای افزایش بهره وری، سطح واقع گرایی را کاهش می‌دهد.

ممکن است در روش فرض نفوذ، آموزش‌های امنیتی کارمندان درباره ایمیل‌های مخرب مورد ارزیابی قرار نگیرند اما عمل کردن با این فرض که بالاخره یک کاربر فریب مهاجمان را خواهد خورد، این امکان را فراهم می‌کند که بیشتر روی شناسایی آسیب‌پذیری‌های خطرناک و قابل بهره برداری وقت صرف شود تا خطاهای انسانی که جزء آسیب‌پذیری‌های همیشه حاضر است.

مزایای تیم قرمز

تعاملات تیم قرمز نسبت به سایر روش‌ها و فناوری‌های مورد استفاده برای بهبود وضعیت امنیتی یک سازمان مزایای خاصی دارند. روش تیم قرمز جزء قوی‌ترین ابزارهای امنیت اطلاعات است. نمی‌توان به راحتی گفت که این روش بهترین روش است یا برای یک شرایط خاص بهترین گزینه محسوب می‌شود اما می‌توان گفت که قوی‌ترین ابزار است. همانطور که قبلاً اشاره شد، مانور تیم قرمز قابلیت شناسایی توانمندی‌ها و کاستی‌های دارایی‌های امنیتی مختلف یک سازمان را دارد و یک ارزیابی منحصربفرد از سطح آمادگی سازمان برای مقابله با تلاش‌های عوامل مخرب فراهم می‌کند. باید توجه داشت که کیفیت این ارزیابی بستگی به عملکرد هکرهای اخلاقی دارد که آن را اجرا می‌کنند و محدودیت عملکرد یا توانمندی ارزیاب‌ها هم بستگی به محدوده و قوانین تعاملی دارد که بر اساس آنها کار می‌کنند. اگر همه چیز متناسب با شرایط باشد، مانور تیم قرمز در مقایسه با استفاده از رویکرد واکنشی برای رسیدگی به نگرانی‌های امنیتی - یعنی پس از اینکه هکرهای مخرب از آنها سوء استفاده کردند - بسیار مقرون به صرفه‌تر است.

مانورهای تیم قرمز ابزاری قوی و تند و تیز محسوب می‌شوند چون حکم یک نوع [چاقوی] جراحی را دارند که اگر در اختیار افراد آموزش ندیده یا غیراخلاقی قرار بگیرند می‌توانند به شدت خطرناک باشند. اما اگر این مانورها توسط یک تیم توانمند اجرا شوند، تنها ابزار قابل استفاده در مرحله پیش از نفوذ و به صورت فعالانه هستند. فناوری‌های زیادی بر اساس مفهوم واکنش طراحی و ساخته شده‌اند اما با مانور تیم قرمز سازمان می‌تواند پیش از شروع اقدام برای نفوذ، وضعیت امنیتی خود را بهبود ببخشد نه پس از آن. شاید این استدلال مطرح شود که فعالیت‌هایی مثل اسکن آسیب‌پذیری و مدیریت درست وصله‌های امنیتی هم حالت واکنشی دارند. اما باید دقت داشت که هر چند این روش‌ها مبتنی بر واکنش به یک رویداد امنیتی در سازمان نیستند اما هر دو واکنش‌هایی به رویدادهای امنیتی در جایی دیگر هستند و اطلاعاتی در رابطه با آسیب‌پذیری‌های جدید فراهم می‌کنند که اسکن یا رفع (آسیب‌پذیری) برای آنها انجام می‌شود.

یکی دیگر از ابزارهایی که از نظر عده‌ای ماهیت منفعل دارد - شکار تهدید - به دنبال شناسایی علائم نفوذ از سمت عاملانی است که در سازمان حضور دارند و ممکن است متجاوز محسوب شوند یا نشوند. اما شکار تهدید بر خلاف مانورهای تیم قرمز جزء فعالیت‌های پس از نفوذ محسوب می‌شود.

ارزیابی آمادگی

مزیت این ویژگی‌های تیم قرمز (یعنی فعال بودن و اجرای آن پیش از نفوذ) این است که میزان آمادگی را مشخص می‌کنند اما سایر ابزارهای امنیتی سعی دارند سازمان‌ها را آماده‌تر کنند. ممکن است این ابزارها سازوکارهای دفاعی سازمان‌ها را برای مقابله با افراد مخرب، نظارت برای شناسایی آنها، مقاومت یا واکنش به آنها آماده‌تر کنند. روش تیم قرمز مشخص می‌کند که آیا این فناوری‌ها برای افزایش سطح آمادگی یک سازمان کارایی دارند یا خیر. همچنین این روش با تشخیص مواردی که شناسایی نشده‌اند و تعیین تکرار غیرضروری تشخیص و ضبط رویدادهای امنیتی توسط فناوری‌های مختلف، به شناسایی منابع اضافه یا اتلاف شده در سازمان کمک می‌کند.

ارزیابی سازوکارهای دفاعی

در یک کارزار تیم قرمز موفق، بسیاری از جنبه‌های دفاعی یک سازمان از طریق تعامل با سیستم‌ها، کاربران و اپلیکیشن‌ها ارزیابی شده و قابلیت این موجودیت‌ها برای مقاومت در برابر اقدامات ارزیابان بررسی می‌شود. نمونه‌ای از یک سیستم دفاعی در یک سازمان، فایروال است. این سیستم برای پیشگیری از حرکت ترافیک ناخواسته یا مخرب از نقطه‌ای به نقطه دیگر در سازمان ساخته شده است. تیم قرمز، فایروال را به هر دو روش مستقیم و غیرمستقیم ارزیابی می‌کند. ارزیابی غیرمستقیم یک موجودیت دفاعی مثل فایروال، به‌واسطه اسکن و سایر فعالیت‌های اکتشافی در سیستم یا سرویس‌هایی انجام می‌شود که قرار بوده این فعالیت‌ها در آنها متوقف شوند اما فایروال به دلایلی مثل پیکربندی نادرست یا وجود نقص در خود سیستم، اجازه عبور آنها را داده است. در هر صورت، آمادگی دفاعی سیستم فایروال بدون اینکه ارزیاب مطلع باشد که قرار است جلوی اقداماتش گرفته شود، انجام می‌شود. ارزیابی مستقیم حالتی است که در آن فرد ارزیابی کننده، آگاهانه سعی می‌کند از یک سازوکار دفاعی عبور کند. این تلاش می‌تواند در گروه بهره برداری‌های خرابکارانه یا بهره برداری‌های مستقیم قرار بگیرد.

بهره برداری خرابکارانه زمانی انجام می‌شود که ارزیاب با دستگاه آشنایی دارد و سعی دارد با استفاده از نقایص خاص آن یا پیدا کردن پیکربندی‌های اشتباهی که اجازه عبور را به او می‌دهد،

قابلیت‌های دفاعی دستگاه را دور بزند. بهره برداری مستقیم وقتی انجام می‌شود که ارزیاب از یک نقص یا پیکربندی اشتباه در سیستم استفاده می‌کند تا امکان اجرای کد از راه دور را به دست آورد و با تغییر تنظیمات امنیتی دستگاه، به آن نفوذ کند.

می‌توان سایر انواع اهداف امنیت دفاعی را به همین صورت ارزیابی کرد. ممکن است یک سیستم‌عامل تنظیمات دفاعی خاصی داشته باشد که از اجرای اسکریپت‌های زمان بندی شده با یک سطح دسترسی خاص جلوگیری می‌کند. وجود یک نقص در پیاده سازی این تنظیمات به تیم قرمز اجازه می‌دهد تا اسکریپت را با همان سطح دسترسی اجرا کند. یا ممکن است تیم قرمز با استفاده از یک روش اجرای کد که سیستم‌عامل توانایی رسیدگی به آن را ندارد یا با نفوذ به سیستم‌عامل و تغییر تنظیمات آن، فعالانه به دنبال دور زدن مکانیزم دفاعی باشد. این حالت در سطح اپلیکیشن هم وجود دارد. ممکن است یک ارزیاب خواسته یا ناخواسته باعث دور زدن اعتبارسنجی مقادیر ورودی برای یک فیلد در یک اپلیکیشن شود یا ممکن است دسترسی مدیریت اپلیکیشن را به روش‌های دیگر پیدا کرده و اعتبارسنجی ورودی را تغییر دهد تا بتواند یک کار خاص را انجام دهد. این اصول ارزیابی آمادگی سازوکارهای دفاعی در یک سازمان، محدود به اهداف امنیتی تکنولوژیکی نیستند. باید کارمندان سازمان را هم جزء اهداف امنیت دفاعی در نظر گرفت و هر زمان ممکن بود آنها را هم در ارزیابی‌های تیم قرمز پوشش داد. کارمندان در صورت در اختیار داشتن آموزش‌ها و روش‌های کارآمد می‌توانند با کارهایی مثل باز نکردن ایمیل‌های مخرب، پیشگیری از "دزدکی نگاه کردن" به اطلاعات مهم روی صفحه نمایش از پشت سرشان و یا عبور افراد غیرمجاز از درب‌های امنیتی پشت سر خودشان، قابلیت‌های دفاعی را تقویت کنند. تشخیص نقطه ضعف‌های موجود در امنیت دفاعی کارمند-محور می‌تواند یکی از ارزشمندترین یافته‌های یک ارزیابی باشد.

ارزیابی سیستم‌های نظارتی

ارزیابی شیوه نظارت یک سازمان بر فعالیت‌های مخرب هم در تعیین میزان آمادگی امنیتی سازمان نقش دارد. نظارت بر فعالیت‌های مخرب در یک سازمان، با یک فرایند دو مرحله‌ای شامل تشخیص و ایجاد هشدار انجام می‌شود. مانورهای تیم قرمز امکان تشخیص محل تخلف در دستگاه‌های نظارتی را فراهم می‌کند. این تخلف می‌تواند تکنولوژیکی و/یا رویه‌ای باشد و هر دو می‌توانند شامل فعالیت‌های دستگاه‌ها و کارمندان باشند. تعیین اینکه سیستم نظارتی در

تشخیص تخلف یا صدور هشدار شکست خورده و اینکه تخلف بر اساس خلأهای امنیتی بوده یا رویه‌ای، برای رسیدگی به مشکلات نظارتی و رفع آنها ضروری است.

تشخیص به شناسایی یک رویداد امنیتی درون یک سازمان گفته می‌شود. رویدادهای امنیتی می‌توانند بسیار متفاوت باشند مثل ثبت تصویر ورود شخصی به یک ساختمان توسط یک دوربین امنیتی یا ارسال یک ایمیل از شبکه به یک آدرس خاص. تعاملات متفاوت تیم قرمز منجر به ایجاد رویدادهای امنیتی متفاوتی می‌شوند و بنابراین مکانیزم‌های تشخیص متفاوتی را درون سازمان ارزیابی می‌کنند. تشخیص رویدادهای امنیتی هم مثل اهداف امنیتی دفاعی به روش خرابکارانه یا مستقیم قابل انجام هستند.

ایجاد هشدار بخش بعدی کار دستگاه نظارتی است و تمرکز آن اتفاقات پس از تشخیص یک رویداد امنیتی است. ممکن است این مرحله هشداردهی قابل چشم پوشی باشد مثل نادیده گرفتن رویداد امنیتی و عدم ثبت گزارش یا بغرنج باشد مثل ارتقای سطح فعالیت قابلیت‌های دفاعی بر اساس هشداری که منجر به شروع یک فعالیت پیگیری می‌شود. علاوه بر همان اصولی که پیش از این برای قابلیت‌های تشخیص و دفاعی گفته شد، ارسال هشدار یک روش جدید به فرایند ارزیابی اضافه می‌کند. می‌توان هشداردهی را با استفاده از تست مستقیم و غیرمستقیم ارزیابی کرد اما می‌تواند شامل یک نوع سوم از تست هدفمند هم باشد. بهره برداری خرابکارانه به ارزیاب امکان می‌دهد که از ایجاد هشداری مناسب برای رویداد شناسایی شده، جلوگیری کند. در بهره برداری مستقیم، ارزیاب هشداردهی مناسب را غیرفعال می‌کند.

سومین نوع از تست هدفمند، بهره برداری از شواهد است. این حالت وقتی صورت می‌گیرد که یک رویداد با موفقیت شناسایی شده و یک هشدار مناسب برای آن ایجاد شده اما صحت هشدار یا شواهد هشدار تغییر کرده باشد. گاهی اوقات این کار شامل بهره برداری مستقیم از سیستم برای حذف هشدارها است که می‌تواند شامل گزارش رویدادهای سیستم، پنجره‌های پاپ-آپ یا کل فایل‌ها باشد. دلیل اینکه چنین فعالیتی به طور کامل در محدوده بهره برداری مستقیم یا غیرمستقیم قرار نمی‌گیرد این است که در بسیاری از موارد، هشدارها بخشی از یک دستگاه نظارتی به شدت توزیع شده هستند و ممکن است سوء استفاده مستقیم از یک سیستم خاص منجر به حذف همه نسخه‌های شواهد هشدار نشود.

سیستمی را در نظر بگیرید که حاوی تعداد مشخصی گزارش رویداد است تا وقتی که شروع به نوشتن رویدادهای جدید بر روی قدیمی‌ترین رکوردها می‌کند یا سیستمی که هر زمان فقط قادر به ثبت تعداد خاصی از رویدادها است. امکان سوء استفاده از روش ضبط شواهد هر دو

سیستم وجود دارد. ارزیاب می‌تواند تعداد زیادی نویز ایجاد کند تا از ایجاد یک هشدار خاص جلوگیری کند یا به دلیل حجم بالای رکوردهای تولید شده، باعث نوشته شدن گزارش‌های جدید روی قدیمی‌ترین گزارش‌ها شود. این بهره برداری از سیستم ثبت شواهد می‌تواند باعث ثبت اطلاعات غلط برای یک هشدار شود مثل جعل آدرس منبع ترافیک مخرب. بهره برداری از شواهد می‌تواند شامل ایجاد یک هشدار مثبت کاذب بسیار جدی‌تر هم شود تا از توجه سیستم نظارتی به هشدارهایی که مربوط به فعالیت‌ها و اهداف واقعی ارزیاب هستند، جلوگیری کند.

ارزیابی واکنش‌ها

آخرین بخش از ارزیابی آمادگی توسط تیم‌های قرمز، مربوط به واکنش سازمان به فعالیت‌های ارزیابی است. واکنش بر اساس هدف و محدوده تست در سطوح مختلفی انجام می‌شود. در برخی از سناریوهای تیم قرمز اگر فعالیت ارزیان شناسایی شود، اولین گام کارمندان امنیتی هماهنگی با مدیر عملیات تیم قرمز است تا مشخص شود که فعالیت موردنظر مربوط به یک عامل تهدید مخرب واقعی بوده یا خود تیم قرمز. پس از مشخص شدن اینکه این کار توسط تیم قرمز انجام شده، ممکن است کارمندان بخش امنیت واکنش را متوقف کرده و اجازه دهند که تیم قرمز بدون مانع کار خود را ادامه دهد. این راحت‌ترین پیاده سازی از تحلیل واکنشی در تعاملات تیم قرمز است اما از نظر تهاجمی بودن هم در پایین‌ترین سطح قرار دارد. تشخیص تهدید توسط کارمندان امنیتی و اطلاع از اینکه تیم قرمز مسئول آن نبوده، منجر به رسیدن به درکی سرتاسری از میزان آمادگی سازمان برای واکنش به آن نوع تهدید مخرب خاص نمی‌شود.

کامل‌ترین سناریو حالتی است که کارمندان امنیت به محض اطلاع از فعالیتی بالقوه مخرب، مثل یک تهدید واقعی نسبت به آن واکنش نشان می‌دهد. در این حالت، تیم قرمز سعی می‌کند از کارمندان امنیتی پیشی گرفته و فعالیت‌های آنها را بی‌اثر کند. این روش شامل تلاش‌های دفاعی برای پاکسازی ماشین‌های آلوده و همچنین تلاش‌هایی برای خنثی کردن مکانیزم‌های شکار تهدید است. ریسک این روش این است که ممکن است حضور تیم قرمز با دور کردن تمرکز تیم امنیت سایبری از فعالیت‌های مخرب واقعی در شبکه، باعث ایجاد نگرانی‌های امنیتی شود. حد واسط بین توقف فوری واکنش و واکنش کاملاً ناآگاهانه به فعالیت‌های تیم قرمز، ارزیابی بهینه سازمان است و باید متناسب با نیازهای خاص ارزیابی انجام شود.

به غیر از ارزیابی آمادگی سازمان برای واکنش به تهدیدات مخرب، تیم قرمز این مزیت را دارد که به تقویت دفاعی سازمان کمک می‌کند. نه تنها تیم قرمز مشکلات موجود در دفاع، نظارت و

واکنش را شناسایی می‌کند بلکه به اصلاح و رفع آنها و شکار تهدید هم کمک می‌کند. اجرای درست ارزیابی توسط تیم قرمز، پس از شناسایی مشکلات سازمان مورد نظر، راهکارهای لازم را برای رفع آسیب‌پذیری‌ها، اصلاح پیکربندی‌ها یا مشکلات رویه‌ای ارایه می‌دهد.

بسیاری از کارشناسان امنیت تهاجمی مسیر حرفه‌ای خودشان را به عنوان مهندس سیستم‌ها، مدیر یا توسعه دهنده شروع کرده و سپس از تجربه و تفکر هکری برای کمک به اصلاح نقطه ضعف‌های امنیتی سازمان استفاده می‌کنند. بسیار بهتر است که این کارشناسان درباره روش اصلاح و رفع آسیب‌پذیری‌ها با مسئولان پیاده سازی آنها در سازمان مثل مدیران یا پرسنل امنیتی گفتگو کنند. اغلب مواقع طرز فکر یا عملکرد یک مهاجم در ایده‌های این افراد برای حل یک مسئله، در نظر گرفته نمی‌شود. مشارکت دادن تیم قرمز در تعیین اقدامات اصلاحی به صرفه جویی در زمان و رسیدگی کارآمدتر به یافته‌های امنیتی کمک می‌کند. بعلاوه، بهتر است که پس از انجام اصلاحات، از تیم قرمز برای یک ارزیابی مختصر دعوت کرد تا مشخص شود که در این اصلاحات به خوبی به یافته‌های ارزیابی اولیه رسیدگی شده است یا خیر.

می‌توان برای مقابله با تهدیدات هم از نظرات تیم قرمز استفاده کرد - چه از گزارش‌های این تیم و چه از گفتگوهایی که با کارمندان بخش امنیت دارند. ممکن است با وجود راهکارهایی برای یکی از یافته‌های خاص تیم قرمز، امکان رسیدگی کارآمدتر یا ارزان‌تر به آن با روش‌های دیگر وجود داشته باشد مثل تغییر در تنظیمات یا پیکربندی‌هایی که تأثیر آسیب‌پذیری را خنثی می‌کنند. یافته‌های تیم قرمز به روش‌های دیگر هم برای کارمندان امنیتی مفید هستند. مثلاً ممکن است یک اسکن آسیب‌پذیری منجر به پیدا کردن یافته‌هایی در برخی از ماشین‌های کم هزینه مورد استفاده یک سازمان شود اما مدیر سازمان اجازه رسیدگی به این یافته‌ها را به کارمندان امنیت ندهد. با توجه به کم هزینه بودن ماشین‌های آسیب‌پذیر، ممکن است سازمان تصمیم بگیرد در صورت تشخیص نفوذ آنها را جایگزین کرده یا تغییر قالب دهد. تعاملات تیم قرمز می‌تواند به کارمندان امنیت نشان دهد که چطور ممکن است یک مهاجم با استفاده از همین دستگاه‌های کم هزینه کل شبکه سازمان را دچار مخاطره کند. به این ترتیب ممکن است مدیریت سطح بالاتر سازمان درباره ادامه استفاده از این سیستم‌ها تجدیدنظر کند.

معایب تیم قرمز

بحث و گفتگو درباره استفاده از تیم‌های قرمز بدون بررسی چالش‌ها و معایب این روش بحثی ناقص است. همانطور که پیش از این اشاره شد، تیم قرمز قوی‌ترین ابزار موجود در زمینه امنیت

اطلاعات است اما ممکن است برای برخی شرایط بهترین روش نباشد. پیاده سازی مانورهای تیم قرمز با پیچیدگی‌های خاصی همراه است حتی اگر به صورت اصیل انجام شوند. مانور غیراصیل (غیر ارگانیک) تیم قرمز، مانوری است که توسط افرادی خارج از سازمان اجرا می‌شود که ممکن است به دلیل فقدان استانداردها و شفافیت، قابل اعتماد یا قابل دفاع نباشد. بعلاوه، ممکن است مانورهای تیم قرمز منجر به ایجاد روابطی پایدار یا خصمانه در محیط کار شود و گزارش حاصل از آن هم مسئولیت‌های بزرگی به همراه داشته باشد.

مسائل زیادی باعث سخت‌تر شدن انجام موفقیت آمیز تعاملات تیم قرمز می‌شوند. برخی از این مسائل قابل اجتناب هستند و برخی دیگر را باید به عنوان هزینه انجام این کار قبول کرد. اجرای مانور تیم قرمز درون سازمان یا استفاده از خدمات بیرونی برای انجام این کار هزینه زیادی دارد. یکی از دلایل مهم هزینه‌های بالای این روش این است که در حال حاضر نیروی متخصص کمی در این حوزه وجود دارد. بعلاوه پیدا کردن هکرهای قابل اعتمادی که قدرت قضاوت خوبی داشته باشند هم سخت است. از آن سخت‌تر پیدا کردن هکرهای با استعداد و قابل اعتمادی است که توانایی برقراری رابطه با دیگران (مثل کارمندان بخش امنیت) را داشته باشند و با مدیران شرکت که قرار است به یافته‌های این هکرها رسیدگی کنند، به خوبی ارتباط برقرار کنند. بنابراین، همانطور که اشاره شد، اجرای عملیات تیم قرمز به صورت حرفه‌ای هزینه‌بر است و بسیاری از سازمان‌ها قادر به حفظ این نیروها نیستند در نتیجه از خدمات برون سازمانی استفاده می‌کنند.

استفاده از خدمات شرکت‌های بیرونی هم برای اجرای مانورهای تیم قرمز بدون مشکل نیست. باز هم این کار برای سازمان میزبان هزینه‌بر است. در چنین شرایطی احتمال قطع چرخه حیات تیم قرمز وجود دارد و تعاملات در حد ۲ تا ۴ هفته حفظ می‌شوند. به خصوص در مواقعی که سازمانی نیاز به برآورده ساختن الزامات امنیتی یا حسابرسی دارد، اما بودجه کافی برای انجام این کار را ندارد، این مشکل ایجاد می‌شود. استفاده از کوتاه‌ترین تعاملات ممکن با یک تیم قرمز برون سازمانی برای صرفه جویی در هزینه‌ها منجر به ایجاد یافته‌هایی غیرقابل اعتماد می‌شود. هر چقدر که ارزیاب‌ها با استعداد باشند باز هم احتمالاً یک تعامل یک هفته‌ای با تیم قرمز برای بررسی همه مسائل کافی نیست و ممکن است در سازمان مشتری حس امنیت کاذب ایجاد کند. بعلاوه، معمولاً به دلیل مسائل رقابتی و برای حفظ اسرار تجاری، اطلاعات مربوط به ابزارها و روش‌های مورد استفاده تیم قرمز فاش نمی‌شوند و این مسئله مانع از حفظ خدماتی قابل دفاع و استاندارد می‌شود.

با این فرض که بودجه لازم برای تشکیل یک تیم قرمز با استعداد درون خود سازمان یا استفاده از خدمات حرفه‌ای تیم قرمز برون سازمانی وجود داشته باشد، باز هم محدودیت‌هایی برای موفقیت چنین تعاملاتی وجود دارد که ناشی از مسائل حقوقی و قراردادی هستند. ممکن است تعاملات تیم قرمز شامل دستگاه‌هایی باشند که اطلاعات درون آنها بر اساس قوانین و مقررات حفاظت شده‌اند [مثل قانون قابلیت انتقال و مسئولیت بیمه سلامت (HIPAA[3])] یا حاوی اطلاعات اقتصادی و هویتی باشند. افرادی که این تعاملات را اجرا می‌کنند باید از قوانین مربوط به چنین داده‌هایی آگاه باشند و در برخی موارد لازم است گواهینامه‌های خاصی برای کار با این داده‌ها داشته باشند.

به غیر از مسائل حقوقی، الزامات قراردادی هم می‌توانند باعث پیچیدگی هر چه بیشتر فرایندهای تیم قرمز شوند. خیلی از سازمان‌ها سعی دارند به طور جزئی یا کامل از خدمات زیرساخت ابر استفاده کنند. تقریباً در همه موارد، ارایه دهندگان چنین خدماتی توافقنامه‌های کاربری خاصی دارند که مانع از اجرای فعالیت‌هایی مثل مانورهای تیم قرمز در سیستم‌های محیط ابر آنها می‌شود. در برخی موارد، می‌توان مجوزهای خاصی کسب کرد که امکان اجرای تست را در این محیط‌ها فراهم می‌کنند اما خیلی از سازمان‌های مشتری از وجود چنین مجوزهایی آگاه نیستند. اگر از همان ابتدا راجع به این مسئله با مشتری صحبت نشود، ممکن است بعداً فعالیت‌های تیم باعث غیرفعال شدن برخی از سرورهای مشتری در محیط ابر یا قرار گرفتن آنها در لیست سیاه شده و منجر به از دست رفتن داده‌ها یا سود مشتری شود. بدتر اینکه ممکن است چنین فعالیتی تعهدات قراردادی بین مشتری تیم قرمز و خدمات میزبانی ابر را نقض کرده و باعث شوند که ارایه دهنده این خدمات با مشتری تیم قرمز قطع همکاری کند. حتی اگر اجازه تست و ارزیابی سیستم‌های میزبانی شده در محیط ابر وجود داشته باشد، باز هم خیلی از خدمات زیرساخت ابر به طور مرتب آدرس سیستم‌های خودشان را تغییر می‌دهند. ممکن است یک روز یک آدرس مربوط به مشتری تیم قرمز باشد اما روز بعد متعلق به یک شرکت دیگر باشد. در چنین شرایطی تیم قرمز ناخواسته در حال تلاش برای هک غیرقانونی یک سازمان ناشناس خواهد بود. موارد ذکر شده از جمله مثال‌هایی بودند که نشان می‌دهند چرا باید هنگام اجرای فعالیت‌های تیم قرمز دقت و مراقبت بسیار زیادی داشت.

اگر مانورهای تیم قرمز به درستی انجام شوند، در مرحله‌های پس از ارزیابی یعنی زمانی که گزارش یافته‌ها تهیه می‌شود هم مراقبت و حرفه‌ای گری زیادی وجود خواهد داشت. یکی از

[3] Health Insurance Portability and Accountability Act

دشوارترین مسائلی که باید در تعاملات تیم قرمز به آن پرداخت، وجود پرسنل متخاصم بین نیروهای امنیتی است. ترس از خجالت زده شدن یا حتی از دست دادن شغل در اثر یافته‌های تیم قرمز می‌تواند باعث شود که برخی از کارمندان در هر مرحله برای تیم قرمز مانع ایجاد کنند. ممکن است در مرحله تعیین محدوده و قوانین تعامل، این افراد فعالیت یک تست را طوری محدود کنند که مانع از ارزیابی سیستم‌های حیاتی شود. در مرحله اجرای تست ممکن است این افراد سعی کنند از فناوری‌های دفاعی و نظارتی خاصی استفاده کنند که فقط مانع از موفقیت تیم قرمز می‌شوند اما تأثیری در وضعیت امنیتی سازمان ندارند. نمونه‌ای از این مسئله وقتی است که یک کارمند امنیتی با ابزارهای مورد استفاده تیم قرمز آشنایی دارد، همه سیستم‌ها را برای پیدا کردن امضاهای مرتبط جستجو کرده و هر بار، فعالیت تیم قرمز را علامت گذاری می‌کند. اگر هکرهای واقعی از این ابزارها استفاده نکنند، این کار هیچ تأثیر واقعی بر امنیت سازمان نخواهد داشت و فقط مانع از اجرای ارزیابی‌های تیم قرمز می‌شود.

بعلاوه، اگر آدرس منبع تیم قرمز حین تعیین قوانین تعامل فاش شود، ممکن است کارمندان امنیتی همه ترافیک ارسال شده از سمت آن آدرس را مسدود کنند تا مانع از اجرای موفقیت آمیز ارزیابی‌ها شوند. در نهایت، ممکن است یک فرد متخاصم سعی کند در تعامل با مدیران سطح بالاتر سازمان برای حفظ وجه خودش، یافته‌های تیم قرمز را کم اهمیت‌تر جلوه دارد. شاید چنین رفتارهایی بعید و عجیب به نظر برسند اما وقتی مردم باور داشته باشند که وسیله معاش و شغل‌شان در خطر است، برای حفاظت از آن هر کاری خواهند کرد.

تیم‌های قرمز باید حرفه‌ای و با سیاست عمل کنند طوری که کارمندان امنیتی سازمان در موضع دفاع از خودشان قرار نگیرند. این مشکلات در همه مراحل ارزیابی ایجاد می‌شوند - از مرحله برنامه ریزی تا اجرا و گزارش دادن نتایج ارزیابی. باید بین پرسنل امنیتی و تیم قرمز روابط کاری خوبی برقرار و حفظ شود.

یکی دیگر از معایب بالقوه تیم قرمز، خود گزارش است. معمولاً احتمال اینکه این بخش از ارزیابی امنیتی تهاجمی پیامدهایی منفی داشته باشد بسیار کم در نظر گرفته می‌شود. گزارش تیم قرمز، فهرست یافته‌هایی را مشخص می‌کند که سازمان را در معرض تهدید قرار می‌دهند و این فهرست می‌تواند مسئولیت‌های زیادی داشته باشد. فرض کنید یک بیمارستان سرویسی را برای اجرای تعاملات تیم قرمز استخدام می‌کند. تیم قرمز، ۱۰ یافته بالقوه آسیب‌پذیر را پیدا می‌کند که مدیران سازمان آنها را تأیید کرده و بر اساس تأثیر اولویت بندی می‌کنند. مدیران از کارمندان

بخش امنیت درخواست می‌کنند که بر اساس اولویت به این آسیب‌پذیری‌ها رسیدگی کنند. فرض کنید که تا ۶ ماه به ۶ مورد از یافته‌ها رسیدگی نمی‌شود اما آسیب‌پذیری‌هایی با الویت بالا رفع می‌شوند. در ماه پنجم، یک هکر از ششمین یافته فهرست استفاده کرده و به یک پایگاه داده بیمارستان که پر از داده‌های هویتی و داده‌های مشمول قانون **HIPAA** است، نفوذ می‌کند. این رخنه فاش شده و چند بیمار از بیمارستان شکایت می‌کنند. در پیگیری‌های قانونی از بیمارستان درخواست می‌شود که ثابت کند تمرین‌های تیم قرمز را به طور منظم اجرا کرده و یافته‌های خودش را نشان دهد. سپس مشخص می‌شود که آسیب‌پذیری مورد استفاده برای دسترسی به داده‌های بیماران، از ماه‌ها قبل برای بیمارستان مشخص بوده است. با اینکه بیمارستان بر اساس میزان اهمیت به یافته‌ها رسیدگی کرده، حالا برای این رخنه مسئول شناخته می‌شود چون وجود آسیب‌پذیری در گزارش تیم قرمز مشخص شده بود. نباید این موارد و سایر مسائل و معایب تیم قرمز مانع از به کار بردن این خدمات شود اما کارشناسان تیم قرمز و افرادی که قصد استفاده از آنها را دارند، باید از این مسائل آگاه باشند.

خلاصه فصل اول

در این فصل مفهوم تیم قرمز و هدف اجرا و پیاده سازی عملیات تیم قرمز را توضیح دادیم. همچنین مزایا و معایب استفاده از این رویکرد امنیتی دفاعی هم بررسی شد تا مقدمه لازم برای درک فصل‌های بعد فراهم شود.

• 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.