تیم قرمز حرفه‌ای

- مهدی لقایی
- سهیل هاشمی

فصل پنجم: قوانین تعامل

فهرست مطالب

۵

فصل پنجم: قوانین تعامل

پس از تکمیل مرحله تشکیل محدوده که در آن "آنچه" قرار است ارزیابی شود مشخص می‌شود، قوانین تعامل (ROE[1]) "چگونگی" انجام این کار را تعیین می‌کنند. مشروعیت و قانونی بودن همه اقدامات تیم قرمز در ارزیابی‌ها، بر اساس سند **ROE** تعیین می‌شود. سند **ROE** باید به درستی تنظیم شده و مورد توافق قرار گرفته باشد. همچنین باید ارایه دهنده خدمات و مشتری هر دو از آن اطلاع یافته و آن را امضاء کرده باشند. در غیر این صورت، عملیات امنیت تهاجمی که توسط هکرهای اخلاقی انجام می‌شود، نقض قانون کلاهبرداری و سوء استفاده‌های کامپیوتری (CFAA[2]) محسوب می‌شود که در آمریکا جزء جرایم فدرال است و در سایر کشورها هم قوانین مشابهی برای مقابله با آن وجود دارد. با این وجود، قرار نیست در این فصل یک مرور کامل از همه جنبه‌های **ROE** که باید برای یک تست خاص در نظر گرفته شود، انجام دهیم یا الزامات قانونی چنین سندی را به طور کامل بررسی کنیم. در تعریف یک **ROE** وجود توصیه‌های قانونی ضروری است و هر سازمان مشتری که با یک **ROE** موافقت می‌کند، باید پیش از امضای آن مشاوره‌های قانونی لازم را انجام دهد.

به غیر از اینکه **ROE** مبنای قانونی لازم برای اجرای یک تعامل را بدون نقض قوانین ملی، ایالتی یا بین المللی فراهم می‌کند، سه هدف و کاربرد اصلی دارد. اولاً **ROE** مجوزهای مناسب را برای ارزیاب‌ها فراهم می‌کند تا عملیات را بدون نگرانی از نقض قوانین فدرال پیش ببرند. ارایه دهنده خدمات و تیم ارزیابی هر دو باید نسخه‌هایی از **ROE** داشته باشند. اگر به هر دلیلی، سازمان مشتری با ارایه دهنده خدمات مشکل پیدا کرده و به دنبال تخریب **ROE** و متهم کردن ارزیابان باشد، وجود این سند می‌تواند به پیشگیری از ایجاد مشکلات قانونی برای تیم ارزیابی کمک کند. در واقع، شما باید به عنوان ارزیاب برای هر مأموریت، به غیر از نسخه‌ای از **ROE** که کارفرما دارد، یک نسخه از **ROE** داشته باشید.

دوماً، همانطور که **ROE** از فرد ارایه دهنده خدمات حفاظت می‌کند، از سازمان ارایه دهنده خدمات هم حفاظت می‌کند تا به اشتباه در برابر آسیب‌های احتمالی ناشی از این تعامل مسئول تلقی نشود. معمولاً این موضوع برای تیم‌های قرمز درون سازمانی کمتر مشکل ایجاد می‌کند. اما در هر مأموریتی در حوزه امنیت تهاجمی احتمال ایجاد اختلال در خدمات یا دستگاه‌ها وجود دارد و ممکن است این اختلالات برای مشتری هزینه داشته باشند. اگر حین یک عملیات چنین اتفاقات بعیدی رخ دهند، غیرمنطقی است که ارایه دهنده خدمات هزینه این آسیب‌ها را پرداخت

[1] rules of engagement
[2] Computer Fraud and Abuse Act

کند. این موضوع ما را به آخرین نکته مطرح شده بر می‌گرداند یعنی اینکه ROE از سازمان مشتری هم حفاظت می‌کند.

ROE آسیب‌های ناشی از فعالیت‌های معمولی هکرهای اخلاقی را پوشش نمی‌دهد اما شرایطی را که سهل انگاری فاحش محسوب می‌شوند، مشخص می‌کند. این بند یک عبارت کلی برای پوشش هر فعالیت ناقص یا نادرستی از سمت ارزیاب است که منجر به آسیب رساندن به مشتری شده و می‌تواند موضوعات ساده‌ای مثل عدم حفاظت از داده‌های مشتری تا موضوعات پیچیده‌تری مثل فعالیت‌های هک غافلانه یا غیرعمدی را شامل شود که تأثیرات نامطلوبی بر دارایی‌های سازمانی دارند. مثالی از سهل انگاری‌های فاحش که به راحتی قابل اثبات است، این است که یکی از اعضای تیم قرمز یک نسخه رمزنگاری نشده یا حفاظت نشده از گزارش آسیب پذیری را روی کامپیوتر خودش نگه می‌دارد و بعد این گزارش فاش شده یا یک هکر واقعی از آن استفاده می‌کند. از طرفی، اثبات اینکه اقدامات یک هکر اخلاقی خارج از محدوده تکنیک‌های مناسب بوده و سهل انگاری آشکار محسوب می‌شود، کار بسیار سخت‌تری است. همچنین، ROE توافقنامه‌های محرمانگی بین سازمان‌های ارایه دهنده خدمات و مشتری را مشخص می‌کند تا اعضای تیم ارزیابی از نظر قانونی ملزم باشند که وقتی با هر شخصی خارج از تیم ارزیابی یا سازمان مشتری گفتگو می‌کنند، در رابطه با آسیب پذیری‌های سازمان صحبت نکرده و آنها را فاش نکنند. بعلاوه، ROE الزامات حفاظت از داده‌ای را که از نظر مشتری رعایت آنها حین و پس از اجرای ارزیابی ضروری است مشخص می‌کند.

انواع فعالیت‌ها

فعالیت‌هایی که یک ROE آنها را برای محدوده یک ارزیابی مجاز می‌دانند، می‌توانند به شدت متنوع باشند. هر نوع از فعالیت‌های امنیت تهاجمی تأثیر خاصی بر شیوه اجرای عملیات تیم قرمز داشته و بنابراین مستلزم در نظر گرفتن ملاحظات متفاوتی در ROE است. ممکن است یک یا چند مورد و یا همه انواع فعالیت‌های ارزیابی زیر در یک مأموریت تیم قرمز وجود داشته باشند:

- فیزیکی
- مهندسی اجتماعی
- شبکه خارجی
- شبکه داخلی
- جابجایی در شبکه
- شبکه بی‌سیم

ضروری است که فعالیت‌های ارزیابی امنیت تهاجمی بر همین اساس دسته بندی شده و در ROE به این فعالیت‌ها و پارامترهای آنها اشاره شود تا مشتری به صورت صریح نوع فعالیت تیم قرمزی که قرار است اجرا شود را درک کند و این اطمینان فراهم شود که هیچ یک از طرفین غافلگیر نمی‌شوند.

فیزیکی

فعالیت‌های امنیت تهاجمی فیزیکی هم برای ارزیاب و هم برای مشتری بسیار پرریسک هستند و معمولاً به همین دلیل در مأموریت‌های تیم قرمز وجود ندارند. همچنین با اینکه معمولاً تیم قرمز مایل است که مجاز به هدف گیری فیزیکی تشکیلات باشد اما تیم‌های کمی تخصص حرفه‌ای لازم برای انجام این کار را دارند. اینکه فعالیت فیزیکی در یک ارزیابی، ریسک وارد شدن آسیب واقعی به دارایی‌های سازمانی و حتی جراحت افراد را ایجاد می‌کند باعث شده که توجیه این کار برای بیشتر تعاملات سخت باشد.

فعالیت‌های فیزیکی سه نوع کلی دارند:

۱. بدون فناوری
۲. با فناوری کم
۳. با فناوری زیاد

مشخص کردن نوع فعالیت‌های فیزیکی مجاز برای تیم قرمز در ROE می‌تواند واقع گرایی برخی از انواع خاص ارزیابی‌ها را افزایش داده و در عین حال ریسک آنها را کاهش داده و بازخوردهای ارزشمندی در اختیار سازمان قرار دهد.

فعالیت‌های فیزیکی بدون فناوری شامل اقداماتی هستند که در آنها ارزیاب برای حمله به سازمان نیاز به استفاده از هیچ ابزار یا لوازم الکترونیکی ندارد. یک نمونه از چنین فعالیت‌هایی، نگاه کردن از پشت سر است که در آن ارزیاب، سعی می‌کند اطلاعاتی را از روی صفحه نمایش دستگاه افراد یا مدارک روی میز آنها به دست آورد یا آنها را حین تایپ کردن یک کد یا رمز عبور تماشا کند. روش بعدی دنبال کردن افراد است که در آن ارزیاب سعی می‌کند افراد مجاز به ورود به یک محوطه امنیتی را دنبال کرده و پشت سر آنها، بدون نیاز به احرازهویت وارد آنجا شود.

سایر اقدامات عمومی‌تری که در این گروه قرار می‌گیرند شامل کارهایی مثل قفل نکردن درها در پایان کار و برگشتن به تشکیلات پس از ساعت کاری است. ممکن است از فعالیت‌های بدون فناوری برای فراهم کردن امکان انجام اقدامات دیگر حین ارزیابی استفاده شود. چنین فعالیت‌هایی، ضعف در رعایت و طراحی سیاست‌ها و رویه‌ها را در سازمان نشان می‌دهند. معمولاً

این فعالیت‌ها و سایر فعالیت‌های بدون فناوری ریسک کمی دارند هر چند همگی فعالیت فیزیکی هستند. اما این ریسک بدیهی وجود دارد که وقتی یک سازوکار امنیت فیزیکی غیرفعال نگه داشته می‌شود تا ارزیاب بعداً برگشته و از آن استفاده کند، یک مجرم واقعی از این شرایط به نفع خودش بهره برداری کند. تیم قرمز می‌تواند این ریسک را هم کاهش دهد.

فعالیت‌های فیزیکی با فناوری کمتر به آنهایی گفته می‌شود که به میزان کمی از فناوری استفاده می‌کنند مثل به کار بردن ابزارهایی مانند قفل باز کن یا سایر ابزارهای ساده برای باز کردن درهای تشکیلات، کشوی پرونده‌ها، در خودروها یا سایر مکان‌هایی که ممکن است ابزارهای احرازهویت (مثل کارت پرسنلی یا اطلاعات ارزشمند) در آنجا قرار داشته باشد. اقداماتی مثل قطع سیم‌های سیستم‌های امنیتی برای ارزیابی واکنش سازمان به از دسترس خارج شدن این سیستم‌ها و عبور از حصارها و سایر سازوکارهای امنیتی معیوب هم در این گروه قرار می‌گیرند. حتی ساده‌ترین اقدام در این گروه یعنی استفاده از قفل بازکن هم می‌تواند پیامدهای دائمی بر سازوکار شکست خورده داشته باشد. همین احتمال ایجاد آسیب دائمی در سیستم‌ها و ریسک کلی فعالیت‌هایی با سطح فناوری پایین، باعث شده که جلب رضایت مشتری برای انجام آنها کار سختی باشد. در واقع، مشتریان بسیار کمی نیاز یا تمایل به اجرای چنین فعالیت‌های ارزیابی دارند. بیشتر سازمان‌ها، باور دارند که تهدیدات فیزیکی با سطح فناوری پایین از طریق اعمال قانون و با وجود مجریان قانون به حداقل می‌رسند.

فعالیت‌های فیزیکی با سطح فناوری بالا شامل اجرای حملات الکترونیک به کمک ابزارهایی مثل کی لاگرهای[۳] فیزیکی، دستگاه‌های شنود صدا و تپ‌های شبکه[٤] با هدف به دست آوردن اطلاعات و کمک به اجرای عملیات تیم قرمز است. این زیرمجموعه، کلیدهای دسترسی فیزیکی را هم شامل می‌شود که برای مثال می‌توان با آنها از یک سیستم عامل لینوکس فعال روی یک حافظه قابل جابجایی برای بوت کردن یک سیستم ویندوزی یا لینوکس، نصب درایو لینوکس و استخراج اعتبارنامه‌های دامنه از این هارد درایو استفاده کرد. چنین اقداماتی در مقایسه با فعالیت‌هایی که سطح فناوری کمی دارند، کم ریسک به نظر می‌رسند. بر خلاف فعالیت‌های بدون فناوری مثل تعقیب کردن افراد که پیروی از سیاست‌ها را ارزیابی می‌کنند، فعالیت‌هایی با سطح فناوری بالا، امکان ارزیابی سیاست‌های امنیت سایبری را فراهم می‌کنند. گرچه اتصال یک کی لاگر سخت‌افزاری به یک پورت USB باز با یک اقدام فیزیکی انجام می‌شود اما در این روش،

---

[3] key logger

[٤] تپ شبکه سیستمی است که رویدادهای یک شبکه محلی را رصد می‌کند

ارزیابی می‌شود که آیا پیکربندی‌ها یا سیاست‌های امنیتی مربوط به USB آنطور که باید کار می‌کنند یا خیر. به همین صورت، تلاش برای نصب یک هارد درایو ویندوزی روی یک سیستم لینوکسی فعال، سیاست‌ها یا پیکربندی‌های مربوط به رمزنگاری هارد درایو و غیره را ارزیابی می‌کند.

واضح است که همه فعالیت‌های فیزیکی برای بیشتر ارزیابی‌ها مناسب یا قابل اجرا نیستند. با این وجود، تعیین اقدامات بدون فناوری و با سطح فناوری بالا مجاز در ROE ، می‌تواند راهکاری جامع برای ارزیابی سازوکارهای امنیتی مختلف یک سازمان با روش‌هایی باشد که ابزارهای نفوذ سایبری معمولی، آن را انجام نمی‌دهند.

مهندسی اجتماعی

مفهوم مهندسی اجتماعی کاملاً ساده و مشخص است: در این روش مهاجم به دنبال شستشوی ذهنی یا فریب دادن هدف برای ارایه اطلاعات یا انجام کاری است که امکان نفوذ بیشتر به سازمان را فراهم می‌کند. پیاده سازی فعالیت‌های مهندسی اجتماعی در یک فرایند ارزیابی می‌تواند کار بسیار پیچیده‌ای باشد. عامل اصلی پیچیده کننده چنین عملیاتی، اجرای این فرایند از طریق هدف گیری کارمندان سازمان در شبکه‌های اجتماعی، ایمیل، تماس تلفنی، پیامک و غیره است.

سناریوی زیر چالش‌های مربوط به اجرای کارزارهای مهندسی اجتماعی را در ارزیابی‌های تیم قرمز نشان می‌دهد. فرض کنید که شما مجوز تلاش برای فریب دادن کاربران را دریافت کرده‌اید تا از طریق ایمیل‌های مخرب، آنها را تشویق به نصب بدافزار کنید. این فعالیت که به آن فیشینگ گفته می‌شود به شما امکان می‌دهد تا عملکرد سیستم‌های امنیتی میزبان محور، سیستم اسکن یا فیلترینگ ایمیل و رعایت سیاست‌های ایمیلی توسط کاربران را بررسی کنید. شما ایمیل آلوده را به آدرس‌های ایمیلی در دامنه سازمان ارسال می‌کنید که فقط روی دستگاه‌های داخل محوطه سازمان، وجود دارند. همان روز چند بدافزار روی کامپیوترهای سازمان نصب شده و عصر آن روز متوجه می‌شوید که یکی از بدافزارهای شما با دستگاه همراه یکی از کارمندان در تماس است. این دستگاه جزء محدوده ارزیابی نبود و حالا ارزیاب مرتکب جرم شده است.

اتفاقی که افتاده این است که یکی از کاربران این ایمیل کاری را به حساب شخصی خودش فوروارد کرده و بعد از ساعت کاری ایمیل مخرب را روی تلفن همراهش باز کرده است. حالا اگر سازمان سیاست مشخصی بر علیه این رفتار داشته باشد و طبق سیاست‌های سازمان، کاربران سیستم‌ها با ارزیابی امنیتی سیستم‌ها موافقت کرده باشند، تیم ارزیابی مرتکب اشتباهی نشده

اما اگر شرایط این طور نباشد، ممکن است برای تیم ارزیابی مشکلات قانونی مهمی ایجاد شود. هنگام تهیه پیش نویس ROE حتماً باید قوانین و دستورالعمل‌های اجرای این کارزارهای شبکه‌های اجتماعی مشخص شده و سیاست‌های سازمانی مربوط به آنها شناسایی شوند. حتی وقتی چنین مقرراتی مشخص شدند، ممکن است در صورت آلوده شدن دستگاه‌های شخصی در اثر اجرای کارزارهای مهندسی اجتماعی، جلب رضایت سازمان برای مقصر دانستن کاربران کار سختی باشد.

تیم ارزیابی هم نباید چنین مسئولیتی را بپذیرد.

مهندسی اجتماعی به غیر از آلودگی‌های تصادفی و ناخواسته پیامدهای دیگری هم دارد. روش‌های فیشینگ متنوع هستند. یکی از این روش‌ها به نام "فیشینگ هدفمند" یک فرد یا یک گروه کوچک را با مسیرهایی که به طور اختصاصی برای آنها طراحی شده، هدف می‌گیرد. در روش بعدی به نام والینگ[5]، افراد قدرتمند در سازمان هدف گرفته می‌شوند مثل مدیران اجرایی یا مدیران ارشد. در همه موارد، احتمال مخالفت شدید با این اقدامات وجود دارد چون در این تکنیک‌ها افراد فریب داده می‌شوند تا یک کار خاص را انجام دهند. اگر کارمندان اجرایی یا مدیران امنیت سایبری در چنین کارزارهایی هدف گرفته شوند، ممکن است این موضوع به حدی روابط تیم قرمز و مشتری را تحت تأثیر قرار دهد که برای کل این عملیات پیامدهای مخربی داشته باشد. هنگام تهیه پیش نویس ROE باید به این حملات مهندسی اجتماعی هم توجه داشت. ممکن است ضروری باشد که برای حفظ اثربخشی ارزیابی، چنین فعالیت‌هایی که مرتبط به مهندسی اجتماعی هستند، اجرا نشوند. حتی محدود کردن این تعاملات به کاربران معمولی هم می‌تواند باعث به وجود آمدن خشم و ناراحتی در سازمان شود و اگر تیم قرمز متشکل از کارمندان درون سازمانی باشد، ممکن است این شرایط باعث خصمانه شدن محیط کار شود.

در یکی از محدود مأموریت‌هایی که مجاز به اجرای حمله مهندسی اجتماعی بودم، عملیات تیم قرمز باعث ناراحتی تعدادی از کارمندان شد و با اینکه این کارزار با موفقیت به پایان رسید اما اجرای حملات مشابه را در آینده توصیه نمی‌کنم. تیم من به عنوان تیم قرمز یک سازمان تجاری بزرگ، مسئولیت اجرای ارزیابی را روی شرکت‌های خریداری شده پیش از نهایی شدن قرارداد برعهده داشت تا سازمان اصلی با خرید شرکت‌های ناامن متحمل بار اقتصادی و ریسک‌های امنیتی جدید نشود. ما از زمان اعلام خبر اکتساب اطلاع داشتیم تا کارمندان سازمان هدف را زودتر از موعد قرارداد هدف بگیریم.

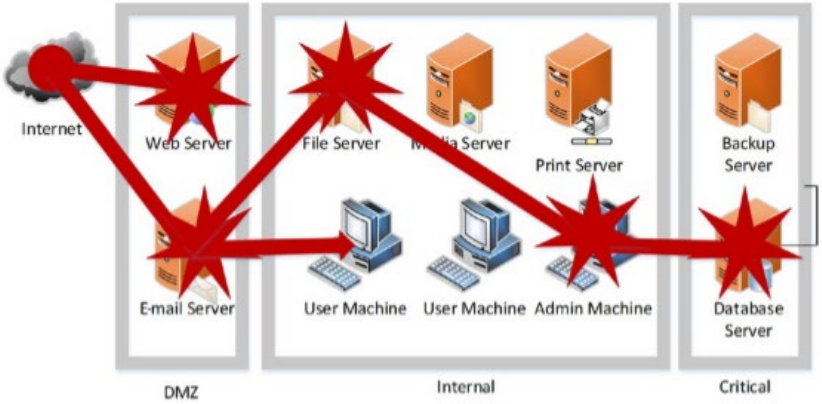
---

[5] whaling

فرض کنید اسم شرکت خریداری شده **Temp Agency** و دامنه ایمیل این شرکت **@tempagency** بود. ما دامنه **ternpagency** را ثبت کرده و از آدرس ایمیل **hr@ternpagency** استفاده کردیم. همانطور که در جریان هستید، با خیلی از فونت‌ها حروف "**rn**" و "**m**" شبیه به هم به نظر می‌رسند به خصوص در نگاه اول. بلافاصله پس از اعلام خبر اکتساب در شرکت هدف، ما ایمیل‌هایی با عنوان "اطلاعات اکتساب" برای کارمندان این شرکت ارسال کردیم که حاوی چند فایل پیوست آلوده با عناوینی مثل "تغییرات حقوق" و سایر عناوین جذاب بودند. ما آدرس ایمیل اهدافمان را با جستجوی سایت‌های شبکه این کسب و کار و سایر تکنیک‌های اپن سورس به دست آورده بودیم. همانطور که حتماً تصور می‌کنید، خیلی از کارمندان کنجکاو و عصبی روی این ایمیل کلیک کرده و فایل‌ها و لینک‌های مخرب ما را دانلود کردند.

شبکه خارجی

ارزیابی از طریق شبکه‌های خارجی در مأموریت‌های تیم قرمز بسیار رایج است و به حملات سایبری گفته می‌شود که تیم قرمز از خارج از مرزهای سیستم، بر علیه سازمان انجام می‌دهند. ممکن است این حملات محدود به دارایی‌های سازمانی باشد که با بیرون در تماس هستند (شکل ۱-۵). این حمله خارجی معمولاً از طریق اینترنت انجام می‌شود. اما در برخی از سازمان‌های بزرگ که تیم‌های قرمز درون سازمانی دارند، ممکن است این حملات شامل حمله به یک سایت منطقی یا فیزیکی از یک سایت منطقی یا فیزیکی دیگر باشند. ملاحظات مهمی که باید در **ROE** چنین مأموریت‌هایی در نظر داشت، مربوط به منشأ حمله هستند. تیم ارزیابی باید در **ROE** آدرس مبدأ را که حملات از طریق آن اجرا می‌شود، مشخص کند تا امکان تشخیص فوری فعالیت‌های تیم قرمز از حمله‌های واقعی وجود داشته باشد.



شکل ۵-۱ فعالیت‌های شبکه خارجی

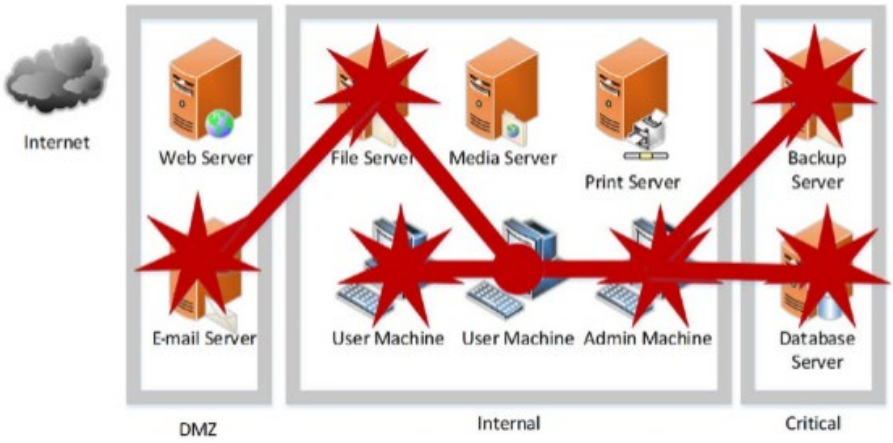
این شرایط، نیاز به وجود یک نوع زیرساخت مبنتی بر ارتباطات خارجی را نشان می‌دهد. ممکن است حین اجرای حملات اینترنتی که برای تغییر مسیر از زیرساخت‌های خارجی استفاده نمی‌کنند، فعالیت‌های تیم ارزیابی منجر به نقض توافقنامه‌هایی که سازمان با شرکت‌های ارایه دهنده خدمات اینترنتی دارد شده و باعث مسدود شدن برخی از آدرس‌ها یا قرار گرفتن آنها در لیست سیاه و یا حتی تعلیق کامل برخی از حساب‌های کاربری شود. چنین شرایطی می‌تواند باعث پیچیدگی و به تأخیر افتادن ارزیابی‌ها شود چون سازمان هدف از آدرس‌های مبدأ و تغییرات آنها اطلاع پیدا می‌کند. همچنین ممکن است در این شرایط بدون وجود ابزارهای تغییر مسیر خارجی، تیم قرمز به دلیل اجرای حملات سایبری که توافقنامه‌های کاربری شرکت ارایه دهنده خدمات میزبانی را نقض می‌کند، امکان دسترسی به اینترنت را از دست بدهد. مزیت استفاده از یک سرور با میزبانی خارجی برای اجرای حمله این است که به چندین ارزیاب امکان می‌دهد تا ارزیابی را از طریق یک دستگاه اجرا کرده و با یکدیگر همکاری کنند.

در یکی از مأموریت‌های ما، یکی از اعضای تیم ارزیابی را از راه دور و از طریق اینترنت منزل انجام می‌داد. سازمان مشتری باید آدرس این ارزیاب را در فایروال مجاز اعلام می‌کرد تا امکان اجرای ارزیابی فراهم می‌شد. دو روز از این ارزیابی ۱۰ روزه، آدرس ارزیاب تغییر کرد و تقریباً دو روز کامل طول کشید تا فایروال آدرس‌های جدید را مجاز در نظر گرفته و فرایند ارزیابی ادامه پیدا کند. به این ترتیب، ۲۰ درصد از فرصت ارزیابی ما از دست رفت و به دلیل سایر تعهدات موجود در این ارزیابی، امکان تغییر و تنظیم مجدد عملیات را نداشتیم. برای پیشگیری از چنین مشکلاتی که هنگام ارزیابی از طریق شبکه‌های خارجی ایجاد می‌شوند، در ROE یک زیرساخت شخص ثالث مجزا با آدرس ایستا را تعیین و استفاده از آن را الزامی کنید.

شبکه داخلی

فعالیت‌های شبکه داخلی شامل حملات سایبری است که از درون شبکه سازمان هدف شروع شده و سایر دارایی‌های داخلی را هدف می‌گیرند (شکل ۵-۲). گرچه این روش امکان اجرای بسیار کارآمدتر ارزیابی را به خصوص در بازه‌های زمانی کوتاه‌تر فراهم می‌کند اما خیلی از مواقع مشتریان با این کار موافق نیستند. همانطور که پیش از این اشاره شد، گاهی اوقات این دیدگاه وجود دارد که اگر ارزیابی شامل دسترسی‌های خارجی نباشد، غیرواقعی یا نادرست است. ما باید سازمان‌های هدف را در رابطه با این واقعیت آموزش دهیم که سهم چشمگیری از حملات و نفوذهای موفق ناشی از تهدیدات داخلی یا فعالیت‌های مهندسی اجتماعی هستند که هر دو از دسترسی به یک دستگاه در شبکه داخلی شروع می‌شوند. اگر نیاز صریحی به اجرای ارزیابی خارجی وجود نداشته

باشد، بهترین حالت از نظر تعدیل هزینه‌ها برای سازمان، اجرای یک ارزیابی کوتاه است که در آن ارزیابی‌ها به جای حمله خارجی یا سایر روش‌ها، با یک حرکت از شبکه داخلی شروع می‌شوند.



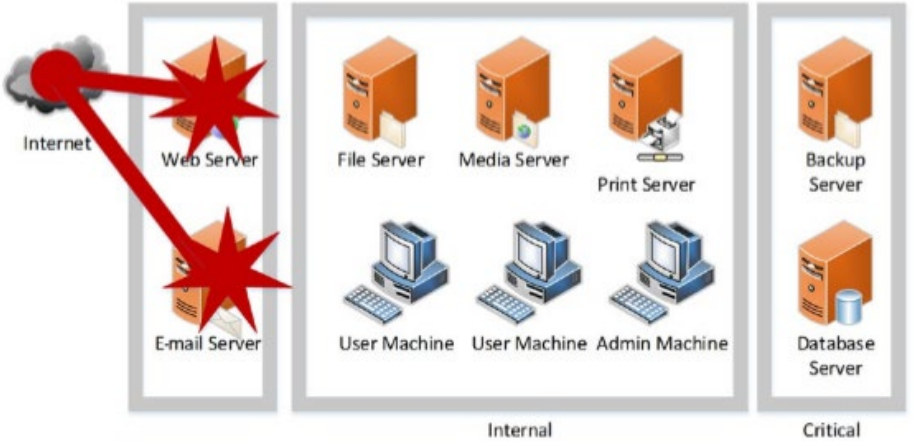
شکل ۵-۲ فعالیت‌های شبکه داخلی

معمولاً چنین ارزیابی‌هایی در صورتی قابل انجام است که ارزیاب دسترسی‌های غیرممتاز خاصی را داشته باشد. اما در برخی شرایط بهتر است که حمله داخلی اول با سطح دسترسی پایین شروع شده و بعد این سطح دسترسی تقویت شود تا حداکثر میزان ممکن از سطح حمله عملیاتی سازمان ارزیابی شود. معمولاً دسترسی که امکان اجرای این فعالیت‌ها را فراهم می‌کند، از طریق یک تهدید داخلی یا یک حمله مهندسی اجتماعی شبیه سازی شده موفق به دست می‌آید. هر دو حالت بیشتر توسط ارزیابانی شروع می‌شود که دسترسی سطح کاربر عادی را به شبکه دارند و بعد سایر تجهیزات درون سازمان را هدف می‌گیرند. **ROE** چنین حمله‌ای باید به وضوح مرز بین افراد و دارایی‌های قابل هدف گیری و غیرقابل هدف گیری را مشخص کند. از آنجایی که ارزیابی از درون محیط امنیتی سازمان شروع می‌شود، ممکن است به سرعت به بخش‌هایی از سازمان منتشر شود که مشتری تصور می‌کرده امکان آلودگی آنها وجود ندارد و هدفگیری نخواهند شد. هنگام تعیین محدوده عملیات و ایجاد **ROE**، باید اهداف و روش‌های ممنوع مشخص شوند حتی اگر مشتری رسیدن به آنها را بعید می‌داند به ویژه برای مواقعی که حملات داخلی انجام می‌شوند.

حرکت در شبکه

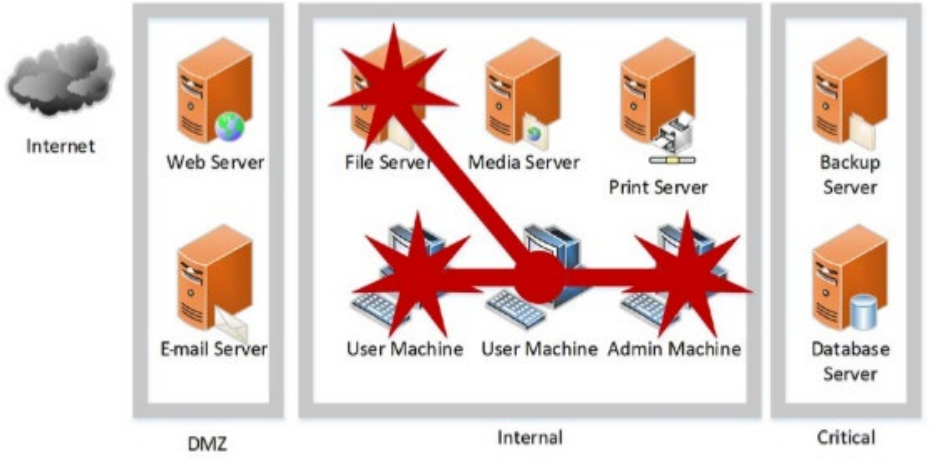
ممکن است در تنظیم **ROE** حرکت در شبکه جزء فعالیت‌های کم اهمیت به نظر برسد اما تعیین مجاز بودن تیم ارزیابی به انتقال در شبکه نقش مهمی در شیوه اجرای عملیات دارد. حرکت

در شبکه دو تعریف دارد که هر دو باید در ROE در نظر گرفته شوند. تعریف اول، به استفاده از امکان دسترسی به یک دستگاه برای سرشماری سایر تجهیزات و حمله به اهداف دیگر در سازمان گفته می‌شود (شکل ۵-۳). در چندین مورد از حملات سایبری که ما انجام داده‌ایم، مشتری مایل به حرکت از یک میزبان به میزبانی دیگر نبوده و این شرایط باعث کاهش محدوده حمله شده است.



شکل ۵-۳ حالت خارجی و بدون جابجایی

اگر جابجایی بین دارایی‌های داخل سازمان مجاز باشد، ردپای حمله بسیار عظیم‌تر خواهد بود و این موضوع بر زمان و محدوده ارزیابی هم تأثیر خواهد داشت (شکل ۵-۴).



شکل ۵-۴ حالت داخلی و باجابجایی

دومین تعریف از جابجایی، به استفاده از یک اپلیکیشن برای نفوذ به یک اپلیکیشن دیگر و ارتقای سطح دسترسی گفته می‌شود. برخی از ارزیابی‌های امنیت تهاجمی محدود به هدف گرفتن یک اپلیکیشن خاص هستند که روی یک یا چند دستگاه میزبانی می‌شوند. برای مثال، یک اپلیکیشن پایگاه داده را در نظر بگیرید. در صورت مجاز نبودن جابجایی، حتی اگر ارزیاب راهی برای نفوذ به سیستم با بهره برداری از پایگاه داده پیدا کند، باز هم امکان انجام این کار را نخواهد داشت. این محدودیت نسبت به محدودیت جابجایی بین دستگاه‌ها کمتر متداول است اما گاهی اوقات در تعریف محدوده تعامل، هر دو روش جابجایی در **ROE** محدود یا ممنوع اعلام می‌شوند.

شبکه بی‌سیم

حمله از طریق شبکه بی‌سیم شبیه حمله فیزیکی است چون معمولاً جزء حوزه‌های تخصصی‌تر و محدودتر در عملیات تیم قرمز است و عده کمی مهارت زیادی در انجام چنین فعالیت‌هایی دارند. همچنین برای این حملات باید ریسک‌های بیشتری را پذیرفته و در **ROE** مشخص کرد. سه روش برای حمله از طریق شبکه فیزیکی وجود دارند که عبارتند از:

۱. شنود غیرفعال با هدف رسیدن به دسترسی‌های بیشتر با گردآوری ترافیک کافی تا امکان کرک کردن رمزنگایی یا تشخیص اعتبارنامه‌های کاربری فراهم شود.

۲. بهره برداری فعال مثلاً برای حمله به یک دستگاه بلوتوث جهت جمع آوری اطلاعات یا دستکاری آن دستگاه.

۳. محروم سازی از شبکه بی‌سیم برای تغییر وضعیت عملیاتی یک سازمان به نفع حملات تیم قرمز.

یک نمونه محروم سازی از شبکه بی‌سیم برای اجرای ارزیابی، اقدامی است که مانع از برقراری ارتباط با یک نقطه دسترسی شده و دستگاه‌های هدف را ملزم به انتقال از نقاط دسترسی بی‌سیم امن به نقاط دسترسی مخرب تنظیم شده توسط تیم قرمز می‌کند. فناوری‌های بی‌سیم طیف وسیعی دارند از جمله استانداردهای **802.11** که معمولاً در منازل و کسب و کارها استفاده می‌شوند تا رادیوها، بلوتوث، مادون قرمز و غیره. اگر حمله به شبکه بی‌سیم در مأموریت تیم قرمز مورد انتظار باشد، باید در **ROE** نوع فعالیت و فناوری‌های قابل هدف گیری مشخص شوند. همچنین اعضای تیم قرمز باید آگاه باشند که برای استفاده از امواج بی‌سیم مقررات خاصی وجود دارد و اگر فعالیت‌های محروم سازی از شبکه بی‌سیم بر ضد سازمان هدف، بر دارایی‌های غیر متعلق به مشتری مثل شبکه بی‌سیم یک کافی شاپ نزدیک تأثیراتی منفی داشته باشند، این فعالیت نقض قانون تلقی شده و قابل پیگرد قانونی است.

بعلاوه ممکن است برخی از افراد در سازمان مشتری دستگاه‌های شخصی خودشان را به شبکه بی‌سیم سازمان متصل کنند و حمله به شبکه بی‌سیم آنها را نیز تحت تأثیر قرار دهد. باید با استفاده از همان روش‌هایی که در بخش مهندسی اجتماعی اشاره شد، با این تضاد احتمالی هم برخورد شود. باید چنین شرایطی به همراه سیاست‌های مربوطه و توافقنامه‌های کاربری به خوبی در ROE درک و ثبت شده باشد تا در این زمینه مسئولیتی متوجه ارزیاب نباشد.

دسته بندی

علاوه بر در نظر گرفتن و تأیید نوع فعالیت در ROE، باید دسته بندی ارزیابی تهاجمی که قرار است تیم قرمز انجام دهد هم مشخص شود. این دسته بندی‌ها شامل تست جعبه سیاه، تست جعبه خاکستری و تست جعبه سفید هستند.

تست جعبه سیاه حالتی است که در آن مأمویت تیم قرمز تقریباً بدون در اختیار داشتن هیچ اطلاعاتی از هدف انجام می‌شود به غیر از اطلاعات ساده‌ای مثل نام هدف. ممکن است چنین تستی به شبیه سازی واقع گرایانه‌تر حمله کمک کند اما باعث صرف زمان بیشتر و ایجاد ریسک برای ارزیابی می‌شود. این احتمال وجود دارد که ارزیابی بسیار فراتر از محدوده قانونی رفته یا بخش‌های زیادی از سازمان را پوشش ندهد. برای مثال، ممکن است در تحقیقات اپن سورس تست جعبه سیاه، تیم ارزیابی به سایتی برخورد کند که به ظاهر متعلق به سازمان است اما وقتی بهره برداری از این سایت را آغاز می‌کند، مشخص شود که این سایت یک کپی از محتوای سایت اصلی سازمان است که به عنوان یک مثال بازاریابی توسط یک شرکت دیگر استفاده شده و چنین اقدامی یعنی نقض قوانین CFAA و سایر مقررات مربوطه توسط تیم قرمز.

در تست جعبه خاکستری، مقداری اطلاعات در اختیار تیم ارزیابی قرار می‌گیرد اما ممکن است این کار برای اجتناب از ریسک‌های تست جعبه سیاه انجام شود. معمولاً فهرست کاملی از نقاط حضور بیرونی ارایه شده و تیم ارزیابی باید بر اساس همین اطلاعات کارهای لازم را انجام دهد.

در نهایت، تست سفید به تستی گفته می‌شود که در آن ارزیابان اطلاعات تقریباً کاملی از سازمان هدف دارند. معمولاً چنین شرایطی در صورت استفاده از تیم‌های قرمز درون سازمانی اجتناب ناپذیر است و لزوماً چیز بدی نیست. دقت داشته باشید که بسیاری از نفوذها حاصل تهدیدات داخلی هستند و ممکن است چنین کارمندانی هم زاویه دید کاملی نسبت به سازمان داشته باشند. در بیشتر مواقع، تست نفوذ جعبه سفید به اندازه تست جعبه سیاه مفید است.

تقویت نیرو

بین همه جوانب عملیات تیم قرمز، تقویت نیرو در **ROE** بیشترین شباهت را به مفهوم نظامی تیم قرمز دارد. تقویت نیرو یکی دیگر از جنبه‌های **ROE** است که درک آن بسیار راحت و ساده است و ثبت و تأیید آن قبل از شروع هر ارزیابی بسیار مهم و ضروری است. در **ROE** تیم قرمز سایبری، تقویت نیرو تعیین کننده محدودیت انواع فعالیت‌هایی است که می‌توان بدون هماهنگی و کسب تأیید اولیه از رابط تیم قرمز در سازمان مشتری، آنها را انجام داد. اخذ چنین تأییدهایی برای مقابله با تأثیرات سهل انگاری فاحش بر مشتری ضروری است و معمولاً هنگام ارزیابی محیط‌های عملیاتی یا تولیدی در **ROE** پوشش داده می‌شود. برای ارزیابی‌ها و سرشماری‌های روزانه سطح خاصی از اقدامات و فعالیت‌ها در **ROE** مجاز است اما برای اقدامات خاصی مثل ارتقای سطح دسترسی یا اجرای کد از راه دور، کسب مجوز و تأییدیه ضروری است. اگر در **ROE** چنین قیود و محدودیت‌هایی در نظر گرفته شده باشند، سازمان مشتری باید یک فرایند تأیید کارآمد و مناسب برای چنین فعالیت‌هایی داشته باشد تا بهره وری عملیات حفظ شود.

من به شخصه طرفدار بزرگ استفاده از یک مأمور رایزنی توسط سازمان هدف هستم. مأمور رایزنی یکی از نمایندگان سازمان است که در طول دوره ارزیابی در دسترس قرار دارد؛ این شخص آگاهی وضعیتی کلی را از فعالیت‌های تیم قرمز داشته و بیشتر تأییدیه‌های لازم را حین ارزیابی فراهم می‌کند. مأمور رایزنی می‌تواند یک کارشناس مجرب امنیت تهاجمی یا یک کارمند فنی باشد یا جزء کارمندان کم مهارت‌تر بخش امنیت یا فناوری اطلاعات باشد. وجود این مأمور به غیر از روان‌تر کردن جریان کار تیم قرمز برای سازمان مشتری هم مفید است به این دلیل که باعث می‌شود یکی از کارمندان سازمان دید بهتری نسبت به عملکرد تیم قرمز داشته باشد؛ اطلاعات به دست آمده از این فرایند را در وظایف روزمره خودش به کار ببندد و باعث تقویت قابلیت‌های امنیتی کلی سازمان شود.

مدیریت حادثه

برای رسیدگی به حادثه و مدیریت آن، وجود یک زنجیره از مقامات مسئول لازم است. حوادث در دو گروه قرار می‌گیرند و هر کدام نیاز به زنجیره گزارش دهی متفاوتی دارد: فعالیت‌های غیرقانونی شناسایی شده درون سازمان و فعالیت‌های غیرقانونی مربوط به سازمان. یک نمونه از فعالیت‌های غیرقانونی وقتی مشاهده می‌شود که اعضای تیم ارزیابی شواهدی پیدا می‌کنند که آنها را مشکوک به انجام اقداماتی غیرقانونی در سازمان می‌کند مثل توزیع مواد مخدر، قاچاق

انسان یا سایر جرایم جدی. در ROE باید مشخص شود که چنین اقدامات مشکوکی چگونه و به چه افرادی گزارش داده می‌شوند. دلیل در نظر گرفتن این مسئله این است که اگر تیم ارزیابی چنین فعالیت‌های غیرقانونی را به جای سازمان مشتری، مستقیماً به مقامات مسئول گزارش دهد، سازمان مشتری امکان پیگرد قانونی تیم قرمز را نداشته باشد.

فرض کنید مقامات یک سازمان معاملات نهانی[۶] انجام می‌دهند و تیم ارزیابی حین اجرای عملیات متوجه این موضوع شده و یافته‌های خودش را به اطلاع مقامات می‌رساند. ممکن است سازمان سعی کند با صدور قرار منع بر اساس توافقنامه‌های محرمانگی که بخشی از ROE هستند، مانع از این اقدام شود. وجود یک بند درباره گزارش حوادث مربوط به فعالیت‌های غیرقانونی می‌تواند به مقابله با چنین شرایطی کمک کرده و تعهدات ارزیاب را برای گزارش دادن چنین حوادثی از همان ابتدای راه مشخص کند. همچنین، ROE باید انتظاراتی را که سازمان از تیم ارزیابی در رابطه با گزارش دهی فعالیت‌های پرسنل و رفتارهای غیرقانونی آنها دارد، مشخص کند. در این گزارش باید انواع اقدامات غیرقانونی کارمندان سازمان که گزارش آنها توسط تیم قرمز ضروری است و دریافت کننده این گزارشات مشخص شوند. از جمله این فعالیت‌ها می‌توان به شواهد آزار و اذیت جنسی، تقلب در کارت حضور غیاب کارمندان یا نقض سایر سیاست‌های سازمانی اشاره کرد. حین اجرای عملیات، باید همه حوادثی که ماهیت امنیتی یا عملیاتی دارند به اطلاع مسئولان مربوطه برسد چون این افراد بیشترین امکانات لازم را برای رسیدگی به چنین گزارشاتی در اختیار دارند.

ابزارها

ابزارهایی که قرار است در عملیات تیم قرمز استفاده شوند هم باید در ROE مشخص شوند. این کار با این هدف انجام می‌شود که تیم ارزیابی به دلیل آسیب‌های ناشی از به کار بردن یک ابزار خاص در ارزیابی متهم شناخته نشود. در صورتی که مشتری طبق ROE با استفاده از آن ابزار موافقت کرده باشد، امکان اقدام قانونی بر علیه تیم قرمز را نخواهد داشت. ثبت مشخصات این ابزارها در ROE برای مشتری هم مفید خواهد بود چون مانع از به کار بردن ابزارهای پر خطر و تأیید نشده توسط تیم قرمز برای دسترسی به سیستمی با شرایط دشوار خواهد شد.

---

[۶] تجارت داخلی یا معاملات نهانی (Insider Trading)، معامله سهام یک شرکت سهامی عام یا سایر اوراق بهادار بر اساس اطلاعات مادی و غیرعمومی درباره شرکت است. در کشورهای مختلف، برخی از انواع تجارت بر اساس اطلاعات داخلی غیرقانونی است

اما این مثال‌ها کاملاً کلی بودند و **ROE** می‌تواند شامل دستورالعمل‌هایی بسیار صریح باشد که به خصوص هنگام کار با سازمان‌های دولتی که در آنها تیم ارزیابی باید قوانین و هماهنگی‌های خاصی را رعایت کند، ضروری خواهد بود. ممکن است در چنین شرایطی استفاده از ابزارهایی که مشکلاتی شناخته شده دارند ممکن نباشد و استفاده از جدیدترین نسخه ابزارها حین اجرای تست، الزامی باشد.

معمولاً در یک **ROE** اشاره به ابزارها در قالب جملاتی مبهم و کلی صورت می‌گیرد مثل "برای اجرای ارزیابی از ابزارهای استاندارد، اپن سورس و اختصاصی استفاده می‌شود." معمولاً در بیشتر شرایط اشاره به ابزارها در قالب همین جمله کافی است و تنها استدلالی که برای استفاده از آن مطرح می‌شود این است که آیا استفاده از ابزارهای اختصاصی مجاز است یا خیر. همین بخش از این جمله، ابزارها و کدهایی که خود تیم ارزیابی آنها را نوشته و از آنها استفاده می‌کند را پوشش می‌دهد. این قابلیت اضافه کردن ابزارها و امکانات اختصاصی جزء شرایط کار تیم‌های قرمز حرفه‌ای و با استعداد است که برخی از سازمان‌ها تمایلی به وجود آن ندارند. اگر قسمت مجاز بودن استفاده از ابزارهای سفارشی از **ROE** حذف شود، تیم ارزیابی باید حین تعامل از ابزارهای شناخته شده اپن سورس که جزء ابزارهای استاندارد در صنعت مربوطه هستند، استفاده کند.

الزامات مجوز

مثل شرایطی که در رابطه الزامات ابزارها وجود دارد، ممکن است تیم قرمز برای فعالیت در شبکه یک سازمان هم نیاز به کسب مجوزهای خاصی داشته باشد. به خصوص ممکن است مشتریان دولتی چنین الزاماتی را برای تیم قرمز در نظر بگیرند. دسترسی سطح بالا به بسیاری از سیستم‌های دولتی، مستلزم داشتن چنین مجوزهایی است. از آنجایی که ممکن است فعالیت‌های تیم قرمز منجر به رسیدن به چنین دسترسی‌هایی شود، این افراد باید مجوزهای لازم را برای چنین دسترسی‌هایی داشته باشند. ممکن است این شرایط برای سیستم‌هایی که اطلاعات **HIPAA** و سایر اطلاعات مشابه را ذخیره می‌کنند هم برقرار باشد. معمولاً چنین مجوزهایی به صورت مورد به مورد اعطا می‌شوند و اگر الزامات خاصی برای کسب مجوز وجود داشته باشد، در **ROE** نام ارزیاب مربوطه ذکر می‌شود. این‌ها از جمله شرایطی هستند که باعث می‌شوند منابع تیم‌های قرمز بزرگ در مأموریت‌های مختلف افزایش یا کاهش پیدا کنند.

در چنین شرایطی ممکن است در ROE اعلام شود اعضایی از تیم قرمز که در سازمان کار می‌کنند باید یک مجوز معتبر با ماهیتی خاص داشته باشند تا نیازی به ذکر نام تک تک افراد تیم ارزیابی از قبل وجود نداشته باشد.

اطلاعات پرسنل

هر زمان ممکن بود، باید همه پرسنل دخیل در ارزیابی - از هر دو سمت تعامل - در ROE مشخص شده و اطلاعات تماس آنها ذکر شود. این کار به فراخوانی افراد، رفع تضاد و تشکیل زنجیره‌های قدرت مناسب در طی مأموریت تیم قرمز کمک می‌کند.

خلاصه فصل پنجم

در این فصل به بررسی اهمیت سند ROE برای هر دو طرف یعنی تیم ارزیابی و سازمان مشتری پرداختیم. همچنین بخش‌های مختلفی از محتوای ROE مثل نوع فعالیت و دسته بندی ارزیابی مورد بررسی و تحلیل قرار گرفت تا اهمیت آنها را برای کل ارزیابی مشخص کنیم.

• 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.