عملیات تیم قرمز و مهندسی اجتماعی

شناسایی اولیه

مهاجم همواره تلاش میکند تا اطلاعات مورد استفاده در برنامه ریزی عملیات آینده را جمع آوری کند. عملیات شناسایی شامل تکنیک هایی است که در آنها مهاجمان به طور فعال یا منفعلانه اطلاعاتی را جمع آوری می کنند. این تکنیک ها برای پشتیبانی از هدف استفاده میشود و اطلاعات بدست آمده از آنها ممکن است شامل جزئیات مربوط به سازمان، زیرساخت ها، یا کارکنان و پرسنل قربانی باشد و توسط مهاجم مورد استفاده قرار گیرد تا در مراحل دیگر چرخه عملیات نفوذ در مواردی مانند انجام Information Gathering برای برنامه ریزی و اجرای مرحله Initial Access به مهاجم کمک کند.

ایجاد دسترسی اولیه

مهاجم در تلاش است تا وارد شبکه شما شود. دسترسی اولیه شامل تکنیک هایی است که از بردار های مختلف ورودی برای بدست آوردن دسترسی اولیه خود در یک شبکه استفاده می کند. تکنیک های استفاده شده برای به دست آوردن دسترسی خود شامل Spear Phishingو بهره برداری از نقاط ضعف در وب سرورهای عمومی است. پایه هایی که از طریق دسترسی اولیه به دست می آیند میتوانند دسترسی مداومی ایجاد کنند مانند حساب های معتبر و سرویس های از راه دور خارجی.

عملیات تیم قرمز

عملیات تیم قرمز متشکل از یک سناریوی واقع گرایانه از یک حمله تهاجمی در سطح جهانی میباشد که اغلب در راستای اهداف بزرگ بکار گرفته می شود، تیم های قرمز از هر روش مستند شده و ابتکاری استفاده میکنند تا به فضای سایبری قربانی نفوذ کنند، این استانداردها مطابق با MITRE ATT&CK بوده و تمامی چهارده پلن مستند شده در خصوص حمله سایبری جهانی را شبیه سازی کنترل شده میکند، این شبیه سازی وضعیت تمامی مکانیزم های دفاعی شما و کیفیت عملکردی آنها را مورد آزمون جدی قرار میدهد، از این روی خدمات تیم قرمز یکی از مهمترین و حساس ترین خدمات امنیت تهاجمی بشمار می آید.

راه ارتباطی

تلفن:
026 368 06249

وبسایت:
unk9vvn.com

ایمیل:
info@unk9vvn.com

پایداری دسترسی

مهاجم در تلاش است دسترسی خود را حفظ کند. پایداری دسترسی شامل تکنیک هایی است که مهاجم برای جلوگیری از ایجاد دسترسی مجدد به سیستم، تغییر اعتبارنامه و سایر وقفه هایی که باعث قطع دسترسی میشود، استفاده می کند. تکنیک های مورد استفاده برای پایداری شامل هرگونه عملکرد یا تغییر در پیکربندی میباشد که به مهاجم امکان می دهد جای خود را در سیستم حفظ کند، مانند جایگزینی یا ربودن کد مجاز یا افزودن کد در Startup.

ارتقاء سطح دسترسی

افزایش سطح دسترسی (Privilege Escalation) شامل تکنیک هایی است که مهاجم برای به دست آوردن مجوزهای سطح بالاتر در یک سیستم یا شبکه استفاده می کند. مهاجمان غالباً می توانند با دسترسی غیرمحرمانه به شبکه ای وارد شوند و آن را کشف کنند اما برای پیگیری اهداف خود به دسترسی بالاتری نیاز دارند. این نیاز از طریق رویکردهای معمول، استفاده از نقاط ضعف یا تنظیمات نادرست و آسیب پذیری های سیستم برطرف میشود. این تکنیک ها اغلب با تکنیک های پایداری دسترسی همراهی دارند.

نامحسوس در دفاع

نامحسوس بودن در مقابل مکانیزم های دفاعی (Defense Evasion) شامل تکنیک هایی است که مهاجمان برای جلوگیری از شناسایی در طول حملات خود از آنها استفاده می کنند. این تکنیک ها شامل حذف و غیرفعال سازی نرم افزار امنیتی یا مبهم سازی و رمزگذاری داده ها و اسکریپت ها است. همچنین مهاجمان برای مخفی کردن و مخفی ماندن بدافزارهای خود، از فرایندهای قابل اعتماد سوءاستفاده می کنند.

تیم قرمز و تست نفوذ

تیم قرمز با تست نفوذ تفاوت هایی دارد: تیم قرمز محدود به دامنه خاصی نیست و سختگیری نمی شود (به عنوان مثال سطح دسترسی فقط به محدوده یک برنامه وب خاص).

کشف آسیب پذیری های مختص به ایجاد دسترسی که برخی از آنها فقط در تیم قرمز موضوعیت دارد، مانند کشف آسیب پذیری از مرورگرها و بکارگیری آن در سناریو حمله.

عملیات های تیم قرمز فقط به تکنیک های فنی محدود نمی شود، بلکه عوامل انسانی (مهندسی اجتماعی) و همچنین امنیت فیزیکی (سطح دسترسی فیزیکی در محل) را هم شامل میشود.

عملیات های تیم قرمز نباید پر سر و صدا باشند چرا که یکی از اهداف، ناشناس ماندن از مکانیزم های دفاعی برای برقراری ارتباط هر چه بهتر با مرکز کنترل و فرمان هکر است.

مهندسی اجتماعی

ما حملات مجاز مهندسی اجتماعی را انجام می دهیم که این حملات معمولاً به تهیه و ارائه کمپین های فیشینگ با هدف قرار دادن کارمندان مشتری اشاره دارد. هدف حمله به صورت جداگانه با هر مشتری ممکن است برنامه ریزی شود.

سناریو های دیگری نیز ممکن است برای کاربران WiFi مستقر در محل قابل انجام باشد که بواسطه یک سخت افزار جانبی یک AP سرکش (EvilTwin) فعال شود. برقراری اولین ارتباط کارمندان با شبکه بیسیم موجب می شود سناریو MiTM حملات (Man-in-The-Middle) برای تزریق فایل های اجرای مخرب در ترافیک یا ربودن پرونده های بارگیری شده برای دستیابی بیشتر به آنها قابل انجام باشد.

شاسایی داخلی

شناسایی داخلی (Discovery) شامل تکنیک هایی است که یک مهاجم ممکن است برای کسب اطلاعات در مورد سیستم و شبکه داخلی از آنها استفاده کند. این تکنیک ها به مهاجمان کمک می کند تا قبل از تصمیم گیری درباره نحوه کار، محیط را مشاهده کرده و جهت گیری کنند .اطلاعات حاصل شده به مهاجمان اجازه می دهد تا آنچه را که می توانند کنترل کنند و آنچه در اطراف نقطه ورود آنها است کشف کنند و دریابند که چگونه میتوان بعد از نفوذ از سیستم قربانی بهره برداری موردنظر را انجام داد. در این راستا ابزارهای سیستم عامل بصورت بومی وجود دارند که اغلب به منظور جمع آوری اطلاعات استفاده می شوند.

حرکت جانبی

حرکت جانبی شامل تکنیک هایی است که مهاجمان برای ورود و کنترل سیستم های از راه دور در شبکه استفاده می کنند. پیگیری هدف اصلی اغلب نیاز به کاوش در شبکه برای یافتن هدف خود و متعاقبا دستیابی به آن دارد. رسیدن به هدف اغلب شامل چرخش از طریق چندین سیستم و حساب برای به دست آوردن است. مهاجمان ممکن است ابزارهای دسترسی از راه دور خود را برای انجام Lateral Movement یا استفاده از اعتبارات مجاز با شبکه محلی و ابزارهای سیستم عامل (که ممکن است مخفی باشد)، نصب کنند.

مجموعه بهره مندی

این مجموعه بهره مندی (Collection) متشکل از تکنیک هایی است که مهاجمان ممکن است از آنها برای جمع آوری اطلاعات استفاده کنند و اطلاعات منابع مورد هدف جمع آوری شود. غالباً، مرحله بعد پس از جمع آوری داده ها سرقت آنهاست. منابع قربانی معمولا شامل انواع مختلف درایو، مرورگرها، صوتی، تصویری و ایمیل است. روش های معمول جمع آوری شامل گرفتن عکس از صفحه و ورودی صفحه کلید است.

شبیه سازی دشمن

ما قادر به انجام حملات شبیه سازی شده در سطح کیفی APT (تهدید مداوم پیشرفته) به واسطه تکنیک های CPH (سایبر-فیزیکی-انسانی) هستیم. منظور از عملیات تیم های قرمز، انعکاس سناریوهای واقعی حمله سایبری است که ممکن است برای یک سازمان خاص باشد.

از تمرینات تیم قرمز به منظور ارزیابی وضعیت امنیتی فعلی در یک شرکت هدفمند، آگاهی کارکنان و همچنین زمان واکنش تیم های امنیتی داخلی مانند SOC (مرکز عملیات امنیتی) استفاده می شود.

تیم قرمز همواره میکوشد تا روش های ابتکاری خود را در تمامی مراحل مورد نیاز حمله بکار گیرد، از این روی کیفیت حمله و محک زدن تدابیر تیم های آبی همواره به سطح دانش بکار برده شده در حمله تیم قرمز بستگی دارد.

حملات فیزیکی و شبکه

هدف اصلی آزمایش امنیت فیزیکی در صورت پیاده سازی سناریو های تیم قرمز که بر مبنای دستیابی به ساختمان سازمان، مناطق دسترسی محدود، اسناد، دستگاه های شرکت و شبکه داخلی خواهد بود، حملات فیزیکی که بر مبنای تجهیزات جانبی پیاده سازی می شود میتواند بسیار خطرناک بوده و خارج از دید مکانیزم های دفاعی باشد.

به عنوان بخشی از عملیات تیم قرمز، حملات شبکه را هم به صورت خارجی و هم به صورت داخلی انجام می دهیم، جایی که هدف اصلی دستیابی به منابع مهم شرکت، داده ها یا راهی برای ورود به شبکه داخلی است .اما در اکثر موارد پس از دستیابی به دسترسی اولیه به شبکه با استفاده از مهندسی اجتماعی یا دسترسی فیزیکی، برای تشدید حمله استفاده می کنیم.