پیشنهاد طرح
خدمات تیم قرمز

تهیه شده توسط
شرکت ارتباط گستر خاورمیانه آپادانا

تعهد عدم افشای اطلاعات:

سند حاضر فقط به منظور ارزیابی دریافت کننده سند ، توسط شرکت ارتباط گستر خاورمیانه تهیه شده است. اطلاعات موجود در این سند تحت مالکیت شرکت ارتباط گستر خاورمیانه می باشد . انتشار، افشا یا استفاده از این سند یا محتویات آن برای هر گونه مقاصدی غیر از ارزیابی دریافت کننده سند، بدون اجازه شرکت ارتباط گستر خاورمیانه ،امکان پذیر نمی باشد.
کلیه مطالب این سند، اطلاعات متعلق به شرکت ارتباط گستر خاورمیانه می باشد و نقل یا کپی یا به اشتراک گذاشتن بدون اجازه کتبی قبلی ممنوع است.

Non Disclosure Agreement:

ErtebatGostar Co. has created this document for your evaluation only. It contains proprietary information. Without our express permission you may not publish, disclose, or use this document or any of its contents for any purpose other than your evaluation.This document is the intellectual property of ErtebatGostar Co. and may not be reproduced or transmitted in any form or by any means, or forwarded to any third party, without prior written consent from ErtebatGostar Co.

کنترل سند

مشخصات سند

مشخصه	مقدار
نام درخواست کننده خدمات	شرکت .....
عنوان سند	پیشنهاد طرح – خدمات تیم قرمز
طبقه بندی	محرمانه
مورد استفاده	پیشنهاد

دریافت کنندگان سند

نام	عنوان	نمایندگی از
جناب مهندس ...	–	شرکت ...

سابقه تغییرات سند

نسخه	تاریخ	وضعیت	تهیه کننده	توضیحات
۱/۰		طرح اولیه	دپارتمان امنیت	پیش نویس اولیه

فهرست مطالب :

1. مقدمه:

هر سازمان یا شرکت اطلاعاتی در اختیار دارد که از دست دادن این اطلاعات برای آنها بسیار پر هزینه خواهد بود. همچنین افراد، شرکت‌ها و یا سازمان‌هایی هستند که برای بدست آوردن این اطلاعات حاضر به انواع هزینه‌ها هستند. این گروه‌ها به نام دشمنان سایبری و یا APT (Advanced Persistent Threat) شناخته می‌شود. دشمنان سایبری همواره به دنبال آسیب رسانی و دزدیدن اطلاعات شما هستند. به همین منظور اکثر سازمان‌ها و شرکت‌ها تیم‌هایی را برای حفظ امنیت سایبری خود استخدام می‌کنند. به این گروه تیم آبی (Blue Team) گفته می‌شود. در مقابل تیم آبی تیم قرمز (Red Team) قرار دارد. تیم‌های قرمز سعی دارند با شبیه سازی تکنیک‌های دشمن سایبری، ساختارهای دفاعی را بهبود بخشند.

خدمات تیم قرمز برخلاف خدمات تست نفوذ که به منظور شناسایی عواقب exploit کردن نقاط ضعف امنیتی به کار می‌روند، به منظور محک زدن قدرت شناسایی و دفاع تیم‌های آبی انجام می‌شوند. به همین منظور بهتر است تیم آبی در جریان مانور تیم قرمز نباشند تا رفتار و رویه‌های آنها نسبت به رفتار و رویه‌های معمول تغییری نکند. گزارش‌های تیم قرمز اطلاعاتی از ضعف‌های ساختاری مجموعه در اختیار مدیریت قرار خواهد داد که با استناد به آن می‌توان این نقاط را بهبود بخشید.

۲. مانور تیم قرمز :

به عملیات تیم قرمز به منظور نفوذ به سازمان، مانور تیم قرمز گفته می‌شود.

مانور تیم قرمز به منظور **شناسایی ضعف‌های امنیتی**
در یک محیط واقعی با دید دشمن سایبری بر روی اهداف
خاص به منظور **بهبود امنیت سازمان** صورت می‌پذیرد.

هدف اصلی مانورهای تیم قرمز ارائه گزارشی است که تیم آبی بتواند با استناد با آن و همکاری تیم قرمز نقاط ضعف خود را شناسایی نموده و در راستای رفع آنها اقدام نماید. این ضعف‌ها ممکن است مربوط به تکنولوژی‌ها، تنظیمات اعمال شده، ساختارها و یا حتی کمبود امکانات باشد.
در ادامه به توصیف قسمت‌های مختلف تعریف می‌پردازیم :

۲-۱. شناسایی ضعف‌های امنیتی :

برای شناسایی ضعف‌های امنیتی، کارشناسان تیم قرمز از تکنیک‌هایی شبیه به تکنیک‌های تست نفوذ استفاده می‌کنند. تفاوت اصلی این تکنیک‌ها و ابزار با تکنیک‌ها و ابزارهای تست نفوذ، تلاش تیم قرمز برای مخفی ماندن این عملیات است. بدین منظور کارشناسان سعی می‌کنند از ابزارهای داخلی سیستم عامل و پروتکل‌های معمول شبکه مانند smb، WMIC، RDP، SSH ، VNC، PowerShell و .... استفاده کنند تا فعالیت‌های مشکوک کمتری تولید کنند و احتمال کشف حضور آنها توسط تیم آبی کاهش یابد. به همین علت مانورهای تیم قرمز دارای پیچیدگی بیشتری نسبت به تست نفوذ هستند و زمان بیشتری خواهند برد.

۲-۲. در یک محیط واقعی با دید دشمن سایبری :

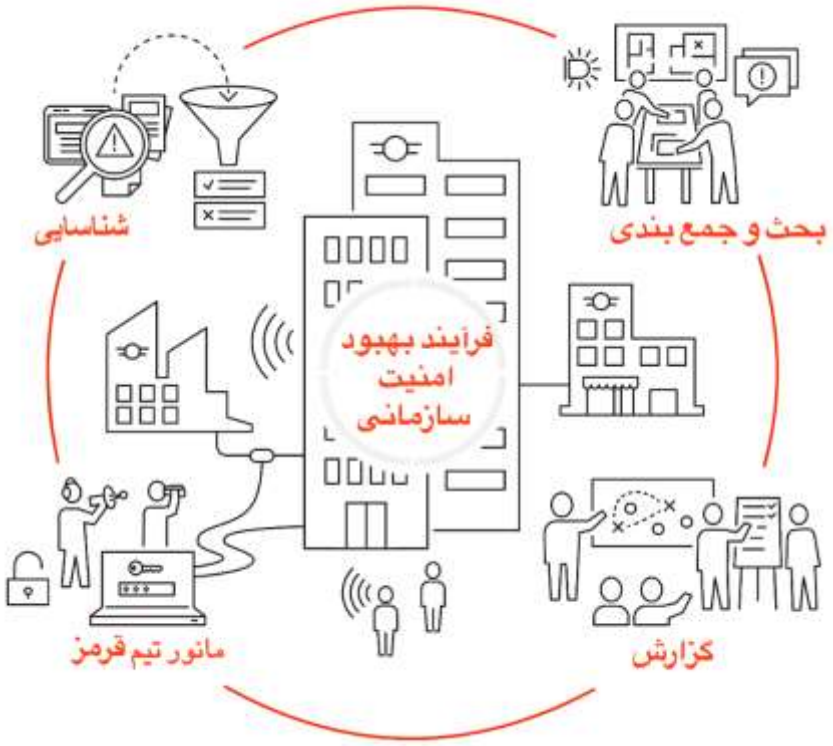
هدف اصلی مانورهای تیم قرمز محک زدن ساختارهای امنیتی در مقابل نفوذ دشمنان سایبری است، بدیم منظور تیم قرمز در ابتدا باید با تحقیق در مورد دشمن سایبری، روش‌ها (Tactics) و تکنیک‌ها (Techniques) و رویه‌های (Procedures) آنها را استخراج کنند. شناسایی این موراد ممکن است بسیار زمانبر بوده و به سایر تخصص‌ها مانند Threat Hunting نیاز داشته باشند. در صورتی که سازمان تیمی برای Threat Hunting در اختیار داشته باشد، نتایج تحقیقات آنها منبع بسیار مناسبی برای طراحی حمله‌ی تیم قرمز است. همچنین چنانچه سازمان قبلا مورد حمله‌ی سایبری قرار گرفته باشد، مستندات این حمله منبع بسیار مناسبی برای طراحی حمله‌ی تیم قرمز است. این منابع کمک خواهند نمود تا حمله‌ی تیم قرمز در شبیه‌ترین حالت به حمله‌ی APT باشد که

سازمان‌هایی شبیه به سازمان شما را مورد حمله قرار می‌دهند تا بیشترین اطلاعات مفید را در اختیار تیم امن سازی قرار دهد.

۲-۳. بهبود امنیت سازمان :

هدف نهایی مانورهای تیم قرمز شناسایی نقاط ضعف است. بدین منظور کلیه‌ی پروسه‌های شناسایی، اقدام، و recovery در شرایط واقعی مورد آزمون قرار خواهد گرفت. در قدم اول تیم قرمز پس از دسترسی اولیه به پیشرفت خود در شبکه تا رسیدن به بالاترین سطح دسترسی که معمولا Domain Administrator است، ادامه خواهند داد. پس از این مرحله چنانچه هنوز تیم آبی متوجه حضور انها در شبکه نشده باشد، با قطع یک یا چندین سرویس در شبکه اعلام حضور می‌کنند. پس از اعلام حضور مشخص می‌شود که آیا تیم امن سازی توانایی شناسایی رد پای نفوذگران در شبکه را دارند و می‌توانند به موقع دسترسی آنها را قطع نمایند. سپس گزارش کلیه‌ی مراحل مانور در اختیار تیم امن سازی قرا می‌گیرد. تیم آبی با استفاده از اطلاعات این گزارش نقاط ضعف ساختاری را متوجه شده و راهکارهای پیشنهادی رفع آنها را تدوین می نمایند. در نهایت با تشکیل جلسات تیم قرمز و آبی از بین راهکارهای رفع این نقایص امنیتی بهترین راهکار انتخاب شده و توسط تیم آبی پیاده سازی خواهد شد.

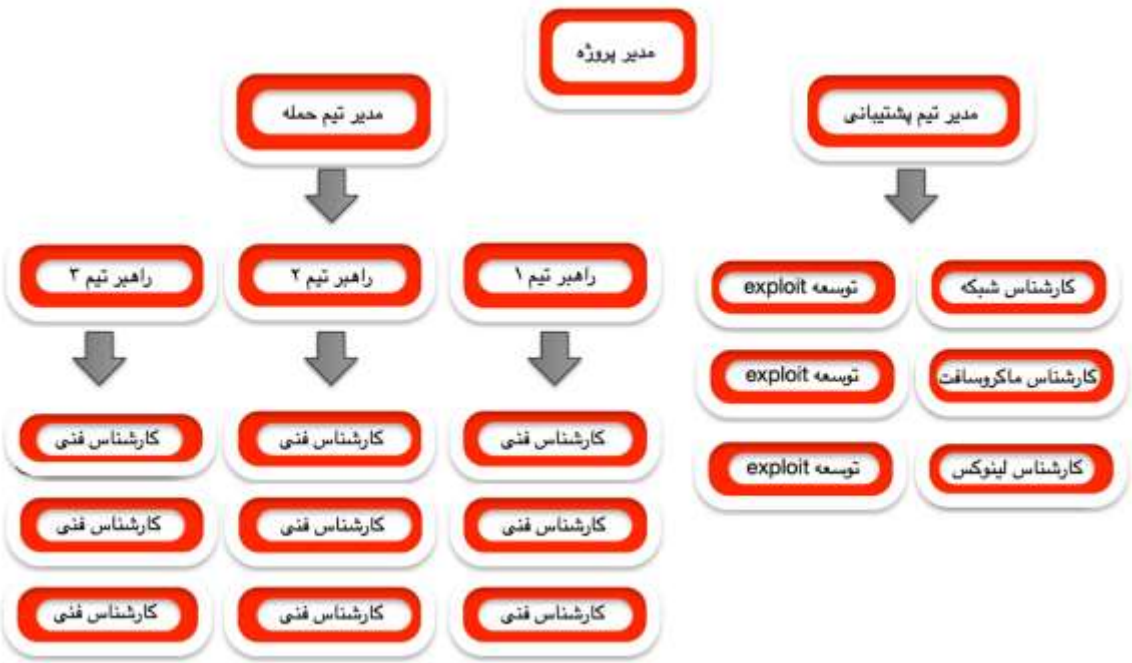
در شکل ۱ فرآیند کلی بهبود امنیت سازمانی با استفاده از مانورهای تیم قرمز ترسیم شده است.



شکل ۱ : فرآیند بهبود امنیت سازمانی با استفاده از مانور تیم قرمز

۳. اعضای تیم قرمز :

هر تیم قرمز، از متخصصین امنیت سایبری با تخصص‌های مختلف تشکیل شده است. در حالی که تیم‌های تست نفوذ عمدتا از کارشناسان تست نفوذ تشکیل شده است، تیم‌های قرمز علاوه بر کارشناسان تست نفوذ به اعضایی مانند کارشناسان شبکه (Network Administrators)، کارشناسان شبکه‌های ماکروسافتی(Microsoft Sys Admin)، کارشناسان سیستم‌عامل لینوکس (Linux Sys Admin) و متخصصین مهندسی اجتماعی (Social Engineering) نیاز دارند. چنانچه منابع تیم قرمز محدود هستند، می‌توان محدوده‌ی هدف را کوچکتر نمود تا با تیم‌های کوچکتر نیز بتوان مانور را ادامه داد. اگرچه پیشنهاد می‌شود اهداف تحت هیچ شرایطی محدود نباشند، چرا که دشمنان سایبری برای حمله به اهداف مختلف، محدودیتی ندارند و نفوذ ممکن است از قسمت‌هایی انجام شود که هنگام مانور تیم قرمز در اهداف وجو نداشته‌اند و نقاط ضعف آنها کشف و بررسی نشده است.
در شکل ۲ یک ساختار پیشنهادی مناسب تیم قرمز را مشاهده می‌نمایید.



شکل ۲ : ساختار پیشنهادی تیم قرمز

در مراحل نفوذ تیم توسعه‌ی exploit با تولید بد افزارهای مورد نیاز تیم حمله آنها را برای رسیدن به اهداف خود یاری می‌رسانند. استفاده از این بد افزارها احتمال شناسایی حرکات تیم قرمز توسط نرم افزارهای حفاظتی مانند Anti-Virus و NIPS بسیار کاهش می‌دهد. همچنین کارشناسان شبکه از تخصص خود برای شناخت بهتر زیر

ساخت استفاده کرده و با اشتراک این اطلاعات با تیم‌های حمله و تیم توسعه exploit به آنها در رسیدن به اهداف خود کمک می‌کنند. همچنین متخصصین مهندسی اجتماعی (Social Engineering) برای گرفتن دسترسی اولیه از روش‌هایی مانند phishing و vishing با تیم حمله همکاری خواهند نمود. علت وجود چندین تیم حمله، نفوذ از راه‌های مختلف به سیستم است. بدین صورت چنانچه دسترسی یکی از تیم‌ها توسط تیم آبی کشف و قطع شد، دسترسی کلی تیم باقی خواهد ماند.

۴. مراحل نفوذ تیم قرمز:

مدل‌های بسیاری سعی در مکتوب سازی فرآیندهای تیم قرمز داشته‌اند. در این میان مدل‌های موفقیت بیشتری دارند که بیشتر شبیه به فرآیندی باشند که دشمنان سایبری یا APTها برای نفوذ طی می‌کنند. APT مخفف عبارت Advanced Persistent Threat می باشد. این عبارت به متخلفان سایبری اطلاق می‌شود که ۳ ویژگی زیر را در کنار یکدیگر دارند.

- **حرفه‌ای هستند** : این گروه‌ها از مجرمان سایبری تشکیل شده‌اند که در حرفه‌ی خود بسیار حرفه‌ای بوده و از سطح فنی بالایی برخوردار هستند.
- **سـماجت دارند** : این گروه‌ها انگیزه‌ی بالایی برای نفوذ دارند و تا وقتی که موفق نشـوند دسـت از تلاش بر نخواهند داشت.
- **تهدید هســـتند** : این گروه‌ها پس از نفوذ اقدام به اســـتخراج اطلاعات و پس از آن ممکن اســـت اعمال خرابکارانه‌ی در راستای نابود سازی اطلاعات و یا قطع سرویس انجام دهند.

دانسـتن تکنیک‌ها، تاکتیک‌ها و روندهایی که دشـمن سـایبری برای نفوذ به شـبکه‌ی یک شـرکت یا سـازمان طی می‌کند، نقش اسـاسـی در مفید بودن خروجی این حملات خواهد داشـت. زیرا با شـبیه سـازی انها می‌توان قدرت شناسایی و دفاعی تیم‌های امن سازی را در هنگام حمله‌ی واقعی مشاهده نمود.

مدل‌های زیادی به بررســـی رفتار APTها می‌پردازند، در این میان مدل Cyber kill Chain از شـــرکت Lockheed Martin یکی از جامع‌ترین مدل‌ها اســـت. در ادامه به تشـــریح هر مرحله از نفوذ با این روش می‌پردازیم. مراحل این مدل در شکل ۳ آورده شده است.

شکل ۳: Cyber Kill Chain by Lockheed Martin

I. **جمع آوری اطلاعات :** در این مرحله نفوذگران اقدام به جمع آوری اطلاعات از منابع مختلف می‌کنند. به تکنیک‌های مورد استفاده در این روش به اختصار OSINT[1] می‌گویند. این مرحله یکی از زمانبرترین مراحل است، زیرا که موفقیت کل نفوذ بستگی به شناخت حاصل شده از افراد، تکنولوژی‌ها و ساختار شبکه دارد که در این مرحل بدست می‌آید.

II. **آماده سازی بد افزار :** در این مرحله با استفاده از اطلاعات جمع آوری شده یک بد افزار به صورت اختصاصی برای هدف نوشته خواهد شد. این بد افزار به گونه‌ای تولید خواهد شد که بازدهی حداکثری را با توجه به تکنولوژی‌های سمت هدف داشته باشد، و در عین حال کشف آن توسط تیم‌های امن سازی مشکل باشد.

III. **تحویل :** در این مرحله بد افزار مورد نظر معمولا به افراد مشخصی توسط ایمیل و یا روش‌های دیگری ارسال می‌شوند. این افراد به گونه‌ای انتخاب می‌شوند که بیشترین احتمال باز کردن بد افزار را داشته باشند. همچنین معمولا بد افزار نهایی در این مرحله ارسال نخواهد شد و فقط یک stager[2] استفاده می‌شود، تا در صورت فاش شدن عملیات، بد افزاری اصلی در اختیار تیم امن سازی قرار نگیرد. در صورتی که به دلیل وجود محدودیت‌های مالی، مدت زمان و یا منابع مالی پروژه‌های تیم قرمز محدود

[1] Open Source Intelligence

[2] یک نرم افزار که وظیفه‌ی ایجاد دسترسی اولیه بر روی سیستم را دارد.

باشد، می‌توان مراحل ۱ تا ۳ را با همکاری کارفرما انجام داد. به این صورت که اطلاعات مورد نیاز در رابطه با شبکه‌ی سازمان را تحویل تیم قرمز داده و بد افزار اولیه را با همکاری بر روی یکی از سیستم‌ها با دسترسی کاربر عادی نصب نمایند. این سطح دسترسی اولیه مدت زمان مانور و هزینه‌های اجرایی را کاهش خواهد داد اما کیفیت گزارش نهایی را حفظ خواهد کرد.

IV. **نفوذ :** پس از تحویل و اجرا شدن stager، مهاجمین اقدام به شناسایی محیط و جمع آوری اطلاعات می‌کنند. یکی از مهمترین بخش‌های نفوذ اولیه، بررسی است که آیا stager در یک محیط Honeypot اجرا شده است؟ چنانچه تیم قرمز در یکی از تله-های تیم آبی گیر افتاده باشد، باید کلیه‌ی عملیات‌های خود را متوقف نماید، زیرا با لو رفتن بد افزار و روش نفوذ، حمله به صورت کامل توسط تیم آبی خنثی می‌شود و تیم قرمز باید ماه‌ها صرف برنامه ریزی و حمله‌ی مجدد نماید.

V. **نصب :** در این مرحله بد افزار به منظور انجام اعمال مختلف بر روی سیستم‌های مختلف شبکه نصب می‌شود. یکی از وظیفه‌های اصلی بد افزار حفظ دسترسی نفوذگران بر روی سیستم است.

VI. **اتصال به مرکز :** پس از نصب ارتباط با مرکز C&C[3] نفوذگران صورت می‌گیرد. در این مرحله بد افزار منتظر دستورات نفوذگران برای اعمال مختلف می‌ماند.

VII. **استخراج :** در این مرحله اطلاعات مورد نیاز از سیستم‌ها استخراج می‌شود. پس از این مرحله نفوذگران ممکن است اقدام به خرابکاری نموده و یا حضور خود در شبکه را برای آینده حفظ نمایند.

تیم‌های قرمز با شبیه سازی همه‌ی این مراحل، زمان کشف و اقدام تیم امن سازی را در مقابل این حملات پیشرفته محک می‌زنند.

۵- گزارش نهایی :

در این مرحله تیم قرمز تمام فرآیندهای طی شده برای نفوذ به سیستم، دسترسی‌های گرفته شده را به صورت یک گزارش اماده کرده و در اختیار تیم فناوری اطلاعات سازمان قرار خواهد داد. این گزارش‌ها باید به گونه‌ای

[3] Command and Control

تهیه و تنظیم شوند که بیشترین کمک را به تیم امن سازی برای بهبود شرایط موجود نماید. همچنین این گزارش می‌تواند منبع خوبی برای بررسی بازده هزینه‌های انجام شده در بخش امن سازی باشد.

۶. تشکیل تیم بنفش :

پس از بررسی گزارش توسط تیم آبی، تیم قرمز و آبی با یکدیگر ترکیب شده و تشکیل تیم بنفش را می‌دهند. وظیفه‌ی اصلی تیم بنفش بررسی راهکارهای ارایه شده توسط تیم امن سازی است. این راهکارها باید به صورت همزمان توسط هر دو تیم بررسی شود به صورتی که هم مشکلات فعلی را رفع نمایند، هم قابلیت اجرایی داشته باشند و هم مشکلات امنیتی جدیدی را به وجود نیاورند. خروجی جلسات تیم بنفش راهکارهای مناسبی برای افزاش امنیت سازمان ارایه خواهد داد.

۷. چرخه‌ی مانور قرمز :

برای حفظ آمادگی تیم آبی، بهتر است مانورهای تیم قرمز تکرار شوند. این تکرارها ممکن است به صورت سالیانه و یا در صورت شناسایی یک APT جدید توسط تیم Threat Hunting اتفاق بیافتد.