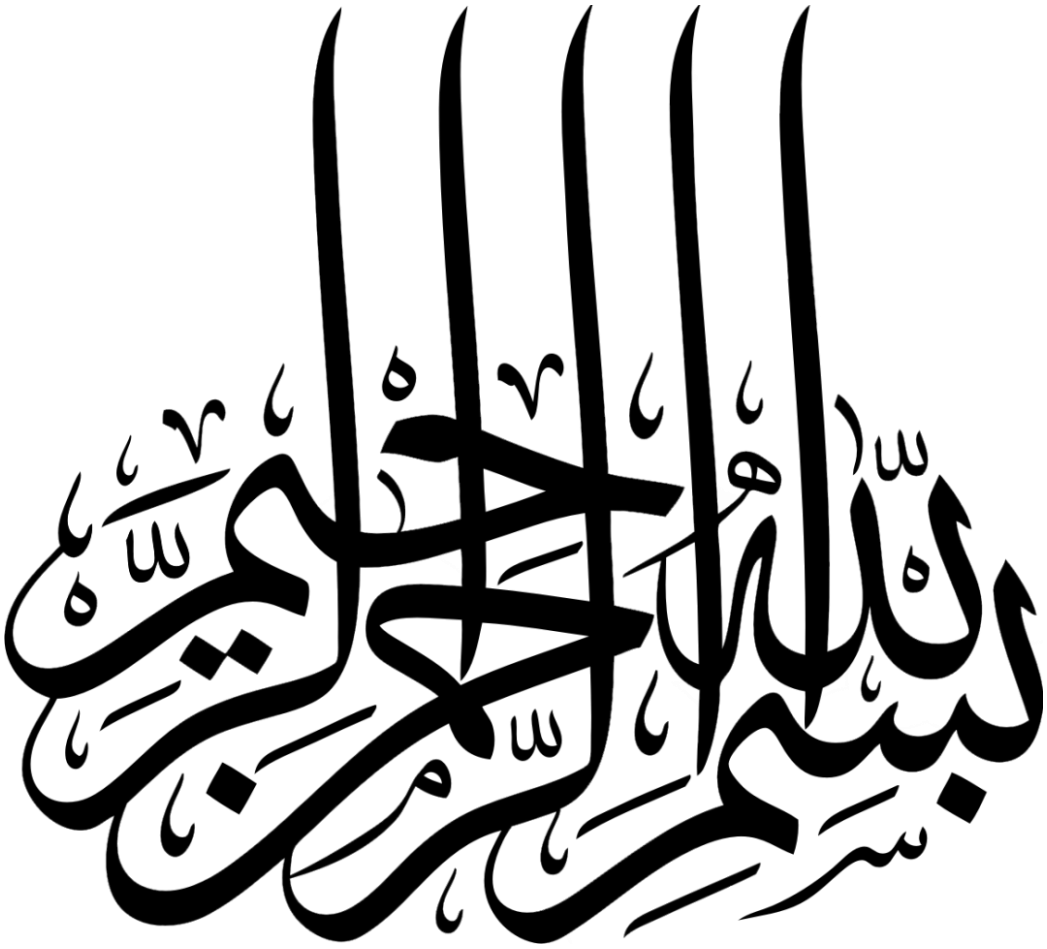
بسم الله الرحمن الرحیم

Assumed Breach

رویکردی واقع‌گرایانه‌تر برای ارزیابی امنیت سازمان

تهیه شده توسط تیم تولید محتوای وب سایت چلنجینو

مقدمه

دنیای امنیت سایبری به‌سرعت در حال تغییر است. روش‌ها و ابزارهای حمله مدام تکامل می‌یابند و مدل‌های سنتی تست نفوذ دیگر همیشه قادر به نمایش ریسک‌های واقعی سازمان‌ها نیستند. یکی از رویکردهای مدرن که توانسته جایگاه ویژه‌ای در ارزیابی امنیتی پیدا کند، تست **Assumed Breach** است.

در این روش، برخلاف تست نفوذ سنتی، فرض می‌شود که مهاجم از قبل موفق به ورود شده و اکنون درون شبکه حضور دارد. این فرض اولیه، فضای تست را به سمت واقعیت‌های امروز حملات سایبری هدایت می‌کند و به سازمان اجازه می‌دهد نقاط ضعف داخلی، قابلیت تشخیص و پاسخ به رخداد خود را به‌صورت عمیق‌تر ارزیابی کند.

در ادامه، مفاهیم کلیدی، فلسفه، مزایا، مراحل و استدلال‌های پشت این رویکرد را بررسی می‌کنیم.

چالش مدل سنتی تست نفوذ

در تست نفوذ سنتی معمولاً چند فرض پایه وجود دارد. نخست اینکه مهاجم از ابتدا هیچ دسترسی‌ای به شبکه داخلی ندارد و باید راهی برای ورود پیدا کند. به همین دلیل تمرکز اولیه اغلب روی پیدا کردن نقطه ورود از بیرون یا حتی داخل سازمان قرار می‌گیرد.

بر اساس همین نگاه، فرض می‌شود مهاجم برای پیشروی باید با اسکن‌های گسترده شبکه و سرویس‌ها آسیب‌پذیری‌ها را شناسایی کند و سپس با استفاده از اکسپلویت‌ها به سیستم‌های داخلی دسترسی پیدا کند. این مدل اگرچه سال‌ها پایه بسیاری از تست‌های نفوذ بوده است، اما همیشه بازتاب دقیقی از الگوی حملات واقعی نیست.

اما واقعیت حملات مدرن متفاوت از این فرض‌های سنتی است. مهاجمان امروزی معمولاً نیازی به نفوذ پیچیده از بیرون ندارند. آن‌ها با روش‌هایی ساده‌تر و مؤثرتر وارد شبکه می‌شوند.

در بیشتر موارد، نقطه ورود از طریق فیشینگ هدفمند یا سرقت Credentials ایجاد می‌شود. مهاجمان برای پنهان‌ماندن از دید سامانه‌های دفاعی، از انجام اسکن‌های گسترده خودداری می‌کنند و به جای بهره‌گیری از اکسپلویت‌های فنی، از خطاهای پیکربندی، ضعف در احراز هویت، یا سهل‌انگاری کاربران سوءاستفاده می‌کنند. همین تفاوت بنیادین است که نیاز به رویکردی واقع‌گرایانه‌تر مانند Assumed Breach را ضروری می‌سازد.

در نتیجه، تست نفوذ سنتی تنها بخشی از ریسک را نمایش می‌دهد و نمی‌تواند تصویری کامل از رفتار مهاجم واقعی ارائه کند.

فلسفه و هدف Assumed Breach

فلسفه Assumed Breach بر این ایده استوار است که در دنیای واقعی، سؤال اصلی دیگر این نیست که «آیا مهاجم می‌تواند وارد شود؟» بلکه موضوع اصلی این است که «پس از ورود چه کار می‌تواند انجام دهد؟»

این رویکرد می‌پذیرد که نفوذ اولیه همیشه ممکن است. چه این نفوذ از طریق یک کمپین فیشینگ انجام شود، چه با سرقت Credential، چه با سوءاستفاده از یک 0-Day یا حتی این دسترسی اولیه بوسیله خطای انسانی یک کارمند رخ داده باشد. بنابراین به جای اتلاف زمان و انرژی برای اثبات امکان ورود، تست از نقطه‌ای آغاز می‌شود که مهاجم معمولاً در دنیای واقعی در آن قرار دارد یعنی **داخل شبکه**.

در این مدل، سازمان به تست نفوذگر یک سیستم داخلی یا نقطه دسترسی معتبر ارائه می‌دهد؛ چیزی شبیه یک کامپیوتر کارمند یا یک دسترسی VPN استاندارد. گاهی برای آسان‌تر شدن اجرای Payloadهای اولیه، این سیستم با سنسورهای امنیتی محدود یا غیرفعال[1] ارائه می‌شود. هدف این کار مخفی‌کاری نیست، بلکه حذف موانع غیرضروری و تمرکز بر بخش‌هایی است که بیشترین ریسک را برای سازمان دارند.

به‌محض شروع تست، سرعت بالا می‌رود و به جای هفته‌ها تلاش برای فیشینگ یا جستجوی آسیب‌پذیری‌های خارجی، مراحل واقعی و خطرناک‌تر چرخه حمله بررسی می‌شود؛ یعنی همان چیزهایی که مهاجمان حرفه‌ای پس از نفوذ انجام می‌دهند. این مراحل شامل حرکت جانبی در شبکه، جمع‌آوری Credential از سیستم‌های مختلف، افزایش سطح دسترسی برای رسیدن به نقش‌های حیاتی یا ادمین، دستیابی به دارایی‌های حساس و در نهایت استخراج داده‌ها یا همان Exfiltration است.

به بیان دیگر، Assumed Breach یک "**Lite Red Team** یا **رد تیم سبک**" است که تلاش نمی‌کند همه آسیب‌پذیری‌ها را کشف کند، بلکه به‌دنبال پاسخ به این سؤال است:

اگر مهاجم فقط یک قدم داخل شود، چقدر می‌تواند پیشروی کند و آیا تیم دفاعی متوجه می‌شود؟

فلسفه کلیدی این رویکرد این است که امنیت واقعی تنها با جلوگیری از ورود حاصل نمی‌شود. بلکه باید توانایی سازمان در کشف، کنترل و پاسخ به فعالیت‌های مهاجم پس از ورود نیز سنجیده شود. این همان جایی است که اکثر سازمان‌ها ضعف دارند و Assumed Breach دقیقاً برای پیدا کردن همین نقاط ضعف طراحی شده است.

[1] degraded sensors

چرا Initial Access نقطه تمرکز مناسبی نیست؟

تمرکز بیش از حد بر جلوگیری از ورود اولیه[2] نه تنها پرهزینه است، بلکه می‌تواند یک امنیت کاذب و گمراه‌کننده ایجاد کند. بسیاری از مدیران اصرار دارند که «تیم قرمز باید دقیقاً مثل یک مهاجم واقعی از بیرون نفوذ کند»، اما این استدلال یک شکاف بزرگ دارد: تسترها محدودیت زمانی و بودجه‌ای دارند، در حالی که مهاجمان واقعی ممکن است ماه‌ها زمان صرف کنند، از اکسپلویت‌های ناشناخته و 0-Day استفاده کنند یا از طریق زنجیره تأمین وارد شوند. بنابراین، اگر فرد تست کننده نتواند وارد شود، به این معنی نیست که سازمان امن است؛ بلکه فقط به این معنی است که در آن بازه زمانی محدود، راهی پیدا نکرده است.

این نگاه سنتی باعث می‌شود سازمان‌ها مانند یک تخم‌مرغ عمل کنند؛ یعنی تمام توان خود را صرف ساختن یک پوسته سخت و نفوذناپذیر کنند، در حالی که بخش داخلی یا همان زرده که دارایی‌های اصلی و داده‌های حساس در آن قرار دارند، کاملاً نرم و آسیب‌پذیر باقی بماند. اگر تمام دفاع شما در لایه پیرامونی (مثل آنتی‌ویروس و فایروال) خلاصه شود، مهاجم با اولین شکاف در این پوسته، به کل دارایی‌های شما دسترسی پیدا می‌کند. امنیت واقعی زمانی معنا پیدا می‌کند که فرض کنیم پوسته شکسته شده و حالا باید از زرده محافظت کنیم.

نکته تکان‌دهنده دیگر، بحث زمان ماندگاری یا Dwell Time مهاجم در شبکه است. آمارها نشان می‌دهد که مهاجمان به‌طور میانگین ۵ تا ۶ ماه قبل از اینکه شناسایی شوند، در شبکه حضور دارند و به‌آرامی اهداف خود را پیش می‌برند. اگر تمرکز تست فقط روی نقطه ورود باشد، عملاً این بازه زمانی حیاتی که مهاجم در آن بیشترین آسیب را می‌زند، نادیده گرفته شده است. تست امنیتی باید به سازمان یاد بدهد که چطور این حضور مخفیانه را کشف و متوقف کند، نه اینکه فقط روی قفل کردن درِ ورودی اصرار بورزد.

در نهایت، خطرناک‌ترین نتیجه‌گیری از یک تست نفوذ ناموفق در مرحله ورود، این است که تصور کنیم "همه چیز امن است". عدم موفقیت تیم قرمز در ورود به شبکه در یک بازه دوهفته‌ای، هرگز به معنای نفوذناپذیر بودن سازمان در برابر یک هکر با انگیزه و صبور نیست.

فلسفه Assumed Breach با عبور از این پیش‌فرض‌های غلط، مستقیماً به سراغ سنجش تاب‌آوری شبکه در برابر مهاجمی می‌رود که هم‌اکنون داخل سازمان است؛ چرا که در دنیای امنیت، نفوذ یک **احتمال** نیست، بلکه یک **قطعیت** است که باید برای آن آماده بود.

[2] Initial Access

حملات مدرن چه می‌گویند؟

گزارش‌های تحلیلی از حملات واقعی نشان می‌دهد که بسیاری از نفوذها از مسیرهایی بسیار ساده‌تر از آنچه تصور می‌شود رخ می‌دهند. بر اساس گزارش Verizon Data Breach Investigations Report (DBIR)، فیشینگ همچنان یکی از رایج‌ترین روش‌های نفوذ به سازمان‌هاست. در بسیاری از این موارد، هدف اصلی حمله نه اجرای بدافزار پیچیده، بلکه سرقت Credentialها است؛ به این معنا که مهاجم تلاش می‌کند نام کاربری و رمز عبور یک کاربر واقعی را به دست آورد و سپس با همان هویت وارد سیستم شود.

در عمل نیز فیشینگ و سرقت اعتبارنامه‌ها اغلب در کنار یکدیگر اتفاق می‌افتند. یک ایمیل فیشینگ می‌تواند کاربر را به صفحه‌ای جعلی هدایت کند که اطلاعات ورود او را دریافت می‌کند، و از آن لحظه به بعد مهاجم می‌تواند دقیقاً مانند یک **کاربر قانونی** به سرویس‌ها و سیستم‌های سازمان دسترسی داشته باشد. این نوع دسترسی معمولاً از بسیاری از مکانیزم‌های دفاعی عبور می‌کند، زیرا از دید سیستم‌ها، فعالیت مهاجم شبیه فعالیت یک کاربر عادی به نظر می‌رسد.

علاوه بر این، آمارها نشان می‌دهد که حدود **۲۰ درصد** از رخدادهای امنیتی به نوعی با افراد داخلی[۳] مرتبط هستند؛ افرادی که ممکن است عمداً یا به‌صورت ناخواسته باعث افشای اطلاعات یا سوءاستفاده از دسترسی‌های خود شوند. در چنین سناریوهایی نیز مهاجم یا عامل تهدید از ابتدا دارای دسترسی معتبر و داخلی است.

نکته مهم این است که در همه این سناریوها (چه فیشینگ، چه سرقت Credential و چه تهدیدات داخلی) مهاجم عملاً از همان ابتدا با یک سطحی از دسترسی معتبر وارد محیط سازمان می‌شود.

دقیقاً همین واقعیت است که مبنای تفکر Assumed Breach را شکل می‌دهد:

به‌جای تمرکز صرف بر جلوگیری از نفوذ، باید فرض کرد مهاجم از قبل وارد شده و بررسی کرد که پس از ورود تا چه حد می‌تواند در شبکه پیشروی کند و به دارایی‌های حساس دست یابد.

[3] Insiders

سه اصل کلیدی برای تصمیم‌گیری بهتر (براساس HBR)

سه اصلی که در مقاله "3Ways to Improve Your Decision Making" مطرح شده‌اند، نه‌تنها برای مدیریت کسب‌وکار بلکه برای امنیت سایبری نیز کاملاً کاربردی هستند. این اصول دقیقاً نقطه‌ضعف‌هایی را هدف می‌گیرند که معمولاً باعث می‌شوند سازمان‌ها تهدیدات را دست‌کم بگیرند و تصور کنند **"برای ما اتفاق نمی‌افتد"**. رویکرد Assumed Breach دقیقاً با همین سه اصل هماهنگ است و آن‌ها را به‌صورت عملی در ارزیابی امنیتی تبدیل می‌کند.

- **کمتر مطمئن باشید (Be less certain)**: اعتماد بیش‌ازحد به کنترل‌های امنیتی یک خطای متداول است. عبارت‌هایی مثل ما بهترین آنتی‌ویروس را داریم، فایروال ما همه چیز را می‌گیرد و کاربران ما آموزش دیده‌اند، اغلب باعث ایجاد توهم امنیت می‌شوند. اصل اول یادآور می‌شود که باید احتمال شکست کنترل‌ها را همیشه در نظر گرفت. چیزی که Assumed Breach دقیقاً به آن تکیه دارد این است که فرض شود مهاجم وارد شده است.
- **بسامد حمله را بررسی کنید (Ask how often this typically happens)**: پرسش کلیدی این نیست که "آیا احتمال دارد این حمله اینجا رخ دهد؟" بلکه باید پرسید "این نوع حمله در دنیای واقعی چند بار اتفاق می‌افتد؟" وقتی آمارهایی مثل DBIR نشان می‌دهد حملات فیشینگ یا سرقت Credential بسیار رایج‌اند، منطقی است که فرض کنیم دیر یا زود یک نمونه از آن به سازمان شما هم می‌رسد. Assumed Breach بر این واقعیت بنا شده که حملات رایج، دیر یا زود موفق می‌شوند.
- **به احتمالات فکر کنید (Think probabilistically)**: ریسک همیشه حاصل‌ضرب احتمال وقوع و شدت اثر است. اگر احتمال نفوذ بالاست و اثر آن برای سازمان فاجعه‌بار، پس باید سنجید که اگر مهاجم وارد شد، چه می‌شود؟ Assumed Breach دقیقاً این بخش را می‌سنجد که شامل اثر واقعی نفوذ، مسیر پیشروی مهاجم، دسترسی‌هایی که می‌تواند به دست آورد، و این‌که دفاع داخلی سازمان چقدر واقعاً کار می‌کند.

در مجموع، این سه اصل یک پیام بسیار مهم دارند:

برای امنیت مؤثر باید از فرضیات خوش‌بینانه فاصله گرفت، به داده‌های واقعی نگاه کرد و احتمال شکست را وارد محاسبات کرد.

فازهای اصلی Assumed Breach

فازهای اصلی رویکرد Assumed Breach دقیقاً همان مراحلی هستند که یک مهاجم واقعی پس از ورود اولیه طی می‌کند. تفاوت در این است که تست، مستقیماً از این نقطه شروع می‌شود تا عمق آسیب‌پذیری سازمان سنجیده شود. چهار فاز اصلی به شکل زیر هستند:

۱. **Situational Awareness**: در این مرحله تست نفوذگر باید بفهمد کجا قرار دارد و چه امکاناتی در اختیار دارد. اینکه سیستم عضو کدام دامنه است، چه سرویس‌ها و سگمنت‌های شبکه قابل مشاهده‌اند، کاربر فعلی چه محدودیت‌هایی دارد و چه دارایی‌هایی در نزدیکی، قابل دسترس‌اند. این مرحله دقیقاً مانند باز کردن نقشه قبل از آغاز مسیر است.

۲. **Privilege Escalation**: در این مرحله تست نفوذگر پس از شناخت محیط، تلاش می‌کند از محدودیت‌های فعلی عبور کند. ابتدا در سطح Local با تبدیل یک کاربر عادی به Administrator روی همان ماشین که معمولاً سریع‌ترین و کم‌هزینه‌ترین روش است، شروع نموده و سپس در سطح Domain برای رسیدن به دسترسی‌های بالاتر اقدام می‌نماید. نکته مهم این است که هدف همیشه Domain Admin نیست؛ هر دسترسی ارزشمند مانند یک سرور حیاتی، یک حساب سرویس یا یک Token قدرتمند می‌تواند برای ادامه مسیر کاملاً کافی باشد.

۳. **Lateral Movement**: در این مرحله تست نفوذگر پس از افزایش دسترسی تلاش می‌کند به سیستم‌ها، سرورها، سرویس‌ها یا ایستگاه‌های کاری دیگر منتقل شود. این بخش معمولاً جایی است که سامانه‌های دفاعی باید فعالیت مشهودی نشان دهند. بنابراین اگر Blue Team در این مرحله هیچ علامت یا هشداری مشاهده نکند، نشان‌دهنده یک ضعف جدی در توان تشخیص و پایش شبکه است.

۴. **Data Exfiltration**: در این مرحله هدف نشان دادن اثر واقعی نفوذ است؛ نیازی نیست داده واقعاً خارج شود، همین که امکان خروج یا ایجاد یک مسیر امن برای انتقال داده ثابت شود کافی است. این مرحله معیار واقعی ریسک سازمان را آشکار می‌کند، زیرا اگر مهاجم بتواند داده حساس را بی‌صدا و بدون شناسایی خارج کند، یعنی در یک سناریوی واقعی هم دقیقاً همین مسیر قابل تکرار است.

این چهار مرحله ماهیت Assumed Breach را نشان می‌دهد. در واقع به‌جای تمرکز بر اینکه مهاجم چطور وارد شده است، تمرکز روی این است که وقتی وی وارد شد، چه فعالیت هایی قابل انجام است. همین سؤال، تصویر واقعی‌تری از ریسک سازمان را ارائه می‌دهد.

چرا Assumed Breach مؤثرتر است؟

رویکرد Assumed Breach به این دلیل مؤثرتر است که به‌جای شبیه‌سازی یک بخش محدود از حمله (ورود اولیه)، کل مسیر واقعی مهاجم پس از ورود را بررسی می‌کند.

۱. تمرکز بر رفتار پس از ورود

در سناریوهای واقعی، مهاجمان دیر یا زود موفق به ورود می‌شوند. بنابراین تمرکز اصلی باید روی این باشد که اگر مهاجم وارد شد چه می‌شود. چطور حرکت می‌کند، چه چیزهایی را می‌بیند، و چگونه به داده‌های حساس می‌رسد. Assumed Breach دقیقاً این مرحله را آزمایش می‌کند، یعنی همان جایی که بیشترین خسارت رخ می‌دهد.

۲. ارزیابی Detection و Response

بسیاری از سازمان‌ها روی جلوگیری از نفوذ هزینه کرده‌اند، اما نمی‌دانند پس از نفوذ چه اتفاقی می‌افتد. Assumed Breach کمک می‌کند بفهمید:

- آیا تیم Blue Team رفتار غیرعادی را می‌بیند؟
- SIEM چه لاگ‌هایی تولید می‌کند؟
- EDR به lateral movement واکنش نشان می‌دهد؟
- تیم امنیت چقدر سریع و چقدر دقیق پاسخ می‌دهد؟

این دقیقاً همان جایی است که امنیت واقعی سنجیده می‌شود.

۳. شبیه‌سازی سناریوهای حمله واقعی

بخش بزرگی از نفوذها به دلیل ضعف‌های غیر تکنیکال مانند Credential reuse، Misconfiguration یا دسترسی های بیش از حد یا اشتباه اتفاق می‌افتند. این موارد در تست نفوذ سنتی معمولاً دیده نمی‌شوند. اما در Assumed Breach کاملاً مشهود و قابل ارزیابی هستند.

۴. یافته‌ها عملی‌تر و قابل اقدام‌تر (Actionable)

به‌جای ارائه یک لیست طولانی از CVEها و آسیب‌پذیری‌های پراکنده، خروجی Assumed Breach معمولاً شامل مسیرهای واقعی حمله است:

- از سیستم X با این دسترسی شروع کردیم.
- به دلیل Misconfiguration به Y رسیدیم.
- به داده حساس Z بدون دیده شدن دست یافتیم.

این نوع یافته‌ها برای مدیران، SOC، تیم IT و حتی مدیران ارشد بسیار ملموس‌تر و قابل اجرا هستند، چون اثر واقعی یک نفوذ را در قالب داستان[4] می‌بینند. به همین دلیل است Assumed Breach را Lite Red Team می‌نامند.

Assumed Breach بسیاری از مزایای Red Team واقعی مانند شبیه‌سازی رفتار مهاجم، ارزیابی Detection و Response و آزمایش مسیرهای حمله را دارد اما سبک‌تر بوده و امکان اجرای سریع‌تر، هزینه کمتر و خروجی واقعی و اثرگذار را فراهم می‌کند و به همین خاطر یک نسخه کوچک‌شده اما بسیار مفید از Red Team محسوب می‌شود.

[4] Attack Path

نتیجه‌گیری

تست Assumed Breach پاسخی هوشمندانه به پیچیدگی‌های حملات سایبری امروزی است. این رویکرد با کنار گذاشتن این فرض که پوسته سازمان نفوذناپذیر است، مستقیماً به سراغ سناریوی واقعی می‌رود. با اتخاذ این استراتژی، سازمان‌ها می‌توانند به سه دستاورد کلیدی برسند:

- **ارزیابی واقع‌گرایانه:** سنجش دقیق امنیت داخلی و شناسایی مسیرهای پنهان حمله که در تست‌های سنتی دیده نمی‌شوند.
- **سنجش تیم دفاعی (Blue Team):** ارزیابی واقعی توانایی Detection و Response در لحظات حساس نفوذ.
- **تصمیم‌گیری داده‌محور:** اختصاص بودجه و منابع بر اساس ریسک‌های ملموس و شبیه‌سازی‌شده، نه فرضیات تئوریک.

در نهایت، Assumed Breach پارادایم امنیتی را تغییر می‌دهد؛ تمرکز را از لایه بیرونی و آسیب‌پذیر یا همان پوسته برداشته و مستقیماً بر حفاظت از زرده یعنی دارایی‌های حیاتی و داده‌های حساس سازمان معطوف می‌کند. این تنها راه برای تاب‌آوری در برابر مهاجمانی است که زمان، انگیزه و منابع کافی برای عبور از هر سد دفاعی را دارند.

اگر مهاجمان سال‌هاست از این روش استفاده می‌کنند، آیا زمان آن نرسیده که ما هم Assumed Breach را وارد چرخه ارزیابی امنیتی سازمان کنیم؟

این مقاله برگرفته از بخش‌هایی از دوره آموزشی تست نفوذ شبکه SEC560 از مؤسسه SANS است.