آموزش CEH (هکر کلاه سفید): مراحل انجام هک اخلاقی چیست؟

ارزیابی‌های امنیتی که یک هکر اخلاق‌مدار بر مبنای آن‌ها کار می‌کند از سه مرحله پیشبرد پروژه که اهداف و دستورالعمل‌هایی تدوین می‌شوند، انجام ارزیابی و آزمایش‌های نفوذ و سرانجام ارائه گزارشی در ارتباط با فعالیت‌ها تشکیل شده است.

برای مطالعه قسمت قبل آموزش رایگان **دوره CEH** اینجا کلیک کنید.

روش‌های مختلف هک اخلاقی

در شماره‌های گذشته به این موضوع اشاره کردیم که یک هکر اخلاقی باید مهارت‌های مختلفی داشته باشد، اکنون ممکن است این سوال برای پیش آمده باشد که هکر اخلاقی چگونه می‌تواند از این مهارترها استفاده کند؟
زیرساخت‌های فناوری‌اطلاعات یک سازمان می‌تواند به روش‌های مختلف ارزیابی شده یا مورد حمله قرار گیرند. برخی از متداول‌ترین روش‌هایی که یک هکر قانون‌مندار برای هک اخلاقی از آن‌ها استفاده می‌کند به شرح زیر است:

گردآوری اطلاعات: این روش آزمایش به دنبال این است که ببیند چه نوع اطلاعاتی از سازمان به بیرون نشت پیدا می‌کند و چگونه یک حمله‌کننده ممکن است این اطلاعات را به دست آورد.

آزمایش نفوذ خارجی: این هک اخلاقی درصدد شبیه‌سازی انواع حملات است که می‌توانند از طریق اینترنت هدایت شوند. این حملات می‌توانند پروتکل انتقال ابرمتن (HTTP)، پروتکل انتقال پست الکترونیکی ساده (SMTP)، زبان پرس و جو ساختریافته (SQL) یا هر سرویس در دسترس را هدف قرار دهند.

آزمایش نفوذ داخلی: این هک اخلاقی انواع حملات و فعالیت‌هایی که ممکن است توسط یک فرد مجاز و دارای مجوز از درون شبکه سازمانی انجام شود را شبیه‌سازی می‌کند.

آزمایش فنی شبکه: دیوارآتش، سامانه تشخیص نفوذ، روترها و سوئیچ‌ها را شامل می‌شود.

آزمایش DoS: این روش تست می‌تواند برای آزمایش تاب‌آوری سیستم یا عدم تأیید توانایی آن در برابر حملات DoS انجام شود.

آزمایش شبکه بی‌سیم: این حمله سیستم‌های بی‌سیم را ارزیابی می‌کند. این حمله ممکن می‌تواند سیستم‌های بی‌سیمی که از پروتکل‌های RFID، ZigBee ، بلوتوث یا سایر پروتکل‌ها استفاده می‌کنند را ارزیابی کند.

آزمایش برنامه‌های کاربردی: آزمایش برنامه کاربردی برای بررسی کنترل‌های ورودی و نحوه پردازش داده‌ها طراحی شده است. در این حمله بخش‌های مختلف یک برنامه ارزیابی می‌شود.

آزمایش مهندسی اجتماعی: حملات مهندسی اجتماعی کارکنان سازمان را هدف قرار داده و سعی می‌کند به نوعی آن‌ها را فریب دهد تا مجوزهای خود را در اختیار هکر قرار دهند. آموزش کارکنان، کنترل‌های مناسب، خط‌مشی‌ها و رویه‌ها در طول مدت حمله محک زده می‌شوند.

آزمایش امنیت فیزیکی: این شبیه‌سازی به دنبال آزمایش کنترل‌های فیزیکی سازمان است. سیستم‌هایی مانند درها، دروازه‌ها، قفل‌ها، دوربین‌های مدار بسته، سامانه‌های هشدار دهنده آزمایش می‌شوند تا میزان نفوذپذیری آن‌ها مشخص شود.

آزمایش سیستم تأیید هویت: این حمله شبیه‌سازی شده کنترل‌های احراز هویت را ارزیابی می‌کند. اگر امکان دور زدن کنترل‌ها وجود دارد، یک هکر اخلاقی بررسی می‌کند که چه تعداد از کنترل‌ها آسیب‌پذیر هستند.

آزمایش بانک اطلاعاتی: این حمله برای ارزیابی سرورهای SQL استفاده می‌شود.

آزمایش سامانه‌های ارتباطی: این روش حمله ارتباطاتی از قبیل Voice over IP (VoIP ، PBX)، مودم‌ها و سیستمرهای ارتباط صوتی را بررسی می‌کند.

حمله با هدف سرقت تجهیزات: این شبیه‌سازی ارتباط نزدیکی با حمله فیزیکی دارد، زیرا تجهیزات سازمان را هدف قرار می‌دهد. این حمله می‌تواند به دنبال سرقت لپ‌تاپ مدیر عامل یا نسخه‌های پشتیبان سازمان باشد. مهم نیست چه دستگاهی هدف قرار می‌گیرد، زیرا هدف نهایی استخراج اطلاعات مهم، نام‌های کاربری و گذرواژه‌ها است. هر هکر اخلاقی هنگام انجام آزمایش‌هایی که به آن‌ها اشاره شد، ملزم است تا از قوانین زیر پیروی کند. اگر اینگونه نباشد، اتفاقات بدی برای او رخ می‌دهد که شامل از دست دادن شغل، مجازات قانونی یا حتا زندان خواهد بود.

هرگز از حد مجاز خود تجاوز نکنید: هر قراردادی مستلزم پیروی از قوانین حاکمیتی سازمان و نهادهای قانونی است. این سند نه تنها شرح وظایف شما در ارتباط با نفوذ را مشخص می‌کند، بلکه حیطه کاری شما در ارتباط با دسترسی به سامانه‌ها را مشخص می‌کند. اگر مسئولیت شما تنها ارزیابی وضعیت سامانه‌های هویتی است، دانلود گذرواژه‌ها و شروع به شکستن گذرواژه‌ها ممکن است فراتر از آن کاری باشد که سازمان از شما انتظار داشته است.

با تنظیم دامنه خسارت‌های وارد شده از خود محافظت کنید. اگر حمله به یک سیستم باعث آسیب‌دیدگی می‌شود باید در مورد بیمه تجهیزات با شرکت صحبت کنید. همچنین در قرارداد خود باید بندی در ارتباط با خطاهای انسانی و ابزارها قید کنید و به روشنی نام افرادی که در تیم تست نفوذ قرار دارند را برای سازمان مشخص کنید تا مشکل حقوقی پیش نیاید.

اخلاق‌مدار باشید. تفاوت بزرگ بین یک هکر مخرب و یک هکر اخلاقی واژه اخلاق است. اخلاق مجموعه‌ای از اصول اخلاقی درباره آنچه صحیح است یا صحیح نیست را شرح می‌دهد. موازین اخلاقی بعضی اوقات با معیارهای قانونی متفاوت هستند، زیرا قوانین آنچه را که مجبور هستیم انجام دهیم یا مجبور به انجام آن نیستیم را تعریف می‌کنند، در حالی که اخلاق آنچه را که بهتر است انجام دهیم یا انجام ندادن آن‌ها بهتر است را تعریف می‌کند.

حفظ محرمانگی اطلاعات: در طول ارزیابی‌های امنیتی اطلاعات محرمانه مختلفی را مشاهده می‌کنید. شما وظیفه قانونی و اخلاقی دارید که با این اطلاعات همانند اطلاعات شخصی خود رفتار کنید و اجازه ندهید افراد دیگر به آن‌ها دسترسی داشته باشند. به عبارت دقیق‌تر، نباید این اطلاعات را با اشخاص ثالث به‌اشتراک بگذارید و نباید از آنها برای اهداف غیرقابل تأیید استفاده کنید. وظیفه محافظت از اطلاعات ارسال شده بین آزمایش‌کننده و مشتری این باید در توافقنامه مشخص شود.

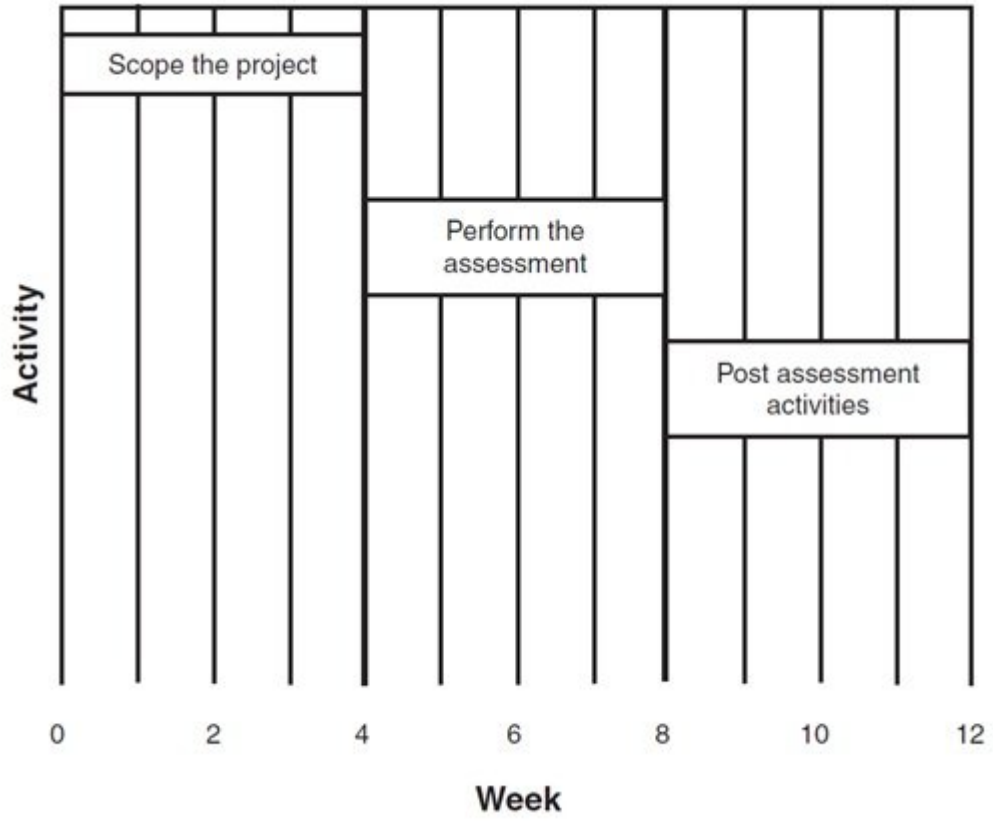
هیچ آسیبی وارد نکنید: این موضوع بسیار مهم است که به سیستم‌هایی که آزمایش می‌کنید آسیبی نرسانید. یک تفاوت عمده بین یک هکر مخرب و یک هکر اخلاقی این است که یک هکر اخلاقی هیچ خسارتی وارد نمی‌کند. ابزارهای امنیتی می‌توانند به حساب‌های کاربری مهم آسیب وارد کرده، باعث پیاده‌سازی حملات انکار سرویس و خرابی سرورها یا برنامه‌های مهم شوند. مراقب باشید از بروز چنین وقایعی جلوگیری کنید.

برنامه‌های آزمایشی — قانونی نگه داشتن فعالیت‌ها

بیشتر ما قبل از انجام یک سفر بزرگ برنامه‌ریزی می‌کنیم، در مورد آنچه تمایل به مشاهده آن داریم، چگونه می‌خواهیم وقت خود را بگذرانیم، قادر به انجام چه کارهایی هستیم و چقدر پول خرج کنیم برآوردی انجام می‌دهیم. هک اخلاقی نیز به یک چنین برنامه‌ریزی نیاز دارد. بسیاری از جزئیات قبل از انجام یک آزمایش واحد باید دست به دست شوند. اگر وظیفه شما مدیریت این پروژه است، باید به برخی از سؤالات اساسی پاسخ دهید. به‌طور مثال، دامنه ارزیابی چقدر گسترده است، اهداف ارزیابی چیست و آزمایش‌ها چگونه باید انجام شوند. در نهایت در گزارش نهایی باید فازهای مختلف انجام داده شده شرح داده شوند. تعیین دامنه ارزیابی یکی از مهم‌ترین اقداماتی است که باید انجام دهید. فراموش نکنید که باید دلایل انجام این آزمایش‌ها را به درستی درک کرده باشید تا ناخواسته یک فرآیند به ظاهر قانونی هک را انجام ندهید.

مراحل انجام هک اخلاقی

ارزیابی‌های امنیتی که یک هکر اخلاق‌مدار بر مبنای آن‌ها کار می‌کند از سه مرحله پیشبرد پروژه که اهداف و دستورالعمل‌هایی تدوین می‌شوند، انجام ارزیابی و آزمایش‌های نفوذ و سرانجام ارائه گزارشی در ارتباط با فعالیت‌ها تشکیل شده است. شکل زیر سه مرحله ارزیابی و زمان معمولی انجام ارزیابی‌ها را نشان می‌دهد.



ایجاد اهداف

تعیین اهداف اهمیت زیادی دارد. ممکن است آماده هک کردن سامانه‌ها باشید، اما آماده‌سازی یک برنامه خوب و تعیین اهداف مانع از آن می‌شود تا وقت خود را صرف آزمایش‌های غیر ضروری کنید. اهداف مشترک شامل بررسی وضعیت صدور گواهینامه‌ها و اعتبارنامه‌های سیستمی، تأیید انطباق خط‌مشی‌ها با مکانیزم‌های امنیتی و تایید این مسئله است که زیرساخت‌های فناوری‌اطلاعات به لحاظ فنی در برابر حملات عملکرد خوبی دارند. بررسی وضعیت صدور گواهینامه‌های ارزیابی فنی سیستم می‌تواند توسط تیم‌های امنیتی مستقل یا توسط کارمندان خود شرکت انجام شود. هدف کشف هرگونه آسیب‌پذیری یا ضعف در اجرای خط‌مشی‌ها و تخصیص مجوزها است. هدف از انجام آزمایش‌های فوق این است که اطمینان حاصل کنید همه چیز به درستی پیکربندی شده، مطابق با پیش‌بینی‌های انجام شده کار می‌کند، سامانه‌ها بدون مشکل با سامانه‌های صدور گواهی‌نامه کار می‌کنند و امکان تخصیص خارج از چارچوب گواهی‌نامه‌ها وجود ندارد.

اگر اهداف آزمون نفوذ تنها بررسی این موضوع است که خط‌مشی‌های فعلی دنبال می‌شوند یا خیر، روش‌های پیاده‌سازی این آزمون متفاوت است. در آزمون نفوذ تیم امنیتی به دنبال پیدا کردن رخنه‌هایی در مکانیزم‌های کنترلی است که برای محافظت از اطلاعات ذخیره‌شده، انتقال داده شده یا پردازش شده استفاده می‌شوند. این نوع آزمون امنیتی ممکن است ارتباط مستقیمی با هک نداشته باشد، اما از تکنیک‌های مهندسی اجتماعی و آزمون‌های کنترل فیزیکی بیشتری در آن استفاده می‌شود. در این حمله ممکن است حتا یکی از اعضا تیم نفوذ مامور شود تا جست‌وجویی در زباله‌های کاغذی شرکت داشته باشد تا اطلاعات مهمی به دست آورد. به این حمله شیرجه در سطل زباله (dumpster diving) می‌گویند. هدف یک حمله فنی ممکن است این باشد که ببینیم کارمندان سازمان یا هکرهای خارجی چگونه می‌توانند به خدمات و سامانه‌ها دسترسی داشته باشند، به دنبال جمع‌آوری چه نوع اطلاعاتی هستند و چگونه از اطلاعات به دست آمده برای حمله به یک وب‌سرور یا سیستم خارجی استفاده خواهند کرد. صرف نظر از این‌که سازمان از شما درخواست کرده چه نوع آزمایشی را انجام دهید، باید در زمان انجام یک آزمایش نفوذ به دنبال پاسخی برای پرسش‌های زیر باشید:

هدف سازمان از انجام آزمایش تست نفوذ چیست؟

چه نتایجی خاص مدنظر سازمان است

چه مقدار بودجه در نظر گرفته شده است

چه زمانی آزمایش‌ها باید انجام شود؟ در ساعات کاری، بعد از ساعت کاری یا آخر هفته؟

سازمان چه مدت زمانی را برای آزمایش‌های نفوذ و برطرف کردن آسیب‌پذیری‌ها در نظر گرفته است؟

آیا به کارمندان درباره این آزمایش‌ها اطلاعی داده شده است؟

آیا به مشتریان درباره انجام انجام آزمایش‌ها اطلاعی داده شده است؟

آزمون قرار است تا چه مدت انجام شود و تا چه سطحی پیش برود؟ باید به سرعت انجام شود یا هدف پیدا کردن رخنه یا دستیابی به گذرواژه مدیرعامل با هدف دریافت جایزه است؟

در سازمان با چه افرادی در ارتباط هستید؟

گزارش‌ها باید به چه کسی تحویل داده شود؟

مدیریت از انجام آزمون‌ها به دنبال چه نتیجه‌ای است؟

دریافت تأییده

گرفتن تأییده یکی از مهم‌ترین کارهایی است که در زمان انجام آزمایش باید انجام دهید. قبل از شروع هرگونه آزمایش باید اطمینان حاصل کنید برنامه‌ای دارید که به‌صورت کتبی تصویب شده است. اگر این کار انجام نشود، شما و تیم‌تان ممکن است با عواقب ناخوشایندی روبرو شوید که ممکن است شامل اخراج یا حتا مواجه شدن با اتهامات کیفری باشد.

نکته: هیچ‌گاه آزمایش‌ها را بدون تأیید کتبی انجام ندهید. اگر یک مشاور مستقل هستید، ممکن است قبل از شروع هر نوع آزمون حتما باید موافقت‌نامه کتبی از سازمان دریافت کنید. موافقت‌نامه باید به خط‌مشی‌های حاکمیتی سازمان، خطاها و مسائلی که ممکن است در فرآیند هک به وجود آیند اشاره داشته باشد. این توافق‌نامه‌ها می‌توانند در صورت بروز یک مشکل ناخواسته از شما محافظت کنند. برای اینکه مطمئن شوید توافق‌نامه به درستی به امضا طرفین رسیده و کارها بدون وجود مشکل خاصی انجام می‌شود، باید طرف مقابل شما یکی از کارمندان ارشد سازمان باشد. این شخص می‌تواند حامی پروژه و فردی باشد که با مدیران ارشد اجرایی در ارتباط است. حامیان پروژه می‌توانند به شما در کسب مجوزها برای شروع آزمایش و تأمین بودجه و الزامات اولیه برای به سرانجام رسیدن کار کمک کنند.

گزارش هک اخلاقی

قبل از آن‌که کار خود را آغاز کنید باید به فکر تهیه گزارش نهایی باشید. در طول این فرآیند، باید ارتباط نزدیکی با مدیریت داشته باشید تا آن‌ها به‌طور مستمر نتایج به دست آمده را ارزیابی کنند. هنگام ارائه گزارش نباید به دنبال غلو کردن باشید. ممکن است مشکلات جدی را پیدا کرده باشید، اما قبل از نوشتن و ارسال گزارش باید با مدیریت گفت‌وگو کنید. هدف این است که مدیریت را در جریان انجام امور قرار بگیرد و اطلاعی درباره وضعیت ارزیابی‌ها داشته باشد. اگر مواردی پیدا کردید که آسیب‌پذیری مهمی به شمار می‌روند، تمام آزمایشات را متوقف کنید و بلافاصله به مدیریت اطلاع دهید. اولویت شما همیشه باید ایمن‌سازی زیرساخت‌های سازمان باشد. در گزارشی که آماده می‌کنید باید به‌طور کامل به نتایج به دست آمده اشاره کرده باشید. آسیب‌پذیری‌ها باید مورد بحث قرار گرفته باشند و به خطرات احتمالی پیرامون آسیب‌پذیری‌ها اشاره شده باشد. درست است که هکرهای اخلاقی به دلیل نوشتن گزارش‌های ضعیف از کار خود اخراج نشده‌اند، اما اگر گزارش‌ها نتوانند به شکل شفاف و روشنی یافته‌های شما را به تصویر بکشند، نباید انتظار داشته باشید که یافته‌های فنی شما مورد تمجید قرار بگیرند. گزارش باید به شکل ساده و قابل خواندنی به نتایج ارزیابی اشاره کند تا حتا افراد غیر فنی قادر به درک آن باشند. یک گزارش جامع شامل بخش‌های زیر است:

مقدمه

شرح فعالیت‌های انجام شده

نتایج و جمع‌بندی

توصیه‌ها

با توجه به این‌که بیشتر سازمان‌ها بودجه لازم برای ایمن‌سازی را تخصیص نمی‌دهند، به همین دلیل توصیه‌هایی که ارائه می‌کنید ممکن است دید روشنی در اختیار سازمان‌ها قرار دهد.

در شماره آینده مبحث فوق را ادامه می‌دهیم.

برای مطالعه رایگان تمام بخش‌های **دوره CEH** روی لینک زیر کلیک کنید:

آموزش رایگان دوره CEH

تاریخ انتشار:

24 بهمن 1398

نشانی منبع:
https://www.shabakeh-mag.com/security/16572/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-ceh-%D9%87%DA%A9%D8%B1-%DA%A9%D9%84%D8%A7%D9%87-

%D8%B3%D9%81%DB%8C%D8%AF-%D9%85%D8%B1%D8%A7%D8%AD%D9%84-
%D8%A7%D9%86%D8%AC%D8%A7%D9%85-%D9%87%DA%A9-
%D8%A7%D8%AE%D9%84%D8%A7%D9%82%DB%8C-
%DA%86%DB%8C%D8%B3%D8%AA%D8%9F