آموزش CEH (هکر کلاه سفید): آشنایی با فرمول‌های ارزیابی خسارات وارد شده بر اثر یک حمله هکری

ارزیابی ریسک فرایند شناسایی خطرات احتمالی سایبری و ارزیابی سلسله اتفاقاتی است که در بروز یک حمله یا یک رویداد ناخواسته رخ می‌دهند. دو روش کیفی و کمی برای ارزیابی ریسک وجود دارد. روش‌های ارزیابی کیفی ریسک از سناریوهای خاصی برای آماده‌سازی فهرستی از اولویت‌های مهم استفاده می‌کنند و مباحث مالی را در نظر نمی‌گیرد. نتایج به دست آمده به صورت بحرانی، زیاد، متوسط یا کم طبقه‌بندی می‌شوند. ارزیابی کمی روی ارزش مادی دارایی‌ها متمرکز است.

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

فرآیند مدیریت حوادث

فرآیندهای مربوط به مدیریت و پاسخ‌دهی به حوادث شامل موارد زیر هستند:

1. آماده شدن برای پاسخ به حادثه
2. شناسایی و تحلیل واکنش مناسب به حادثه
3. طبقه‌بندی یک حادثه و اولویت‌بندی آن

4- اطلاع‌رسانی و آگاهی دادن

5- بازدارندگی

6. انجام بررسی‌های دقیق و کشف شواهد قانونی در ارتباط با حادثه
7. بررسی علت بروز مشکل و بازیابی

8- اقدامات متقضا پس از شناسایی حادثه

مسئولیت تیم واکنش به حوادث

تیم پاسخگویی به حوادث متشکل از اعضایی است که در مواجه شدن با حوادث دانش و تجربه لازم را دارند. تیم

پاسخگویی متشکل از متخصصان آموزش دیده‌ای است که در جمع‌آوری اطلاعات متخصص هستند و کلیه مدارک مربوط به حمله به سامانه‌ها را طبقه‌بندی می‌کنند. در حالت کلی این تیم متشکل از کارمندان فناوری‌اطلاعات، منابع انسانی، کارمندان روابط عمومی، مجریان قانونی و مدیر بخش امنیت است. مسئولیت اصلی این تیم اقدام مقتضا بنابر خط‌مشی‌های تعریف شده در برنامه واکنش به حوادث (IRP) سرنام Incident Response Plan است. اگر برنامه واکنش به حوادث تعریف نشده باشد، تیم مجبور است بر مبنای الگوی آزمون پیشرو کارهای مربوطه را انجام دهد. بررسی و ارزیابی رویدادها، تعیین خسارت یا شناسایی محدوده حمله، مستندسازی رویدادها و فرآیندها، در صورت لزوم کمک گرفتن از کارشناسان امنیتی برون سازمانی، جمع‌آوری حقایق و گزارش‌نویسی از جمله این اقدامات هستند.

ارزیابی ریسک

ارزیابی ریسک فرایند شناسایی خطرات احتمالی سایبری و ارزیابی سلسله اتفاقاتی است که در بروز یک حمله یا یک رویداد ناخواسته رخ می‌دهند. دو روش کیفی و کمی برای ارزیابی ریسک وجود دارد. روش‌های ارزیابی کیفی ریسک از سناریوهای خاصی برای آماده‌سازی فهرستی از اولویت‌های مهم استفاده می‌کنند و مباحث مالی را در نظر نمی‌گیرد. نتایج به دست آمده به صورت بحرانی، زیاد، متوسط یا کم طبقه‌بندی می‌شوند. ارزیابی کمی روی ارزش مادی دارایی‌ها متمرکز است. در ادامه بر مبنای فرمولی زیان‌های مالی سازمان در اثر یک حمله را محاسبه کند. مراحل ارزیابی ریسک به شرح زیر است:

مرحله 1. پیش‌بینی ضرر واحد (SLE): این مرحله شامل تعیین مقدار ضرر واحدی است که در اثر بروز یک حمله متوجه دارایی‌ها می‌شود. این پیش‌بینی می‌تواند برآورد دقیقی از تهدیدی باشد که ممکن است واقعی باشد یا ممکن است مقدار ضرری باشد که انتظار دارید در صورت بروز یک حمله متوجه یک دارایی شود. SLE بر مبنای فرمول ارزش دارایی ضرب در احتمال در معرض خطر قرار گرفتن محاسبه می‌شود.

SLE = asset value × exposure factor

فاکتور احتمال در معرض تهدید قرار گرفتن (EF) سرنام exposure factor اشاره به ضرر بالقوه‌ای دارد که متوجه یک دارایی خاص است.

مرحله 2. ارزیابی نرخ وقوع سالانه (ARO): بیان‌گر این موضوع است که ضرر هر چند وقت یکبار اتفاق می‌افتد و همچنین بیان‌گر احتمال وقوع ضرر است.

مرحله 3. پیش‌بینی ضرر سالانه (ALE): بیان‌گر ارزش یک ضرر واحد از منبع است. این مقدار ممکن است تمامی یا بخشی از منبع را شامل شده و همچنین تاثیر ضرر را نشان می‌دهد. پیش‌بینی ضرر سالانه بر مبنای فرمول زیر محاسبه می‌شود.

ALE = SLE × ARO

آزمون CEH ممکن است از شما بخواهد که از فرمول‌های ریسک SLE و ALE استفاده کنید. به‌طور مثال، ممکن است سؤالی با این مضموم مطرح شود، "اگر داده‌ای به ارزش 500 دلار داشته باشید که به دلیل عدم پیاده‌سازی اقدامات متقابل مانند نصب ضدویروس به میزان 50٪ در معرض تهدید قرار گرفته چگونه از فرمول SLE برای محاسبه پیش‌بینی ضرر واحد استفاده می‌کنید؟ فرمول انجام این‌کار به شرح زیر است:

SLE × EF = SLE, or $500 × .50 = $250

همچنین، ممکن است سوال دیگری در ارتباط با آزمون پیگیری مطرح شود که "اگر می‌دانستید که این نوع رویداد به‌طور معمول چهار بار در سال اتفاق می‌افتد، آیا می‌توانستید از فرمول ALE برای محاسبه ضرر سالانه استفاده کنید؟ پاسخ مثبت است. در این‌جا ارزیابی نرخ وقوع سالیانه (ARO) برابر با 4 است. بنابراین فرمولی به صورت زیر داریم:

ALE = SLE × ARO or $250 × 4 = $1,000

فرمول فوق نشان می‌دهد که به‌طور متوسط در سال 1000 دلار از دست می‌دهیم.

از آنجایی که یک سازمان نمی‌تواند از تمام دارایی‌های خود به شکل کاملی محافظت کند، باید سیستمی برای رتبه‌بندی ریسک و آسیب‌پذیری ایجاد شود. سازمان‌ها باید به دنبال شناسایی رویدادهای پرخطر با تاثیرگذاری بالا روی مکانیسم‌های محافظتی باشند. بخشی از کار هکرهای اخلاقی شناسایی آسیب‌پذیری‌های احتمالی پیرامون دارایی‌های مهم، تاثیر بالقوه این آسیب‌پذیری‌ها و آزمایش سامانه‌ها برای شناسایی اکسپلیوت‌هایی است که ممکن است مقررات را نقض کرده یا توسط هکرها مورد سوء استفاده قرار گیرد.

نکته: درست است که آشنایی با مراحل هک کردن است، اما آگاهی در مورد فرمول‌های مورد استفاده برای ارزیابی ریسک، حائز اهمیت است. به همین دلیل باید فرمول‌های SLE = AV × EF و ALE = SLE × ARO را به خاطر بسپارید.

آزمون امنیتی

کار اصلی یک هکر اخلاقی آزمایش سامانه‌ها با هدف شناسایی آسیب‌پذیری‌ها است. این آزمایش‌ها ممکن است به‌گونه‌ای تنظیم شود که هکرهای اخلاقی هیچ دانش کاملی در ارتباط با هدف ارزیابی (TOE) نداشته باشند و به درخواست یک سازمان چنین آزمون‌هایی را انجام دهند.

نکته: اصطلاح هدف از انجام ارزیابي براي شناسايي يك محصول یا سیستم فناوری‌اطلاعات یکی از موضوعات مهم دنیای فناوری‌اطلاعات است. شورای EC و برخی دستورالعمل‌ها و استانداردهای امنیتی از این اصطلاح برای توصیف سیستم‌هایی استفاده می‌شود که تحت آزمون‌های مبتنی بر CIA قرار گرفته‌اند. هدف از آزمون امنیتی (صرف نظر از نوع) این است که هکر اخلاقی کنترل‌های امنیتی را به درستی ارزیابی کند و برآوردی از آسیب‌پذیری‌های احتمالی پیرامون سامانه‌ها داشته باشد.

آزمون‌های با حداقل دانش موجود (جعبه سیاه)

آزمون‌های جعبه سیاه عمدتا به آزمون‌ها بدون دانش معروف هستند. به بیان ساده، تیم امنیتی هیچ اطلاعی از شبکه هدف یا سیستم‌های مرتبط ندارد. آزمون جعبه سیاه یک حمله بیرونی را شبیه‌سازی می‌کند، زیرا کارشناسان امنیتی برون‌سازمانی در بیشتر موارد اطلاعی در مورد شبکه یا سیستم‌های مورد نظر ندارند. مهاجم باید انواع مختلفی از اطلاعات مرتبط با هدف را جمع‌آوری کند تا نقاط قوت و ضعف کار خود را بداند. مزایای آزمایش جعبه سیاه شامل موارد زیر است:

این آزمایش کاملا بی طرفانه است، زیرا طراح و آزمایش‌کننده مستقل از یکدیگر هستند.

آزمایش کننده آگاهی قبلی از شبکه یا هدف مورد بررسی ندارد. بنابراین هیچگونه پیش تصوری در مورد عملکرد شبکه ندارد.

معمولاً طیف گسترده‌ای از کارهای شناسایی و اکتشاف به شکل مکتوب انجام می‌شود که که می‌تواند به شناسایی نشت اطلاعات سامانه‌ها کمک کند.

آزمون به همان روشی که یک مهاجم خارجی به یک شبکه حمله می‌کند انجام می‌شود.

البته آزمایش جعبه سیاه خالی از معایب نیست. از مهم‌ترین معایب پیرامون یک آزمون جعبه سیاه به موارد زیر می‌توان اشاره کرد:

آزمون‌های امنیتی جعبه سیاه می‌توانند به نسبت زمانی که یک هکر به جزییات کاملی دسترسی دارد زمان‌بر باشند.

آزمون‌ها هزینه‌بر تر هستند، زیرا اجرای آن‌ها به زمان بیشتری نیاز دارد.

آزمون فوق تنها روی مواردی متمرکز است که هکرهای خارجی مشاهده می‌کنند، در حالی که در واقعیت بسیاری از حملات توسط کارمندان درون شرکتی انجام می‌شود.

آزمون‌های مبتنی بر دانش کامل (White Box)

آزمون جعبه سفید عملکردی بر عکس آزمون جعبه سیاه دارد. در آزمون جعبه سفید فرض بر این است که آزمایش‌کننده امنیت شبکه، درباره سیستم‌ها و زیرساخت‌ها اطلاعات کاملی دارد. این اطلاعات به آزمایش‌کننده امنیتی اجازه می‌دهد تا یک رویکرد ساختارمند دنبال کند و نه تنها اطلاعات ارائه شده را بررسی کند بلکه صحت اطلاعات را نیز بررسی کند. در حالی که آزمون جعبه سیاه معمولاً زمان بیشتری را برای جمع‌آوری اطلاعات می‌طلبد، اما آزمون جعبه سفید آن زمان را صرف بررسی آسیب‌پذیری‌ها می‌کند.

آزمون مبتنی بر دانش جزئی (Gray Box)

در دنیای آزمایش نرم‌افزارهای کاربردی، آزمایش جعبه خاکستری به عنوان یک آزمون مبتنی بر دانش جزئی انجام می‌شود. شورای EC آزمون جعبه خاکستری را نوعی آزمایش داخلی توصیف می‌کند. بنابراین، هدف این است که مشخص کنیم کارمندان یک سازمان به چه مواردی دسترسی دارند. این شکل از آزمون ممکن است برای سازمان‌ها مفید باشد، زیرا حمله‌های زیادی توسط خودی‌ها انجام می‌شود.

انواع آزمون‌های امنیتی

انواع مختلفی از آزمون‌های امنیتی در زیر گروه سه آزمون یاد شده انجام می‌شود. این آزمون‌ها ممکن است محدوده گسترده‌ای از ارزیابی‌های مرتبط با خط‌مشی‌ها تا کوشش به هک کردن از طریق اینترنت را شامل شوند. این آزمون‌های امنیتی به نام‌های زیر شناخته می‌شوند:

آزمون‌های آسیب‌پذیری

ارزیابی شبکه

آزمون‌های تیم قرمز

آزمون تست نفوذ

ارزیابی آسیب‌پذیری میزبان

ارزیابی آسیب‌پذیری

هک اخلاقی

مهم نیست چه آزمایش امنیتی انجام شود، برای بررسی منظم شبکه، خط‌مشی‌ها و کنترل‌های امنیتی یک سازمان لازم است آزمون‌های یاد شده انجام شوند. هدف از انجام این آزمون‌ها تعیین شایستگی سنجه‌های امنیتی، شناسایی نواقص امنیتی، ارائه داده‌هایی که از آن‌ها می‌توان برای پیش‌بینی اثربخشی اقدامات امنیتی احتمالی و تأیید شایستگی چنین اقداماتی پس از اجرا استفاده کرد. آزمون‌های امنیتی فوق را می‌توان به صورت یکی از سه حالت زیر تعریف کرد:

نکته: اگرچه آزمون **CEH** روی یک نوع آزمون امنیتی متمرکز است، با این حال باید از انواع مختلف این آزمون‌ها اطلاع داشته باشید تا بتوانید به‌طور کامل چالش‌های پیش‌رو را برطرف کنید.

ارزیابی/ ممیزی سطح بالا: آزمون فوق به‌نام ارزیابی سطح ا نیز معروف است. آزمون فوق به خط‌مشی‌های سازمانی، روال‌ها و دستورالعمل‌های سازمانی یک نگاه از بالا به پایین دارد. این نوع ارزیابی آسیب‌پذیری یا ممیزی شامل هیچ آزمون دستی نیست. هدف از ارزیابی بالا به پایین دستیابی به پاسخی برای پرسش‌های زیر است:

آیا خط‌مشی‌ها، روال‌ها و دستورالعمل‌های قابل اجرا وجود دارد؟

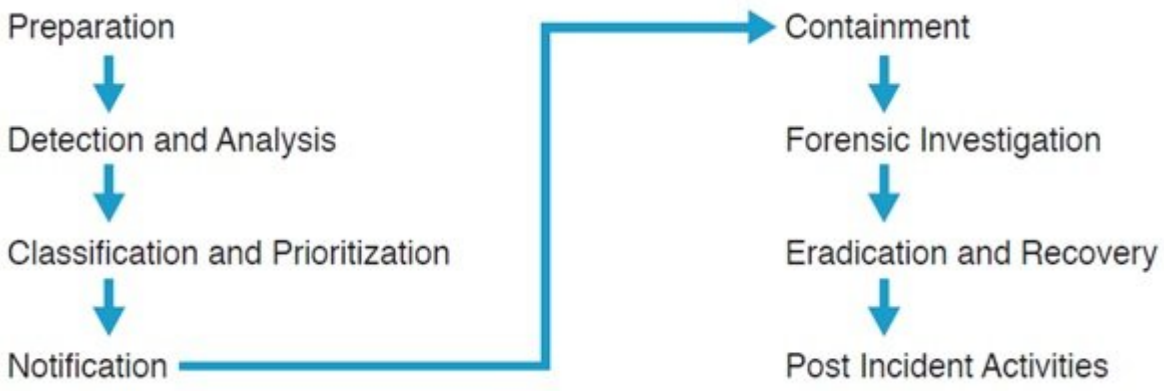
آیا خط‌مشی‌ها، روال‌ها و دستورالعمل‌ها دنبال می‌شوند؟

آیا محتوای آن‌ها برای محافظت در برابر خطرات احتمالی کافی است؟

ارزیابی شبکه: آزمون‌های فوق به‌نام ارزیابی سطح II نیز معروف است و تمامی عناصر مشخص شده در ارزیابی سطح I و فعالیت‌های کاربردی را شامل می‌شود. این فعالیت‌ها شامل جمع‌آوری اطلاعات، اسکن، ارزیابی آسیب‌پذیری‌ها و سایر فعالیت‌های مفید مرتبط با امنیت است.

آزمون نفوذ: برخلاف ارزیابی‌ها و شناسایی‌ها، آزمون‌های نفوذ عملکردی متضاد با موارد یاد شده دارند. آزمایشات نفوذ به عنوان ارزیابی سطح III نیز شناخته می‌شوند. این آزمون‌ها حالت تهاجمی دارند و نشان می‌دهد یک هکر خارجی می‌تواند به چه محتوایی دسترسی پیدا کرده و آن‌را کنترل کند. آزمون‌های نفوذ متمرکز روی خط‌مشی‌ها و روال‌ها نیست و بیشتر به دنبال پیدا کردن اطلاعاتی است که هکرها روی دست یافتن آن‌ها در شبکه متمرکز شده‌اند.

به یاد داشته باشید در صورت عدم وجود خط‌مشی‌ها و روال‌هایی برای کنترل امنیت، آزمون‌های نفوذ اثرگذاری چندان خاصی نخواهند داشت. بدون خط‌مشی‌ها و روال‌های کافی، پیاده‌سازی یک الگوی امنیتی تقریبا غیرممکن است، به همین دلیل کنترل‌های مستندسازی شده ضروری هستند. اگر هیچ خط‌مشی یا روالی وجود ندارد، لازم است الگوهای فعلی را ارزیابی کنید. خط‌مشی‌های امنیتی پایه و اساس یک زیرساخت امنیتی کارآمد هستند. سازمان‌ها می‌توانند انواع مختلفی از خط‌مشی‌ها همچون کنترل دسترسی، گذرواژه، حساب کاربری، ایمیل و پاسخ‌گویی به حوادث را به کار گیرند. به‌طور مثال، یک طرح پاسخ‌گویی به حوادث شامل اقداماتی است که ضمن پاسخ‌گویی به حوادث رویکرد بازیابی پس از حوادث را نیز شامل شود. رویکردهای مختلفی برای پاسخ‌گویی به حوادث وجود دارد. رویکرد شورای EC در زمنیه پاسخ‌گویی به حوادث در شکل زیر نشان داده شده است.



ممکن است شما وظیفه ایجاد خط‌مشی‌های امنیتی را بر اساس فعالیت‌های موجود و بهترین روش‌های شناخته شده بر عهده بگیرید. منابع خوب و رایگان برای آشنایی با خط‌مشی‌های SANS وجود دارد. پیشنهاد می‌کنم به **این آدرس** مراجعه کنید.

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:

21 بهمن 1398

نشانی منبع:
https://www.shabakeh-mag.com/security/16559/%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-%D8%A2%D8%B4%D9%86%D8%A7%DB%8C%DB%8C-%D8%A8%D8%A7-%D9%81%D8%B1%D9%85%D9%88%D9%84%E2%80%8C%D9%87%D8%A7%DB%8C-%D8%A7%D8%B1%D8%B2%DB%8C%D8%A7%D8%A8%DB%8C-%D8%AE%D8%B3%D8%A7%D8%B1%D8%A7%D8%AA-%D9%88%D8%A7%D8%B1%D8%AF-%D8%B4%D8%AF%D9%87-%D8%A8%D8%B1-%D8%A7%D8%AB%D8%B1-%DB%8C%DA%A9-%D8%AD%D9%85%D9%84%D9%87