آموزش CEH (هکر کلاه سفید): آشنایی با مباحث اولیه امنیت اطلاعات

روش‌ها و فرآیندهای مختلفی برای محافظت از اطلاعات و سیستم‌های اطلاعاتی به منظور پیشگیری از دسترسی غیر مجاز به اطلاعات، افشای اطلاعات و ویرایش غیر مجاز اطلاعات وجود دارد. هرم سه‌گانه محرمانگی، یکپارچگی و دسترس پذیری تضمین می‌کند که اطلاعات ثبت شده درون بانک‌های اطلاعاتی از هرگونه دسترسی غیرمجاز در امان هستند. یک سازمان بدون خط‌مشی‌ها و قواعد امنیتی مناسب در برابر انواع مختلفی از تهدیدات آسیب‌پذیر است. به‌طوری‌که اطلاعات و داده‌های محرمانه مربوط به یک سازمان در فقدان نبود یک خط‌مشی جامع امنیتی هر لحظه در معرض تهدیدات سایبری قرار دارد. سازمان‌ها برای پیشگیری از بروز چنین مشکلاتی مجبور هستند به سراغ کارشناسان امنیتی بروند.

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

پیش‌درآمدی بر گواهی‌نامه‌های EC-Council

شورای بین‌المللی مشاوران تجارت الکترونیک (EC-Council) یک سازمان تخصصی متشکل از افرادی است که در زمینه‌های مختلف تجارت الکترونیک و امنیت اطلاعات متبحر هستند. این سازمان مالک و خالق گ**واهینامه معتبر هک اخلاقی (CEH)**، دوره رهگیری هک و کشف جرایم کامپیوتری و مبارزه با آنها (CHFI)، دوره تحلیلگر امنیتی (ECSA) / دوره تست نفوذ (LPT) و گواهی‌نامه‌های مختلفی است. در مجموع دوره‌های ارائه شده توسط این شورا در بیش از 87 کشور جهان آموزش داده می‌شود. ماتریس زیر دوره‌ها و مهارت‌هایی که EC-Council یاد می‌دهد را نشان می‌دهد.

اطلاعات مختصر درباره آزمون CEH

یک هکر اخلاقی متخصصی است که می‌داند چگونه به دنبال نقاط ضعف‌ها و آسیب‌پذیری‌های مستتر در سامانه‌ها باشد و از دانش و ابزارهایی که دارد برای انجام کارهای قانونی و ارزیابی وضعیت امنیتی سامانه‌ها استفاده می‌کند. مفاد آزمون **CEH** به شرح زیر است:

Background 04%

Analysis/Assessments 13%

Security 25%

Tools/Systems/Programs 32%

Procedures/Methodology 20%

Regulation/Policy 04%

Ethics 02%

مقدمه‌ای بر هک اخلاقی

سازمان‌هایی که خط‌مشی‌ها و روال‌های امنیتی را به درستی تعریف کرده باشند قادر هستند به بهترین شکل از داده‌های خود محافظت می‌کنند و مانع از آن می‌شوند تا افراد فاقد صلاحیت بدون مجوز لازم به داده‌ها دسترسی پیدا کرده یا آن‌ها را ویرایش کنند. در دنیای مدرن که جدیدترین فناوری‌ها و زیرساخت‌ها در دسترس قرار دارند و میلیون‌ها کاربر در هر دقیقه با این زیرساخت‌ها در ارتباط هستند، پیاده‌سازی یک خط‌مشی امنیتی کارآمد اجتناب‌ناپذیر است. در هر لحظه ممکن است هکرها از آسیب‌پذیری‌های شناسایی نشده‌ای برای نفوذ به یک سامانه اطلاعاتی استفاده کنند. به همین دلیل لازم است سازمان‌ها از کارشناسان امنیتی برای شناسایی رخنه‌ها استفاده کنند. در دنیای امنیت همانند سایر حوزه‌های فناوری‌اطلاعات تخصص‌های مختلفی وجود دارد که یک دارنده **مدرک CEH** که به آن هکر کلاه سفید می‌گوییم قادر است در شناسایی این رخنه‌ها به سازمان‌ها کمک فراوانی کند. اینترنتی که روزانه از آن استفاده می‌کنیم، رایج‌ترین و مرسوم‌ترین زیرساختی است که به هکرها اجازه می‌دهد انواع مختلفی از کدهای مخرب، اسکریپت‌ها، ویروس‌ها، هرزنامه‌ها و بدافزارها منتشر کنند و در کمتر از یک دقیقه صدها هزار سامانه کامپیوتری را آلوده کنند. به همین دلیل خطرات امنیتی پیرامون یک شبکه یا یک سیستم هیچ‌گاه از میان نخواهند رفت. مدیران و کارشناسان امنیتی همیشه با یک چالش بزرگ در زمینه پیاده‌سازی یک خط‌مشی امنیتی روبرو هستند. یک خط‌مشی کارآمد باید به شکل موثر و سودمندی از سازمان محافظت کند، منابع سازمانی را بیهوده هدر ندهد و خود زمینه‌ساز بروز یک شکاف امنیتی نشوند.

یک مثال واقعی در ارتباط با رخنه‌های داده‌ای شرکت eBay

یک نمونه واقعی که نشان می‌دهد امنیت اطلاعات و شبکه برای هر سازمانی حائز اهمیت است شرکت eBay است. eBay به عنوان یک خرده‌فروشی بزرگ در جهان شناخته می‌شود که به شکل گسترده‌ای از سوی کاربران در سراسر جهان استفاده می‌شود. این زیرساخت حراجی آنلاین در سال 2014 میلادی اعلام کرد یک رخنه داده‌ای باعث شد اطلاعات نزدیک به 145 میلیون مشتری این شرکت در دسترس هکرها قرار گیرد. به گفته ای‌بای، این نقض داده‌ای باعث به خطر افتادن اطلاعات زیر شد:

- نام مشتریان
- گذرواژه‌های ذخیره شده
- آدرس ایمیل
- کدپستی
- شماره‌های تماس
- تارخ تولد

این اطلاعات حساس باید توسط یک روال رمزنگاری شده ذخیره‌سازی می‌شدند، اما اطلاعات به جای آن‌که به شکل رمزگذاری شده ذخیره شوند در قالب یک متن خام ذخیره‌سازی شده بودند. ای‌بای می‌گوید هیچ یک از اطلاعات حساس امنیتی همچون اطلاعات کارت‌های اعتباری و بانکی مورد سوء استفاده قرار نگرفته‌اند، هر چند گذرواژه و شناسه‌های هویتی به سرقت رفته احتمال به وجود آوردن مخاطرات امنیتی را افزایش دادند. بانک‌اطلاعاتی ای‌بای شامل اطلاعات تراکنش‌های مالی کارت‌های اعتباری و سایر اطلاعات مالی مرتبط است که ای‌بای ادعا می‌کند اطلاعات فوق به شکل رمزگذاری شده درون یک بانک‌اطلاعاتی دیگری قرار داشتند. تحلیل‌های انجام شده نشان می‌دهند ای‌بای به واسطه یک حمله هکری ساده در خلال ماه‌های فوریه تا مارس سال 2014 قربانی شد. در این ماه‌ها تعدادی از کارمندان ای‌بای که سطح دسترسی بالایی به اطلاعات داشتند قربانی یک حمله فیشینگ شدند. این کارمندان ممکن است با هدف دسترسی به شبکه ای‌بای هدف این حمله قرار گرفته باشند یا شبکه ای‌بای به‌طور کامل زیر نظر قرار داشته و پس از نفوذ قربانی حمله سایبری شده است. ای‌بای اعلام کرد ظرف مدت دو هفته

این حمله سایبری را کشف کرد.

هک گوگل‌پلی

یک هکر اهل کشور ترکیه به‌نام ابرای بالیک موفق شد دو بار گوگل پلی را هک کند. او مسئولیت حمله به گوگل‌پلی را قبول کرد، اما این تنها تلاش موفق او نبود. او همچنین مدعی حمله به سایت طراحان اپل شد. او موفق شده بود رخنه‌هایی در کنسول توسعه‌دهندگان گوگل در سیستم‌عامل اندروید پیدا کند. او پس از آن‌که موفق به شناسایی آسیب‌پذیری‌ها شد، یک برنامه اندرویدی را برای بهره‌برداری از این آسیب‌پذیری طراحی کرد. زمانی‌که کنسول توسعه‌دهندگان دچار مشکل شد، کاربران نمی‌توانستند برنامه‌ها را دانلود کنند و توسعه‌دهندگان نیز قادر به بارگذاری برنامه‌های کاربردی خود نبودند.

نقض داده‌ای Home Depot

سرقت اطلاعات پرداختی همچون کارت‌های اعتباری این روزها متداول است. در سال 2014 میلادی سیستم فروش Home Depot در معرض یک حمله هکری قرار گرفت. این شرکت در تاریخ 9 می سال 2014 میلادی اعلام کرد، سیستم‌های آن‌ها دچار یک نقض داده‌ای شده است. در این حمله، هکرها موفق شده بودند گواهی‌نامه ورود به سیستم متعلق به فروشندگان ثالث را برای دستیابی به Pos به دست آورند. در این حمله آسیب‌پذیری روز صفر سیستم‌عامل ویندوز مورد سوء استفاده قرار گرفت و حفره‌ای در شبکه سازمانی Home Depot ایجاد شد که مسیری به شبکه این شرکت از طریق فروشندگان ثالث را به وجود آورد. پس از آن‌که هکرها موفق شدند به شبکه سازمانی نفوذ کنند بدافزار Memory scraping Network را در شبکه منتشر کردند تا به پایانه فروش نفوذ کنند. Memory Scaping Network به اندازه‌ای قدرتمند طراحی شده بود که موفق شد اطلاعات میلیون‌ها کارت اعتباری را به دست آورد. Home Depot برای پیشگیری از وقوع حملات مشابه کارهای زیادی انجام داد و تصمیم گرفت از کارت‌های پرداختی EMV chip-&-pin استفاده کند. این کارت‌های پرداختی Chip-&-pin به یک تراشه امنیتی توکار و نوار مغناطیسی دوگانه برای اطمینان از امنیت بالا تجهیز شده‌اند.

اصطلاحات پایه‌ای

Hack Value

اصطلاح ارزش هک (Hack Value) به مفهومی اشاره دارد که توصیف‌کننده جذابیت، علاقه یا موجودیتی ارزشمند است که ارزش سطح جذابیت اهداف را توصیف می‌کند.

حمله روز صفر

حملات روز صفر اشاره به تهدیدات و آسیب‌پذیری‌هایی دارند که می‌توانند برای رخنه به سامانه‌ها و آسیب وارد کردن به زیرساخت‌ها مورد استفاده قرار گیرند، قبل از آن‌که توسعه‌دهنده بتواند آن‌ها را شناسایی کند و وصله‌های مربوطه را برای آن‌ها منتشر کند.

آسیب‌پذیری

آسیب‌پذیری به یک نقطه، حفره یا عاملی که باعث می‌شود یک مهاجم بتواند برای ورود به سیستم یا شبکه از آن‌ها استفاده کند اشاره دارد. هرگونه آسیب‌پذیری می‌تواند یک نقطه ورود برای رسیدن به هدف باشد که مدنظر هکر است.

Exploit

بهره‌برداری یک نقض امنیتی سیستمی است که توسط آسیب‌پذیری‌ها، حملات روز صفر یا هر نوع حمله هکری به وقوع می‌پیوندد.

Doxing

Doxing به انتشار اطلاعات یا مجموعه‌ای از اطلاعات مرتبط با یک شخص واحد اشاره دارد. این اطلاعات بیشتر از

طریق رسانه‌های اجتماعی یا سایر منابع مشابه جمع‌آوری می‌شوند.

Payload

بارداده به بخش‌هایی از داده‌ها یا اطلاعات واقعی که در قالب یک فریم قرار دارند و در نقطه مقابل ابرداده‌هایی هستند که به شکل خودکار تولید می‌شوند قرار دارند. در امنیت اطلاعات، بارداده یک بخش یا قسمتی از یک کد مخرب یا بهره‌برداری است که پتانسیل آسیب وارد کردن و انجام کارهایی همچون بهره‌برداری، باز کردن درب‌های پشتی و ربایش را دارند.

Bot

بات‌ها، نرم‌افزارهایی هستند که برای کنترل اهداف از راه دور و اجرای وظایف از پیش تعیین شده استفاده می‌شوند. بات‌ها می‌توانند کارهای از پیش تعریف شده و اسکریپت‌های خودکار را از طریق اینترنت دارند. بات‌ها به نام‌های دیگری همچونت بات اینترنت (Internet Bot) یا روبات وب (Web Robot) شناخته می‌شوند. این بات‌ها می‌توانند برای اهداف اجتماعی از قبیل chatterbots، اهداف تجاری، اهداف مخرب از قبیل Spambots، ویروس‌ها و کرم‌های گسترشی، شبکه زامبی و حملات منع سرویس انکار شده استفاده شوند.

اجزا تشکیل دهنده امنیت اطلاعات

محرمانگی

ما به دنبال آن هستیم تا اطمینان حاصل کنیم داده‌های مخفی و حساس ما ایمن است. محرمانگی به معنای آن است که تنها افراد مجاز می‌توانند منابع و زیرساخت‌های دیجیتالی را مشاهده کنند و با آن‌ها کار کنند. محرمانگی همچنین به این اصل اشاره دارد که افراد غیرمجاز نباید به داده‌ها دسترسی داشته باشند. به‌طور کلی دو نوع داده وجود دارد:

داده‌هایی که در حال استفاده استفاده هستند و در شبکه استفاده می‌شوند و داده‌هایی که در حال استفاده نیستند و روی رسانه‌های ذخیره‌ساز (سرورها، هارددیسک‌های محلی و فضای ابری) ذخیره‌سازی شده‌اند. در ارتباط با داده‌های درحال استفاده باید قبل از ارسال داده‌ها از طریق شبکه آن‌ها را رمزگذاری کنیم. گزینه دیگری که همراه با رمزنگاری اطلاعات در اختیار ما قرار دارد به‌کارگیری یک شبکه جداگانه در ارتباط با داده‌های حساس است. برای اطلاعاتی که استفاده نمی‌شوند باید از مکانیسم‌های رمزنگاری استفاده کنیم تا در صورت سرقت فیزیکی یا نفوذ هیچ فرد غیرمجازی موفق نشود محتویات آن‌ها را مشاهده کنید.

یکپارچگی

اصل یکپارچگی به معنای آن است که ما نمی‌خواهیم اطلاعات ما توسط افراد غیر مجاز دستکاری شود یا این افراد به اطلاعات دسترسی داشته باشند. یکپارچگی داده‌ها تضمین می‌کند که فقط افراد واجد شرایط قادر به ویرایش یا تغییر اطلاعات هستند.

دسترس‌پذیری

اصل فوق به معنی آن است که دسترسی به سامانه‌ها و داده‌ها در هر شرایطی امکان‌پذیر است. اگر اشخاص مجاز به دلیل خرابی کلی شبکه یا حمله انکار سرویس (DOS) نتوانند به داده‌ها دسترسی پیدا کنند به معنای آن است که اصل دسترس‌پذیری نقض شده است. این مشکل در برخی موارد از دست رفتن داده‌ها و درآمدها به همراه دارد. ما می‌توانیم از اصطلاح CIA برای یادآوری این مفاهیم اساسی که نقش کلیدی در دنیای امنیت بازی می‌کنند استفاده کنیم (جدول 1).

سه اصل دنیای امنیت	مخاطره	کنترل
محرمانگی	از دست رفتن حریم خصوصی، دسترسی غیر مجاز به اطلاعات . سرقت هویت یا شناسه کارمندان	رمزنگاری. احراز هویت. کنترل دسترسی
یکپارچگی	اطلاعات به مدت طولانی قابل اعتماد یا دقیق نیستند	سازنده/بررسی کننده. تضمین کیفیت. گزارش‌های حساب‌رسی
دسترس‌پذیری	از دست رفتن اعتماد مشتریان، از دست رفتن درآمدها، مغشوش شدن وضعیت کسب‌وکار	تداوم تجارت. برنامه‌ها و آزمون. ذخیره‌سازی نسخه پشتیبان. ظرفیت کافی.

جدول 1- مخاطرات و مکانیسم‌های امنیتی که CIA برای محافظت از اطلاعات پیشنهاد می‌کند.

احراز هویت (تایید اعتبار)

احراز هویت فرآیندی است که یک کاربر یا دستگاهی را برای تخصیص مجوزها، تعیین سطح دسترسی و اعمال برخی خط‌مشی‌ها و قواعد اعتبارسنجی کرده و هویت آن‌ها را تعیین می‌کند. احراز هویت با هدف شناسایی هویت واقعی افراد انجام می‌شود تا اطمینان حاصل شود کارمندان واقعی یک سازمان به شبکه ارتباطی و داده‌ها دسترسی دارند. در فرآیند احراز هویت از ترکیب گذرواژه و اطلاعات هویتی افراد برای تایید اصالت آن‌ها استفاده می‌شود.

عدم انکار (Non-Repudiation)

برای حصول اطمینان از انتقال و دریافت اطلاعات بین فرستنده و گیرنده می‌توان از تکنیک‌های مختلفی همچون امضاهای دیجیتال و رمزگذاری استفاده کرد. به عبارت دقیق‌تر، در انتقال اطلاعات یا انجام عملی روی اطلاعات، گیرنده، فرستنده یا فردی که تغییراتی روی اطلاعات انجام می‌دهد، نباید قادر به انکار عمل خود باشد. به‌طور مثال، فرستنده یا گیرنده نتواند ارسال یا دریافت پیامی را انکار کند. قراردادهای دیجیتالی، امضاها و پیام‌های ایمیل از رویکرد عدم انکار (Nonrepudiation) استفاده می‌کنند.

در شماره آینده مبحث فوق را ادامه خواهیم داد.

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

آموزش رایگان دوره CEH

تاریخ انتشار:

09 بهمن 1398

نشانی منبع:
https://www.shabakeh-mag.com/tricks/security-tricks/16524/%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%85%D8%A8%D8%A7%D8%AD%D8%AB-
%D8%A7%D9%88%D9%84%DB%8C%D9%87-%D8%A7%D9%85%D9%86%DB%8C%D8%AA-
%D8%A7%D8%B7%D9%84%D8%A7%D8%B9%D8%A7%D8%AA