آموزش CEH (هکر کلاه سفید): آشنایی با مثلث امنیت و معروف‌ترین بردارهای حمله

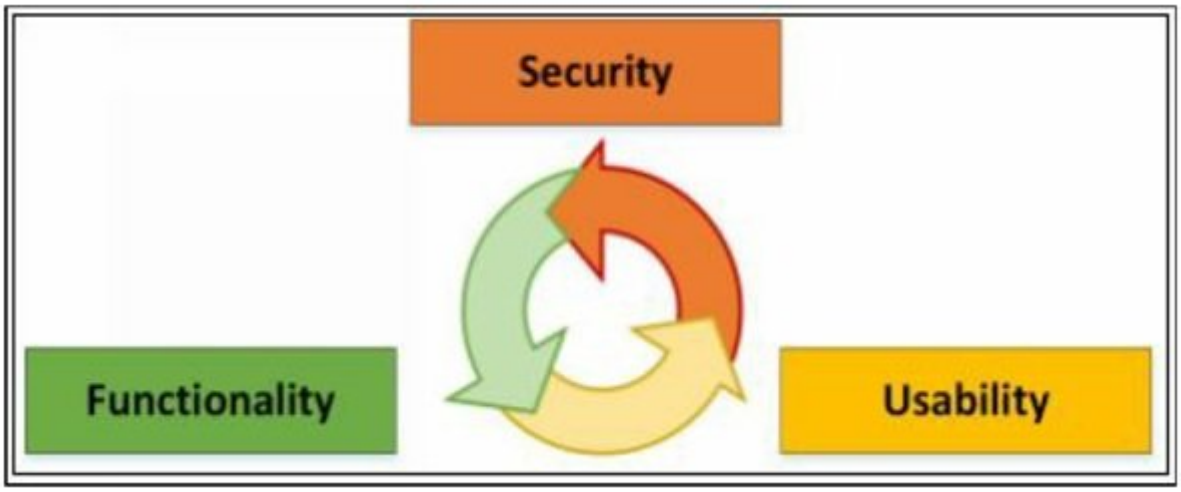
برخی از کاربران تصور می‌کنند، یک حمله هکری به صورت تصادفی یا از روی سرگرمی انجام می‌شود. در حالی که واقعیت این‌گونه نیست و هکرهای حرفه‌ای برای حمله به یک سامانه از مدت‌ها قبل برنامه‌ریزی می‌کنند. یک حمله هکری تنها زمانی با موفقیت به سرانجام می‌رسد که هکر اطلاعات کافی در مورد یک سامانه داشته باشد. رویکرد فوق درست در نقطه مقابل پیاده‌سازی یک استراتژی امنیتی قرار دارد. شاید تاکنون از این مسئله اطلاع نداشتید که پیاده‌سازی یک استراتژی امنیتی بر پایه محاسبات ریاضی انجام می‌شود. در یک محاسبه ریاضی اگر 98.5 درصد امنیت سیستم تامین شده باشد و تنها 1.5 درصد احتمال نفوذ به یک سامانه وجود داشته باشد، مکانیزم‌های امنیتی ضریب خطای زیادی دارند.

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

قبل از ادامه بحث لازم است به این موضوع اشاره کنم، جملاتی که با عبارت نکته مشخص می‌شوند، تجربیات شخصی نویسنده در ارتباط با مسائل امنیتی و پیاده‌سازی استراتژی‌های امنیتی است.

مثلث امنیت، کارایی و قابلیت استفاده

سطح توان‌مندی دفاعی یک سیستم با محاسبه سه فاکتور کارایی، قابلیت استفاده و امنیت اندازه‌گیری می‌شود. سه مؤلفه یاد شده به مثلث Security، Functionality and Usability معروف هستند. اجازه دهید برای روشن شدن بحث به ذکر مثالی بپردازیم. توپی درون این مثلث را تصور کنید، اگر توپ در وسط قرار داشته باشد به این بدان معنا است که هر سه مؤلفه عملکرد قدرتمندی دارند، حال اگر توپ به مولفه امنیت نزدیک‌تر باشد، به این معنا است که منابع و ویژگی‌های سیستمی مختلفی برای برقراری امنیت استفاده شده‌اند و باید به عملکرد و پایداری سیستم توجه دقیقی کرد. یک سیستم امن باید ضمن ارائه یک مکانیزم محافظتی قدرتمند، تمامی سرویس‌ها و ویژگی‌ها را به شکل پایداری در اختیار کاربر قرار دهد. شکل زیر عملکرد این مولفه‌ها را نشان می‌دهد.



زمانی که قرار باشد یک سطح امنیتی بالا را پیاده‌سازی کرد، تاثیرگذاری روی دو فاکتور قابلیت استفاده و پایداری اجتناب‌ناپذیر است. کاهش عملکرد به معنای روان نبودن کار با یک سیستم است، زیرا منابع مهم سیستمی همواره در اختیار ابزارهای امنیتی قرار دارند. در زمان تهیه یک برنامه امنیتی و استقرار آن در یک سامانه باید این اصل مهم در نظر گرفته شود که عملکرد و قابلیت استفاده از سیستم حفظ شوند. به عبارت دقیق‌تر، پیاده‌سازی یک استراتژی امنیتی به معنای برقرار تعادل میان سه مولفه یاد شده است.

بردارهای حمله و تهدیدات پیرامون امنیت اطلاعات

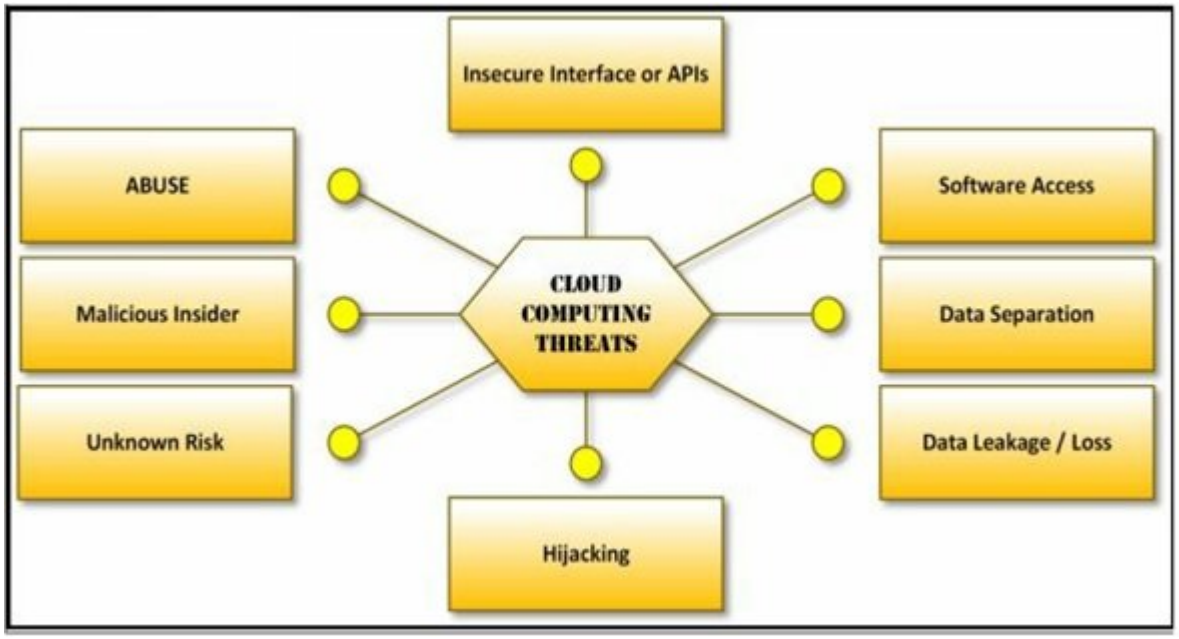
حملات هکری به دلایلی همچون انگیزه‌های انتقام‌جویانه، اهداف خاص یا محرک‌های اجتماعی رخ می‌دهند. انگیزه‌های انتقام‌جویانه یا محرک‌های اجتماعی باعث می‌شوند یک مهاجم به شکل متمرکزی در صدد حمله به یک سیستم خاص باشد. هکرها از روش‌های مختلفی برای دسترسی به یک سیستم استفاده می‌کنند. در یک حمله هکری آسیب‌پذیری‌های مستتر در یک سامانه به مهاجم کمک می‌کنند به اهداف مدنظر خود دست پیدا کند. سه مولفه انگیزه، هدف و محرک‌ها همراه با روش (Method) بلوک‌های اصلیو شکل دهنده یک حمله هستند.

نکته: پس زمانی که به عنوان یک کارشناس امنیتی جذب یک سازمان شدید، در زمان بروز حملات ابتدا باید به دنبال پاسخی برای این سه مولفه باشید.

انگیزه و هدف یک هکر برای حمله به یک سیستم ممکن است محتوایی باشد که درون یک سیستم خاص ذخیره شده است. این محتوا می‌تواند اطلاعات حساس مالی یا تصاویر و فیلم‌های شخصی قربانی باشد. در پس هر حمله هکری هدفی وجود دارد که باعث شده یک سیستم در معرض یک تهدید قرار بگیرد. از مهم‌ترین انگیزه‌های پیاده‌سازی یک حمله هکری می‌توان به سرقت اطلاعات، دستکاری داده‌ها، اختلال، گرایشات مذهبی یا سیاسی، شهرت یک فرد یا سازمان یا انتقام‌جویی اشاره کرد. در یک حمله هکری دو فاکتور روش به‌کار گرفته شده و آسیب‌پذیری مکمل یکدیگر هستند. هکرها از ابزارهای مختلف، روش‌های نوین و سنتی به منظور استخراج آسیب‌پذیری‌های درون یک سیستم استفاده می‌کنند. شکل زیر سه ترکیب سه فاکتور آسیب‌پذیری، روش و محرکی که باعث شکل‌گیری موفقیت‌آمیز یک حمله می‌شوند را نشان می‌دهد.

معروف‌ترین بردارهای حمله به امنیت اطلاعات
تهدیدات پیرامون رایانش ابری

رایانش ابری رایج‌ترین و محبوب‌ترین فناوری حال حاضر است و همین مسئله باعث شده تا تهدیدهای مرتبط با رایانش ابری روبه‌افزایش باشند. بیشتر اوقات، همان چالش‌های امنیتی پیرامون محیط‌های میزبانی سنتی در ارتباط با محاسبات ابری نیز وجود دارد. به همین دلیل مهم است امنیت محاسبات ابری، خدمات و داده‌های میزبانی شده در ابر به شکل جدی مورد توجه قرار گیرند. شکل زیر تهدیدات پیرامون محاسبات ابری را نشان می‌دهد.



از مهم‌ترین تهدیدات پیرامون امنیت ابر به موارد زیر می‌توان اشاره کرد:

در محیط‌های مبتنی بر رایانش ابری یک تهدید بزرگ پیرامون امنیت ابر نقض داده‌ای است که می‌تواند منجر به از دست رفتن داده‌ها یا دسترسی به فایل‌های دیگر شود. یک نقض داده‌ای در یک زیرساخت ابری به هکرها اجازه می‌دهد به سایر فایل‌های میزبانی شده روی فضای ابری دسترسی پیدا کنند. سناریو فوق بدترین وضعیت ممکن است که چالش‌های قانونی جدی را متوجه یک ارائه‌دهنده خدمات ابری کند.

از دست رفتن داده‌ها یکی دیگر از تهدیدات بالقوه پیرامون خدمات ابری است. از دست رفتن داده‌ها ممکن است عمدی یا سهوی و در مقیاس کوچک یا بزرگ باشد، اما در تمامی موارد نتیجه یکسان است، زیرا ارائه‌دهنده خدمات ابری مجبور است خسارت وارد شده به یک سازمان که منجر به از دست رفتن داده‌ها شده را تامین کند.

تهدید مهم دیگری که پیرامون خدمات ابری قرار دارد، سرقت حساب‌های کاربری و خدمات ابری است. برنامه‌های در حال اجرا روی ابر که دارای نقص نرم‌افزاری، رمزگذاری ضعیف، نقاط ضعف و آسیب‌پذیری‌ها هستند به مهاجمان

اجازه کنترل‌ها نرم‌افزارها یا خدمات را می‌دهند. علاوه بر موراد یاد شده، تهدیدات مهم دیگری همچون APIهای غیر ایمن، انکار خدمات، کارمندان مخرب، امنیت ضعیف، چند مستجری نیز پیرامون محاسبات ابری قرار دارند.

تهدیدهای مداوم پیشرفته

یک تهدید مداوم پیشرفته (APT) سرنام Advanced Persistent Threats به فرآیند سرقت مستمر اطلاعات اشاره دارد. یک تهدید مداوم پیشرفته معمولاً سازمان‌های خصوصی یا چهره‌های سیاسی را تهدید می‌کند. یک تهدید مداوم پیشرفته برای بهره‌برداری از آسیب‌پذیری‌های موجود در یک سیستم به تکنیک‌های پیشرفته و اغواگرانه متکی است. در این بردار حمله اصطلاح "پایدار" به فرآیند کنترل مستمر بر یک سیستم از طریق ابزارهای خارجی اشاره دارد که به‌طور مداوم در حال نظارت و واکشی داده‌ها از یک هدف هستند. واژه "تهدید" نیز توصیف‌کننده یک فعالیت مخرب از سوی هکر است. یک تهدید مدام پیشرفته ویژگی‌های زیر را دارد:

توضیحات	مشخصات
هدف یا محرکی که باعث شکل‌گیری تهدید شده	هدف
مدت زمان صرف شده برای جست‌وجو و دسترسی به هدف	زمان
سطح دانش و ابزارهای استفاده شده	منابع
مقاومت در برابر ابزارهای امنیتی با هدف شناسایی نشدن	مخاطره‌پذیری
تکنیک‌ها و ابزارهای استفاده شده در یک حمله	روش‌ها و مهارت‌ها
پیاده‌سازی دقیق حمله	اقدامات
تعداد نقاطی که قرار است به آن‌ها حمله شود	حمله به نقاط مشخص شده
تعداد سامانه‌های داخلی و خارجی که تحت تاثیر حمله قرار دارند	تعداد حملات انجام شده
اطلاعاتی که در ارتباط با شناسایی تهدیدات در دسترس است	منبع دانش

ویروس‌ها و کرم‌ها

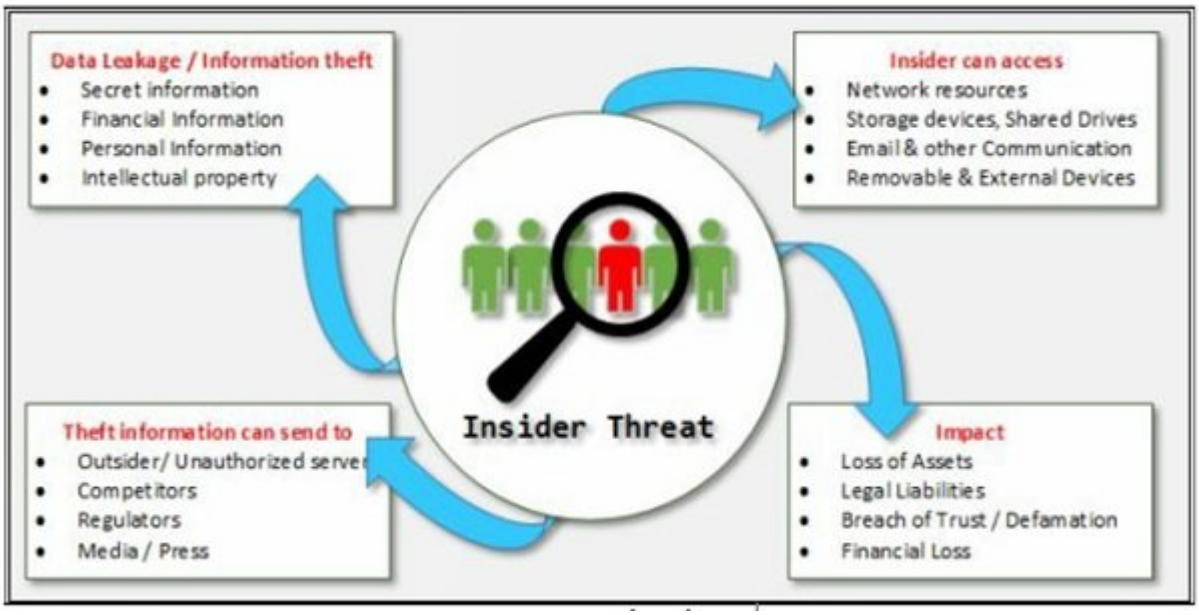
اصطلاح ویروس در دنیای امنیت اطلاعات و شبکه‌های کامپیوتری توصیف کننده نرم‌افزار مخرب است. نرم‌افزار مخرب برای پخش، تکثیر خود و الصاق به سایر فایل‌ها ساخته شده باشد. الصاق به فایل‌های دیگر کمک می‌کند تا ویروس سامانه‌های دیگر را آلوده کند. ویروس‌ها برای شروع فعالیت‌های مخرب در سیستم میزبان به تعامل با کاربر نیاز دارند. برخلاف ویروس‌ها، کرم‌ها قابلیت خودتکثیری دارند. این قابلیت باعث می‌شود که آن‌ها خیلی سریع در سامانه‌های مختلف پخش شوند. کرم‌ها از دهه 80 میلادی تا به امروز به اشکال مختلفی شبکه‌ها و سامانه‌ها را آلوده کرده‌اند. برخی از کرم‌های نوظهور کاملا مخرب هستند و بیشتر برای پیاده‌سازی حملات انکار سرویس (DoS) نوشته می‌شوند.

تهدیدات موبایل

فناوری نوظهور موبایل به ویژه تلفن‌های هوشمند باعث شده تمرکز مهاجمان روی دستگاه‌های همراه افزایش پیدا کند. از آن‌جایی که محبوبیت تلفن‌های هوشمند در سراسر جهان بالا است، هکرها مترصد فرصتی هستند تا اطلاعات تجاری و شخصی ذخیره شده در گوشی‌های هوشمند را سرقت کنند. از مهم‌ترین تهدیدات پیرامون دستگاه‌های همراه می‌توان به نشت داده‌ها، وای‌فای غیر ایمن، شنود اطلاعات، حملات فیشینگ، جاسوسی، رمزنگاری شکسته شده و پیکربندی اشتباه دستگاه اشاره کرد.

حملات درون سازمانی

حمله داخلی، نوع دیگری از حمله به یک سامانه تحت شبکه است که توسط یک کارمندی که سازمان به او اعتماد دارد انجام می‌شود. کارمند مورد تایید، فردی است که مجوزهای به دسترسی به سامانه‌ها و منابع شبکه را دارد. شکل زیر نمایی از تهدیدات سازمانی را نشان می‌دهد.



بات‌نت‌ها

بات‌نت اشاره به شبکه‌ای از کامپیوترها دارد که به‌طور مداوم و خودکار یک فرآیند را تکرار می‌کنند، توسط یک بدافزار آلوده شده‌اند، دستورات را توسط یک سرور راه دور دریافت کرده و کنترل می‌شوند. بات‌نت‌ها عمدتا برای انجام فرآیندهای تکراری استفاده می‌شوند. کامپیوترهایی که عضو یک شبکه بات‌نت می‌شوند را اسب‌های بارکش (workhorses) می‌نامند. بیشتر بات‌نت‌ها در ارتباط با Internet Relay Chat به کار گرفته می‌شوند که نوع قانونی و سودمند بات‌نت‌ها هستند. یک شبکه بات‌نت ممکن است برای کارهای مثبتی به کار گرفته شود، در حالی که برخی دیگر برای انجام کارهای غیرقانونی و فعالیت‌های مخرب پیاده‌سازی می‌شوند. بات‌نت‌های مخرب می‌توانند با هک کردن مستقیم یک سیستم یا از طریق عنکوبتی و با اتکا بر اسکریپت‌ها و کدهای مخرب به سامانه‌ها وارد شده و به آن‌ها دسترسی پیدا کنند. برنامه خزنده عنکبوتی روی بستر اینترنت شروع به جست‌جوی حفره‌های امنیتی می‌کند. بات‌ها می‌توانند سیستم قربانیان را با کامپیوتر اصلی که تحت کنترل یک هکر است متربط کنند. هنگامی که سیستم تحت کنترل قرار گرفت با ارسال پیامی برای هکر این موضوع را به او اطلاع می‌دهند. مهاجم از راه دور می‌تواند تمامی بات‌ها را توسط یک کامپیوتر اصلی کنترل کند.

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:
12 بهمن 1398

نشانی منبع:
https://www.shabakeh-mag.com/tricks/security-tricks/16529/%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%AB%D9%84%D8%AB-%D8%A7%D9%85%D9%86%DB%8C%D8%AA-%D9%88-%D9%85%D8%B9%D8%B1%D9%88%D9%81%E2%80%8C%D8%AA%D8%B1%DB%8C%D9%86-

%D8%A8%D8%B1%D8%AF%D8%A7%D8%B1%D9%87%D8%A7%DB%8C-
%D8%AD%D9%85%D9%84%D9%87