آموزش CEH (هکر کلاه سفید): آشنایی با مراحل فنی پیاده‌سازی یک حمله سایبری

مهاجمان از یک روش ثابت برای نفوذ به سامانه‌ها استفاده می‌کنند. به همین دلیل برای مغلوب کردن هکرها باید همانند یک هکر فکر کنید. مراحلی که یک هکر برای حمله به سامانه یا شبکه‌ای بر مبنای آن کار می‌کند به شش مرحله شناسایی و ردیابی، پویش و سرشماری، به دست آوردن دسترسی/ حفظ دسترسی، ترفیع امتیاز، حفظ دسترسی‌ها و پنهان‌سازی ردپاها و قرار دادن درب‌های پشتی مرحله تقسیم شود.

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

اخلاقی و قانون‌مداری

واژه اخلاق از کلمه یونانی ethos (شخصیت) اقتباس شده است. دو واژه قانون و اخلاق تفاوت زیادی با یکدیگر دارند، زیرا اخلاق عمدتا روی موضوعات و مباحث خاکستری متمرکز است که برای قانون چندان مهم نیست. اکثر متخصصان و شرکت‌های فعال در زمینه امنیت همچون EC-Council روی موضوعات اخلاقی حساس هستند و خط‌مشی‌های مختلفی در این زمینه دارند. از جمله شرکت‌هایی که روی مباحث اخلاقی تاکید خاصی دارند باید به EC-Council، ISC و ISACA اشاره کرد.

https://www.eccouncil.org/code-of-ethics

https://www.isc2.org/ethics/default.aspx

http://www.isaca.org/Certification/Code-of-Professional-Ethics/ Pages/default.aspx

برای تبدیل شدن به یک هکر اخلاق‌مدار، باید درک خوبی از موازین اخلاقی داشته باشید، زیرا ممکن است در طول دوران حرفه‌ای خود با مباحث اخلاقی مختلفی روبرو شوید. همچنین در آزمون CEH باید در انتظار پرسش‌هایی حول محور اخلاقیات باشید.

گزارش‌های اخیر سازمان‌های دولتی نشان می‌دهد استفاده غیر مجاز از کامپیوترها رشد روزافزونی دارد و روزانه انواع مختلفی از حملات به شبکه‌های کامپیوتری انجام می‌شود. هکرها از رایانه‌ها به عنوان ابزاری برای ارتکاب جرم یا برنامه‌ریزی برای انجام فعالیت‌های مخرب و انجام حملات هکری پیرامون شبکه‌ها استفاده می‌کنند. وظیفه شما به عنوان یک هکر اخلاقی پیدا کردن آسیب‌پذیری‌ها قبل از حمله مهاجمان و پیشگیری از بروز حملات هکری است. پیگیری و پیگرد قانونی هکرها می‌تواند کار دشواری باشد، زیرا قوانین بین‌المللی غالباً برای مقابله با این مشکل

چندان راهگشا نیستند. برخلاف جنایات متعارف که در یک مکان اتفاق می‌افتند ممکن است سرچشمه جنایات هکری در یک کشور اروپایی باشد، در یک کشور آسیایی پیاده‌سازی شده باشد و شرکتی در ایالات متحده یا کانادا را هدف قرار داده باشند. هر کشوری دیدگاه‌های خاص خود را در قبال جرایم سایبری دارد. حتا اگر امکان مجازات هکرها وجود داشته باشد، تلاش برای تحت پیگرد قانونی قرار دادن آن‌ها ممکن است شبیه به کابوسی باشد. اعمال مرزبندی برای رسانه‌ای مانند اینترنت که اساساً بدون مرز است کار سختی است. به عنوان یک هکر قانون‌مدار لازم است درباره قوانین وضع شده در ارتباط با جرایم سایبری اطلاعات کافی داشته باشید. بنابراین پیشنهاد می‌کنم با صرف کمی وقت اطلاعات خود درباره قوانین زیر را افزایش دهید:

Electronic Communication Privacy Act

Computer Fraud and Abuse Act of 1984

The Cyber Security Enhancement Act of 2002

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001

The Federal Information Security Management Act

Federal Sentencing Guidelines of 1991

Economic Espionage Act of 1996

همچنین پیشنهاد می‌کنم درباره قوانین مبارزه با جرایم سایبری ایران نیز اطلاعات لازم را کسب کنید.

مفاهیم تکنیکی هک

اکنون با مفاهیم اخلاقی، بایدها و نبایدهای مرتبط با هک اخلاقی آشنا شدیم، زمان آن رسیده تا به سراغ مباحث فنی مربوط به هک برویم. در ابتدا به بررسی فرآیندهایی می‌پردازیم که یک هکر برای نفوذ به یک سامانه یا شبکه ارتباطی بر مبنای آن‌ها رفتار می‌کند.

فرآیندهای مورد استفاده یک هکر

مهاجمان از یک روش ثابت برای نفوذ به سامانه‌ها استفاده می‌کنند. به همین دلیل برای مغلوب کردن هکرها باید همانند یک هکر فکر کنید. مراحلی که یک هکر برای حمله به سامانه یا شبکه‌ای بر مبنای آن کار می‌کند به شش مرحله زیر تقسیم شود.

- شناسایی و ردیابی
- پویش و سرشماری
- به دست آوردن دسترسی/ حفظ دسترسی
- ترفیع امتیاز
- حفظ دسترسی‌ها
- پنهان‌سازی ردپاها و قرار دادن درب‌های پشتی

نکته: اگر هکری موفق نشود به سامانه یا شبکه‌ای نفوذ کرده و دسترسی‌های مربوطه را به دست آورد، سع یمی‌کند با قطع خدمات سازمان و پیاده‌سازی یک حمله منع سرویس (DoS) باجی از سازمان دریافت کند.

اجازه دهید هر یک از مراحل مذکور را با جزییات بیشتری بررسی کنیم.

مرحله اول شناسایی و جمع آوری اطلاعات (Reconnaissance and Foot printing)

شناسایی و جمع‌آوری اطلاعات اولین قدم در پیاده‌سازی یک حمله سایبری است. در این مرحله هکر به شکل سیستماتیک سعی می‌کند اطلاعات مورد نیاز درباره هدف را جمع‌آوری کند. در این مرحله هکر سعی می‌کند تا جایی که امکان دارد اطلاعات بیشتری در مورد یک قربانی به دست آورد. به عبارت دقیق‌تر در این مرحله اطلاعات غیرفعالی جمع‌آوری می‌شود. به‌طور مثال، در بسیاری از فیلم‌ها مشاهده کرده‌اید که کاراگاهی تمام شب در خارج از خانه یک مظنون منتظر می‌ماند و هنگامی که خانه را با خودرو خود ترک کرد با فاصله او را تعقیب می‌کند. این مرحله شناسایی است و ماهیتی منفعل دارد. مرحله فوق اگر به درستی انجام شود، هدف متوجه نخواهد شد که فردی در حال تعقیب او است. هکرها می‌توانند اطلاعات را از طرق مختلف جمع‌آوری کنند. اطلاعات به‌دست آمده به آن‌ها امکان می‌دهد تا نقشه‌ای برای حمله آماده کنند. ممکن است برخی از هکرها ممکن است برای پیدا کردن اطلاعات بیشتر در مورد قربانی به سراغ سطل زباله خانه او بروند. اگر سازمانی خط‌مشی خوبی برای نظارت بر فعالیت‌های رسانه‌ای و همچنین امحاء اطلاعات تدوین نکرده باشد، به احتمال زیاد اطلاعات حساس زیادی را ناآگاهانه در سطل‌های زباله قرار می‌دهد. به همین دلیل سازمان‌ها باید به کارکنان خود دستور دهند که اطلاعات حساس را به روش‌های مختلفی امحاء کنند. این فکر را از ذهن خود درون کنید که اگر از اسناد کاغذی استفاده نکنید برای همیشه در امان هستید.

یکی دیگر از ترفندهای موارد مورد علاقه هکرها مهندسی اجتماعی است. یک متخصص مهندس اجتماعی، فردی است که می‌تواند افراد دیگر را برای آشکار کردن اطلاعات حساس اغوا کند. هکر می‌تواند با کارمند یک سازمان تماس مستقیم برقرار کند و از او بخواهد گذرواژه حساب کاربری خود را تغییر دهد یا از طریق ارسال نامه الکترونیکی به ظاهر درون سازمانی به کارمند بگوید که حساب کاربری او به تنظیم مجدد نیاز دارد. اگر هکر مصمم باشد تا اطلاعاتی به دست آورد سعی می‌کند از ابزارهای مختلفی برای این منظور استفاده کند. یکی از قدرتمندترین ابزارها اینترنت است. بله درست شنیدید. اینترنت امکانات زیادی برای جمع‌آوری اطلاعات در اختیار هکرها قرار می‌دهد. اجازه دهید کار را با وب‌سایت شرکتی شروع کنیم. در وب‌سایت شرکتی ممکن است اسامی برخی از کارمندان کلیدی همراه با موقعیت شغلی و فناوری‌هایی که از آن‌ها استفاده می‌کنند فهرست شده باشد. برخی از سایت‌ها نیز از یک بانک اطلاعاتی که حاوی نام کارمندان و آدرس ایمیل آن‌ها است استفاده می‌کنند.

نکته: خط‌مشی‌های امنیتی اولین دفاع قدرتمند در برابر حملات شناسایی هستند.

پویش و شمارش (Scanning and Enumeration)

پویش و سرشمارش دومین مرحله قبل از حمله هستند. پویش یک مرحله فعال است که برای اتصال به سیستم‌ها و دریافت پاسخ انجام می‌شود. سرشماری برای جمع‌آوری اطلاعات عمیق‌تر درباره هدف، مانند اطلاعات به‌اشتراک گذاشته شده و اطلاعاتی پیرامون حساب‌های کاربری انجام می‌شود. در این مرحله، رویکرد هکر از جمع‌آوری اطلاعات غیرفعال به سمت جمع‌آوری اطلاعات فعال متمایل می‌شود. در این مرحله هکرها فرآیند تزریق بسته‌ها به شبکه را آغاز می‌کنند و ممکن است از ابزارهای اسکن همچون Nmap استفاده کنند. هدف نقشه‌برداری از درگاه‌ها و برنامه‌های باز است. ممکن است هکر ممکن است از تکنیک‌هایی استفاده کند تا سرعت پویش درگاه‌ها کم شود تا شناسایی شدن را به حداقل برساند. به‌طور مثال، به جای بررسی تمام برنامه‌های کاربردی بالقوه تنها در چند دقیقه ممکن است از یک پویش زمان‌بر استفاده کند که شاید چند روز طول بکشد. در این فرآیند هکر بررسی می‌کند که چه برنامه‌هایی روی یک سامانه یا شبکه در حال اجرا هستند. بسیاری از سازمان‌ها از سیستم‌های تشخیص نفوذ (IDS) برای شناسایی اسکن پورت استفاده می‌کنند. با این حال، تصور نکنید هکر به نقشه‌برداری از پورت‌های باز بسنده خواهد کرد. او در مرحله بعد به سراغ بررسی نسخه مورد استفاده از یک برنامه کاربری می‌رود که روی شبکه سازمانی در حال اجرا است. او سعی می‌کند به سراغ نرم‌افزارهای قدیمی برود که روی شبکه سازمانی استفاده می‌شوند و همچنان آلوده به آسیب‌پذیری‌های شناخته شده هستند. نمونه‌ای از این نرم‌افزارهای قدیمی ویندوز ایکس‌پی است. یک سیستم‌عامل قدیمی که آسیب‌پذیری‌های زیادی در آن وجود دارد، اما توسط برخی از شرکت‌ها و حتا سازمان‌های دولتی استفاده می‌شود. هرچه نرم‌افزارهای مورد استفاده یک سازمان قدیمی باشد، آسیب‌پذیری‌های زیادی در آن‌ها وجود دارد. برای اطلاع در مورد آسیب‌پذیری‌ها و کدهای آسیب‌پذیر مستتر در نرم‌افزارهای کاربردی هکرها از سایت‌هایی شبیه به http://www.exploit-db.com استفاده می‌کنند

نکته: واژه انکار (deny) به معنای مسدود شدن تمامی خدمات و برنامه‌های کاربردی است. از سرگیری فعالیت‌ها منوط به دریافت تاییده مربوطه از سرویس‌های مجاز است. رویکرد فوق می‌تواند به کاهش اثربخشی فعالیت هکرها کمک کند.

هکرها از برنامه‌هایی شبیه به OpenVAS برای یافتن آسیب‌پذیری‌ها استفاده می‌کنند. درست است که این برنامه‌ها با هدف هک کردن سامانه‌ها طراحی نشده‌اند، اما اطلاعات مفید زیادی در ارتباط با شبکه‌ها در اختیار هکرها قرار می‌دهند. یکی از نکات منفی اسکنرهای آسیب‌پذیری شناسایی سریع آن‌ها است، زیرا نرخ ارسال و دریافت بسته‌های اطلاعاتی توسط این اسکنرها بالا است.

حفظ دسترسی/ به دست آوردن دسترسی (Gaining Access)

برای آن‌که هکری بتواند به یک سامانه یا شبکه‌ای حمله کرده و خسارت‌هایی به وجود آورد باید بتواند دسترسی که به‌دست آورده را حفظ کند. در این مرحله حمله آغاز می‌شود و هکر دیگر در جست‌وجوی اطلاعات نیست، بلکه به دنبال پیاده‌سازی حمله است. زمانی که هکر موفق شود دسترسی مربوطه را به دست آورد، سعی می‌کند از یک سامانه به سامانه دیگری حرکت کند و کدها یا اسکریپت‌های مخرب را درون سامانه‌های مختلف پخش کند. دسترسی به روش‌های مختلفی به دست می‌آید. یک هکر ممکن است یک نقطه دسترسی بی‌سیم باز پیدا کند که به او اجازه می‌دهد به‌طور مستقیم با شبکه در ارتباط باشد یا ممکن است با استفاده از ترفندهای خاصی شماره تلفنی را برای اتصال به شبکه‌های ناشناخته در اختیار کارمندان یک سازمان قرار دهد. زمانی که هکر بتواند آسیب‌پذیری در یک برنامه تحت وب پیدا کند که می‌داند سازمان از آن استفاده می‌کند، در مرحله بعد به سراغ به دست آوردن دسترسی خواهد رفت. هکر ممکن است برنامه وب را با بدافزار آلوده کند، زیرا از این موضوع اطمینان خواهد داشت که برخی از کارمندان سازمان از برنامه آلوده استفاده خواهند کرد.

تکنیک فوق به‌نام حلمه watering-hole شهرت دارد. اگر هکر واقعاً جسور باشد، ممکن است به سازمان مراجعه کند و به مسئول پذیرش اعلام کند که برای شرکت در جلسه‌ای دیر رسیده و اگر امکان اشت در اتاق کنفرانس منتظر باشد، به این امید که بتواند در اتاق کنفرانس روزانه‌ای برای دسترسی به شبکه پیدا کند. در این حالت مسئول مربوطه بی اطلاع از همه‌جا و ناآگاهانه امکان دسترسی به شبکه را برای یک هکر مخرب فراهم می‌کند. این مشکلات برای سازمان‌هایی رخ می‌دهد که که نتوانسته‌اند رویه‌ها و خط‌مشی‌های امنیتی را به خوبی به کارمندان خود آموزش دهند. هکرها بر مبنای سطح مهارت، مهارت‌های اجتماعی، معماری شبکه هدف و نحوه پیکربندی شبکه قربانی از روش‌های مختلفی برای به دست آوردن سطح دسترسی استفاده می‌کنند.

ترفیع امتیاز (Privilege escalation)

درست است که هکرها زمانی که یک سطح دسترسی پیدا کنند خوشحال می‌شوند، اما نباید انتظار داشته باشید کار آن‌ها تنها با دسترسی به یک حساب کاربری به اتمام برسد. در اختیار گرفتن یک حساب کاربری معمولی به هکر اجازه انجام کار خاصی در شبکه را نمی‌دهد، بنابراین تلاش خواهد کرد تا سطح امتیازهای خود را به سمت مدیر دامنه یا مجوزهای ریشه ارتقا دهد. مدیر دامنه فردی است که شبکه را کنترل می‌کنند و همان مجوز و قدرتی را در اختیار دارد که هکر به دنبال آن است. ترفیع امتیاز در برخی مواقع انجام می‌شود، زیرا ممکن است یک باگ، پیکربندی اشتباه یا آسیب‌پذیری در یک برنامه کاربردی یا سیستم‌عامل وجود داشته باشد که به هکر اجازه می‌دهد به منابع دسترسی پیدا 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:

26 بهمن 1398

نشانی منبع:
https://www.shabakeh-mag.com/security/16578/%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%B1%D8%A7%D8%AD%D9%84-%D9%81%D9%86%DB%8C-%D9%BE%DB%8C%D8%A7%D8%AF%D9%87%E2%80%8C%D8%B3%D8%A7%D8%B2%DB%8C-%DB%8C%DA%A9-%D8%AD%D9%85%D9%84%D9%87-%D8%B3%D8%A7%DB%8C%D8%A8%D8%B1%DB%8C