

هائبرد

دنیای تجارت بدون مرز
SHIBERO
 شرکت تجارت الکترونیک هائبرد
www.hiberd.com
 ۸ ۸ ۹ ۳ ۶ ۹ ۵ ۸

CMS، طراحی وب سایت، فروشگاه اینترنتی

تجارت هوشمند، جامعه ای مدرن
 دانشگاه مجازی
 ویندوز سرور ۲۰۰۸
 بانکداری از طریق موبایل
 مقدمه ای بر تجارت همراه

فناوری اطلاعات

اولین ماهنامه تخصصی IT در ایران

سال چهارم، شماره ۳۸، آذر ماه ۱۳۸۷، ۱۰۰۰ تومان

ITE Magazine, Vol.4, No.38, December 2008
www.infotechera.com

در مسابقه تفسیر طرح روی جلد شرکت کنید



Commerce





مقدمه‌ای بر هک اخلاق مدارانه (بررسی قواعد، ضمن رعایت اصل مطابقت با قوانین) سلسله گزارش‌های فنی، شماره یک

مهندس علی کسرایی

واژگان کلیدی:

امنیت اطلاعات، فناوری‌های هکینگ، هک اخلاق مدار، آزمون‌های آسیب‌شناسی

چکیده:

اغلب مردم می‌اندیشند که هکرها، از مهارت‌های غیر عادی، فوق العاده و شگفت‌انگیزی برخوردار بوده و دانش آنهاست که در نفوذ به سیستم‌های کامپیوتری، به ایشان کمک می‌کند؛ بطوری که می‌توانند به اطلاعات ارزشمندی، دست یابند. اصطلاح هک، برای یک جوان، تصویری از جادوگری را مجسم می‌کند که می‌تواند با تایپ چند دستور کوچک در کامپیوتر مقصد، ... (و همه چیز نابود می‌شود)!

بدین معنی که به راحتی بیرون انداختن آبی از دهانش، کامپیوتر مزبور را مورد حمله قرار می‌دهد و اطلاعات محرمانه آن را بیرون می‌کشد. ولی در حقیقت، یک هکر ماهر، فقط به این درک رسیده است که سیستم‌های کامپیوتری، چگونه کار می‌کنند و در این راستا، با تحقیق و ممارست بسیار، کشف می‌کند که چه ابزاری را بکار گیرد تا ضعف‌ها و حفره‌های امنیتی سیستم‌های مزبور را پیدا کرده و در نهایت، به اهداف خود دست یابد. در ادامه، شایان ذکر است که بدانید، قلمرو هکرها و نحوه عملکردشان، برای بیشتر کاربران حرفه‌ای کامپیوتر و محققان مباحث امنیتی نیز مشخص نشده است. لذا هدف از نگارش این گزارش فنی، معرفی دنیای هکرها و همچنین، تعریف اصطلاحاتی است که در آزمون (CEH) یا گواهینامه هک اخلاق مدار، مورد پرسش واقع می‌شوند. در خاتمه، شایسته می‌داند که به مورد ترجمه عبارات انگلیسی توجه کنند؛ چرا که همگان اشراف دارند که برخی از مصطلحات علمی دانش رایانه، بخصوص مباحث هکینگ، معادل فارسی پر معنایی ندارد.

لذا، اگر در ترجمه آنان، سهواً القلمی مشاهده شد، بزرگان، به دیده بخشش نظر کنند.

گر خطا گفتیم اصلاحش تو کن مصلحی تو ای تو سلطان سخن

الف - درک مفاهیم و اصطلاحات علمی هک اخلاق مدارانه:

توانایی در درک و آرایه تعاریف اصطلاحات علمی این دانش، از اهداف مهم آزمون (CEH)، به شمار می‌رود. در این بخش، به ذکر تعدادی از پرکاربردترین آن‌ها، بسنده می‌شود.

• (Threats) یا تهدیدات:

یک تهدید، محیط یا وضعیتی است که می‌تواند به یک شکاف امنیتی بالقوه، منتهی شود. هک‌های اخلاق مدار، در این بین، به هنگام بررسی و تحلیل موارد امنیتی محیط مزبور، این تهدیدات را بر حسب ارجحیت و اولویت، خطر سازی، رده بندی می‌کنند.

• (Exploit) ها:

در مبحث امنیت و حفاظت داده‌ها، یک (Exploit) اکسپلویت، در واقع یک قطعه نرم افزار یا رویداد نرم افزاری است که با بهره گیری از باگ در سیستم‌ها، همگام با وارد ساختن ضربات امنیتی و ایجاد آسیب، دسترسی غیر مجاز به سیستم‌های مورد حمله را تعدیل بخشیده و همچنین می‌تواند باعث ایجاد آمادگی برای نوعی حمله با عنوان (Dos) یا (Denial of service) گردد. که به منزله قطع، یا از کار انداختن سرویس خاصی در رایانه مزبور می‌باشد.

• (Exploit) ها، از دیدگاه متد و عملکرد به ۲ دسته تقسیم می‌شوند:

الف (Remote exploit):

یک (Remote exploit)، روی یک شبکه و نقاط آسیب پذیر آن کار می‌کند، و بدون هرگونه دسترسی قبلی به سیستم آسیب پذیر، از آن بهره‌کشی می‌کند.

ب - (Local exploit):

یک (Local exploit)، بر روی افزایش دسترسی، به سیستم آسیب پذیر، از طریق مسیرهای قابل دسترسی قبلی تمرکز دارد. پس یک (Exploit)، یک راه تعریف شده جهت ورود به شکاف‌ها و حفره‌های امنیتی یک سیستم، با ادعای داشتن بستر حفاظتی و اطلاعاتی کامل، اما با درصد آسیب پذیری بالا، می‌باشد.

• نقاط آسیب پذیر (Vulnerability):

یک نقطه آسیب پذیر می‌تواند، نقص موجود یک نرم افزار در طراحی منطقی یا عدم توجه به یک خطای خاص و اجرای غیر منظره آن باشد، که اغلب منجر به اجرای رویدادهای نامطلوب یا اجرای دستورالعمل‌های آسیب رسان به سیستم می‌شود.

• هدف‌ها (Target):

اهداف، در حقیقت ارزیابی سیستم‌ها، برنامه‌ها و شبکه‌ها می‌باشند که موضوع تحلیل امنیت آن‌ها در بین است و بررسی نقاط آسیب پذیرشان، به جهت حمله کردن.

• حمله (Attack):

یک حمله، زمانی اتفاق می‌افتد که حداقل نقطه یا حفره‌ای برای آسیب پذیری یک سیستم، یافت شده و موجود باشد. بسیاری از حمله‌ها به کمک (Exploit) ها، بصورت روتین و همیشگی انجام می‌شوند. هک‌های اخلاق مدار، از ابزارهایی به جهت شناسایی نقاط آسیب پذیر سیستم‌ها استفاده می‌شوند. چراکه ممکن است که این نرم افزارهای مخرب، باعث صدمه رساندن به سیستم‌های عامل، پیکربندی شبکه‌ها یا برنامه‌های نصب شده بر روی سیستم‌ها شوند. و هک‌های اخلاق مدار، با عنایت به کاربرد صحیح ابزارهای مذکور، مانع از حمله به سیستم‌ها می‌شوند و باعث کاهش نقاط آسیب پذیر آنان، می‌گردند. در نهایت، معترفیم که این سلسله مقالات، ابزارها و دانش لازم را جهت تبدیل شما به یک هکر اخلاق مدار، فراهم می‌سازد. همچنین، علاوه بر احاطه علمی داشتن، به تعاریف اصطلاحاتی که شرحشان گذشت، خیلی مهم است که فرق بین هک‌های اخلاق مدار

و هکرهاى بدخیم یا آسیب رسان را بدانید و درک کنید که هکرهاى اخلاق مدار، چه کارهائى را برای برقرارى امنیت، انجام داده و حیطه وظايفشان تا کجاست؟

ب - تشخیص انواع متفاوت فناوری های هک کردن

روش ها و ابزار بسيارى برای (حمله و يا) تشخیص نقاط آسیب پذیر، اکسپلویت هاى در حال اجرا و کشف رمز سیستم ها وجود دارد. تروجان ها، بک دورها، اسنیفرها، روت کیت ها، اکسپلویت ها، اورفلوها و اس.کیو.ال اینجکشن ها، همه آن فناوری هاى هستند که برای هک شبکه ها و سیستم هاى رایانه اى، مورد بهره بردارى قرار مى گیرند. (سعى بر آنست که در مورد روش هاى حمله و تحلیل فناوری ها، به سبب پیچیدگى مطالب، در گزارشات فنى بعدى، بحث شود). بیشتر این ابزارها در هک، به سوء استفاده از نقاط ضعف، در چهار حفره زیر اشاره داشته و متمرکزند:

الف - سیستم های عامل

بسيارى از مدیران سیستم ها (Administrators)، سیستم هاى عامل را در حالت تنظیمات از پیش تعیین شده تولیدکننده، نصب و راه اندازى مى کنند. این حالت هم به بالا بردن پتانسیل آسیب پذیری سیستم ها منتج شده و هم شبکه هاى متصل به آن ها را به خطر مى اندازد.

ب - برنامه ها

دیده مى شود که اغلب برنامه ها، پس از پایان طراحی و کد نویسى، توسط توسعه دهندگان، به جهت شناخت نقاط آسیب پذیر و سایر تهدیدات از این دست، مورد آزمایش قرار نمى گیرند، که این خود فرصتى است که به یک نفوذگر برای اخلال، نه فقط در برنامه مذکور، بلکه در رایانه حامل، ارایه خواهد شد.

ج - شبه کدها یا کدهاى قابل اجرا با حجم کم:

بعضى از نرم افزارها، در درون خود، قابلیت اجرای شبه کدها و یا کدهائى به زبان هاى مختلف را دارند که مى توان این مورد را به نوعى، عاملی برای سوء استفاده هکرها از رایانه ها، دانست. به طور مثال، ماکروها در محصول آفیس از شرکت مایکروسافت که به هکرها اجازه مى دهند تا برنامه هاى اجرایی بسيارى را بصورت ماکرو، اجرا کنند و این گونه است که حفره اى جهت نفوذ به سیستم، گشوده مى شود.

د) پیکربندى غلط

پیکربندى نادرست و یا تنظیم امنیت سیستم در درجه پایین، اغلب، حاصل دستکاری غیر علمى کاربران نا آگاه است که باعث افزایش نقاط آسیب پذیر در سیستم ها شده و امکان حمله به آن را فراهم مى آورد.

نکته

در سلسله مقالات بعدى و به تکامل، به بحث و تحلیل، پیرامون فناوری ها و ابزار هک کردن خواهد پرداخت؛ ولى هم اکنون، لازم است تا قبل از بررسى موارد فوق، به درک و شناخت عمیق انواع حملات و اساس امنیت سیستم ها، نائل شوید. بنابراین ابتدا درک، سپس تحلیل. علاوه بر انواع فناوری هاى که یک هکر مى تواند استفاده کند، باید خاطر نشان کرد که حملات و تهدیدات مختلفی نیز وجود دارند.

متخصصان امنیت، حملات را به ۲ بخش دسته بندى مى کنند:

الف - فعال (Active)

ب - غیر فعال (Passive)

شایان ذکر است که این ۲ نوع حمله، می‌توانند هم بر روی زیرساخت‌های امنیت شبکه‌ها و هم بر روی سیستم‌های میزبان (Hosts) اثر بگذارند. در واقع در حملات فعال، توجه هکر به سیستم‌ها و شبکه‌ها معطوف است و آن‌ها را مورد حمله قرار می‌دهد؛ در صورتی که در حملات غیر فعال، هدف هکر، به دستیابی به اطلاعات سودمند (و یا مورد نظرش) منتج می‌شود. به دیگر سخن، حملات فعال بر قابلیت دسترسی، تمامیت و صحت یا درستی داده‌ها اثر می‌گذارند و این در حالی است که حملات غیر فعال، به شکاف و رخنه در قابلیت اعتماد در دسترسی به داده‌ها، اشاره می‌کنند. علاوه بر دسته بندی حملات به فعال و غیر فعال، آن‌ها را به دو دسته حملات داخلی (درونی) و خارجی (بیرونی) نیز طبقه بندی می‌کنند. یک حمله درونی، توسط یک نیروی داخلی درون سازمانی انجام می‌پذیرد، چراکه ممکن است، حمله کننده، دسترسی قابل توجهی به منابع سازمان مورد نظر، داشته باشد، لذا، در سوء استفاده از اطلاعات، سود بیشتری نیز حاصل می‌کند؛ ولی یک حمله بیرونی، از یک مبدأ خارج از سازمان، سرچشمه می‌گیرد، مانند، اینترنت یا یک ارتباط منجر به دستیابی از راه دور.

نکته

بسیاری از شکاف‌های امنیتی شبکه‌ها، از عوامل داخلی همان سازمان یا کمپانی، سرچشمه می‌گیرند، مانند: کارمندان یا پیمانکاران.

ج- درک مراحل متفاوت درگیر در یک اخلاقی و همچنین فهرست پنج مرحله‌ی

هک کردن اخلاقی :

یک هکر اخلاق مدار، از فرآیند و روش‌ها، همانند یک هکر بدخیم، پیروی می‌کند. به دیگر سخن، مراحل و روش‌های ورود به سیستم‌های رایانه‌ای، برای هکرهای اخلاق مدار، همان است که نفوذگران سیستم‌ها، از آن‌ها بهره می‌جویند. سطور زیر، پنج مرحله‌ای که هکرها در حالت کلی، در سرقت اطلاعات از آن‌ها استفاده می‌کنند را نشان می‌دهد. بدیهی است که در ادامه، به تحلیل این مراتب، می‌پردازیم.

مرحله ۱: شناسایی - کشف اطلاعات مقدماتی از هدف

مرحله ۲: پیمایش یا اسکن جهت شناخت معایب و محاسن اهداف

مرحله ۳: دستیابی به سیستم (بدست آوردن یا حصول دستیابی)

مرحله ۴: نگهداری یا حفظ مسیر دسترسی

مرحله ۵: پوشاندن رد پا

مرحله ۱: شناسایی فعال یا غیر فعال بودن:

شناسایی غیر فعال، شامل مرحله‌ای از گردآوری اطلاعات از هدف توسط هکر می‌شود، که به طور عام بدون هیچ گونه اطلاعات قبلی از هدف مذکور صورت می‌پذیرد. شناسایی غیر فعال، به سادی توسط نگهبان یک سازمان انجام شده که می‌تواند رفت و آمد کارمندان و سایرین را تحت کنترل، قرار دهد. با این وجود، با جستجو در اینترنت و همچنین از گفتگو با افراد آن سازمان نیز، به سادگی قادر به کسب اطلاعات خواهد بود. این فرآیند را (گردآوری اطلاعات) می‌نامند. مهندسی اجتماعی و همچنین روبرداری از اطلاعات، از ارکان غیر فعال روش‌های غیر فعال گردآوری اطلاعات می‌باشند. اسنایف کردن، نیز از ابزار شناسایی غیر فعال به شمار می‌آید. فهرست زیر به دستاورد حاصل از این نوع حمله اشاره دارد:

الف - محدوده آدرس‌های IP شبکه‌ها

ب - استانداردهای سخت افزاری سیستم‌ها در شبکه‌ها

ج - سرویس‌های پنهان در شبکه‌ها

د - سرویس‌های در دسترس و فعال روی سیستم‌های عضو شبکه‌ها

عمل اسنایف کردن یک شبکه همانند زیر نظر داشتن یک ساختمان بوده؛ توجه یک هکر به روند تبادل داده‌ها معطوف است. به طوریکه مواظب است که ببیند، داده‌ها از کجا می‌آیند و به چه مسیری، هدایت می‌شوند. در این بین، شناسایی فعال، شامل کاوشی است که، به کشف سیستم‌ها و (Host) های شخصی، منجر می‌شود، مانند: آدرس‌های (IP) و سرویس‌های فعال در شبکه و مشاهده می‌شود که به نوعی، تداعی کننده روش‌های شناسایی غیرفعال بوده، که (Rattling The Doorknobs) یا (دستگیره درب هوشمند) نامیده می‌شوند. شناسایی فعال، می‌تواند به یک هکر، کلید و یا درب ورودی اطلاعاتی، نظیر این‌که، آیا درب‌های ورودی سیستم مورد نظر باز است یا نه را بدهد. این حداقل کاریست که فرآیند شناس و ورود به یک سیستم را افزایش داده و یا سوء ظن این‌که هکر به سراغ درب‌های دیگر نرود را کاهش می‌دهد. پس شناسایی فعال و غیرفعال، می‌تواند به کشف اطلاعات مهمی که یک هکر در یک حمله، بدان نیازمند است، منجر شود. به طور مثال، به راحتی می‌توان از نوع وب سرور و ورژن سیستم عامل روی آن‌که در یک سازمان، در حال بهره‌برداری است، آگاه شد. این اطلاعات، به هکر توانایی می‌بخشد تا به عنوان مثال نوعی اکسپلویت را طراحی کرده که با نسخه سیستم عامل وب سرور مذکور، سازگار بوده و با تکیه بر نقاط آسیب پذیر در این سرور، بتواند موجبات دسترسی بیشتر به داده‌های آن را برای خود، فراهم آورد.

مرحله ۲: پیمایش (Scan)

اسکن کردن، در واقع مرحله‌ای است که هکر، اطلاعات کشف شده قبلی، که در طول مرحله شناسایی بدست آمده بود را به منظور بررسی قابلیت استفاده در حمله به شبکه مزبور، امتحان می‌کند. ابزاری را که هکرها، در طول مرحله اسکن شبکه‌ها، ممکن است از آن‌ها، استفاده کنند، شامل موارد زیراند:

الف - شماره گیرها (Dialers)

ب - اسکنر پورت‌ها (Port Scanners)

ج - نمایشگر معماری و ساختار شبکه‌ها (Network mappers)

د - جاروکش‌ها (Sweepers)

ه - و اسکنرهای کشف نقاط آسیب پذیر

هکرها، در جستجوی هرگونه اطلاعاتی هستند که به آن‌ها در آماده‌سازی حملات شان، کمک می‌کنند. همانند:

الف - نام کامپیوترها

ب - آدرس‌های IP آن‌ها و حساب‌های کاربران

نکته

روش‌ها و ابزارهای بکار رفته در مرحله اسکن، به تفصیل در گزارشات فنی بعدی، تحت عنوان (اسکن و شماره گذاری) مورد بررسی قرار گرفته است.

مرحله ۲: حصول دستیابی

در این مرحله است که سرقت واقعی اطلاعات، انجام می‌شود. نقاط آسیب پذیر در طول مرحله شناسایی و پیمایش، کشف و امتحان شده‌اند و آماده‌اند تا در یک اکسپلویت شبکه‌ای، منجر به سوء استفاده از سیستم مزبور شوند. روش اتصال هکر برای سوء استفاده از یک سیستم می‌تواند، اکسپلویت به یک شبکه محلی (مانند Lan، شبکه باسیم یا بی سیم) باشد و یا حتی دسترسی به یک رایانه شخصی از طریق اینترنت یا (Offline).

● نمونه حملات نیز می‌توانند شامل موارد زیر باشند:

الف - حمله سرریزی مبنی بر پشته [بافر]

ب - Dos

ج - (Hijacking) یا لایه دزدی

این مباحث نیز در سلسله مباحث بعدی، به تفصیل مورد تحلیل قرار خواهند گرفت. اشاره) مرحله حصول دستیابی، در دنیای هکرها مانند این است که به سیستم شخصی خود، دسترسی دارند و این یعنی همه چیز...

مرحله ۴: حفظ مسیر دسترسی

وقتی که یک هکر موفق به دستیابی به سیستم‌ها می‌شود، سعی می‌کند تا برای حملات و سوء استفاده‌های آینده، مسیر دسترسی را حفظ کند. بعضی اوقات، هکرها به سختی می‌توانند، مسیر دسترسی را حفظ کنند. چرا که کارمندان بخش‌های امنیتی، با اعمال تمهیدات بهینه امنیتی جدید، باعث زحمت نفوذگران می‌شوند. لذا، در این حالت هکرها به وسیله (بک دورها - Backdoors)، (روت کیت‌ها - Rootkits) و یا تروجان‌ها، برای رسیدن به اهداف‌شان تلاش وافی می‌کنند. در گونه‌ای از حملات، هنگامی که یک هکر، کنترل سیستمی را در دست می‌گیرد، می‌تواند آن را مبنایی برای حمله به سیستم‌های دیگر قرار دهد. بطوری که در (مپینگ)، سیستم مزبور به عنوان منبع حمله به سیستم‌های مذکور، شناسائی می‌شود. در این حالت به این سیستم، (Zombie) یا سیستم جادو شده اطلاق می‌گردد.

مرحله ۵: پوشاندن رد پا

هنگامی که هکرها، به یک سیستم دسترسی پیدا می‌کنند، سعی می‌کنند تا با پوشاندن رد پای حملات‌شان در سیستم‌ها، مانع از آشکار سازی تجاوزات‌شان، به وسیله کارمندان بخش‌های امنیتی شوند. چرا که ممکن است با کشف مدارک غیر قابل انکار، علیه آن‌ها اقدام قانونی صورت گیرد. لذا، نفوذگران سعی می‌کنند تا همه رد پاهای ناشی از حملات خود، مانند فایل‌های ثبت وقایع (Log File) و اخطارهای (آلارم‌های) سیستم‌های کشف نفوذ (IDS) را از بین ببرند.

• در زیر، مثال‌هایی از مرحله پوشاندن رد پا، ارائه شده است:

الف - پوشیده نویسی یا (Steganography)

ب - استفاده از پروتکل‌های تونلینگ (Tunneling protocols)

ج - پاکسازی فایل‌های ثبت وقایع (Log files)

استگانوگرافی و تونلینگ، روش‌هایی از حملات، توسط هکرها هستند، که در مقالات بعدی، به تفصیل، مورد تحلیل قرار خواهند گرفت.

د - هکتیویسم چیست؟

هکتیویسم به عمل هک کردن، به واسطه وجود یک علت خاص، اشاره دارد. هکرها به طور معمول، برای خود دارای یک دستور کار معین و یا خط مشی اجتماعی سیاسی هستند. هدف بیشتر آنان، فرستادن پیام‌هایی به افراد، سازمان‌ها و یا... است، البته تا زمانی که آن علت بخصوص، هنوز وجود داشته و مجموعه دلالی که بخاطر آن، دست به چنین حرکاتی می‌زنند، متوقف نشده باشد. بر اساس تحقیق مشاهده شده است که در بسیاری مواقع، هکرها با یکدیگر جهت اعمال حملاتی چون: الف) بدشکل کردن و دفورمه کردن سایت‌های وب (ب) خلق ویروس‌ها (ج) حملات Dos و طرح‌هایی برای ارایه حملات شکننده و سهمگین به سازمان‌ها، همکاری وافر و شبانه روزی داشته و به یکدیگر یاری می‌رسانند. البته، این همکاری تا زمانی است که بنا به نظر خودشان، آن دلیل ننگ آور مشترک، هنوز باقی مانده و به طور مثال، سازمان‌های مذکور، هیچ گونه عکس العملی نشان نداده باشند. پس می‌توان نتیجه گرفت که هکتیویسم، مراکز اصلی حکومت‌های ظالم را هدف قرار می‌دهد و یا حتی، دیگر گروه‌های سیاسی و یا اجتماعی موجود، بطوری که وابستگی خود را به یکی از موارد ذیل، حفظ کرده باشند:

الف - حکومت‌های ظالم و استبدادی

ب - افراد و اشخاص یا گروه‌هایی با اندیشه‌های غیر انسانی وابسته به دولت‌های ستمگر (البته این تعابیر، همگی، از ذهنیت هکرها بدخیم، ناشی می‌شود)

ه - طبقه بندی انواع متفاوت هکرها؛ هکرها می توانند به (۳) گروه تقسیم شوند

الف - هکرهاى کلاه سفید

ب - هکرهاى کلاه سیاه

ج - هکرهاى کلاه خاکستری

به طور کلی، هکرهاى اخلاق مدار، در گروه هکرهاى کلاه سفید دسته بندى می شوند. ولى گاهی، پس از رسیدن به درجه حرفه‌ای گری در آزمون‌های امنیتی و استفاده از مهارت‌های اخلاقی‌شان در جهت خدمت به امنیت سیستم‌ها، در دسته هکرهاى کلاه خاکستری، آن هم در حالى که حس انسانی آن‌ها، بر حس تهاجمی آن‌ها غالب است، قرار می گیرند.

الف - هکرهاى کلاه سفید

کلاه سفیدها یا هکرهاى اخلاق مدار، اشخاص خوب و اخلاق مداری هستند. آن‌ها همیشه، با رعایت اصول اخلاقی و قانونی و ضمن تبعیت همیشگی از آن، از دانش خود، در جهت مقاصد دفاعی، استفاده می کنند. هکرهاى کلاه سفید، همگی از حرفه‌ای‌های دانش هکینگ هستند و سعی می کنند، با توجه به دانش و ابزارکاری که دارند، ضعف سیستم‌ها را شناسائی کنند و اقدامات جبرانی را برای مبارزه با ضعف سیستم‌های مذکور، طراحی و پیاده سازی کنند.

ب - هکرهاى کلاه سیاه

کلاه سیاه‌ها، اشخاص بدی هستند. این دسته از هکرهاى بدخیم یا (کراکرها) افرادی هستند که از مهارت‌های‌شان برای مقاصد غیر قانونی استفاده کرده و از روی عناد، دست به اقدامات نفوذ گرانه علیه سیستم‌ها می زنند. آن‌ها با نهایت بد خواهی، بیشتر اوقات و از راه دور، وارد سیستم‌ها شده و به تمامیت اطلاعاتی آن‌ها تجاوز می کنند. دسترسی غیر مجاز و خراب کردن اطلاعات حیاتی و محروم ساختن استفاده کنندگان قانونی از سرویس‌های مشروع، همگی، تجاوزاتی هستند که هکرهاى کلاه سیاه، به هر حال، با ادعای وجود علت العللی، برای حرکات‌شان، انجام می دهند. پس به آسانی می توان فرق بین هکرهاى کلاه سفید و کلاه سیاه (کراکرها) را تشخیص داد؛ کافی است به اهداف متجاوزانه کلاه سیاه‌ها، توجه کرد.

ج - هکرهاى کلاه خاکستری

هکرهاى کلاه خاکستری، شامل، آن دسته می شوند که متکی به وضعیت روحی و موقعیت‌شان، گاهی حالت تهاجمی داشته و گاهی حالت تدافعی. پس این خود می تواند به مثابه خطی جداکننده، مابین هکرها و کراکرها باشد. هر دوی آن‌ها در عرصه اینترنت و اراده قوی جهت اعمال حملات سهمگین، در هر وضعیتی، از نیروهای قدرتمند و فعال، برخوردارند، ولى هر کدام، از صلاحیت منحصر بفردی، در عملکردشان، بهره می برند. چنین اشخاصی، نزد مردم، ممکن است، به صورت‌هایی، گروه بندى شوند. به هر حال، به هکرهاى اخلاق مدار، از این رو هکرهاى اخلاق می گردد: چرا که به هر جهت، از نقطه نظر حس کنجکاری، با هکرهاى بدخیم، مشترکند. آن‌ها، با توجه به آشنایی، که به روشهای برقراری امنیت دارند، به تعلیم قربانیانی می پردازند که قرار است، از این به بعد سیستم‌های‌شان، محفوظ بماند و در واقع به قربانیان‌شان، لطف و رحمت نشان می دهند. به عنوان مثال، اگر ضعیفی و یا حفره‌ای، در یک سرویس رایانه‌ای موجود در یک بانک، گزارش شود، هکرهاى اخلاق مدار، در واقع محبت کرده و آسیب مورد نظر را تصحیح می کنند. نکته، این که، به هر حال، مردم، هر گونه فعالیت‌های هکرمعابانه، اعم از اخلاق مدار یا بدخیم را، خلاف اخلاق می دانند. چرا که آنان، هکرها را اشخاصی می دانند که میل به ورود غیر قانونی به حریم افراد را دارند. مردم هیچ روش فکری خاصی، از جمله میانه روی در افکار را در خصوص تفاوت قایل شدن مابین هکرهاى اخلاق مدار و بدخیم، عملی نمی دانند؛ یعنی، نمی توانند با نگاهی معتدل، هکینگ اخلاقی را از نوع بدخیم خود، مستثنی کرده و اخلاق مداران را بی خطر ببینند. بر طبق نظریه‌ای، یکی از شکل‌های ادب هکری، ممکن است آن باشد که به سیستمی به زور و غیر قانونی نفوذ می کنند و سپس با اپراتور آن رایانه، تماس برقرار کرده و به ایشان توضیح می دهند که مکانیزم این نفوذ چگونه بوده و چگونه می تواند حفره مورد بحث را مسدود کنند. در واقع، هکر مذکور، به عنوان عضوی از یک گروه ببری (Tiger team) عمل نکرده و به هر شکل، ناخواسته، رفتاری انسانی دارد. (شاید با ارایه این رفتار، می خواهد به یک تیم امنیتی، خود را معرفی کند تا مراتب استخدامش را در سازمان مربوطه، فراهم سازند). بنا بر این توصیه می شود که این راه دستیابی را به نوعی، غیر قانونی، تلقی کنند. اطمینان حاصل کنید که قوانین را می شناسید؛ چرا که ممکن است تاوان سنگینی را بخاطر این فعالیت‌های هکینگ به ظاهر

اخلاق مدار سرگرم کننده، بردارید. بر اساس آمار موثق، گزارشاتی در دست است که نشان می دهد، هنگامی که هکر مر بوطه، به سازمان مورد نظر برای استخدام خود، مراجعه می کند، ناگهان خود را در دام پلیس و نیروهای امنیتی می بیند. بدین معنی که تفاوت قابل شدن بین هکرای اخلاق مدار و بدخیم، درصدی برابر و پنجاه، پنجاه، دارد. لذا اگر از این دسته از هکرها هستید، مواظب اعمال و رفتار غیر قانونی خود باشید.

• هکرای اخلاق مدار و کراکرها. آن ها چه کسانی هستند؟

خیلی ها می پرسند که آیا هک کردن، می تواند اخلاقی باشد یا نه؟ بله - جواب مثبت است. هکرای اخلاق مدار، به طور معمول، در علوم امنیتی رایانه، حرفه ای هستند و در واقع ایشان، امتحان کنندگانی هستند که شبکه ها را به منظور یافتن حفره های امنیتی، بررسی کرده و به نوعی کارشناس این دانش محسوب می شوند و از ابزارهای هکینگ، برای مقاصد دفاعی در مقابل تهاجمات بهره می جویند. پس می توان نتیجه گرفت که هر حرفه ای علم کامپیوتری، می تواند، مهارت های هکینگ اخلاقی را بیاموزد. ولی بر اساس آنچه در گذشته، شرحش گذشت، اصطلاح (کراکر)، افراد کاردانی را به ذهن، متبادر می سازد که با ابزار متفاوتی، چون پراکنده ساختن ویروس ها، حمله به سیستم ها و مختل ساختن شبکه ها و... با مقاصد مخرب یا تهاجمی، باعث سلب آسایش و آرامش محیط های کار، می شوند. مشاهده شده است که حتی گاهی، این اعمال را، فقط به منظور تفریح انجام می دهند. مثلاً با دزدیدن شماره کارت های اعتباری افراد و ضمن اطلاع دادن به ایشان، به باج گیری مشغول و به قول خودشان، تفریح می کنند. نکته) یکی دیگر از نام های کراکرها، هکرای بدخیم یا (Malicious hackers) می باشد.

• هکرای اخلاق مدار، چه می کنند؟

شکی نیست که شاید توانائی هکرای اخلاق مدار، با کراکرها برابر باشد ولی یقیناً، اهداف شان متفاوت است. چرا که آن ها، تلاش می کنند تا مزاحمت های ایجاد شده برای شبکه ها را شناسائی کرده و می توانند تشخیص دهند که سارق، با چه مدتی به اطلاعات دستبرد زده است. این فرآیند امنیتی - آزمایشی تست نفوذ پذیری یا آزمون آسیب شناسی سیستم (Penetration Testing)، نامیده می شود. هکرای بدخیم، در سیستم ها اشکال ایجاد کرده و باعث توقف کار آن ها می شوند. بر خلاف افسانه ای که مردمان، از هکرها، در ذهن خود ساخته اند که آن ها را اشخاصی می دانند که به راحتی، با نوشتن یک دستور، سیستم ها را نابود می کنند؛ هکرها، گاهی با پایداری و با داشتن اندیشه های مرموزانه، ضمن تکرار سرسختانه فرآیندهای طولانی و آزمون حفره های متداول امنیتی در سیستم ها، موفق به دسترسی و در نهایت امر، سرقت اطلاعات می شوند. بنابراین، کراکرها، به نوعی، هکرای نوع متوسط محسوب می شوند، در بسیاری از مواقع، این هکرای اخلاق مدار هستند که موفق به شناسائی هکرای بدخیم شاغل در تیم امنیتی یک سازمان می شوند. بدین معنی که لااقل، اگر اشخاصی یا سازمانی با ایشان تماس برقرار کرده و از آنان بخواهند تا در مورد نوعی حملات، به ایشان مشاوره بدهند، هکرای اخلاق مدار از آن ها سؤال خواهد کرد که:

• چه کسانی یا سازمان هایی از حمله مذکور سود می برند؟

و این گونه است که به لحاظ امنیتی، می توانند به کشف سر نخ های جرم مذکور، نایل شوند.

• اهداف نفوذ گران، تلاش در دستیابی:

اصول و بنیاد امنیت، بر چهار رکن، استوار است:

الف - سری بودن (قابلیت اعتماد) - (Confidentiality)

ب - سندیت (صحت) - (Authenticity)

ج - درستی (تمامیت) - (Integrity)

د - قابلیت دسترسی (دسترس پذیری) - (Availability)

هدف یک سارق اطلاعات، بهره برداری از ضعف امنیت شبکه ها، در یکی یا تمامی ارکان ذکر شده، می باشد و در ابتدا، تلاش می کند، تا اطلاعات جامعی، از این نقایص، جمع آوری کند. مثلاً، در حمله از انواع Dos، یک هکر، در واقع به رکن قابلیت دسترسی سیستم ها و یا شبکه ها، دست درازی می کند. اگر چه حملات از نوع Dos، انواع مختلفی دارند؛ ولی در حالت کلی، مقصود اصلی، استفاده از منابع سیستم ها و همچنین، پهنای باند مصرفی شبکه های مذکور است. گاهی با فرستادن پیام های با

تعداد بالا به سیستم مورد نظر، باعث می شود تا رایانه مزبور خاموش (Shut down) شود، بدینوسیله باعث محروم کردن کاربران، از سرویس های قانونی خود، می شوند. اگرچه، تمرکز این حمله، بر روی رسانه های استفاده شده در شبکه های مذکور می باشد ولی در حقیقت، این دسته از حملات، قربانیان فراوانی دارند. لذا هدف نهایی متخصصان امنیتی باید آن باشد که این مزاحمت های سیستمی را کنترل کنند. اطلاعات دزدیده شده، مانند سرقت کلمات عبور و انواع داده ها، که به ظاهر در یک محیط امن، در یک شبکه ای مطمئن نگهداری می شوند؛ نیز حمله به عامل سری بودن و قابلیت اعتماد (Confidentiality) در تبادل اطلاعات است. چراکه به هر صورت، با وجود این اطلاعات، هر شخصی قادر به دسترسی به داده های مذکور بوده و به سوء استفاده های خود، ادامه خواهد داد. البته، لازم بذکر است که این دزدی، فقط به داده های روی سرورهای شبکه ها محدود نمی شود. لپ تاپ ها، دیسک ها، نوارهای پشتیبان داده ها، همگی در معرض تهدید، قرار دارند. وسایل مذکور، در هر زمانی که باشند، ممکن است، پر از داده های محرمانه باشند. یک هکر، به راحتی با تحلیل داده های درون این وسایل، می تواند به اطلاعاتی، پیرامون میزان قدرت امنیتی سازمان مورد بحث، دست یابد. حملات (Bit - Flipping) بر روی عامل درستی یا تمامیت داده ها (Integrity)، متمرکزند. چراکه می دانید، داده ها در مسیرهای انتقال در حال عبور هستند؛ پس به راحتی می توان آن ها را دستکاری کرد. (بدین معنی که ممکن است، در راه رسیدن به ما، داده ها، دستکاری شده باشند) و این بدان مفهوم است که مدیران سیستم ها نمی توانند، صحت درستی داده ها و همچنین، فرستنده واقعی داده مذکور را شناسایی و تایید کنند. حمله (Bit - flipping) در واقع، حمله به پوشیدگی یا رمزمداری داده ها است. به عنوان مثال، هنگام ارسال داده از (A) به (B)، داده مورد نظر، رمز گذاری شده و به دست (B) گسیل می شود. اگر در میان مسیر، رمز داده مذکور، کشف شده و هکر بتواند، تغییری را در آن اعمال کرده و به سمت (B) بفرستد، صحت و درستی داده، زیر سؤال رفته است. تازه این حمله، زمانی می تواند به یک فاجعه تبدیل شود که هکر بتواند فرمت پیام مورد بحث را شناسایی کند. بدین مفهوم که هکر مذکور، می تواند برای همیشه و از یک کانال به خصوصی، حملاتی را بر ضد پیام های ارسالی، انجام دهد. وقتی که حمله (Bit - flipping)، بر روی یک امضای دیجیتال، اعمال شود، حمله کننده، ممکن است بتواند، متن پیام را این گونه تغییر دهد؛ یعنی شما، هنگامی که باید به شکل دیجیتالی، سند بدهکاری (۱۰) دلاری خود را به یک سازمان، تأیید کنید، هکر مذکور عدد (۱۰) را به (۱۰۰۰۰۰) دلار تغییر داده و شما در یک چشم به هم زدن، با دست خود، در کسری از ثانیه، بدهکار سازمان مذکور، خواهید شد؛ آن هم به مقدار عددی جعلی جدید. حمله (Mac address spoofing) با مفهوم کلاهبرداری و سوء استفاده از آدرس (MAC)، نیز یکی از انواع حملات به عامل سندیت (Authentication) می باشد، به یک وسیله غیر مجاز اجازه اتصال به یک شبکه را می دهد؛ بطور مثال، اتصال به یک شبکه بی سیم (Wireless)، (Spoof) کردن آدرس های (MAC) به هکر، امکان شناسایی ایستگاه های فرستنده را دیوبی داده ها را می دهد. سپس وی با جابجایی کردن فرکانس دریافتی و با استفاده از ابزاری خاص، نسبت به شناخت نقاط ضعف شبکه مذکور، اقدام کرده و پس از دسترسی به آن، به راحتی، از امکانات آن شبکه استفاده خواهد کرد.

● مثلث امنیت، عملکرد، کاربری آسان.

در مباحث حرفه ای امنیتی، مشکلی وجود دارد و آن به ارتباط بین اجزای مثلثی که راس های آن عبارتند از: امنیت (Security)، عملکرد (Functionality)، کاربری آسان و ساده (Ease of use) بر می گردد. چراکه برقراری تعادل میان پیاده سازی امنیت برای جلوگیری از حملات و ایجاد کاربری آسان برای استفاده کاربران، امری سخت و گاهی اوقات غیر قابل اجرا است. بطور کلی مثلث امنیت، عملکرد، کاربری آسان؛ بیان کننده نوعی ذهنیت است. بدین مفهوم که، با بالا رفتن ضریب برقراری امنیت در سیستم ها، از ضریب عملکرد و کاربری آسان برای کاربران، کاسته می شود.

در یک دنیای ایده آل، حرفه ای های امنیت میل دارند که سیستم ها و مکان های تحت نظارت شان، از بالاترین سطح امنیتی برخوردار باشند و این در حالی است که افرادی هستند که امنیت مذکور را نوعی مشکل، برای عملکرد سیستم های شان می پندارند. برای مثال فرض کنید که برای وارد شدن به بخش فیزیکی شرکت خودتان، ابتدا باید از یک نقطه بازبینی اولیه که بخش نگهبانان است گذشته و بعد از گرفتن کارتی که شماره سریالی، جهت سوار شدن به آسانسور، روی آن حک است، به بخش کاری خود، رسیده اید که تازه باید، پس از تحویل کارت مزبور به مسئول آن، به اخذ کلید درب دفتر خود، نایل شوید. بعد از ورود به دفتر کارتان و نشستن پشت میز کار، تازه متوجه می شوید که کلید درب کمد های میز کارتان را در ماشین خود، جا گذاشته اید و باید تمامی این مراحل شناسایی را پشت سر گذاشته و به دفتر خود، بازگردید. البته خوب می دانید که ۵ دقیقه دیگر نیز، یک جلسه مهم کاری دارید که تاخیر در حضورتان، باعث برهم خوردن یک قرارداد مالی - کاری مهم خواهد شد، حال اسنادی که باید در جلسه ارائه دهید، نیز در میز کار محبوس است. در این وادی، اگر دیگری جای شما باشد، آیا امنیت را عذاب آور نمی پندارد؟

و - تعریف مهارت لازم برای یک هکر اخلاق مدار شدن

هکرهای اخلاق مدار، باید نسبت به هکرهای بد خیم، همیشه در موارد زیر، یک پله، جلوتر باشند:

الف - برنامه نویسی کامپیوتر

ب - شبکه

ج - سیستم عامل

همچنین شناخت کامل و عمیق، پیرامون هدف های نفوذگران در پلاتفرم های ویندوز، یونیکس و لینوکس، لازم و ضروری بنظر می رسد. حوصله، پایداری و پشتکار، خواص و خصایل مهم اخلاقی هکرهای اخلاق مدار در تمامی طول مدت کاری شان محسوب شده؛ به طوری که بتوانند روی سطوح مختلف حملات متمرکز شده و در نتیجه گیری ها، دقیق و راسخ، عمل کنند. در تحقیقی، اشاره شده است که بسیاری از هکرهای اخلاق مدار، از دانش بالائی، در مباحث امنیت رایانه ای، برخوردار می باشند؛ ولی نسبت به هکرهای بد خیم، فاقد آگاهی لازم، در خصوص مکانیزم حملات و راه های مقابله با آن، می باشند. در گزارشات فنی بعدی، صراحتاً به تحلیل مقولات مذکور می پردازیم و ضمن آموزش آگاهی های لازم، به بررسی راه های مقابله با این حملات، خواهیم پرداخت.

ز - تحقیق پیرامون آسیب پذیری سیستم ها یعنی چه ؟

تحقیق پیرامون بررسی و کشف نقاط آسیب پذیر سیستم ها (Vulnerability Research)، فرآیندی است که نقاط ضعف سیستم ها را آشکار می سازد که می توانند، منجر به یک حمله، به روی یک سیستم شوند. سایت های وب و ابزار بسیاری وجود دارند که به هکرهای اخلاقی مدار، در کشف این حفره ها کمک کرده و به وسیله آن ها، جلوی سوء استفاده از سیستم های تحت نظارت خود را می گیرند.

ذکر این مطلب ضروری بنظر می رسد که مدیران سیستم ها، باید نکات زیر را رعایت کنند:

الف - ضمن استفاده از آنتی ویروس ها، همیشه آن ها را به روز نگه دارند.

ب - از ابزارهای به روز در شناسائی تروجان ها و سایر سوء استفاده کننده هایی که در سیستم ها و شبکه های تحت نظارت وجود دارند، استفاده کنند.

ج - همچنین ضمن پدیدار شدن انواع جدیدی از حملات و تهدیدها، بتوانند با تحقیق، راه شناسائی این حملات را کشف کرده و بیاموزند که چگونه از حملات مشابه، ممانعت بعمل آورده و بتوانند حملات مذکور را در پوشش عملیاتی خود کنترل کنند.

ح - فرآیند رهبری - اجرایی در یک اخلاق مدارانه

هکینگ اخلاقی، به طور معمول در چهار چوب یک نظام ساختار یافته عملی و سازمان یافته اندیشه ای بوده و عملکرد در آن، مانند بخش های بازرسی امنیتی - حراستی و آزمایشگاه های نفوذ می باشد. معمول، عمل آزمایش نفوذ به طور عمیق، بر روی سیستم ها و نرم افزارهای مورد نیاز سرویس گیرنده، انجام می پذیرد.

رعایت مراحل زیر چهار چوبی است برای متکامل کردن بازرسی امنیتی یک سازمان:

الف - با سرویس گیرنده صحبت کنید و از کلیه مواردی که در طول آزمایش، مورد بررسی قرار می دهید، وی را مطلع سازید.

ب - با سرویس گیرنده تان موافقت نامه عدم افشاء را همراه با رد و بدل کردن مدارک لازم، امضاء کنید؛ (NDA = Non-disclosure agreement)

ج - یک تیم از هکرهای اخلاق مدار آماده کرده و برنامه ای مشخص را جهت انجام آزمون، آماده کنید.

د - آزمون را رهبری کرده و اجرا کنید.

ه - نتایج حاصل از آزمایش را تجزیه و تحلیل کرده و از آن ها گزارش کاملی، تهیه کنید.

و - در نهایت، گزارش مذکور را به طور رسمی، به سرویس گیرنده خود تحویل دهید.

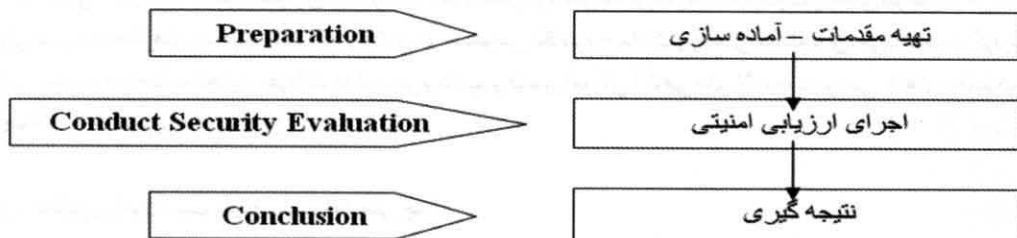
نکته

روش های عمیق آزمون نفوذ و اطلاعات بازرسی امنیتی، در گواهی نامه (LPT) = Licensed Penetration Tester شرکت (EC - Council) مورد بررسی و تحلیل، قرار گرفته است.

• خلق یک طرح ارزیابی امنیتی:

بسیاری از هکرهای اخلاق مدار، در نقش یک حرفه ای مباحث امنیتی، با استفاده از مهارت های شان، به ارزیابی امنیتی یا برگزاری آزمون نفوذ، می پردازند. این آزمون ها و ارزیابی ها، در نهایت، دارای ۳ فاز عملیاتی هستند که به قرار زیر ارایه می گردد:

در واقع، مرحله آماده سازی، شامل عقد یک موافقت نامه مابین هکر اخلاقی و سازمان مربوطه می باشد. این موافقت نامه باید شامل اخذ اختیارات تام در خصوص موارد زیر باشد:



- ۱- اجازه انجام کامل انواع آزمون ها در سازمان
- ۲- اجازه بررسی کامل در خصوص بررسی انواع حملات انجام شده که شامل حملات (داخلی یا خارجی) می شود.
- ۳- اجازه برگزاری آزمون در انواع مختلف که شامل موارد زیر اند:

- الف - آزمون باکس سفید
- ب- آزمون باکس سیاه
- ج- آزمون باکس خاکستری

(در سطور بعدی، در قسمت (انواع آزمون ها)، به تعریف کامل این باکس ها، می پردازیم) در مرحله اجرای ارزیابی موارد امنیتی، آزمایشات انجام شده و بعد از تجزیه و تحلیل داده ها و اخذ نتایج لازم، گزارشی رسمی از نقاط آسیب پذیر و دیگر یافته ها، تهیه می گردد و در مرحله آخر، گزارش مزبور، همراه با پیشنهاداتی برای بهبودی موارد امنیتی، به سازمان مورد بحث، تقدیم می گردد.

• انواع هک اخلاقی:

هکرهای اخلاق مدار، روش های متفاوتی را در طول شبیه سازی حملات مختلف در یک سازمان، همراه با آزمون های نفوذ، به جهت کشف نقائص امنیتی، بکار می گیرند.

متداول ترین این روش ها، عبارتند از:

۱- شبیه سازی شبکه راه دور (Remote network):

هکر اخلاق مدار، با شبیه سازی یک حمله از طریق اینترنت، سعی در هم شکستن نقاط آسیب پذیر شبکه مذکور کرده و تلاش وافی می کند تا عمل مستحکم سازی این شبکه در مقابل حملات بیرونی، بدرستی انجام شده که عبارتند از:

- الف- نصب فایروال (دیوار آتش)
- ب - استفاده از پروکسی
- ج - استفاده از گزارش دهنده های اتوماتیک حملات

۲- شبکه شماره گیری از راه دور (Remote Dial - up Network)

در شبیه سازی حمله از نوع فوق، هکر اخلاق مدار، به بررسی حملاتی که پیرامون مودم (Modem) کلانیت، انجام می پذیرد، می پردازد. (War dialing) یا فرآیند جنگ شماره گیری، در واقع، تلاشی است در جهت یافتن نقاط باز سیستم که خود نمونه ای از این روش محسوب می شود.

۳- شبیه سازی شبکه محلی (Local network)

با این نوع شبیه سازی، هکر اخلاقی، سعی دارد تا مفاهیمی اعم از احتمال سرقت اطلاعات و سوء استفاده های امنیتی، در محیط های داخلی سازمان، توسط افرادی که به هر حال به عنوان کاربر، مجوزهایی جهت استفاده از منابع داده ها را دارند، را بررسی کند و بدین وسیله پیشنهاداتی را جهت توقف این فرآیند، ارایه می کند.

۴- بهره کشی اطلاعاتی از لوازم مسروقه: (Stolen Equipment)

بهره کشی اطلاعاتی از لوازم معیوب یا مسروقه سازمان ها، یکی دیگر از روش های اخذ و سرقت داده ها، توسط هکرها بدخیم است. به طور مثال اگر لپ تاپ کارمندی، از رده های مهم سازمانی، که ممکن است در آن داده های طبقه بندی شده و مهم وجود داشته باشد، دزدیده شود، (اطلاعاتی نظیر کلمات عبور کاربران شبکه، و...)، هکر مذکور با تحلیل این داده ها، به بالاترین سطح از نظر آسیب رسانی به سازمان مورد نظر، قرار خواهد گرفت.

۵- مهندسی اجتماعی (Social Engineering)

در مهندسی اجتماعی، هکر بدخیم، برای مثال، توسط تلفن، ضمن برقراری ارتباط با کارمندان، به جمع آوری اطلاعاتی می پردازد که برای ارتباط رو در روی خود، در آینده بدان نیازمند است. مهندسی اجتماعی بطور معمول، برای کسب اطلاعاتی در مورد کلمات عبور و نام های کاربران، اطلاعات مربوط به تنظیمات و میزان قدرت امنیتی در سازمان ها، کاربرد فراوان دارد.

۶- ورود فیزیکی (Physical entry)

یک حمله از نوع ورود فیزیکی، در دوی بخش مورد تحلیل قرار می گیرد.

الف - حمله از نوع ورود غیر مجاز افراد به سازمان ها که ممکن است باعث خسارات جبران ناپذیری شود.
ب - حمله از نوع وارد ساختن کدهای مخرب در سیستم های داخلی سازمان ها، مانند بهره برداری از ویروس ها، تروجان ها، روت کیت ها (Rootkits) و جاسوس های سخت افزاری (Key loggers) که به ضبط رکوردهای کاری در سخت افزار، مانند کی بورد و... می پردازد.

انواع آزمون ها:

یک آزمایش نمایش امنیتی و یا یک آزمون نفوذ، در واقع شبیه سازی انواعی از حملات است که توسط هکرها بدخیم انجام می شود، که به صورت آزمایشی، روی سیستم ها، اجرا می شود. با توجه به متفاوت بودن نوع حملات، هکرها اخلاق مدار، در سطوح مختلفی، این موارد را شبیه سازی کرده و گزارشات خود را تهیه می کنند، که عبارتند از:

الف - آزمون جعبه سیاه:

آزمون جعبه سیاه، در واقع، یک ارزیابی امنیتی، بدون هیچ گونه شناخت قبلی از زیر ساخت های شبکه ای را شامل می شود. بدین معنی که هکر اخلاقی، به شبیه سازی آزمایشی حمله یک هکر بدخیم، که سعی دارد از خارج سازمان، به شبکه سازمانی، نفوذ کند، می پردازد.

ب - آزمون جعبه سفید

در این آزمون، هکر اخلاقی به ارزیابی امنیتی شبکه مذکور، این بار، با شناخت و دسترسی کامل، می پردازد. مانند یک مدیر ارشد سیستم یا (Network Administrator)

ج- آزمون جمعه خاکستری

در این نوع آزمون، به ارزیابی امنیتی شبکه مذکور، با توجه به مجوزهای کاربران داخلی سازمان پرداخته می‌شود.

• گزارش هک اخلاقی

نتیجه برگزاری یک آزمون نفوذ در شبکه و یا بازرسی های امنیتی و گزارش فنی یک هکر اخلاق مدار را شامل می‌شود. در این گزارش فنی، نتایج حاصل از انجام آزمایشات و روش های به کار گرفته شده در آن را مشاهده می‌کنیم. این نتایج برگرفته از رعایت همان نکاتی است که در بخش ارزیابی امنیتی، مورد تحلیل قرار گرفت. به طوری که ممکن است، هر آسیمی بند مفصل و اقدامات جبرانی زیادی را به خود اختصاص دهد. بخشی از این گزارش، به طور معمول بصورت و فرمت خاصی از نظر امنیتی، به سازمان ارایه شده و جزئیات مفصل این اطلاعات، محرمانه بوده و باید در مکان خاصی، نگهداری شوند. چراکه ممکن است، امنیت داده‌ای سازمان مورد بحث را به مخاطره اندازد؛ اگر که به دست افراد نابکار بیافتد. آری، اتفاق مصیبت آمیزی به وقوع خواهد پیوست.

ط- درک مفاهیم قانونی هک کردن

یک هکر اخلاق مدار، باید جریمه های قانونی مربوط به سرقت های اطلاعات غیر مجاز را بشناسد. هر گونه انجام آزمون های نفوذ و بازرسی های امنیتی سیستم های شبکه‌ای، غیر قانونی بوده مگر این که ضمن عقد قرارداد رسمی و قانونی با سازمان مورد نظر، به شکل قانون مدار، عمل شود. هک های اخلاق مدار، باید عاقل بوده و ضمن کار دان بودن، از پیامدهای قانونی ناشی از کاربرد بدخیم مهارت های شان، آگاه باشند.

• جرائم رایانه‌ای، بطور وسیع و کلی به دو دسته تقسیم می‌شوند

الف- جرائمی که وسیله ارتکاب آن، رایانه است

ب- جرائمی که هدف و محل وقوع جرم، خود رایانه می‌باشد

در ادامه، دو بخش از مهم ترین قوانین جزائی کشور آمریکا، در خصوص جرایم رایانه، ارایه شده است، اگر چه دامنه امتحانات (CEH) جهانی است، ولی آشنایی شما را با دو قانون، که در خصوص مجازات تعیین شده برای سرقت های اطلاعات، تبیین شده اند را لازم و ضروری می‌داند. بخاطر داشته باشید که نه فقط هک های بدخیم، بلکه هک های اخلاق مدار نیز، اگر که قوانین مذکور را رعایت نکنند، مورد تعقیب قانونی قرار خواهند گرفت. بر اساس قانون حاکم بر جرایم سایبر مصوبه ۲۰۰۲، هکرها را به اشد مجازات محکوم کرده است. چراکه قانون، ایشان را افرادی می‌داند که با بی اعتنایی، وارد زندگی اشخاص می‌شوند و امنیت زندگی آن ها را به خطر می‌اندازند. آن ها از نظر قانون، تهدیدات مهمی برای شبکه های رایانه‌ای، سیستم های انتقال دهنده داده، سرویس های عمومی و... به شمار می‌آیند.

ی- درک قوانین هجده گانه فدرال آمریکا

بر اساس این قوانین، ۱۸ مورد، عنوان جرم به خود گرفته و آئین دادرسی کیفری در این خصوص وجود دارد. در قسمت شماره (۱۰۲۹)، کلاهبرداری به وسیله رایانه و اعمالی که در ارتباط با وسائل دسترسی به داده ها باشد، ایجاد موقعیت سوء استفاده، فروش و وسائل ایجاد کننده دسترسی، استفاده از ارتباطات از راه دور به صورت جعلی و... استعمال غیر قانونی کلمات عبور کامپیوتری و وسائل دسترسی به سوء استفاده از کارت های اعتباری و... از این دست جرایم محسوب می‌شوند.

در بخش شماره (۱۰۳۰)، به کلاهبرداری و حرکتی که به طور مستقیم، در ارتباط با رایانه ها، انجام می‌شود، اشاره دارد. ورود غیر مجاز به رایانه های حفاظت شده، پخش کدهای مخرب و ویروس در شبکه ها و... خود از نمونه های نقض قانون، توسط این مجرمان، به شمار می‌آید.

نکته:

متن کامل قوانین فوق الذکر، برای مزید اطلاع، به عنوان ضمیمه، در آخرین قسمت از این سلسله مقالات، ارایه خواهد شد.

۱- درک درست و عمیق از اصطلاح هکر، داشته باشید.

در مورد آشنایی با مفهوم هکر، اطمینان حاصل کنید و با تعاریف اصطلاحاتی چون تهدیدات (Threat)، بهره‌کشی یا سوء استفاده کردن‌ها (Exploit)، آسیب پذیری (Valnerability) و همچنین با ارزیابی هدف‌ها و حملات، آشنا باشید.

۲- تفاوت بین هک‌های اخلاق مدار و کراکرها را بدانید.

هک‌های اخلاقی، حرفه‌ای‌های امنیت هستند که به شکل قانون مدار، از سیستم‌ها، در برابر هجوم هک‌های بد خیم، مدافعت می‌کنند. ولی کراکرها، هک‌های بد خیمی هستند که کارشان، وارد ساختن زیان، به سیستم‌های مورد نظرشان و در نهایت نقض قانون است.

۳- کلاس‌ها و انواع هکرها را بشناسید.

این مطلب، بسیار مهم است که تفاوت عمیق هک‌های کلاه سیاه، کلاه سفید و کلاه خاکستری را بشناسید، همچنین بدانید که کدامیک از آنان در دنیای هکرها، خوب و کدامیک بد هستند.

۴- از مراحل هک کردن، شناخت حاصل کنید.

از درک مراحل پنج گانه هک کردن که شامل؛ شناسایی حملات فعال و غیرفعال، اسکن کردن، دسترسی به جهت سواستفاده، حفظ مسیر دسترسی و پوشاندن ردپاها بعد از نفوذ می‌باشند، اطمینان حاصل کرده و بدانید که در هر مرحله، چه عملکردی در جریان است.

۵- از انواع حملات، آگاهی داشته باشید.

تفاوت میان حملات فعال و غیرفعال، داخلی و خارجی را بدانید و مقطعی راکه حملات در آن اتفاق می‌افتند را بررسی کنید.

۶- از انواع هک اخلاقی، شناخت حاصل کنید.

هکرها، می‌توانند به روش‌های مختلفی، به شبکه‌ها، حمله کنند. مانند: حمله شبکه از راه دور، حمله توسط شماره گیر از راه دور، حمله از طریق شبکه محلی، حمله به وسیله استفاده از تکنیک‌های مهندسی اجتماعی، حمله به وسیله سواستفاده از بازآوری داده‌های درون وسایل مسروقه و یا از طریق دسترسی فیزیکی.

۷- آگاهی از انواع آزمون‌های امنیتی الزامیست.

هک‌های اخلاق مدار، به وسیله تکنیک‌های مختلفی به آزمایش شبکه‌ها، برای بررسی نقاط ضعف‌شان می‌پردازند که شامل مراحل چو؛ آزمون‌های جعبه سیاه، جعبه سفید و جعبه خاکستری می‌باشند.

۸- آشنایی با مضامین و مکانیزم گزارش‌های ارایه شده، توسط هک‌های اخلاقی، الزامیست.

بدین مفهوم که گزارش مزبور، شامل شناسایی نوع هکینگ اطلاعات در شبکه مذکور، شناسایی نقاط آسیب پذیر سیستم و یا شبکه

مورد نظر و همچنین ارایه راه‌های مقابله با تهدیدات و آسیب‌ها، می‌باشد.

۹- شناخت مباحث قانونی درگیر در مفاهیم هکینگ، بایسته است. بدین معنی که آگاهی داشتن از مضامین قانونی، در خصوص جرایم امنیتی سایر، الزامیست.

۱۰- آگاه بودن از قوانین و مجازات قابل اعمال، در خصوص تجاوز و نقوذ به کامپیوتر و حریم افراد، الزامیست. بدین مفهوم که همگان باید از حداقل، (۱۸) مورد، اعمالی که در قانون، جرم محسوب شده و برای آن حدودا جرایمی و قضایی مشخص شده است، آگاه باشند.

منابع:

- 1-Official Certified Ethical Hacker Review Guide / Kimberly Graves - 2007
- 2-Computer Hacking Forensics Investigators / CHFI - 2007
- " Dave Kleiman
- " Kevin Cardwell
- " Timothy Clinton
- " Michael Cross
- " Michael Gregg
- " Jesse Varsalone
- " Craig Wright

دبیرخانه

بایگانی

سیستم مکانیزه ثبت نامه،
آرشیو پرونده، اسناد، عکس،
صدا، فیلم، کتاب، مجله، سی دی، نوار و ...
دارای تقویم شمسی و امکانات فارسی
برای ویندوزهای ۹۰۰۰، XP و ۷۰۰۰

ثبت نامه های وارده و صادره - وارده از صادره و صادره از وارده
امکان تفکیک نامه های پستی - فکسی - دستی و پست الکترونیکی
ورود اطلاعات نامه ها در کمترین زمان و بدون نیاز به استفاده از ماوس
جستجوی سریع در میان نامه های ثبت شده به دو صورت ساده و کامل
گزارش گیری متنوع از مطالب ثبت شده
امکان گروه بندی نامه ها و شماره سریال مختص به هر گروه
امکان ثبت رونوشت نامه ها به هر تعداد
ثبت ارجاعات نامه ها به تعداد دلخواه با ساعت و تاریخ ارجاع همراه با ثبت
الخدمات انجام شده
دارای کار تابل خاص برای هر کاربر (در نسخه شبکه)
امکان ثبت نامه توسط دو یا چند کاربر به طور همزمان (در نسخه شبکه)
دارای امکان اسکن نامه ها با هر تعداد صفحه و بدون نیاز به اختصاص نام
به فایل های اسکن شده
دسترسی به برنامه word جهت تایپ نامه ها بدون نیاز به اختصاص نام
به فایل های ایجاد شده
ارسال یک نامه به دسته ای از مخاطبین همراه با سابقه ارسال
چاپ فرم ادغام پستی با درج تاریخ، شماره ثبت، پیوست، فرستنده، گیرنده
و عنوان نامه به صورت خودکار
چاپ آدرس و مشخصات مخاطبین بر روی پاکت از روی فرم ادغام پستی
ایجاد پرونده به تعداد نامحدود و ارتباط خودکار با قسمت های مختلف برنامه
دارای دفتر تلفن گسترده همراه با جستجوی آسان
نمایش محتویات پرونده و دسته بندی موضوعات و اختصاص شماره برگه
به هر کدام
استفاده گسترده از صفحه کلید و بدون نیاز از ماوس
ثبت و دسته بندی موضوعات مختلف شامل مخاطبین، پرونده های
کامپیوتری، کتاب، مجله، نوار و
دسترسی به سیستم در سطوح مختلف امنیتی (مدیر، کاربر و گزارشگر و)
دارای سیستم پشتیبان گیری دستی و خودکار بر روی هارد یا کارت های حافظه
محیط کاملاً فارسی و دارای نمایش راهنمای استفاده از بخش ها
امکان نصب بر روی ویندوزهای ۲۰۰۰ - ایکس پی و ۲۰۰۳
و امکانات ویژه دیگر

تهیه شده جهت سازمانها،
ادارات دولتی، شرکتها، موسسات خصوصی

www.sinapardazeshsoft.com

نرم افزار سیناپاردازش

۱۵۸۷۵/۹۶۶۳: صندوق پستی
واحد پشتیبانی: ۸۸۴۲۳۵۷۲ (خط ۵)
دفتر فروش: ۸۸۴۳۹۰۲۶ (خط ۵)
روابط عمومی: ۸۸۴۵۲۷۳۵
فکس: ۸۸۴۳۵۷۰۶
info@sinapardazeshsoft.com

تیم پشتیبانی فعال از تهران
تهران و کشورهای فارسی زبان