Hacking And Penetration Testing

www.itssc.ir

@itssc

itssc_society

هک چیست ؟

در دنیای واقعی اگر فردی به سرقت بانک برود و یا بدون اجازه وارد خانه ی شما بشود در واقع شما را هک کرده است.
اما از لغت هک در حوزه ی کامپیوتر استفاده کرده و مختص آن قرار داده شده.
بصورت کلی به ورودی غیر مجاز هک گویند.

هکر کیست؟

هکر ها مثل شخصیت های داستانی هم می توانند شخصیت منفوری داشته باشند و هم می توانند قهرمان یک داستان باشند .

انواع هکر ها:

هکر کلاه سفید: به هکری گفته می‌شود که به منظور پیدا کردن مشکلات موجود در سرورها و نرم افزارها به آن‌ها نفوذ می‌کند و پس از گزارش مشکل به مسئولین در رفع عیب آن عیب سهیم است. هکرهای کلاه سفید برخی اوقات در مسابقاتی شرکت می‌کنند که شرکت‌های امنیتی برگذار می‌کنند.

مثلا شرکت گوگل و تلگرام برای گزارش باگ به کاربران هدایای نقدی می‌دهند. هکرهای کلاه سفید می‌توانند از این طریق جوایز ده‌ها هزار دلاری و یا حتی چند صد دلاری برنده شوند.
برخی مدیران سایت‌ها و سرورها نیز به گروه‌های هک کلاه سفید مبالغی می‌دهند تا سعی کنند آن سیستم را هک کنند و عیب‌های موجود را گزارش دهند.

هکر کلاه سیاه: به هکری گفته می‌شود که به منظور اخاذی و یا تخریب وارد سیستم‌ها و سایت‌ها می‌شوند. هکرهای کلاه سیاه در همه جای دنیا تحت تعقیب هستند و اعمال آن ها خلاف قانون تلقی می‌شوند.

هکر کلاه خاکستری:به هکری گفته می‌شود که گاهی اعمال هکرهای کلاه سیاه و گاهی اعمال هکرهای کلاه سفید را انجام می‌دهد.

هکر کلاه صورتی: به افراد آماتوری گفته می‌شود که برای ارضای حس کنکجاوی خود دست به اعمالی می‌زنند که یا سایت‌ها را تخریب کنند و یا به اطلاعاتی دست پیدا کنند که حق دسترسی به آن‌ها را ندارند.

برای ورود به دنیای هکر ها باید با اصطلاحات رایج این زمینه آشنا شوید که به توضیح مختصری از آنها می پردازیم:

واکر:به نفوذگر کلاه سیاهی گفته می‌شود که به منظور سرقت اطلاعات وارد سیستم‌های دیگر می‌شود. مثلا یک واکر بر اساس سفارشی که می‌گیرد وارد سامانه ثبت احوال شده و اطلاعات محل سکونت یک شخص را در اختیار خلاف کاران می‌گذارد.

پریکـر: در دهه‌هـای پیـش پریکرهـا بیشـترین جـولان را می‌دادنـد. پریکرهـا بـه شـبکه‌های تلفـن نفـوذ می‌کننـد و مکالمه‌هـا را اسـتراق می‌کننـد. ایـن پریکرهـا ممکـن اسـت عملیاتـی را بـرای سـازمان‌های مخفـی و خلافـکار اجـرا کننـد، بنابرایـن پریکـر بـودن یـک جـرم اسـت و پریکرهـا در تمـام نظام‌هـای حقوقـی جهـان محاکمـه و مجـازات می‌شـوند.

البتـه برخـی از پریکرهـا نیـز تنهـا بـرای خـود کار می‌کننـد و از دانـش خـود بـرای تمـاس مجانـی اسـتفاده می‌کننـد!

مهندسی اجتماعی

خیلـی از افـراد فکـر می‌کننـد عملیـات هـک تنهـا بـا دانـش فنـی و تخصـص انجـام می‌پذیـرد در صورتـی کـه اصـلا اینگونـه نیسـت. بسـیاری از عملیـات هـای هـک بـزرگ بـا کمـک مهندسـی اجتماعـی کـه کمک گرفـتن از قربانـی اسـت انجـام می‌پذیـرد. سـناریو زیـر را بـا دقـت بخوانیـد:

یـک هکـر می‌خواهـد وارد یـک شـبکه کامپیوتـری شـود ولـی نمی‌توانـد ضعفـی در ورود بـه شـبکه پیـدا کنـد. یـک خانـم را مامـور می‌کنـد بـا یکـی از کارمنـدان آن شـبکه دوسـت شـود و بـه او یـک فلـش بـا آهنگ‌هـای مـورد علاقـه بدهـد. در سـاعت کاری ایـن خانـم بـا کارمنـد شـبکه تمـاس می‌گیـرد و می‌گویـد یکـی از کلیپ‌هـای موجـود در فلـش بـا نامـی معیـن را اجـرا کنـد چـون یـک آهنـگ نیسـت بلکـه یـک پیغـام صوتـی عاشـقانه اسـت.

کارمنـد شـبکه بـا ذوق و شـوق آن فلـش را بـرای شـنیدن آن فایـل صوتـی بـه کامپیوتـر خـود می‌زنـد و یـک ویـروس مخـرب را ناخواسـته وارد آن شـبکه می‌کنـد و بـرای نفوذگـر امـکان نفـوذی بـی درد سر را مهیـا می‌کنـد.

به سناریو بالا مهندسی اجتماعی می‌گویند.

حملات فیشینگ

حمـلات فیشـینگ را می‌تـوان از حمـلات مرتبـط بـا حـوزه مهندسـی اجتماعـی دانسـت. شـخص نفوذگـر بـا اسـتفاده از فیشـینگ شروع بـه سرقـت اطلاعـات از حجـم عظیمـی از کاربـران می‌کنـد. یکـی از حمـلات معـروف فیشـینگ ارسـال ایمیل‌هـای جعلـی از سـمت بانـک اسـت. بدین نحـو که یـک نفوذگر ایمیـل جعلی از سـمت یـک بانـک را بـرای تعـداد زیـادی کاربـر ایمیـل می‌کنـد و در آن یـک لینـک قـرار می‌دهـد کـه بـه جـای هدایـت بـه صفحـه اصلـی بانـک کاربـر را بـه صفحـه‌ای مشـابه صفحـه بانـک هدایـت می‌کنـد. کاربـر پـس از دیـدن صفحـه‌ای مشـابه صفحـه بانـک و وارد کـردن یوزرنیـم و پسـورد خـود در دام هکـر می‌افتـد. در برخـی حمـلات فیشـینگ نـام کاربـری و رمـز عبـور هـزاران کاربـر بانـک بـه سرقـت می‌رونـد.

البتـه فیشـینگ بـه سرقـت اطلاعـات از طریـق مکالمـات تلفنـی یـا پیـام کوتـاه نیـز اطـلاق می‌شـود. بـه ایـن معنـا کـه گاهـی نفوذگـران بـا تمـاس تلفنـی سـعی در تخلیـه اطلاعاتـی کاربـران دارنـد.

تست نفوذ چیست و چه تفاوتی با هک دارد؟

عملیات تست نفوذ بر اساس یکسری استاندارد ها بر روی پلتفرم های مختلف اما از نوع قانونمند آن توسط هکر های اخلاقی یا همان کلاه سفید صورت می گیرد.

هکر اخلاقی یک متخصص شبکه کامپیوتری است که امنیت یک سازمان را بر عهده میگیرد. کار او میتواند تست نفوذ شبکه سازمان باشد تا نقص های احتمالی برای هر نوع نفوذی به سازمان را پیدا کند. نکته کلیدی که یک هکر اخلاقی نسبت به یک هکر مخرب دارد این است که تمام کارهای یک هکر اخلاقی با اجازه مالکین سازمان و بدون هر گونه هدف مخرب انجام شود.

بعد از فرا گرفتن مهارت های کافی، داشتن تجربه مهم ترین بخش کار می باشد. حداقل زمانی که لازم است تا بتوانید به یک هکر اخلاقی با تجربه تبدیل شوید حداقل ۵ سال می باشد. و زمانی جواب خواهد داد که فرد علاقه کافی را به این کار داشته باشد. پس علاقه و تلاش میتواند مهم ترین پیش نیاز های تبدیل شدن به یک هکر باشد.

حال در آزمون نفوذ هک ، هکر به ارزیابی امنیت سایبری در سیستم های خاص IT می پردازد و نقص های امنیتی سیستم را از طریق بسیاری از رویکرد های هک، که در آن تست نفوذ یکی از ویژگی های آن است ارزیابی می کند

تست نفوذ به دو روش زیر انجام می پذیرد:

۱. White Box Testing
۲. Black Box Testing

White Box Testing(تست جعبهٔ سفید) : نوعی فرایند تست است که در آن ما دسترسی کاملی به کدهای نرم‌افزار داریم؛ که معمولاً هدف از انجام این نوع تست، پیدا کردن حفره‌های امنیتی، یافتاری معماری‌های ضعیف و آسیب‌پذیر نرم‌افزاری، آزمودن جریان ورودی (و البته مشاهدهٔ خروجی مورد انتظار)، ارزیابی عملکرد شرط‌های قرار گرفته در منطق نرم‌افزار و در نهایت آزمودن هر خط از کد، آبجکت، تابع و کلاً هر موجودیت در نرم‌افزار است.

Black Box Testing(تست جعبهٔ سیاه) : نوعی از تست است که ما دیگر دسترسی به سورس‌کد نرم‌افزار نداشته است؛ در تست جعبهٔ سیاه، ابتدا نیازمندی‌ها و ویژگی‌های راه‌اندازی و اجرای نرم‌افزار را مورد بررسی قرار داده سپس ورودی‌های مجاز را برای اینکه ببینیم نرم‌افزار آن‌ها را به درستی پردازش می‌کند یا خیر، مورد تست قرار می‌دهند.
به طور کلی تست جعبهٔ سفید ساختار داخلی را ارزیابی می‌کند در حالی که تست جعبهٔ سیاه بر روی عملکرد نرم‌افزار متمرکز است.

هکر اخلاقی باید دارای دانش گسترده و کامل از مهارت برنامه نویسی و سخت افزار باشد.

CEH

CEH(Certified Professional Ethical Hacker) گواهی نامه ای است که بیشتر هکر ها ی اخلاقی به دنبال کسب آن می باشند.

انواع گواهی نامه هایی که یک هکر اخلاقی می تواند دریافت کند :

گواهینامه SANS GIAC

ارزیابی آسیب پذیری ها (Certified Vulnerabilit Assessor)

هکر اخلاقی حرفه ای (Certified Professional Ethical Hacker)

مهندسی تست نفوذ (Certified Penetration Testing Engineer)

و...

بعد از فرا گرفتن مهارت های کافی، داشتن تجربه مهم ترین بخش کار می باشد. حداقل زمانی که لازم است تا بتوانید به یک هکر اخلاقی با تجربه تبدیل شوید حداقل ۵ سال می باشد. و زمانی جواب خواهد داد که فرد علاقه کافی را به این کار داشته باشد. پس علاقه و تلاش میتواند مهم ترین پیش نیاز های تبدیل شدن به یک هکر باشد.

همونطور که اکثرا میدونید هر کسی در هر زمینه ای مهارت کافی را داشته باشد میتواند به درآمد کافی برسد. پس شرط اصلی برای کار و رسیدن به درآمد، مهارت کافی شما میباشد.

ماهنامه انجمن علمی مهندسی کامپیوتر زیر نظر معاونت فرهنگی دانشجویی موسسه آموزش عالی ارشاد دماوند

نویسنده:

محیا کریمی

تهیه کنندگان :

لیلا نوری (سردبیر نشریه)

محیا کریمی

موفقیت انتهای مسیر نیست, شکست آنقدرها وخیم نیست.
مهم این است که شجاعت ادامه دادن
داشته باشی!

وینستون چرچیل

شماره هشتم مگیت

فروردین ۱۳۹۹