Introduction to Ethical Hacking

معرفی هک قانونی

هک اخلاقی: به هکی گفته میشود که هکر بجای اینکه بیاد از نقاط ضعف یک شبکه سوء استفاده کنند و به آن نفوذ کنند و به شبکه آسیب بزند–روی شبکه تست و آنالیز انجام میدهد برای پیدا کردن آسیب پذیری موجود در آن و به مدیر شبکه گزارش میدهد تا اشکلات و ضعف های شبکه خود را برطرف کنند یا در قبال مبلغی آسیب های آن شبکه را برطرف کند.

*شبکه در اینجا میتواند(سایت–سرور–کامپیوتر–شبکه های کامپیوتری–برنامه–سامانه های صعنتی و...)هر چیزی که مربوط به حوزه سایبری و کامپیوتر میشود.

آشنای با مفاهیم و اصطلاحات هک و نفوذ

- ✓ هک (Hack) : به استفاده کردن و دسترسی غیر مجاز به یک شبکه را هک میگویند.هک را به معنی رخنه–نفوذ–دسترستی غیر مجاز–دزدیدن هم تعریف میکنند.
- ✓ هکر (Hacker) : به فرد خبره ای که به شبکه نفوذ میکند و اطلاعاتی را بدست می آورد و درون آن شبکه میتواند اختلال ایجاد کند یا نکند و آسیب بزند یا نزند به آن فرد هکر گویند

نویسنده و مولف : حامد مقدسی پور

- ✓ انواع هکر : **1**–هکرهای کلاه سفید (White Hat Hackers) : به هکرهای گفته میشود که کارهای مفیدی انجام میدهند در زمینه ای هک ولی نیت بدی ندارند و به شبکه آسیب نمیزنند و باج گیری نمیکنند هکرهای کلاه سفید گویند. **2**–هکرهای کلاه سیاه (Black Hat Hackers) : به هکرهای گفته میشود که بر خلاف هکرهای کلاه سفید عمل میکنند و به شبکه آسیب میزنند و یا اطلاعاتی را بدست می آورند و در قبالش باج گیری میکنند هکرهای کلاه سیاه گویند.**3**–هکرهای کلاه خاکستری (Gray Hat Hackers) : به هکرهای گفته میشود که هم کارهای هکرهای کلاه سفید و کلاه سیاه را انجام میدهند.
- ✓ تست نفوذ (Pentration Testing) : راهی است که یک هکر یا کارشناس امنیت به دنبال آن می رود که معمولا هکرهای کلاه سفید یا هکرهای قانونمند بدنبال آن میروند.در این راه هکر روی شبکه ها عمل نفوذ انجام میدهد اما به شبکه آسیب نمیزند و دقیقا شبیه هک اخلاقی هست که میتواند با بستن قرارداد کتبی با مدیر آن شبکه بصورت قانونی روی آن شبکه عمل نفوذ انجام دهد و آسیب ها و ضعف های شبکه را بیابد و به مدیر شبکه با ارائه یک سند (Document)گزارش دهد و آن ها رفع کند.
- ✓ انواع تست نفوذ : **1**–تست نفوذ با جعبه سفید (White Box Pen Test) : در این تست هکر در اصل به اجازه ی مدیر آن شبکه و سازمان با استفاده از یک سیستم داخل شبکه روی شبکه تست میزند و به شناسایی آسیب پذیری های شبکه میپردازد و تست نفوذ در این نوع روش خیلی زودتر از بقیه روش هاست. **2**–تست نفوذ با جعبه سیاه (Black Box Pen Test) : در این تست هکر با استفاده ی از یک سیستم خارج شبکه روی شبکه تست میزند و به جمع آوری اطلاعات آن شبکه و شناسایی آسیب پذیری های شبکه میپردازد(یعنی یک هکر از اول مراحل تست نفوذ یا هک اخلاقی را انجام میدهد) و تست نفوذ در این روش خیلی دیرتر از بقیه روش هاست.**3**– تست نفوذ با جعبه خاکستری (Gray Box Pen Test) : در این تست هکر با استفاده از اطلاعات جزئی در مورد شبکه و سطح دسترسی آن در شبکه محدود است و به شناسایی آسیب پذیری های شبکه میپردازد.
- ✓ حفره امنیتی (Bug) : به خرابی ها یا اشکالات و خطاهای موجود در یک شبکه را حفره امنیتی گویند.

نویسنده و مولف : حامد مقدسی پور

- ✓ هدف (Target) : به شبکه ای که مورد حمله و نفوذ قرار میگیرد یا قرار گرفته را هدف گویند.
- ✓ آسیب پذیری (Vulnerability) : به ضعف و تهدیدی که در یک شبکه موجود است را آسیب پذیری گویند.
- ✓ حمله (Attack) : (هدف + روش انجام کار با آن (آسیب پذیری) + آسیب پذیری).به روش انجام کار با آسیب پذیری موجود در یک هدف(شبکه) که موجب نفوذ وصدمه به آن میشود را حمله گویند.
- ✓ دیفیس (Deface) : به معنی تغییر ظاهری یک صفحه است که به تغییراتی گفته میشود که روی یک تارگت صورت گرفته را دیفیس گویند.
- ✓ دور زدن (Bypass) : به گول زدن یک سری ابزارهای امنیتی و فایروال های یک شبکه که با استفاده یک سری دستورات و کد ها صورت میگرد را دور زدن گویند.
- ✓ صفحه ی جعلی (Fake Page) : به صفحاتی که توسط یک هکر یا یک سری ابزارها ساخته میشود و در آن صفحات یک سری کدها و متدها تغییر یافته و به قربانی داده میشود که پس وارد کردن اطلاعات خود باعث فاش شدن اطلاعات میشود را صفحه ی جعلی گویند.این صفحات جعلی مانند صفحات درگاه های پرداخت اینترنتی –پنل های ورود به یک سایت – صفحات ثبت نام یک سایت

- ✓ درب پشتی (BackDoor) : روشی است که بتوانیم به وسیله ی اون مجوزهای دسترسی اطلاعات را دور زد و در اصل به روشی که بدون شناسایی وارد شبکه شد و یا اطلاعات شبکه را خارج کرد در اصل درب پشتی یا بکدور گویند از بکدور برای ارتقای دسترسی استفاده میشود.
- ✓ ربات شبکه (BotNet) : به مجموعه ای از نرم افزارها یا ابزارهای که با استفاده از پروتکل های اینترنت با برنامه ای اصلی که نقش یک شبکه (سرور) را بازی میکند ربات شبکه گویند. از بات نت ها در حملات دیداس و داس استفاده میشود.

نویسنده و مولف : حامد مقدسی پور

- ✓ رَت (Rat) : Remote Access Torjan–برنامه ای که با ترکیبی از برنامه های راه دور و ابزارهای مخرب یا کی لاگر ساخته میشود و بعد از اجرا شدن روی شبکه(سیستم) اطلاعات آن شبکه را در اختیار هکر قرار میدهد.
- ✓ شل (Shell) : در اصل به معنی پوسته است که در سیستم عامل یونیکس و لینوکس جزو قسمت های که رابط بین کاربر و سخت افزار سیستم است اما در مفاهیم هک و نفوذ – به هک سیستم تارگت و کنترل اون با استفاده از نفوذ را شل گرفتن گویند.
- ✓ بایند (Bind) : به مخلوط کردن یا ترکیب دو فایل را بایند گویند. از بایند برای مخلوط یک فایل مخرب و یک فایل مثل (عکس–ویدیو–برنامه و...)استفاده میشود.
- ✓ بروت فورس (Brute Force) : یک نوع حمله محسوب میشود که هکر از این حمله برای بدست آوردن پسورد و رمز عبور از آن استفاده میشود. در این نوع حملات معمولا از کاراکترها و حروف زیادی مثل (0 تا 9 –-*&^%$#@!~ – A تا Z بزرگ و کوچک)استفاده میشود.
- ✓ سر ریز بافر (Buffer Over Flow) : در اصل یک نوع باگ است که در نرم افزار ها و سرور ها رخ میدهد–زمانی رخ میدهد که یک سرور اطلاعات زیادی را دریافت میکند و سعی میکند این اطلاعات را در جای بنویسد یا ذخیر کند که آن اطلاعات را برای مقصدی در نظر گرفته باشد.را اصطلاحا میگویند سر ریز بافر رخ داده هست.
- ✓ کوکی (Cookie) : فایل های بسیار کوچکی هستند که برای نگهداری اطلاعات کاربرانی که وارد سایت شده اند استفاده میشود که این برای مدت کوتاهی اگر کاربر مجددا وارد سایت شد برای او به نمایش در می آید.
- ✓ کراک (Crack) : به شکستن پسورد ها یا دیکد کردن کدها و شکستن کدهای اپلیکشن ها را کراک گویند و به کسی که این عمل را انجام میدهد کراکر میگویند که معمولا دارای قدرت برنامه نویسی بالای هست.

نویسنده و مولف : حامد مقدسی پور

- ✓ اکسپلویت (Exploit) : کدی است که برای سوء استفاده از باگ های یک شبکه (سیستم–نرم افزار–سایت–سرور و...)استفاده میشود که به زبان های برنامه نویسی مختلفی نظیر C,PHP,Ruby,Python,Asp.net,Java,Per نوشته میشود.
- ✓ صفر روزه (0Day) : باگی است که توسط هکر ها کشف میشود یا با ابزارهای مختلف آن را پیدا میکنند که در درون نرم افزار ها و صفحات وب و اکسپلویتی برای آن مینویسند Zero Day یا Private میگویند معمولا این نوع باگ ها شاید سالها طول بکشد یک هکر آن ها را کشف کند.
- ✓ پویشگر آسیب پذیری (Vulnerability Scanner) : برنامه های هستند که باگ ها و آسیب پذیری های موجود در یک شبکه را کشف میکنند.مانند Acunetix-Nessus و...
- ✓ اسکم (Scam) : نامه های هستند که برای یک تارگت فرستاده میشوندکه چه ایمیل چه پیامک که این نامه ها دروغ هستند و تارگت مورد نظر را هدایت به یک صفحه ی آلوده یا استفاده از اطلاعات تارگت.

مراحل هک اخلاقی

1– شناسایی : در این مرحله به کشف و جمع آوری اطلاعات در مورد یک شبکه می پردازیم.

2– اسکن : در این مرحله با استفاده از ابزارهای پویشگر آسیب پذیری و اسکنر های مختلف بدنبال نقاط ضعف یک شبکه را پیدا میکنیم.

3– ایجاد دسترسی : در این مرحله با استفاده از آسیب پذیری ها و حفره های امنیتی اقدام به نفوذ به شبکه می کنیم.

4– حفظ دسترسی : در این مرحله ما با استفاده از بکدور دسترسی خودمون رو بالا می بریم و حفظ میکنیم.

5– از بین بردن رد پا : در این مرحله میایم تمام لاگ ها و ردپاهای موجود خودمون رو در شبکه پاک میکنیم.

نویسنده و مولف : حامد مقدسی پور

مثلث امنیت

امنیت صرفا برای جلوگیری از فاش شدن اطلاعات نیست بلکه در دسترس نبودن اطلاعات در زمان مورد نیاز و حتی تغییر اطلاعات در یک مسیر تبادل نیز باعث فاش شدن اطلاعات و از دست دادن آن می شود.

1- محرمانگی : محرمانه بودن فقط یعنی افراد و سیستم ها و کاربران مجاز بتوانند از اطلاعات استفاده کنند و افراد و سیستم های بیکانه نباید به آن ها دسترسی داشته باشند.

2- صحت و تمامیت : یعنی فقط افراد و سیستم های مجاز امکان تغییر و ویرایش داده ها و فایل ها را داشته باشند.

3- دسترسی پذیری : یعنی افراد و سیستم های مجاز در زمان مجاز به داده ها و فایل ها دسترسی داشته باشن.

*این مثلث توسط موسسه **NIST** در جهت اجرای طرح دولت الکترونیک در ایالت متحده (آمریکا) برای سازمان های دولتی و غیر دولتی تعریف کرده است.

متدها و روش های حمله

1- شناسایی : کشف ضعف های موجود در یک شبکه که براساس این ضعف ها میتوان به شبکه مورد نظر حمله کرد.

2- مهندسی اجتماعی : در این متد هکر با استفاده از نقطه ضعف شبکه خود را به جای مدیر و کاربر آن شبکه میتواند جا بزند.

نویسنده و مولف : حامد مقدسی پور

3- کشف پسورد : در ایم روش هکر سعی میک ند که پسورد شبکه را کشف کند راه های مختلفی برای کشف پسورد وجود دارد که یکی از این راه ها جستجوی پیچده است.

4- بات نت : هکر با استفاده ربات های شبکه میتواند حملات گسترده روی یک شبکه ایجاد کند که یکی از حملات گسترده مثل حملات تکذیب سرویس یا **DDOS** است.

5- حملات امنیتی : این حملات دو نوع هستند فعال و غیر فعال – حملات امنیتی فعال به حملاتی گفته میشه که هکر اطلاعات رو شنود و جمع آوری میکند و اقدام به تغییر اطلاعات و داده ها میکند اما در حملات امنیتی غیر فعال هکر فقط اطلاعات شنود و جمع آوری میکند و تغییری بر روی داده ها انجام نمیدهد.

6- حملات مرد میانی : در روش هکر بین فرستنده و گیرنده قرار میگیرد و هویت خودش رو برای دو طرف جعل میکند،تمام اطلاعات در حال تبادل هکر مشاهده میکند و میتواند اطلاعات بعد از تغییر برای هر طرف ارسال کند.

7- هرزنامه : به ایمیل های ناگهانی و ناخواسته هرزنامه گفته میشود، در این درون این نوع ایمیل ها کدهای مخرب وجود داشته باشد و باعث آلودگی سیستم یا شبکه شود و یا حاوی لینک آلوده باشد که تارگت مورد نظر بعد از کلیک روی آن ،آن را وارد صفحه ی آلوده و مخرب بکند و سیستم را آلوده بکند.

8- اسنیف : اسنیف برای نظارت و جمع آوری اطلاعات در حال تبادل بر روی شبکه استفاده میشود که ابزارهای مختلفی وجود دارد که مثل وایرشارک،در این نوع روش هکر میتواند از این نوع ابزارها برای دزدی پکت ها یا اطلاعات و داده بکند یعنی یک عملکرد نامشروع داشته باشند ،اما مدیران و متخصصین امنیت شبکه برای تجزیه و تحلیل از آن استفاده میکند یعنی یک عملکرد مشروع دارند.

9- اسپوف : در این روش هکر با استفاده از جعل آدرس آیپی کامپیوتری به جای آدرس آیپی خودش اقدام به دسترسی غیر مجاز به داده های یک شبکه بکند– این روش بیشتر در دور زدن ابزارهای امنیتی و فایروال ها استفاده میشود.

نویسنده و مولف : حامد مقدسی پور

اصول و قوانین اساسی امنیت اطلاعات

1- قانون حداقل امتیاز : در این قانون حداقل دسترسی به داده های یک شبکه فراهم بشه و نه بیشتر .

2- دفاع در عمق : در این قانون باید امنیت در لایه های مختلف شبکه وجود داشته باشد یعنی اینکه در همه ی لایه ها وجود داشته باشد و اگر در یکی از لایه ها خطا و ضعفی رخ داد کل شبکه زیر سوال نرود.

3- تفکیک وظایف : در این قانون باید در شبکه و سازمان خود افراد خاصی رو قرار بدید که امنیت و سیاست ها بدرستی اجرا بشه و همچنین این افراد خاص بصورت دوره ای در بخش های مختلف شبکه قرار بگیرند تا از خظا ها و آسیب پذیری ها کاسته شود.

4- بازرسی : در این قانون تمام اتفاقات و مشکلاتی که در شبکه رخ میدهد باید ضبط و نگهداری شود و طی یک دوره ای مورد بررسی با دوره های قبلی قرار بگیرد تا نمودار و چارت اتفاقات کاهش پیدا کرده است یا خیر.

تهدیدات

***تهدید به معنی هر سیستمی یا شبکه ای دارای اطلاعات مهمی باشد که در معرض خطر باشد را تهدید سایبری میگویند.**

1- حملات نرم افزاری : مثل ویروس ها ،بد افزارها ،تروجان ها ،بکدورها ،کرم ها و...

2- جاسوسی : زمانی که یک فرد به اطلاعات محرمانه یک شبکه و سازمان دسترسی پیدا کند.

3- کنترل های ناقص : بروز نبودن تجهیزات نرم افزاری و سخت افزاری که باعث آسیب پذیری درون اون شبکه میشه.

نویسنده و مولف : حامد مقدسی پور

4- **اشتباهات انسانی** : کارهای مخرب که توسط یک کاربر مجاز انجام میشه و باعث مشکلاتی در شبکه میشه.

5- **سرقت** : سرقت به معنی دزدیدن است ما در اینجا به سرقت الکترونیکی اشاره میکنیم نه سرقت فیزیکی ،در سرقت الکترونیکی اطلاعات توسط یک هکر دزدیده میشوند اما اون اطلاعات سر جای خودش است فقط هکر اطلاعات کپی کرده و شما نمیدونید اطلاعات شما در دست هکر هم قرار دارد.

6- **اشتباهات نرم افزاری و سخت افزاری** : در این نوع تهدید شاید نرم افزار و سخت افزار باهم سازگار نباشن یا اینکه نرم افزار ها روی کدهاشون تحلیل و آنالیز صورت نگرفته باشد (دیباگ یا خطایابی)که موجب آسیب پذیری میشود.

7- **بلایای طبیعی** : یکی از خطرناک ترین تهدیدات است مانند سیل ،رعد و برق ، زلزله و... که میتوان باعث نابود شدن اطلاعات شود.

8- **سیاست های اشتباه** : برنامه ریزی ها و سیاست های نادرست که باعث حملات و آسیب پذیری ها میشود.

9- **اخاذی در مقابل اطلاعات** : در این روش هکر اطلاعاتی از یک شبکه بدست آورده و در عوض فاش نکردن و باز گرداندن اون اطلاعات از مدیر اون شبکه و سازمان باج میگیره و مدیر اون شبکه ناچار است این امر رو از هکر قبول کنه.

نویسنده و مولف : حامد مقدسی پور