# آموزش هک

## برای مبتدی‌ها

علی‌اصغر جعفری لاری

انتشارات پندار پارس

سرشناسه : جعفری لاری، علی‌اصغر، ۱۳۶۷ -
عنوان و نام پدیدآور : آموزش هک برای مبتدی‌ها/علی‌اصغر جعفری‌لاری.
مشخصات نشر : تهران : پندار پارس، ۱۳۹۳.
مشخصات ظاهری : ۱۸۴ ص.: مصور (رنگی).
شابک : 978-600-6529-61-5: ۱۱۰۰۰۰ ریال
وضعیت فهرست نویسی : فیپا
موضوع : کامپیوترها -- ایمنی اطلاعات
موضوع : شبکه‌های کامپیوتری -- تدابیر ایمنی
موضوع : هکرها
موضوع : حفاظت اطلاعات
رده بندی کنگره : ۱۳۹۳۵۹/۵۱۰۵TK ۸ٍ۷ج/
رده بندی دیویی : ۸/۰۰۵
شماره کتابشناسی ملی : ۳۴۵۲۶۲۲

*انتشارات پندارپارس*

**دفتر فروش**: انقلاب، ابتدای کارگرجنوبی، کوی رشتچی، شماره 14، واحد 16 **www.pendarepars.com**
تلفن: 66572335 - تلفکس: 66926578 همراه: 09122452348 **info@pendarepars.com**

**نام کتاب** : **آموزش هک برای مبتدی‌ها**
**ناشر** : **انتشارات پندار پارس**
**ترجمه و تالیف** : **علی‌اصغر جعفری لاری**
**چاپ نخست** : **اردیبهشت 93**
**شمارگان** : **1000 نسخه**
**لیتوگرافی** : **ترام‌سنج**
**چاپ، صحافی** : **فرشیوه، خیام**
**قیمت** : **11000 تومان** **شابک** : 978-600-6529-61-5

# فهرست

## سلب مسئولیت قانونی از نویسنده و ناشر

مسئولیت هر گونه اقدام یا فعالیت مربوط به محتوای موجود در این کتاب منحصرا به عهده‌ی شما خواننده‌ی گرامی می‌باشد. نویسنده هیچ مسئولیتی در قبال وقوع هرگونه اتهام غیر قانونی که افراد با سوء استفاده از اطلاعات داخل این کتاب برای نقض قانون انجام می‌دهند، نخواهد داشت. این کتاب حاوی مباحث و منابعی است که به طور بالقوه مخرب یا خطرناک است و تنها برای اهداف آموزشی و پژوهشی نوشته شده است.

طبق ماده‌ی 1 قانون جرایم رایانه‌ای، "هر کس به طور غیرمجاز به داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی که به‌وسیله‌ی تدابیر امنیتی حفاظت شده است دسترسی یابد، به حبس از 91 روز تا یک سال یا جزای نقدی از پنج تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد."

## شرایط و مقررات این کتاب

در حالی که از این کتاب استفاده می‌کنید و آموزش‌های مختلف هک کردن را مطالعه می‌کنید، شرایط و مقررات زیر را پذیرفته‌اید:

1. تمام اطلاعات ارائه شده در این کتاب برای مقاصد آموزشی است. نویسنده‌ی کتاب به هیچ وجه مسئول هرگونه سوء استفاده از اطلاعات نمی‌باشد.
2. "هک برای مبتدیان" تنها یک اصطلاح است که عنوان کتاب را نشان می‌دهد و این کتاب هیچ اطلاعات غیرقانونی را ارائه نمی‌کند. کتاب "هک برای مبتدیان" مربوط به امنیت کامپیوتر است و دزدی نرم افزار/کرک کردن/هک کردن را ترویج نمی‌کند.
3. این کتاب کاملا برای ارائه‌ی اطلاعات در موضوع‌های "امنیت کامپیوتر"، "برنامه‌نویسی کامپیوتر" و دیگر موضوع‌های مرتبط نوشته شده است و به هیچ وجه به مباحث "CRACKING" یا "HACKING" (غیر اخلاقی) نمی‌پردازد.
4. هک یا نفوذ (بدون اجازه) به کامپیوتری که متعلق به شما نیست، غیر قانونی است.
5. تمام اطلاعات موجود در این کتاب برای توسعه‌ی دفاع در مقابل هکرها نوشته شده است و به جلوگیری از حمله‌های هکرها کمک می‌کند. "هک برای مبتدیان" تأکید دارد که این اطلاعات نباید برای ایجاد هر نوع آسیب مستقیم یا غیرمستقیمی استفاده شود. هرچند، می‌توانید از این کدها به روی سیستم خود (با مسئولیت خودتان) امتحان نمایید.
6. واژه‌ی "هک" یا "هک کردن" که در این کتاب استفاده شده است به عنوان "هک اخلاقی" یا "هک کردن اخلاقی" در نظر گرفته شده است.

7. اینجانب تنها به هکرهای کلاه سفید و کلاه خاکستری باور دارم و از سوی دیگر، هکرهای کلاه سیاه را محکوم می‌کنم.
8. بسیاری از اطلاعات ارائه شده در این کتاب، ترفندهای ساده‌ی کامپیوتر هستند (که ممکن است با عنوان هک نامیده شود) و به هیچ وجه به اصطلاح Hacking مربوط نمی‌شود. هدف از بیان این ترفندها با توجه به اینکه بیشتر مخاطبان کتاب مبتدی هستند، عدم ایجاد یکنواختی در مباحث آموزشی بوده است.
9. برخی از ترفندهای ارائه شده ممکن است به دلیل رفع اشکالات، دیگر کارایی نداشته باشد. اینجانب مسئول هرگونه خسارت مستقیم یا غیرمستقیم ناشی از استفاده از هک‌های ارائه شده در این کتاب، نخواهم بود.
10. شما می‌توانید پرسش‌های خود را در هنگام مطالعه‌ی کتاب یا پس از پایان آن، در وبسایت پرسش و پاسخ Http://SecurityAdviser.ir در میان گذارید یا در صفحه‌ی مربوط به این کتاب در سایت انتشارات پندار پارس (pendarepars.com) مطرح کنید.

## پیش‌گفتار

پیش از ورود به مباحث "آموزش هک برای مبتدی‌ها"، از شما بابت انتخاب این کتاب، سپاسگزارم.

این کتاب که مباحث آن، به طور ابتدایی، جذاب و کاربردی نوشته شده است مرجع مفیدی برای دانش آموزان، دانشجویان و هر فردی که به علم هک و امنیت علاقه‌مند است و می‌خواهد آن را از ابتدا شروع کند، خواهد بود. در این کتاب، ابتدا به تعاریف و مقدمات هک و امنیت خواهم پرداخت و سپس شما را با دنیای واقعی هک آشنا می‌کنم. در نگارش این کتاب، خود را در جایگاه یک مخاطب مبتدی قرار داده‌ام تا بتوانم به هر شکل ممکن، ذهنیات او را به طور کارآمد، درک کنم و از نگرانی‌های فراگیری این علم تا حدی بکاهم.

اگر می‌خواهید چگونگی اجرای حمله‌های مخرب، ترفندهای سرقت آنلاین، دور زدن تدابیر امنیتی و یا قطع سرویس‌ها را فرا بگیرید، پیشنهاد می‌کنم در جای دیگری به دنبال آن بگردید. اما اگر می‌خواهید هک اخلاقی را از ابتدا شروع کنید و به دنبال مرجعی مناسب برای فراگیری آن می‌گردید، به‌شدت پیشنهاد می‌کنم که این کتاب را به طور کامل مطالعه فرمایید.

با خواندن این کتاب، گام نخست را برای فراگیری هک برداشته‌اید. گام‌های بعدی شما به پشتکار، استعداد و هدفتان بستگی دارد. جست‌وجو در اینترنت، مطالعه‌ی کتاب‌های خارجی و داخلی و فراگیری زبان‌های برنامه‌نویسی می‌تواند در رسیدن به هدفتان به شما کمک شایانی کند. پس از خواندن این کتاب، تشخیص خواهید داد که چگونه علم هک بر روال کاری روزانه‌ی ما تأثیر می‌گذارد و می‌تواند در بسیاری از زمینه‌ها مانند هک حساب‌های بانکی و. . . بسیار خطرناک باشد. افزون بر این، پس از خواندن این کتاب می‌توانید درک کنید که هکر کیست و چگونه می‌توان از تهدیدهای او دفاع کرد. اما کار به اینجا ختم نمی‌شود، چراکه با پی بردن به قدرت واقعی هک، بسیار به این علم علاقه‌مند می‌شوید و مصمم‌تر از پیش به فراگیری تکنیک‌های مختلف در منابع دیگر خواهید پرداخت.

فراموش نکنید که، اگر بدانید چگونه هکرها نفوذ می‌کنند، می‌توانید از نفوذ هکرها جلوگیری کنید و من تلاش کرده‌ام شما را با این هدف سالم بیشتر آشنا نمایم. پس از سپاس و ستایش به درگاه پروردگار، از مدیریت محترم انتشارات پندار پارس، جناب آقای مهندس حسین یعسوبی و تمامی همکارانشان که مهربانانه دست مرا در انجام این هدف مهم فشردند، تشکر و قدردانی می نمایم.

**علی اصغر جعفری لاری**

Http://Parsing.ir
Http://SecurityAdviser. ir
Admin@SecurityAdviser.ir

# فصل نخست

# آشنایی با مفاهیم هک و امنیت

## 1-1 مفهوم هک اخلاقی

هک اخلاقی، تست منابع با هدفی خیرخواهانه و برای بهبود فناوری است. به طور فنی، هک اخلاقی به معنی تست نفوذی است که به روی ایمن‌سازی و حفاظت از سیستم‌های IT تمرکز می‌کند.

**هک**

- هنر بررسی نقض‌های مختلف امنیتی را **هک**[1] می‌نامند.
- هکرهای کامپیوتر از سالیان متمادی در این عرصه حضور داشته‌اند. از آنجا که اینترنت به‌طور گسترده در جهان استفاده می‌شود، ما بیشتر و بیشتر درباره‌ی علم هک می‌شنویم. تنها شمار اندکی از هکرها مانند Kevin Mitnick به خوبی شناخته شده‌اند.
- هکرها با هم برابر نیستند و هر کدام، انگیزه، روش و مهارت خود را دارند.
- هکرها کنجکاو هستند که در مورد چیزهای جدید بیشتر بدانند. با شجاعت گام بر می‌دارند و بیشتر، دارای ذهنی باز و وسیع هستند.
- بیشتر مردم می‌اندیشند که هکرها، جنایتکاران کامپیوتری هستند. در واقع جنایتکاران و هکرها، دو چیز کاملا نامربوط هستند و رسانه‌ها در قبال این کار مسئول هستند. هکرها درواقع افراد خوب و بسیار هوشمندی هستند که با استفاده از دانش خود به سازمان‌ها، شرکت‌ها، دولت و... کمک سودمندی می‌کنند و تأمین امنیت اعتبارنامه‌ها و اطلاعات محرمانه را بر روی اینترنت فراهم می‌کنند.
- سال‌های پیش، هیچ کس نگران نقض امنیت کامپیوتر و نصب ویروس‌های تروجانی توسط کراکرها یا استفاده از کامپیوترتان برای انجام حمله‌ها بر علیه دیگر کاربران، نبود. اکنون داستان تغییر کرده است و بهتر است که از چگونگی دفاع در برابر آسیب نفوذگران کلاه سیاه آگاه باشیم. هک کردن در سراسر جهان رایج است، البته نه هک کردن بلکه اجرای هک بدون نقص توسط نفوذگر برای به خطر انداختن سیستم، سرقت هر چیز باارزش و سپس پاک کردن ردپای خودشان در 20 دقیقه نیز رایج است.

---

[1] Hack

## هکر

- به طور سنتی، **هکر**[1] کسی است که دوست دارد با نرم‌افزار یا سیستم‌های الکترونیکی بازی کند. هکرها از کاوش و یادگیری درباره‌ی چگونگی به‌کارگیری سیستم‌های کامپیوتری لذت می‌برند. آنها عاشق کشف روش‌های جدید هستند.
- به‌تازگی، "هکر" معنای جدیدی گرفته است؛ کسی که به طور مخرب سیستم‌ها را برای منافع شخصی نقض می‌کند. به طور فنی این جنایتکاران، کراکرها[2] هستند. کراکرها سیستم‌ها را با اهداف مخرب نقض می‌کنند.
- کراکرها بیشتر این کار را برای منافع شخصی، شهرت، سود و حتی انتقام انجام می‌دهند. کراکرها اطلاعات مهم و حساس را تغییر می‌دهند، حذف می‌کنند و یا به سرقت می‌برند.
- میزان زیادی از معنای هک، به دانش فرد و نیت کاری او بستگی دارد. هک، یک هنر و همچنین یک مهارت است. هک دانشی است که با آن می‌توان به اهداف خود با استفاده از قدرت و مهارت دست یافت.
- بنابراین، Hacker شخصی است که هدف اصلی او، نشان دادن قدرت خود به کامپیوتر و دیگر ماشین‌هاست. وارد شدن به سیستم و یا شکست دادن محاسبات، کنجکاوی در اطلاعات‌محرمانه از خصوصیات یک هکر می‌باشد. این فرد، یک برنامه‌نویس کنجکاو است که آسیبی به اهداف (وب‌سایت/شبکه/سرویس‌ها و...) وارد نمی‌کند و در اصل با انگیزه‌ای سالم، باعث تحکیم جابه‌جایی‌ها می‌شود.

### چه تفاوتی بین هکر و کراکر وجود دارد؟

- مقاله‌های بسیاری در مورد تفاوت‌های بین هکرها و کراکرها وجود دارد که در آنها تلاش شده است تا تصورهای غلط عمومی در مورد هک تصحیح شود. برای سال‌های بسیاری، رسانه‌ها واژه‌ی هکر را به‌جای واژه‌ی کراکر در جهان به‌کار می‌بردند. بنابراین مردم معتقد بودند که هکر کسی است که سیستم‌های کامپیوتری را نقض می‌کند و اطلاعات محرمانه را به سرقت می‌برد. این تصور بسیار غیر واقعی و توهین به برخی از هکرهای با استعداد در سراسر جهان است.

**نکات مختلفی برای تعیین تفاوت بین هکرها و کراکرها وجود دارد**

- تعریف: یک هکر کسی است که به کارکردن با سیستم‌عامل کامپیوتر علاقه‌مند است. در بیشتر موارد، هکرها برنامه‌نویس هستند. هکرها دانش پیشرفته‌ای از سیستم‌عامل‌ها و زبان‌های برنامه‌نویسی دارند. آنها حفره‌های امنیتی مختلف و دلایل به‌وجود آمدن آن در درون سیستم‌ها را می‌دانند. هکرها به طور پی‌درپی به دنبال دانش بیشتر و به اشتراک گذاشتن آنچه که کشف کرده‌اند، هستند. هکرها هرگز اهدافی هچون آسیب رساندن و یا سرقت اطلاعات ندارند.

---

[1] Hacker

[2] Cracker

- تعریف: یک کراکر کسی است که سیستم‌های افراد دیگر را با اهداف مخرب نقض می‌کند. کراکرها دسترسی غیرمجاز کسب می‌کنند، اطلاعات مهم را نابود می‌کنند، خدمات ارائه شده‌ی سرور را متوقف می‌کنند و یا اساسا مشکلاتی را برای اهدافشان ایجاد می‌کنند. کراکرها می‌توانند به سادگی شناخته شوند زیرا اقدامات‌شان مخرب می‌باشد.
- به هر روی، بسیاری از افراد هکر را یک فرد منفی می‌دانند. بسیاری از هکرهای مخرب سارقان الکترونیکی هستند. درست مانند کسی که دزد یا راهزن است و هر کسی می‌تواند این شخصیت را داشته باشد بدون در نظر گرفتن سن، جنس یا مذهب. مهارت‌های فنی هکرها نسبت به یکدیگر متفاوت است. طبق نظر برخی از پایگاه‌ها، برخی از هکرها به سختی می‌دانند که چگونه به گشت و گذار در اینترنت بپردازند در حالی که برخی دیگر، نرم‌افزاری را می‌نویسند که هکرهای دیگر به آن نیازمند هستند. البته شخصا باور دارم که هکرها یکتا هستند و کسی که دانش و معیارهای لازم را در این حوزه ندارد، واژه‌ی هکر زیبنده‌ی وی نیست.

## انواع هکرها

### دسته‌بندی هکرها بر اساس دانش

**کدنویسان**[1]

- ✓ هکرهای واقعی کدنویسان هستند. کسانی که روش‌ها را بازنگری می‌کنند و ابزارهایی را می‌آفرینند که در فروشگاه‌ها در دسترس است. کدنویسان می‌توانند حفره‌های امنیتی و نقاط ضعف را در نرم‌افزار برای ایجاد اکسپلویت‌هایشان کشف کنند. این دسته از هکرها می‌توانند از این اکسپلویت[2]ها برای توسعه‌ی کامل سیستم‌ها به صورت امن استفاده کنند.
- ✓ کدنویسان، برنامه‌نویسانی هستند که توانایی پیدا کردن آسیب‌پذیری‌های یکتا در نرم‌افزارهای موجود و توانایی ایجاد کدهای اکسپلویت کارآمد را دارند. این افراد با درک عمیق مدل لایه‌ی OSI و پشته‌ی TCP/IP یکتا هستند.

**مدیران**[3]

- ✓ مدیران، افراد کامپیوتری هستند که از ابزارها و اکسپلویت‌های تهیه شده توسط کدنویسان استفاده می‌کنند. آنها تکنیک‌های خود را توسعه نمی‌دهند؛ هرچند، مدیران از ترفندهایی استفاده می‌کنند که هم‌اینک توسط کدنویسان تهیه شده است. آنها به طور کلی مدیر سیستم یا کنترل کننده‌ی شبکه‌ی کامپیوتری هستند. بسیاری از هکرها و افراد امنیتی در این جهان‌دیجیتالی در این دسته جای دارند.

---

[1] Coders

[2] Exploit

[3] Admins

- ✓ مدیران تجربه‌ی کار با چندین سیستم‌عامل را دارند و می‌دانند که چگونه از آسیب‌پذیری‌های مختلف موجود، بهره‌برداری کنند. بیشتر مشاوران امنیتی در این گروه قرار دارند و گاهی در بخشی از یک تیم امنیتی کار می‌کنند.

**Script Kiddies**

- ✓ دسته‌ی خطرناک بعدی هکرها، Script Kiddies هستند. آنها نسل جدیدی از کاربران کامپیوتر هستند که امکان استفاده از مقالات و ابزارهای هکرها را به روی اینترنت به صورت رایگان دارند؛ اما هیچ دانشی از آنچه که در پشت صحنه روی می‌دهد، ندارند. درباره‌ی این دسته از هکرهای نوجوان در رسانه‌های خبری بیشتر شنیده می‌شود؛ با اینکه آنها کمترین مهارت‌های مورد نیاز را برای انجام حمله‌های خود دارند.
- ✓ Script Kiddies کسانی هستند که از اسکریپت و برنامه‌های توسعه داده شده توسط دیگران برای حمله به سیستم‌های کامپیوتری و شبکه‌ها استفاده می‌کنند. این دسته، آزاردهنده‌ترین و خطرناک‌ترین دسته‌ای هستند که می‌توانند مشکلات بزرگی را بدون اینکه در واقع بدانند چه کاری را انجام می‌دهند، به‌وجود آورند.

## دسته‌بندی هکرها بر اساس فعالیت‌های انجام داده شده

**هکر کلاه سفید**[1]

- ✓ هکر کلاه سفید، یک فرد کامپیوتری است که هک اخلاقی انجام می‌دهد. این افراد معمولا متخصصان امنیتی با دانش هک و مجموعه ابزار هکرها هستند. هکرهای کلاه سفید، از این دانش برای جست‌وجوی نقاط ضعف امنیتی و اجرای اقدامات متقابل در منابع استفاده می‌کنند.
- ✓ همچنین آنها به عنوان یک هکر اخلاقی یا یک تست کننده‌ی نفوذ شناخته می‌شوند. آنها بر تضمین امنیت و حفاظت از سیستم‌های IT تمرکز دارند.

**هکر کلاه سیاه**[2]

- ✓ هکر کلاه سیاه، یک فرد کامپیوتری است که هک غیراخلاقی انجام می‌دهد. این افراد، هکرهای جنایی یا کراکرهایی هستند که از دانش و مهارت خود برای اهداف غیرقانونی و یا مخرب استفاده می‌کنند. آنها به نقض یکپارچگی سیستم از راه دور با نیت مخرب می‌پردازند.
- ✓ همچنین آنها به عنوان یک هکر غیراخلاقی یا یک کراکر امنیتی شناخته می‌شوند. آنها بر کرک امنیت و سرقت داده‌ها تمرکز دارند.

**هکر کلاه خاکستری**[3]

[1] White Hat Hacker

[2] Black Hat Hacker

[3] Grey Hat Hacker

- ✓ هکر کلاه خاکستری، یک فرد کامپیوتری است که گاهی به صورت قانونی و با اراده‌ی خوب فعالیت می‌کند و گاه این چنین فعالیت نمی‌کند. آنها معمولا برای منافع شخصی یا با داشتن نیت مخرب هک نمی‌کنند؛ هرچند، ممکن است در طول دوره‌ی بهره‌برداری از فناوری‌ها، جرائمی را نیز مرتکب شوند.
- ✓ آنها ترکیبی بین هکرهای کلاه سفید و هکرهای کلاه سیاه هستند.

## مهندسی اجتماعی چیست ؟

- عمل فریب و ترغیب افراد به انجام اقدامات یا افشای اطلاعات محرمانه را *مهندسی اجتماعی*[1] می‌گویند. در مهندسی اجتماعی، نفوذ به هدف یا شکستن سیستم با استفاده از تکنیک‌های فنی کرک صورت نمی‌گیرد، بلکه مهندس اجتماعی تنها با حیله‌گری و تعامل با قربانیان، آنها را به افشای اطلاعاتشان، ترغیب می‌کند. در بیشتر موارد مهندس اجتماعی (نفوذگر) با قربانی چهره به چهره قرار نمی‌گیرد.
- "مهندسی اجتماعی" به‌عنوان عملی از روش‌های روانشناسی توسط هکر مشهور دنیا به نام Kevin Mitnick رایج شد. این اصطلاح پیش‌تر در علوم اجتماعی مطرح بود اما امروزه در علم هک و امنیت نیز کاربرد دارد.
- مثال1: یک پست الکترونیکی دریافت می‌کنید که در آن فرستنده، خود را به‌جای مدیر یا شخصی به نمایندگی او و یا پرسنلی از بخش پشتیبانی بانک‌تان جا می‌زند. در پیام او اشاره می‌شود که سرویس بانکداری آنلاین با مشکل رو به رو است و این مشکل می‌تواند با دانلود و اجرای برنامه‌ای که در پست الکترونیکی پیوست شده است، رفع شود. با اجرای این برنامه، یک صفحه همانند آن صفحه‌ای که برای دسترسی به حساب بانک‌تان از آن استفاده می‌کنید، آشکار می‌شود. شما گذرواژه‌ی خود را تایپ می‌کنید و در حقیقت، این برنامه آماده می‌شود تا به سرقت گذرواژه‌تان برای دسترسی به حساب بانکی توسط نفوذگر بپردازد.
- مثال2: یک پست الکترونیکی دریافت می‌کنید که در آن آمده است که کامپیوترتان به یک ویروس آلوده شده است. در این پیام پیشنهاد شده که برای از بین بردن ویروس، نرم‌افزار ضد-ویروس را که پیوست پست الکترونیکی است، دانلود و نصب نمایید. با نصب این نرم‌افزار، نه تنها ویروس از بین نمی‌رود، بلکه اطلاعات محرمانه‌تان برای نفوذگر ارسال می‌شود.
- یک غریبه به شماره تلفن خانه‌تان تماس می‌گیرد و اذعان می‌دارد که پرسنل بخش پشتیبانی‌فنی مرکز ارائه دهنده‌ی سرویس اینترنت (ISP) است. در این ارتباط، او می‌گوید که اتصال‌تان با اینترنت با مشکل رو به رو شده است و برای رفع آن، از شما درخواست گذرواژه‌تان را دارد. چنانچه گذرواژه‌ی خود را به این غریبه بدهید، او می‌تواند اقدامات بسیار مخربی را با نام شما، انجام دهد.

[1] Social Engineering

- روش‌های مهندسی اجتماعی عبارت‌اند از: Phishing (روش متقلبانه‌ی به‌دست آوردن اطلاعات خصوصی، Vishing (روش بهره‌برداری غیرمجاز از سیستم‌های تلفن گویا)، Baiting (نصب بدافزارها به روی فلاپی‌ها، لوح‌های فشرده یا فلش درایوهای USB برای نصب به روی دستگاه‌های قربانیان به منظور سرقت اطلاعات از روی کنجکاوی نفوذگر) و Quid pro quo (به معنای چیزی برای چیزی است و اشاره دارد به این مثال که فرد با قربانی تماس می‌گیرد و از او می‌خواهد که دستورها را همان موقع اجرا کند. در این مثال، مهندس اجتماعی، افزون بر فریب قربانی، از او می‌خواهد که دستورهای او را نیز قربانی به اجرا گذارد.)

## هک اخلاقی

- ❖ هک اخلاقی[1]، تست منابع با هدفی خیرخواهانه و برای بهبود فناوری است. هک اخلاقی به طور فنی به معنی تست نفوذی است که بر روی ایمن‌سازی و حفاظت از سیستم‌های IT تمرکز می‌کند.
- ❖ هک اخلاقی، فرایند یافتن و بهره‌برداری از آسیب‌پذیری‌ها در سیستم و سپس اصلاح آنها برای مقابله با هکرها می‌باشد.

## Hacktivism

- ❖ نوع دیگری از هکرها، Hacktivistها هستند که تلاش در انتشار پیام‌های سیاسی یا اجتماعی دارند. یک Hacktivist می‌خواهد که آگاهی عمومی نسبت به یک موضوع افزایش پیدا کند.

## Cyber Terrorist

- ❖ این هکرها که تروریس‌های سایبری نامیده می‌شوند کسانی هستند که به کامپیوترهای دولتی یا زیرساخت‌های منافع عمومی مانند نیروگاه‌ها و برج‌های کنترل ترافیک هوایی، حمله می‌کنند. آنها سیستم‌های بحرانی را خراب می‌کنند و یا اطلاعات طبقه‌بندی شده‌ی دولتی را به سرقت می‌برند. در یک درگیری با کشورهای دشمن، برخی از دولت‌ها از طریق اینترنت جنگ سایبری را آغاز می‌کنند.

## هکرها چرا هک می‌کنند؟

- ❖ دلیل اصلی اینکه چرا هکرها هک می‌کنند این است که آنها می‌توانند هک کنند. هک یک سرگرمی گاه به گاه برای برخی از هکرهاست – آنها تنها هک می‌کنند تا ببینند می‌توانند هک کنند یا خیر و معمولا توسط سیستم‌های خود تست می‌کنند. بسیاری از هکرها، افرادی هستند که از شرکت‌ها و یا بخش IT دولتی و سازمان‌های امنیتی اخراج شده‌اند. آنها تلاش می‌کنند وضعیت سازمان را با حمله یا سرقت اطلاعات به ارمغان بیاورند.

[1] Ethical Hacking

❖ دانشی که هکرهای مخرب کسب می‌کنند و نفسی که همراه این دانش است مانند اعتیاد است. برخی از هکرها می‌خواهند زندگی کاربری را نابود سازند و برخی دیگر به سادگی می‌خواهند معروف شوند. برخی از انگیزه‌های رایج هکرهای مخرب، انتقام، حس کنجکاوی، خستگی، به چالش کشاندن، سرقت برای سود مالی، باج‌گیری، اخاذی و فشار کاری به شرکت‌های بزرگ می‌باشد.

## پارامترهای بنیادی امنیت

زمانی می‌توان گفت به شبکه‌ای حمله شده است که یکی از پارامترهای بنیادی امنیت زیر با اختلال روبه‌رو شود:

- محرمانه ماندن اطلاعات (Confidentiality)
- صحت و یکپارچگی اطلاعات (Integrity)
- در دسترس بودن اطلاعات (Availability)
- احراز هویت (Authentication)
- کنترل دسترسی (Access Control)

## جلوگیری از نفوذ هکرها

برای جلوگیری از پیدا کردن حفره‌های جدید در نرم‌افزار و بهره‌برداری از آنها توسط هکرها، چه باید کرد؟

❖ تیم‌های تحقیقاتی امنیت اطلاعات وجود دارد – به منظور تلاش برای یافتن این حفره‌ها و اطلاع به صاحبان کالاها (یا فروشندگان) پیش از اینکه آنها مورد بهره‌برداری قرار گیرند. رقابت مفیدی بین هکرهایی که سیستم‌ها را تأمین امنیت می‌کنند و هکرهایی که این سیستم‌ها را نقض می‌کنند، رخ داده است. این رقابت، ما را با امنیت بهتر و قوی‌تر و همچنین تکنیک‌های پیچیده‌تر حمله آشنا می‌سازد.

❖ هکرهای مدافع، سیستم‌های تشخیص را برای پیگیری حمله‌های هکرها ایجاد می‌کنند؛ درحالی که هکرهای تهاجمی تکنیک‌های دور زدن را توسعه می‌دهند و در آخر، سیستم‌های تشخیص و پیگیری، بهتر نتیجه می‌دهند. نتیجه‌ی این تعامل به عنوان پرورش افراد باهوش، بهبود امنیت، ثبات بیشتر در نرم‌افزارها، خلق تکنیک‌های حل مشکل و حتی یک اقتصاد جدید می‌تواند مثبت باشد.

❖ یک هکر اخلاقی دارای مهارت، تفکر و ابزارهای هکرها می‌باشد اما قابل اعتماد است. هکرهای اخلاقی، هک را به عنوان تست امنیتی سیستم‌های کامپیوتری انجام می‌دهند.

- هک اخلاقی – که با عنوان تست نفوذ[1] یا هک کلاه سفید نیز شناخته می‌شود – شامل همان ابزارها، ترفندها و تکنیک‌هایی است که هکرها استفاده می‌کنند اما با یک تفاوت‌عمده: هک اخلاقی، قانونی است.
- هک اخلاقی، با اجازه‌ی صاحب هدف انجام می‌شود. هدف از هک اخلاقی، کشف آسیب‌پذیری‌ها از منظر یک هکر است. بنابراین سیستم می‌تواند بهتر امن شود. هک‌اخلاقی بخشی از کل یک برنامه‌ی مدیریت ریسک اطلاعات است که اجازه می‌دهد بهبود وضعیت امنیتی انجام شود. همچنین هک اخلاقی می‌تواند اطمینان دهد که ادعای فروشندگان درباره‌ی امنیت کالاهای‌شان قانونی است.
- همان‌گونه که هکرها دانش خود را گسترش می‌دهند، شما نیز باید دانش خود را افزایش دهید. باید بیاندیشید مانند آنچه که هکرها برای محافظت از سیستم‌های خود فکر می‌کنند. شما به عنوان یک هکر اخلاقی باید اقدامات انجام شده‌ی هکرها و چگونگی خنثی کردن تلاش‌هایشان را بدانید.
- لازم نیست که از سیستم‌تان در برابر هر چیزی محافظت کنید، چون که نمی‌توانید این کار را انجام دهید.

تنها روش حفاظت در برابر هر چیزی، جدا کردن سیستم کامپیوترتان و قفل کردن آن و گذاشتن آن در جایی دور است که هیچ کس نتواند آن را لمس کند.

- رویکرد بالا، بهترین رویکرد برای امنیت اطلاعات نیست. آنچه که مهم است حفاظت از سیستم خود از آسیب‌پذیری‌های شناخته شده و حمله‌های رایج هکرهاست.
- چیرگی بر همه‌ی آسیب‌پذیری‌های احتمالی سیستم‌تان ممکن نیست. نمی‌توانید برای تمام حمله‌های احتمالی برنامه‌ریزی کنید – به‌ویژه آن حمله‌هایی که اینک ناشناخته است و در اصطلاح به آن اکسپلویت‌های Zero Day می‌گویند. اینها حمله‌هایی هستند که در جهان شناخته نشده‌اند. هرچند، در هک اخلاقی، ترکیب‌های بیشتری را امتحان می‌کنید – بیشتر به تست کل سیستم‌ها به‌جای آزمایش تک تک واحدهای فردی بپردازید – در این صورت شانس‌تان برای کشف آسیب‌پذیری‌ها افزایش پیدا می‌کند.

[1] Penetration Testing

## مراحل انجام شده توسط هکرها


1. شناسایی[1]
2. پویش[2]
3. کسب دسترسی[3]
4. حفظ دسترسی[4]
5. پاک کردن رد پا[5]

***فاز 1: شناسایی***

- ✓ شناسایی را می‌توان به‌عنوان فاز پیش از حمله توصیف نمود و این فاز، یک تلاش سیستماتیک برای جست‌وجو، گردآوری، شناسایی و ثبت اطلاعات درباره‌ی هدف می‌باشد.

***فاز 2: پویش و شمارش***

- ✓ پویش و شمارش[6]، فاز دوم پیش از حمله در نظر گرفته می‌شود. این فاز شامل مصرف اطلاعات کشف شده در طول فاز شناسایی و استفاده از آن برای بررسی شبکه می‌باشد. پویش شامل مراحلی همچون پویش هوشمند پورت سیستم است که برای تعیین پورت‌های باز سرویس‌های آسیب‌پذیر مورد استفاده قرار می‌گیرد. در این مرحله نفوذگر می‌تواند از ابزارهای مختلف خودکار برای کشف آسیب‌پذیری‌های سیستم استفاده نماید.

***فاز 3: کسب دسترسی***

- ✓ این فاز، فازی است که در آن هک واقعی شکل می‌گیرد. آسیب‌پذیری‌های کشف شده در طول فاز شناسایی و پویش، اکنون برای کسب دسترسی، مورد بهره‌برداری قرار می‌گیرد. روش اتصال هکر برای استفاده از اکسپلویت می‌تواند در یک شبکه‌ی محلی، دسترسی محلی به یک کامپیوتر شخصی یا به‌صورت آفلاین باشد. کسب دسترسی در دنیای هکرها به‌عنوان مالکیت بر سیستم شناخته می‌شود. در طول یک نقض امنیتی واقعی، هکر می‌تواند به سادگی از روش‌هایی برای آسیب رساندن جبران‌ناپذیر به سیستم هدف، استفاده کند.

---

[1] Reconnaissance

[2] Scanning

[3] Gaining Access

[4] Maintaining Access

[5] Clearing Tracks

[6] Enumeration

***فاز 4: حفظ دسترسی و قرار دادن درب پشتی***[1]

- ✓ هنگامی که یک هکر کسب دسترسی می‌کند، او می‌خواهد که دسترسی را برای بهره‌برداری و حمله‌های بیشتر نگه دارد. گاهی، هکرها با ایمن‌سازی یکتای دسترسی خود با درب‌های پشتی، Root kitها و تروجان[2]ها، دسترسی را برای دیگر هکرها یا پرسنل امنیتی سخت می‌کنند.
- ✓ نفوذگر می‌تواند از اسکریپت‌های خودکار و ابزار اتوماتیک برای پنهان کردن شواهد حمله و همچنین برای ایجاد درب پشتی برای حمله‌های بیشتر، استفاده کند.

***فاز 5: پاک کردن رد پا***

- ✓ در این فاز، هکر قادر به کسب و حفظ دسترسی است و او باید برای جلوگیری از تشخیص توسط پرسنل امنیتی، ادامه‌ی استفاده از سیستم تحت تسلط، حذف شواهد و مدارک هک و یا برای جلوگیری از اقدامات قانونی، رد پای خود را پاک کند. هم‌اینک، بسیاری از رخنه‌های امنیتی موفق به‌وجود آمده‌اند اما هرگز تشخیص داده نشده‌اند.

## شروع به کار یک هکر اخلاقی

- **رعایت دستورهای هک اخلاقی**:

- ✓ هر هکر اخلاقی باید چند اصل پایه را دنبال کند. بیشتر وقت‌ها به این اصول توجه می‌شود و یا ممکن است در هنگام برنامه‌ریزی یا اجرای تست هک اخلاقی، فراموش شوند.

- **اخلاقی کار کردن**:

- ✓ واژه‌ی اخلاقی یا ethical می‌تواند به‌عنوان کار کردن با اصول و اخلاق حرفه‌ای بالا تعریف شود. اینکه آیا تست هک اخلاقی را در برابر سیستم‌تان انجام می‌دهید یا برای این کار، کسی را استخدام کرده‌اید. هر چیزی که به‌عنوان هکر اخلاقی انجام می‌دهید باید مورد تأیید و پشتیبانی اهداف شرکت باشد. هیچ دستور کار پنهانی اجازه داده نمی‌شود! اعتماد هدف نهایی است. سوء استفاده از اطلاعات به‌هیچ وجه مجاز نیست.

- **احترام به حریم خصوصی**:

- ✓ اطلاعاتی که با احترام کامل در طول تست گردآوری کرده‌اید – از فایل‌های لاگ برنامه‌کاربردی وب تا گذرواژه‌های متن واضح – باید خصوصی نگه داشته شود.

- **خراب نکردن سیستم تان**:

- ✓ یکی از بزرگ‌ترین اشتباه‌ها هنگامی به‌وجود می‌آید که افراد تلاش می‌کنند سیستم خود را هک کنند؛ آنها به خراب کردن سیستم خود می‌پردازند. دلیل اصلی برای این کار، برنامه‌ریزی

---

[1] Backdoor

[2] Trojan

ضعیف است. این تست کننده‌ها، یا اسناد را نخوانده‌اند و یا در طرز استفاده و قدرت ابزارهای امنیتی و تکنیک‌ها دچار سوءتفاهم شده‌اند.

- ✓ می‌توانید به سادگی در هنگام تست بر روی سیستم‌تان، شرایط بیچاره کننده‌ای را ایجاد کنید. اجرای بیش از حد بسیاری از تست‌ها با سرعت بالا به روی سیستم، موجب هنگ کردن سیستم می‌شود. هرچند، بسیاری از ابزارهای ارزیابی امنیتی می‌توانند چگونگی برخی از تست‌های انجام شده به روی سیستم را کنترل کنند. این ابزارها چنانچه نیاز به اجرای تست به روی سیستم‌های تولیدی در طول ساعت‌های کسب و کار (به طور منظم) داشته باشد، ویژگی خاصی را برایتان فراهم می‌کند.

**اجرای پلان:**

- ✓ در هک اخلاقی، زمان و صبر مهم است. در هنگام انجام تست هک اخلاقی مراقب باشید. یک هکر در شبکه‌تان یا یک کارمند در کنارتان ممکن است به تماشای آنچه که انجام می‌دهید پرداخته باشد. این شخص می‌تواند از این اطلاعات بر علیه‌تان استفاده کند. پیش از شروع مطمئن شوید که هیچ هکری به روی سیستم‌تان، ننشسته باشد. تنها اطمینان حاصل کنید که همه چیز را آرام و خصوصی نگه دارید.
- ✓ ارسال و ذخیره‌ی نتایج تست‌تان بسیار مهم است. شما اکنون مأموریت شناسایی دارید. پیدا کردن اطلاعات به‌هر اندازه‌ای در مورد سازمان و سیستم‌هایتان همان چیزی است که هکرهای مخرب انجام می‌دهند. با یک دید ذهنی گسترده و دقیق، تمرکزتان را آغاز کنید. برای به‌دست آوردن نام سازمان خود، اسامی سیستم شبکه و کامپیوترهای خود و آدرس‌های IP، به‌روی اینترنت جست‌وجو نمایید. Google بهترین محل برای آغاز این کار است.

## 1-2 واژگان فنی

توانایی درک و تعریف اصطلاحات هک، بخش مهمی از مسئولیت یک هکر اخلاقی یا قانونمند است. در این بخش، در مورد برخی از اصطلاح‌های رایج در دنیای هک آشنا می‌شوید.

- تهدید (threat): شرایط یا حالتی است که می‌تواند امنیت را مختل کند. هکرهای اخلاقی، زمانی که تحلیل امنیتی انجام می‌دهند، تهدیدها را اولویت‌بندی می‌کنند.
- اکسپلویت (exploit): قطعه‌ای از نرم‌افزار، ابزار، کد مخرب یا تکنیک است که به نفوذگر اجازه می‌دهد تا به طور خودکار، داخل سیستم را بشکند و از آن بهره‌برداری کند.
- آسیب‌پذیری (vulnerability): وجود ضعفی در طراحی یا پیاده‌سازی نرم‌افزار سیستم است. با پیاده‌سازی صحیح و اقدامات امنیتی، آسیب‌پذیری‌ها کاهش می‌یابند.
- هدف ارزیابی (target of evalution): سیستم، برنامه یا شبکه‌ای است که مورد حمله یا ارزیابی امنیتی قرار می‌گیرد.

- حمله (attack): زمانی رخ می‌دهد که سیستمی به خاطر آسیب‌پذیری‌ها، به خطر می‌افتد. بسیاری از حمله‌ها با استفاده از اکسپلویت‌ها، بهره‌برداری می‌شوند.
- TCP/IP[1]: پروتکل کنترل انتقال/پروتکل اینترنت، زبان اینترنت است. یکی از مهم‌ترین ویژگی‌های TCP/IP، پروتکل "باز" آن می‌باشد و هر کسی که مایل باشد می‌تواند آزادانه این پروتکل را پیاده‌سازی نماید.
- پروتکل اینترنت (IP): پروتکل اصلی ارتباط است که برای انتقال دیتاگرام (که به بسته‌های شبکه نیز شناخته می‌شود) در سراسر internetwork با استفاده از مجموعه‌ی پروتکل‌اینترنت که مسئولیت مسیریابی بسته‌های اطلاعاتی در شبکه را دارد، مورد استفاده قرار می‌گیرد. IP، پروتکلی اولیه است که اینترنت را ایجاد کرده است. در تعریفی دیگر، IP، پروتکل "لایه شبکه" می‌باشد. این لایه اجازه می‌دهد تا در واقع میزبان‌ها با یکدیگر صحبت کنند. چنین چیزی داده‌ها را حمل کرده، آدرس اینترنت را به آدرس فیزیکی شبکه نگاشت کرده و مسیریابی می‌کند.
- پورت (port): در حوزه‌ی شبکه‌های کامپیوتری، Port، برنامه‌ی خاص یا فرایند ویژه نرم‌افزاری است که سرویسی را به‌عنوان یک درگاه ارتباطی در سیستم‌عامل میزبان کامپیوتر، ایجاد می‌کند. Port با آدرس IP میزبان در ارتباط است و همچنین نوعی از پروتکل است که برای ارتباطات مورد استفاده قرار می‌گیرد. هدف پورت‌ها، شناسایی یکتای برنامه‌های مختلف یا فرایندهای در حال اجرا به روی کامپیوتری واحد و در نتیجه قادر ساختن آنها برای به اشتراک گذاری اتصال فیزیکی واحد به بسته‌ی سوئیچ شده‌ی شبکه، مانند اینترنت است.
- کلاینت (Client): برنامه یا سیستمی است که به سرویسی که توسط سرور در دسترس، ساخته شده است، دسترسی پیدا می‌کند. به بیان بسیار ساده‌تر، مثلا به کاربری که یک وب‌سایت را مشاهده می‌کند و یا از سرویس‌های آن استفاده می‌کند، کلاینت یا سرویس‌گیرنده می‌گویند.
- سرور (Server): سیستمی است که به درخواست‌ها برای ارائه یا کمک به ارائه‌ی یک سرویس شبکه در سراسر شبکه‌ی کامپیوتری، پاسخ می‌دهد. به بیان بسیار ساده‌تر، مثلا به وب‌سایتی که یک سرویسی را به کاربر ارائه می‌دهد، سرور یا سرویس‌دهنده می‌گویند.

## 3-1 هک آدرس پست الکترونیکی

### پست الکترونیکی چگونه کار می‌کند؟

❖ ارسال و دریافت پست الکترونیکی[2] توسط سرور پست الکترونیکی کنترل می‌شود. تمام ارائه دهندگان سرویس پست الکترونیکی، پیش از اینکه هر کسی به حسابش وارد شود و آغاز به برقراری ارتباط دیجیتالی کند، سرور پست الکترونیکی (Email Server) را پیکربندی می‌کنند.

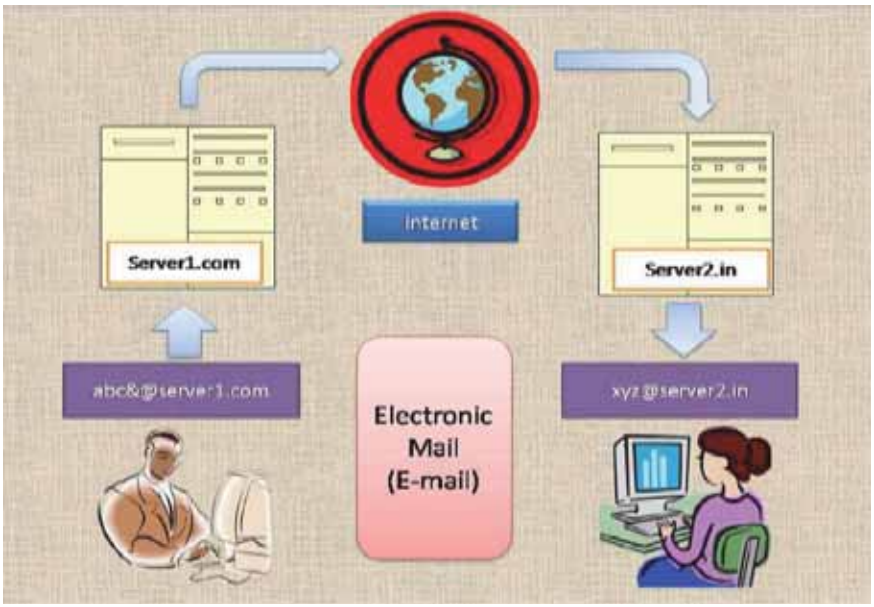
[1] Transport Control Protocol/Internet Protocol

[2] Email

- هنگامی که سرور آماده شد، کاربران از سراسر جهان در این سرورهای پست الکترونیکی ثبت‌نام می‌کنند و یک حساب کاربری راه‌اندازی می‌کنند. برای استفاده‌ی کامل از سرویس پست الکترونیکی، کاربران می‌بایست به حساب خود وارد شوند.

## مسیر حرکت پست الکترونیکی

- اجازه دهید با یک مثال بگوییم که ما دو ارائه دهنده‌ی پست الکترونیکی یا ایمیل داریم. یکی Server1.com و دیگری server2.in، و ABC کاربری است که در Server1.com ثبت نام کرده است و XYZ کاربری است که در Server2.in ثبت نام کرده است.
- ABC به حساب پست الکترونیکی خود در Server1.com وارد می‌شود. سپس او یک پست برای xyz@server2.in نوشته و به روی دکمه‌ی Send کلیک می‌کند و سپس پیامی را مبنی بر ارسال موفقیت پست الکترونیکی دریافت می‌کند.
- اما آنچه که پشت پرده اتفاق می‌افتد چیست؟ پست الکترونیکی از کامپیوتر abc@server1.com به سرور پست الکترونیکی Server1.com فوروارد می‌شود. سپس Server1 به جست‌وجوی Server2.in به روی اینترنت می‌پردازد و پست الکترونیکی را به server2.in برای حساب XYZ فوروارد می‌کند. Server2.in پست الکترونیکی را از Server1.com دریافت می‌کند و آن را در حساب XYZ قرار می‌دهد.
- سپس XYZ وارد آدرس پست الکترونیکی خود شده و پیام‌ها را در صندوق ورودی پست‌الکترونیکی خود مشاهده می‌کند.



## پروتکل‌های سرویس پست الکترونیکی

### SMTP

- SMTP مخفف Simple Mail Transfer Protocol است. SMTP زمانی مورد استفاده قرار می‌گیرد که: 1) پست‌الکترونیکی از سرویس‌گیرنده‌ی[1] پست‌الکترونیکی مانند Outlook Express به سرویس‌دهنده‌ی[2] پست‌الکترونیکی تحویل داده شود و یا 2) هنگامی که پست‌الکترونیکی از یک سرویس‌دهنده‌ی پست‌الکترونیکی به دیگر سرویس‌دهنده‌ی پست‌الکترونیکی تحویل داده شود. SMTP از پورت 25 استفاده می‌کند.

### POP3

- POP3 مخفف Post Office Protocol است. POP3 اجازه می‌دهد که یک سرویس‌گیرنده‌ی پست الکترونیکی، یک پست‌الکترونیکی را از سرویس‌دهنده دانلود کند. پروتکل POP3 ساده است و بسیاری از ویژگی‌ها را به جز ویژگی دانلود، فراهم نمی‌کند. این پروتکل با این فرض طراحی شده است که سرویس‌گیرنده‌ی پست‌الکترونیکی تمام پست‌های‌الکترونیکی در دسترس را از سرویس دهنده دانلود نماید و آنها را از سرویس‌دهنده یا سرور حذف کند و سپس ارتباط را قطع کند. POP3 معمولا از پورت 110 استفاده می‌کند.

### IMAP

- IMAP مخفف Internet Message Access Protocol است. IMAP بسیاری از ویژگی‌های مشابه POP3 را به اشتراک می‌گذارد. این پروتکل، پروتکلی است که سرویس‌گیرنده‌ی پست الکترونیکی می‌تواند برای دانلود پست الکترونیکی از سرویس‌دهنده‌ی پست‌الکترونیکی، استفاده کند. هرچند، ویژگی‌های IMAP بسیار بیشتر از POP3 است. پروتکل IMAP طراحی شده است تا به کاربران اجازه دهد که پست الکترونیکی خود را به روی سرور یا سرویس‌دهنده نگه دارند. IMAP نیاز به فضای دیسک بیشتری به روی سرور و منابع بیشتری از CPU نسبت به POP3 دارد، در حالی که پست‌های الکترونیکی به روی سرور ذخیره می‌شوند. IMAP معمولا از پورت 143 استفاده می‌کند.

## پیکربندی سرور پست الکترونیکی

- نرم‌افزارهای سرور پست الکترونیکی مثل Post cast Server، Hmailserver، Surge mail و... می‌توانند برای تبدیل کامپیوتر شخصی‌تان به یک سرور ارسال پست‌الکترونیکی مورد استفاده قرار گیرد.
- HMailServer، یک سرور پست الکترونیکی برای سیستم‌عامل Windows است. این نرم‌افزار اجازه می‌دهد که تمام پست‌های الکترونیکی‌تان را بدون نیاز به ISP (ارائه دهنده‌ی سرویس

[1] Client

[2] Server

اینترنت) برای مدیریت آن، اداره نمایید. HMailServer انعطاف‌پذیری، امنیت و کنترل کامل بر حفاظت از اسپم‌ها را فراهم می‌کند.

## امنیت پست الکترونیکی

- اینک اجازه دهید به بررسی امنیت پست الکترونیکی بپردازیم. حمله‌های بسیاری وجود دارد که به روی پست‌های الکترونیکی اجرا می‌شود. افرادی هستند که استادان این چنین حمله‌هایی هستند و همیشه دنبال کاربرانی هستند که از این ترفندهای پست الکترونیکی آگاه نیستند.
- باید مطمن شوید که یک هدف آسان برای این دسته از هکرها نیستید. باید پروفایل و هویت پست الکترونیکی خود را ایمن کنید و از خودتان، یک هدف دشوار بسازید.
- اگر یک شناسه‌ی پست الکترونیکی دارید که احساس می‌کنید هیچ وقت هک نمی‌شود به این دلیل که هیچ اطلاعات مهمی در آن ندارید، سخت در اشتباهید؛ چون نمی‌دانید که هکرها با دانستن گذرواژه‌ی پست الکترونیکی‌تان قادر خواهند بود تهدیدهایی را به وزارت‌خانه‌ها و یا کانال‌های خبری از طریق پست الکترونیکی ارسال نمایند.
- نفوذگر، اطلاعات درون پست الکترونیکی‌تان را مورد آزار قرار نمی‌دهد. او تنها یک قربانی شناسه‌ی پست الکترونیکی می‌خواهد تا در حمله‌ی خود، از آن استفاده کند. روش‌های بسیاری وجود دارد که با آن می‌توان از پست الکترونیکی شما در راه‌های غلط استفاده کرد.

## جعل پست الکترونیکی[1]

- جعل پست الکترونیکی[2]، جعل هدر پست الکترونیکی است؛ به‌گونه‌ای که به نظر برسد پیام از شخص یا محلی دیگر غیر از مبداء واقعی، نشأت گرفته شده است. توزیع کننده‌ی اسپم‌ها اغلب از جعل یا Spoofing استفاده می‌کنند تا گیرندگان، پست‌های الکترونیکی را باز کنند.
- راه‌های بسیاری برای ارسال یک پست الکترونیکی جعلی حتی بدون دانستن گذرواژه‌ی شناسه‌ی پست الکترونیکی وجود دارد. اینترنت به‌گونه‌ای آسیب‌پذیر است که می‌توانید از شناسه‌ی پست‌الکترونیکی هر شخصی برای ارسال پست‌های تهدیدآمیز به کاربران دیگر، استفاده کنید.

## روش‌های ارسال پست الکترونیکی جعلی

- Open Relay Server
- Web Script

[1] Email Spoofing

[2] برای اطلاعات بیشتر رجوع کنید به: کتاب "در جستجوی امنیت"، علی اصغر جعفری لاری، ص 148

## پست الکترونیکی جعلی: به‌وسیله‌ی Open Relay Server

- Open Mail Relay، یک سرور SMTP است که به شیوه‌ای پیکربندی شده تا به هر شخصی در اینترنت اجازه دهد پست الکترونیکی را از طریق آن، ارسال کند.
- یک نفوذگر می‌تواند به‌وسیله‌ی Telnet به Open Relay Server متصل شود و برای ارسال پست الکترونیکی، به سرور دستور دهد.
- Open Relay Email Server نیاز به هیچ گذرواژه‌ای برای ارسال پست الکترونیکی ندارد.

## پست الکترونیکی جعلی: به‌وسیله‌ی Web Script

- زبان‌های برنامه‌نویسی وب مانند PHP و ASP حاوی توابع ارسال پست الکترونیکی هستند که از آن می‌توان برای ارسال پست الکترونیکی با هدرهای جعلی برنامه‌نویسی استفاده کرد. برای نمونه "From: To: Subject: "
- در اینترنت وبسایت‌های بسیاری در دسترس است که دارای این اسکریپت‌های ارسال پست الکترونیکی می‌باشند. بیشتر آنها یک سرویس رایگان را ارائه می‌دهند.
- دو وب‌سایت زیر سرویس ارسال پست الکترونیکی جعلی را فراهم می‌کنند:

http: //www.fakemailer.net
http: //www.deadfake.com

**اسکریپت PHP ارسال پست الکترونیکی :**

```php
<?php
$to      = 'nobody@example.com';
$subject = 'the subject';
$message = 'hello';
$headers = 'From: webmaster@example.com' . "\r\n" .
    'Reply-To: webmaster@example.com' . "\r\n" .
    'X-Mailer: PHP/' . phpversion();

mail($to, $subject, $message, $headers);
?>
```

## نمونه‌هایی از پیامدهای پست الکترونیکی جعلی

- اعلام انفجار بمب از شناسه‌ی پست الکترونیکی‌تان به آژانس امنیتی می‌تواند باعث شود که باقی عمرتان را پشت میله‌های زندان بگذرانید.
- تقاضای استعفا یا هر درخواست دیگر به رئیس شرکت از شناسه‌ی پست الکترونیکی‌تان طوری که رئیس شرکت فکر کند شما این درخواست را داشته‌اید.

## اثبات یک پست الکترونیکی جعلی

- هر پست الکترونیکی یک سربرگ یا هدر[1] را حمل می‌کند که در آن اطلاعاتی درباره‌ی مسیر حرکت پست الکترونیکی قرار دارد.
- بررسی هدر و دریافت محلی که پست الکترونیکی فرستاده شده است.
- بررسی پست الکترونیکی فرستاده شده از هر وب‌سایت یا سرور پست الکترونیکی.
- هدرها نام وب‌سایتی را حمل می‌کنند که در آن اسکریپت ارسال پست الکترونیکی مورد استفاده قرار گرفته است.

## بمباران پست الکترونیکی

- بمباران پست الکترونیکی[2]، ارسال انبوه پیام پست الکترونیکی به یک نشانی خاص می‌باشد. در بسیاری از موارد، پیام‌ها، انبوه و از اطلاعات بی‌معنا ساخته شده‌اند که در تلاش است منابع شبکه و سیستم‌ها را مصرف کند.

## هرز نامه‌های پست الکترونیکی

- هرزنامه‌های پست الکترونیکی[3] یا اسپم‌ها گونه‌ای بمباران پست الکترونیکی است که به ارسال پست الکترونیکی به صدها یا هزاران کاربر اشاره دارد. اگر گیرنده‌ی هرزنامه به آن پاسخ دهد، هرزنامه‌های پست الکترونیکی می‌تواند پیامدهای بدتری هم داشته باشد؛ چراکه با این کار، تمام مخاطبان اصلی، پاسخ او را دریافت می‌کنند، با اینکه ممکن است او اطلاعی از این موضوع نداشته باشد اما باعث شود صدها یا هزاران کاربر پاسخ او را همچون هرزنامه‌ها دریافت کنند.

## هک گذرواژه‌ی آدرس پست الکترونیکی

- هیچ حمله‌ی مشخص شده‌ای تنها برای هک گذرواژه‌ی حساب‌های پست الکترونیکی وجود ندارد. همچنین، به خطر انداختن سرورهای پست الکترونیکی همچون Yahoo، Gmail و... کار ساده‌ای نیست.
- هک گذرواژه‌ی آدرس پست الکترونیکی می‌تواند به‌وسیله‌ی برخی از حمله‌های سمت سرویس گیرنده انجام شود. نفوذگران تلاش می‌کنند که کاربر را به خطر انداخته و گذرواژه‌ی حساب پست‌الکترونیکی او را پیش از رسیدن به سرور پست الکترونیکی مورد نظر به‌دست آورند.

---

[1] Header

[2] Email Bombing

[3] Email Spamming

## فیشینگ[1]

- عمل فرستادن پست الکترونیکی با ادعای دروغ به کاربر، برای تسلیم اطلاعات خصوصی اوست که در سرقت هویت مورد استفاده قرار می‌گیرد. برای نمونه، نفوذگر با ارسال یک پست الکترونیکی با مضمون تأسیس یک شرکت قانونی، تلاش می‌کند تا به کلاه‌برداری مبادرت ورزد و اطلاعات شخصی و خصوصی افراد را برای سرقت هویت آنان مورد استفاده قرار دهد.
- یک پست الکترونیکی، کاربر را به مشاهده‌ی یک وب‌سایت که در آن اطلاعات شخصی همچون گذرواژه و شماره حساب‌های بانکی پرسیده می‌شود، هدایت می‌کند. هرچند، وب‌سایت ساختگی تنها برای سرقت اطلاعات کاربر راه‌اندازی شده است.


معمولا هکر برای پیاده‌سازی حمله‌ی فیشینگ، یک صفحه‌ی تقلبی را می‌سازد یا از اینترنت دانلود می‌کند. این صفحه‌ی تقلبی می‌تواند صفحه‌ی ورود به پست الکترونیکی سرویس Yahoo، Gmail، Hotmail و. . . باشد یا صفحات ورود به شبکه‌های اجتماعی و یا بدتر از آن، درگاه‌های پرداخت آنلاین بانک‌ها باشد. پس از ورود کاربر به این صفحات تقلبی، کاربر با این فرض که به سایت اصلی متصل شده است،

[1] Phishing

اطلاعات خود را وارد می‌کند. در اینجاست که هکر اطلاعات کاربر را به‌دست می‌آورد و کاربر، قربانی فریب هکر شده است.[1]

**کلاه برداری فیشینگ می‌تواند. . .**

- یک پست الکترونیکی باشد که شما را به پیوستن به یک گروه اجتماعی با پرسیدن نام کاربری و گذرواژه‌ی ورود، دعوت کند.
- یک پست الکترونیکی باشد که اذعان می‌دارد حساب بانکی شما قفل شده است و برای بازگشایی آن، باید دوباره وارد آن شوید.
- یک پست الکترونیکی باشد که حاوی برخی از اطلاعات مورد علاقه‌تان باشد و از شما درخواست کند تا به حسابتان وارد شوید.
- هر پست الکترونیکی باشد که یک لینک برای کلیک و درخواست برای ورود را با خود به همراه داشته باشد.


## پیشگیری در برابر فیشینگ

- تمام پست‌های الکترونیکی را با دقت بخوانید و فرستنده‌ی اصلی را بررسی کنید.
- لینک‌ها را پیش از کلیک کردن به روی آن، با دقت ببینید.
- پیش از ورود به حسابتان، همیشه URL (آدرس) را در مرورگر بررسی کنید.
- همیشه پس از باز کردن وب‌سایت‌های مورد اعتماد، نه با کلیک در هر پست‌الکترونیکی یا وبسایت‌های دیگر، به حسابتان وارد شوید.

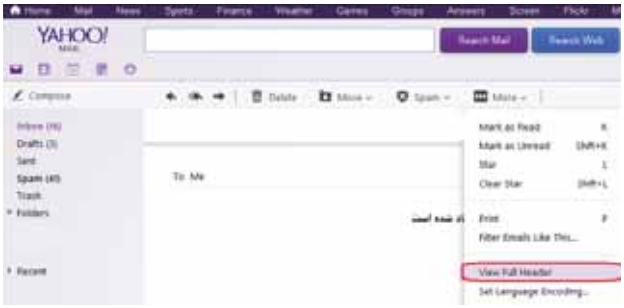
## ردیابی آدرس پست الکترونیکی

- ردیابی یک آدرس پست الکترونیکی عبارت است از تعیین موقعیت فرستنده‌ی اصلی و آدرس IP او به روی شبکه‌ای که در واقع پست الکترونیکی در آن ایجاد شده است.
- برای دریافت اطلاعات بیشتر درباره‌ی فرستنده‌ی پست الکترونیکی باید با ساختار پست الکترونیکی آشنا شویم.

[1] برای مطالعه بیشتر رجوع کنید به : کتاب "در جستجوی امنیت"، علی اصغر جعفری لاری، ص151

- هر پیام دقیقا یک هدر دارد که با فیلدهایی، ساختاربندی شده است. هر فیلد یک نام و مقدار دارد. هدر پست الکترونیکی حاوی تمام اطلاعات ارزشمند درباره‌ی مسیر و فرستنده‌ی اصلی پست الکترونیکی می‌باشد.
- برای ردیابی آدرس پست الکترونیکی، نیاز دارید که به حساب پست الکترونیکی خود وارد شده و سپس فایل هدر پست الکترونیکی را پیدا کنید.
- اینک، کد منبعی از پست الکترونیکی را به‌دست می‌آورید.
- برای نمونه برای Rediffmail:


- برای نمونه برای Yahoo Mail:




- برای نمونه برای Gmail:


اکنون از پایین تا بالا را نگاه کنید. نخستین آدرس IP که پیدا کردید، آدرس IP فرستنده است. می‌توانید با رفتن به آدرس www.ip2location.com و وارد کردن آدرسIP فرستنده، از محل جغرافیایی فرستنده تا حدودی آگاه شوید.