آموزش Hack

جلسه اول - ترمینولوژی (اصطلاح شناسی)

Hacker کیست؟

هکر کسی است که با سیستم‌های کامپیوتری آشناست و می‌تواند با روش‌هایی خاص (بدون‌اجازه) وارد آنها شود... این انسان می‌تواند خوب یا بد باشد (درهرحال هکر است).

سؤال: یک هکر از چه راهی وارد یک سیستم می‌شود؟

از راه شبکه (نه بابا !!!)

باید توجه کنید که هر سیستم کامپیوتری (به عبارت بهتر هر سیستم عامل) به‌هرحال محصول کار تعدادی انسان است و حتماً دارای تعدادی Bug (خطاهایی که بعد از ارائه محصول به بازار به‌تدریج کشف می‌شوند) خواهد بود. بعد از اینکه یک باگ مشخص شد، شرکت‌ها نرم‌افزارهایی را به‌سرعت (درعرض چند ساعت) ایجاد می‌کنند تا مشکل رفع شود. این‌ها را Patch می‌گویند. سپس مدیران شبکه (Webmasters) درعرض چند روز، چند ماه یا حتی چند سال (این آخری درمورد ایرانه!!!) آنها را Downloadکرده و مشکل را حل می‌کنند. در این فاصله، هکرها دمار از روزگار این سایت‌ها درمی‌آورند...

تعریف چند اصطلاح:

- Hacker واقعی = سامورایی: کسی که هدفش از نفوذ به سیستم‌ها نشان‌دادن ضعف سیستم‌های کامپیوتری است نه سوءاستفاده...
- Wacker (واکر): کسی که هدفش از نفوذ به سیستم‌ها، استفاده از اطلاعات آن سیستم‌هاست (جزو هکرهای کلاه‌سفید).
- Cracker (کراکر): کسی که هدفش از نفوذ به سیستم‌ها، خرابکاری و ایجاد اختلال در سیستم‌های کامپیوتری است (جزو هکرهای کلاه سیاه).
- Preaker: از قدیمی‌ترین هکرها هستند که برای کارشان نیاز (و دسترسی) به کامپیوتر نداشتند و کارشان نفوذ به خطوط تلفن برای تماس مجانی، استراق‌سمع و... بوده که این‌مورد جزو آموزش من نیست چون کار خیلی بدی است...

زنگ تفریح:

۱. جوجه هکرها (احمق کوچولوها): توانایی‌ها: بلدند از Sub7 و MagicPS و 187Final استفاده‌کنند و فکرکنند که همه‌چیز رو یاد گرفته‌اند !
۲. خروس‌هکرها یا مرغ‌هکرها (احمق‌های بزرگتر): Mailbox را هم می‌توانند Bomb کنند... ماشاءا... !
۳. هکرهای قابل‌احترام (مثل خود شما): دارند یاد می‌گیرند و هنوز ۲، ۳ سال کار دارند.
۴. هکرهای پیش‌کسوت: دیگه آفتاب لب بوم هستند... هکرهای قابل‌احترام را دوست دارند !

تقسیم‌بندی کامپیوترهای شبکه:

- کامپیوترهای Server: کامپیوترهایی که کارشان تأمین اطلاعات در شبکه است. مثلاً کامپیوترهایی که سایت‌ها را نگه می‌دارند.
- کامپیوترهای Client: کامپیوترهایی که استفاده‌کننده هستند مثل همین کامپیوتر خودتان که دارید از آن کار می‌کشید !

انواع سیستم‌عامل کامپیوترهای Server:

- خانواده Unix (مثل Sun Solaris، Linux، FreeBSD)
- خانواده Windows (مثل Win2000، WinNT، WinServer2003)
- MacOS
- سیستم‌های قدیمی‌تر مثل DEC20، DEC10، IRIS، AIX و...

سؤال: کدام‌ها را باید یاد گرفت؟

به عقیده من، Unix (Linux) و Win2000 را باید یاد بگیرید. پیشنهاد من این‌است که Win2000 و RedHat Linux را هم‌زمان روی کامپیوتر خود داشته‌باشید.

برای شروع چه‌چیزی لازم‌است؟

۱. Linux و Win2000 را روی کامپیوتر خود نصب‌کرده و شروع به یادگیری کنید.
۲. شروع به یادگیری زبان C کنید.
۳. شروع به یادگیری TCP/IP کنید.
۴. (مهم‌ترین مورد) علاقه به طی‌کردن یک راه طولانی جهت یادگیری داشته‌باشید.

تقسیم‌بندی انواع حملات:

اولین نکته‌ای که لازم‌است بگویم این‌است که وقت خود را برای هک‌کردن کامپیوترهای Client هدر ندهید (اگرچه برای افراد مبتدی کار با نرم‌افزاری مثل Sub7 زیاد هم بد نیست ولی نباید زیاده‌روی‌کرد) علت هم این‌است که هربار که به اینترنت وصل می‌شوند، IP جدیدی به آنها اختصاص می‌یابد و زحمات شما به‌هدر می‌رود (البته برای جلوگیری از این‌امر هم روش‌هایی هست که در آینده، ان‌شاءا... می‌گویم).

و حالا تقسیم‌بندی:

۱. حمله به‌روش Denial of Service Attack (DoS)
۲. حمله به‌روش Exploit
۳. حمله به‌روش Info Gathering (TelNet یکی‌از روش‌های آن است که در درس بعد می‌آموزید).
۴. حمله به‌روش Disinformation

به‌زودی با هرکدام از این روش‌های حمله آشنا خواهید شد.

زبان نوشتاری هکرها:

هکرها معمولاً درهنگام نوشتن به‌جای تعدادی از حروف انگلیسی، معادل‌های قراردادی به‌کار می‌برند که لیست بعضی‌از آنها را در زیر می‌بینید:

```
 0    <--    O
 1    <--    L, I
 2    <--    Z
 3    <--    E
 4    <--    A
 5    <--    S
 6    <--    G
 T    <--    7
 B    <--    8
At    <--    @
 S    <--    $
 H    <--    )(
 H    <--    }{
 N    <--    /\/
 M    <--    /\/\
 W    <--    \/\/
P, D  <--    |>
 K    <--    |<
 F    <--    ph, |>}{, |>)(
 S    <--    Z
```

البته تعداد این علامت‌ها خیلی بیشتر است و اکثراً قراردادی هستند و ممکن‌است با شکل‌های متفاوت دیگری هم مواجه‌شوید. مثلاً `He Speaks` می‌شود `}{3 $|>3A|<Z!`

توصیه بنده این است که تا جایی که امکان‌دارد، از این علائم استفاده نکنید؛ اما آنها را یاد داشته‌باشید تا اگر لازم‌شد، کم‌نیاورید !!!

ترسیم مسیر برای آینده:

۱. اولین و مهم‌ترین تصمیم، انتخاب نوع کامپیوتری است که می‌خواهید هک‌کنید (`Client` یا `Server`)، زیرا روش هک‌کردن این‌دو، به‌جز در مراحل ابتدای کار، کاملاً متفاوت‌است.

۲. دومین‌گام، انتخاب یک کامپیوتر مشخص (مثلاً کامپیوتری که فلان‌سایت را نگه‌می‌دارد که مثالی ازنوع `Server` است، یا کامپیوتر فلان‌شخص که با او `Chat` می‌کنید که مثالی برای کامپیوتر `Client` است) و سپس جمع‌آوری اطلاعات درمورد کامپیوتر هدف (قربانی) می‌باشد. این جمع‌آوری اطلاعات از قربانی (`Victim`) را `FootPrinting` گویند. اولین مشخصه‌ای که باید کشف‌شود، `IP` آن است. یکی‌دیگر از اطلاعات مهم که معمولاً دنبالش هستیم، پیداکردن نوع سیستم‌عامل و نیز برنامه‌هایی است که کامپیوتر مشخص‌شده، از آنها بهره می‌برد. یکی‌از مهم‌ترین (و گاه خطرناک‌ترین) کارها، تست‌کردن پورت‌های آن کامپیوتر برای دیدن اینکه کدام پورت‌ها باز و کدام‌ها بسته هستند، می‌باشد.

۳. مرحله بعدی، درواقع شروع تلاش برای نفوذ به سیستم است. این نفوذ سطوح مختلف دارد و بالاترین آن کـه در کامپیوترهـای Server روی می‌دهد، حالتی است که بتوانید Username و Password مربوط‌به مـدیر کـامپیوتر (Administrator) یـا نـاظر شبکه (Supervisor) را به‌دست‌آورده و ازطریق این اطلاعات مفید (Shell Account)، به نهایت نفوذ دسـت‌یابیـد؛ ولـی گـاه به‌دلایل مختلف (مربوط‌به سطح علمی خود و...) نمی‌توان به این‌سطح دست‌یافت اما به‌هرحال، بـرای مرحلـه بعـدی مـی‌توانـد استفاده‌شود. این‌مرحله جایی‌است که هنر شما به‌عنوان یک Hacker آغازشده و نیز به‌پایان می‌رسد.

۴. این مرحله بعد از نفوذ روی می‌دهد که در آن به سطحی از کنترل سیستم رسیده‌اید. رفتار شما دراین‌مرحله مشخص می‌کنـد که چه‌نوع هکری هستید (گروه‌های مطرح‌شده در ابتدای این جلسه را به‌یاد بیاورید)، و اینکه آیا جنبه یادگیری را داشته‌اید یـا نه؟

۵. مرحله آخر، پاک‌کردن رد پاست تا گیر نیفتیم (البته بعضی‌اوقات برای کلاس‌گذاشتن باید گیر بیفتـیم !). بعـضی‌از سیـستم‌هـا آمار Login را نگه‌می‌دارند که درمورد آنها، این‌مرحله بسیار مهم‌است.

خلاصه مراحل فوق بدین‌صورت است:

```
Selection -> FootPrinting -> Penetration -> [Behavior] -> Cleaning
```