زمان تقریبی مطالعه: حدوداً 10-12 دقیقه

مقدمات قبل از شروع یادگیری هک

هدف این مقدمه، آشنایی با مبانی اولیه و اصطلاحات لازم برای ورود به دنیای امنیت و هک است.

1. ترمینولوژی (اصطلاح‌شناسی) و معرفی هکر

- **هکر (Hacker) کیست؟**
هکر فردی است که با سیستم‌های کامپیوتری آشناست و توانایی ورود به آن‌ها را از طریق روش‌های خاص و بدون اجازه دارد. هکر می‌تواند دارای اهداف خوب یا بد باشد؛ در هر دو صورت، همچنان یک هکر محسوب می‌شود.

- **سوال اساسی:** هکر از چه طریقی وارد یک سیستم می‌شود؟
از طریق **شبکه**. هر سیستم کامپیوتری (و سیستم عامل آن) محصول کار انسان‌هاست و حتماً دارای **باگ (Bug)** است. باگ‌ها خطاهایی هستند که پس از عرضه محصول کشف می‌شوند. شرکت‌ها با ارائه **پچ (Patch)** (نرم‌افزارهای اصلاحی) این باگ‌ها را رفع می‌کنند. مدیران شبکه این پچ‌ها را نصب می‌کنند، اما در بازه زمانی بین کشف باگ و نصب پچ، هکرها می‌توانند از ضعف‌های سیستم سوءاستفاده کنند.

2. تعریف چند اصطلاح کلیدی:

- **هکر واقعی (Hacker واقعی = سامورایی):**
کسی که هدفش از نفوذ به سیستم‌ها، نشان دادن ضعف‌های امنیتی سیستم‌های کامپیوتری است، نه سوءاستفاده از آن‌ها.
- **واکر (Wacker):**
کسی که هدفش از نفوذ، استفاده از اطلاعات سیستم‌هاست (از هکرهای کلاه سیاه).
- **کراکر (Cracker):**
کسی که هدفش از نفوذ، خرابکاری و ایجاد اختلال در سیستم‌های کامپیوتری است (از هکر های کلاه سیاه).
- **پری‌کر (Preaker):**
از هکرهای قدیمی که بدون نیاز به دسترسی مستقیم به کامپیوتر، از طریق خطوط تلفن نفوذ می‌کردند (مانند تماس رایگان، استراق سمع). این مبحث جزو آموزش‌های اصلی این مجموعه نیست زیرا بدیهی تلقی می‌شود.

3. تقسیم‌بندی هکرها (از دیدگاه نویسنده):

- **جوجه‌هکرها (احمق کوچولوها):**
توانایی: استفاده از ابزارهایی مانند Sub7 و 8187 و تصور اینکه همه‌چیز را آموخته‌اند.

- **خروس‌هکرها یا مرغ‌هکرها (احمق‌های بزرگتر):**
توانایی: بمباران صندوق‌های پستی (Mail Bombing) و فعالیت‌های مشابه.
- **هکرهای قابل‌احترام (مثل شما):**
در حال یادگیری و نیازمند 2 تا 3 سال تجربه بیشتر.
- **هکرهای پیشکسوت:**
کسی که در سطح بالایی از مهارت قرار دارد و هکرهای قابل احترام را حمایت می‌کند.

4. انواع کامپیوترها در شبکه:

- **کامپیوترهای Server:** کامپیوترهایی که وظیفه تأمین اطلاعات در شبکه را دارند (مانند سرورهای میزبانی وب‌سایت‌ها).
- **کامپیوترهای Client:** کامپیوترهای استفاده کننده (مانند کامپیوتر شخصی شما).

سیستم‌عامل‌های مورد استفاده سرورها:

- **سیستم‌های فعلی:**
  - خانواده Unix (مانند FreeBSD, Linux, Sun Solaris)
  - خانواده Windows (مانند WinNT, Win2000)
  - macOS
- **سیستم‌های قدیمی (منقرض شده):** AIX, IRIS, DEC10, DEC20 و غیره.

کدام سیستم‌عامل‌ها را باید یاد گرفت؟

- **ضروری:** Win2000 و Unix (به ویژه Linux).
- **پیشنهاد عملی:** نصب همزمان Win2000 و RedHat Linux بر روی کامپیوتر شخصی.

5. ملزومات شروع یادگیری:

1. نصب و یادگیری Win2000 و Linux.
2. شروع یادگیری **زبان برنامه‌نویسی C**.
3. آغاز یادگیری **TCP/IP** (با مطالعه کتاب).
4. **مهمترین عامل:** علاقه و تحمل برای طی کردن مسیری بسیار طولانی و با جزئیات فراوان.

6. تقسیم‌بندی انواع حملات:

- **تذکر مهم:** زمان خود را برای هک کردن کامپیوترهای Client تلف نکنید. اگرچه استفاده از ابزارهایی مانند Sub7 برای مبتدیان مفید است، اما زیاده‌روی نکنید. دلیل: IP کلاینت‌ها معمولاً پویا است و زحمات شما بی‌نتیجه می‌ماند (با وجود روش‌هایی برای دور زدن این مشکل که در ادامه توضیح داده خواهد شد).

- **تقسیم‌بندی حملات:**

1. **حمله از نوع serangan DoS (Denial of Service Attack):** جلوگیری از دسترسی کاربران مجاز به سرویس.
2. **حمله با استفاده از اکسپلویت (Exploit):** بهره‌برداری از آسیب‌پذیری‌های نرم‌افزاری.
3. **حمله با جمع‌آوری اطلاعات (Info Gathering):** مانند استفاده از Telnet برای کسب اطلاعات.
4. **حمله انتشار اطلاعات غلط (Disinformation):** انتشار اطلاعات نادرست.
توضیحات کامل‌تر در مورد هر حمله در ادامه ارائه خواهد شد.

7. Speak 1337 (لیت اسپیک):

گاهی هکرها در مکاتبات خود، حروفی از کلمات را با نمادهای مشابه جایگزین می‌کنند. (مانند: 0 به جای O، 1 به جای I یا L، 7 به جای T و الی آخر).

- **مثال:** "He Speaks" به صورت "}{3 $|34<|z >" نوشته می‌شود.
- **توصیه:** تا حد امکان از این معادل‌ها استفاده نکنید؛ فقط هدف آشنایی با آن‌هاست تا در صورت مواجهه، متوجه منظور شوید.

8. ترسیم مسیر برای آینده (مراحل یادگیری و عملیات هک):

1. **انتخاب هدف:** تصمیم‌گیری برای هک کردن کامپیوتر Client یا Server. روش‌های هک این دو کاملا متفاوت است.
2. **جمع‌آوری اطلاعات (Footprinting):** انتخاب یک کامپیوتر مشخص (هدف) و جمع‌آوری اطلاعات اولیه درباره آن.
   - کشف IP آدرس هدف.
   - تعیین نوع سیستم‌عامل و نرم‌افزارهای نصب شده.
   - **تست پورت‌ها:** بررسی باز یا بسته بودن پورت‌های فعال روی کامپیوتر هدف (یکی از مهمترین و خطرناک‌ترین مراحل).
3. **تلاش برای نفوذ (Penetration):** شروع فرآیند نفوذ. بالاترین سطح نفوذ در سرورها، دستیابی به نام کاربری و رمز عبور مدیر (Administrator/Superuser) و گرفتن دسترسی کامل (Shell Account) است. هنر یک هکر در این مرحله شکوفا می‌شود.
4. **پس از نفوذ (Post-Exploitation):** در این مرحله که سطحی از کنترل سیستم حاصل شده، رفتار هکر نشان‌دهنده نوع او (سامورایی، واکر یا کراکر) و میزان یادگیری اوست.
5. **پاکسازی ردپا (Cleaning):** از بین بردن شواهد باقی‌مانده برای جلوگیری از شناسایی. این مرحله در سیستم‌هایی که لاگ‌های ورود را ثبت می‌کنند، بسیار حیاتی است.

خلاصه مراحل:
Selection -> **Footprinting** -> **Penetration** -> **[Changings]** -> **Cleaning**

9. تعریف IP و Port:

- **IP (Internet Protocol):**
  - شماره‌ای منحصربه‌فرد که به هر کامپیوتر متصل به اینترنت اختصاص داده می‌شود.
  - **IP ثابت:** معمولاً به سرورها و کامپیوترهای متصل به اینترنت از طریق اتصالات غیر از Dial-up اختصاص می‌یابد.
  - **IP پویا (متغیر):** مانند اتصال از طریق Dial-up، که هر بار پس از اتصال، IP جدیدی تخصیص می‌یابد.
  - **ساختار:** یک عدد 32 بیتی (4 بایتی) که به صورت xxx.xxx.xxx.xxx نوشته می‌شود، که هر xxx عددی بین 0 تا 255 است. مثال: 195.219.176.69.
  - **نقش نام‌های دامنه:** نام‌هایی مانند www.yahoo.com در نهایت باید به IP تبدیل شوند تا اتصال برقرار شود.
  - **کلاس‌های IP:**
    - **کلاس A:** xxx بین 1 تا 126 (برای شبکه‌های بزرگ اینترنتی و Backbone ها).
    - **کلاس B:** xxx بین 128 تا 191 (کاربرد عملی بالا).
    - **کلاس C:** xxx بین 192 تا 223 (معمولاً اختصاص یافته به ISP های ارائه دهنده Dial-up).
    - **عدد 127:** رزرو شده برای **localhost** (کامپیوتر خودمان، مثال: 127.0.0.1).
  - **شناسایی IP خود:** استفاده از دستور ipconfig در Command Prompt. برای تشخیص IP کلاینت‌ها در ایران، معمولاً عدد اول IP آن‌ها بین 192 تا 223 است.

- **Port:**
  - در ساده‌ترین تعریف، محلی برای ورود و خروج داده‌ها.
  - در هک، بیشتر با **پورت‌های نرم‌افزاری** سروکار داریم که از 1 تا 65535 شماره‌گذاری شده‌اند.
  - هر پورت به یک سرویس یا نرم‌افزار خاص اختصاص داده شده است. (مثلاً پورت 25 برای ارسال ایمیل). نرم‌افزاری که مسئول آن سرویس است، بر روی آن پورت "منتظر" می‌ماند.
  - **مهمترین پورت‌ها و کاربردها (بخشی از لیست):**
    - 7: echo (تکرار متن ورودی)
    - 8: echo
    - 9: discard (حذف بی‌صدا داده)
    - 13: daytime (زمان سیستم میزبان)
    - 21: ftp (انتقال فایل)
    - 23: telnet (ورود به سیستم از راه دور)
    - 25: smtp (برای ارسال ایمیل)
    - 53: domain (سرویس نام دامنه DNS)
    - 79: finger (اطلاعات کاربران)
    - 80: http (وب سرور)

- 110: pop3 (دریافت ایمیل)
- 443: shttp (وب سرور امن)

10. Command Prompt (خط فرمان):

- روش دسترسی:
  - Start > Programs > Accessories > Command Prompt
  - در پنجره Run، تایپ command یا cmd.
- **اهمیت:** بخش مهمی از درس‌های آینده برای اجرای دستورات مختلف خواهد بود.

11. یافتن IP یک سایت (تبدیل نام دامنه به IP):

- **روش‌های متداول:**

1. **مشاهده Status Bar مرورگر (IE) یا گرفتن اسکرین‌شات:** روشی غیردقیق و پیشنهادی **فقط برای مبتدیان شدید و با احتیاط بالا **.
2. **استفاده از دستور ping [domain_name] در Command Prompt:** (مثال: ping sazin.com). علاوه بر نمایش IP، وضعیت اتصال و تأخیر را نیز نشان می‌دهد. این دستور در واقع برای تست اتصال و سرعت است، اما ما از آن برای یافتن IP استفاده می‌کنیم.
3. **استفاده از Whois Query (کاملترین روش):** مراجعه به وب‌سایت‌هایی مانند samspade.org (یا جستجو در گوگل "ws whois") و وارد کردن نام دامنه. این روش اطلاعات کامل‌تری درباره مالک دامنه و IP را نمایش می‌دهد.

- **تحلیل نتایج:** مشاهده می‌شود که سایت‌ها ممکن است چندین IP داشته باشند یا IP آن‌ها با گذشت زمان تغییر کند. استفاده از Whois برای سایت‌های بزرگ دقیق‌تر است.

12. به دست آوردن IP خود پس از اتصال به اینترنت:

- **استفاده از ipconfig در Command Prompt:** نمایش IP، Subnet Mask و Default Gateway متصل به سیستم شما.
- **استفاده از netstat -an یا netstat -n:** نمایش اتصالات فعال از کامپیوتر شما به سایر کامپیوترها. در بخش Local Address، IP و پورت خروجی شما نمایش داده می‌شود.

13. یافتن IP طرف مقابل هنگام چت (Yahoo Messenger – روش قدیمی):

- **نکته:** این روش در گذشته کار می‌کرد اما با تغییر پروتکل‌ها و امنیت، دیگر قابل اعتماد نیست.
- **روش (توضیح تاریخی):**
  1. استفاده از دستور netstat -n یا netstat در Command Prompt.

2. جستجو در خروجی برای سطری که پورت مربوط به چت (مانند 5101 برای Yahoo Messenger) را در ستون Foreign Address یا Local Address داشته باشد.
3. IP طرف مقابل در ستون Foreign Address همان سطر یافت می‌شد.

- **مشکل این روش:** با فعال شدن پروتکل‌های جدیدتر و امنیت بالاتر، IPها مبهم شده و یا به نام‌های هاست تبدیل می‌شوند.

14. بحث Port ها و Telnet:

- **TCP و UDP:** دو پروتکل اساسی در لایه انتقال مدل TCP/IP.

  - **TCP (Transmission Control Protocol):** پروتکلی قابل اعتماد، با قابلیت اطمینان بالا، کنترل خطا و اطمینان از رسیدن بسته‌ها (مثلاً برای وب، FTP، ایمیل).
  - **UDP (User Datagram Protocol):** پروتکلی سریع‌تر اما بدون تضمین تحویل و کنترل خطا (مناسب برای مواردی که سرعت مهمتر است، مانند برخی بازی‌های آنلاین یا استریم).
  - هنگام ارتباط با پورت، می‌توان از هر دو برای اتصال استفاده شود، لذا هر دو باید بررسی شوند.

- **تقسیم‌بندی پورت‌ها بر اساس شماره:**

1. **پورت‌های 0 تا 1023:** پورت‌های Well-Known؛ معمولاً برای سرویس‌های استاندارد اینترنتی استفاده می‌شوند (مانند HTTP, FTP, SMTP).
2. **پورت‌های 1024 تا 49151:** پورت‌های Registered؛ توسط برنامه‌ها برای ارتباطات خودکار (مانند مرورگرها، کلاینت‌های ایمیل) استفاده می‌شوند و به طور تصادفی باز می‌شوند.
3. **پورت‌های 49152 تا 65535:** پورت‌های Dynamic/Private؛ عمدتاً برای استفاده موقت، سرویس‌های خاص یا تروجان‌ها (نرم‌افزارهای مخرب).

- **چگونه به یک پورت Telnet کنیم؟**

  - Telnet ابزاری برای برقراری ارتباط مستقیم با یک پورت خاص روی یک سیستم راه دور است. این کار به ما امکان می‌دهد رفتار پورت را آزمایش کنیم.
  - **دستور:** `[telnet [hostname/IP] [port_number`
  - مثال: `telnet iums.ac.ir 13` یا `telnet iums.ac.ir daytime` (برای دریافت ساعت و تاریخ).
  - **اهمیت برای هکر:** Telnet اولین ابزاری است که هکرها برای شناسایی پورت‌های باز و جمع‌آوری اطلاعات اولیه استفاده می‌کنند، زیرا برخی پورت‌ها اطلاعات حساسی را فاش می‌کنند.

15. Port Scanning (پورت‌اسکنینگ):

- **هدف:** تعیین اینکه کدام پورت‌ها روی یک سیستم باز هستند و کدام بسته.

- **روش‌های اسکن TCP:**
  - **TCP Connect Scan:** مراحل 1 (SYN), 2 (SYN/ACK), 3 (ACK) از دست‌دهی سه‌طرفه TCP. اتصال کامل برقرار می‌شود و در لاگ سرور ثبت می‌گردد.
  - **TCP SYN Scan (Half-Open Scan):** مراحل 1 (SYN) و 2 (SYN/ACK) انجام می‌شود، اما مرحله 3 (ACK) انجام نمی‌شود. اگر SYN/ACK دریافت شود، پورت باز است. این روش کمتر در لاگ‌ها ثبت می‌شود چون اتصال کامل نمی‌شود.
  - انواع دیگر: FIN Scan, Null Scan, Xmas Tree Scan, UDP Scan.

- **چگونه Port Scanning را انجام دهیم؟**
  - در ویندوز، ابزارهای داخلی مانند `ping` برای اسکن پورت مناسب نیستند. نیاز به ابزارهای خارجی دارید.
  - **ابزارهای محبوب (برای ویندوز یا در لینوکس):**
    1. **NMap/NMapWin:** ابزار بسیار قدرتمند و کامل برای انواع اسکن‌ها، تشخیص سیستم‌عامل و... (بخش عمده‌ای از آن برای لینوکس است اما نسخه ویندوز گرافیکی NMapWin نیز وجود دارد).
    2. **NetScanTools Pro:** ابزاری جامع و پولی.
    3. **WinScan:** برایTCP Scan (کارایی متوسط).
    4. **ipEye v1.2:** (ابزار مورد استفاده در این آموزش) فقط در ویندوز XP/2000 کار می‌کند، فقط یک IP را در هر بار اسکن می‌کند و TCP را تست می‌کند. جهت استفاده:
       - دانلود و اجرای نرم‌افزار از طریق Command Prompt با دستور `ipEye <target IP> <scan type> -p <port range>`.
       - مثال: `ipeye 63.148.227.65 -syn -p 1 200` (اسکن SYN از پورت 1 تا 200 سایت سازین).
       - نتایج: نمایش پورت‌های باز (open)، بسته (closed/reject) یا دراپ شده (drop).

- **تعیین پورت‌های باز کامپیوتر خودتان:**
  - `netstat -an` (نمایش همه اتصالات و پورت‌ها به صورت عددی)
  - `netstat -a` (مشابه بالا اما نام سرویس‌ها را بجای شماره پورت نمایش می‌دهد)
  - `netstat -n` (نمایش IP و پورت‌ها به صورت عددی، بدون نام سرویس). این دستور برای یافتن IP حین چت مفید بود.
  - **اهمیت:** کشف برنامه‌های مخرب (تروجان‌ها) که روی پورت‌های خاص منتظر دستور می‌مانند.

دستور `nslookup`: برای جستجوی DNS (تبدیل نام‌ها به IP و برعکس).

پاسخ به سوالات متداول کاربران:

- **نفوذ به سیستم بدون اتصال به اینترنت:** بله، با استفاده از نرم‌افزارهای خاص (مانند تروجان‌ها) که از طریق تلفن یا شبکه داخلی ارتباط برقرار می‌کنند و نیازمند رعایت دو شرط: استفاده طرفین از نرم‌افزار یکسان و داشتن شماره تلفن مقصد.
- **تفاوت Windows 2000/XP با 98 برای هک:** Windows 98 قدیمی و ضعیف‌تر است. نسخه‌های NT-based مانند 2000 و XP برای هک آماتوری امن‌تر و با پتانسیل بیشتری بوده است.
- **پیدا کردن IP از طریق Proxy Server:** اگر از ISP یکسان به اینترنت وصل شوید، حتی با Proxy، ممکن است IP اصلی شما در نهایت قابل ردیابی باشد.
- **تشخیص Port Scanning:** استفاده از فایروال‌ها که هنگام اسکن هشدار می‌دهند، یا بررسی Loadهای سرور که اتصالات ورودی را ثبت می‌کنند.
- **تفاوت NMap و FireWalk:** Nmap بیشتر برای اسکن پورت‌ها و شناسایی اولیه سیستم‌عامل استفاده می‌شود؛ FireWalk تخصصی‌تر به آنالیز رفتار فایروال‌ها می‌پردازد.
- **پیدا کردن رمز عبور:** روش‌های متفاوتی وجود دارد که برخی از آن‌ها در پاسخ‌های بعدی ذکر شده (کرک کردن فایل SAM، رمزهای ستاره‌ای و غیره).
- **بررسی امنیت پورت 80:** با ارسال دستورات خاص (مانند کاراکترهای مخرب) به سمت وب‌سرور روی پورت 80. این موضوع در ادامه مباحث پیشرفته‌تر توضیح داده خواهد شد.
- **تفاوت SuSE با Red Hat Linux:** بیشتر سلیقه‌ای و بستگی به تجربه کاربر دارد. SuSE به دلیل راحتی نصب درایورها و اجرای برنامه‌ها، بیشتر توصیه شده است.
- **استفاده از `tracert`:** مشاهده مسیر رسیدن بسته‌ها به مقصد. تغییرات در نتایج ممکن است به دلیل تغییرات در شبکه یا تنظیمات (مانند TTL).
- **یافتن رمز عبور ادمین ویندوز XP:** از طریق نرم‌افزارهایی مانند LC4 برای کرک فایل SAM، یا استفاده از ترفندهای ورود به سیستم (مانند CTRL+ALT+DEL دو بار در صفحه Login).