آموزش شبکه و امنیت سایبری

اصطلاح‌شناسی در امنیت سایبری

در دنیای امنیت اطلاعات، درک دقیق اصطلاحات کلیدی اولین قدم برای یادگیری آموزش شبکه و امنیت سایبری است. بسیاری از واژه‌ها مانند "هکر" سال‌هاست که به اشتباه معنا شده‌اند. بیایید با هم این مفاهیم را روشن کنیم.

هکر چیست؟

هکر فردی است که دانش عمیقی از سیستم‌های کامپیوتری و شبکه‌ها دارد و می‌تواند با استفاده از این دانش، نقاط ضعف سیستم‌ها را کشف کند. اما مهم است بدانید: **هکر بودن به معنای نفوذ غیرقانونی نیست**. هکرها به دو دسته اصلی تقسیم می‌شوند:

...

```
nmap -sn -PR 192.168.1.0/24
```

جمع‌بندی و هشدار اخلاقی

- اسکن شبکه یک ابزار مدیریتی و امنیتی است، نه ابزار نفوذ — بخشی ضروری از آموزش شبکه و امنیت سایبری.
- همیشه از ابزارهای به‌روز مثل **Nmap** استفاده کنید — ابزاری که در آموزش شبکه و امنیت سایبری نقش کلیدی دارد.
- اسکن بدون مجوز، غیرقانونی است و ممکن است عواقب جدی داشته باشد.
- استفاده از این ابزارها فقط در شبکه‌های تحت مدیریت شما یا با مجوز رسمی مجاز است.
- هدف از این آموزش، **درک بهتر امنیت شبکه** و **حفاظت از سیستم خود** است، نه نفوذ به سیستم دیگران — اصلی‌ترین هدف آموزش شبکه و امنیت سایبری.

مطالب حقوقی بیشتر در: https://irlawyers.ir/ --- الکترونیک، کامپیوتر، بورس و غیره در: https://229-415.ir/

...

سرویس توضیح

21FTPانتقال فایل (غیرامن — توصیه نمی‌شود)22SSHدسترسی امن به سرور (توصیه شده)23Telnetدسترسی از راه دور (غیرامـن — قـدیمی)25SMTPارسال ایمیـل (اغلـب فیلتـر می‌شود)53DNSتبـدیل نـام دامنـه بـه IP80HTTPاوب‌سایت‌های غیرامن110POP3دریافت ایمیل (نسخه قدیمی)...

143IMAPدریافت ایمیل (نسخه مدرن)

443HTTPSوب‌سایت‌های امن (رمزنگاری شده)3389RDPدسکتاپ ریموت ویندوز

چرا بررسی پورت‌ها مهم است؟

یکی از اولین مراحل در ارزیابی امنیت یک سیستم، **اسکن پورت** (Port Scanning) است — مفهومی کلیدی در آموزش شبکه و امنیت سایبری. این کار به شما نشان می‌دهد کدام سرویس‌ها فعال هستند و ممکن است هدف حمله قرار بگیرند. اما توجه داشته باشید:

- اسکن پورت بدون مجوز می‌تواند غیرقانونی باشد.
- فقط باید روی سیستم‌هایی که مالک آن هستید یا مجوز تست دارید، انجام شود.

...
ابزارهایی مانند **Nmap** برای این منظور استفاده می‌شوند، اما باید با مسئولیت کامل به کار گرفته شوند — بخشی اساسی از آموزش شبکه و امنیت سایبری.

RFC چیست؟

RFC مخفف عبارت *Request for Comments* است و به مجموعه‌ای از اسناد فنی اشاره دارد که استانداردهای اینترنت، پروتکل‌ها، روش‌ها و مفاهیم شبکه‌ای را تعریف می‌کنند. این اسناد توسط **IETF** (گروه کاری مهندسی اینترنت) منتشر می‌شوند و سنگ بنای فناوری‌های مدرن دیجیتال محسوب می‌شوند — بخشی حیاتی از آموزش شبکه و امنیت سایبری.

...
nmap -sn 192.168.1.0/24

 نکته: شما می‌توانید از Zenmap برای ساخت دستور استفاده کنید — در پایین پنجره، دستور واقعی nmap نمایش داده می‌شود. این دستور را کپی کرده و در خط فرمان اجرا کنید.

مطالب حقوقی بیشتر در: https://irlawyers.ir/ --- الکترونیک، کامپیوتر، بورس و غیره در: https://229-415.ir/

جمع‌بندی و هشدار اخلاقی

- nmap یک ابزار قدرتمند برای **مدیریت شبکه** و **ارزیابی امنیتی** است — ستون فقرات آموزش شبکه و امنیت سایبری.
- استفاده از آن فقط در شبکه‌های تحت مدیریت شما یا با **مجوز رسمی** مجاز است.
- اسکن بدون مجوز، **غیرقانونی و نقض حریم خصوصی** است.

...

- هدف از این آموزش، **درک بهتر امنیت شبکه** و **حفاظت از سیستم‌ها** است، نه نفوذ به آنها — هدف اصلی آموزش شبکه و امنیت سایبری.

> ⚠ **هشدار قانونی:** طبق قوانین جرایم رایانه‌ای در ایران و بسیاری از کشورها، انجام هرگونه فعالیت شبکه‌ای روی سیستم‌هایی که مالک آن نیستید، **جرم محسوب می‌شود**. این محتوا فقط برای **آموزش، مدیریت شبکه و تست امنیتی قانونی** طراحی شده است — بخشی اساسی از آموزش شبکه و امنیت سایبری.

ping چیست؟ بررسی فعال بودن دستگاه‌ها در شبکه

ping یکی از ساده‌ترین و پرکاربردترین ابزارهای شبکه است که برای بررسی اینکه آیا یک دستگاه (سرور، روتر یا کامپیوتر) در شبکه فعال و قابل دسترس است، استفاده می‌شود — مفهومی پایه در آموزش شبکه و امنیت سایبری. این دستور با ارسال بسته‌های **ICMP Echo Request** به مقصد و دریافت **ICMP Echo Reply**، وضعیت ارتباط را ارزیابی می‌کند.

نحوه استفاده از ping

در Command Prompt یا PowerShell دستور زیر را وارد کنید:

```
ping آدرس
```

آدرس می‌تواند یک **IP** یا **نام دامنه** باشد.

مثال: تست ارتباط با یک سایت

```
ping sazin.com
```

مطالب حقوقی بیشتر در: https://irlawyers.ir/ --- الکترونیک، کامپیوتر، بورس و غیره در: https://229-415.ir/

خروجی نمونه:

```
Pinging sazin.com [63.148.227.65] with 32 bytes of data:
   Reply from 63.148.227.65: bytes=32 time=861ms TTL=105
   Reply from 63.148.227.65: bytes=32 time=852ms TTL=105
   Reply from 63.148.227.65: bytes=32 time=851ms TTL=105
   Reply from 63.148.227.65: bytes=32 time=881ms TTL=105
                      Ping statistics for 63.148.227.65:
     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
                             Approximate round trip times:
       Minimum = 851ms, Maximum = 881ms, Average = 861ms
```

...

User Datagram Protocol (UDP)پروتکل انتقال سریع و بدون ارتباطRFC 792Internet Control Message Protocol (ICMP)برای تشخیص خطا و مدیریت شبکه (مثل دستور ping)

🌐 سیستم نام دامنه (DNS)

شماره	عنوان	توضیح
RFC 1034	Domain Names — Concepts and Facilities	مفاهیم پایه DNS
RFC 1035	Domain Names — Implementation and Specification	جزئیات فنی پیاده‌سازی DNS
RFC 974	Mail Routing and the Domain System	راه‌اندازی MX Record برای ایمیل

📧 ایمیل و انتقال فایل

...
...

شماره	عنوان

تفسیر خروجی:

- **Reply from:** سرور پاسخ داده — یعنی فعال است.
- **time:** زمان رفت و برگشت بسته (چه کمتر، بهتر).

مطالب حقوقی بیشتر در: https://irlawyers.ir/ --- الکترونیک، کامپیوتر، بورس و غیره در: https://229-415.ir/

- **TTL:** Time To Live — نشان‌دهنده تعداد هاپ‌های باقی‌مانده (معمولاً 64، 128 یا 255).
- **Lost = 100%:** سرور پاسخ نمی‌دهد (ممکن است خاموش، فیلتر شده یا ICMP بلاک شده باشد).

پارامترهای مفید ping

...

پارامتر	توضیح

⚠ **هشدار قانونی:** طبق قوانین جرایم رایانه‌ای در ایران و بسیاری از کشورها، انجام هرگونه فعالیت شبکه‌ای روی سیستم‌هایی که مالک آن نیستید، **جرم محسوب می‌شود**. این محتوا فقط برای **آموزش، مدیریت شبکه و تست امنیتی قانونی** طراحی شده است — بخشی ضروری از آموزش شبکه و امنیت سایبری.

nmap چیست؟ ابزاری قدرتمند برای امنیت و مدیریت شبکه

nmap مجموعه‌ای از قابلیت‌های حرفه‌ای را در اختیار مدیران شبکه و متخصصان امنیت قرار می‌دهد — ابزاری اساسی در آموزش شبکه و امنیت سایبری:

- شناسایی دستگاه‌های فعال در شبکه (Host Discovery)
- اسکن پورت‌ها (TCP و UDP)
- تشخیص سرویس‌ها و نسخه‌های نرم‌افزاری (Service Detection)
- تشخیص سیستم‌عامل (OS Detection)
- تجزیه و تحلیل فایروال و فیلترینگ
- خروجی گزارش‌گیری (متن، Grepable، XML)

رابط Zenmap — نسخه گرافیکی nmap

Zenmap محیطی کاربرپسند فراهم می‌کند که از طریق آن می‌توانید بدون دانش عمیق از دستورات، اسکن انجام دهید — ابزاری کاربردی در آموزش شبکه و امنیت سایبری.

اجزای اصلی رابط Zenmap:

مطالب حقوقی بیشتر در: https://irlawyers.ir/ --- الکترونیک، کامپیوتر، بورس و غیره در: https://229-415.ir/

1. قسمت ورودی (Network Section)

...

شماره	عنوان	توضیح
RFC 2401	IPSec Architecture	امنیت در لایه شبکه
RFC 2828	Glossary of Internet Terms	واژه‌نامه استاندارد امنیت و شبکه
RFC 2827	نفوذپذیری BCP 38	جلوگیری از Spoofing آدرس IP
RFC 1244	Site Security Handbook	راهنمای امنیتی برای سازمان‌ها

⚙ مدیریت شبکه و پروتکل‌های کمکی

- **RFC 1157**: Simple Network Management Protocol (SNMP)
- **RFC 1350**: TFTP (Trivial File Transfer Protocol)
- **RFC 1035**: DNS (نیز در بالا آمده)
- **RFC 868**: Time Protocol (همگام‌سازی زمان)
- **RFC 1149**: انتقال داده از طریق حمل‌ونقل پرنده! (طنازه — ولی واقعی!)

نکات مهم برای استفاده از RFCها

- همیشه بررسی کنید که آیا RFC مورد نظر **منسوخ (Obsoleted)** نشده باشد. مثلاً RFC 821 توسط RFC 5321 جایگزین شده است.
- RFCها جایگزین آموزش‌های مقدماتی نیستند. بهتر است ابتدا مفاهیم را از منابع آموزشی یاد بگیرید، سپس به RFCها مراجعه کنید — بخشی از آموزش شبکه و امنیت سایبری.
- برای متخصصان امنیت، خواندن RFCهای مربوط به پروتکل‌ها (مثل TCP، DNS، SMTP) به درک عمیق‌تر از نقاط ضعف کمک می‌کند — مهارتی کلیدی در آموزش شبکه و امنیت سایبری.

در نهایت، RFCها مثل "قانون‌های اینترنت" هستند. کسی که بخواهد واقعاً شبکه را بفهمد، باید حداقل با چندتا از این اسناد کلیدی آشنا باشد — هسته اصلی آموزش شبکه و امنیت سایبری.

Command Prompt چیست؟

Command Prompt (cmd) یک محیط خط فرمان (Command Line Interface) در ویندوز است که به شما اجازه می‌دهد دستورات شبکه، سیستم و مدیریتی را مستقیماً اجرا کنید. این ابزار یکی از ابزارهای ضروری برای متخصصان شبکه و امنیت سایبری است — بخشی اساسی از آموزش شبکه و امنیت سایبری.

مطالب حقوقی بیشتر در: https://irlawyers.ir/ --- الکترونیک، کامپیوتر، بورس و غیره در: https://229-415.ir/

چگونه Command Prompt را باز کنیم؟

- **روش 1:** کلیدهای Win + R را فشار دهید، سپس عبارت cmd یا command را تایپ و Enter بزنید.

...

→ سرور از **Microsoft Exchange** نسخه قدیمی استفاده می‌کند — نیاز به به‌روزرسانی دارد.
پورت 110 (POP3):

```
OK Microsoft Exchange 2000 POP3 server version 6.0.5762.3 ready+
```

→ نسخه Exchange 2000 — بسیار قدیمی و آسیب‌پذیر.
پورت 119 (NNTP):

```
NNTP Service 5.00.0984 Version: 5.0.2195.2966 Posting Allowed
```

→ سرویس اخبار فعال است و ممکن است قابلیت ارسال داشته باشد.
...
این دستور علاوه بر نمایش IP، مسیر شبکه‌ای بین شما و سرور را نیز نشان می‌دهد:

```
tracert example.com
```

مفید برای تشخیص تأخیرها و نقاط واسط.

روش ۴: استفاده از ابزارهای آنلاین (مثل WHOIS)

برای اطلاعات بیشتر (مانند مالک دامنه، ISP، محل سرور)، می‌توانید از ابزارهای WHOIS استفاده کنید:

- whois.domaintools.com
- whois.com

این ابزارها IP سرور را نمایش می‌دهند و اطلاعات ثبت دامنه را ارائه می‌کنند.
...
استفاده از ابزارهای شبکه مانند **tracert**، **ping** و **telnet** فقط در شبکه‌هایی مجاز است که:

- شما مالک یا مدیر آن هستید
- یا مجوز رسمی برای تست امنیتی دارید

انجام این فعالیت‌ها روی سیستم‌های شخص ثالث بدون مجوز، **غیرقانونی بوده و نقض حریم خصوصی**

محسوب می‌شود. این آموزش صرفاً برای **مدیریت شبکه**، **امنیت سازمانی** و **یادگیری قانونی** طراحی شده است — بخشی از آموزش شبکه و امنیت سایبری.

Social Engineering چیست؟ تهدید انسانی در امنیت سایبری

مهندسی اجتماعی (Social Engineering) یکی از پرخطرترین و مؤثرترین روش‌های نفوذ در دنیای امنیت سایبری است — نه با کد، بلکه با **فریب انسان‌ها**. در این روش، مهاجمان از روانشناسی، فشار زمانی، ترس یا کنجکاوی برای وادار کردن کاربران به افشای اطلاعات حساس (مثل رمز عبور، اطلاعات بانکی یا دسترسی داخلی) استفاده می‌کنند. نکته کلیدی: اغلب سیستم‌های فنی امن هستند، اما **انسان‌ها نقطه ضعیف اصلی** هستند — موضوعی حیاتی در آموزش شبکه و امنیت سایبری.
...

255.0.0.0 (/8)شبکه‌های بسیار بزرگ (مثل ISPها)16/) 191255.255.0.0 – Class B128)شرکت‌های بزرگ24/) 223255.255.255.0 – Class C192)شبکه‌های کوچک و متوسط

سیستم مدرن: CIDR

امروزه از نمادگذاری **CIDR** استفاده می‌شود، مثلاً:

- `192.168.1.0/24` — شبکه‌ای با 256 آدرس
- `10.0.0.0/8` — شبکه بزرگ با 16 میلیون آدرس

این روش انعطاف‌پذیری بیشتری دارد و از هدررفت IP جلوگیری می‌کند.

آدرس‌های ویژه و رزرو شده

...

> ⚠ **توجه:** این محتوا برای **آگاهی، آموزش و دفاع** طراحی شده است، نه برای سوءاستفاده. شناسایی تکنیک‌های مهندسی اجتماعی، وظیفه هر کاربر هوشمند و هر سازمان امنیتی است — بخشی از آموزش شبکه و امنیت سایبری.

چرا مهندسی اجتماعی خطرناک است؟

- نیاز به دانش فنی پیشرفته ندارد.
- قابلیت دور زدن تمام سیستم‌های امنیتی (فایروال، آنتی‌ویروس، رمزنگاری) را دارد.
- اغلب از طریق کانال‌های قانونی (ایمیل، تلفن، شبکه‌های اجتماعی) انجام می‌شود.

مطالب حقوقی بیشتر در: https://irlawyers.ir/ --- الکترونیک، کامپیوتر، بورس و غیره در: https://229-415.ir/

- بسیار مؤثر است — طبق گزارش‌های Verizon و IBM، بیش از **90٪** از حملات سایبری شامل مهندسی اجتماعی هستند — تأکیدی بر اهمیت آموزش شبکه و امنیت سایبری.

...

روش‌های رایج مهندسی اجتماعی و نحوه دفاع

1. تماس تلفنی (Vishing)

مهاجم با تماس تلفنی، خود را به عنوان کارمند پشتیبانی فنی، بانک یا مدیر شرکت جا می‌زند و از کاربر می‌خواهد رمز عبور، اطلاعات حساب یا دسترسی به سیستم را افشا کند.
مثال:"سلام، من از بخش فناوری اطلاعات هستم. سیستم شما مشکل دارد. لطفاً رمز عبور کاربری خود را برای راه‌اندازی مجدد سرور ارسال کنید."
راه دفاع:هرگز رمز عبور را تلفنی افشا نکنید. شماره تماس را قطع کنید و از طریق کانال رسمی شرکت، تماس بگیرید.

2. ارسال فایل آلوده از طریق چت یا ایمیل

...

- whatismyipaddress.com
- iplocation.net
- icanhazip.com (فقط IP را نمایش می‌دهد)

هشدار اخلاقی: استفاده از ابزارهای شبکه برای رصد یا شناسایی دیگران بدون رضایت آنها، غیرقانونی و غیراخلاقی است. این دستورات فقط برای **تشخیص سیستم خود** یا **سیستم‌های تحت مدیریت شما** مجاز هستند — اصلی‌ترین قانون در آموزش شبکه و امنیت سایبری.

...
مهاجم با بهره‌گیری از کنجکاوی، فایلی با نام جذاب (مثل "عکس من.exe" یا "فاکتور جدید.pdf.exe") ارسال می‌کند که در واقع یک بدافزار یا تروجان است.
نکته: فایل‌های با پسوند `.bat`, `.scr`, exe می‌توانند اجرایی باشند.
راه دفاع:فایل‌های اجرایی را از افراد ناشناس باز نکنید. از آنتی‌ویروس به‌روز و فیلتر ایمیل استفاده کنید.

مطالب حقوقی بیشتر در: https://irlawyers.ir/ --- الکترونیک، کامپیوتر، بورس و غیره در: https://229-415.ir/

3. ایمیل‌های کلاهبرداری (Phishing)

ایمیل‌های جعلی که شبیه به ایمیل‌های رسمی بانک‌ها، شبکه‌های اجتماعی یا سرویس‌های ابری هستند و کاربر را به سایت جعلی هدایت می‌کنند.
مثال:
"رمز عبور شما منقضی شده. برای بازیابی، روی لینک زیر کلیک کنید: http://yahoo-login.fake-site.com"
راه دفاع:روی لینک‌ها کلیک نکنید. آدرس واقعی سایت را مستقیماً در مرورگر وارد کنید. به آدرس HTTPS و لوگوی سازمان دقت کنید.

4. حمله CEO Fraud (فریب مدیران)

مهاجم خود را به عنوان مدیر ارشد (CEO، مدیر مالی) جا می‌زند و از کارمند دستور انتقال وجه یا افشای اطلاعات می‌دهد.
مثال:ایمیل از "مدیر مالی": "فوراً 500 میلیون تومان به حساب X واریز کنید. موضوع بسیار حساس است و نباید با کسی در میان بگذاری."
راه دفاع:
...
دستورات مالی و حساس را از طریق کانال‌های تأییدشده (مثلاً تماس تلفنی رسمی) تأیید کنید.

5. ساخت سایت جعلی (Fake Login Page)

مهاجم سایتی شبیه به گوگل، یاهو، بانک یا شبکه‌های اجتماعی می‌سازد و کاربران را با لینک فیشینگ به آن هدایت می‌کند. وقتی کاربر نام کاربری و رمز عبور را وارد می‌کند، اطلاعات مستقیماً به مهاجم ارسال می‌شود.
راه دفاع:قبل از ورود به سایت، آدرس URL را بررسی کنید. سایت‌های واقعی از HTTPS و گواهی SSL استفاده می‌کنند.

6. حمله پیشخوان (Baiting)

...

- کنترل خطا و بازارسال بسته‌های از دست رفته

کاربردها: صفحات وب (HTTP/HTTPS)، ایمیل (SMTP, POP, IMAP)، انتقال فایل (SSH ،FTP)

مطالب حقوقی بیشتر در: https://irlawyers.ir/ --- الکترونیک، کامپیوتر، بورس و غیره در: https://229-415.ir/

2. UDP (User Datagram Protocol)

UDP یک پروتکل **بدون اتصال** و **سریع** است. داده را بدون تأییدیه ارسال می‌کند و سرعت بالاتری دارد، اما تضمینی برای رسیدن آن وجود ندارد. مزایای UDP:

- کاهش تأخیر (Low Latency)
- مناسب برای جریان‌های زنده
- مصرف منابع کمتر

کاربردها: تماس‌های صوتی و ویدئویی (VoIP, Zoom)، بازی‌های آنلاین، DNS، پخش زنده
...

- **آموزش کارکنان:** دوره‌های منظم آگاهی امنیتی برگزار کنید.
- **سیاست‌های صریح:** هرگونه درخواست رمز عبور یا انتقال وجه باید تأیید دو مرحله‌ای داشته باشد.
- **استفاده از احراز هویت دو عاملی (2FA):** حتی اگر رمز عبور افشا شود، دسترسی محدود می‌شود.
- **گزارش حملات:** کاربران باید بتوانند به راحتی ایمیل‌ها یا تماس‌های مشکوک را گزارش دهند.
- **شبیه‌سازی حمله:** تست فیشینگ دوره‌ای برای ارزیابی آمادگی کارکنان.

جمع‌بندی

...

نکته مهم: وقتی یک پورت فعال است، می‌تواند از نوع TCP یا UDP (یا هر دو) باشد. بنابراین، بررسی یک سیستم باید شامل اسکن هر دو نوع پورت باشد.

تقسیم‌بندی پورت‌ها بر اساس شماره

پورت‌ها از 1 تا 65535 هستند و به سه دسته اصلی تقسیم می‌شوند:

1. پورت‌های خطرناک (Well-Known Ports): 1 تا 1023

این پورت‌ها معمولاً برای سرویس‌های سیستمی و استاندارد استفاده می‌شوند و نیاز به دسترسی مدیریتی (root/admin) دارند.

مطالب حقوقی بیشتر در: https://irlawyers.ir/ --- الکترونیک، کامپیوتر، بورس و غیره در: https://229-415.ir/

- مثال: 80 (HTTP)، 443 (HTTPS)، 22 (SSH)، 53 (DNS)

2. پورت‌های ثبت‌شده (Registered Ports): 1024 تا 49151

...

- مهندسی اجتماعی **حمله به انسان** است، نه به سیستم.
- روش‌های آن شامل **فیشینگ، Baiting، CEO Fraud و vishing** و غیره است.
- بسیاری از حملات موفق به دلیل **بی‌توجهی یا عدم آگاهی** انجام می‌شوند.
- مقاومت در برابر آن با **آموزش، سیاست‌گذاری و فرهنگ امنیتی** ممکن است — بخشی از آموزش شبکه و امنیت سایبری.

> ⚠ **هشدار قانونی و اخلاقی:**
> استفاده از تکنیک‌های مهندسی اجتماعی برای دسترسی غیرمجاز به سیستم‌ها، **جرم سایبری محسوب می‌شود**. این محتوا فقط برای **آگاهی، دفاع و آموزش امنیتی** ارائه شده است. مقاومت در برابر این حملات، مسئولیتی اجتماعی و حرفه‌ای است — بخشی اساسی از آموزش شبکه و امنیت سایبری.

...

توضیح

21TCPFTPانتقال فایل — غیرامن (توصیه نمی‌شود)22TCPSSHدسترسی امن به سرور — توصیه شده23TCPTelnetدسترسی از راه دور — غیرامن و قدیمی25TCPSMTPارسال ایمیل — معمولاً فیلتر می‌شود53UDP/TCPDNSتبدیل دامنه به IP80TCPHTTPوب‌سایت‌های غیرامن110TCPPOP3...

برخی از طنزهای قدیمی جامعه هکرها را بازتاب می‌دهد، اما امروزه بیشتر برای یادآوری مراحل یادگیری به کار می‌رود:

1. **جوجه‌هکرها (Script Kiddies)**: افرادی که ابزارهای آماده را بدون درک فنی استفاده می‌کنند. معمولاً فکر می‌کنند با یک اسکریپت ساده "هکر" شده‌اند!
2. **مرغ‌هکرها**: کمی بیشتر می‌دانند، شاید بتوانند یک حمله ساده مثل اسپم یا DoS انجام دهند، اما هنوز عمیق نیستند.
3. **هکرهای قابل احترام**: کسانی که دارند واقعاً یاد می‌گیرند، زبان برنامه‌نویسی، شبکه و سیستم‌عامل را مطالعه می‌کنند — بخشی از آموزش شبکه و امنیت سایبری.

مطالب حقوقی بیشتر در: https://irlawyers.ir/ --- الکترونیک، کامپیوتر، بورس و غیره در: https://229-415.ir/

...

1. **هکرهای پیشکسوت**: افرادی که سال‌ها تجربه دارند و بیشتر به عنوان مربی یا متخصص امنیت فعالیت می‌کنند — فارغ‌التحصیلان واقعی آموزش شبکه و امنیت سایبری.

آدرس IP چیست؟

آدرس IP (Internet Protocol Address) یک شناسه منحصر به فرد است که به هر دستگاه متصل به یک شبکه (مانند اینترنت) اختصاص داده می‌شود. این آدرس شبیه "آدرس خانه" در دنیای واقعی عمل می‌کند و امکان ارسال و دریافت داده بین دستگاه‌ها را فراهم می‌کند — مفهومی بنیادین در آموزش شبکه و امنیت سایبری.

انواع آدرس IP

آدرس‌های IP به دو نوع اصلی تقسیم می‌شوند:

...

nmap مجموعه‌ای از قابلیت‌های حرفه‌ای را در اختیار مدیران شبکه و متخصصان امنیت قرار می‌دهد:

- شناسایی دستگاه‌های فعال در شبکه (Host Discovery)
- اسکن پورت‌ها (TCP و UDP)
- تشخیص سرویس‌ها و نسخه‌های نرم‌افزاری (Service Detection)
- تشخیص سیستم‌عامل (OS Detection)
- تجزیه و تحلیل فایروال و فیلترینگ
- خروجی گزارش‌گیری (متن، Grepable، XML)

رابط Zenmap — نسخه گرافیکی nmap

Zenmap محیطی کاربرپسند فراهم می‌کند که از طریق آن می‌توانید بدون دانش عمیق از دستورات، اسکن انجام دهید.

اجزای اصلی رابط Zenmap:

1. قسمت ورودی (Network Section)

...

- شناسایی دستگاه‌های متصل بدون مجوز (Shadow IT)

مطالب حقوقی بیشتر در: https://irlawyers.ir/ --- الکترونیک، کامپیوتر، بورس و غیره در: https://229-415.ir/

- تأمین انطباق با استانداردهای امنیتی (مثل ISO 27001، PCI DSS)
- پایش شبکه و تشخیص ناهنجاری
- آموزش و تمرین در محیط‌های کنترل‌شده — بخشی از آموزش شبکه و امنیت سایبری

جمع‌بندی

- **Port Scanning**: برای شناسایی سرویس‌های فعال روی یک دستگاه
- **IP Scanning**: برای شناسایی دستگاه‌های فعال در یک شبکه
- هر دو ابزاری قدرتمند در دست مدیران شبکه و امنیتی هستند
- اما **بدون مجوز، غیرقانونی محسوب می‌شوند**
- همیشه از این ابزارها با مسئولیت و اخلاق حرفه‌ای استفاده کنید — اصلی‌ترین نکته در آموزش شبکه و امنیت سایبری

...

```
Proto Local Address Foreign Address State PID
TCP 0.0.0.0:80 0.0.0.0:0 LISTENING 4
TCP 127.0.0.1:3306 0.0.0.0:0 LISTENING 1234
UDP 0.0.0.0:53 *:* 5678
```

برای شناسایی فرآیند، PID را در Task Manager جستجو کنید.

> **نکته امنیتی:** اگر پورت‌های ناشناخته‌ای باز بودند (مثل 6666، 7778)، ممکن است نشانه وجود بدافزار یا تروجان باشد. همیشه سرویس‌های غیرضروری را غیرفعال کنید — نکته‌ای مهم در آموزش شبکه و امنیت سایبری.

IP Scanning — شناسایی دستگاه‌های فعال در شبکه

قبل از اسکن پورت، باید بدانید کدام دستگاه‌ها در شبکه فعال هستند. این فرآیند **Host Discovery** نام دارد.

مطالب حقوقی بیشتر در: https://irlawyers.ir/ --- الکترونیک، کامپیوتر، بورس و غیره در: https://229-415.ir/