# دوره جامع هک قانونمند و مهندسی امنیت سایبری

Advanced Cybersecurity & Ethical Hacking

Complete Career Training Program

---

راهنمای کامل و گام‌به‌گام برای تبدیل شدن به یک مهندس امنیت حرفه‌ای

از صفر مطلق تا متخصص امنیت سایبری

---

این دوره توسط تیم امنیت صفر و یک سایبر طراحی شده است

---

هشدار قانونی: این سند صرفاً برای آموزش امنیت سایبری قانونمند تهیه شده است

هرگونه استفاده غیرقانونی از مطالب بر عهده کاربر می‌باشد

این دوره مسیر شغلی شما را از یک فرد مبتدی تا یک مهندس امنیت حرفه‌ای طراحی کرده است

# فصل ۲

## فرماندهی لینوکس برای هکرها

لینوکس سیستم عامل شماره یک در امنیت سایبری است. شما باید لینوکس را در سطح حرفه‌ای بلد باشید تا بتوانید هکر شوید

# ساختار فایل‌سیستم لینوکس

## ساختار فایل‌سیستم لینوکس :

/

├── /bin - دستورات پایه (ls, cp, mv)

├── /boot - فایل‌های بوت

├── /dev - دستگاه‌ها (sda, tty, null)

├── /etc - فایل‌های پیکربندی

├── /home - دایرکتوری کاربران

├── /lib - کتابخانه‌ها

├── /media, /mnt - مانت

├── /opt - نرم‌افزارهای اضافی

├── /proc - فایل‌های سیستمی (فرایندها)

├── /root - کاربر root

├── /sbin - دستورات سیستمی

├── /tmp - فایل‌های موقت

├── /usr - برنامه‌های کاربر

└── /var - لاگ‌ها، دیتابیس‌ها

# دستور ضروری لینوکس برای هکر

مدیریت فایل :

| | |
|---|---|
| ls -la | لیست فایل‌ها با جزئیات |
| pwd | مسیر فعلی |
| cd~ | برو به home |
| cp -r src dst | کپی بازگشتی |
| mv src dst | انتقال یا تغییر نام |
| rm -rf dir | حذف بازگشتی (مراقب باشید!) |
| mkdir -p a/b/c | ساخت دایرکتوری تو در تو |
| touch file.txt | ساخت فایل خالی |
| find / -name "*.conf" | جستجوی فایل |
| locate nmap | جستجوی سریع در دیتابیس |
| cat file.txt | نمایش فایل |
| less file.txt | نمایش صفحه‌بندی شده |
| tail -f log.txt | دنبال کردن انتهای فایل |

مدیریت فرایند :

| | |
|---|---|
| ps aux | همه فرایندها |
| top / htop | مانیتورینگ لحظه‌ای |
| kill -9 PID | کشتن فرایند |
| pkill -f name | کشتن با نام |
| jobs | نمایش کارهای پس‌زمینه |
| bg / fg | ارسال به پس/پیش زمینه |
| nohup cmd & | اجرا پس از خروج |

شبکه :

| نمایش IP | ip a |
| --- | --- |
| جدول مسیریابی | ip route |
| پورت‌های باز | ss -tulpn |
| پورت‌ها (قدیمی) | netstat -ano |
| تست ارتباط | ping 8.8.8.8 |
| مسیریابی | traceroute 8.8.8.8 |
| جستجوی DNS | dig google.com ANY |
| DNS lookup | nslookup google.com |
| هدر HTTP | curl -I http://site.com |
| دانلود | wget http://file.com |

کاربران و دسترسی :

| | |
|---|---|
| کاربر فعلی | whoami |
| UID, GID | id |
| دسترسی‌های sudo | sudo -l |
| تغییر به کاربر | su - user |
| ساخت کاربر | useradd -m u1 |
| تغییر رمز | passwd u1 |
| تغییر مجوز | chmod 755 file |
| تغییر مالک | chown user:group file |
| پیشفرض مجوز | umask |
| ACL | getfacl file |

فشرده‌سازی و بایگانی :

| بایگانی | tar -cvf archive.tar dir/ |
| --- | --- |
| خارج کردن | tar -xvf archive.tar |
| فشرده با gzip | tar -czvf archive.tar.gz dir/ |
| | tar -xzvf archive.tar.gz |
| | zip -r archive.zip dir/ |
| | unzip archive.zip |

مدیریت سرویس‌ها :

| | systemctl start service |
| --- | --- |
| | systemctl stop service |
| فعالسازی در بوت | systemctl enable service |
| | systemctl status service |
| دنبال کردن لاگ سرویس | journalctl -u service -f |

# Bash Scripting برای هکر

## اسکریپت‌نویسی bash برای خودکارسازی وظایف هکری ضروری است :

```
===== اسکنر سریع شبکه =====

echo "[*] Scanning network 192.168.1.0/24"...

for ip in $(seq 1 254); do

ping -c 1 -W 1 192.168.1.$ip | grep "bytes from" | cut -d" " -f4 | cut -d":" -f1&

done

wait

echo "[*] Done"!
```

```
===== Bash سریع با Port Scanner =====

HOST=$1

PORTS=(21 22 23 25 53 80 110 143 443 445 1433 1521 2049 3306 3389 5432 5900 6379
8080 8443)

echo "[*] Scanning $HOST"...

for port in "${PORTS[@]}"; do

timeout 1 bash -c "echo >/dev/tcp/$HOST/$port" 2>/dev/null && echo "  [+] Port $port is OPEN"

done

echo "[*] Scan complete"!
```

===== Hydra با Brute Force SSH =====

hydra -l admin -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.100 -t 4 -V

===== Brute Force FTP =====

hydra -L users.txt -P pass.txt ftp://192.168.1.100

===== Brute Force HTTP POST =====

hydra -l admin -P pass.txt 192.168.1.100 http-post-form "/login:user=^USER^&pass=^PASS^:F=Invalid"

# Forensics لینوکس

( ردیابی و تحلیل )

آخرین کاربران لاگین شده

last

لاگین‌های ناموفق

lastb

کاربران آنلاین

w

تاریخچه دستورات

history

cat ~/.bash_history

cat ~/.zsh_history

## بررسی لاگ‌ها

/var/log/auth.log احراز هویت

/var/log/syslog سیستم

/var/log/kern.log کرنل

journalctl -xe لاگ سیستم

## فرایندهای مخفی

ps aux | grep -v "^\["

lsmod ماژول‌های کرنل

## فایل‌های مخفی

find / -name ".*" -type f | head -50

## اتصالات شبکه

ss -tunap

lsof -i فایل‌های باز شده توسط شبکه

# Hardening لینوکس

( امن‌سازی )

## به‌روزرسانی سیستم

sudo apt update && sudo apt upgrade -y

## غیرفعال کردن سرویس‌های غیرضروری

sudo systemctl disable --now bluetooth cups avahi-daemon

## پیکربندیSSH

/etc/ssh/sshd_config:

PermitRootLogin no

PasswordAuthentication no

Port 2222

## فایروال

sudo ufw enable

sudo ufw default deny incoming

sudo ufw allow ssh

sudo ufw allow 80,443/tcp

## Fail2Ban

(ضد Brute Force)

```
sudo apt install fail2ban

sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
```

# تمرینات جامع فصل ۲

**۱. تمام ۵۰ دستور بخش ( دستور ضروری لینوکس ) را یک بار اجرا کنید و خروجی را مشاهده کنید**

**۲. یک اسکریپت bash بنویسید که IP شما را گرفته و با nmap اسکن کند**

**۳. اسکریپت بنویسید که از یک فایل IP (targets.txt)ها را خوانده و ping کند**

**۴. یک for-loop بنویسید که پورت‌های 1-1024 را با bash اسکن کند (بدون nmap)**

**۵. Cron job تنظیم کنید که هر شب یک اسکن از شبکه بگیرد**

**۶. یک سرویس systemd سفارشی برای یک اسکریپت بنویسید**

**۷. فایل‌های لاگ auth.log را تحلیل کنید و IPهای مشکوک را پیدا کنید**

**۸. یک لینوکس سرور (در VM) را با راهنمای Hardening امن کنید**

**۹. Fail2Ban را برای SSH پیکربندی کنید**

**۱۰. یک bash script بنویسید که با یک دستور تمام مراحل Recon اولیه را انجام دهد**