درس ۱۰ از ۱۲

Arch & Kali Linux

Rolling · pacman · AUR · Security Lab

گشتی در ابزارهای Kali: شناسایی، وب، رمزها، بی‌سیم و فارنزیک

دوره کامل · Arch 2026.11 · Kali 2026.3 (Nov 2026)



در درس دهم چه یاد می‌گیرید

- مراحل یک ارزیابی مجاز
- شناسایی: Nmap روی شبکه لابراتوار شما
- اصول آزمایش ویب: Burp Suite، Nikto، Gobuster روی DVWA
- رمزها: چرا hash های قوی و رمزهای طولانی مهم هستند
- تحلیل ترافیک با Wireshark
- بی‌سیم: Kali چه چیزی را می‌تواند آزمایش کند — و محدودیت‌های قانونی
- فارنزیک: Autopsy و حالت بوت forensic

مراحل یک ارزیابی مجاز

ابزارهای نمونه	هدف	مرحله
اسناد — نه نرم‌افزار	اجازه کتبی، محدوده، قوانین	**۰. اجازه**
nmap، whatweb، theHarvester (OSINT)	پیدا کردن میزبان‌ها و سرویس‌ها در محدوده	**۱. شناسایی**
nikto، nuclei، OpenVAS/GVM	پیدا کردن ضعف‌ها	**۲. تحلیل آسیب‌پذیری**
Burp Suite، Metasploit (لابراتوار)	اثبات امن خطر، داخل قوانین	**۳. تأیید**
یادداشت‌ها، عکس صفحه، قالب گزارش	توضیح یافته‌ها و اصلاح‌ها	**۴. گزارش**
Kali Purple (درس ۱۱)	همان قدم‌ها نشان می‌دهد چه چیزی patch و نظارت شود	**دید مدافع**

شناسایی: Nmap (فقط لابراتوار)

```
kali@kali:~$ ip -br a | grep eth1            # confirm you are on the lab network
eth1  UP  192.168.56.10/24
kali@kali:~$ nmap -sn 192.168.56.0/24        # which lab hosts are up?
Nmap scan report for 192.168.56.20  Host is up.
Nmap scan report for 192.168.56.30  Host is up.
kali@kali:~$ nmap -sV -T3 192.168.56.20      # services and versions on target1
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
22/tcp open  ssh     OpenSSH 4.7p1
80/tcp open  http    Apache httpd 2.2.8
kali@kali:~$ nmap -sV -oA ~/lab/target1 192.168.56.20   # save results for the report
```

اصول آزمایش وب (روی DVWA / Juice Shop)

درس مدافع	چه کاری می‌کند	ابزار
هرگز به ورودی کلاینت اعتماد نکنید	proxy برای دیدن و تغییر درخواست‌های مرورگر	Burp Suite (Community)
banner نسخه را پنهان/patch کنید	شناسایی فناوری‌ها و نسخه‌های وب	whatweb
فایل‌های پیش‌فرض را حذف، تنظیمات را سخت کنید	بررسی تنظیمات اشتباه رایج وب سرور	nikto
به URL های «مخفی» تکیه نکنید	پیدا کردن فولدرهای پنهان در برنامه لابراتوار	gobuster / ffuf
از parameterized query استفاده کنید	آزمایش SQL injection در لابراتوار	sqlmap
راهنمای کودنویسی امن	دسته‌های اصلی خطرهای وب	OWASP Top 10

رمزها و Hash ها (hash های آزمایشی خودتان)

```
# Create YOUR OWN test hashes to learn why password strength matters
kali@kali:~$ echo -n 'summer2026' | sha256sum
kali@kali:~$ mkpasswd -m yescrypt 'summer2026'     # modern Linux hash (slow on purpose)
$y$j9T$...
kali@kali:~$ hashid '<hash>'                       # identify a hash type
kali@kali:~$ ls /usr/share/wordlists/               # rockyou.txt.gz etc.
# Lesson for defenders:
#   short/common passwords fall to wordlists in seconds
#   long passphrases + slow hashes (yescrypt, bcrypt, Argon2) + MFA resist attacks
#   never store plain or fast-hashed (MD5/SHA1) passwords
```

تحلیل ترافیک با Wireshark

```
kali@kali:~$ sudo usermod -aG wireshark kali     # capture without root (log in again)
kali@kali:~$ wireshark &                          # GUI: capture on eth1 (lab)
kali@kali:~$ tshark -i eth1 -c 20 -f 'port 21'    # CLI capture of lab FTP
# Display filters:
#   ip.addr == 192.168.56.20      http.request      ftp      tls.handshake
# Lesson: FTP and plain HTTP send passwords in clear text — use SFTP/HTTPS
# Capture only on networks you own or are authorized to monitor
```

بی‌سیم: Kali چه چیزی را آزمایش می‌کند — و محدودیت‌ها

موضوع	جزئیات
سخت‌افزار	Wi-Fi USB adapter با پشتیبانی monitor mode (VM به USB passthrough نیاز دارد)
ابزارها	مجموعه aircrack-ng، kismet، wifite، bettercap
چه نشان می‌دهد	passphrase های ضعیف WPA2، نقص‌های WPS، access point های جعلی
درس مدافع	WPA3 یا WPA2 با passphrase طولانی؛ WPS را خاموش؛ firmware روتر را آپدیت کنید
محدودیت قانونی	فقط access point خودتان یا اجازه کتبی — هرگز همسایه، کافه، مکتب
همچنین غیرقانونی	jam کردن یا قطع کردن دستگاه‌های دیگران

فارنزیک: Autopsy و حالت Forensic

```
# Boot Kali live in 'forensic mode': no auto-mount, no swap, no disk writes
kali@kali:~$ sudo apt install -y kali-tools-forensics
kali@kali:~$ sudo dc3dd if=/dev/sdb hash=sha256 of=/cases/usb.img log=/cases/usb.log
kali@kali:~$ sha256sum /cases/usb.img            # verify the image matches the log
kali@kali:~$ autopsy                              # web UI: new case, add usb.img
kali@kali:~$ binwalk firmware.bin ; exiftool photo.jpg
# Work on the IMAGE, never the original evidence; keep a chain-of-custody record
```

خلاصه و کارخانگی

- مراحل: اجازه، شناسایی، تحلیل، تأیید، گزارش
- nmap -sn / -sV فقط روی 192.168.56.0/24؛ ذخیره با -oA
- ویب: Burp، whatweb، nikto، gobuster، sqlmap روی DVWA/Juice Shop
- رمزها: passphrase طولانی + hash کُند + MFA؛ Wireshark خطر متن آشکار را نشان می‌دهد
- بی‌سیم و capture فقط روی شبکه‌های خودتان؛ فارنزیک روی ایمِج‌ها
- کارخانگی: target1 را اسکن کنید، سرویس‌ها را فهرست کنید، و ۳ توصیه «چگونه اصلاح کنیم» بنویسید

تشکر از شما! 🤲

ویدیوها و PDF های رایگان: www.MyWebUniversity.com

سلایدهای این درس: MyWebUniversity.com/presentations

YouTube: @MyWebUniversity-Dari · @MyWebUniversity

وحیدالله لطفی – مؤسس و رئیس IT مای وب یونیورسیتی، و استاد علوم کامپیوتر

یاد بگیرید و به دیگران انتقال دهید