درس ۱۱ از ۱۲

Arch & Kali Linux

Rolling · pacman · AUR · Security Lab

ساختن لابراتوار تمرین امن و دفاع با Kali Purple

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



در درس یازدهم چه یاد می‌گیرید

- طراحی لابراتوار: جداسازی، هدف‌ها، snapshot ها
- ساختن شبکه host-only
- هدف‌های تمرینی: Metasploitable، DVWA، Juice Shop در کانتینر
- قوانین امنیت لابراتوار و یک دفترچه لابراتوار
- Kali Purple: نسخه دفاعی
- کشف فعالیت لابراتوار با Suricata و لاگ‌ها
- Purple teaming: حمله، کشف، اصلاح، تکرار

طراحی لابراتوار

بخش	انتخاب ما	چرا
Hypervisor	VirtualBox یا KVM/virt-manager	رایگان، snapshot، شبکه‌های داخلی
شبکه	Host-only 192.168.56.0/24، بدون راه به اینترنت	هدف‌ها به LAN یا اینترنت شما نمی‌رسند
مهاجم	kali (192.168.56.10) + NAT برای آپدیت	در زمان تمرین می‌توانید NAT را خاموش کنید
هدف‌ها	target1 Metasploitable 2 (.20)، target2 کانتینرها (.30)	عمداً آسیب‌پذیر — هرگز باز نگذارید
مدافع	Kali Purple VM (.40) یا Suricata روی target2	ترافیک خودتان را از طرف آبی ببینید
Snapshot ها	'clean' روی هر VM	بعد از هر تمرین ریست کنید

ساختن شبکه Host-only

```
# VirtualBox
$ VBoxManage hostonlyif create                          # -> vboxnet0
$ VBoxManage hostonlyif ipconfig vboxnet0 --ip 192.168.56.1 --netmask 255.255.255.0
$ VBoxManage modifyvm target1 --nic1 hostonly --hostonlyadapter1 vboxnet0
$ VBoxManage modifyvm kali --nic2 hostonly --hostonlyadapter2 vboxnet0

# KVM / libvirt: an isolated network (no <forward>)
$ cat lab.xml
<network><name>lab</name><ip address='192.168.56.1' netmask='255.255.255.0'/></network>
$ sudo virsh net-define lab.xml && sudo virsh net-start lab && sudo virsh net-autostart lab
# Verify from target1: ping 8.8.8.8 must FAIL
```

هدف‌های تمرینی

```
# target1: Metasploitable 2 (download from its official SourceForge page)
#   Import the VMDK, host-only NIC ONLY, login msfadmin/msfadmin (lab only!)

# target2: vulnerable web apps in containers (on an isolated VM)
student@target2:~$ docker run -d --name dvwa -p 8080:80 vulnerables/web-dvwa
student@target2:~$ docker run -d --name juice -p 3000:3000 bkimminich/juice-shop
student@target2:~$ docker ps --format '{{.Names}} {{.Ports}}'
dvwa   0.0.0.0:8080->80/tcp
juice  0.0.0.0:3000->3000/tcp
# Browse from Kali: http://192.168.56.30:8080  and  http://192.168.56.30:3000
```

قوانین امنیت لابراتوار

تمرین	قانون
فقط host-only؛ با آزمایش ping تأیید کنید	هدف‌ها هرگز روی انترنت
کاربران، رمزها و فایل‌های جعلی	بدون دیتای واقعی در لابراتوار
هر تمرین تمیز شروع می‌شود	قبل snapshot، بعد بازگردانی
تاریخ، هدف، فرمان‌ها، نتایج، آنچه یاد گرفتید	یک دفترچه لابراتوار نگه دارید
بدون shared folder یا clipboard به میزبان	نمونه‌های بدافزار فقط در VM جدا
هدف‌ها عمداً آسیب‌پذیر — و جدا — می‌مانند	Kali را آپدیت کنید، نه هدف‌ها را

Kali Purple: نسخه دفاعی

ابزارهای نمونه در Kali Purple	بخش (NIST CSF)
کشف دارایی‌ها و آسیب‌پذیری‌ها (nmap، GVM/OpenVAS)	Identify
سخت‌سازی، فایروال‌ها، تنظیمات امن	Protect
Suricata و Zeek (IDS شبکه)، Elastic/OpenSearch SIEM، Arkime	Detect
TheHive (مدیریت پرونده)، Cortex، playbook ها	Respond
بکاپ‌ها، بازگردانی و درس‌های آموخته	Recover
Kali Purple ISO، یا: sudo apt install kali-linux-purple / kali-tools-detect	نصب

فعالیت لابراتوار خودتان را با Suricata کشف کنید

```
purple@purple:~$ sudo apt install -y suricata
purple@purple:~$ sudo vim /etc/suricata/suricata.yaml    # af-packet: interface: eth1
purple@purple:~$ sudo suricata-update                   # download open rule sets
purple@purple:~$ sudo systemctl enable --now suricata
# From kali: nmap -sV 192.168.56.20   (your own lab scan)
purple@purple:~$ sudo tail -f /var/log/suricata/fast.log
[**] ET SCAN Suspicious inbound to mySQL port 3306 [**] 192.168.56.10 -> .20
purple@purple:~$ jq 'select(.event_type=="alert") | .alert.signature' \
      /var/log/suricata/eve.json | sort | uniq -c | sort -rn | head
```

Purple Teaming: حمله، کشف، اصلاح، تکرار

قدم	مثال در لابراتوار ما
۱. حمله (red)	target1 را با nmap -sV اسکن کنید؛ سرویس قدیمی FTP را پیدا کنید
۲. کشف (blue)	آیا Suricata هشدار داد؟ آیا لاگ target1 اتصال‌ها را نشان می‌دهد؟
۳. بهبود کشف	قوانین را تنظیم کنید، لاگ‌ها را به SIEM بفرستید
۴. اصلاح	روی یک کاپی target1: سرویس را خاموش/ارتقا دهید، قانون فایروال اضافه کنید
۵. تکرار	اسکن را دوباره اجرا کنید: سرویس رفته، هشدار هنوز کار می‌کند
۶. گزارش	بنویسید چه پیدا کردید، چه دیدید، و چه اصلاح کردید

خلاصه و کارخانگی

- شبکه host-only و جدا؛ تأیید کنید هدف‌ها به انترنت نمی‌رسند
- هدف‌ها: Metasploitable 2، DVWA، Juice Shop — عمداً آسیب‌پذیر، هرگز باز نیستند
- امنیت: بدون دیتای واقعی، snapshot، دفترچه لابراتوار، بدافزار فقط در VM جدا
- Kali Purple: NIST CSF — شناسایی، محافظت، کشف، پاسخ، بازیابی
- Suricata اسکن‌های لابراتوار شما را کشف می‌کند؛ purple teaming = حمله، کشف، اصلاح، تکرار
- کارخانگی: لابراتوار را بسازید، جداسازی را تأیید کنید، یک چرخه purple team اجرا و یک گزارش یک صفحه‌ای 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