6. **Install rootkits detectors and study variety of options**

RootKits

1. Rootkits are special type of malware gives the root level access to the attacker.
2. Wrapper and cloak for other code.
3. Not necessarily malicious.
4. Insidiously cloaked.
5. Quiet behaviour.
6. Can be installed by unprivileged user.
7. Nearly impossible to detect and remove.

Infecting the target with rootkits

1. Determine what code you want to hide(payload).
2. Develop or buy a rootkit packager.
3. Wrap the payload with the packager.
4. Distribute the rootkit to the target.
5. Spyware is a broad category of software.
6. Monitors users and network activity.
7. Reports back to source.

List the latest rootkit checkers or antiviruses available for linux and windows

Rkhunter and chkrootkit are used to check any rootkits installed in kali linux. To get rkhunter tool, type the following command
>>sudo su
Enter the password for kali
>>apt-get install rkhunter
It will install the rkhunter in kali
>>
It will scan the kali for any root kits installed.

Using chkrootkit
>>sudo su
Enter the password for kali
>>apt-get install **chkrootkit**
It will install the chkrootkit in kali
>> chkrootkit -h
It will give the options for chkrootkit as follows

```
┌──(geet㉿ kali)-[~/Downloads]
└─$ chkrootkit -h
Usage: /usr/sbin/chkrootkit [options] [test ...]
Options:
        -h               show this help and exit
        -V               show version information and exit
        -l               show available tests and exit
        -d               debug
        -q               quiet mode
        -x               expert mode
        -e 'FILE1 FILE2'  exclude files/dirs from results. Must be followed by a
 space-separated list of files/dirs.
                         Read /usr/share/doc/chkrootkit/README.FALSE-POSITIVES
first.
        -s REGEXP        filter results of sniffer test through 'grep -Ev REGEX
P' to exclude expected
                         PACKET_SNIFFERs. Read /usr/share/doc/chkrootkit/README
.FALSE-POSITIVES first.
        -r DIR           use DIR as the root directory
        -p DIR1:DIR2:DIRN path for the external commands used by chkrootkit
        -n               skip NFS mount points
        -T FSTYPE        skip mount points of the specified file system type
```

To scan the system just type as follows

>>chkrootkit

1. It will scan the kali for any root kits installed

8. Study of Techniques uses for Web Based Password Capturing.

Password cracking typically refers to the process of recovering scrambled passwords. It can be used to help a user get back a forgotten password or to help a system administrator to check for weak passwords. But more often, password cracking is used y bad actors to gain unauthorized access to systems and resources.

Password cracking generally falls into two categories:

1. Password guessing
2. Password cracking.

Types of Passwords

1. System Password (Windows password, Android lock, Bypass)
2. Browser password(Browser all store passwords)
3. Application password(app password, file password, etc)
4. Wifi password

Attacks

1. Brute Force attack

2. Dictionary Attack
3. Rainbow Table
4. Credential Stuffing attack
5. Hybrid attack
6. Key loggers
7. Phishing attacks

Tools in kali linux

1. Hashcat
2. John the Ripper
3. Crunch
4. Hydra
5. Cewl

Steps for password Cracking

1. Now open Kali Linux and metasploitable machine.
2. Now go Applications and scroll to password attacks. By selecting the password attacks, You can view all types of password attacks supported by KL.
3. Now we will use hydra tool. Type the command to learn about hydra tool.
   >>hydra
4. Open metasploitable tool, user name – msfadmin, password- msfadmin. Get IP address of metasploitable m/c by typing ifconfig.
5. Our metasploitable m/c address is 19 2.168.56.101.
6. Now go to Kali Linux, create a password (text file) in the desktop and type the following command
   $hydra –l msfadmin –P Desktop/text.txt ftp://192.168.56.101

Next we will crack a zip file's password

1. Create a text file in the desktop by **right-click on desktop** and select **create document→empty File.**
2. Give the filename as **sample-file.txt**
3. In the terminal go to Desktop and create password protected zip file as follows.
4. **$zip sample-zip –P abc sample.txt**
5. Type ls to view the files in the desktop. It should display the password protected zip file in the list.
6. Create hash file as follows.
7. **$zip2john sample-zip.zip > hash1.txt**

8. It will create the hash1.txt in the desktop. We can display using cat command.
9. **With $sudo hash1.txt,** we get
   sample.zip/sample.txt:$pkzip$1*2*2*0*1e*12*d4313f2b*0*44*0*1e*710b*c522094babf4491ef59fe9ebb3d:$pkzip$ sample.txt/sample.zip::sample.zip
10. Open hash1.txt in nano editor and delete the contents from start and end till $.
11. The final contents will be
12. $pkzip$1*2*2*0*1e*12*d4313f2b*0*44*0*1e*710b*c522094babf4491ef59fe9ebb3d:$pkzip$
13. From here we see that it is using **pkzip** mode to archive.
14. Now check the mode number with
15. **$hashcat -help**
16. For pkzip we get
17. 17220 | PKZIP (Compressed Multi-File) | Archive
    17200 | PKZIP (Compressed) | Archive
    17225 | PKZIP (Mixed Multi-File) | Archive
    17230 | PKZIP (Mixed Multi-File Checksum-Only) | Archive
    17210 | PKZIP (Uncompressed) | Archive
    20500 | PKZIP Master Key | Archive
    20510 | PKZIP Master Key (6 byte optimization) | Archive

18. Now we can crack the pwd with hashcat command. Type the hashcat command as follows. Here **text in the command** in the password file. Or we can also use rockyou.txt file
    $hashcat –a 0 –m 17210 hash1.txt passlist.txt
19. -m is the mode in which password protected archived file is created.
20. -a is the attack mode
21. [Attack Modes] -

    # | Mode
    ===+======
    0 | **Straight**
    1 | Combination
    3 | Brute-force
    6 | Hybrid Wordlist + Mask
    7 | Hybrid Mask + Wordlist
    9 | Association

22. **$hashcat -h** for more details.
    For zip files – 13600, 7-zip – 11600 and so on. We can check the mode by analysing the hash.txt file.
23. It will give the password after $ sign in the output.

24. We can create the archive files directly from the desktop. Right click on the file and select archive option and select the type of the archive file by clicking on the dropdown list.
25. For 7zip we need some john-the-ripper packages. To get those type github john the ripper github in google. Go to the site and copy the link by clicking code.
26. Create a file sample.txt and add some contents.
27. Right click on the file – select 'compress 1 file' option.
28. Give the filename as sample.txt.7z and select the extension as 7z.
29. Select encrypt option and give the password.
30. Here the encrypted .7z file is generated.
31. Go to Terminal in Desktop, clone the john-the-ripper packages as follows
32. **$git clone "https://github.com/opewall/john.git" -b bleeding-jumbo john**
33. The above will install john-the-ripper packages in john folder in desktop.
34. Go to /john/run
35. **$ls**
36. **$chmod +x 7z2john.pl**
37. **$./7z2john.pl /home/geet/Desktop/sample.txt.7z>/home/geet/Desktop/hash3.txt**
38. It will create hashfile in Desktop. Open it in nano or text editor and delete till $ from beginning and type the following command in Desktop folder.
39. **$hashcat -a 0 -m 11600 hash3.txt passlist.txt**

40. In the terminal, in the /desktop
41. Navigate

7. Implement Passive scanning, active scanning, session hijacking, cookies grabbing.

Aim::

To perform a port scanning experiment using Nmap to identify open ports on a target system and gain insight into its network security posture.

Use burpsuit to intercept the traffic between source and destination.

Requirements:

1. **Nmap**: Ensure that Nmap is installed on your system. You can download it from the official website (https://nmap.org/download.html) or install it using package managers like apt (for Linux) or Homebrew (for macOS).

2. **Target System**: Choose a target system or network to scan. Ensure that you have permission to perform the scan, as port scanning can be considered intrusive and may violate network policies or laws if conducted without authorization.

Steps:

1. Identify the Target:

- Determine the IP address or hostname of the target system or network you want to scan.

2. Determine Scan Type:

- Decide on the type of scan you want to perform based on your objectives and the level of intrusiveness allowed:
- **TCP SYN Scan (-sS)**: Stealthy and fast scan, commonly used for initial reconnaissance.
- **TCP Connect Scan (-sT)**: Completes the TCP three-way handshake, less stealthy than SYN scan.
- **UDP Scan (-sU)**: Scans for open UDP ports.
- **Intensive Scan (-T4 or -T5)**: Faster scans, but may be more detectable.
- **Comprehensive Scan (-A)**: Enables OS detection, version detection, script scanning, and traceroute.
- For this experiment, let's use the TCP SYN Scan (-sS) as it's stealthy and efficient.

3. Execute the Scan:

- Open a terminal or command prompt.
- Use the following command syntax to perform the TCP SYN Scan:

```
nmap -sS [target]
```

Replace `[target]` with the IP address or hostname of the target system.

- Optionally, you can specify additional options to customize the scan according to your requirements.

4. Analyze the Results:

- Once the scan is complete, Nmap will provide a detailed report indicating the status of each scanned port (open, closed, filtered) and may include additional information

such as service versions, operating system detection, and potential vulnerabilities.
- Interpret the results to identify open ports, which could indicate services running on the target system. Pay attention to any unexpected or unauthorized services that may pose security risks.

5. Experiment with Additional Options:
- Explore other Nmap options and scan types to gain a deeper understanding of network reconnaissance techniques.
- Experiment with different timing options (-T), output formats (-oA, -oX, -oG), and script scanning (--script) to tailor the scan to your specific requirements.

6. Documentation and Reporting:
- Document the scan parameters, results, and any observations or insights gained during the experiment.
- Prepare a comprehensive report summarizing the findings, including recommendations for mitigating any identified security vulnerabilities or risks.

By following these steps, you can conduct a thorough port scanning experiment using Nmap to assess the security posture of a target system or network. Remember to approach the experiment responsibly and ethically, respecting the privacy and integrity of the target infrastructure.

Use burpsuit to intercept the traffic between source and destination.

Here are the **steps to install Burp Suite Community Edition on Windows**:

✅ Step 1: Download Burp Suite Community Edition

1. Go to the official PortSwigger website: https://portswigger.net/burp/communitydownload
2. Click on the **"Download"** button for **Windows**.
3. It will download a `.exe` installer (e.g., `BurpSuiteCommunity_2025.5.1_64bit.exe`).

✅ Step 2: Run the Installer

1. Locate the downloaded `.exe` file and **double-click** it.
2. If prompted by **Windows SmartScreen**, click **"More info" → "Run anyway"**.
3. Follow the installation wizard:
    - Click **Next**
    - Choose installation directory (default is fine)
    - Click **Install**
4. After installation, click **Finish** to close the setup wizard.

✅ Step 3: Launch Burp Suite

1. Open the **Start Menu**, search for **"Burp Suite Community Edition"**, and launch it.
2. On the first run:
    - Accept the license agreement.
    - Choose **"Temporary Project"** or create a new one.
    - Click **"Start Burp"**.

✅ Step 4: Set Up Your Browser (Optional but Recommended)

To capture and analyze HTTP/HTTPS traffic:

1. Configure your browser to use Burp as a **proxy**:
    - **Proxy IP:** `127.0.0.1`
    - **Port:** `8080`
2. Install **Burp's CA Certificate** to avoid SSL warnings:
    - In Burp, go to **Proxy** > **Options** > **Import / Export CA Certificate**.
    - Or, visit `http://burp` in your proxy-configured browser to download it directly.

Here are the **steps to configure Firefox to use Burp Suite** for intercepting HTTP/HTTPS traffic:

✅ Step 1: Launch Burp Suite

1. Start **Burp Suite Community Edition**.
2. Create or open a project (choose **Temporary Project → Start Burp**).
3. Go to **Proxy → Options** tab.
4. Confirm that **Proxy Listener** is active on `127.0.0.1:8080` (default).

✅ Step 2: Open Firefox and Set Proxy Settings

1. Open **Firefox**.
2. In the address bar, type: `about:preferences` and hit Enter.
3. Scroll to the **bottom** and click on **"Settings…"** under the **Network Settings** section.
4. In the **Connection Settings** dialog:
    - Select **Manual proxy configuration**.
    - Set the **HTTP Proxy** to: `127.0.0.1`
    - Set the **Port** to: `8080`
    - **Check the box**: “Use this proxy server for all protocols”
    - Click **OK**

Now Firefox is routing all traffic through Burp Suite.

✅ Step 3: Install Burp's CA Certificate in Firefox (for HTTPS sites)

1. In Firefox, go to: `http://burp`
    - This opens Burp's web interface.
    - Click on **"CA Certificate"** to download it (`cacert.der` file).
2. In Firefox:
    - Open `about:preferences`
    - Scroll to **Privacy & Security**
    - Under **Certificates**, click **"View Certificates…"**
    - Go to the **Authorities** tab and click **"Import…"**
    - Select the downloaded `cacert.der` file.
    - **Check both boxes**:
        - "Trust this CA to identify websites"
        - "Trust this CA to identify email users" (optional)
    - Click **OK**

✅ Step 4: Test the Setup

1. Make sure **Intercept** is **ON** in Burp (Proxy → Intercept).
2. Open any website in Firefox.
3. Burp should capture the request.

✅ To Restore Firefox to Default Later:

1. Go to `about:preferences` → **Network Settings** → **Settings…**
2. Select **Use system proxy settings** or **No proxy**
3. Click **OK**

Now open the new tab in the browser and check if the traffic is intercepted by the burpsuit or not. And collect all the information, whatever the burpsuit provides.