3.	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 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

B

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.
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.

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

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