**Traffic Sniffing**

**TCP Sniffing**

**5. Observe the traffic in Wireshark and report the following**

* **Application data sent**
* **Application data received**
* **IP address of the server that “tcp\_client” communicates with**
* **Port that the communication occurs on**

**HTTP Sniffing**

**8. Observe the traffic in Wireshark and report the following**

* IP address of the server that "http\_client" communicates with
* **“GET” request being made**
* **Application data received**

**HTTPS Sniffing**

**11. Observe the traffic in Wireshark and report the following**

* The protocol that is being used
* **Take a screenshot showing the “Client/Server Hello” message**

**OpenSSL**

**Decrypting Messages**

**14. What is the decrypted string?**

**OpenSSL Configuration**

**16. How many ciphers are accepted?**

**17. What are the server’s preferred ciphers?**

**19. Turn in a screenshot of the “Client Hello” request with the** "Cipher Suites" section expanded under the "Secure Sockets Layer".

20. What was the “openssl” command that you used?

**SSL DOS**

**Insecure Renegotiation Allowed**

**21. What version of OpenSSL is running on the insecure server?**

**24. What is the max number of connections that you see?**

**25. Af**ter “thc-ssl-dos” reaches the max number of connections, reload the insecure server's webpage. How long does it take to load? Does it load like it did previously?

26. What command did you use to perform the attack?

**Insecure Renegotiation Disabled**

**28. What script did you use to perform the attack?**

**Are Secure Sites That You Use Susceptible to SSL DOS Attacks**

**30. Report which three websites you tested and whether insecure renegotiation was enabled or disabled for them.**

**SSL Stripping**

**31. Take a screenshot of the secure connection.**

**33. Take a screenshot of the same connection after using “sslstrip”**

**34. Report the text inside of your sslstrip log file.**

**TLS Renegotiation**

**39. What is the new line of log text after posting from the Kali VM?**

**40. What is the new line of log text after posting from your host computer?**

**42. What is the new line of log text after performing the TLS renegotiation attack?**

**43. Take a screenshot of Wireshark witnessing the TLS renegotiation attack.**

**44. What was the command that you used to perform the attack?**