

Lab 6: Tunnelling

Windows 7 login: Password: napier, Kali login: User: root, Password: toor

1 Viewing details

No	Description	Result
1	<p>Go to your Kali Linux instance. Run Wireshark and capture traffic from your main network connection. Start a Web browser, and go to www.napier.ac.uk.</p> <p>Stop Wireshark and identify some of your connection details:</p>	<p>Your IP address and TCP port:</p> <p>Napier's Web server IP address and TCP port:</p> <p>Right-click on the GET HTTP request from the client, and follow the stream:</p> <p>What does the red and blue text identify?</p> <p>Can you read the HTTP requests that go from the client to the server? [Yes][No]</p>
2	<p>Go to your Windows 7 instance. Run Wireshark and capture traffic from your main network connection. Start a Web browser, and go to www.napier.ac.uk.</p> <p>Stop Wireshark and identify some of your connection details:</p>	<p>Your IP address and TCP port:</p> <p>Napier's Web server IP address and TCP port:</p> <p>Right-click on the GET HTTP request from the client, and follow the stream:</p> <p>What does the red and blue text identify?</p>

		Can you read the HTTP requests that go from the client to the server? [Yes][No]
3	<p>Go to your Kali Linux instance. Run Wireshark and capture traffic from your main network connection. Start a Web browser, and go to Google.com.</p> <p>Stop Wireshark and identify some of your connection details:</p>	<p>Your IP address and TCP port:</p> <p>Google's Web server IP address and TCP port:</p> <p>Which SSL/TLS version is used:</p> <p>By examining the Wireshark trace, which encryption method is used for the tunnel:</p> <p>By examining the Wireshark trace, which hash method is used for the tunnel:</p> <p>By examining the Wireshark trace, what is the length of the encryption key:</p> <p>By examining the certificate from the browser which encryption method is used for the tunnel:</p> <p>By examining the certificate from the browser, which hash method is used for the tunnel:</p> <p>By examining the certificate from the browser is the length of the encryption key:</p>

4	<p>Go to your Windows 7 instance. Run Wireshark and capture traffic from your main network connection. Start a Web browser, and go to https://twitter.com.</p> <p>Stop Wireshark and identify some of your connection details:</p>	<p>Your IP address and TCP port:</p> <p>Twitter's Web server IP address and TCP port:</p> <p>Which SSL/TLS version is used:</p> <p>By examining the Wireshark trace, which encryption method is used for the tunnel:</p> <p>By examining the Wireshark trace, which hash method is used for the tunnel:</p> <p>By examining the Wireshark trace, what is the length of the encryption key:</p> <p>By examining the certificate from the browser which encryption method is used for the tunnel:</p> <p>By examining the certificate from the browser, which hash method is used for the tunnel:</p> <p>By examining the certificate from the browser is the length of the encryption key:</p>
---	---	---

2 OpenSSL

No	Description	Result
1	Go to your Kali Linux instance, and make a connection to the www.live.com Web site:	Which SSL/TLS method has been used:

	<code>openssl s_client -connect www.live.com:443</code>	<p>Which encryption method is used for the tunnel:</p> <p>Which hash method is used for the tunnel:</p> <p>What is the length of the encryption key:</p> <p>What is the serial number of the certificate:</p> <p>Who has signed the certificate:</p>
2	Now, add the <code>-ssl3</code> option and note the changes:	<p>Which SSL/TLS method has been used:</p> <p>Which encryption method is used for the tunnel:</p> <p>Which hash method is used for the tunnel:</p> <p>What is the length of the encryption key:</p>

3 Installing HTTPS and Heartbleed

No	Description	Result
1	<p>Go to your Kali Linux instance. Setup a secure Web server using the commands:</p> <pre>sudo apt-get install apache2 sudo a2enmod ssl sudo a2ensite default-ssl sudo openssl req -new -x509 -days 365 -sha1 -newkey rsa:1024 -nodes -keyout server.key -out server.crt</pre>	<p>Which OpenSSL is used on your Kali instance:</p> <p>Can you connect from Kali to your local host with:</p> <p><code>https://localhost</code></p>

	<pre>sudo /etc/init.d/apache2 restart</pre>	<p>Can you connect to your Kali instance from a Web browser on Windows 7:</p> <p><code>https://10.200.0.x</code></p> <p>[Yes][No]</p>
2	<p>On Kali, now download the following Python script to detect Heartbleed:</p> <p><code>http://asecuritysite.com/heart.zip</code></p> <p>Test your server with:</p> <pre>python heart.py 10.200.0.x</pre>	<p>Is your server vulnerable?</p> <p>What is used to detect the vulnerability?</p>
3	<p>On Wireshark, now repeat 2, and capture data packets.</p>	<p>Can you find the data packet which contains the Heartbleed vulnerability? What are the details that are sent?</p>

4 Examining traces

No	Description	Result
1	Download the following file, and examine the trace with Wireshark: http://asecuritysite.com/log/ssl.zip	Client IP address and TCP port: Web server IP address and TCP port: Which SSL/TLS method has been used: Which encryption method is used for the tunnel: Which hash method is used for the tunnel: What is the length of the encryption key:
2	Download the following file, and examine the trace with Wireshark: http://asecuritysite.com/log/heart.zip	Client IP address and TCP port: Web server IP address and TCP port: Which SSL/TLS method has been used: Which encryption method is used for the tunnel: Which hash method is used for the tunnel: What is the length of the encryption key: Can you spot the packet which identifies the Heartbleed vulnerability?

3	Download the following file, and examine the trace with Wireshark: http://asecuritysite.com/log/ipsec.zip	Which is the IP address of the client and of the server: Which packet number identifies the start of the VPN connection (Hint: look for UDP Port 500): Determine one of the encryption and hashing methods that the client wants to use: Now determine the encryption and hashing methods that are agreed in the ISAKMP:
----------	---	---