Lab 8: Tunnelling

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

1 Viewing details

No	Description	Result
1	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**. Stop Wireshark and identify some of your connection details:	Your IP address and TCP port: Napier's Web server IP address and TCP port: Right-click on the GET HTTP request from the client, and follow the stream: What does the red and blue text identify? Can you read the HTTP requests that go from the client to the server? [Yes][No]
3	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**. Stop Wireshark and identify some of your connection details:	Your IP address and TCP port: Google's Web server IP address and TCP port: Which SSL/TLS version is used: By examining the Wireshark trace, which encryption method is used for the tunnel:

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

		By examining the certificate from the browser which encryption method is used for the tunnel: By examining the certificate from the browser, which hash method is used for the tunnel: By examining the certificate from the browser is the length of the encryption key:

2 OpenSSL

No	Description	Result
1	Go to your Kali Linux instance, and make a connection to the **www.live.com** Web site: `openssl s_client -connect www.live.com:443`	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: What is the serial number of the certificate: Who has signed the certificate:
2	Now, add the –ssl3 option and note the changes:	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:

3 Installing HTTPS and Heartbleed

No	Description	Result

1	Go to your Kali Linux instance. Setup a secure Web server using the commands:
	
	`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`
	
	`sudo /etc/init.d/apache2 restart`
		Which OpenSSL is used on your Kali instance:
		
		Can you connect from Kali to your local host with:
		
		https://localhost
		
		Can you connect to your Kali instance from a Web browser on Windows 7:
		
		https://10.200.0.x
		
		[Yes][No]

2	On Kali, now download the following Python script to detect Heartbleed:
	
	`http://asecuritysite.com/heart.zip`
	
	Test your server with:
	
	`python heart.py 10.200.0.x`
		Is your server vulnerable?
		
		What is used to detect the vulnerability?

3	On Wireshark, now repeat 2, and capture data packets.	Can you find the data packet which contains the Heartbleed vulnerability? What are the details that are sent?

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:
