**CYBR 644 Assignment-2**

Part - 1: Capturing live traffic and visiting a non-encrypted website.

1. Launch Wireshark, and start sniffing on your active network adapter. (You can tell by the 'heartrate monitor' by each interface)
2. Launch a web browser and go to http://www.bom.gov.au/ and perform a few random searches
3. Close your browser and stop Wireshark and review your network traffic
4. Take note of the DNS requests and responses

Ans: A screenshot of a computer

Description automatically generated

1. What is the DNS server for your computer

Ans: IP Address of the DNS Server: 192.168.17.2

1. Take note of the HTTP requests and responses

Ans: A screenshot of a computer

Description automatically generated

1. Can you see the queries made (plain text)

Ans: Yes, all the GET requests made by the website to call the assets can be seen made in plain text.

Part - 2: Capturing live traffic and visiting an encrypted website.

1. Launch Wireshark and start sniffing again.
2. Launch a web browser again, but this time go to https://www.google.com
3. Close your browser and stop Wireshark and review your network traffic
4. Take note of the HTTP requests and responses

Ans: A screenshot of a computer

Description automatically generated

We can see that there are two types of requests made over HTTP. One of them is GET/FOUND requests and other is OCSP. Online Certificate Status Protocol (OCSP) requests are HTTP messages that are encoded in ASN.1. OCSP requests are a way for web browsers to check the revocation status of a website's X.509 digital certificate.

1. Can you see the queries made (plain text)

Ans: A screenshot of a computer

Description automatically generated

No, all the requests made by the website are encoded and protected.

Part - 3: Analyzing a saved packet capture to determine a vulnerability in a website.

Lastly, open the startwalkingnow.pcap from the Kali VM using a web browser, either on your host machine with Wireshark installed, or within Kali. At a terminal, run the following command to ensure the Webserver is running on your Kali VM. When prompted for a password, enter the Kali user password.

sudo service apache2 restart

In Firefox, simply browse to the IP address of the Kali VM in your browser (http://[Kali IP] and click on "Lab-files", then "pcaps". After downloading the file, open in Wireshark in order to being analysis. Can you identify the vulnerability?

Ans: A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

The obvious vulnerability is the use of HTTP protocol which can be seen in previous screenshots. HTTP has no encryption and all the calls made over HTTP are in plain text.  
Apart from HTTP, I can see a lot of calls made over LLMNR (Link-Local Multicast Name Resolution), NBNS (NetBIOS Name Service), and SSDP (Simple Service Discovery Protocol). These protocols are commonly used for network discovery, name resolution, and service advertisement on local networks. Seeing high volumes can mean there are issues with DNS resolution forcing clients to fall back to LLMNR and NBNS. Aggressive usage may indicate network reconnaissance activity by malicious tools and malware.

LLMNR, NBNS and SSDP have weaknesses that make them vulnerable to spoofing, poisoning and man-in-the-middle attacks.

Some of the vulnerabilities associated with these protocols can be:

* LLMNR and NBNS have no authentication and spoofing can lead to client impersonation or traffic interception.
* SSDP has no encryption allowing attackers to discover and map networks.
* Suspicious tools like Responder leverage these protocols to intercept credentials and hashes.
* Poisoning caches/responses can redirect clients to malicious servers.

Recommendation would be to disable these protocols and rely on DNS/mDNS/uPnP instead.