Ethical Hacker 8 – Network Sniffing and Spoofing

* **What can and cannot be seen when sniffing traffic with Wireshark?**

On the capturing screen, the user can see the time of capture, the number of each package, the source (the IP address of the device where the traffic comes from), the destination (the IP address that the package is trying to reach), the protocol, the length of the package, and additional information

Graphical user interface

Description automatically generated

* **Try to intercept a plain text password (HTTP or FTP) by capturing a login-name and password:**
* The first step is to enter on a non-secured website with a login form. In this example, I am using one of my older websites made for a semester 2 assignment.

Graphical user interface, application, website

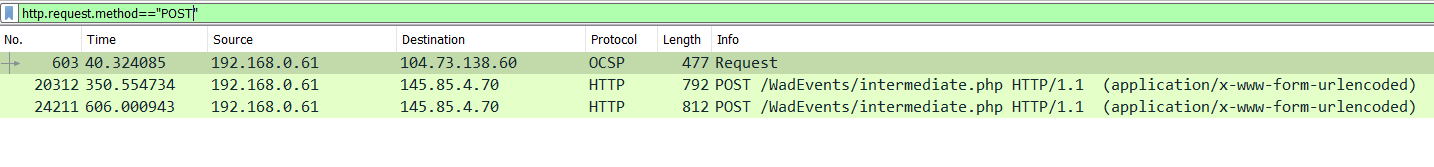
Description automatically generated

This is followed by typing a random username and password. In this case, the username is “something” and the password is “somethingelse”.

Graphical user interface, text, application

Description automatically generated

After filtering the traffic using the instruction on the green background, the name and file in question of the website is present in 2 of the 3 entries.



Now that the correct package has been found, the following instructions will lead to more information about it:

Graphical user interface, text, application, email

Description automatically generated

The username and password can be seen in the Follow HTTP Stream page, and they have been highlighted by me:

Graphical user interface, text, application

Description automatically generated

* **Demo and explain ARP spoofing a private VLan in the seclab with arpspoof.**

First, I will find out what my IP address is, using *ipconfig* on my windows command prompt:

A picture containing text

Description automatically generated

A picture containing text

Description automatically generated

I will open 2 terminals in the kali machine because I have to initialize the ARP spoof twice. In the following command, i stands for interface, in this case wlan0, t is for target, which is the windows IP address, followed by the default gateway.

Text

Description automatically generated

To be continued…

* **Explain what can be done to protect against ARP spoofing.**

There are several ways you can prevent ARP spoofing attacks. One of them is to invest in detection software that will allow you to spot potential threats. Alternatively, you could set yourself up with packet inspection software, that will check all the data on the network perimeter. This type of filtering can usually be performed by a firewall. Another option would be to create a static ARP address for every device on the network. Static ARP addresses cannot be manipulated by ARP reply packets. Although useful, this will only mitigate the most basic of threats.

* **Resources:**
* [**https://proprivacy.com/blog/ARP-spoofing**](https://proprivacy.com/blog/ARP-spoofing)
* [**https://www.youtube.com/watch?v=lb1Dw0elw0Q**](https://www.youtube.com/watch?v=lb1Dw0elw0Q)
* [**https://www.youtube.com/watch?v=FcwrrAT1H7o**](https://www.youtube.com/watch?v=FcwrrAT1H7o)
* [**https://www.guru99.com/wireshark-passwords-sniffer.html**](https://www.guru99.com/wireshark-passwords-sniffer.html)
* [**https://www.golinuxcloud.com/man-in-the-middle-attack-arp-spoofing/**](https://www.golinuxcloud.com/man-in-the-middle-attack-arp-spoofing/)
* [**https://www.youtube.com/watch?v=8SIP36Fym7U**](https://www.youtube.com/watch?v=8SIP36Fym7U)