**Part 1**

1. **Identify host IP and MAC addresses**

**IP Address 1:** 192.168.60.10

**Mac Address 1:** b8:27:eb:80:86:9b

**IP Address 2:** 192.168.60.11

**Mac Address 2:** b8:27:eb:00:cc:43

**IP Address [Router]** : 192.168.60.1

**Mac Address [ Router] :** 30:85:a9:fb:91:48

1. **Identify Network Traffic Between Hosts**

Since this was a open network I was able to view the traffic without a need of any key. I analysed that 2 raspberry pie devices were communicating via various networking protocols. Some of these are highlighted below.

Networking Protocols :- ICMP, DNS, TELNET, TCP, FTP, FTP-DATA, ARP, 802.11, SSDP, STP

1. **Provide a \*.pcap dump**

Provided in the zip folder

**Part 2:**

1. **Identify host IP and MAC addresses**

**IP Address 1 :** 192.168.70.10

**Mac Address 1 :** b8:27:eb:22:ed:4a

**IP Address 2:** 192.168.70.11

**Mac Address 2:** b8:27:eb:82:40:91

**IP Address [Router] :** 192.168.70.1

**Mac Address [Router]** : 30:85:A9:FB:8E:D0

Note: *I was able to view the IP Address after decrypting the traffic in this case.*

1. **Identify network traffic between hosts and how it differs from part 1**

Traffic in this case was encrypted. As a result, for these 2 raspberry pie devices I was unable to view to view the IP address and Protocols via which they were communicating.

After cracking the WEP key and decrypting the traffic using the cracked WEP key, I was able to analyze the traffic & found that it was almost same as Part 1.

Protocols Identified after Decryption :- FTP, TCP, ICMP, DNS, TELNET, STP, SSDP, FTP-DATA, ARP, 802.11

1. **Provide a \*.pcap dump**

Provided in the zip folder.

**Part 3: PROVIDE WEP KEY**

C3:C3:DA:84:26



**Part 4:**

1. **Identify open ports on the host.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Port** | **State** | **Service** | **Version** |
| 21 | open | ftp | GNU Inetutils FTPd 1.9.4 |
| 22 | open | ssh | OpenSSH 7.9p1 Raspbian 10+deb10u2+rpt1 (protocol 2.0) |
| 23 | open | telnet |  |

1. **Upload a file on the Server.**

Uploaded apoorvgahlot.txt

**Security Implications**: -

Having a Weak security protocol such as WEP exposes us to many security attacks such as Man-in-The-Middle attack, sniffing and snooping.

Additionally, I also found that one of the hosts was running with an FTP service which allowed anonymous login. This also poses many security threats.

Implementing strong security protocol such as WPA2 and having proper authentication mechanism is a must in order to avoid these kind of attacks.