## **Assignment 7 - Wireless Security**

- This is an individual assignment and worth 20 points.
- This is due on Wednesday, November 29 at midnight.
- Apply the usual naming convention.

## **Background**

- This assignment is from National Cyber League (NCL) exercise. Use the attached "NCL-PCAP1.pcap".
- You need to use Kali to answer the questions below. You can use your own Kali VM.
- When you use Proxmox, send the attached pcap file to the Kali on Proxmox. The file will be downloaded to the following directory: /home/kali/Downloads.
- Use aircrack-ng on Kali. Refer to the "CIS 480 Aircrack-ng.pptx" for ideas. You do not need to install aircrack-ng on Kali.
- You can find several websites that discuss "how to crack WEP with aircrack-ng." For example, refer
  to: <a href="https://null-byte.wonderhowto.com/how-to/hack-wi-fi-cracking-wep-passwords-with-aircrack-ng-0147340/">https://null-byte.wonderhowto.com/how-to/hack-wi-fi-cracking-wep-passwords-with-aircrack-ng0147340/</a>.

## **Tasks**

1. How many IVs are in the packet capture? Provide a screenshot that supports your answer. Run the following command: aircrack-ng NCL-PCAP1.pcap.

There are 14337 IVs in the packet capture.

```
[00:00:04] Tested 134106 keys (got 14337 IVs)
```

2. What is the initialization vector (IV) in the first packet in the capture (in hex)? Provide a screenshot that supports your answer.

The initialization vector of the first packet in the capture is 0x003a33

```
P Qos Control: 0x00000
WEP parameters
Initialization Vector: 0x003a33
Key Index: 0
WEP ICV: 0x9ad2e8d3 (not verified)
P Data (1508 bytes)
```

3. What is the key (i.e., password input) you obtained after running aircrack-ng? Provide a screenshot that supports your answer.

The key obtained is A4:81:53:B4:CF.

```
KEY FOUND! [ A4:81:53:B4:CF ]
Decrypted correctly: 100%
```

4. What is the TCP checksum in the first packet of the capture (in hex)? Provide a screenshot that supports your answer. You must decrypt the capture with the key you obtained.

## The TCP checksum of the first packet of the capture is 0x897b.

```
Source Port: 56985
 Destination Port: 22
  [Stream index: 0]
  [Conversation completeness: Incomplete (12)]
  [TCP Segment Len: 1448]
 Sequence Number: 1
                        (relative sequence number)
 Sequence Number (raw): 3890121788
 [Next Sequence Number: 1449
                                (relative sequence number)]
 Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 4190872430
 Acknowledgment Number: 1
 1000 .... = Header Length: 32 bytes (8)
Flags: 0x010 (ACK)
 Window: 4096
  [Calculated window size: 4096]
 [Window size scaling factor: -1 (unknown)]
  Checksum: 0x897b [unverified
  [Checksum Status: Unverified]
 Urgent Pointer: 0
> Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[Timestamps]
 [SEQ/ACK analysis]
 TCP payload (1448 bytes)
```

- How to decrypt the capture?
  - Go to Wireshark > Edit > Preferences > IEEE 802.11 > ...

