Network Forensics and WPA2 PSK

1. Lab Overview

The learning objective of this lab is for students to gain hands-on experience on packet decoding for network forensics and using sniffed packets for WPA2 PSK cracking. In this lab, students will be given a few packet capture files that the instructor made to make sense of what is happening on the network and what is needed to crack a weak WPA2 PSK password. Their task is to learn to use the right tools for and gain insight into network forensics and WPA2 PSK cracking.

2. Lab Tasks

2.1 Task 1: TCP packet decoding for network forensics

Deliverable: Screenshots and answers to questions as indicated in the instructions below.

1. For this task, use the forensics.cap file located in Files/Programming Assignments on Canvas. You can use tcpdump, windump, or Wireshark (recommended). I have included example commands for each utility below.

2. We first learn how to find important control packets containing flag bits for connection setup through an example. Try the following commands and answer the following questions.

   (a) Open forensics.cap in Wireshark and enter tcp.port==34404 in the Apply a display filter field I showed you in class (for Wireshark)
   tcpdump -nn -r forensics.cap 'tcp port 34404' (for tcpdump)
   windump -nn -r forensics.cap "tcp port 34404" (for windump)

   Q1: How many packets are printed out (screenshot)? What are the TCP flags in each packet?

   (b) Open forensics.cap in Wireshark and enter tcp.port==34404&&tcp.flags==2 in the Apply a display filter field (for Wireshark)
   tcpdump -nn -r forensics.cap 'tcp port 34404 and tcp[13]=2' (for tcpdump)
   windump -nn -r forensics.cap "tcp port 34404 and tcp[13]=2" (for windump)

   Q2: With this modified filter, what is being filtered for? How many packets are printed out (screenshot)?

3. Now design your own filters for the following tasks and answer the questions.

   (a) Design a filter for the utility you are using to find packets *with and only with* SYN and ACK flags turned on.

   Q3: How many packets are printed out (screenshot)? What is your filter?

(b) Design a filter for the utility you are using to find packets with the SYN flag turned on. The other flags are don't-cares.

Q4: How many packets are printed out (screenshot)? What is your filter?

(c) Design an alternative filter for (b).

Q5: What is your filter?

4. Next, we will review the file forensics.cap to identify the local DNS and HTTP servers. By "local", I mean that the resource should have a source IP address of 12.33.x.x.

Q6: What are the IP addresses of the HTTP and DNS servers? (If there are multiple HTTP or DNS servers, show the IP address all of them.) Describe the method you used.

Hint: You will need to design packet filters to find the packets you want. When you find the IP address of an HTTP or DNS server, exclude it from your filter and run it again to see there are other HTTP or DNS servers. HTTP usually runs on TCP port 80, DNS on TCP and UDP port 53.

2.2 Task 2: Inspecting captured packets to crack weak passwords in WPA2 PSK

Deliverable: Screenshots and answers to questions as indicated in the instructions below.

1. You will need the illustration on the board in the lecture to understand this task and answer the questions.

2. As shown in class, it is crucial to capture the 4-way handshake messages and use a good dictionary file to crack the password used in WPA2 PSK. I have captured the 4-way handshake for you in WPA2handshake.cap located in Files/Programming Assignments on Canvas.

3. Open WPA2handshake.cap with Wireshark and type eapol in the filter field (filter for 4-way handshake messages). TPLink is the AP and Apple is the host.

Q7: What are the messages you see?

Q8: Inspect these messages by expanding them.

- What is the Anonce value (screenshot with this number highlighted)? How long is it in bits?
- What is the Snonce value (Screenshot with this number highlighted)? How long is it?
- How many different non-zero MACs, or Message Authentication Codes are there in the messages? How long are they?
- Explain the use of the nonces and MACs in this scenario.

Q9: When can WEP be cracked?

A. Always.
B. Only if a weak key/passphrase is chosen.
C. Under special circumstances only.
D. Only if the AP runs old software.

Q10: When can WPA2 be cracked?

A. Always.
B. Only if a weak key/passphrase is chosen.
C. If the client contains old firmware.
D. Even with no client connected to the wireless network.