CYBERSECURITY LAB #3

Giacomo Gori – Tutor didattico

g.gori@unibo.it

Exercise

Complete the 3 exercises, taking notes of all the steps that you take

Write a **small** report and upload it on Virtuale

Remember: write name, surname and the number of the lab session on the report!

Prerequisites

Virtualbox and the configured Kali VM.
Instructions are on Virtuale!
Also, we will see Wireshark

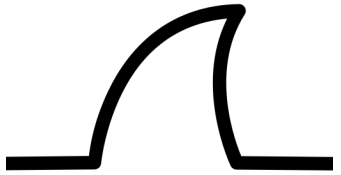
Wireshark

It is a free and open-source **packet analyzer**.

Similar to tcpdump, but it has a **graphical interface** to show sniffed packets.

Has a lot of **filtering capability** to find the packets that you want.

Wireshark



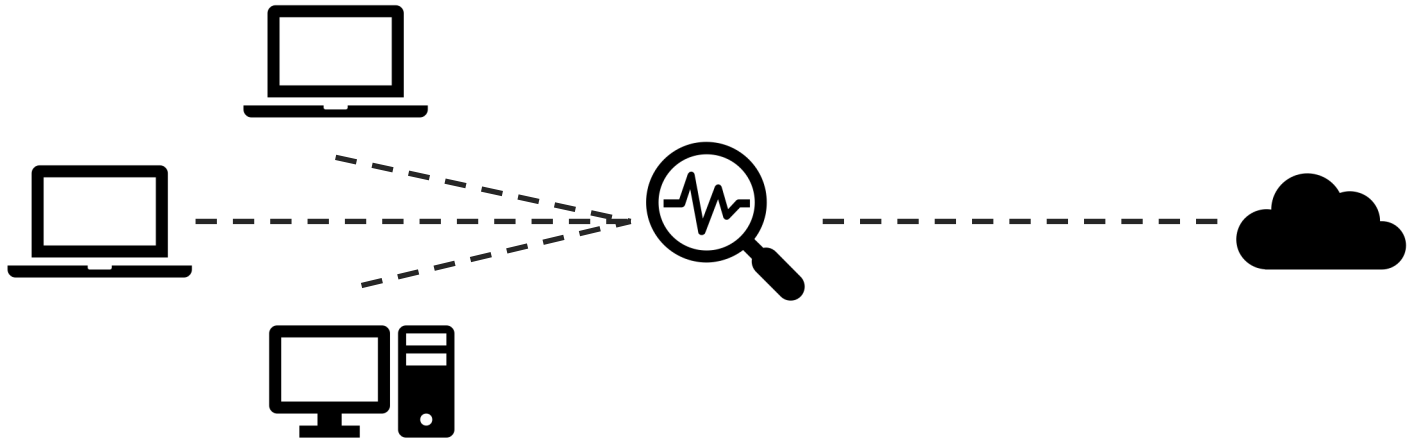
- It can perform **real-time analysis** or on **previously recorded traffic file** (e.g. **PCAP** files)
- It show a **packet list with a summary** of each of them
  - If you click on one, it will show all the detail of every TCP/IP layer with their respective protocol
  - Wireshark could be wrong with the dissection rules (e.g. based on port)
- **Filtering** capability
  - You can select a property of a specific packet and set it as a filtering rule
- You can follow streams

What can we see from a packet analyzer?

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.2.1	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
2	1.000498	192.168.2.1	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
3	2.001016	192.168.2.1	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
4	3.002419	192.168.2.1	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
5	14.589681	192.168.2.1	192.168.2.255	BROWSER	243	Local Master Announcement LAPTOP-HCSFMST7, Workstation, Ser
6	21.094272	fe80::8dd3:64c9:4e…	ff02::1:3	LLMNR	84	Standard query 0x724e A wpad
7	21.094285	192.168.2.1	224.0.0.252	LLMNR	64	Standard query 0x724e A wpad
8	21.506682	fe80::8dd3:64c9:4e…	ff02::1:3	LLMNR	84	Standard query 0x724e A wpad
9	21.506697	192.168.2.1	224.0.0.252	LLMNR	64	Standard query 0x724e A wpad
10	35.861119	00:0c:29:b9:02:a9	ff:ff:ff:ff:ff:ff	ARP	60	Who has 10.0.0.5? Tell 10.0.0.6
11	37.894161	10.0.0.9	10.0.0.5	UDP	66	5000 → 8990 Len=24
12	37.909319	10.0.0.6	10.0.0.4	TCP	74	48520 → 8000 [SYN, ECE, CWR] Seq=0 Win=29200 Len=0 MSS=1460
13	37.909341	10.0.0.4	10.0.0.6	TCP	54	8000 → 48520 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
14	37.926274	00:0c:29:b9:02:a9	ff:ff:ff:ff:ff:ff	ARP	60	Who has 10.0.0.5? Tell 10.0.0.6
15	39.962355	10.0.0.9	10.0.0.5	UDP	66	5000 → 8990 Len=24
16	39.967619	10.0.0.6	10.0.0.4	TCP	74	48522 → 8000 [SYN, ECE, CWR] Seq=0 Win=29200 Len=0 MSS=1460
17	39.967637	10.0.0.4	10.0.0.6	TCP	54	8000 → 48522 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
18	39.985954	00:0c:29:b9:02:a9	ff:ff:ff:ff:ff:ff	ARP	60	Who has 10.0.0.5? Tell 10.0.0.6
19	42.016389	10.0.0.9	10.0.0.5	UDP	66	5000 → 8990 Len=24
20	42.022649	10.0.0.6	10.0.0.4	TCP	74	48524 → 8000 [SYN, ECE, CWR] Seq=0 Win=29200 Len=0 MSS=1460
21	42.022666	10.0.0.4	10.0.0.6	TCP	54	8000 → 48524 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	42.039326	00:0c:29:b9:02:a9	ff:ff:ff:ff:ff:ff	ARP	60	Who has 10.0.0.5? Tell 10.0.0.6
23	42.920199	00:0c:29:91:d8:c7	00:0c:29:b9:02:a9	ARP	42	Who has 10.0.0.6? Tell 10.0.0.4

Why should we use a packet analyzer?

- Monitor(***sniffing***) the traffic could be essential for the discovery of attacks
- But also to perform attacks.....



Where should we use a packet analyzer?

Network

- To listen to all the traffic coming from and to **different hosts**

Host

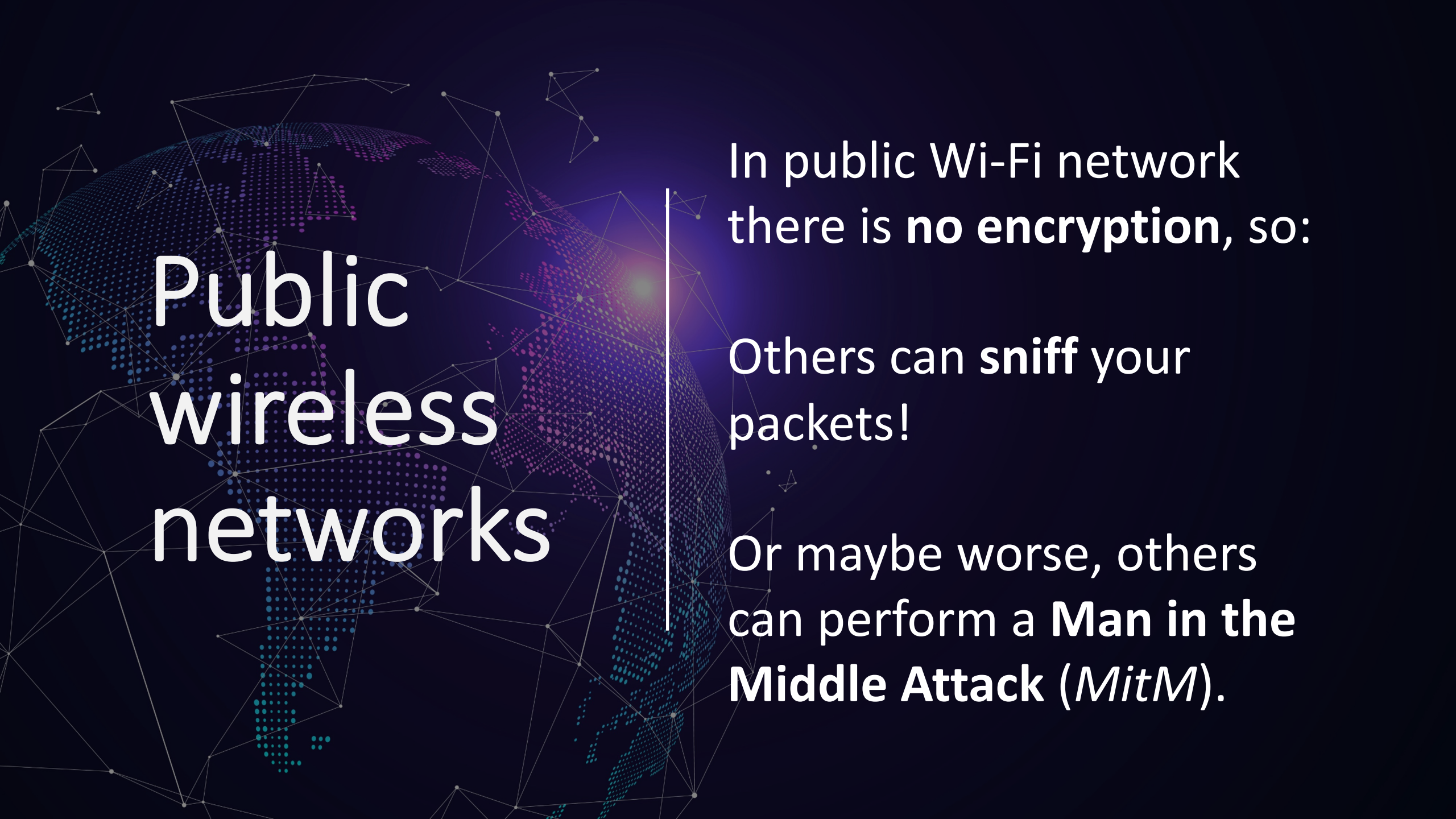
- To listen to all the traffic coming from and to the **actual host**
  - I can see also **application data layers**!

But.. From which interface?

Your computer could have more than one, in general we can choose **wired or wireless interfaces**.

In the case of wired, you can see only the traffic directed/coming exactly to/from you (Ethernet case).

But, **in the case of wireless, I can "sniff" everything…**



Public wireless networks

In public Wi-Fi network there is **no encryption**, so:

Others can **sniff** your packets!

Or maybe worse, others can perform a **Man in the Middle Attack** (*MitM*).

"Protected" wireless networks

Encryption makes your packets confidential

...Right?

It depends on algorithms

In Wi-Fi we can choose different algorithms:

- WEP
  - Stream cipher RC4 algorithm, CRC32 checksum, **INSECURE**
- WPA
  - TKIP
- WPA2
  - Not RC4 anymore..
- WPA3

And passwords!!

- As always, weak password can be **cracked**
  - Remember brute-force/dictonary attacks?

Attacking WEP

WEP was designed many years ago, now is **obsolete**.

If you know the shared key, you can decrypt every packets of the others.

It used Initializing Vector (IV), sent in plaintext in the packets, with few bits (24), so… Collecting some of them lead you to **crack (*mathematically derive*) the shared key**!

Attacking WPA

By **sniffing** the 4-way handshake we can perform an **offline** attack

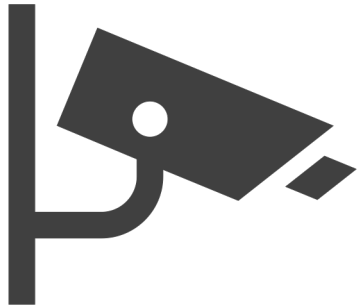
Attackers can get all the informations to perform **dictonary and brute force attack**.

So, in this case, the probability of success it’s more password-related…

How to sniff packets “*in the air*”

- With physical cable, not considering the (old) *hub topologies*, we cannot see packets unless we are physically connected to the specific cables!
- With wireless instead, everything is in the *air*. So **we can simply listen to receive all the packets**.

That’s what is called **Monitor Mode**



Monitor Mode

It permits to capture and see all the packets coming from a specific wireless channel.

First step: find the channel of the interested AP

Second step: monitor the channel

Monitor mode in linux

- To enable monitor mode on your pc, it depends on the wireless card. You can follow the **aircrack-ng guide**: *https://www.aircrack-ng.org/doku.php?id=cracking_wpa*

- With **airmon-ng**, once you **capture a WPA handshake**, you can stop the analysis and go to the next step with the PCAP file obtained.
  - For the exercise, I will give you an example PCAP file.

Capturing the handshake

- With monitor mode we can capture the packets sent for the handshake

- Then, we save the .pcap file that contains the packets and we can try an **offline attack** of dictionary/brute-force. You can also use Wireshark to investigate the packets.

Attacking

- We will use **aircrack-ng suite**, able to attack WEP and WPA/WPA2

- Usage: **aircrack-ng (-w wordlist) (-b BSSID) (pcap file) [OPTIONS]**
  - **Wordlist:** pass the wordlist to use for cracking the password
  - **BSSID:** MAC address of the interested AP
  - **PCAP file:** the file containing the sniffed handshake
  - **In OPTIONS:** settings for optimized WEP or WPA/2 attacks..

Crack the wifi passwd

Use your knowledge to **find the passwords** (if it's possible) of the wireless access point from the traffic in the "wifi" **PCAP files** in virtuale.

Land the Dreamliner

Find the commands to control the plane.

Complete the challenge: *http://dreamliner.challs.cyberchallenge.it/*

You have **3 hints** in the help file on virtuale.

Detect the intruder

It has been detected that an intruder has **downloaded a file**, find out more.

Analyze the traffic and find the *flag*, that has this form at CCIT{*flag*}, from the PCAP file (s3cret.pcapng) in virtuale.

Hints are in the help file on virtuale