# Network Hacking

## NIC (Network Interface Card)

- دا كارت الشبكه اللي بيكون ف كل جهاز سواء موبايل او لاب او بي سي او حتي شاشه
- دا المسؤول علي انو يستقبل البيانات من الواي فاي او الكابل ويبعتها للجهاز من جوا

## NIC Modes

### Managed Mode

- دا المود العادي وهنا الكارت بيستقبل البيانات عادي وبيأدي شغله طبيعي

### Montior Mode (Hacking Mode)

- دا بقي الوضع الخطر لأني فالوضع ده الكارت بيأدي شغله انو يتصنت علي الtraffic ويشتغل كا شبكه وهميه hotspot
- فا لازم قبل ما اهكر اي شبكه لازم اخلي ال NIC ف ال Monitor Mode

## Network Sniffing

- ببساطه كدا ال network sniffing هو التصنت علي الشبكه يعني قبل اصلا ما اخترق شبكه لازم اعمل الخطوه دي عشان اعرف ايه نوع ال traffic ومين بيكلم مين واجمع معلومات بقدر كافي
- فا هنا اقدر التقط الpackets اللي بتتنقل بين الاجهزه عالشبكه
- طبعا ال packets اللي بتتنقل دي بتكون sensitive زي مثلا بيانات الفيزا بتاعتك او الاكونت بتاعك
- يعني تخيل معايا لو انت بتفتح موقع جوميا مثلا وبتشتري حاجه وبتدخل الفيزا بتاعتك وحد كان بيعمل sniffing فا هيقدر يشوف ال traffic اللي بيتنقل بينك وبين الموقع ويشوف الحاجه اللي بتبعتها زي بيانات الفيزا

## Man in the Middle Attack

- اكتر Attack مشهور فالموضوع ده هيا ال Man in the Middle (MITM) ودي زي اسمها بالظبط الرجل فالمنتصف يعني الهاكر بيكون شايف اي traffic بين جهازين ويقدر يأكسس علي ال packets اللي بتتبعت
- بل انه ممكن يتلاعب بالمحتوي اللي جوا ال packet ويغيرها او ينتحل شخصية ال source او destination ويوهم الطرف التاني انو دا الطرف الصحيح Spoofing

"Pasted image 20250111001455.png" could not be found.

- عاوز انبهك لحاجه لو انت مذاكر كويس الدروس بتاعتنا اللي فاتت هتقول بس انت قولتلنا علي بروتوكول اسمه https ودا بيكون امان جدا هقولك اه كلامك صح عشان كدا لازم انا كا Attacker اشوف المواقع اللي بتستخدم ال http عشان ساعتها هيكون سهل اني اخترقها عن الhttps

### طب لو الموقع بيستخدم HTTPS؟

- فالحاله دي هضطر اعمل downgrade للموقع يعني ايه؟ يعني انزل صلاحيات الموقع من https اخليه أكنو http عشان يكون سهل عليا اخترقه ودا بيكون عن طريق tool اسمها SSL Strip

### خطوات ال MITM

1. اول حاجه لو الموقع https هعمل downgrade
2. اخلي ال NIC في وضع ال Monitor Mode
3. بعد كدا هستعمل تول ettercap عشان دي اللي هتقوم بعملية ال mitm
4. هستعمل تول wireshark عشان بقي اشوف ال packets واحللها اشوف ايه محتواها وكدا

## Wireshark

- اولا دي تول بستخدمها عشان اقدر اشوف ال packets اللي بيحصل ف ال traffic بتاعي مش شرط يكون في mitm يعني

1. اول حاجه يا باشا انت هتحددلو نوع ال NIC بتاعك شوف انت بتستعمل واي فاي (wlan0 , wlan0mon) ولا كابل (ethernet)

“Pasted image 20250111002327.png” could not be found.

2. بعد ما تحدد ال NIC هيظهرلك الاف الpackets اللي بتتبعت ودا طبيعي عادي ف كل packet بيكون فيها source (الشخص اللي بيبعت الطلب) وال destination (الشخص اللي رايحلو ال packet والبروتوكول اللي بيتنقل بيه

“Pasted image 20250111002811.png” could not be found.

“Pasted image 20250111002947.png” could not be found.

“Pasted image 20250111003002.png” could not be found.