DHCP Starvation

يعني ايه DCHP؟

- دلوقتي لو انا اتصلت بشبكه بحتاج اني اخد ip فا بيكون في طريقين يا اما احط انا ip بنفسي او استعمل ال DHCP انه يديني ip بشكل عشوائي
- فا ال DHCP هنا مهمته انه بيديني ip عشوائي يعني اول ما اكونكت بالشبكه جهازي بيبعت طلب للراوتر يروح باعت لل DHCP Server يقولو هاتلي عدد واحد ip وصلحه هه
- عاوزك تاخد بالك من حاجه انك مثلا ف شبكه لو دا ip الشبكه `192.168.1.0/24` هنا عدد الأيبهات المتاحه اصلا من 1-254 طب افرض كل الايبهات خلصت هيحصل ايه؟

ازاي الأتاك ده بيشتغل؟

1. الـDHCP Request Flooding

- هنا الهاكر بيبدأ يغرق الشبكه وال DHCP بطلبات IP وهميه كتير جدا
- خلي بالك انو ف كل مره بيطلب ip باستخدام MAC مختلف ووهمي عن اللي قبله , عشان ياذكي لما ياخد ip بMAC معين هييجي يطلب تاني بنفس ال MAC الDHCP هيقوله انت عبيط ياعم منتا واخد مره , فا الهاكر هنا بيغير ال MAC ف كل request (عشان يبان انه جهاز مختلف يعني) وبيكون وهمي اصلا

2. استنزاف العناوين

- دلوقتي يا باشا كل الايبهات الهاكر خدها لو في بقي يوزر عادي عاوز يعمل يتصل بالشبكه ال DHCP هيقولو لا والله مفيش عندي ايبيهات انطر ياض فا بالتالي مش هيقدر اليوزر العادي انو يتصل بالشبكه

3. تعطيل الشبكه

- كدا خلاص انت عطلت الشبكه ومفيش حد هيقدر يعمل كونكت

“Pasted image 20250118160900.png” could not be found.

الهدف من الهجوم؟

- **تعطيل الخدمه (Denial of Service - DoS)** : منتا مخلتش حد يعرف يكونكت فا انت عطلت الخدمه
- **اتاك الرجل في المنتصف (MITM)** : - بعد استنزاف DHCP ، المهاجم ممكن يعمل سيرفر DHCP وهمي ويوزع عناوين IP مزيفة لجعل الضحايا يتصلوا بالشبكة المزيفة دي

تنفيذ الأتاك بشكل عملي

“Pasted image 20250118160920.png” could not be found.

مبدأيا احنا هنستخدم tool اسمها yersinia

- `sudo apt-get install yersinia` => install yserinia tool
- `sudo yersinia -G` => Run yersinia tool in GUI Mode

1. “Pasted image 20250118161112.png” could not be found.

- هنا انا بسيب ال MAC زي ماهو
- ببدأ اغير ال Source IP بخليه 0.0.0.0 وال DIP بخليه 255.255.255.255
- الportبخليه اي حاجه عادي

1. “Pasted image 20250118161209.png” could not be found.

- بحدد هنا الشبكه اللي هعمل عليها الattack

2. “Pasted image 20250118161251.png” could not be found.

- بحدد الأوبشن ده sending DISCOVER packet

3. “Pasted image 20250118161338.png” could not be found.

- لو بصينا ف ال wireshark هنا هنلاقي في طلبات DHCP كتير جدا ودا معناه اني الهجمه حصلت فعلا