Man In the Middle Attack

يعني ايه Man in the Middle ؟

- دلوقتي في جهازين بيكلمو سواء ف نفس ال network او ممكن جهاز بيتواصل مع سيرفر زي طلبات ال http مثلا اي traffic عمتا بيطلع من الجهاز راح لجهاز تاني سواء جهاز تاني علي نفس الشبكه او سيرفر
- الهاكر هنا بيكون ف النص وبيوهم الvictim او الجهاز الاولاني انو ده ال destination او السيرفر اللي بيكلمو يعني وف نفس الوقت بيوهم السيرفر انو ده الجهاز اللي باعت الطلب

“Pasted image 20250118010455.png” could not be found.

- بالتالي هو كل حاجه بتتبعت بين الجهاز بتوصلو وبتكون معاه
- بيبدأ يوهم الجهازين عن طريق ال ARP Poisoning
- الARP Poisioning دي الطريقه اللي هوهم بيها الراوتر اني انا الجهاز اللي عالشبكه معاه وهوهم الجهاز اني الراوتر عن طريق اني انا كا هاكر هبعت طلبات ARP مزيفه فا الجهاز هيستقبلها وهيتوهم اني انا الراوتر والراوتر نفس الكلام هيتوهم اني انا الجهاز
- بس احنا ليه بنوهم الراوتر مش المفروض نوهم السيرفر؟ - اقولك تعالي تخيل معايا السيناريو ده

Example

- دلوقتي مثلا يوزر بيستخدم اللاب بتاعه عشان يفتح موقع فيسبوك العملية بتكون ازاي؟ اول حاجه الطلب بتاعه لما بيكتب لينك الفيس ف المتصفح الطلب دا هيروح للراوتر والراوتر هو اللي هيوجه الطلب بتاعه ده للسيرفر بتاع الفيس ويرجعله Response
- انا كا هاكر هنا هبعت طلبات ARP مزيفه وهقول للجهاز اليوزر ده (انا الراوتر ياض) وهروح اقول للراوتر (انا الجهاز اللي الip بتاعي كذا وعاوز افتح الفيس ياعم) انا كدا ضحكت عالاتنين
- فا دلوقتي اي traffic هيحصل بين الاتنين هيبقي معاك ياباشا وتشوفه

ملحوظه مهمه

هجمات ال MITM دلوقتي حاليا (احنا بنتكلم ف يوم 18/1/2025) مش شغاله علي بروتوكلات ال https شغاله علي ال http بس فالاول كانت شغاله علي الhttps عادي لما كان المواقع بتستعمل ال ssl cert كنا بنعملها downgrade انما دلوقتي بقو يستخدمو شهاده اقوي في الحمايه اسمها TLS فا دي اقوي من SSL ولحد دلوقتي مفيش طريقه لكسرها

تنفيذ الAttack بشكل عملي

- هنستخدم اداتين مهمين واساسين في عملية الMITM هما Wireshark , Ettercap
- لازم قبل ما تعمل الattack تخلي كارت الشبكه فال vmware يكون Bridged بدل NAT (هشرحهم ف الاخر)

1. اول حاجه هتفتح الاداه علي كالي
2. هتحدد كارت الشاشه اللي انت بتستخدمه سواء wlan0, eth0

“Pasted image 20250118011805.png” could not be found.

“Pasted image 20250118011822.png” could not be found.

3. بعد كدا هتعمل scan علي ال hosts اللي فالشبكه

“Pasted image 20250118011924.png” could not be found.

“Pasted image 20250118011939.png” could not be found.

- ظهرلك هنا كل الاجهزه اللي عالشبكه ولو مظهروش كلهم اعمل scan تاني

4. هنبدأ اني احنا هنضيف ip الراوتر كا target 1 لأني زي ما قولنا فوق احنا هنستهدف الراوتر وجهاز الضحيه

“Pasted image 20250118012110.png” could not be found.

- وبعد كدا هنحدد جهاز الضحيه كا target 2

4. بعد كدا هنفعل بقي ال ARP Poisoning

“Pasted image 20250118012200.png” could not be found.

- بكدا اي traffic هيحصل من ال target 2 هيظهرلك علاطول بس خلي بالك هو هيطلعلك ال POST Requests بس عشان دي المهمه ليك كا هاكر المفروض برضو اني packets تانيه بتتبعت فا انت محتاج تحللها فا هتروح لل wireshark

“Pasted image 20250118012330.png” could not be found.

“Pasted image 20250118012344.png” could not be found.

“Pasted image 20250118012406.png” could not be found.

الفرق بين ال NAT وال Bridged

- فالعادي انت بتكون مشغل الكالي كا vm علي الويندوز فا الويندوز بقي بيكون واخد ip من الراوتر عادي جدا طب لو شغلت نت علي ال vm هيبقي عامل ازاي
- الNAT هنا هيعملك شبكه افتراضيه كدا وهياخد ip افتراضي من الويندوز يعني الراوتر مش شايف ال vmware لأنه مش متصل بيه دايركت دا عامل شبكه افتراضيه وواخد ال ip من الويندوز اصلا
- الBridged هنا بقي انا بقوله لا ياباشا انا عاوز الكالي علي ال vmware ياخد ip من الراوتر مباشر ويبقي جهاز لوحده مستقل عادي ملهوش دعوه بالويندوز

ملحوظه مهمه

انا مشرحتش ال sslstrip لأني خلاص مبقاش ليها لازمه لأني زي ماقولت مبقاش حد بيستعمل ssl وكلو بيستعمل tls فا هيا هتكون معرفه اضافيه ليك بس مش هتحتاجها لو عاوز تشوفها تقدر تشوف سيشن بشمهندس حسام شادي ف module ال network hacking واسم السيشن بنفس اسم الشرح ده برضو