NFS & RPC Hacking

NFS (Network File System)
RPC (Remote Procedure Call)

NFS

- الnfs عامل بالظبط زي الsmb مبيختلفش كتير عنو
- عباره عن نقطه مركزيه بيتشير فيها الملفات وكل عضو ف الشركه يقدر يأكسس علي الملفات حسب قسمه
- بيشتغل ف ال TCP/IP Model علي بورت 111 او 2049

NFS Architecture

- **Client**: دا بيطلب الملف من السيرفر
- **Server**: السيرفر او المكان اللي بيكون فيه الملفات اللي الكلاينت بيطلبها منو
- **Network**: الشبكه وهي اللي بتنظم الحركه بين الكلاينت والسيرفر وبتتمثل في بروتوكول nfs

NFS Operation

- بيستخدم ال RPC عشان ينظم الريكويستات اللي جايه من الكلاينت للسيرفر
- ال RPC وال NFS مرتبطين ببعض

NFS Security Concerns

- استخدام تشفير ضعيف او عدم استخدامه اصلا وعلي فكره الاصدارات القديمه من ال NFS تشفيرها ضعيف وممكن تكسره عادي
- ممكن يحصل عليه عملية IP Spoofing او تزييف او اني انتحل شخصية جهاز وابقي اعمل ريكويست واحصل علي ملفات حساسه
- اني اكون مش عامل configuration كويسه برضو
- دخول غير مصرح ليا اني ادخل اصلا (Unauthorized Access)

- ممكن اعمل MITM او Data Interception
- ممكن اعمل DoS Attack برضو

NFS Hacking Scenarios

Scenario 1 : Unauthrozied Access

- اول لما اعمل Nmap scan علي السيرفر والاقي اني البروتوكول شغال ابدأ علاطول اعمل اللي هقولك عليه ده
- عاوزين نشوف بقي ايه الملفات اللي عالسيرفر فا هنعمل الكوماند ده

“Pasted image 20250209131655.png” could not be found.

“Pasted image 20250209131730.png” could not be found.

- بص هنا جابلي ايه جابلي اني في dir اسمه nfs_share دا متشير لجهاز 10.10.10.1 وفي ملف shared ده متشير للكل (علامة ال * دي يعني للكل)
- حلو اوي انا دلوقتي عرفت الملفات وعرفت متشيره لمين انا عاوز بقي اسحبهم بقي ليا عالجهاز عندي هتروح عامل الكوماند ده

“Pasted image 20250209131920.png” could not be found.

- اي كوماند ف دول عادي

“Pasted image 20250209131939.png” could not be found.

Scenario 2 : Data Interception

- ودي عبارة عن MiTM Attack عادي جدا
- بنستخدم ال ettercap وال wireshark
- وتقدر بقي تشوف اي باسوردات او ملفات بتتبعت

Scenario 3 : DoS Attack

- هنا انت بتعمل هجمات حجب الخدمه عادي جدا

.Pasted image 20250209132224.png” could not be found“