SMB Protocol Hacking

SMB (Server Message Block)

SMB

- دا بروتوكول مختص بنقل الملفات بين الاجهزه وبعضها
- هو مختلف عن ال FTP شويه عشان هو هنا بيكون عن نقطة مركزيه او سيرفر يعني بيكون عليها ملفات shared وكل جهاز علي نفس الشبكه بيأكسس عليها وبيحمل اللي مسموح ليه انه يحمله
- بيشتغل علي بروتوكول 139 للاصدارات القديمه وال 445 للاصدارات الجديده
- ال SMB كان مستخدم بشكل كبير في الwindows انما من فتره كدا خلوه بقي يشتغل علي اللينكس والماك برضو عادي

SMB Vulnerabilities Overview

- اول ثغره فال SMB اني ممكن الهاكر ياخد unauthrozied access علي الملفات المتشيره علي السيرفر
- عدم وجود نظام تشفير او استخدام نظام تشفير قديم
- استخدام Guest Acc حد هيقولي ايه المشكله لما جيست يستخدم السيرفر اقولك ياغبي ماهو الجيست ده مبيحتاجش باسورد عشان يخش
- وجود ثغره زي ال EternalBlue ودي CVE مشهوره وخطيره جدا استغلالها بيديك RCE علي السيرفر
- استخدام باسورد او بوليسي ضعيفه

SMB Hacking Scenarios

Scenario 1 : SMB Share Enumeration

- هنا ممكن الهاكر انو يستكشف الملفات المتشيره علي ال smb server والusers ويقدر انو ينزلها علي جهازه من خلال شويه ادوات هنعرفها مع بعض

1. nmap

- اول اداة ممكن اعرف اليوزرز والملفات المتشيره علي السيرفر

"Pasted image 20250208172842.png" could not be found.

- من خلال الامر ده ممكن اقدر اوصل للملفات المتشيره او اليوزرات

"Pasted image 20250208173013.png" could not be found.

- خلي بالك لو طلعلك نتيجه ولقيت مثلا يوزرين C$ و HR اول متشوف ال $ اعرف اني الملف ده عليه صلاحيات ادمن وليه كل الصلاحيات

"Pasted image 20250208173031.png" could not be found.

- بص هنا لقي يوزر guest وكتبلي password not required
- تعالي نعلي شويه ونستخدم تول تانيه

2. SMBClient

"Pasted image 20250208173141.png" could not be found.

```
-L => بقولو اعملي ليستة
-N => بقولو ادخلي باليوزر الجيست
```

"Pasted image 20250208173221.png" could not be found.

- بص هنا بيقولي ايه جابلي الملفات ADMIN$, C$, HR
- تعالي نعلي اكتر شويه ونشوف اداه ادق فالتفاصيل

3. enum4linux

- دي تعتبر ادق اداه فيهم وبتجبلك تفاصيل كتير

"Pasted image 20250208173805.png" could not be found.

- هنا انا بنفذ الامر عادي جدا

"Pasted image 20250208173829.png" could not be found.

- دي النتيجه وطبعا هيا بتكون كبيره جدا فا مش هعرف اجبها كلها
- طيب بعد دا كله يعني وعملت enumeration وبتاع عاوز بقي اخد ملفات

"Pasted image 20250208173939.png" could not be found.

- هتروح جاي يا باشا وتعملي اي كوماند من الاتنين فوق ويفضل تعمل اللي تحت
- طيب دلوقتي بقي دا كان اول سيناريو تعالي اقولك بقيت السيناريوهات

Scenario 2 : Exploiting Unauthenticated SMB Share

- زي ماقولتلك فوق لو عملنا enumeration ولقينا اني في يوزر guest ساعتها اقدر ادخل علي السيرفر من غير باسورد
- طب ازاي استغل حاجه زي دي؟ من خلال اداة ال SMBClient

“Pasted image 20250208174155.png” could not be found.

- بحددلو هنا الايبي ومعاه الملف المعين اللي عاوز ادخل عليه
- يعني بقولو دخلني كا جيست -N

“Pasted image 20250208174236.png” could not be found.

“Pasted image 20250208174244.png” could not be found.

Scenario 3 : Brute Force SMB Login

- فاكر ال brute force اللي كان ف ال FTP ؟ بالظبط هو ده ف ال SMB
- بحاول استخدم اي اداة كراك بحيث تطلعلي الباسورد
- احنا بعد ما عملنا ال enumeration وعرفنا اليوزر نيجي نحطو ف اداة الكراك اللي هيا Hydra مثلا ونقولو يلا يا باشا اعملي cracking للباسورد

“Pasted image 20250208174427.png” could not be found.

“Pasted image 20250208174433.png” could not be found.

“Pasted image 20250208174452.png” could not be found.

- بص هنا انا هنا دخلت عالسيرفر -U دي يعني كا ادمن انما -N كا جيست
- ودخلت بقي الباسورد عادي ودخلت

Scenario 4: Exploiting SMB with EternalBlue

- اخر سيناريو ده عباره عن اني لو لقيت ثغرة ال EternalBlue دي ابدأ اني استغلها
- ملوش لازمه الشرح لأنها خلاص اكتشفت ف 2019 وبقت معروفه ومبقتش موجوده كتير ف السيرفرات
- عاوزك تسرش عنها وتقرأ writeup ليها برضو عشان تفهمها

- EternalBlue (MS17–010/CVE-2017–0144)
  - دول شويه writeups برضو عنها لو مكسل تسرش
- EternalBlue (MS17–010/CVE-2017–0144): Exploit and Vulnerability Overview | by Yash Pawar @HackersParadise | Medium
- Mastering EternalBlue MS17–010 & MS08–067: A Hands-On, Step-by-Step Walkthrough to Exploiting Legacy Windows Vulnerabilities | by Ends2Tech | Medium