FTP Protocol Hacking

FTP (File Transfer Protocol)

FTP

- دا بروتوكول بيستخدم عشان لو هيتم نقل ملفات بين السيرفرات وبعضها
- لو هنزل حاجه من سيرفر او هرفعلو حاجه هستخدم البروتوكول ده
- بيشتغل ف ال Application Layer في ال TCP/IP Model
- ال default port بتاعه هو 21 بس في حالة ال Active Mode ممكن يشتغل علي 20

Models Of Operation

1. Active Mode

- الكلاينت بيبدأ الاتصال على منفذ الـ Command (منفذ 21).
- لما يحتاج نقل بيانات (تحميل/رفع ملفات)، الكلاينت يبعت أمر `PORT` للسيرفر ويقوله "اتصل بيا على المنفذ ده".
- السيرفر يفتح منفذ 20 ويتصل بالكلاينت لنقل البيانات.

✅ مناسب لما يكون عندك كلاينت مش وراه فايروول أو NAT، لأنه يسمح بالاتصال العكسي من السيرفر.

⚠️ المشكلة؟
لو الكلاينت خلف Firewall/NAT، السيرفر مش هيقدر يتصل بيه، وبالتالي الاتصال هيفشل!

2. Passive Mode

- الكلاينت بيبدأ الاتصال على منفذ 21 كالعادة.
- بدلاً من انتظار اتصال من السيرفر، الكلاينت يبعت `PASV` للسيرفر.
- السيرفر يفتح منفذ عشوائي ويقوله للكلاينت "اتصل بيا على المنفذ ده".
- الكلاينت هو اللي يتصل بالسيرفر لنقل البيانات.

✅ مناسب لما يكون الكلاينت خلف Firewall/NAT، لأنه هو اللي بيبدأ كل الاتصالات، وبالتالي الفايروول مش هيمنعه.

FTP Authentication

- عشان اعرف اتصل بسيرفر ftp لازم اكون عارف ال user وال pass بتوعه عشان اقدر اكونكت بيه
- خلي بالك لو انا ب sniff علي ال traffic فا ال user وال pass بيتبعتو كا plain text يعني اي حد عامل mitm يقدر يشوفهم عادي جدا طب ايه الحل؟
- الحل في ال FTPS (FTP Secure) او SFTP (Secure FTP via SSH)

  FTPS: FTP over SSL/TLS (adds encryption)

  SFTP: FTP over SSH (more secure, widely used)

  HTTP/HTTPS: Can also be used for file transfers with web servers

  WebDAV: An HTTP extension for file management over the web
- طب انا دلوقتي معرفش ال user وال pass اعمل ايييه؟ تعالي بقي نشوف ال scenarios اللي ممكن تخلينا نعرفهم

FTP Hacking Scenarios

Scenario 1 : FTP Brute Force Attack

- مفهوم ال brute force ومتحاولش تترجمها نصيحه مني هيا اني بقعد اجرب كلمات سر كتير جدا من خلال اداة معينه وهو بيشوف وبيجرب ولو في حاجه نفعت هيقولي خد دا الباس

  خطوت الattack
- لازم اشوف اذا البورت بتاع ال ftp مفتوحه ولا لأ الاول

"Pasted image 20250208132713.png" could not be found.

النتيجه ادتني انو مفتوح كدا تمام

- هنستخدم اداة اسمها Hydra او اي اداة cracking يعني بس ف السيناريو هنستخدم hydra

```
hydra -L /path/to/user-list.txt -P /path/to/password-list.txt ftp://10.10.10.1
```

هنا هيبدأ انو يخملي اليوزر والباس ولو حاجه نفعت هيديني اليوزر والباس الصح

Scenario 2 : Exploiting Anonymous Access

- في ناس بيكونو ناسيين الftp server وعاملين اليوزر والباس anonymous وناس كتير كدا فا انت تجرب تدخل بيهم يمكن تنفع

Scenario 3 : MITM Attack on FTP

- هنا لازم يكون الهاكر ف نفس الشبكه اللي عليها السيرفر
- هنعمل ال man in the middle عادي جدا زي ماشرحنا قبل كدا
- هنستخدم ال wireshark عشان نشوف الtraffic وcapture الداتا

Scenario 4 : Directory Traversal Attack

- الattack دا ممكن اعملو لما اخش علي السيرفر بقي
- وهو اني عباره عن ثغره كدا ممكن توصلني لملفات حساسه جدا جوا السيرفر

“Pasted image 20250208133507.png” could not be found.

- هنا انا اتصلت بالسيرفر عادي ودخلت اليوزر والباس عادي

“Pasted image 20250208133528.png” could not be found.

- الكوماند ده هو اللي ممكن يدخلني علي ال etc وال etc طبعا فيه كل الباسوردات اللي تخص السيرفر وفيه حاجات مهمه تانيه طبعا بس خلي بالك اني الطريقه مش هتنفع ف كل السيرفرات لأنها عبارة عن ثغره اصلا

“Pasted image 20250208133624.png” could not be found.

- هنا مثلا بعد ما اشتغلت معايا ببدأ انزل ملف الباسوردات علي جهازي بقي

Scenario 5 : Exploiting Misconfigured Permissions

- الattack دا برضو بيحصل لما ادخل علي السيرفر
- بعد ما ادخل علي السيرفر ببدأ اشوف ايه ال directories اللي فيها permissions ال write

- اول ما الاقي dir فيه البريمشن دي ببدأ ارفعلو malicious code عباره عن reverse shell وده عباره عن اني بفتح backdoor علي السيرفر واتحكم فيه remotely بالكامل ودي بنسميها RCE او Remote Code Execution

“Pasted image 20250208133918.png” could not be found.

“Pasted image 20250208133924.png” could not be found.

- بعدا كدا عاوز بقي اشغل الملف ده فا هشغلو عن طريق الويب

“Pasted image 20250208134053.png” could not be found.

To execute RCE attack you can put code inside shell.php