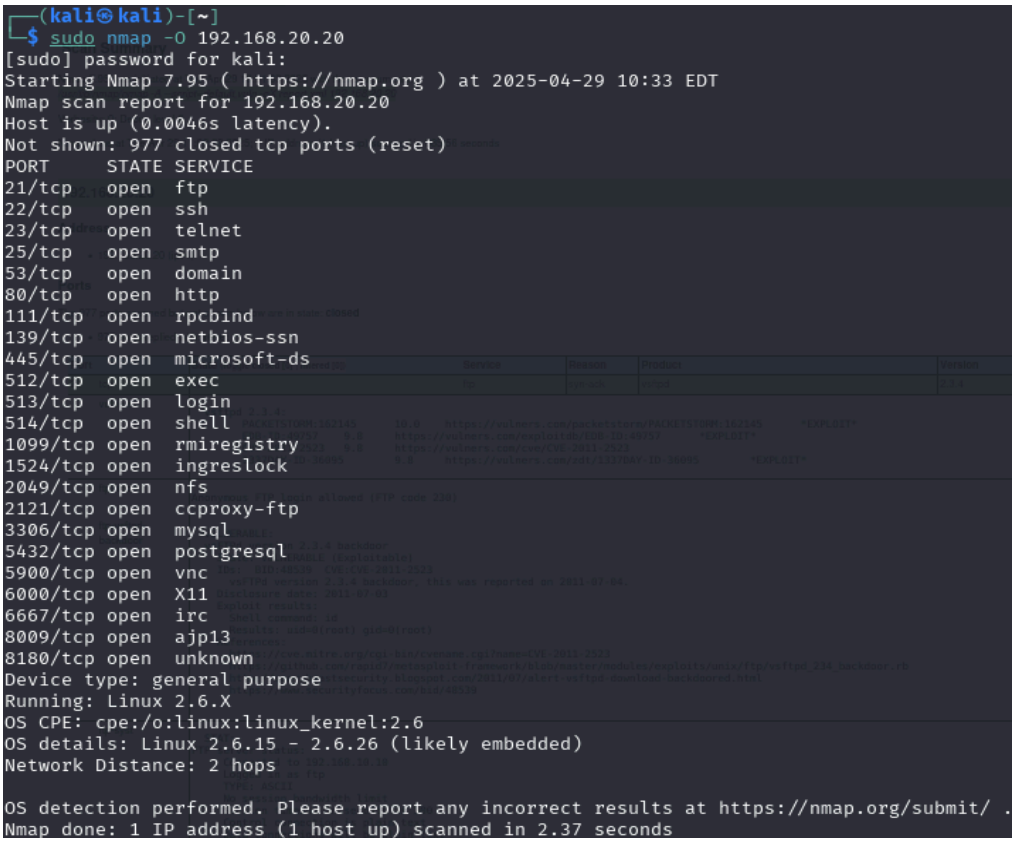
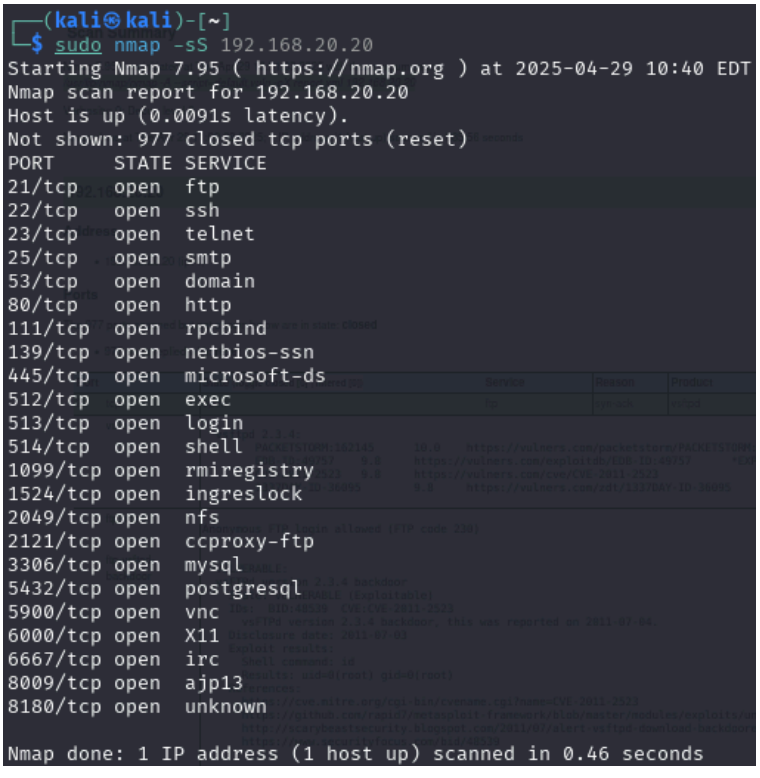
Tecniche di scansione con Nmap su Metasploitable e Windows

Metasploitable:

La scansione Nmap **OS fingerprint**, inviando una serie di pacchetti TCP/IP all'host (Metasploitable) e confrontando le risposte con il suo database fingerprint os, appunto, ci riporta dettagli sul suo sistema operativo, le porte aperte e i servizi in ascolto su di esse.

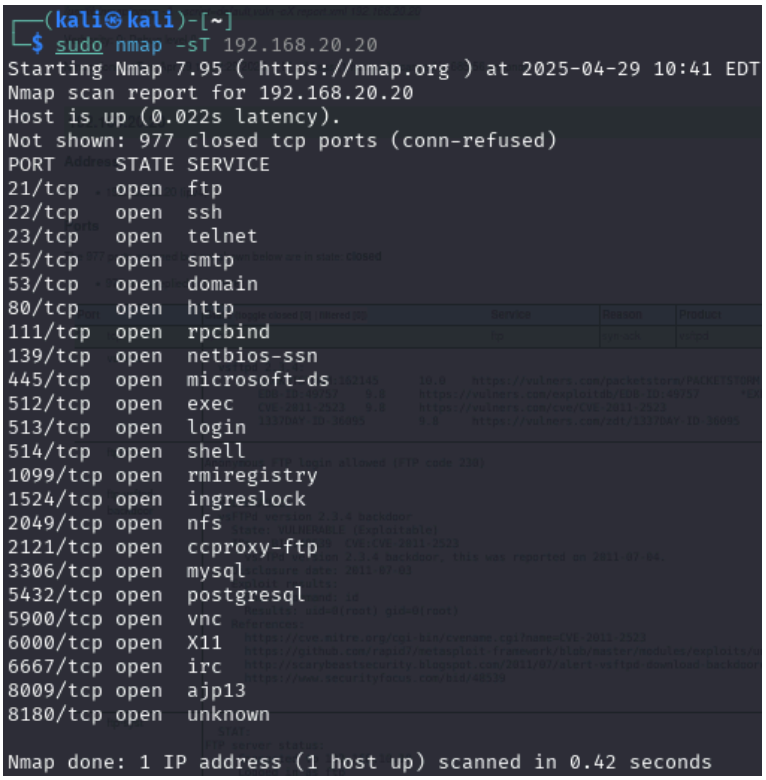


La scansione Nmap **Syn Scan** ci riporta una scansione di tutte le porte apert su un host.

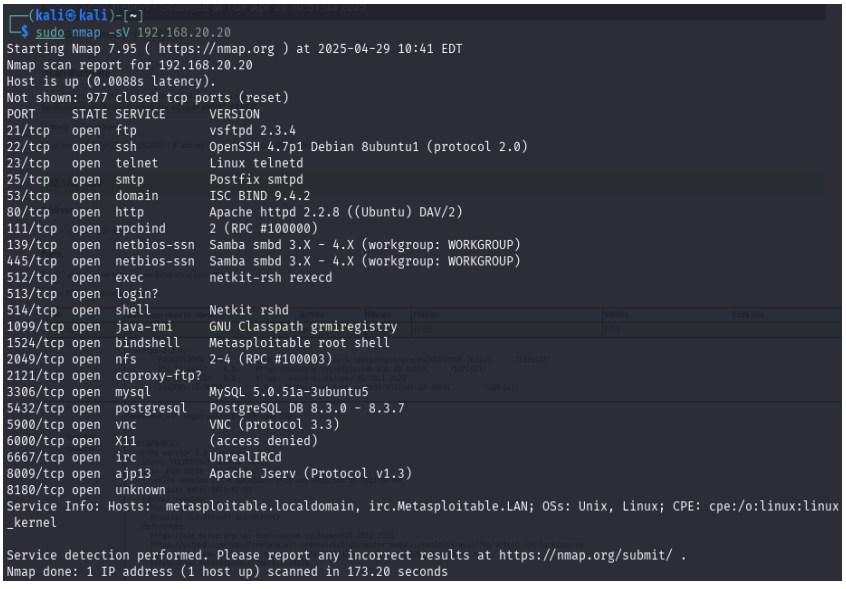


La scansione Nmap **TCP Connect** ha la stessa funzionalità della SYN Scan. Non c'è molta differenza nell'uno e nell'altro, se non che nell'analisi del pacchetto.

La Syn Scan è una scansione più veloce e discreta, per cui spesso non viene registrata nei log del sistema target, host.
La TCP Connect è una scansione diretta che stabilisce una connessione completa con le porte dell'host, quindi più facilmente rilevabile nei log del sistema target.



La scansione Nmap **Version Detection** ci fa una scansione delle porte, ma non si ferma alla connessione TCP. Ci dà anche la versione software, molto importante per capire la sua vulnerabilità.
Riesce a fare questo interrogando i Banner servizio per servizio e risalendo alla versione del servizio in esecuzione sull'host.
Fornisce una visione dettagliata dei servizi attivi, utile per valutazioni di sicurezza e pen testing. In sintesi, è uno strumento potente per il banner grabbing e la rilevazione delle versioni dei servizi, automatizzando e migliorando il processo di identificazione rispetto ai metodi manuali. Utilizzare questa scansione ci consente di ottenere rapidamente una visione dettagliata dei servizi attivi su un host.

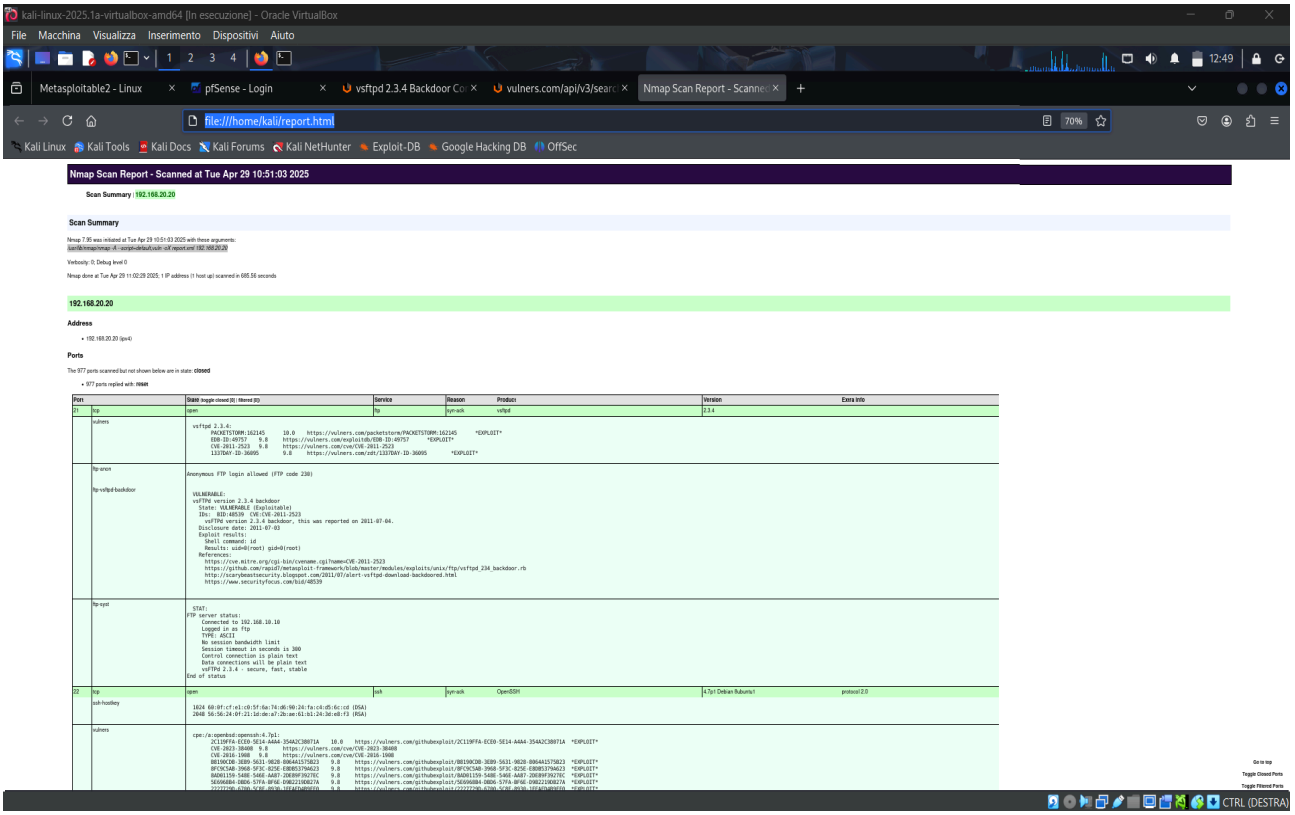


Eseguendo sul terminale della Kali il comando:

```
sudo nmap -A --script=default,vuln -oX report.xml 192.168.20.20
```

È possibile visualizzare un report delle scansioni effettuate, e convertire il file .xml in .html, sulla cartella della Kali, per leggerle in maniera ancora più chiara, eseguendo il comando:

```
xsltproc report.xml -o report.html
```



Windows:

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.1.154
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 16:47 EDT
Nmap scan report for 192.168.1.154
Host is up (0.0033s latency).
Not shown: 990 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
5357/tcp open  wsdapi
8443/tcp open  https-alt
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows 10 1607 (97%), Microsoft Windows Phone 7.5 or 8.0 (94%), Microsoft Windows
 Embedded Standard 7 (93%), Microsoft Windows 10 1511 - 1607 (92%), Microsoft Windows 7 or Windows Server 2008 R2 (
91%), Microsoft Windows Server 2008 R2 or Windows 8.1 (91%), Microsoft Windows Server 2016 (91%), Microsoft Windows
 Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (91%), Microsoft Windows 11 21H2 (91%), Microsoft Windows
Vista SP2, Windows 7 SP1, or Windows Server 2008 (90%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.14 seconds
```

Eseguiamo stavolta la scansione Nmap OS Fingerprint sul target Windows.
Come detto prima, per la Metasploitable, esegue la sua solita scansione ma in questo caso non riesce ad identificare con precisione il sistema operativo, probabilmente a causa del Firewall di sistema attivo che modifica o blocca i pacchetti usati da Nmap per l'OS Fingerprint, a

differenza di Metasplitable.