Traccia: Tecniche di scansione con Nmap

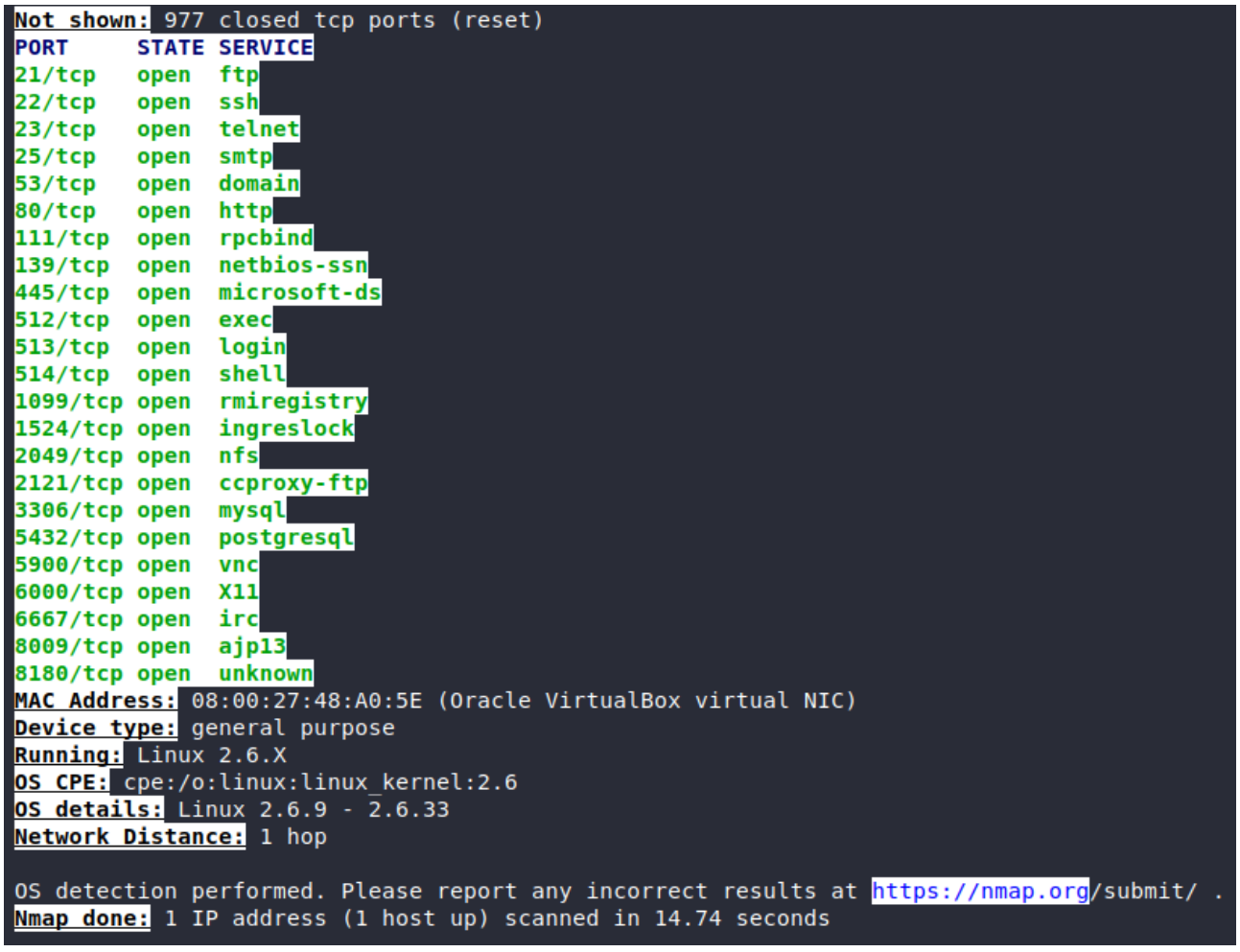
Si richiede allo studente di effettuare le seguenti scansioni sul target Metasploitable:

-OS fingerprint

Una scansione TCP che ha come obiettivo quello di identificare il OS del target.

Il sistema target viene analizzato in base all ispezione dei pacchetti di risposta ricevuti, la determinazione del OS viene stabilita in base a TTL e alla grandezza della finestra TCP (che rapresenta in numero di byte che il sistema necessita di ricevere in input prima di rispondere ad un messaggio ricevuto).

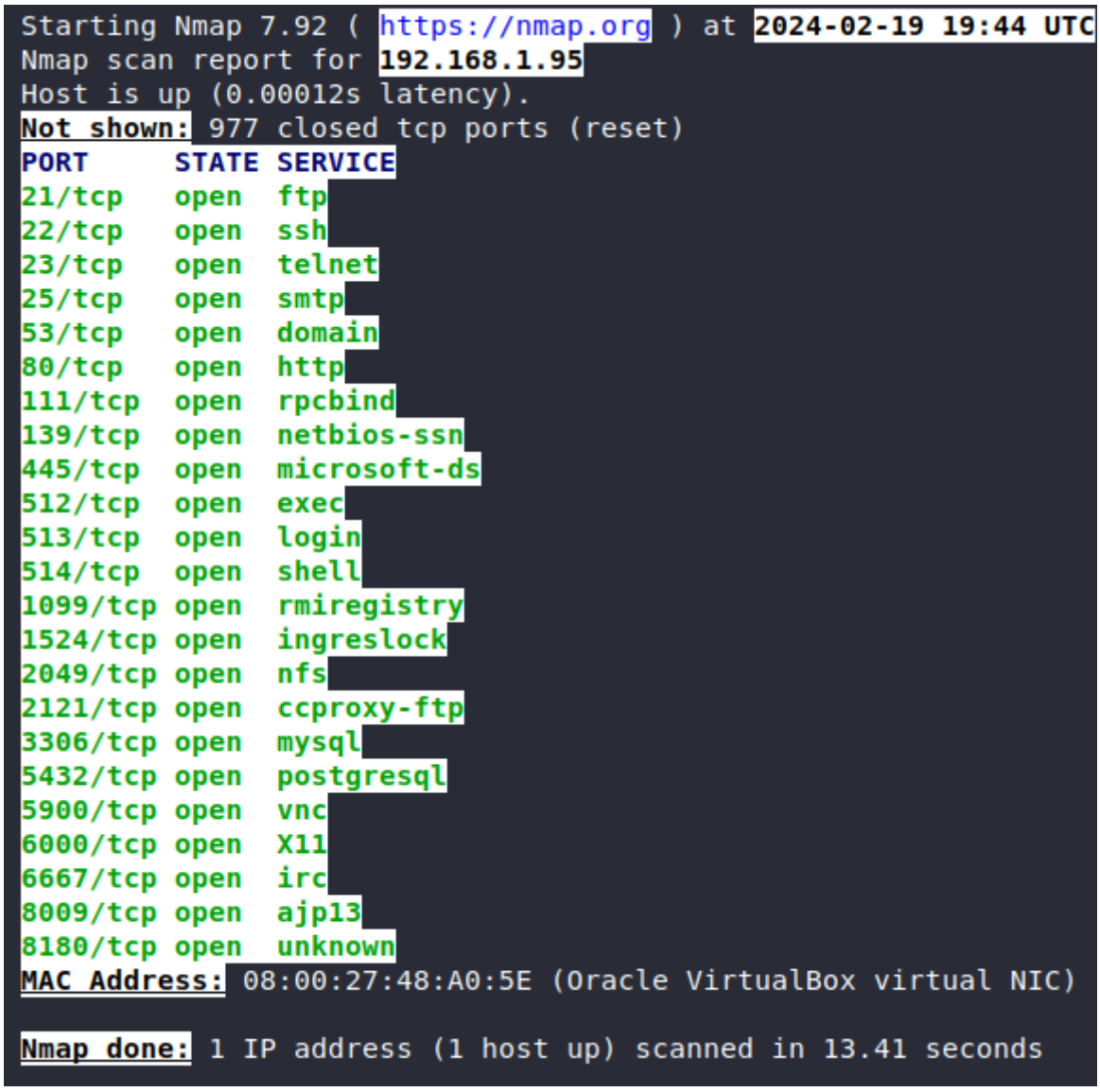
Questa scansione e fondamentale in quanto conoscendo OS del target , sapremo di conseguenza i suoi punti deboli .



Vediamo come il comando nmap -o IP target restituisce in output N di porte chiuse , le porte (TCP) aperte con i loro relativi servizi ,MAC address ,OS e la sua versione di aggiornamento.

Syn Scan:

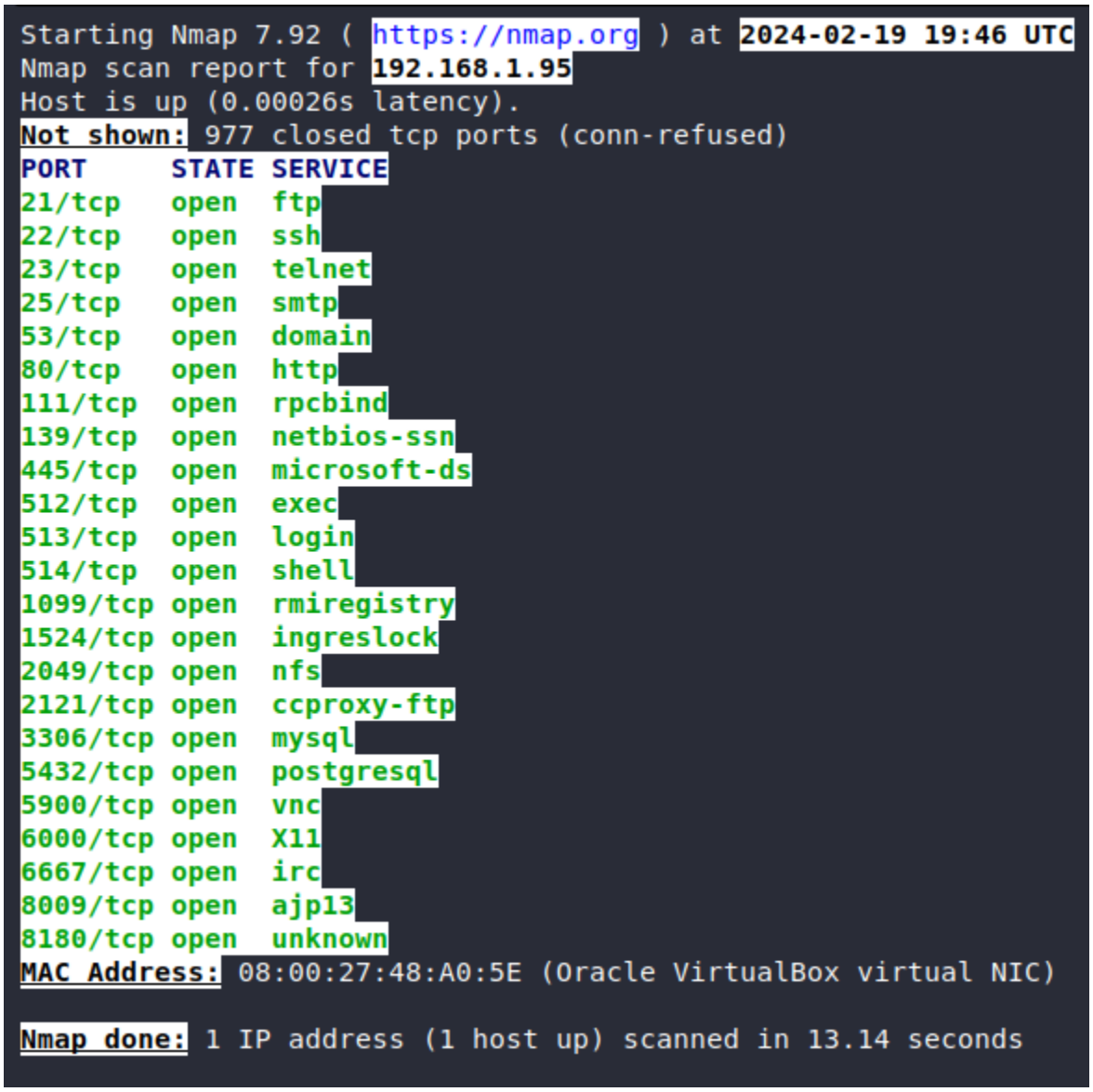
Scansione poco invasiva difficilmente tracciabile in quanto non si basa sula connessione 3 way-handshack , utilizzando il protocollo RST/ACK evitando cosi di 1 chreare un ponte di comunicazione trai 2 sistemi coinvolti , di conseguenza 2 evita che il sistema attaccante venga loggato (e quindi lasci il segno di un suo passaggio) sulle porte scansionate del target.



Vediamo come l output del comando nmap -sS IP target restituisca come risultato

Porte i loro relativi servizi e l indirizzo MAC

TCP connect: nmap -sT IP target



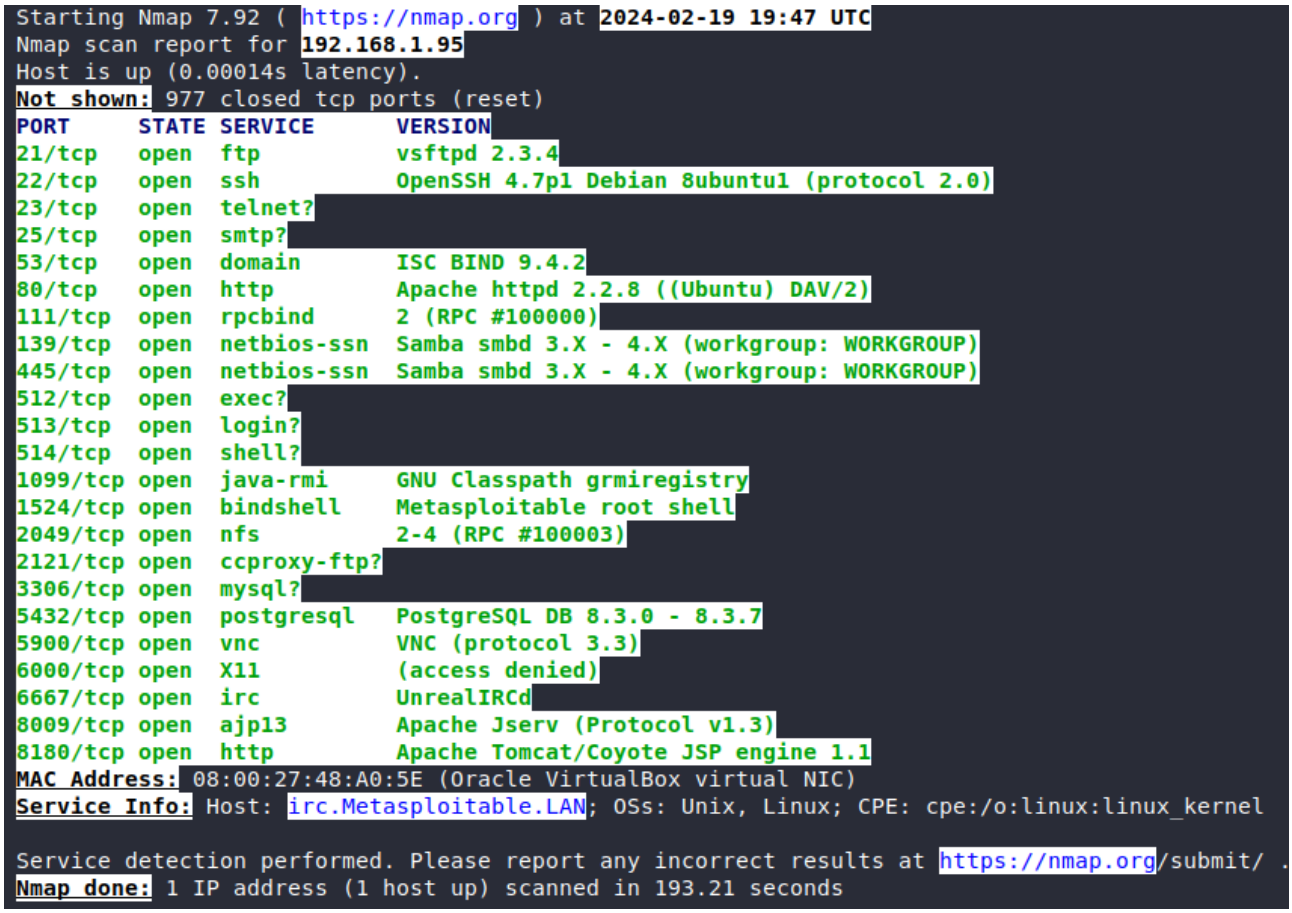
Come vediamo le differenze tra Syn scan e TCP connect come output sono identiche

La differenza sostanziale si puo verificare tramite dei sniffer come wireshark,

lo TCP scan crea ,anche se per breve tempo, dei canali di comunicazione (3 way handshack) con le porte che analizza. Di conseguenza e una scansione facilmente rilevabile non solo durante la sua esecuzione, ma anche in un secondo momento controllando i log delle porte scansionate (del target).

Version detection: nmap -sV

Scansione lenta e pesante ma precisa. Fornisce come output non solo le porte aperte con i loro relativi servizi ma anche la versione dei software che le gestiscono e informazioni dettagliate sul OS utilizzato dal target



IP/OS

Host: Kali GNU/Linux 2024.1 Target: Metasploitable Linux 2.6.x

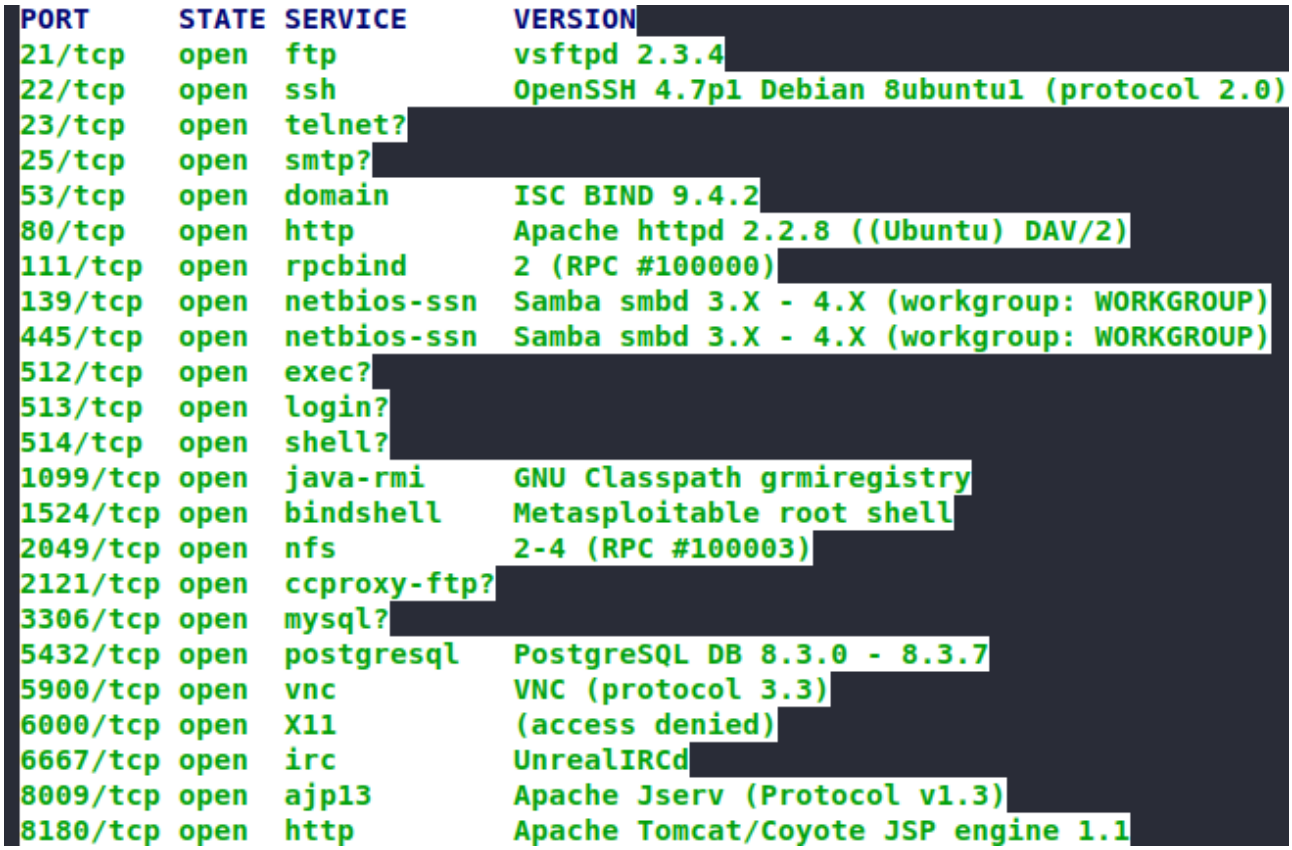
192.168.1.100 192.168.1.95

OS protetto da un firewall

Nessuna porta scansionata

Target: : Metasploitable Linux 2.6.x

192.168.1.95



```
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          vsftpd 2.3.4
22/tcp   open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet?
25/tcp   open  smtp?
53/tcp   open  domain       ISC BIND 9.4.2
80/tcp   open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind      2 (RPC #100000)
139/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec?
513/tcp  open  login?
514/tcp  open  shell?
1099/tcp open  java-rmi     GNU Classpath grmiregistry
1524/tcp open  bindshell    Metasploitable root shell
2049/tcp open  nfs          2-4 (RPC #100003)
2121/tcp open  ccproxy-ftp?
3306/tcp open  mysql?
5432/tcp open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc          VNC (protocol 3.3)
6000/tcp open  X11          (access denied)
6667/tcp open  irc          UnrealIRCd
8009/tcp open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp open  http         Apache Tomcat/Coyote JSP engine 1.1
```

Descrizione dei servizi:

ftp : File Transfer Protocol : protocollo di livello applicativo per il transfetimento di file basata su TCP e con architettura di tipo client-server

ssh: Scure Shell protocollo che permette di stabilire una sessione remota cifrata tramite interfaccia a riga di comando con un altro host di una rete informatica.

telnet : e un protocollo di rete, utilizzato tramite interfaccia a riga di comando per fornire all utente sessioni di login remoto.

Smtp: e un protocollo per la trasmisione di email.

Domain: Domain Name System indica un Sistema utilizzato per assegnare nomi ai nodi delle reti

http : protocollo di livello applicativo usato come principale sistema per la trasmisione d informazione sul web

rpcbind : un mecanismo per la gestione di aolicazioni client/server

netbios-ssn: protocollo di livello sessione e riferito ad um API per comunicazioni sulla rete locale

exec: e una funzione di sistema presente nelle libretie standard del C del progetto GNU

Java-rmi : e una tecnologia che consente a processi java distribuiti di comunicazione