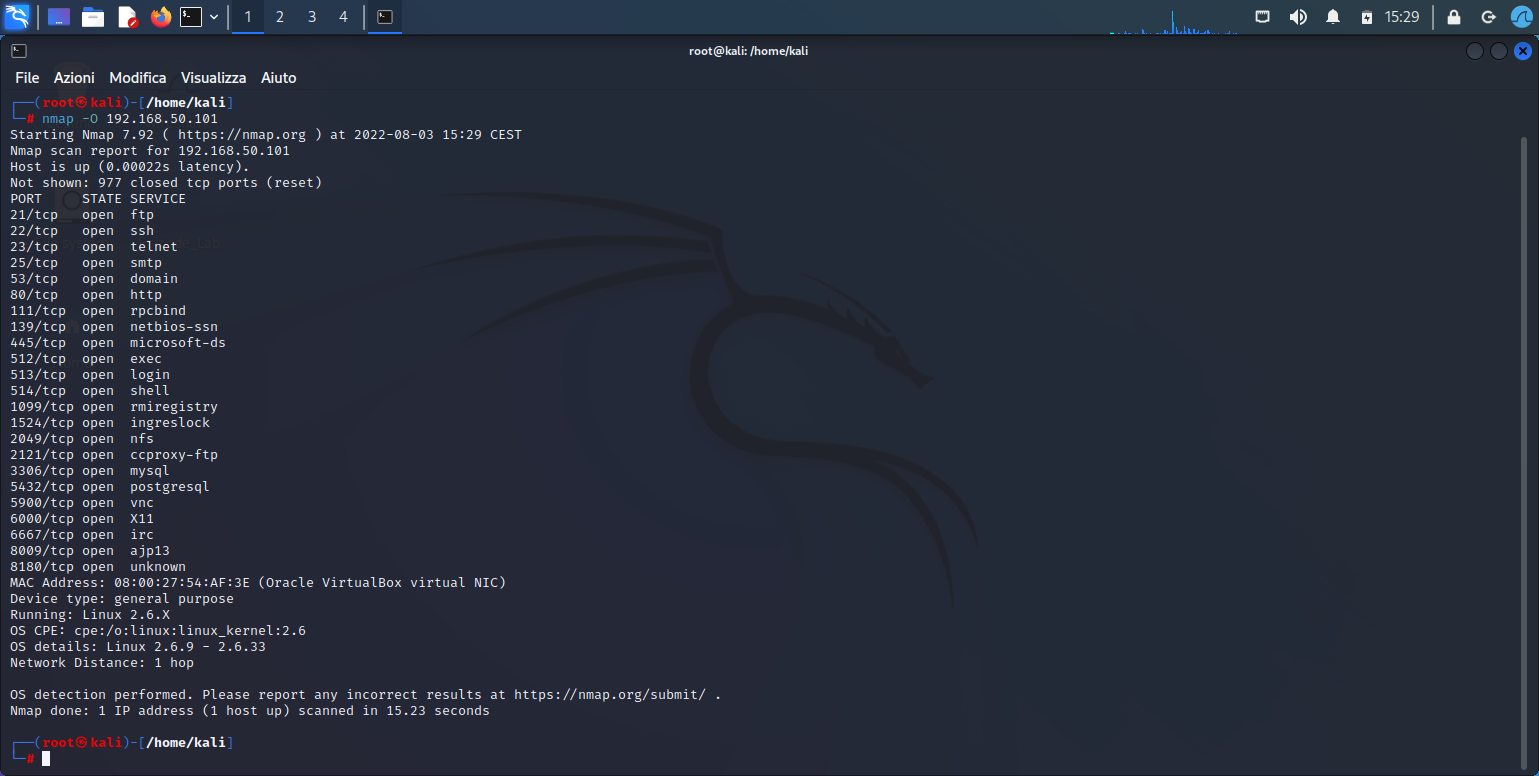
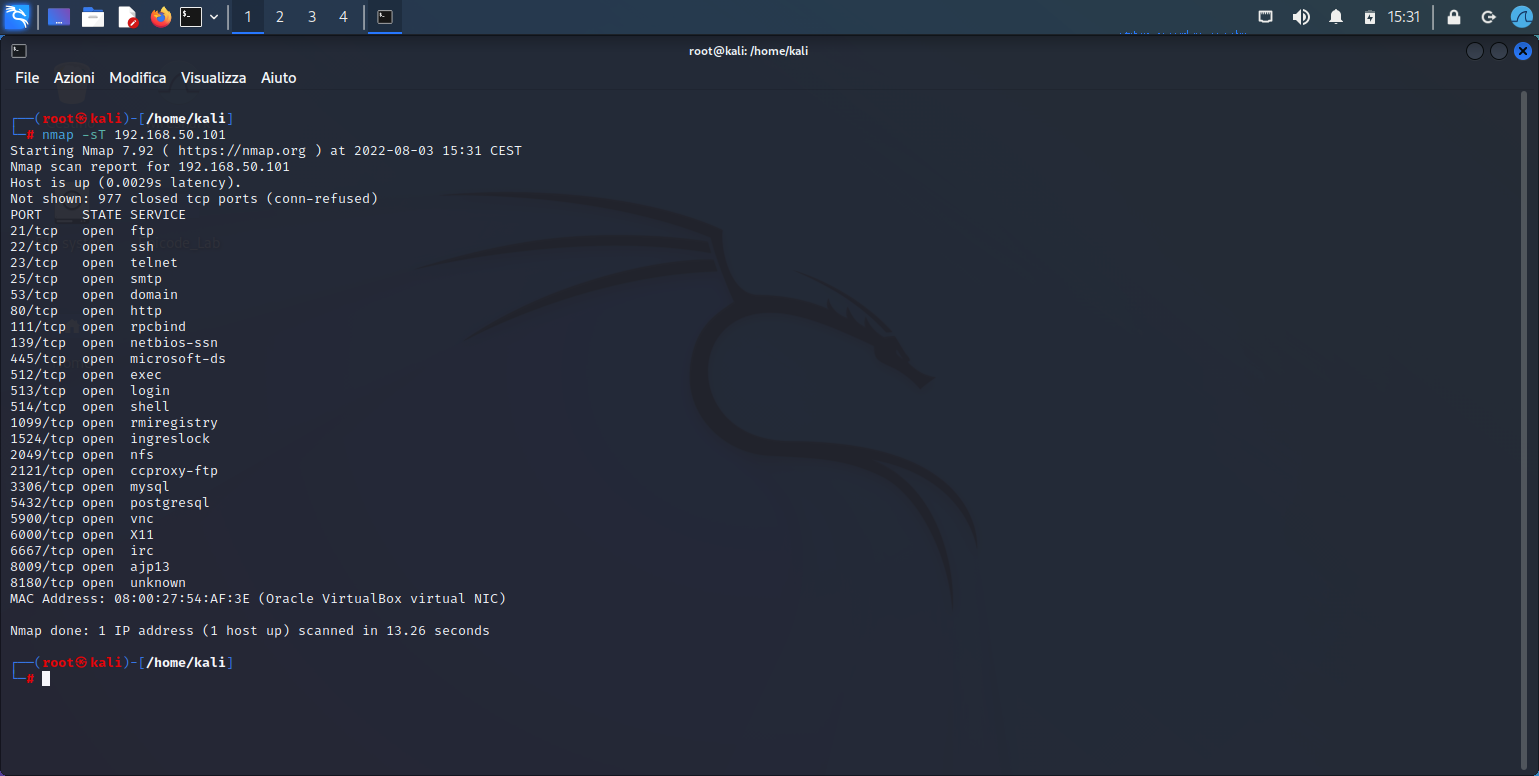
REPORT SCANSIONE NMAP

Metasploitable



Lo scan OS fingerprint (-0) serve a determinare il tipo di sistema operativo che la macchina vittima ha attualmente in uso, dando modo all’attaccante di acquisire informazioni e probabili vulnerabilità del sistema operativo per poter lanciare di conseguenza un attacco.



SCANSIONE TCP

Tramite il comando -sT si avvia una scansione TCP. Nello screenshot seguente si possono vedere le porte con relativo stato e servizio con accanto,

21/tcp(porta): ftp (servizio) = File Transfer Protocol, basato su architettura client/server, ed è un protocllo utilizzato per trasferire file tra computer su internet.

22/tcp: ssh= Secure Shell, protocollo che consente di stabilire una sessione remota con un altro host di una rete

25/tcp: smtp= Simple Mail Transfer Protocol, protocollo standard per la trasmissione di email.

53/tcp: domain = associa il nome di un dominio ad un indirizzio IP

80/tcp: http = HyperText Transfer Protocol, protocollo utilizzato per la trasmissione di informazioni sul web.

139/tcp netbios-ssn = Network Basic Input/Output System, solitamente riferito ad un’API per comunicazione sulla rete locale.

445/tcp Microsoft-ds, servizio che viene utilizzato per le risorse condivise smb(sever message block)

512/tcp exec= qui troviamo il servizio exec(Remote Execution Control) che viene utilizzato per eseguire un programma su un server remoto

513/tcp login= servizio login che veniva utilizzato per l’amministrazione da remoto, ma è stato rimpiazzato dal servizio SSH

514/tcp shell= servizio per lo spoofing degli indirizzi IP.

1099/tcp open rmiregistry= comunicano tramite porte casuali finchè una porta fissa viene specificata quando viene esportato un oggetto remoto.

1524/tcp ingreslock = è un servizio legittimo che blocca parti di un database ingres

2049/tcp nfs = è un’applicazione client/server che permette all’utente di visualizzare e di salvare o aggiornare files su un pc all’altro in remoto.

2121/tcp ccproxy-ftp = porta proxy-ftp che permette di connettersi in remoto tra due host e trasferire dati. Spesso usata dagli attaccanti come exploit tramite myscadagate.exe

3306/tcp mysql = è un sistema di gestione di database, che può contenere ad esempio una lista di elementi o di informazioni di una network aziendale.

5432/tcp postgresql = viene usata per l’autenticazione adattiva e per il salvataggio di dati di molte applicazioni analitiche, web ecc.

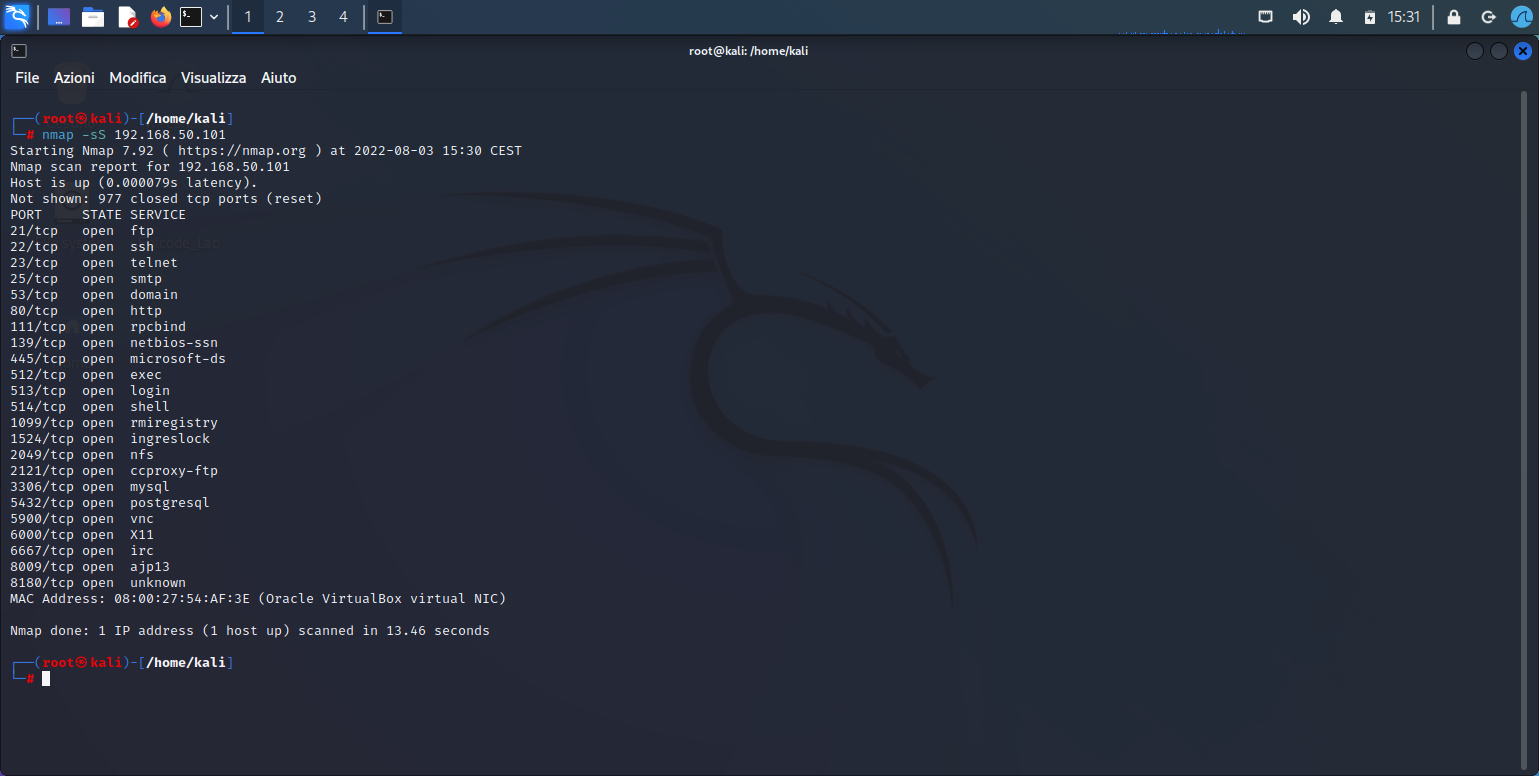
5900/tcp vnc = viene usata per l’accesso/controllo remoto del proprio computer a distanza

6000/tcp x11 = protocollo usato dalle macchine linux per il display in remoto

6667/tcp IRC = usa un protocollo specifico per far comunicare in tempo reale conversazioni tra due host o tra altri dispositivi.

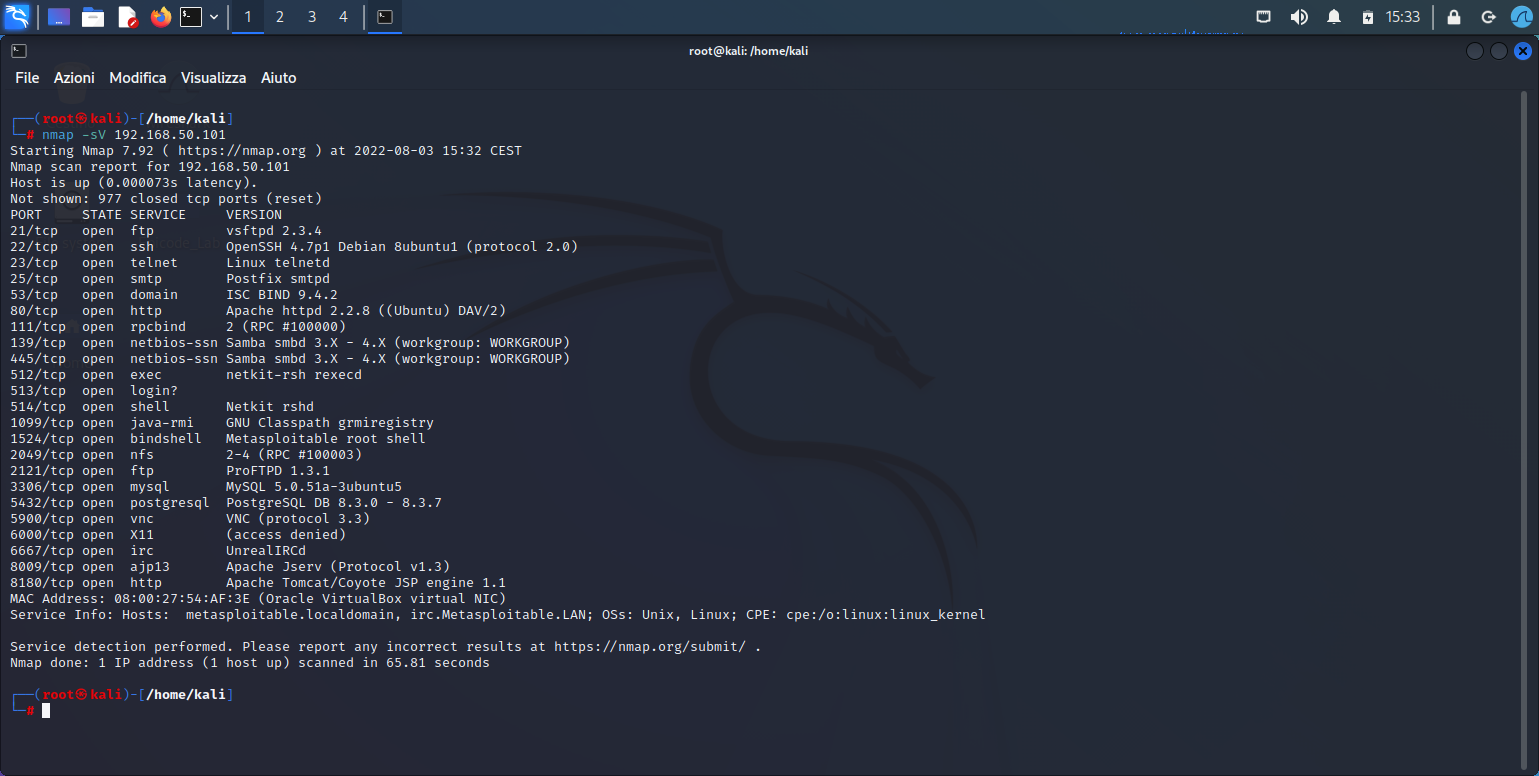
8009/tcp ajp13 = è una versione ottimizzata del protocollo http che permette a un server web standalone di comunicare a Tomcat (ad esempio Apache).

8180/tcp unknown= non si conosce la porta.



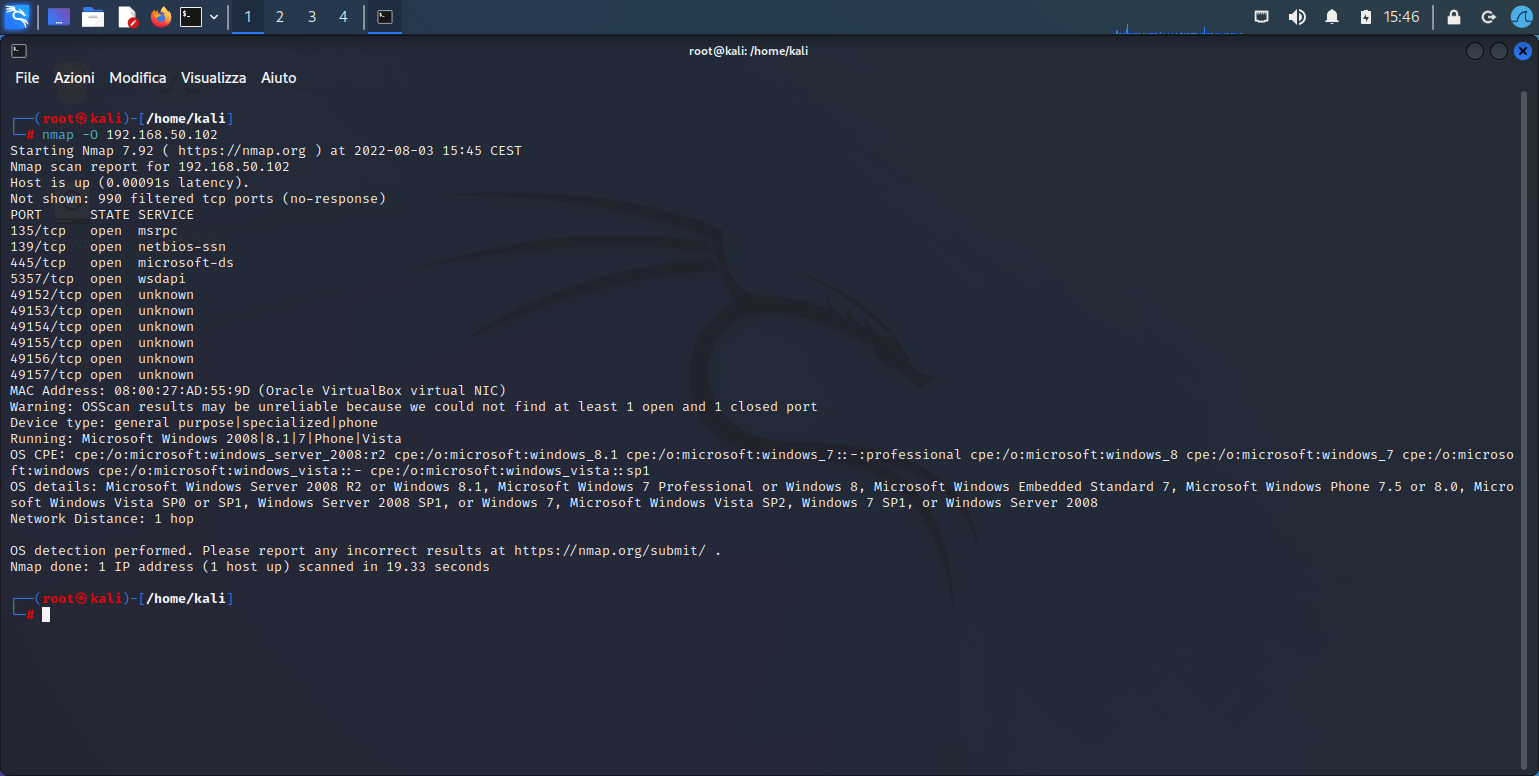
SCANSIONE SYN (-sS)

La scansione SYN è meno invasiva, Nmap non completa il 3 way handshake, ma chiude la comunicazoine inviando un pacchetto RST(reset). Tuttavia, recupera informazioni sullo stato della porta generando meno meno traffico e cosi definita come ‘’stealth scan’



VERSION DETECTION (-sV)

La scansione -sV è una variante della scansione TCP con la differenza di alcuni test per la rilevazione dei servizi sulle porte in ascolto. Anche suddetta scansione è abbastanza facile da rilevare perché genera molto traffico di rete.



OS FINGERPRINT (KALI A WINDOWS 7)

Qui è stato usato lo scan del sistema operativo per windows 7, ma come in figura, lo scan ha generato esito negativo perchè il firewall di windows ha negato la connessione e di conseguenza chiuso le porte a nmap.