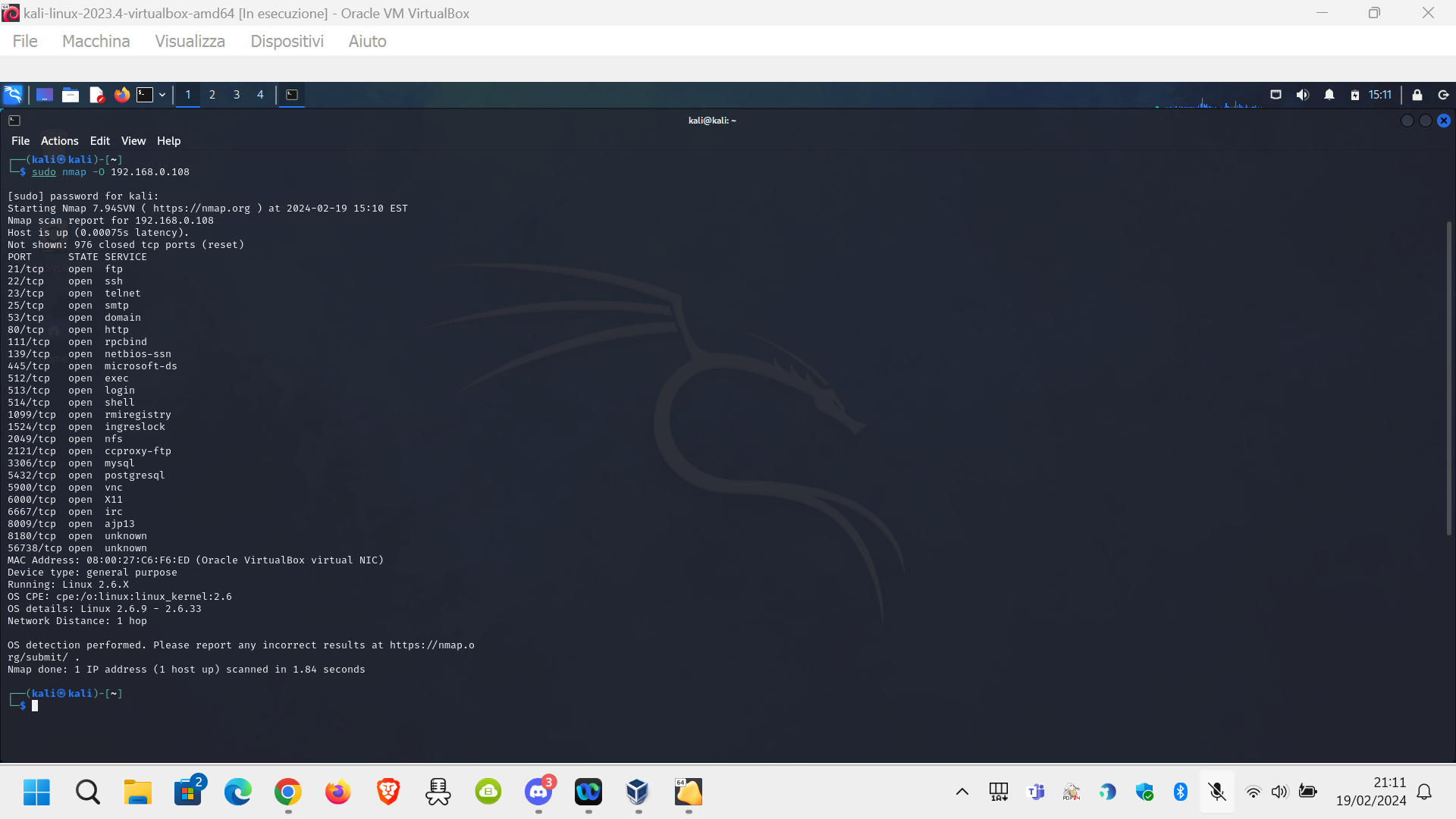
SCANSIONE OS FINGERPRINT CON IP METASPLOITABLE:



**Ecco il report della scansione dell'OS fingerprint per l'IP 192.168.0.108:**

IP e Sistema Operativo:

Indirizzo IP: 192.168.0.108

Sistema Operativo: Linux (dalle informazioni fornite da Nmap)

Porte Aperte:

21/tcp (ftp)

22/tcp (ssh)

23/tcp (telnet)

25/tcp (smtp)

53/tcp (domain)

80/tcp (http)

111/tcp (rpcbind)

139/tcp (netbios-ssn)

445/tcp (microsoft-ds)

512/tcp (exec)

513/tcp (login)

514/tcp (shell)

1099/tcp (rmiregistry)

1524/tcp (ingreslock)

2049/tcp (nfs)

2121/tcp (ccproxy-ftp)

3306/tcp (mysql)

5432/tcp (postgresql)

5900/tcp (vnc)

6000/tcp (X11)

6667/tcp (irc)

8009/tcp (ajp13)

8180/tcp (unknown)

56738/tcp (unknown)

Servizi in ascolto con versione:

I servizi in ascolto includono FTP, SSH, Telnet, SMTP, DNS, HTTP, RPC, NetBIOS, SMB, exec, login, shell, RMI registry, PostgreSQL, NFS, MySQL, VNC, X11, IRC, AJP13 e altri. Le versioni specifiche dei servizi possono essere identificate utilizzando ulteriori comandi Nmap o altri strumenti di analisi.

Descrizione dei servizi:

FTP: Protocollo di trasferimento file.

SSH: Shell sicura, utilizzata per accesso remoto sicuro e trasferimento file.

Telnet: Protocollo di comunicazione remota non crittografato.

SMTP: Protocollo di trasferimento della posta elettronica.

HTTP: Protocollo di trasferimento ipertestuale per il World Wide Web.

DNS: Sistema di nome di dominio per la risoluzione dei nomi degli host in indirizzi IP.

RPC: Protocollo di chiamata remota di procedure.

NetBIOS: Servizio di supporto per la condivisione di file e la stampa su reti Microsoft.

SMB: Protocollo di condivisione di file e stampanti su reti Microsoft.

MySQL: Sistema di gestione di database relazionali.

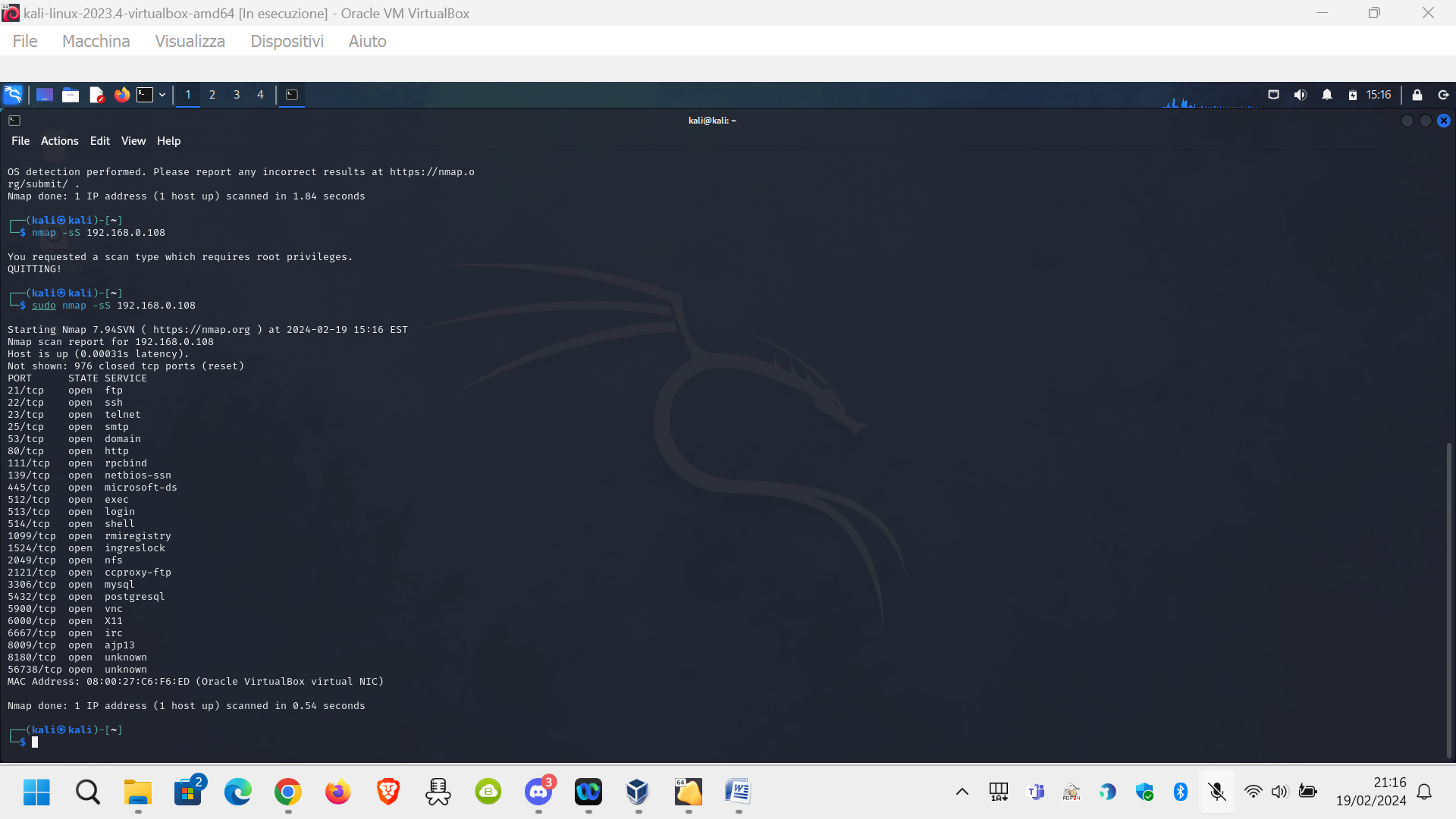
VNC: Controllo remoto del desktop.

X11: Sistema di finestre per sistemi UNIX.

IRC: Internet Relay Chat, sistema di chat in tempo reale.

AJP13: Protocollo di comunicazione tra web server e application server.

SCANSIONE SYN-SCAN:



**Ecco il report della scansione Syn Scan per l'IP 192.168.0.108:**

Porte Aperte:

21/tcp (ftp)

22/tcp (ssh)

23/tcp (telnet)

25/tcp (smtp)

53/tcp (domain)

80/tcp (http)

111/tcp (rpcbind)

139/tcp (netbios-ssn)

445/tcp (microsoft-ds)

512/tcp (exec)

513/tcp (login)

514/tcp (shell)

1099/tcp (rmiregistry)

1524/tcp (ingreslock)

2049/tcp (nfs)

2121/tcp (ccproxy-ftp)

3306/tcp (mysql)

5432/tcp (postgresql)

5900/tcp (vnc)

6000/tcp (X11)

6667/tcp (irc)

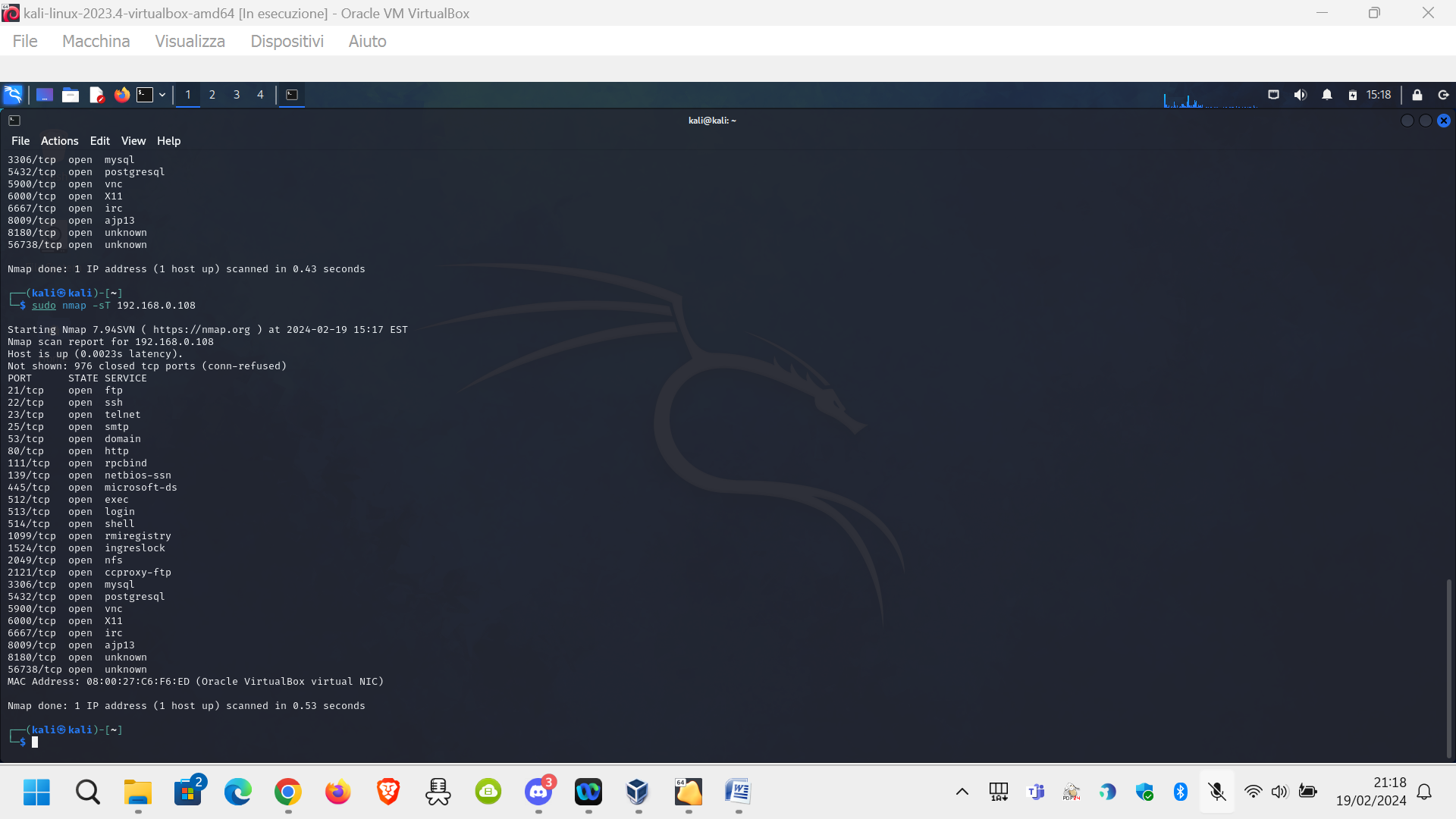
8009/tcp (ajp13)

8180/tcp (unknown)

56738/tcp (unknown)

La scansione Syn Scan ha confermato le stesse porte aperte riscontrate nella scansione dell'OS fingerprint. Non ci sono differenze significative nei risultati tra le due scansioni Syn Scan e OS fingerprint.

SCANSIONE TCP CONNECT-SCAN:



**Ecco il report della scansione TCP connect per l'IP 192.168.0.108:**

Porte Aperte:

21/tcp (ftp)

22/tcp (ssh)

23/tcp (telnet)

25/tcp (smtp)

53/tcp (domain)

80/tcp (http)

111/tcp (rpcbind)

139/tcp (netbios-ssn)

445/tcp (microsoft-ds)

512/tcp (exec)

513/tcp (login)

514/tcp (shell)

1099/tcp (rmiregistry)

1524/tcp (ingreslock)

2049/tcp (nfs)

2121/tcp (ccproxy-ftp)

3306/tcp (mysql)

5432/tcp (postgresql)

5900/tcp (vnc)

6000/tcp (X11)

6667/tcp (irc)

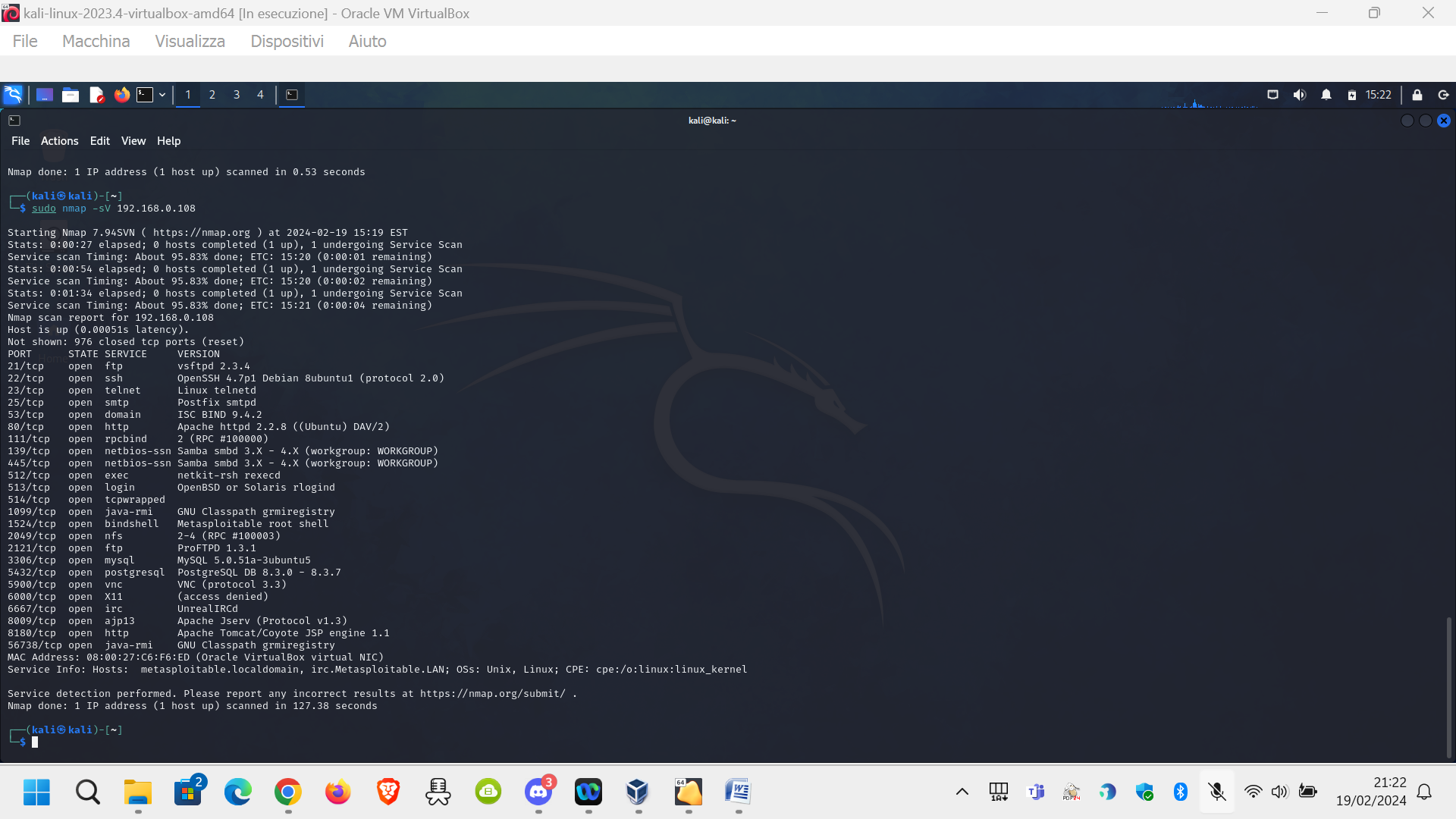
8009/tcp (ajp13)

8180/tcp (unknown)

56738/tcp (unknown)

La scansione TCP connect ha confermato le stesse porte aperte riscontrate nelle scansioni Syn Scan e OS fingerprint. Non ci sono differenze significative nei risultati tra le tre scansioni.

SCANSIONE VERSION DETECTION:



**Ecco il report della scansione di rilevamento delle versioni dei servizi (Version Detection) per l'IP 192.168.0.108:**

Porte Aperte con Servizi e Versioni:

21/tcp: vsftpd 2.3.4 (FTP)

22/tcp: OpenSSH 4.7p1 Debian 8ubuntu1 (SSH)

23/tcp: Linux telnetd (Telnet)

25/tcp: Postfix smtpd (SMTP)

53/tcp: ISC BIND 9.4.2 (DNS)

80/tcp: Apache httpd 2.2.8 (Ubuntu) DAV/2 (HTTP)

111/tcp: RPCbind 2 (RPC)

139/tcp: Samba smbd 3.X - 4.X (NetBIOS-SSN)

445/tcp: Samba smbd 3.X - 4.X (NetBIOS-SSN)

512/tcp: netkit-rsh rexecd (Exec)

513/tcp: OpenBSD or Solaris rlogind (Login)

514/tcp: tcpwrapped

1099/tcp: GNU Classpath grmiregistry (Java RMI)

1524/tcp: Metasploitable root shell (Bindshell)

2049/tcp: NFS 2-4 (RPC)

2121/tcp: ProFTPD 1.3.1 (FTP)

3306/tcp: MySQL 5.0.51a-3ubuntu5 (MySQL)

5432/tcp: PostgreSQL DB 8.3.0 - 8.3.7 (PostgreSQL)

5900/tcp: VNC (protocol 3.3)

6000/tcp: Accesso negato (X11)

6667/tcp: UnrealIRCd (IRC)

8009/tcp: Apache Jserv (Protocol v1.3) (AJP13)

8180/tcp: Apache Tomcat/Coyote JSP engine 1.1 (HTTP)

56738/tcp: GNU Classpath grmiregistry (Java RMI)

Altre Informazioni:

Sistema Operativo: Unix, Linux (dalle informazioni fornite da Nmap)

Indirizzo MAC: 08:00:27:C6:F6:ED (Oracle VirtualBox virtual NIC)

La scansione di rilevamento delle versioni dei servizi ha fornito informazioni più dettagliate sui servizi in esecuzione sul dispositivo target, inclusi i nomi e le versioni dei servizi.