

## INDICE

INDICE.....	1
INTRODUZIONE ED OBIETTIVO.....	2

## NETCAT

VERIFICA CONFIGURAZIONE DI RETE.....	3
CONNESSIONE NETCAT.....	4
ESECUZIONE COMANDI REMOTI.....	5
RACCOLTA INFO SISTEMA.....	6
ESECUZIONE COMANDI REMOTI.....	7
REVERSE SHELL.....	8

## NMAP

RILEVAZIONE PORTE.....	9
SCANSIONE SYN.....	10
SCANSIONE.....	11

## INTRODUZIONE ED OBIETTIVO

**INTRODUZIONE:** il laboratorio ha l'obiettivo di verificare in modo chiaro e strutturato il funzionamento delle comunicazioni tra due macchine virtuali presenti nello stesso ambiente di rete.

Attraverso l'utilizzo di strumenti standard, l'esercizio permette di osservare come avviene una connessione tra due sistemi, come vengono scambiati i dati e quali risposte restituisce la macchina che riceve la richiesta.

Il lavoro svolto fornisce una visione pratica dei meccanismi di base che regolano l'interazione tra dispositivi collegati, consentendo di comprenderne il comportamento in condizioni controllate.

**OBIETTIVO:** verificare la comunicazione tra due macchine virtuali, stabilendo un collegamento diretto e osservando le risposte prodotte durante lo scambio di dati. Il fine è documentare in modo semplice e riproducibile i passaggi essenziali che caratterizzano l'interazione tra i due sistemi nella stessa rete.

## VERIFICA CONFIGURAZIONE DI RETE

```

KALI [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi

kali@kali: ~
Session  Actions  Edit  View  Help

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNK
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_co
   link/ether 08:00:27:1f:b7:23 brd ff:ff:ff:ff:ff:ff
   inet 192.168.32.100/24 brd 192.168.32.255 scope global nopr
       valid_lft forever preferred_lft forever
   inet 169.254.164.60/16 brd 169.254.255.255 scope global nop
       valid_lft forever preferred_lft forever
   inet6 fe80::b9ae:eb4:50fa:7b37/64 scope link
       valid_lft forever preferred_lft forever
   inet6 fe80::4374:263c:f825:8e33/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:83:88:d0
          inet addr:192.168.32.101  Bcast:192.168.32.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe83:88d0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:17  errors:0  dropped:0  overruns:0  frame:0
          TX packets:38  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1574 (1.5 KB)  TX bytes:4108 (4.0 KB)
          Base address:0xd020  Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:101  errors:0  dropped:0  overruns:0  frame:0
          TX packets:101  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:0
          RX bytes:23573 (23.0 KB)  TX bytes:23573 (23.0 KB)

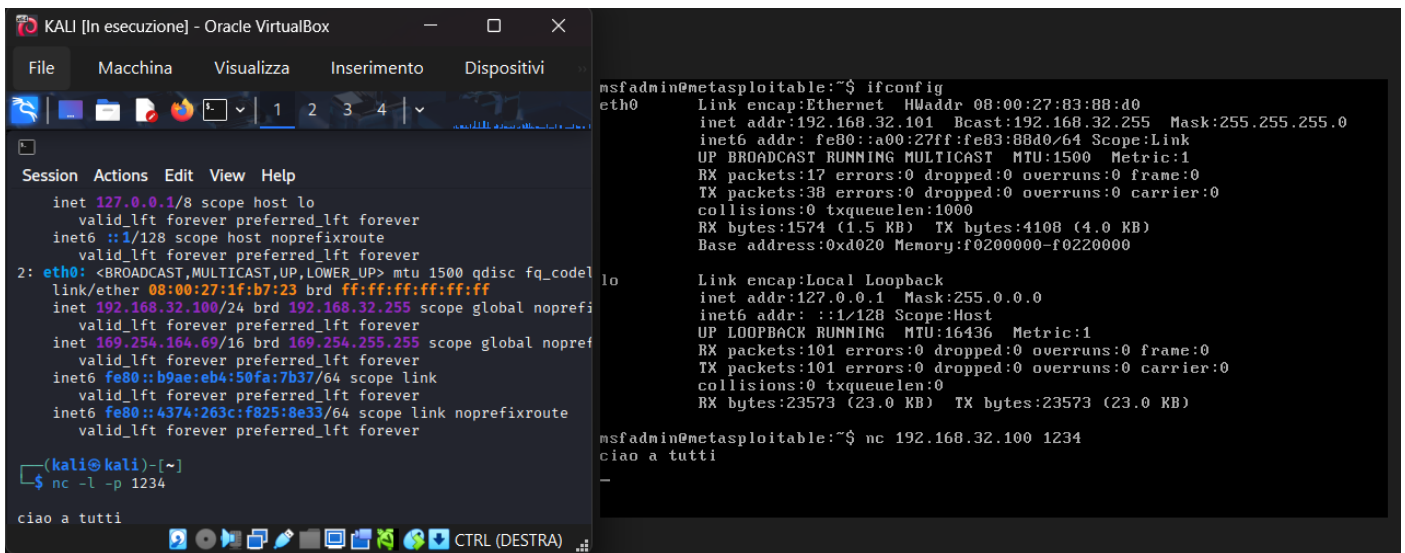
msfadmin@metasploitable:~$

```

Per avviare il laboratorio è stata verificata la configurazione di rete delle due macchine virtuali coinvolte.

Su *Kali Linux* è stato utilizzato il comando **ip a**, mentre sulla macchina remota è stato eseguito **ifconfig**, così da identificare indirizzi IP, interfacce attive e parametri assegnati. Entrambi i sistemi risultano correttamente collegati alla stessa rete e presentano indirizzi compatibili, condizione necessaria per permettere lo scambio di dati previsto nelle attività successive. Questa verifica preliminare garantisce che le due postazioni possano comunicare senza interferenze o problemi di connettività.

## CONNESSIONE NETCAT



```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:83:88:d0
          inet addr:192.168.32.101  Bcast:192.168.32.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe83:88d0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:17 errors:0 dropped:0 overruns:0 frame:0
          TX packets:38 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1574 (1.5 KB)  TX bytes:4108 (4.0 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:101 errors:0 dropped:0 overruns:0 frame:0
          TX packets:101 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:23573 (23.0 KB)  TX bytes:23573 (23.0 KB)

msfadmin@metasploitable:~$ nc 192.168.32.100 1234
ciao a tutti
-
```

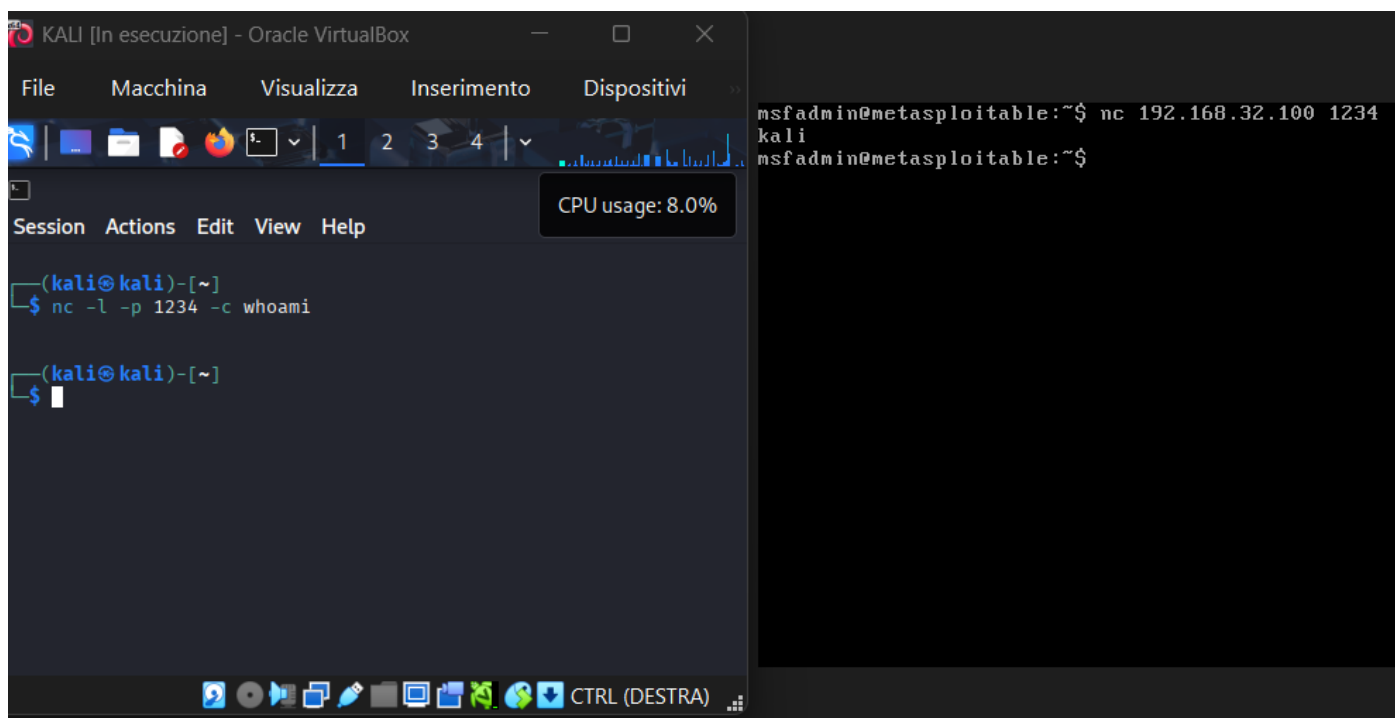
```
(kali@kali)-[~]
$ nc -l -p 1234
ciao a tutti
```

Dopo aver confermato che entrambe le macchine si trovano nella stessa rete, è stata avviata una prima comunicazione diretta tramite **Netcat**.

Sulla macchina Kali è stato aperto un **listener sulla porta 1234**, mentre dalla macchina remota è stata effettuata la connessione verso l'indirizzo di Kali utilizzando la stessa porta. Alla ricezione del messaggio di prova inviato dalla macchina remota, il *listener* ha risposto correttamente, confermando che la comunicazione tra i due sistemi è attiva e funziona come previsto.

Questo passaggio dimostra che il collegamento è stabilito correttamente e che i messaggi possono essere scambiati senza interruzioni.

## ESECUZIONE COMANDI REMOTI

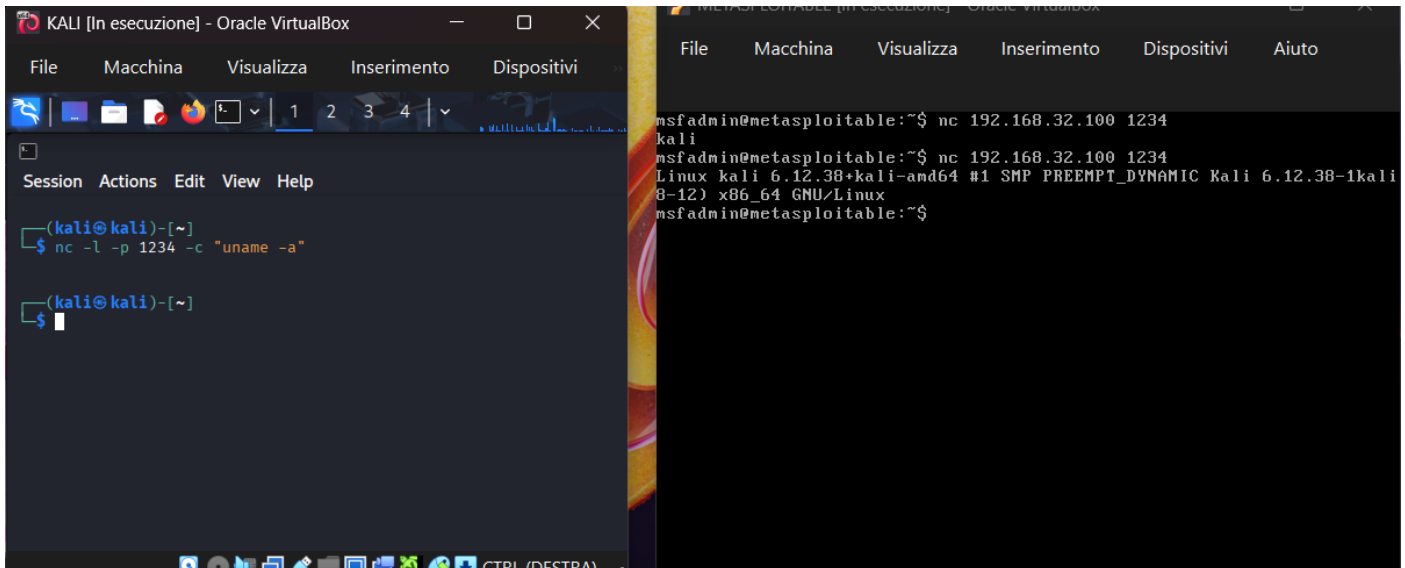


Dopo aver stabilito la connessione, è stato utilizzato Netcat per inviare comandi direttamente alla macchina remota.

In questo passaggio il listener di Kali è stato configurato per eseguire in automatico il comando **whoami** non appena la connessione veniva ricevuta; collegandosi alla porta indicata la macchina remota ha *restituito il proprio nome utente*, confermando che l'esecuzione dei comandi inviati da Kali avviene correttamente.

Ciò dimostra la piena operatività del canale stabilito e la sua capacità di eseguire istruzioni in modo immediato.

## RACCOLTA INFO SISTEMA



```
KALI [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi

Session Actions Edit View Help

(kali@kali)-[~]
$ nc -l -p 1234 -c "uname -a"

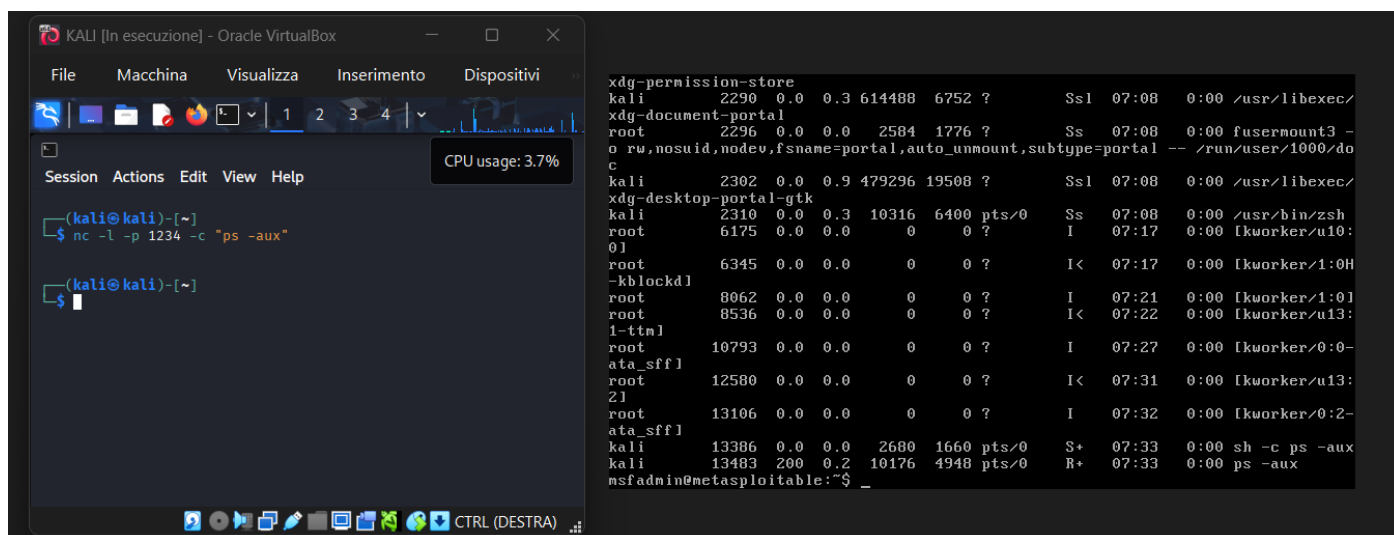
(kali@kali)-[~]
$

msfadmin@metasploitable:~$ nc 192.168.32.100 1234
kali
msfadmin@metasploitable:~$ nc 192.168.32.100 1234
Linux kali 6.12.38+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.38-1kali8-12) x86_64 GNU/Linux
msfadmin@metasploitable:~$
```

Proseguendo con la verifica della comunicazione, il listener di Kali è stato configurato per eseguire automaticamente il comando *uname -a* al momento della connessione.

Questo ha permesso di ottenere dalla macchina remota informazioni dettagliate sul sistema in uso, come versione del kernel e architettura; l'output restituito conferma che la connessione stabilita consente non solo l'invio di comandi, ma anche la raccolta immediata di dati utili sul sistema collegato, dimostrando la continuità e l'affidabilità dello scambio.

## ESECUZIONE COMANDI REMOTI



```
(kali@kali)~$ nc -l -p 1234 -c "ps -aux"

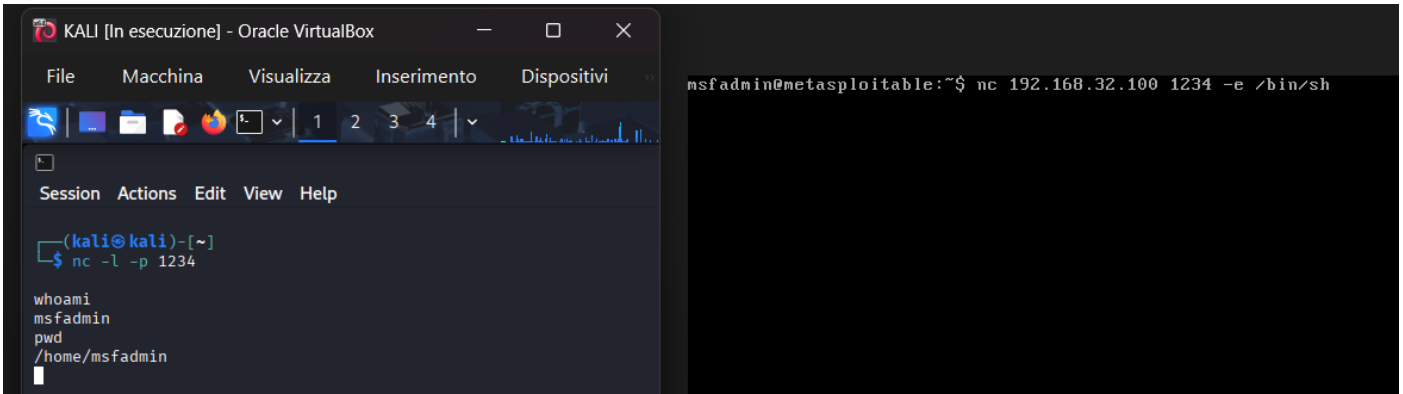
(kali@kali)~$

xdg-permission-store
kali      2290  0.0  0.3 614488 6752 ?        Ssl  07:08   0:00 /usr/libexec/
xdg-document-portal
root     2296  0.0  0.0   2584 1776 ?        Ss   07:08   0:00 fusermount3 -
o rw,nosuid,nodev,fsname=portal,auto_unmount,subtype=portal -- /run/user/1000/do
c
kali     2302  0.0  0.9 479296 19508 ?        Ssl  07:08   0:00 /usr/libexec/
xdg-desktop-portal-gtk
kali     2310  0.0  0.3  10316  6400 pts/0    Ss   07:08   0:00 /usr/bin/zsh
root     6175  0.0  0.0      0      0 ?        I    07:17   0:00 [kworker/u10:
0]
root     6345  0.0  0.0      0      0 ?        I<   07:17   0:00 [kworker/1:0H
-kblockd]
root     8062  0.0  0.0      0      0 ?        I    07:21   0:00 [kworker/1:0]
root     8536  0.0  0.0      0      0 ?        I<   07:22   0:00 [kworker/u13:
1-ttm]
root    10793  0.0  0.0      0      0 ?        I    07:27   0:00 [kworker/0:0-
ata_sff]
root    12580  0.0  0.0      0      0 ?        I<   07:31   0:00 [kworker/u13:
Z]
root    13106  0.0  0.0      0      0 ?        I    07:32   0:00 [kworker/0:2-
ata_sff]
kali    13386  0.0  0.0   2680  1660 pts/0    S+   07:33   0:00 sh -c ps -aux
kali    13483  200  0.2  10176  4948 pts/0    R+   07:33   0:00 ps -aux
msfadmin@metasploitable:~$ _
```

Durante questa fase è stato stabilito un collegamento diretto dalla macchina remota verso il listener in esecuzione su Kali. L'utilizzo del comando "nc -l -p 1234 -c "ps -aux" ha permesso di inviare, al momento della connessione, l'elenco completo dei processi attivi sul sistema Kali.

La macchina remota, collegandosi all'indirizzo e alla porta indicati, ha ricevuto immediatamente l'output del comando e lo ha visualizzato nel proprio terminale; ciò conferma la corretta esecuzione di comandi remoti e la piena funzionalità del canale di comunicazione stabilito tra le due macchine.

## REVERSE SHELL



In questa ultima fase del laboratorio è stato stabilito un collegamento inverso tra due macchine virtuali allo scopo di verificare il comportamento di un sistema quando riceve comandi eseguiti in remoto.

La macchina bersaglio ha aperto una connessione verso l'indirizzo indicato, mentre l'altra macchina era in ascolto sulla porta dedicata e pronta a ricevere l'interazione.

Una volta instaurato il collegamento è stato possibile inviare comandi direttamente alla macchina remota e osservarne le risposte in tempo reale, confermando la corretta instaurazione della sessione.

I test eseguiti hanno dimostrato che la comunicazione avviene in maniera stabile e che la macchina destinataria elabora correttamente le istruzioni ricevute.

La procedura ha permesso di evidenziare in modo concreto come un sistema possa essere controllato attraverso un canale di comunicazione inverso, offrendo una visione chiara delle modalità con cui due dispositivi interagiscono quando la connessione parte dal nodo remoto anziché da quello locale.



# NMAP

## RILEVAZIONE PORTE

```
(kali@kali)-[~]
$ nmap -sT 192.168.32.101

Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-25 07:41 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.32.101
Host is up (0.0052s latency).
Not shown: 977 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
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:83:88:D0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds

(kali@kali)-[~]
$
```

La scansione è stata eseguita per identificare i servizi attivi sulla macchina remota e verificare quale comportamento presentasse il sistema in risposta a una richiesta di connessione standard.

L'analisi effettuata consente di osservare in modo chiaro quali porte risultano aperte, quali servizi sono associati e come la macchina gestisce le comunicazioni in ingresso. Il risultato fornisce una panoramica immediata dell'esposizione del sistema all'interno della rete e permette di comprendere il livello di accessibilità dei vari servizi, offrendo così una base concreta per ulteriori verifiche o per successive attività di configurazione.

## SCANSIONE SYN

```
(kali@kali)-[~]
$ nmap -sS 192.168.32.101

Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-25 07:43 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.32.101
Host is up (0.00051s latency).
Not shown: 977 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
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:83:88:D0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.57 seconds

(kali@kali)-[~]
```

La scansione SYN del sistema remoto è stata eseguita per identificare rapidamente le **porte TCP aperte** senza stabilire una connessione completa.

Questa modalità di analisi permette di rilevare i servizi attivi inviando soltanto *pacchetti SYN* e valutando la risposta del sistema, riducendo l'impatto sulla macchina analizzata e il rischio di generare traffico eccessivo.

Il risultato mostra in modo immediato quali porte sono in ascolto e quali servizi risultano disponibili, offrendo una visione affidabile della superficie di comunicazione esposta dal dispositivo.

## SCANSIONE

```
(kali@kali)-[~]
$ nmap -A 192.168.32.101

Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-25 07:44 EST
nmap_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled
Nmap scan report for 192.168.32.101
Host is up (0.0021s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
ftp-syst:
STAT:
FTP server status:
  Connected to 192.168.32.100
  Logged in as ftp
  TYPE: ASCII
  No session bandwidth limit
  Session timeout in seconds is 300
  Control connection is plain text
  Data connections will be plain text
  vsFTPd 2.3.4 - secure, fast, stable
_End of status
ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
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
sslv2:
SSLv2 supported
ciphers:
  SSL2_DES_192_EDE3_CBC_WITH_MD5
  SSL2_RC4_128_WITH_MD5
  SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
  SSL2_DES_64_CBC_WITH_MD5
  SSL2_RC4_128_EXPORT40_WITH_MD5
  SSL2_RC2_128_CBC_WITH_MD5
ssl-date: 2025-11-25T12:45:12+00:00; -1s from scanner time.
smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY,
ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=O
Not valid before: 2010-03-17T14:07:45
Not valid after: 2010-04-16T14:07:45
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-title: Metasploitable2 - Linux
_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
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           40259/tcp  mountd
```

La scansione eseguita con Nmap ha permesso di ottenere una panoramica completa dei servizi attivi sulla macchina analizzata.

Questa modalità integra diverse tecniche di rilevazione, consentendo di identificare con precisione le porte aperte, le versioni dei servizi esposti e ulteriori informazioni utili per comprendere la superficie di comunicazione del sistema.

L'analisi ha evidenziato la presenza di numerosi servizi in esecuzione, confermando che la macchina ospita diversi componenti di rete, tra cui server FTP, SSH, HTTP, SMTP, database e altri servizi applicativi. La scansione fornisce quindi una mappatura dettagliata dello stato del sistema e rappresenta un passaggio fondamentale per documentarne le caratteristiche operative in un ambiente controllato.

