

# W10D4

con nmap controllo le porte aperte di metasploitable 2

```
(kali@kali)-[~/Desktop]
$ sudo nmap -sV --top-ports 10 192.168.1.17 -v

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-26 10:36 CEST
NSE: Loaded 46 scripts for scanning.
Initiating ARP Ping Scan at 10:36
Scanning 192.168.1.17 [1 port]
Completed ARP Ping Scan at 10:36, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:36
Completed Parallel DNS resolution of 1 host. at 10:36, 0.00s elapsed
Initiating SYN Stealth Scan at 10:36
Scanning Host-007.homenet.telecomitalia.it (192.168.1.17) [10 ports]
Discovered open port 80/tcp on 192.168.1.17
Discovered open port 445/tcp on 192.168.1.17
Discovered open port 25/tcp on 192.168.1.17
Discovered open port 22/tcp on 192.168.1.17
Discovered open port 23/tcp on 192.168.1.17
Discovered open port 21/tcp on 192.168.1.17
Discovered open port 139/tcp on 192.168.1.17
Completed SYN Stealth Scan at 10:36, 0.02s elapsed (10 total ports)
Initiating Service scan at 10:36
Scanning 7 services on Host-007.homenet.telecomitalia.it (192.168.1.17)
Completed Service scan at 10:36, 6.10s elapsed (7 services on 1 host)
NSE: Script scanning 192.168.1.17.
Initiating NSE at 10:36
Completed NSE at 10:36, 0.03s elapsed
Initiating NSE at 10:36
Completed NSE at 10:36, 0.02s elapsed
Nmap scan report for Host-007.homenet.telecomitalia.it (192.168.1.17)
Host is up (0.00074s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet   Linux telnetd
25/tcp    open  smtp     Postfix smtpd
80/tcp    open  http     Apache httpd 2.2.8 ((Ubuntu) DAV/2)
110/tcp   closed pop3
139/tcp   open  tcpwrapped
443/tcp   closed https
445/tcp   open  tcpwrapped
3389/tcp  closed ms-wbt-server
MAC Address: 08:00:27:B3:55:73 (Oracle VirtualBox virtual NIC)
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.48 seconds
Raw packets sent: 11 (468B) | Rcvd: 11 (456B)
```

faccio partire metasploit con il comando **msfconsole**

```

msf6 > msfconsole
Metasploit tip: View all productivity tips with the tips command
/usr/share/nmap/scripts/tls-ticketbleed.nse
/usr/share/nmap/scripts/tor-consensus-checker.nse
/usr/share/nmap/scripts/traceroute-geolocation.nse
/ it looks like you're trying to run a \
\ module /usr/share/nmap/scripts/tso-enum.nse /
/usr/share/nmap/scripts/very.nse
/usr/share/nmap/scripts/unittest.nse
/usr/share/nmap/scripts/unusual-port.nse
/usr/share/nmap/scripts/upnp-info.nse
/usr/share/nmap/scripts/uptime-agent-info.nse
/usr/share/nmap/scripts/url-sharf.nse
@ @ /usr/share/nmap/scripts/ventrilo-info.nse
/usr/share/nmap/scripts/versant-info.nse
// // /usr/share/nmap/scripts/vmauthd-brute.nse
// // /usr/share/nmap/scripts/vmware-version.nse
// \ /usr/share/nmap/scripts/vnc-brute.nse
\ \ /usr/share/nmap/scripts/vnc-info.nse
\ \ /usr/share/nmap/scripts/vnc-title.nse
/usr/share/nmap/scripts/voldemort-info.nse
usr = [ metasploit v6.4.1-dev num.nse ]
+ -- -- [ 2407 exploits - 1239 auxiliary - 422 post ]
+ -- -- [ 1468 payloads - 47 encoders - 11 nops ]
+ -- -- [ 9 evasion /usr/share/nmap/scripts/wdb-version.nse ]
/usr/share/nmap/scripts/weblogic-t3-info.nse
Metasploit Documentation: https://docs.metasploit.com/
msf6 >

```

con il comando **grep scanner use smtp** mi filtra gli exploit riguardanti il protocollo smtp

```

msf6 > grep scanner use smtp
4 auxiliary/scanner/http/gavazzi_em_login_loot . normal
No Carlo Gavazzi Energy Meters - Login Brute Force, Extract Info and Dump Plant Database
37 auxiliary/scanner/smtp/smtp_version ARP 62 who has 192.168.1.8? Tell 192.168.1.1 normal 1.128
No SMTP Banner Grabber ARP 62 who has 192.168.1.8? Tell 192.168.1.1 normal 1.1
38 auxiliary/scanner/smtp/smtp_ntlm_domain ARP 62 who has 192.168.1.12? Tell 192.168.1.1 normal 1.1
No SMTP NTLM Domain Extraction IGMPv2 62 Membership Query, general
39 auxiliary/scanner/smtp/smtp_relay NBNS 94 Name query NB WORKGROUP<id> normal
No SMTP Open Relay Detection 355 NBNS 112 Release NB MACBOOKAIR-2437<88>
41 auxiliary/scanner/smtp/smtp_enum NBNS 112 Release NB MACBOOKAIR-2437<2> normal
No SMTP User Enumeration Utility NBNS 112 Release NB WORKGROUP<88>
66 auxiliary/scanner/http/wp_easy_wp_smtp ARP 62 who has 192.168.1.11? Tell 192.168.1.18 normal 1.18
No WordPress Easy WP SMTP Password Reset

```

scelgo lo script che la enumerazione smtp con il comando **use 41**

```

msf6 > grep scanner use smtp
4 auxiliary/scanner/http/gavazzi_em_login_loot . normal
No Carlo Gavazzi Energy Meters - Login Brute Force, Extract Info and Dump Plant Database
37 auxiliary/scanner/smtp/smtp_version ARP 62 who has 192.168.1.8? Tell 192.168.1.1 normal 1.128
No SMTP Banner Grabber ARP 62 who has 192.168.1.8? Tell 192.168.1.1 normal 1.1
38 auxiliary/scanner/smtp/smtp_ntlm_domain ARP 62 who has 192.168.1.12? Tell 192.168.1.1 normal 1.1
No SMTP NTLM Domain Extraction IGMPv2 62 Membership Query, general
39 auxiliary/scanner/smtp/smtp_relay NBNS 94 Name query NB WORKGROUP<id> normal
No SMTP Open Relay Detection 355 NBNS 112 Release NB MACBOOKAIR-2437<88>
41 auxiliary/scanner/smtp/smtp_enum NBNS 112 Release NB MACBOOKAIR-2437<2> normal
No SMTP User Enumeration Utility NBNS 112 Release NB WORKGROUP<88>
66 auxiliary/scanner/http/wp_easy_wp_smtp ARP 62 who has 192.168.1.11? Tell 192.168.1.18 normal 1.18
No WordPress Easy WP SMTP Password Reset

msf6 > use 41
[-] Unknown command: 41. Run the help command for more details.
msf6 > use 41
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):

  Name      Current Setting      Required  Description
  ----      -
  RHOSTS    yes                  The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     25                  The target port (TCP)
  THREADS   1                  The number of concurrent threads (max one per host)
  UNIXONLY  true               Skip Microsoft bannered servers when testing unix users
  USER_FILE /usr/share/metasploit-framework/data/wordlists/unix_users.txt yes The file that contains a list of probable users accounts.

```

set rhost seguito dall'ip di metaexploitable e poi lancio lo script exploit, il quale mi restituirà gli user presenti sulla macchina attaccata, trovati grazie al file unix\_users.txt

```
msf6 auxiliary(scanner/smtp/smtp_enum) > rhosts 192.168.1.18
[-] Unknown command: rhosts. Did you mean hosts? Run the help command for more details.
msf6 auxiliary(scanner/smtp/smtp_enum) > set rhosts 192.168.1.18
rhosts => 192.168.1.18
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum): local_length 100
Name      Current Setting  Required  Description
-----
RHOSTS    192.168.1.18    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     25              yes       The target port (TCP)
THREADS   1              yes       The number of concurrent threads (max one per host)
UNIXONLY  true            yes       Skip Microsoft bannered servers when testing unix users
USER_FILE /usr/share/metasploit-framework/data/wordlists/unix_users.txt yes       The file that contains a list of probable users accounts.

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smtp/smtp_enum) > exploit

[*] 192.168.1.18:25 - 192.168.1.18:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[*] 192.168.1.18:25 - 192.168.1.18:25 Users found: , backup, bin, daemon, distccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysql, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, uucp, www-data
[*] 192.168.1.18:25 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) > telnet 192.168.1.18 25
[-] Unknown command: telnet192.168.1.18. Run the help command for more details.
msf6 auxiliary(scanner/smtp/smtp_enum) > telnet 192.168.1.18 25
[*] exec: telnet 192.168.1.18 25
```

faccio **banner grabbing** con telnet con il comando VRFY

```
Trying 192.168.1.18...
Connected to 192.168.1.18. 18, 255: 192.168.1.18
Escape character is '^]'. 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY backup
252 2.0.0 backup
VRFY sys
252 2.0.0 sys
```