## ESERCITAZIONE CON TOOL DI KALI LINUX

#HHAP

NMAP È UNO STRUMENTO DI NETWORK EXPLORATION E AUDITING. PUÒ SCANSIONARE SIA RETI DI GRANDI DIMENSIONI CHE SINGOLI HOST, DETERMINANDO QUALI HOST SONO DISPONIBILI SU UNA RETE E CHE SERVIZI OFFRONO (NOME APPLICAZIONE E VERSIONE), EVENTUALMENTE VULNERABILI. DETERMINA INOLTRE CHE SISTEMA OPERATIVO E CHE TIPO DI FIREWALL E PACKET FILTERS SONO IN USO.

PER PRENDERE CONFIDENZA CON IL TOOL L'ESERCIZIO RICHIE-DE DI SCANSIONARE DA KALI LINUX (MACCHINA ATTACCANTE) LE PORTE WELL-KNOWN (1-1023) DISPONIBILI SU METASPLOI-TABLE (MACCHINA VITTIMA) IN TRE DIVERSE MODALITÀ:

- 1) LA SCANSIONE "SYN" CON IL COMANDO nmop -sS
  192.168.50.101 -p 1-1024. È LA MENO INVASIVA E RUMOROSA DI TUTTE, IN QUANTO, UNA VOLTA APPURATO CHE UNA
  PORTA È APERTA, NON CONCLUDE IL TERZO PASSAGGIO
  DEL THREE-WAY-HANDSHAKE CHIUDENDO LA COMUNICAZIONE CON RST (RESET). QUESTO EVITA L'OVERLOAD DATO
  DALLA CREAZIONE DEL CANALE STESSO.
- 2) LA SCANZIONE "TCP" CON IL COMANDO nmop -sT 192.168.50.101 -p 1-1024. È UN METODO PIÙ INVASIVO, CHE PER STABILIRE SE UNA PORTA È APERTA E RECUPERARE INFORMAZIONI SUL SERVIZIO IN ASCOLTO, COMPLETA IL THREE-WAY-HANDSHAKE E STABILISCE DI FATTO UN CANALE.
- 3) LA SCANSIONE CON LO SWITCH "-A" CON IL COMANDO nmop -A 192.168.50.101 -p 1-1024. È DI FATTO LA SCANSIO-NE PIÙ INVASIVA E PIÙ LENTA, MA PERMETTE DI OTTENERE MOLTI PIÙ DATI

INIZIAMO CON L'HOST DISCOVERY - TECNICA PER CAPIRE SE UN HOST È ATTIVO E QUINDI RAGGIUNGIBILE SU UNA RETE. COMANDO PER PING SENZA SCAN: nmap -sn 192.168.50.101 DOPODICHE PROCEDIAMO CON LE TRE MODALITÀ DI SCANSIONE DELLE PORTE WELL-KNOWN E ANALIZZIAMO LE DIFFERENZE CATTURANDO I PACCHETTI CON WIRESHARK

```
[/home/django]
      nmap -sn 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-04 16:44 EST
Nmap scan report for 192.168.50.101
Host is up (0.00037s latency).
MAC Address: 08:00:27:DC:03:D4 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.11 seconds
     (<mark>root⊚kali</mark>)-[/home/django]
nmap -sS 192.168.50.101 -p 0-1024
Nmap scan report for 192.168.50.101 Pt 0-1024

Nmap scan report for 192.168.50.101

Host is up (0.00014s latency).

Not shown: 1013 closed tcp ports (reset)
                                                            ) at 2024-01-04 16:48 EST
PORT
            STATE SERVICE open ftp
21/tcp open
22/tcp
23/tcp
           open
open
                     ssh
                      telnet
                     smtp
25/tcp
           open
                                                PORTE APERTE = OPEN
53/tcp open
80/tcp open
                    domain
http
                                                 nº 12, CON SERVIZIO INDICATO
                     rpcbind
111/tcp open
139/tcp open
445/tcp open
                     netbios-ssn
                     microsoft-ds
512/tcp open
513/tcp open
                      exec
                      login
514/tcp open
                      shell
MAC Address: 08:00:27:DC:03:D4 (Oracle VirtualBox virtual NIC)
```

```
-[/home/django]
Nap scan report for 192.168.50.101

Host is up (0.00068s latency).

Not shown: 1013 closed tcp ports (conn-refused)
                                                                                                                                                                             ) at 2024-01-04 17:07 EST
                                 STATE SERVICE
PORT
                                                               ftp
                                 open
22/tcp
23/tcp
                                open
open
                                                              ssh
                                                               telnet
25/tcp open
                                                           smtp
                                                          domain
53/tcp open
                                                                                                                                            PORTE APERTE = OPEN
                                                               http
80/tcp
                                    open
                                                         rpcbind
                                                                                                                                           nº 12, CON SERVIZIO INDICATO
 111/tcp open
139/tcp open netbios-ssn
445/tcp open
512/tcp open
513/tcp open
                                                               exec
                                                             login
514/tcp open
                                                               shell
MAC Address: 08:00:27:DC:03:D4 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.26 seconds
                                                                                                                    root@kali: /home/diango
   File Actions Edit View Help
 (roor 0 koll)-[/home/django]
In mmap -A 192.168.50.101 -p 0-1024
Starting Rmap r-94 (n thtps://mmap.org ) at 2024-01-04
Nmap scan report for 192.168.50.101
Host is up (0.0013s latency).
Not shown: 1013 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)
I ftp-syst:
STAT:
| FTP server statue.
                                                                                                      rg ) at 2024-01-04 1/:1/ ESI
    SSLVZ SUPPORTER

SSL2_DES_64_CBC_WITH_MD5

SSL2_DES_102_EDE3_CBC_WITH_MD5

SSL2_RC4_128_WITH_MD5

SSL2_RC4_128_EXPORT40_WITH_MD5

SSL2_RC2_128_CBC_WITH_MD5

SSL2_RC2_128_CBC_WITH_MD5

SSL2_RC2_128_CBC_EXPORT40_WITH_MD5

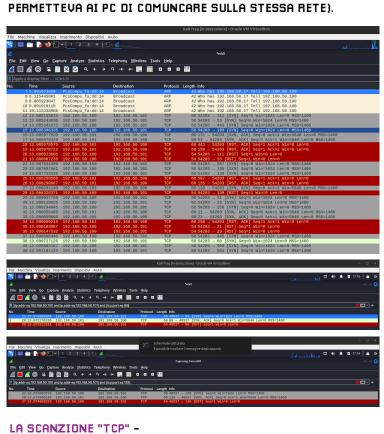
CCP open domain ISC_BIND 9.4.2_
  111/tcp open rpcbind 2 (RFC #100000) | rpccinor | rpcc
```

OP RTT ADDRESS 1.33 ms 192.168.50.101 5 and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . nap done: 1 IP address (1 host up) scanned in 98.47 seconds

## LA SCANSIONE "SYN" -

CON IL COMANDO nmop -sS 192.168.50.101 -p 1-1024.

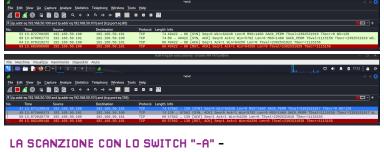
LA MACCHINA KALI LINUX MANDA UN PACCHETTO SYN A META-SPLOITABLE CHE RISPONDERÀ CON SYN-ACK IN CASO DI PORTA APERTA, AL CHE KALI INTERROMPERÀ LA COMUNICAZIONE CON RST (RESET) NON CPLETANDO IL 3-WAY-HANDSHAKE. VEDIAMO L'ESEMPIO SULLE PORTE WELL-KNOWN 80 (SERVER WEB HTTP) E 139 (PROTOCOLLO DI RETE SMB; SUI SISTEMI WINDOWS STAVA SU UN VECCHIO LIVELLO DI TRASPORTO DATI NETBIOS CHE



## CON IL COMANDO nmop -sT 192.168.50.101 -p 1-1024.

LA MACCHINA KALI LINUX MANDA UN PACCHETTO SYN A META-SPLOITABLE CHE RISPONDERÀ CON SYN-ACK IN CASO DI PORTA

APERTA, AL CHE KALI RISPONDERÀ STABILENDO UN CANALE E POI INTERROMPERÀ LA COMUNICAZIONE CON RST (RESET).



## CON IL COMANDO nmop -A 192.168.50.101 -p 1-1024. LA MACCHINA KALI LINUX MANDA UN PACCHETTO SYN A META-

SPLOITABLE CHE RISPONDERÀ CON SYN-ACK IN CASO DI PORTA

APERTA, AL CHE KALI RISPONDERÀ STABILENDO UN CANALE E PROCEDERÀ A RECUPERARE MOLTI DATI, COME SI VEDE NELLO SCREENSHOT SOTTOSTANTE DEL TRAFFICO WIRESHARK, CHE SI POSSONO CONSULTABE

