

Oracle

# Recolección de info

Nmap y otras herramientas

Armando Flores  
6-8-2023

Dirección IP de equipos:

Para esta primera practica lo que realizo es un escaneo en mi propia red para ver si hay otros equipos conectados, pero como es una red privada en la que esta la maquina virtual no veo otra mas que mi propia máquina virtual y el host mismo, en la siguiente imagen podemos ver como se realizo el escaneo

```
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    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
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 52:71:fa:a9:7a:35 brd ff:ff:ff:ff:ff:ff permaddr 08:00:27:22:46:4f
    inet6 fe80::9f1:f4c6:392b:b118/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: bridge0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether e6:3c:08:95:1b:04 brd ff:ff:ff:ff:ff:ff

(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    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
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 52:71:fa:a9:7a:35 brd ff:ff:ff:ff:ff:ff permaddr 08:00:27:22:46:4f
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
        valid_lft 86399sec preferred_lft 86399sec
    inet6 fe80::9f1:f4c6:392b:b118/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: bridge0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether e6:3c:08:95:1b:04 brd ff:ff:ff:ff:ff:ff

(kali㉿kali)-[~]
$ nmap -v -sn 10.0.2.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-06-04 23:20 EDT
Initiating Ping Scan at 23:20
Scanning 256 hosts [2 ports/host]
Completed Ping Scan at 23:20, 3.31s elapsed (256 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:20
Completed Parallel DNS resolution of 1 host. at 23:20, 0.01s elapsed
Nmap scan report for 10.0.2.0 [host down]
Nmap scan report for 10.0.2.1 [host down]
Nmap scan report for 10.0.2.2 [host down]
Nmap scan report for 10.0.2.3 [host down]
Nmap scan report for 10.0.2.4 [host down]
Nmap scan report for 10.0.2.5 [host down]
Nmap scan report for 10.0.2.6 [host down]
Nmap scan report for 10.0.2.7 [host down]
Nmap scan report for 10.0.2.8 [host down]
Nmap scan report for 10.0.2.9 [host down]
Nmap scan report for 10.0.2.10 [host down]
Nmap scan report for 10.0.2.11 [host down]
Nmap scan report for 10.0.2.12 [host down]
Nmap scan report for 10.0.2.13 [host down]
Nmap scan report for 10.0.2.14 [host down]
Nmap scan report for 10.0.2.15
Host is up (0.00045s latency).
```

Después podemos hacer un escaneo más avanzado para determinar los puertos que se tiene abiertos y con cuales servicios.

```

(kali㉿kali)-[~]
$ nmap -sV -p- -Pn 10.10.11.214
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-05 16:25 EDT
Nmap scan report for 10.10.11.214
Host is up (0.077s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
50051/tcp open  unknown

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port50051-TCP:V=7.93%I=7%D=6/5%Time=647E4535%P=x86_64-pc-linux-gnu%r(NU
SF:LL,2E,"\\0\\0\\x18\\x04\\0\\0\\0\\0\\0\\0\\x04\\0\\?\\xff\\xff\\0\\x05\\0\\?\\xff\\xff\\0\\x06
SF:\\0\\0\\x20\\0\\xfe\\x03\\0\\0\\0\\0\\0\\0\\x04\\x08\\0\\0\\0\\0\\0\\0\\?\\0\\0")%r(GenericI
SF:ines,2E,"\\0\\0\\x18\\x04\\0\\0\\0\\0\\0\\0\\0\\04\\0\\?\\xff\\xff\\0\\x05\\0\\?\\xff\\xff\\0\\x
SF:06\\0\\0\\x20\\0\\xfe\\x03\\0\\0\\0\\0\\0\\0\\x04\\x08\\0\\0\\0\\0\\0\\0\\?\\0\\0")%r(GetReq
SF:uest,2E,"\\0\\0\\x18\\x04\\0\\0\\0\\0\\0\\0\\x04\\0\\?\\xff\\xff\\0\\x05\\0\\?\\xff\\xff\\0\\x
SF:06\\0\\0\\x20\\0\\xfe\\x03\\0\\0\\0\\0\\0\\0\\x04\\x08\\0\\0\\0\\0\\0\\0\\?\\0\\0")%r(HTTPOp
SF:tions,2E,"\\0\\0\\x18\\x04\\0\\0\\0\\0\\0\\0\\x04\\0\\?\\xff\\xff\\0\\x05\\0\\?\\xff\\xff\\0\\
SF:x06\\0\\0\\x20\\0\\xfe\\x03\\0\\0\\0\\0\\0\\0\\x04\\x08\\0\\0\\0\\0\\0\\0\\?\\0\\0")%r(RTSPR
SF:equest,2E,"\\0\\0\\x18\\x04\\0\\0\\0\\0\\0\\0\\x04\\0\\?\\xff\\xff\\0\\x05\\0\\?\\xff\\xff\\0\\
SF:x06\\0\\0\\x20\\0\\xfe\\x03\\0\\0\\0\\0\\0\\0\\x04\\x08\\0\\0\\0\\0\\0\\0\\?\\0\\0")%r(RPCC
SF:heck,2E,"\\0\\0\\x18\\x04\\0\\0\\0\\0\\0\\0\\x04\\0\\?\\xff\\xff\\0\\x05\\0\\?\\xff\\xff\\0\\x
SF:06\\0\\0\\x20\\0\\xfe\\x03\\0\\0\\0\\0\\0\\0\\x04\\x08\\0\\0\\0\\0\\0\\0\\?\\0\\0")%r(DNSVer
SF:sionBindReqTCP,2E,"\\0\\0\\x18\\x04\\0\\0\\0\\0\\0\\0\\x04\\0\\?\\xff\\xff\\0\\x05\\0\\?\\x
SF:ff\\xff\\0\\x06\\0\\0\\x20\\0\\xfe\\x03\\0\\0\\0\\0\\0\\0\\x04\\x08\\0\\0\\0\\0\\0\\0\\?\\0\\0"
SF:)%r(DNSStatusRequestTCP,2E,"\\0\\0\\x18\\x04\\0\\0\\0\\0\\0\\0\\x04\\0\\?\\xff\\xff\\0\\
SF:x05\\0\\?\\xff\\xff\\0\\x06\\0\\0\\x20\\0\\xfe\\x03\\0\\0\\0\\0\\0\\0\\x04\\x08\\0\\0\\0\\0\\
SF:\\0\\?\\0\\0")%r(Hello,2E,"\\0\\0\\x18\\x04\\0\\0\\0\\0\\0\\0\\x04\\0\\?\\xff\\xff\\0\\x05\\0\\
SF:?:\\xff\\xff\\0\\x06\\0\\0\\x20\\0\\xfe\\x03\\0\\0\\0\\0\\0\\0\\x04\\x08\\0\\0\\0\\0\\0\\0\\?\\0
SF:\\0")%r(SSLSessionReq,2E,"\\0\\0\\x18\\x04\\0\\0\\0\\0\\0\\0\\x04\\0\\?\\xff\\xff\\0\\x05
SF:\\0\\?\\xff\\xff\\0\\x06\\0\\0\\x20\\0\\xfe\\x03\\0\\0\\0\\0\\0\\0\\x04\\x08\\0\\0\\0\\0\\0\\0\\
SF:?:\\0\\0")%r(TerminalServerCookie,2E,"\\0\\0\\x18\\x04\\0\\0\\0\\0\\0\\0\\x04\\0\\?\\xff
SF:\\xff\\0\\x05\\0\\?\\xff\\xff\\0\\x06\\0\\0\\x20\\0\\xfe\\x03\\0\\0\\0\\0\\0\\0\\x04\\x08\\0\\
SF:0\\0\\0\\0\\?\\0\\0")%r(TLSSessionReq,2E,"\\0\\0\\x18\\x04\\0\\0\\0\\0\\0\\0\\x04\\0\\?\\
SF:ff\\xff\\0\\x05\\0\\?\\xff\\xff\\0\\x06\\0\\0\\x20\\0\\xfe\\x03\\0\\0\\0\\0\\0\\0\\x04\\x08
SF:\\0\\0\\0\\0\\0\\0\\?\\0\\0")%r(Kerberos,2E,"\\0\\0\\x18\\x04\\0\\0\\0\\0\\0\\0\\x04\\0\\?\\xf
SF:f\\xff\\0\\x05\\0\\?\\xff\\xff\\0\\x06\\0\\0\\x20\\0\\xfe\\x03\\0\\0\\0\\0\\0\\0\\x04\\x08\\0\\
SF:\\0\\0\\0\\0\\0\\0\\?\\0\\0")%r(SMBProgNeg,2E,"\\0\\0\\x18\\x04\\0\\0\\0\\0\\0\\0\\x04\\0\\?\\xf
SF:f\\xff\\0\\x05\\0\\?\\xff\\xff\\0\\x06\\0\\0\\x20\\0\\xfe\\x03\\0\\0\\0\\0\\0\\0\\x04\\x08\\0\\
SF:\\0\\0\\0\\0\\0\\0\\?\\0\\0")%r(X11Probe,2E,"\\0\\0\\x18\\x04\\0\\0\\0\\0\\0\\0\\x04\\0\\?\\xff\\
SF:ff\\0\\x05\\0\\?\\xff\\xff\\0\\x06\\0\\0\\x20\\0\\xfe\\x03\\0\\0\\0\\0\\0\\0\\x04\\x08\\0\\0\\
SF:\\0\\0\\0\\0\\?\\0\\0");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 118.42 seconds

```

En este caso este escaneo lo hice a una maquina de prueba de la plataforma hackthebox ya que hicimos varias pruebas con maquinas virtuales pero en este caso decidí esta porque tenía un puerto abierto que no es de los puertos comunes.