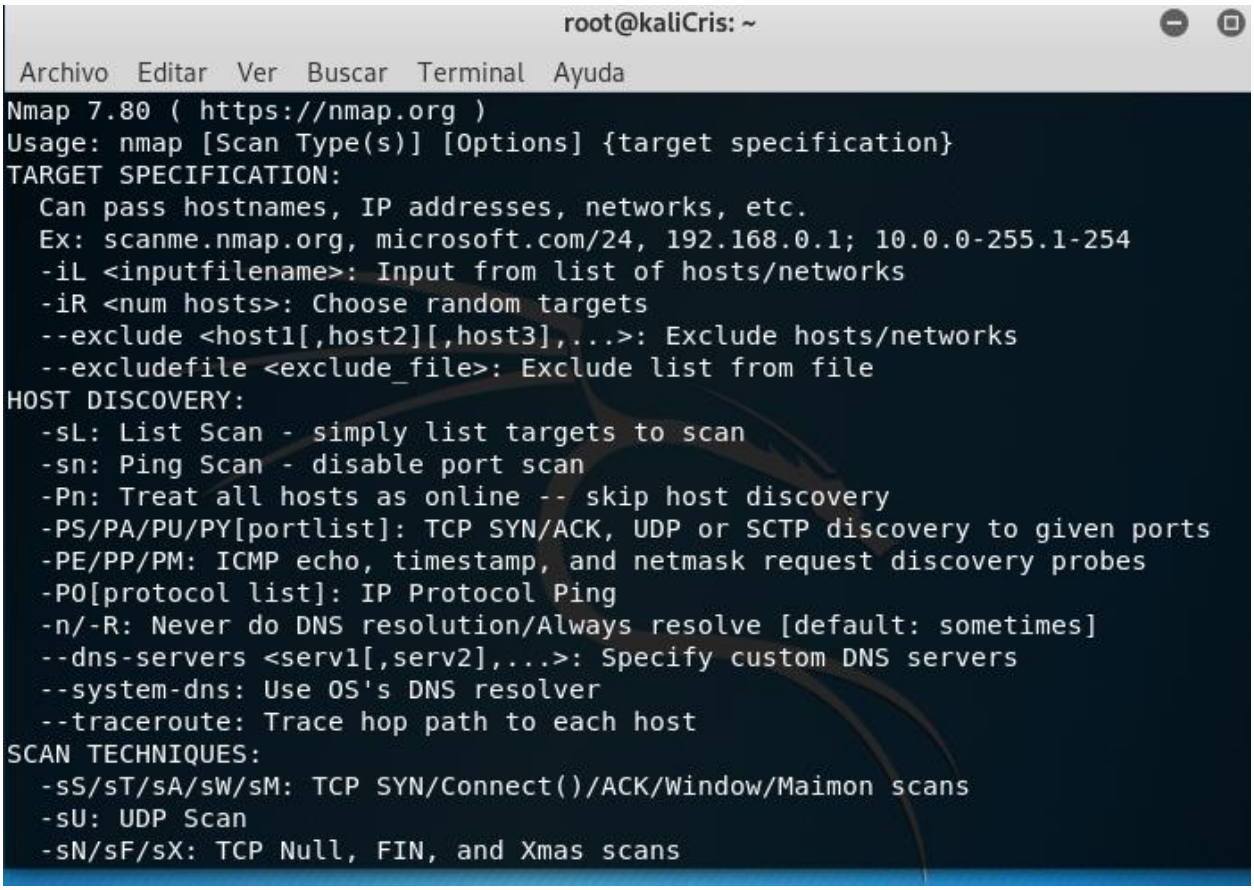
Kali-linux.Herramientas de kali-linux

Ejemplo 1:Nmap

Network Mapper es una herramienta gratuita y de código abierto utilizada por los administradores del sistema para descubrir redes y auditar tu seguridad.

Es rápido en su funcionamiento, está bien documentado, cuenta con una interfaz gráfica, admite transferencia de datos, inventario de red, etc.



Algunos comandos útiles de Nmap:

Los desarrolladores ponen a nuestra disposición varios servidores que permiten ser escaneados.

- scanme.nmap.org
- analizame2.nmap.org

Escaneo de puertos TCP básico

Esta opción analiza y muestra todos los puertos *TCP* (Transmission Control Protocol) reservados actualmente en la máquina destino.

```
root@kaliCris:~# nmap -v scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-23 21:39 CEST
Initiating Ping Scan at 21:39
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 21:39, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:39
Completed Parallel DNS resolution of 1 host. at 21:39, 0.03s elapsed
Initiating SYN Stealth Scan at 21:39
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 25/tcp on 45.33.32.156
Discovered open port 143/tcp on 45.33.32.156
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 993/tcp on 45.33.32.156
Discovered open port 110/tcp on 45.33.32.156
Discovered open port 995/tcp on 45.33.32.156
Discovered open port 587/tcp on 45.33.32.156
Discovered open port 80/tcp on 45.33.32.156
Increasing send delay for 45.33.32.156 from 0 to 5 due to 11 out of 24 d
robes since last increase.
Discovered open port 119/tcp on 45.33.32.156
```

La opción –v (verbose) es para hacer un análisis al detalle.

Escanear un rango de IP's

Escanear un rango de IPs nos resultaría útil en casos de un posible ataque de red. si queremos intentar averiguar donde tiene lugar. También ahorraría tiempo al rastrear este tipo de ataques.