Msfconsole

Scanning using Metasploitable in Kali

`sudo su`

`systemctl postgresql start`

`msfconsole`

`db_status`

`nmap -Pn -sS -A -oX Test [IP ADDRESS]`

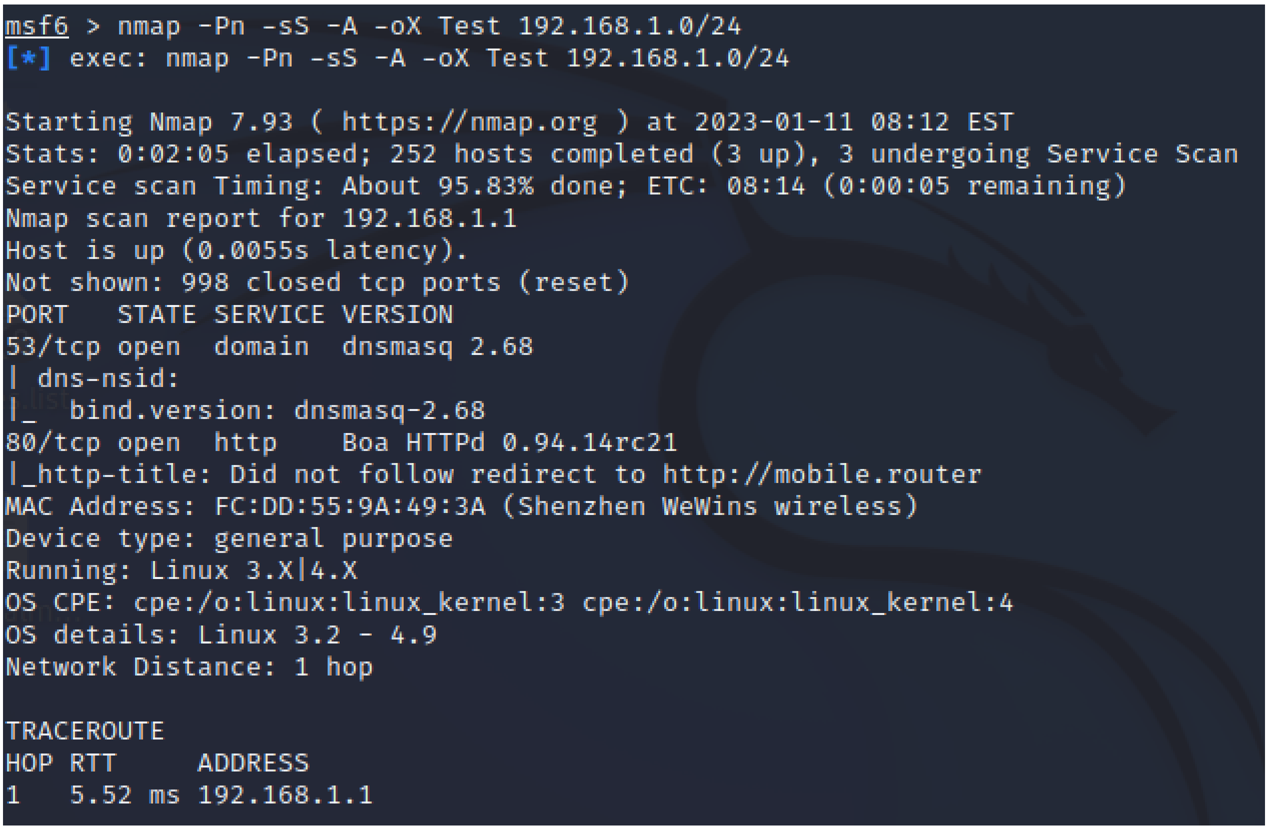
Where:

`-Pn` - Treat all hosts as online -- skip host discovery

`-sS` - TCP SYN

`-A` - Enable OS detection, version detection, script scanning, and traceroute

`-oX` - output is XML



```
msf6 > nmap -Pn -sS -A -oX Test 192.168.1.0/24
[*] exec: nmap -Pn -sS -A -oX Test 192.168.1.0/24

Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-11 08:12 EST
Stats: 0:02:05 elapsed; 252 hosts completed (3 up), 3 undergoing Service Scan
Service scan Timing: About 95.83% done; ETC: 08:14 (0:00:05 remaining)
Nmap scan report for 192.168.1.1
Host is up (0.0055s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
53/tcp open  domain  dnsmasq 2.68
| dns-nsid:
|_  bind.version: dnsmasq-2.68
80/tcp open  http    Boa HTTPd 0.94.14rc21
|_http-title: Did not follow redirect to http://mobile.router
MAC Address: FC:DD:55:9A:49:3A (Shenzhen WeWins wireless)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   5.52 ms 192.168.1.1
```

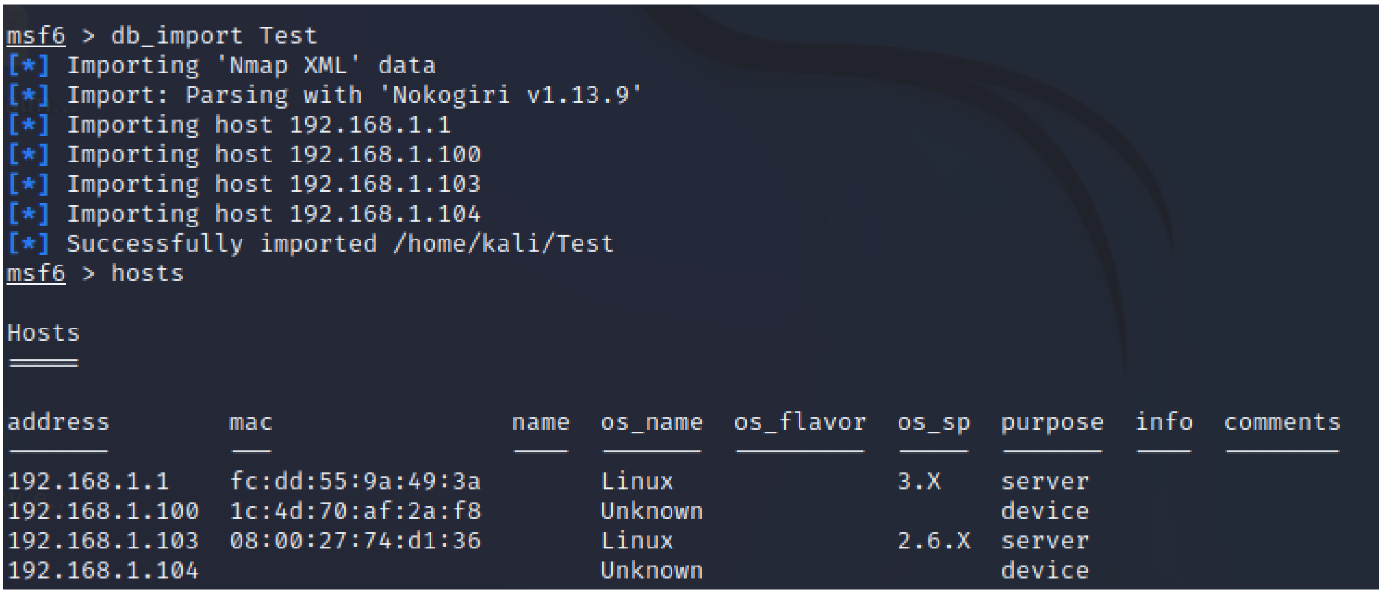
`db_import Test` -> imports Nmap results to the database

`hosts` -> to list active hosts based on scan

`services` -> to view services running on hosts

`search portscan`

`use auxiliary/scanner/portscan/syn` -> to use msfconsole's port scanner



```
msf6 > db_import Test
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.13.9'
[*] Importing host 192.168.1.1
[*] Importing host 192.168.1.100
[*] Importing host 192.168.1.103
[*] Importing host 192.168.1.104
[*] Successfully imported /home/kali/Test
msf6 > hosts

Hosts
=====

address        mac                name  os_name  os_flavor  os_sp  purpose  info  comments
-------        ---                ----  -------  ---------  -----  -------  ----  --------
192.168.1.1    fc:dd:55:9a:49:3a        Linux               3.X    server
192.168.1.100  1c:4d:70:af:2a:f8        Unknown                    device
192.168.1.103  08:00:27:74:d1:36        Linux               2.6.X  server
192.168.1.104                           Unknown                    device
```