Project Title:

Network Port Scanning & Security Analysis using Nmap

PROJECT OVERVIEW

Objective

Identify open ports and services on a target system and analyze potential security risks.

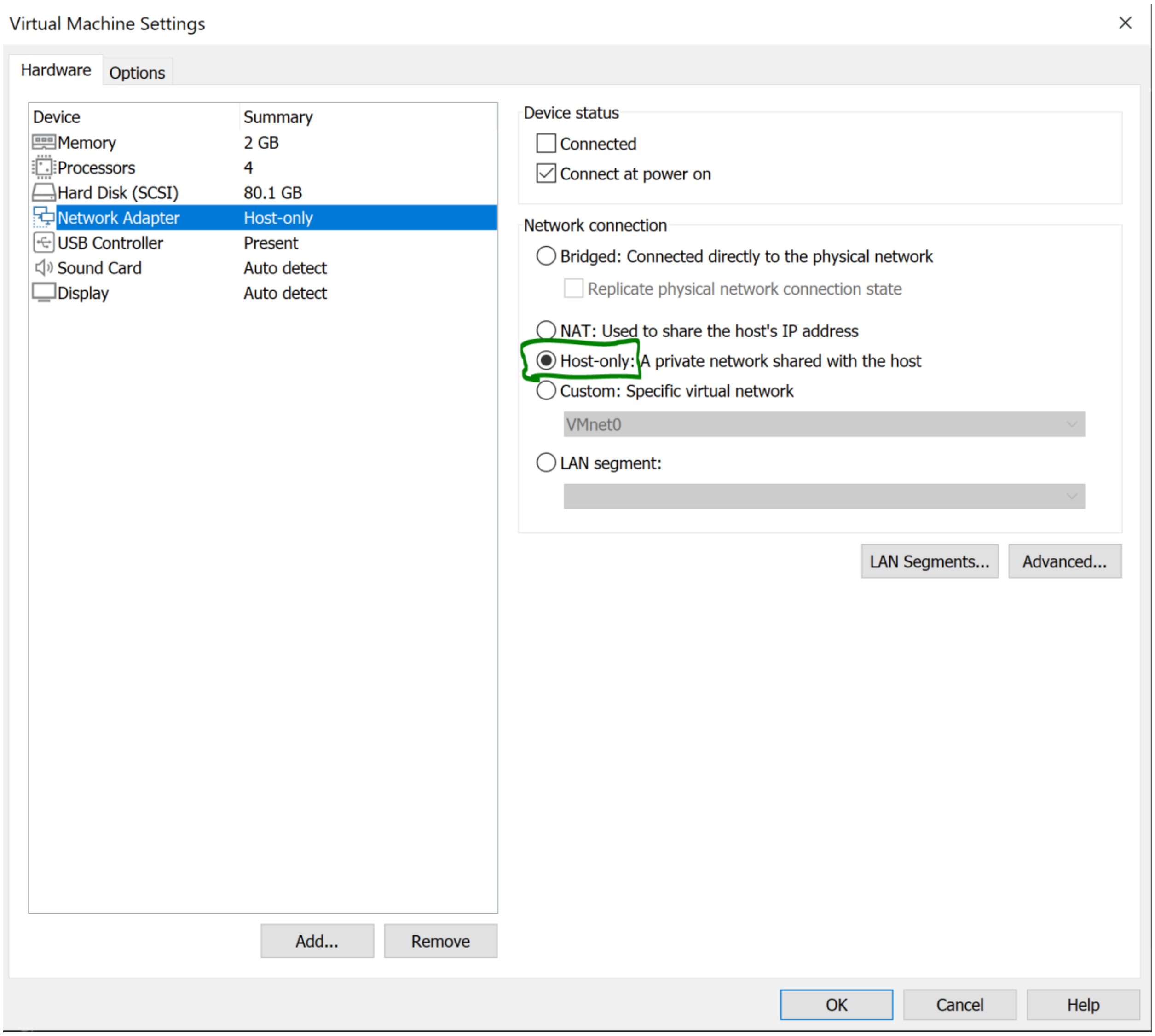
Tools

- Kali Linux
- Nmap
- VirtualBox
- Target: Metasploitable2 **OR** Your own test VM

STEP 1: Setup Environment

Set **both machines** to:

Network → Host-Only Adapter



Virtual Machine Settings

Hardware | Options

Device	Summary
Memory	2 GB
Processors	4
Hard Disk (SCSI)	80.1 GB
Network Adapter	Host-only
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Device status

□ Connected

☑ Connect at power on

Network connection

○ Bridged: Connected directly to the physical network

□ Replicate physical network connection state

○ NAT: Used to share the host's IP address

● Host-only: A private network shared with the host

○ Custom: Specific virtual network

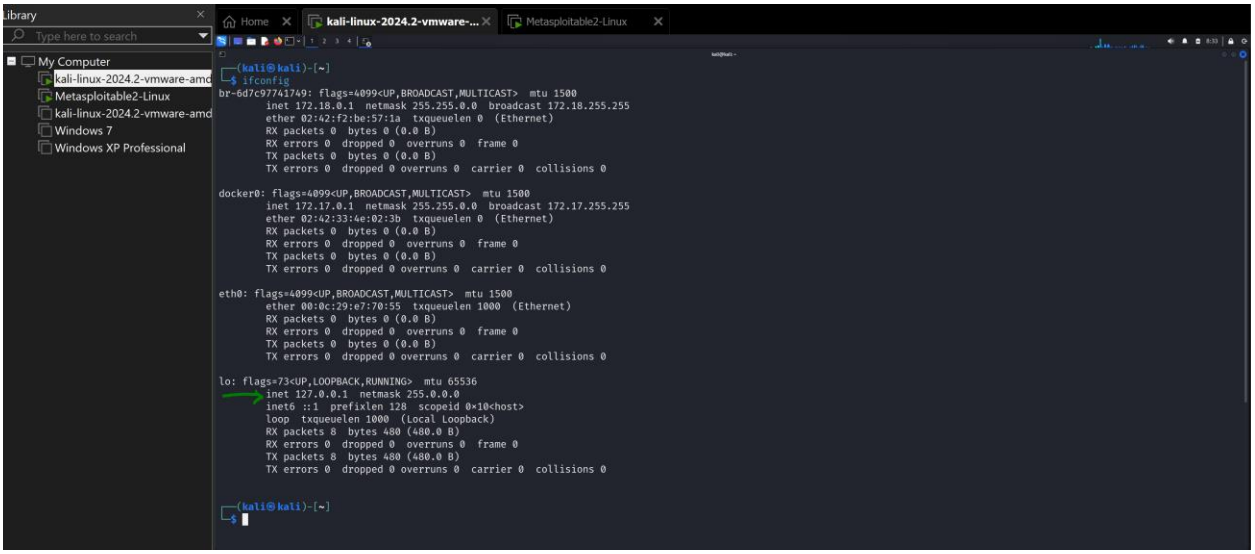
VMnet0

○ LAN segment:

STEP 2: Find Target IP

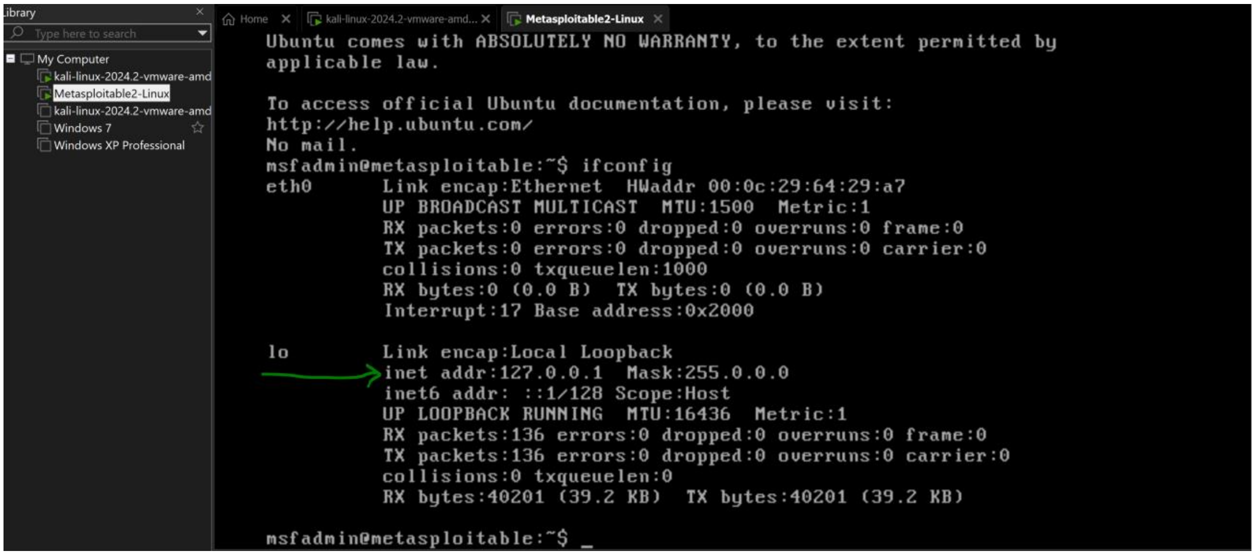
Command ifconfig:

On Kalli Linux



```
┌──(kali㉿kali)-[~]
└─$ ifconfig
br-6d7c97741749: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.18.0.1  netmask 255.255.0.0  broadcast 172.18.255.255
        ether 02:42:f2:be:57:1a  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:33:4e:02:3b  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 00:0c:29:e7:70:55  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$
```

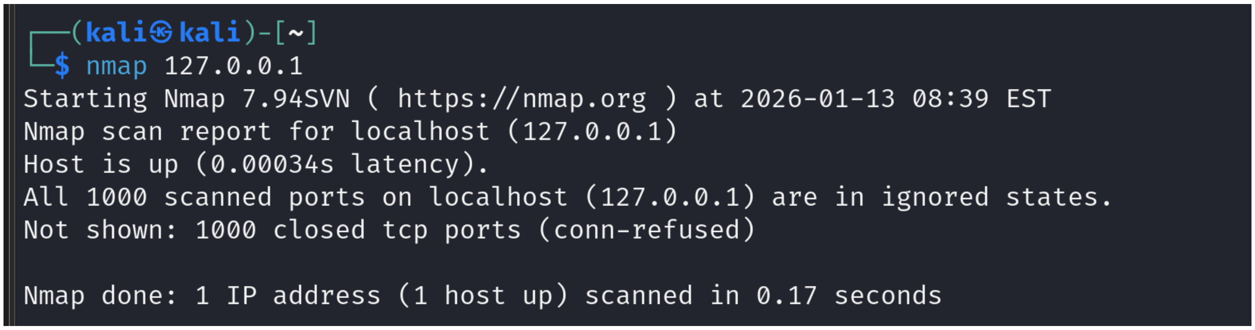
On Metasploitable2:



```
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:64:29:a7
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:136 errors:0 dropped:0 overruns:0 frame:0
          TX packets:136 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:40201 (39.2 KB)  TX bytes:40201 (39.2 KB)

msfadmin@metasploitable:~$ _
```

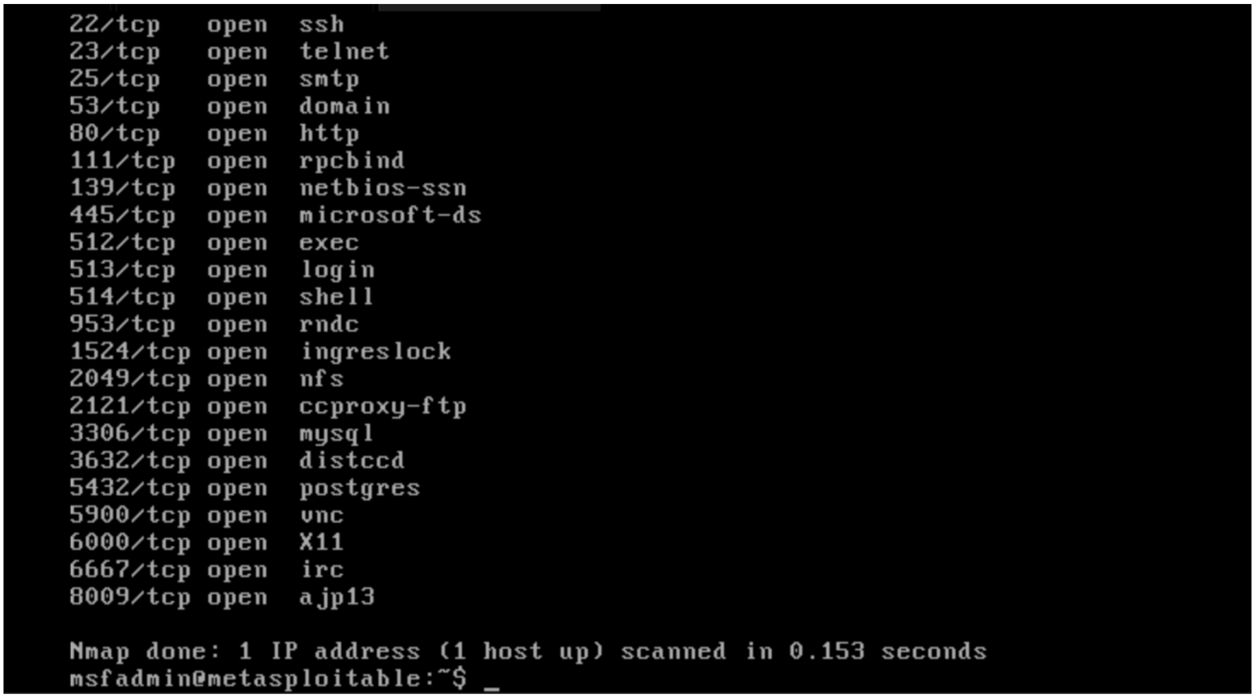
STEP 3: Basic Nmap Scan

On Kali:



```
┌──(kali㉿kali)-[~]
└─$ nmap 127.0.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-13 08:39 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00034s latency).
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```

On Metasploitable2:

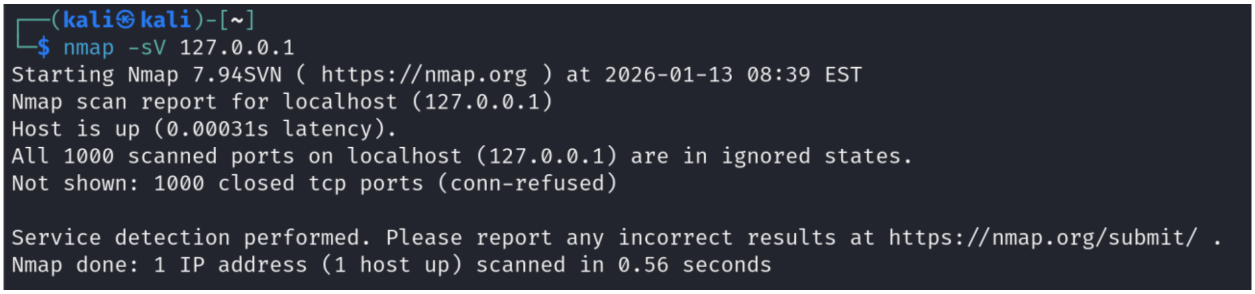


```
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
953/tcp  open  rndc
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
3632/tcp open  distccd
5432/tcp open  postgres
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13

Nmap done: 1 IP address (1 host up) scanned in 0.153 seconds
msfadmin@metasploitable:~$ _
```

STEP 4: Service Detection Scan

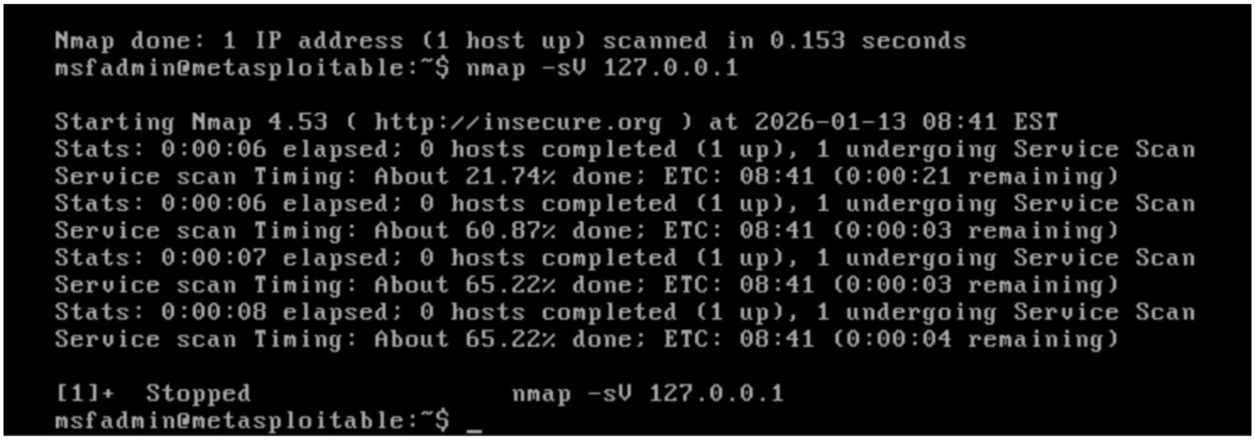
nmap -sV 127.0.0.1

On Kali:



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 127.0.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-13 08:39 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00031s latency).
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.56 seconds
```

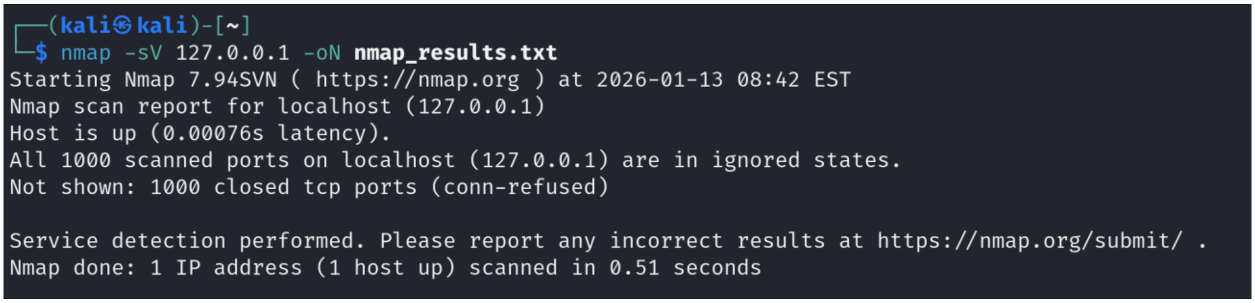
On Metasploitable2:



```
Nmap done: 1 IP address (1 host up) scanned in 0.153 seconds
msfadmin@metasploitable:~$ nmap -sV 127.0.0.1

Starting Nmap 4.53 ( http://insecure.org ) at 2026-01-13 08:41 EST
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 21.74% done; ETC: 08:41 (0:00:21 remaining)
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 60.87% done; ETC: 08:41 (0:00:03 remaining)
Stats: 0:00:07 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 65.22% done; ETC: 08:41 (0:00:03 remaining)
Stats: 0:00:08 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 65.22% done; ETC: 08:41 (0:00:04 remaining)

[1]+  Stopped                 nmap -sV 127.0.0.1
msfadmin@metasploitable:~$ _
```

STEP 5: Save Scan Results

nmap -sV 127.0.0.1 -oN nmap_results.txt



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 127.0.0.1 -oN nmap_results.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-13 08:42 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00076s latency).
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.51 seconds
```