**NMAP**

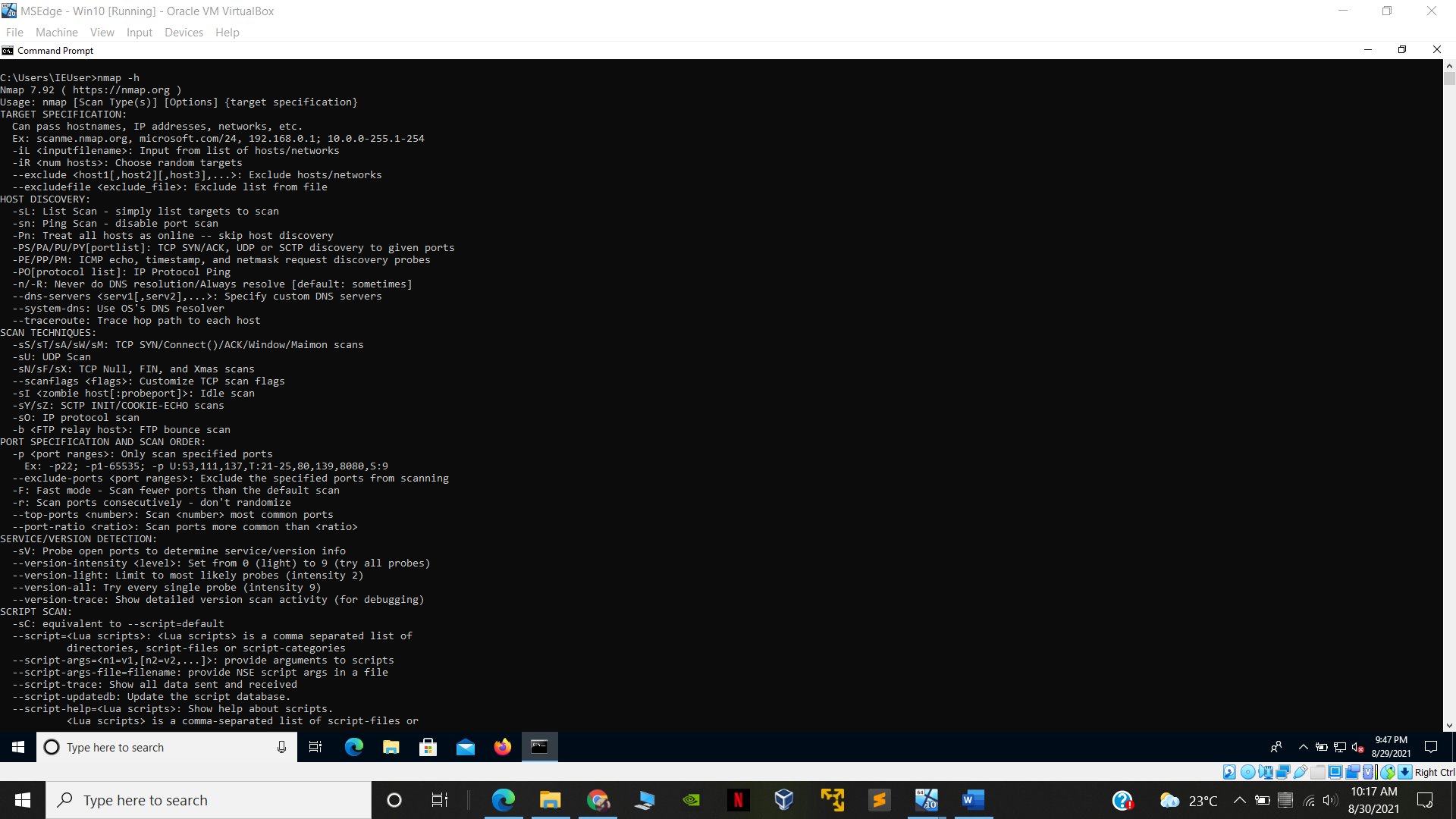
Perform Scanning Module by using Nmap tool (Download from Internet) and scan kalilinux and Windows 7 machine and find the open/closed ports and services running on machine .

Hacker Machine : Windows 10

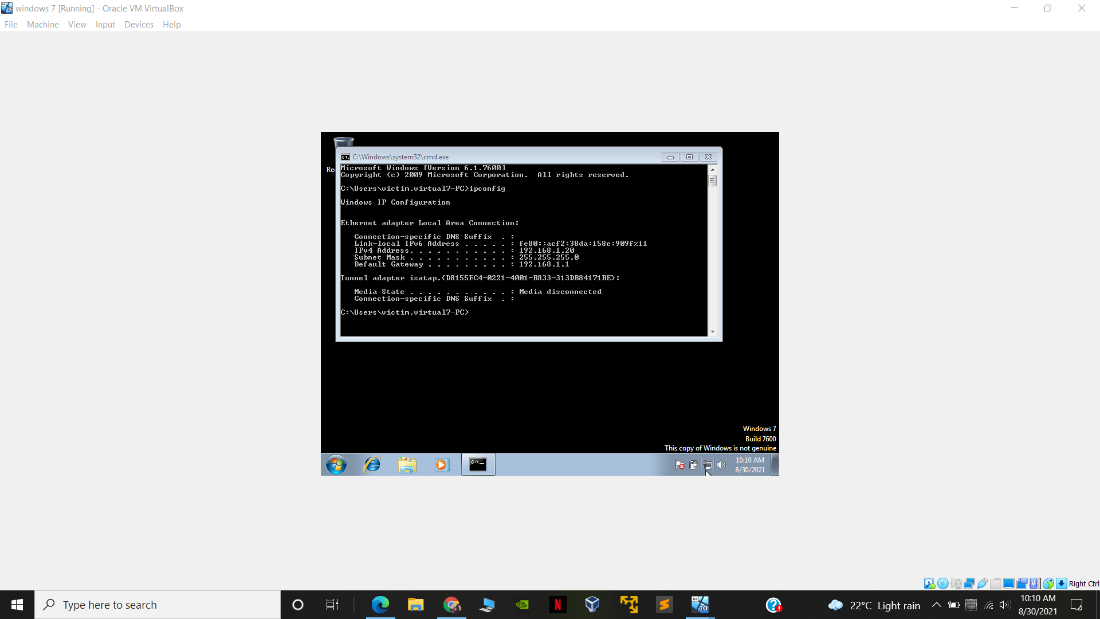
Victim machine : Kali Linux and Windows 7

So my hacker machine is windows 10 as mentioned and targets are kali linux and windows 7

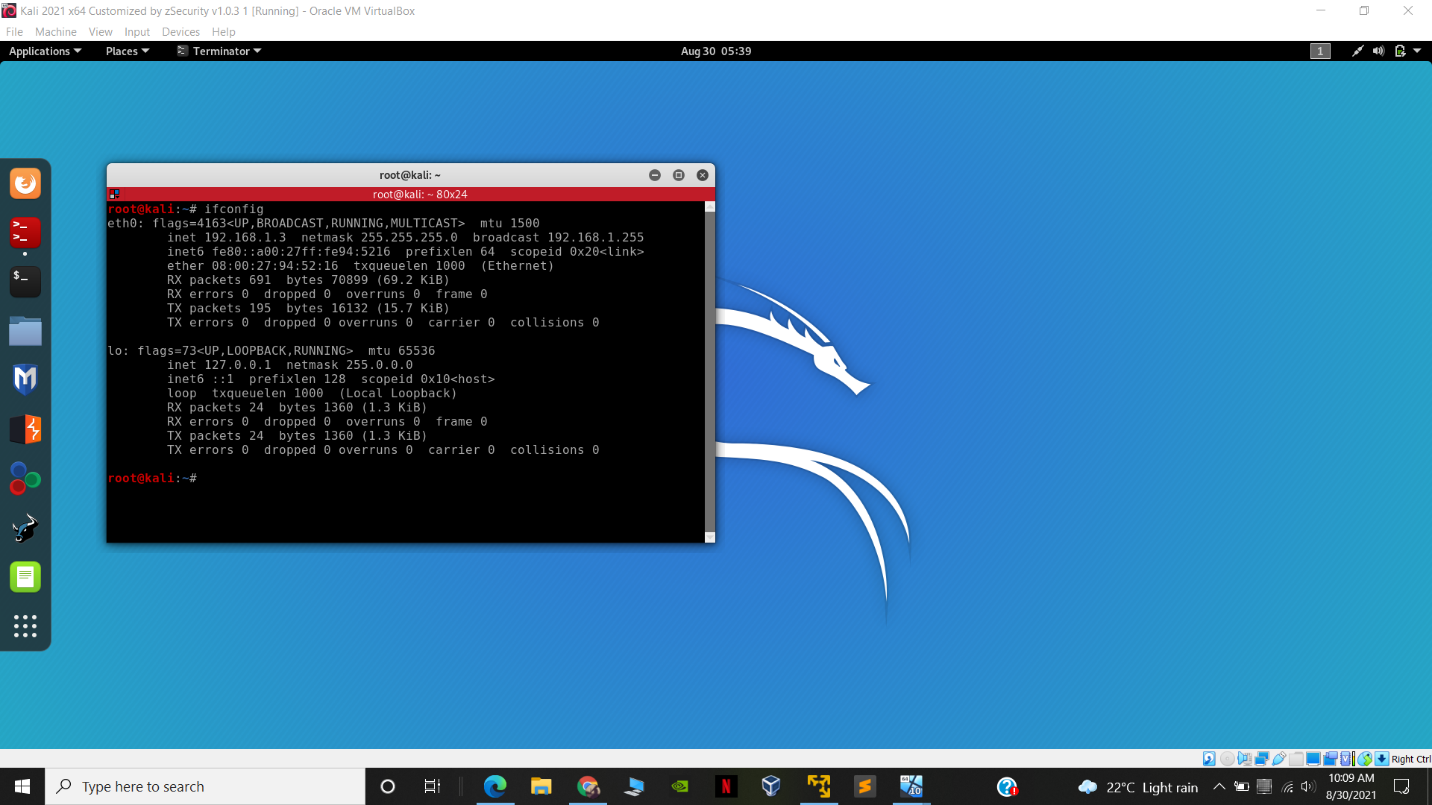
My hacker machine windows 10:



* Winodws 7 ip address: 192.168.1.20



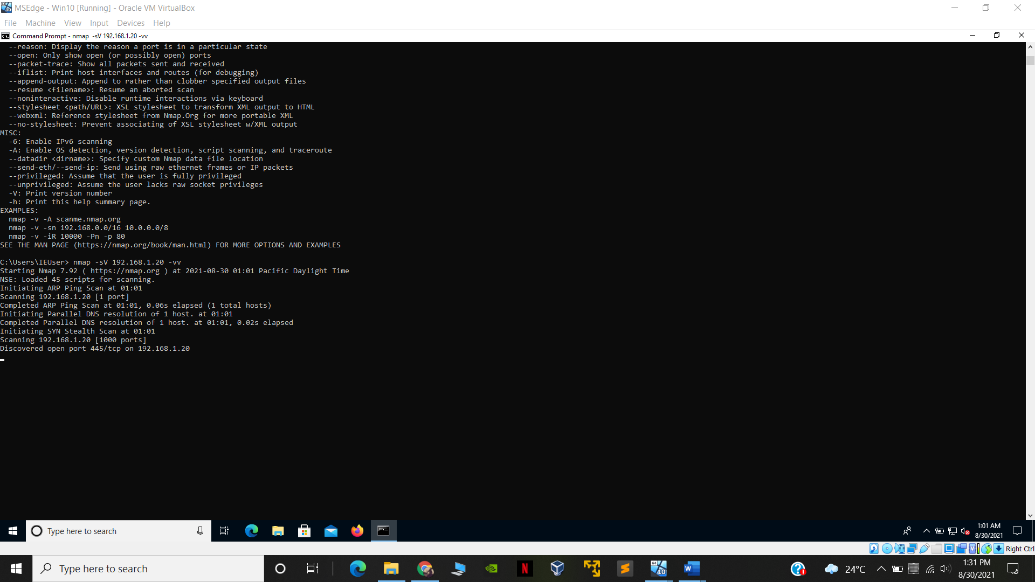
* Kali linux ip address: 192.168.1.3



Steps :

-in windows 10 hacker machine we will use nmap for port scaning

- command



nmap -sV <ip address> -vv

* nmap -sV 192.168.1.20 -vv

**RESULT:**

C:\Users\IEUser> nmap -sV 192.168.1.20 -vv

Starting Nmap 7.92 ( https://nmap.org ) at 2021-08-30 01:01 Pacific Daylight Time

NSE: Loaded 45 scripts for scanning.

Initiating ARP Ping Scan at 01:01

Scanning 192.168.1.20 [1 port]

Completed ARP Ping Scan at 01:01, 0.06s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 01:01

Completed Parallel DNS resolution of 1 host. at 01:01, 0.02s elapsed

Initiating SYN Stealth Scan at 01:01

Scanning 192.168.1.20 [1000 ports]

Discovered open port 445/tcp on 192.168.1.20

Discovered open port 135/tcp on 192.168.1.20

Discovered open port 139/tcp on 192.168.1.20

Completed SYN Stealth Scan at 01:01, 4.83s elapsed (1000 total ports)

Initiating Service scan at 01:01

Scanning 3 services on 192.168.1.20

Completed Service scan at 01:01, 6.09s elapsed (3 services on 1 host)

NSE: Script scanning 192.168.1.20.

NSE: Starting runlevel 1 (of 2) scan.

Initiating NSE at 01:01

Completed NSE at 01:01, 0.01s elapsed

NSE: Starting runlevel 2 (of 2) scan.

Initiating NSE at 01:01

Completed NSE at 01:01, 0.00s elapsed

Nmap scan report for 192.168.1.20

Host is up, received arp-response (0.0017s latency).

Scanned at 2021-08-30 01:01:47 Pacific Daylight Time for 12s

Not shown: 997 filtered tcp ports (no-response)

PORT STATE SERVICE REASON VERSION

135/tcp open msrpc syn-ack ttl 128 Microsoft Windows RPC

139/tcp open netbios-ssn syn-ack ttl 128 Microsoft Windows netbios-ssn

445/tcp open microsoft-ds syn-ack ttl 128 Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)

MAC Address: 08:00:27:4B:28:DE (Oracle VirtualBox virtual NIC)

Service Info: Host: VIRTUAL7-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

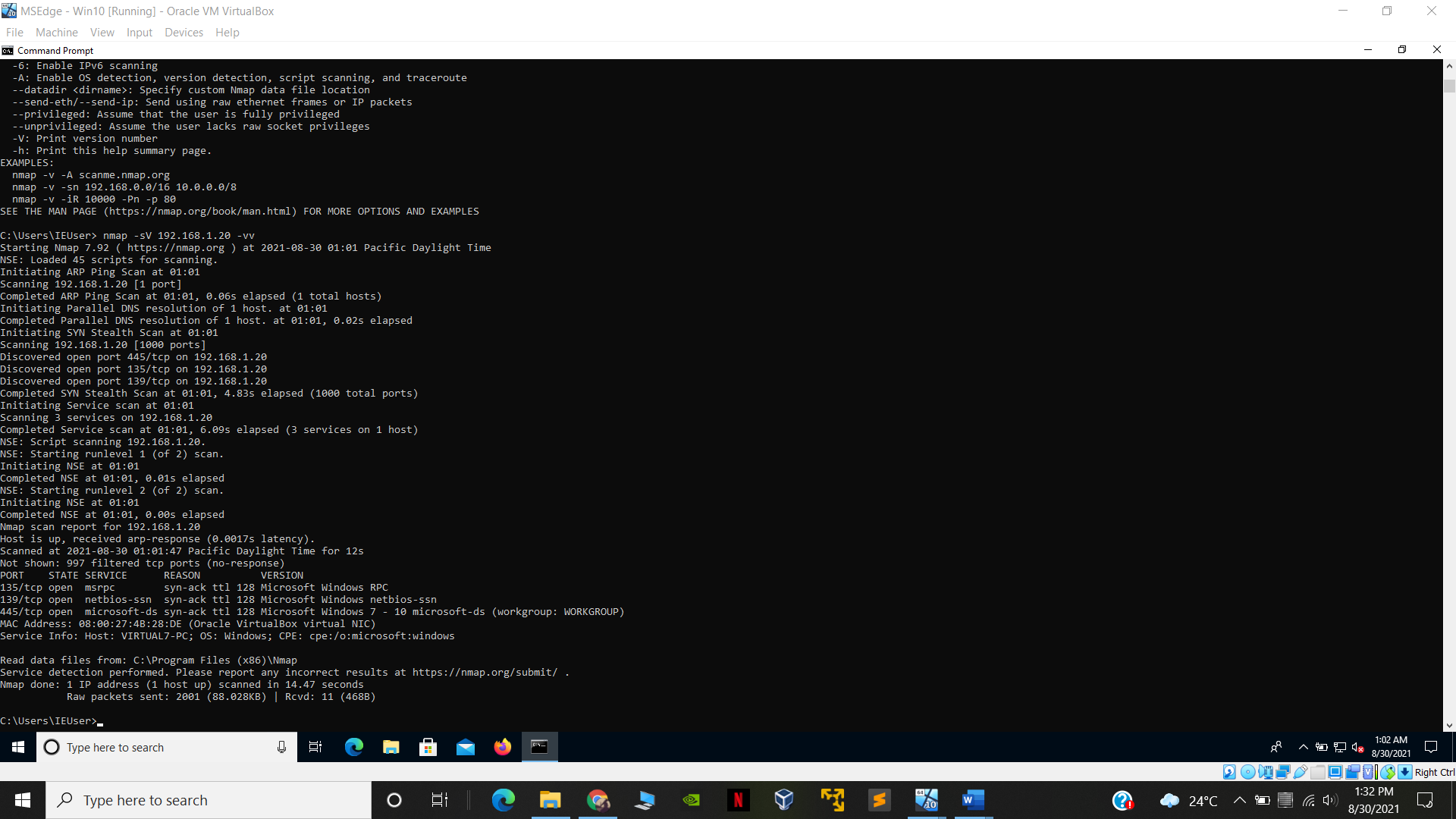
Read data files from: C:\Program Files (x86)\Nmap

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 14.47 seconds

Raw packets sent: 2001 (88.028KB) | Rcvd: 11 (468B)

C:\Users\IEUser>



for kali linux target :

* nmap -sV 192.168.1.3 -vv

RESULTS:

C:\Users\IEUser>nmap -sV 192.168.1.3 -vv

Starting Nmap 7.92 ( https://nmap.org ) at 2021-08-30 01:06 Pacific Daylight Time

NSE: Loaded 45 scripts for scanning.

Initiating ARP Ping Scan at 01:06

Scanning 192.168.1.3 [1 port]

Completed ARP Ping Scan at 01:06, 0.05s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 01:06

Completed Parallel DNS resolution of 1 host. at 01:06, 0.02s elapsed

Initiating SYN Stealth Scan at 01:06

Scanning 192.168.1.3 [1000 ports]

Discovered open port 80/tcp on 192.168.1.3

Completed SYN Stealth Scan at 01:06, 0.11s elapsed (1000 total ports)

Initiating Service scan at 01:06

Scanning 1 service on 192.168.1.3

Completed Service scan at 01:06, 6.04s elapsed (1 service on 1 host)

NSE: Script scanning 192.168.1.3.

NSE: Starting runlevel 1 (of 2) scan.

Initiating NSE at 01:06

Completed NSE at 01:06, 0.02s elapsed

NSE: Starting runlevel 2 (of 2) scan.

Initiating NSE at 01:06

Completed NSE at 01:06, 0.02s elapsed

Nmap scan report for 192.168.1.3

Host is up, received arp-response (0.00062s latency).

Scanned at 2021-08-30 01:06:52 Pacific Daylight Time for 7s

Not shown: 999 closed tcp ports (reset)

PORT STATE SERVICE REASON VERSION

80/tcp open http syn-ack ttl 64 Apache httpd 2.4.46 ((Debian))

MAC Address: 08:00:27:94:52:16 (Oracle VirtualBox virtual NIC)

Read data files from: C:\Program Files (x86)\Nmap

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 6.95 seconds

Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.032KB)

C:\Users\IEUser>

