Andrew Perry | Deontae Carter | Geneva Knott | Jordan Marshall | Sierra Maldonado

What we did: Initial Scan using Nmap
Target Network: **Nmap –open 10.0.0.0/24**

Initial scan was conducted on June 19, 2023 at approximately 1335(EST) hours on Geneva's Kali Linux (VM). Utilizing the following command "**nmap --open 10.0.0.0/24**" in the terminal. Known systems listed below were removed from the findings.

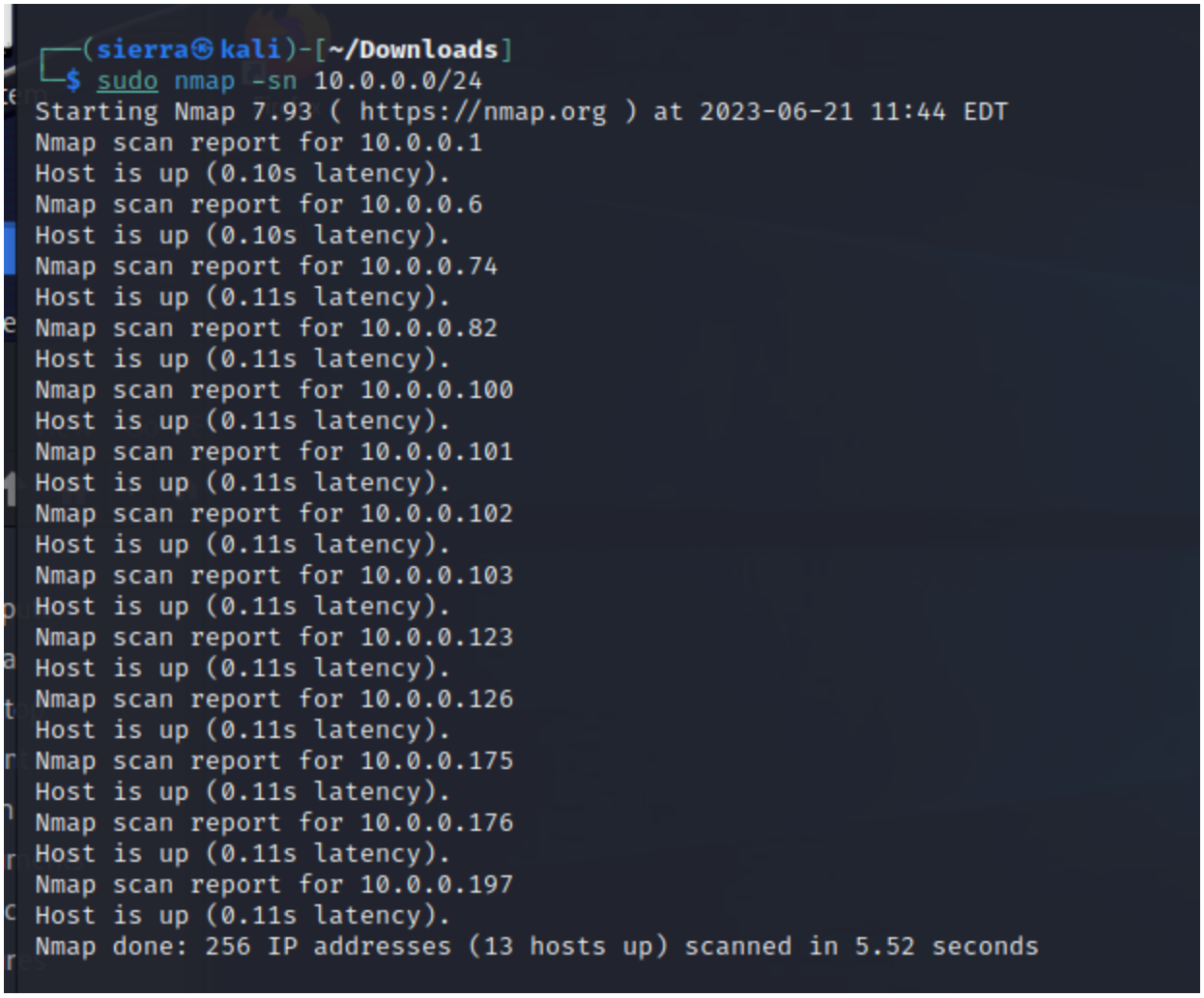
A secondary scan was conducted on June 19, 2024 at approximately 1409(EST) hours Sierra's Kali Linux (VM). Utilizing the following command " **nmap -O 10.0.0.0/24**" in the terminal. The "-O" command looks for the operating system. Known systems listed below were removed from the findings. (See Table in red).

Third scan was conducted using '**nmap -A 10.0.0.0/24"** in the terminal by Sierra at 1421(EST)

Fourth scan was conducted **"nmap -open 10.0.0.0/24 -sV"** by Andrew at 1437(EDT)

Known Systems that are out of bounds

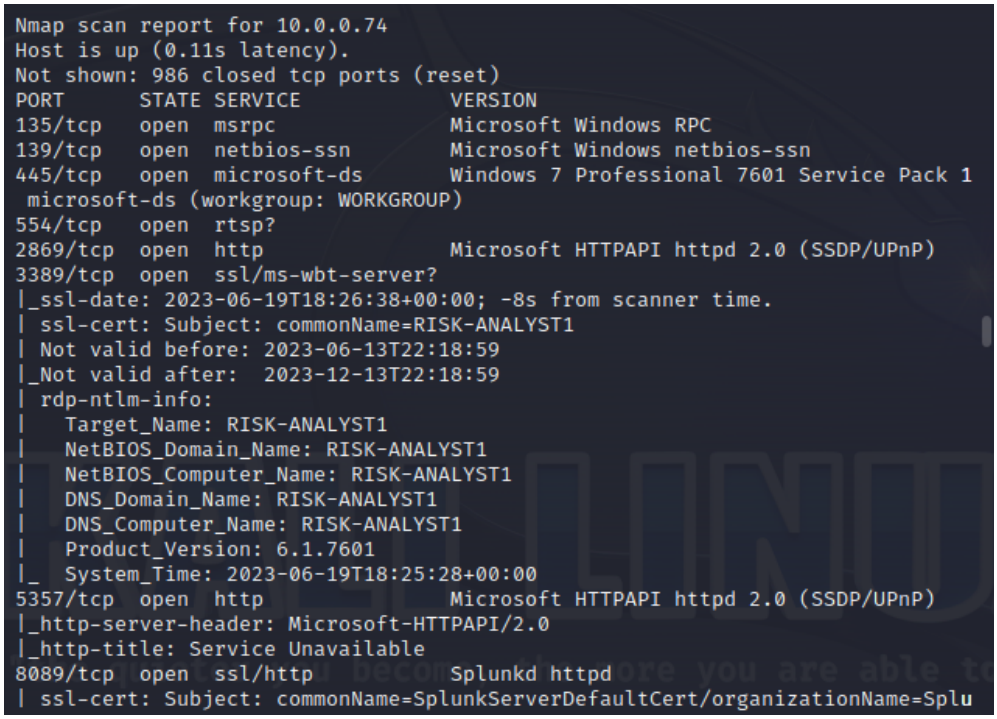
Public IP	Private IP	Hunter 1	Hunter 2	Splunk
44.225.235.60	10.0.0.176	10.0.0.100	10.0.0.102	10.0.0.6
		10.0.0.101	10.0.0.103	



First found: Nmap scan report for **10.0.0.74**
Windows 7
Host is up (0.087s latency).
Not shown: 986 closed tcp ports (conn-refused)

PORT	STATE	SERVICE
21/tcp	open	ftp
80/tcp	open	http
3389/tcp	open	ms-wbt-server
49152	open	unknown
49153	open	unknown

49154	open	unknown
49155	open	unknown
49165	open	unknown

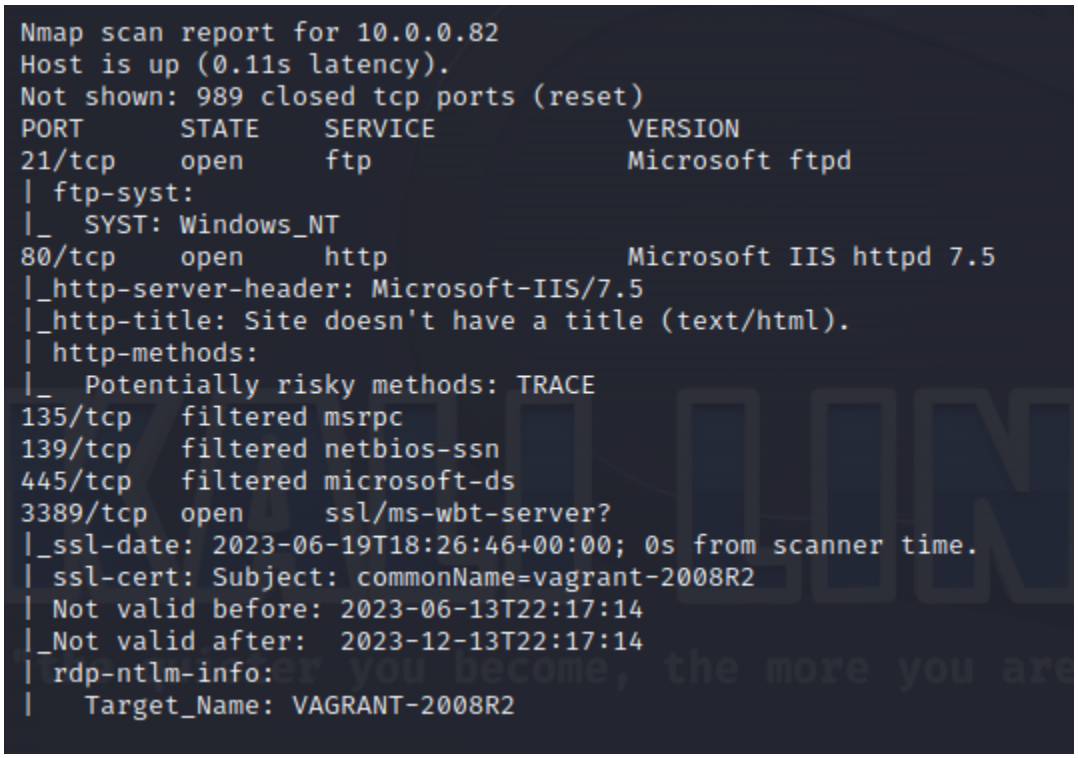


This machine seems to shut down BF attacks almost immediately.

Second found: Nmap scan report for **10.0.0.82**
Windows 7
Host is up (0.085s latency).
Not shown: 989 closed tcp ports (conn-refused), 3 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit

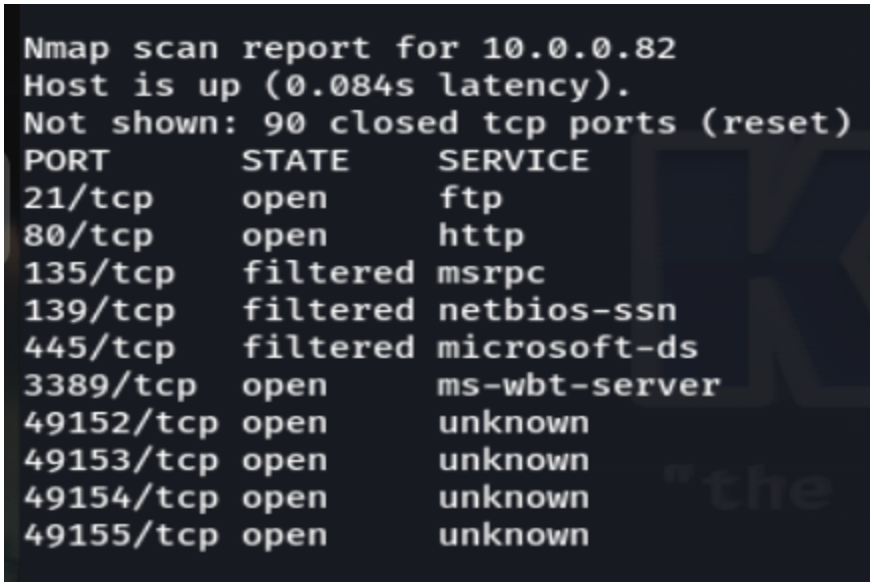
PORT	STATE	SERVICE
21/tcp	open	ftp
80/tcp	open	http
3389/tcp	open	ms-wbt-server
49152/tcp	open	unknown

49153/tcp	open	unknown
49154/tcp	open	unknown
49155/tcp	open	unknown
49165/tcp	open	unknown



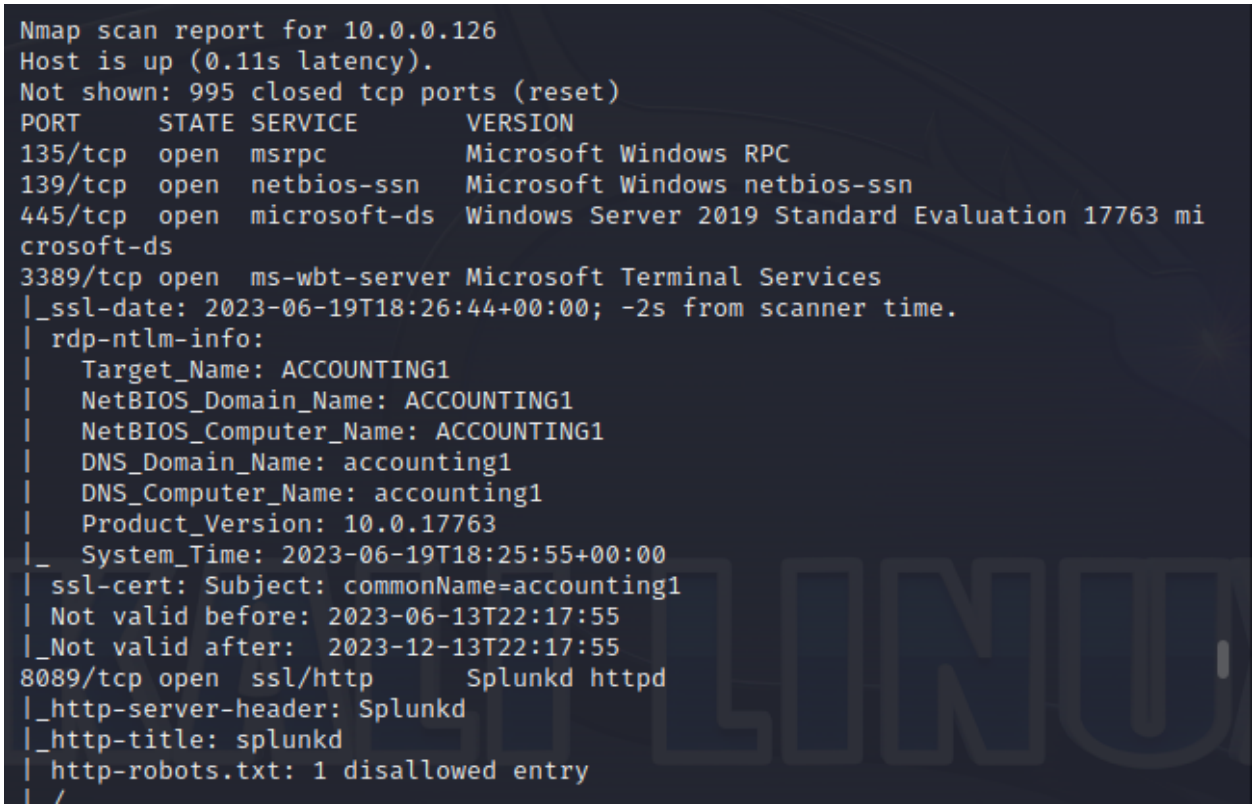
```
Nmap scan report for 10.0.0.82
Host is up (0.11s latency).
Not shown: 989 closed tcp ports (reset)
PORT      STATE    SERVICE            VERSION
21/tcp    open     ftp                Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
80/tcp    open     http               Microsoft IIS httpd 7.5
|_http-server-header: Microsoft-IIS/7.5
|_http-title: Site doesn't have a title (text/html).
| http-methods:
|_  Potentially risky methods: TRACE
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
3389/tcp  open     ssl/ms-wbt-server?
|_ssl-date: 2023-06-19T18:26:46+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=vagrant-2008R2
| Not valid before: 2023-06-13T22:17:14
|_Not valid after:  2023-12-13T22:17:14
| rdp-ntlm-info:
|   Target_Name: VAGRANT-2008R2
```

“sudo nmap --top-ports 100 --traceroute 10.0.0.0/24”
Starting Nmap 7.93 (https://nmap.org) at 2023-06-19 17:25 EDT



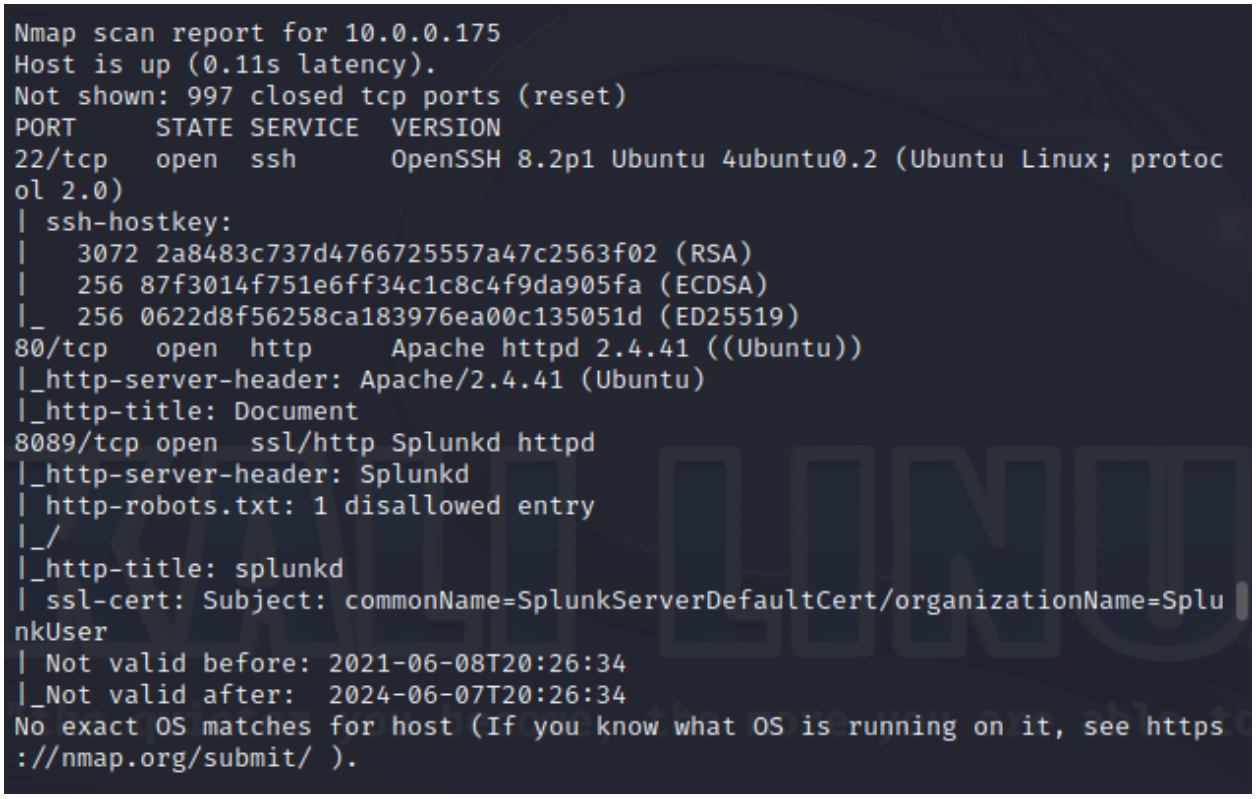
Third Found: Nmap scan report for **10.0.0.126**
Windows Server 2019
Host is up (0.085s latency).
Not shown: 995 closed tcp ports (conn-refused)

PORT	STATE	SERVICE
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
3389/tcp	open	ms-wbt-server
8089/tcp	open	unknown



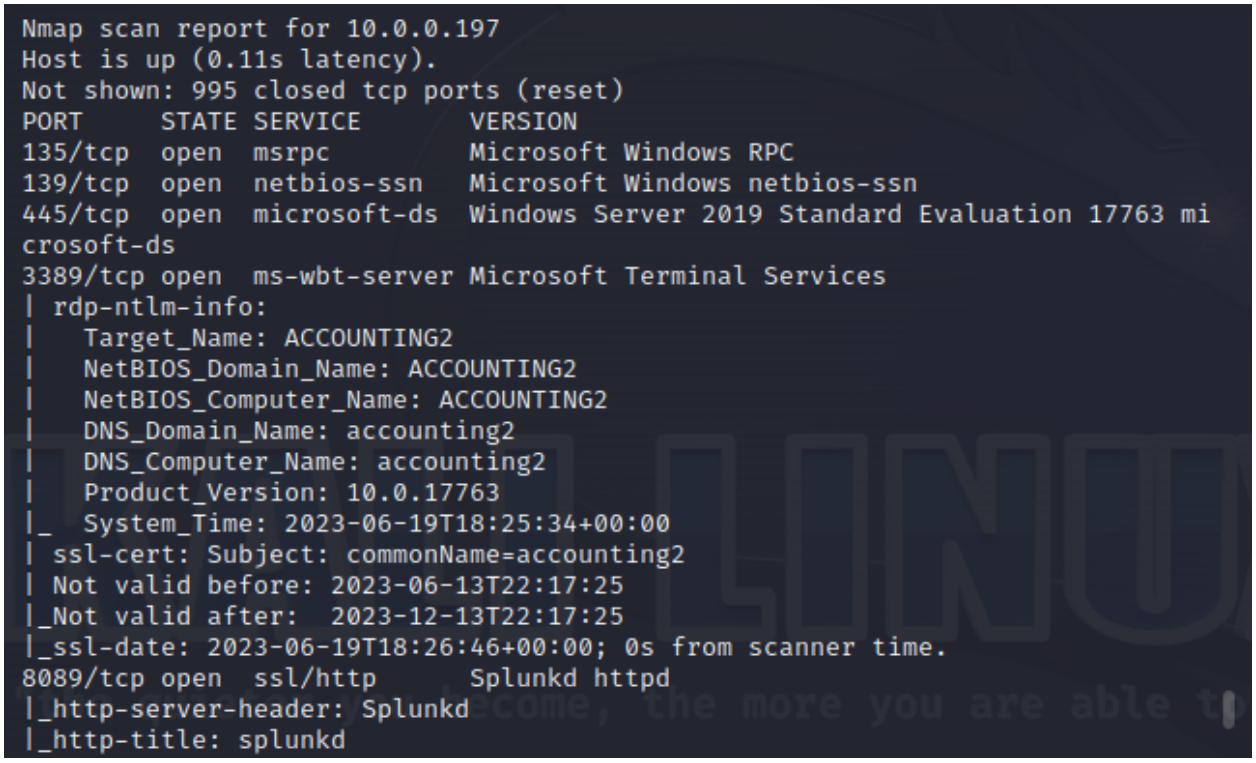
Fourth Found: Nmap scan report for **10.0.0.175**
Linux
Host is up (0.085s latency).
Not shown: 997 closed tcp ports (conn-refused)

PORT	STATE	SERVICE
22/tcp	open	ssh
80/tcp	open	http
8089/tcp	open	unknown



Fifth Found: Nmap scan report for **10.0.0.197**
Windows 2019 Server
Host is up (0.088s latency).
Not shown: 995 closed tcp ports (conn-refused)

PORT	STATE	SERVICE
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
445/tcp	open	mircrosoft-ds
3389/tcp	open	ms-wbt-server
8089/tcp	open	unknown



Sixth found: Nmap scan report for: **10.0.0.123**
Linux
Host is up (0.11s latency)
Not shown: 996 closed TCP ports (reset)

PORT	STATE	SERVICE
22/tcp	open	OpenSSH
111/tcp	open	Rpcbind
2049/tcp	open	nfs_acl
8089/tcp	open	ssl/http

```
Nmap scan report for 10.0.0.123
Host is up (0.11s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 7a9bb9326f957710c0a0803534b1c000 (RSA)
|   256 240c7a8278182d66463b1a362206e1a1 (ECDSA)
|_  256 b915597885789ea5e616f6cf962d1d36 (ED25519)
111/tcp  open  rpcbind  2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  3           2049/udp   nfs
|   100003  3           2049/udp6  nfs
|   100003  3,4         2049/tcp   nfs
|   100003  3,4         2049/tcp6  nfs
|   100005  1,2,3      33504/udp   mountd
```