

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	

```
(sierra@kali)-[~/Downloads]
$ sudo nmap -sn 10.0.0.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-21 11:44 EDT
Nmap scan report for 10.0.0.1
Host is up (0.10s latency).
Nmap scan report for 10.0.0.6
Host is up (0.10s latency).
Nmap scan report for 10.0.0.74
Host is up (0.11s latency).
Nmap scan report for 10.0.0.82
Host is up (0.11s latency).
Nmap scan report for 10.0.0.100
Host is up (0.11s latency).
Nmap scan report for 10.0.0.101
Host is up (0.11s latency).
Nmap scan report for 10.0.0.102
Host is up (0.11s latency).
Nmap scan report for 10.0.0.103
Host is up (0.11s latency).
Nmap scan report for 10.0.0.123
Host is up (0.11s latency).
Nmap scan report for 10.0.0.126
Host is up (0.11s latency).
Nmap scan report for 10.0.0.175
Host is up (0.11s latency).
Nmap scan report for 10.0.0.176
Host is up (0.11s latency).
Nmap scan report for 10.0.0.197
Host is up (0.11s latency).
Nmap done: 256 IP addresses (13 hosts up) scanned in 5.52 seconds
```

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

```
Nmap scan report for 10.0.0.74
Host is up (0.11s latency).
Not shown: 986 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
135/tcp    open  msrpc             Microsoft Windows RPC
139/tcp    open  netbios-ssn       Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds       Windows 7 Professional 7601 Service Pack 1
microsoft-ds (workgroup: WORKGROUP)
554/tcp    open  rtsp?
2869/tcp   open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp   open  ssl/ms-wbt-server?
|_ssl-date: 2023-06-19T18:26:38+00:00; -8s from scanner time.
|_ssl-cert: Subject: commonName=RISK-ANALYST1
|_Not valid before: 2023-06-13T22:18:59
|_Not valid after: 2023-12-13T22:18:59
|_rdp-ntlm-info:
|_Target_Name: RISK-ANALYST1
|_NetBIOS_Domain_Name: RISK-ANALYST1
|_NetBIOS_Computer_Name: RISK-ANALYST1
|_DNS_Domain_Name: RISK-ANALYST1
|_DNS_Computer_Name: RISK-ANALYST1
|_Product_Version: 6.1.7601
|_System_Time: 2023-06-19T18:25:28+00:00
5357/tcp   open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
8089/tcp   open  ssl/http           Splunkd httpd
|_ssl-cert: Subject: commonName=SplunkServerDefaultCert/organizationName=Splu
```

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

```

Nmap scan report for 10.0.0.82
Host is up (0.084s latency).
Not shown: 90 closed tcp ports (reset)
PORT      STATE      SERVICE
21/tcp    open      ftp
80/tcp    open      http
135/tcp   filtered  msrpc
139/tcp   filtered  netbios-ssn
445/tcp   filtered  microsoft-ds
3389/tcp  open      ms-wbt-server
49152/tcp open      unknown
49153/tcp open      unknown
49154/tcp open      unknown
49155/tcp open      unknown

```

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

```

Nmap scan report for 10.0.0.126
Host is up (0.11s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
135/tcp    open  msrpc             Microsoft Windows RPC
139/tcp    open  netbios-ssn       Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds       Windows Server 2019 Standard Evaluation 17763 mi
crosoft-ds
3389/tcp   open  ms-wbt-server      Microsoft Terminal Services
|_ssl-date: 2023-06-19T18:26:44+00:00; -2s from scanner time.
|_rdp-ntlm-info:
|   Target_Name: ACCOUNTING1
|   NetBIOS_Domain_Name: ACCOUNTING1
|   NetBIOS_Computer_Name: ACCOUNTING1
|   DNS_Domain_Name: accounting1
|   DNS_Computer_Name: accounting1
|   Product_Version: 10.0.17763
|_System_Time: 2023-06-19T18:25:55+00:00
|_ssl-cert: Subject: commonName=accounting1
|_Not valid before: 2023-06-13T22:17:55
|_Not valid after: 2023-12-13T22:17:55
8089/tcp   open  ssl/http           Splunkd httpd
|_http-server-header: Splunkd
|_http-title: splunkd
|_http-robots.txt: 1 disallowed entry
|_ /

```

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

```

Nmap scan report for 10.0.0.175
Host is up (0.11s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   3072 2a8483c737d4766725557a47c2563f02 (RSA)
|   256 87f3014f751e6ff34c1c8c4f9da905fa (ECDSA)
|_  256 0622d8f56258ca183976ea00c135051d (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-title: Document
8089/tcp  open  ssl/http Splunkd httpd
|_ http-server-header: Splunkd
|_ http-robots.txt: 1 disallowed entry
|_/
|_ http-title: splunkd
|_ ssl-cert: Subject: commonName=SplunkServerDefaultCert/organizationName=SplunkUser
|_ Not valid before: 2021-06-08T20:26:34
|_ Not valid after:  2024-06-07T20:26:34
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).

```

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	microsof-ds
3389/tcp	open	ms-wbt-server
8089/tcp	open	unknown

```

Nmap scan report for 10.0.0.197
Host is up (0.11s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
135/tcp    open  msrpc            Microsoft Windows RPC
139/tcp    open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds     Windows Server 2019 Standard Evaluation 17763 mi
crosoft-ds
3389/tcp   open  ms-wbt-server    Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: ACCOUNTING2
|   NetBIOS_Domain_Name: ACCOUNTING2
|   NetBIOS_Computer_Name: ACCOUNTING2
|   DNS_Domain_Name: accounting2
|   DNS_Computer_Name: accounting2
|   Product_Version: 10.0.17763
|_  System_Time: 2023-06-19T18:25:34+00:00
| ssl-cert: Subject: commonName=accounting2
| Not valid before: 2023-06-13T22:17:25
|_ Not valid after: 2023-12-13T22:17:25
|_ ssl-date: 2023-06-19T18:26:46+00:00; 0s from scanner time.
8089/tcp   open  ssl/http         Splunkd httpd
|_ http-server-header: Splunkd
|_ http-title: splunkd

```

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
```