**Team –**

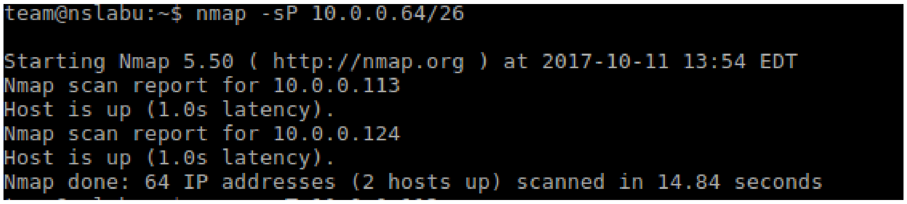
a. **Suraj Bhatia**
b. **Soumya Mohanty**

1. **The output of your discovery scan.**

Two hosts were found using discovery scan in the 10.0.0.64/26 subnet –

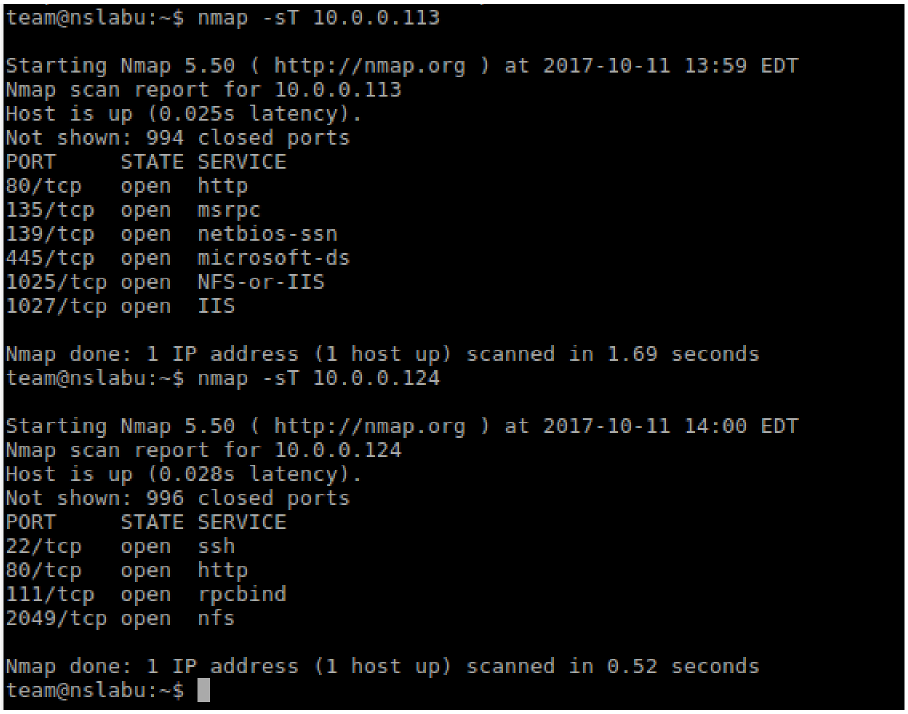
Host 1 – 10.0.0.113

Host 2 – 10.0.0.124



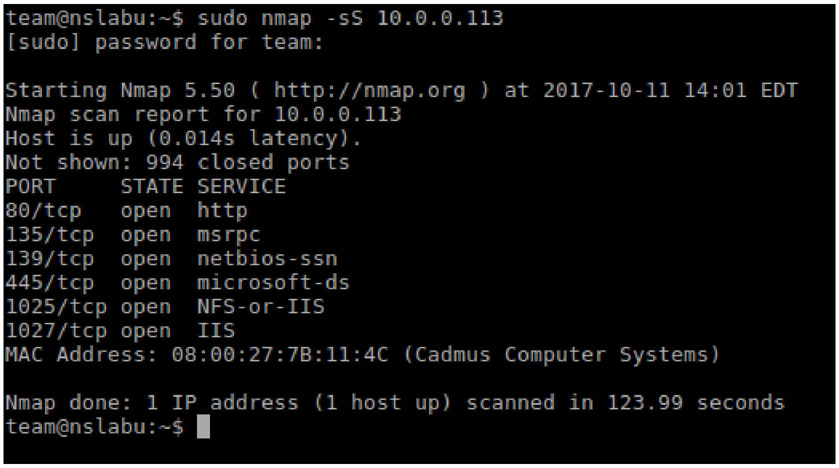
```
team@nslabu:~$ nmap -sP 10.0.0.64/26

Starting Nmap 5.50 ( http://nmap.org ) at 2017-10-11 13:54 EDT
Nmap scan report for 10.0.0.113
Host is up (1.0s latency).
Nmap scan report for 10.0.0.124
Host is up (1.0s latency).
Nmap done: 64 IP addresses (2 hosts up) scanned in 14.84 seconds
```

2. **The output of your full TCP connect() scan.**

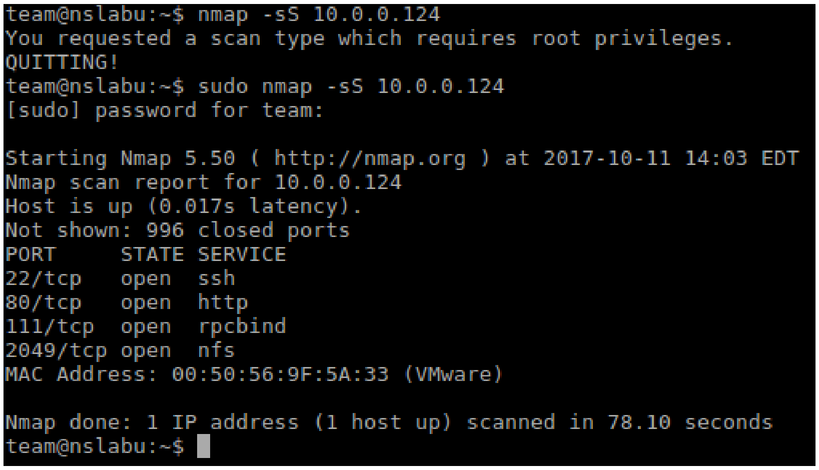


```
team@nslabu:~$ nmap -sT 10.0.0.113

Starting Nmap 5.50 ( http://nmap.org ) at 2017-10-11 13:59 EDT
Nmap scan report for 10.0.0.113
Host is up (0.025s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1027/tcp open  IIS

Nmap done: 1 IP address (1 host up) scanned in 1.69 seconds
team@nslabu:~$ nmap -sT 10.0.0.124

Starting Nmap 5.50 ( http://nmap.org ) at 2017-10-11 14:00 EDT
Nmap scan report for 10.0.0.124
Host is up (0.028s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
2049/tcp open  nfs

Nmap done: 1 IP address (1 host up) scanned in 0.52 seconds
team@nslabu:~$ 
```

3. **The output of your TCP SYN scan.**

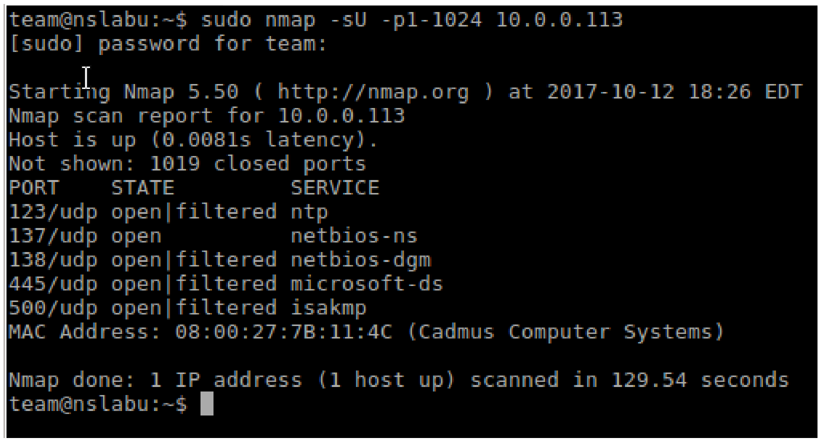


```
team@nslabu:~$ sudo nmap -sS 10.0.0.113
[sudo] password for team:

Starting Nmap 5.50 ( http://nmap.org ) at 2017-10-11 14:01 EDT
Nmap scan report for 10.0.0.113
Host is up (0.014s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1027/tcp open  IIS
MAC Address: 08:00:27:7B:11:4C (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 123.99 seconds
team@nslabu:~$
```

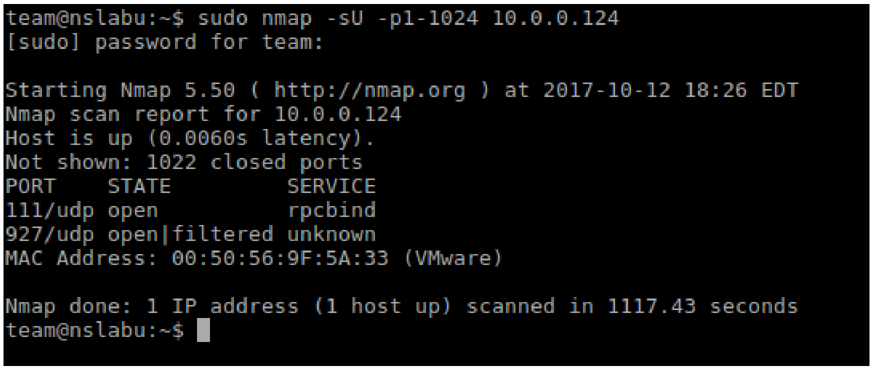


```
team@nslabu:~$ nmap -sS 10.0.0.124
You requested a scan type which requires root privileges.
QUITTING!
team@nslabu:~$ sudo nmap -sS 10.0.0.124
[sudo] password for team:

Starting Nmap 5.50 ( http://nmap.org ) at 2017-10-11 14:03 EDT
Nmap scan report for 10.0.0.124
Host is up (0.017s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
2049/tcp open  nfs
MAC Address: 00:50:56:9F:5A:33 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 78.10 seconds
team@nslabu:~$
```

4. **The output of your UDP scan.**

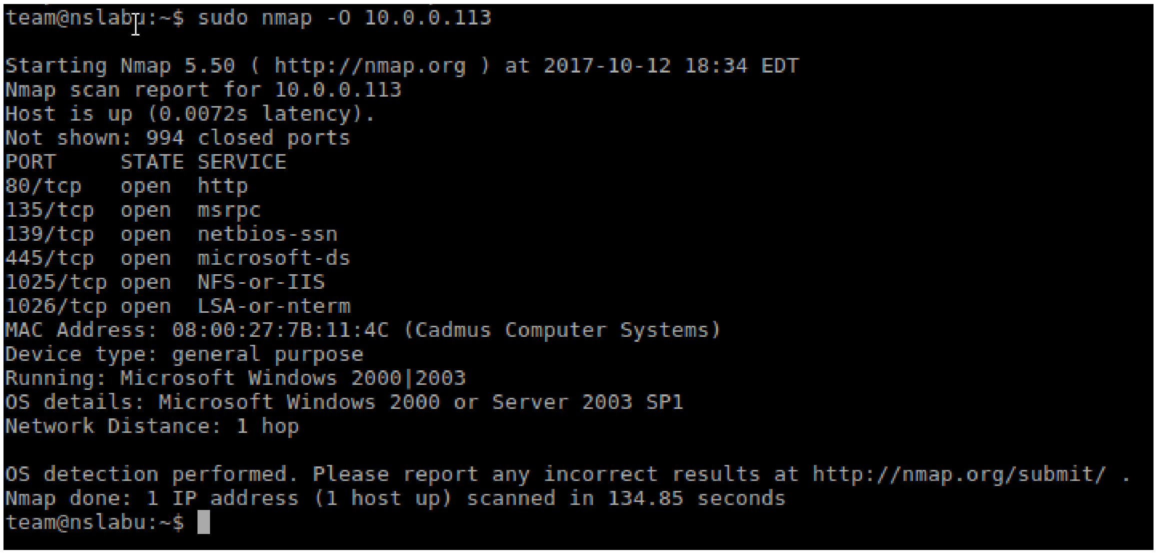


```
team@nslabu:~$ sudo nmap -sU -p1-1024 10.0.0.113
[sudo] password for team:

Starting Nmap 5.50 ( http://nmap.org ) at 2017-10-12 18:26 EDT
Nmap scan report for 10.0.0.113
Host is up (0.0081s latency).
Not shown: 1019 closed ports
PORT    STATE         SERVICE
123/udp open|filtered ntp
137/udp open          netbios-ns
138/udp open|filtered netbios-dgm
445/udp open|filtered microsoft-ds
500/udp open|filtered isakmp
MAC Address: 08:00:27:7B:11:4C (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 129.54 seconds
team@nslabu:~$
```

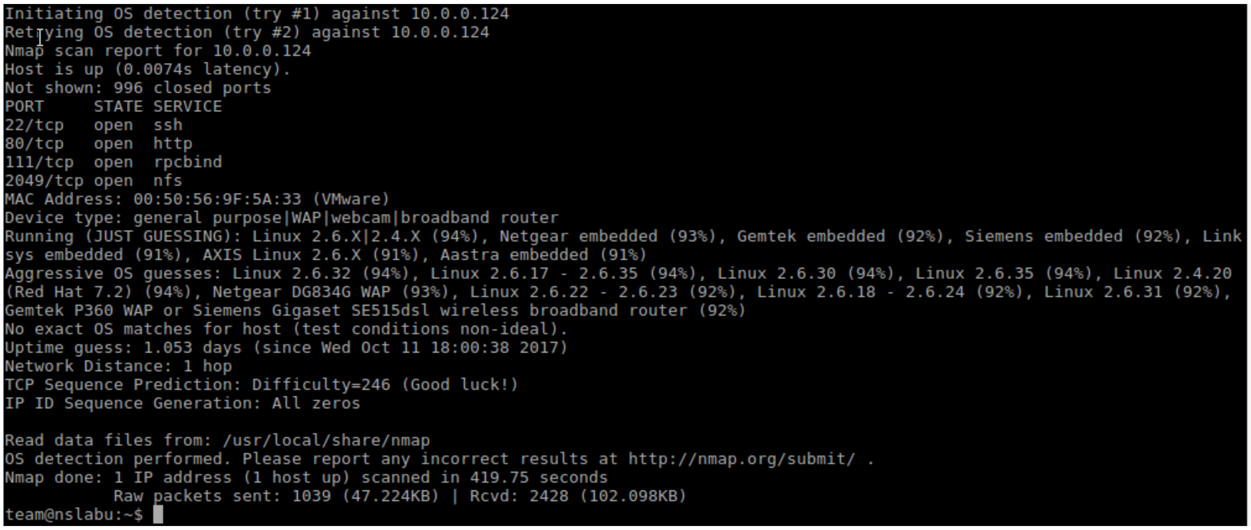


```
team@nslabu:~$ sudo nmap -sU -p1-1024 10.0.0.124
[sudo] password for team:

Starting Nmap 5.50 ( http://nmap.org ) at 2017-10-12 18:26 EDT
Nmap scan report for 10.0.0.124
Host is up (0.0060s latency).
Not shown: 1022 closed ports
PORT    STATE         SERVICE
111/udp open          rpcbind
927/udp open|filtered unknown
MAC Address: 00:50:56:9F:5A:33 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1117.43 seconds
team@nslabu:~$ 
```

5. **The output of your operating system identification scan.**

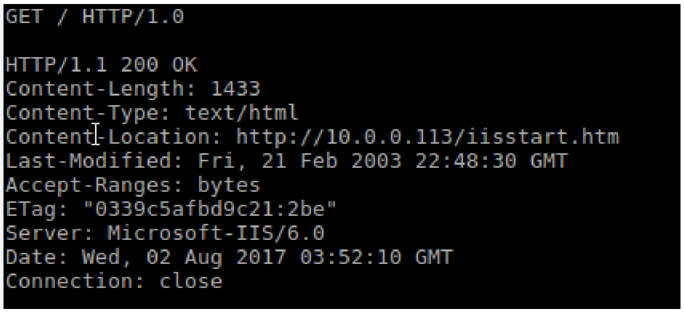


```
team@nslabu:~$ sudo nmap -O 10.0.0.113

Starting Nmap 5.50 ( http://nmap.org ) at 2017-10-12 18:34 EDT
Nmap scan report for 10.0.0.113
Host is up (0.0072s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
MAC Address: 08:00:27:7B:11:4C (Cadmus Computer Systems)
Device type: general purpose
Running: Microsoft Windows 2000|2003
OS details: Microsoft Windows 2000 or Server 2003 SP1
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 134.85 seconds
team@nslabu:~$ 
```

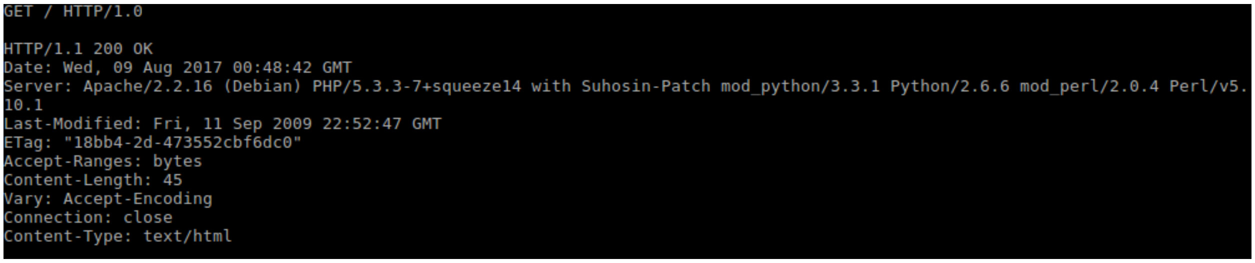


```
Initiating OS detection (try #1) against 10.0.0.124
Retrying OS detection (try #2) against 10.0.0.124
Nmap scan report for 10.0.0.124
Host is up (0.0074s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
2049/tcp open  nfs
MAC Address: 00:50:56:9F:5A:33 (VMware)
Device type: general purpose|WAP|webcam|broadband router
Running (JUST GUESSING): Linux 2.6.X|2.4.X (94%), Netgear embedded (93%), Gemtek embedded (92%), Siemens embedded (92%), Link
sys embedded (91%), AXIS Linux 2.6.X (91%), Aastra embedded (91%)
Aggressive OS guesses: Linux 2.6.32 (94%), Linux 2.6.17 - 2.6.35 (94%), Linux 2.6.30 (94%), Linux 2.6.35 (94%), Linux 2.4.20
(Red Hat 7.2) (94%), Netgear DG834G WAP (93%), Linux 2.6.22 - 2.6.23 (92%), Linux 2.6.18 - 2.6.24 (92%), Linux 2.6.31 (92%),
Gemtek P360 WAP or Siemens Gigaset SE515dsl wireless broadband router (92%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 1.053 days (since Wed Oct 11 18:00:38 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=246 (Good luck!)
IP ID Sequence Generation: All zeros

Read data files from: /usr/local/share/nmap
OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 419.75 seconds
           Raw packets sent: 1039 (47.224KB) | Rcvd: 2428 (102.098KB)
team@nslabu:~$ 
```

6. **The output of your server header grab.**

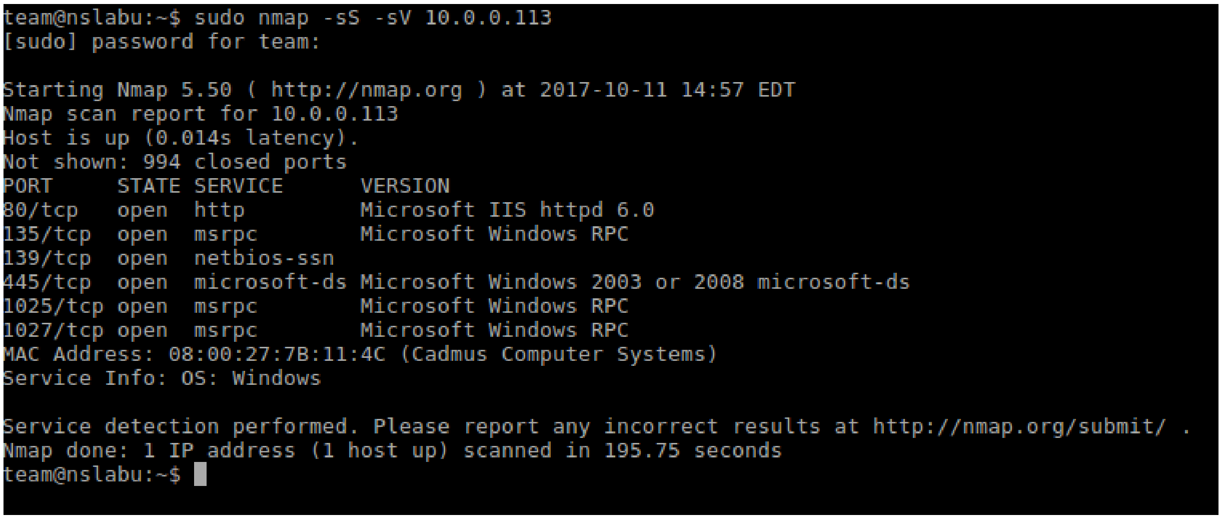


```
GET / HTTP/1.0

HTTP/1.1 200 OK
Content-Length: 1433
Content-Type: text/html
Content-Location: http://10.0.0.113/iisstart.htm
Last-Modified: Fri, 21 Feb 2003 22:48:30 GMT
Accept-Ranges: bytes
ETag: "0339c5afbd9c21:2be"
Server: Microsoft-IIS/6.0
Date: Wed, 02 Aug 2017 03:52:10 GMT
Connection: close
```

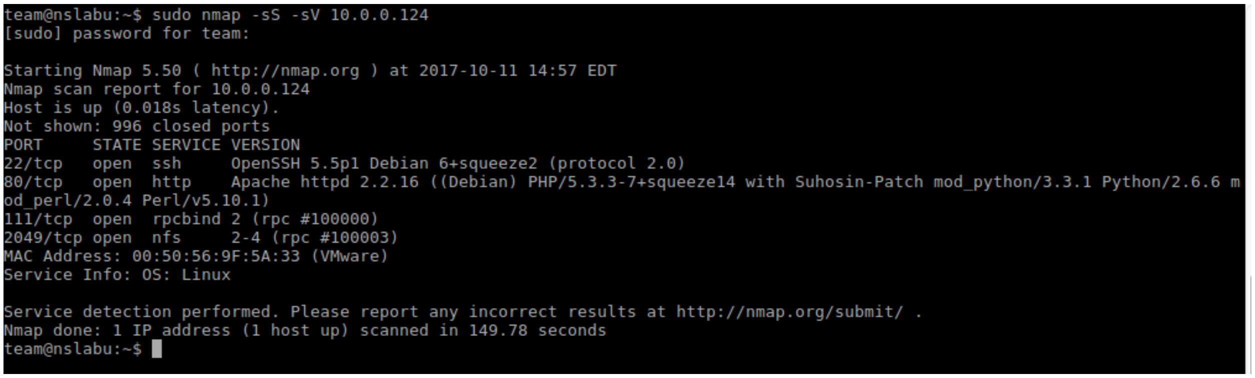


```
GET / HTTP/1.0

HTTP/1.1 200 OK
Date: Wed, 09 Aug 2017 00:48:42 GMT
Server: Apache/2.2.16 (Debian) PHP/5.3.3-7+squeeze14 with Suhosin-Patch mod_python/3.3.1 Python/2.6.6 mod_perl/2.0.4 Perl/v5.
10.1
Last-Modified: Fri, 11 Sep 2009 22:52:47 GMT
ETag: "18bb4-2d-473552cbf6dc0"
Accept-Ranges: bytes
Content-Length: 45
Vary: Accept-Encoding
Connection: close
Content-Type: text/html
```

7. **The output of your service probes.**

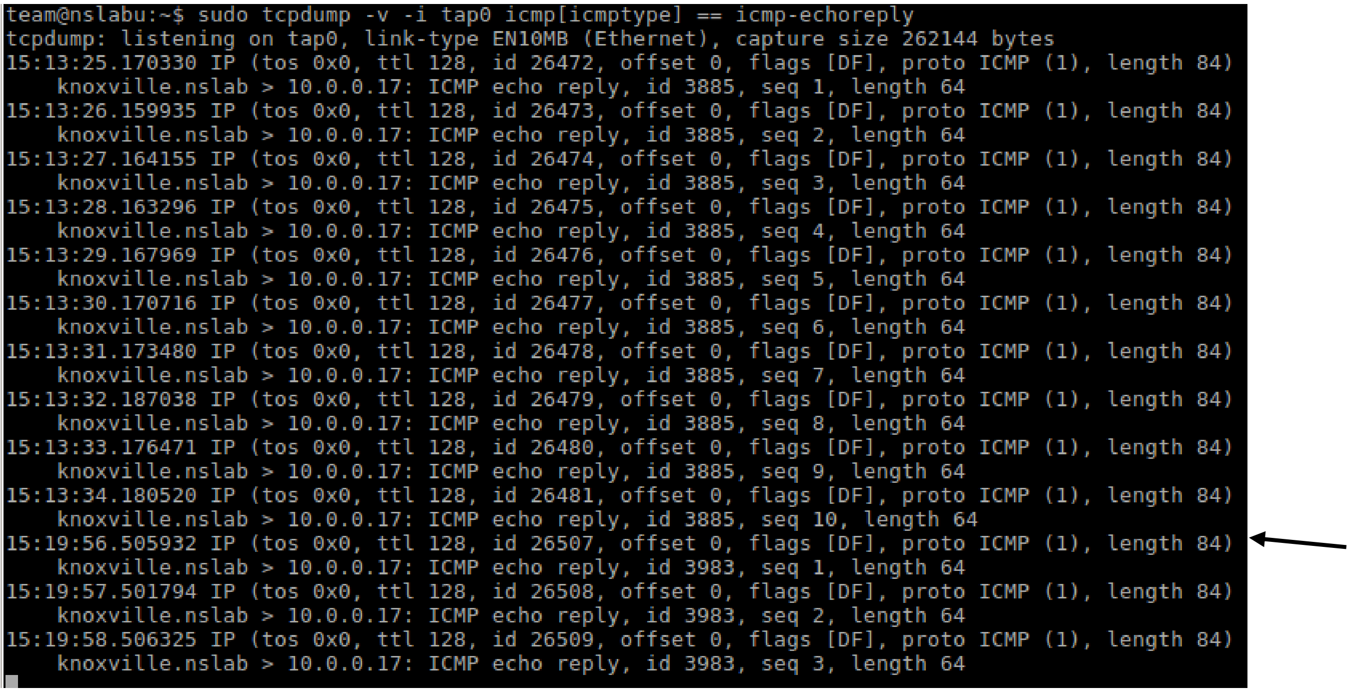


```
team@nslabu:~$ sudo nmap -sS -sV 10.0.0.113
[sudo] password for team:

Starting Nmap 5.50 ( http://nmap.org ) at 2017-10-11 14:57 EDT
Nmap scan report for 10.0.0.113
Host is up (0.014s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE      VERSION
80/tcp   open  http         Microsoft IIS httpd 6.0
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows 2003 or 2008 microsoft-ds
1025/tcp open  msrpc        Microsoft Windows RPC
1027/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:7B:11:4C (Cadmus Computer Systems)
Service Info: OS: Windows

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 195.75 seconds
team@nslabu:~$
```



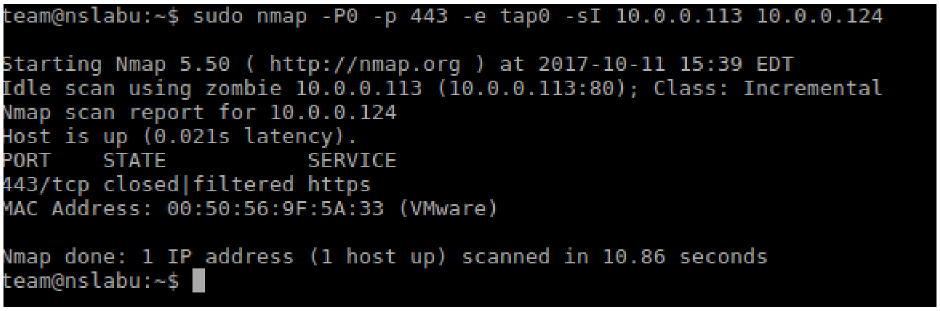
```
team@nslabu:~$ sudo nmap -sS -sV 10.0.0.124
[sudo] password for team:

Starting Nmap 5.50 ( http://nmap.org ) at 2017-10-11 14:57 EDT
Nmap scan report for 10.0.0.124
Host is up (0.018s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 5.5p1 Debian 6+squeeze2 (protocol 2.0)
80/tcp   open  http    Apache httpd 2.2.16 ((Debian) PHP/5.3.3-7+squeeze14 with Suhosin-Patch mod_python/3.3.1 Python/2.6.6 m
od_perl/2.0.4 Perl/v5.10.1)
111/tcp  open  rpcbind 2 (rpc #100000)
2049/tcp open  nfs     2-4 (rpc #100003)
MAC Address: 00:50:56:9F:5A:33 (VMware)
Service Info: OS: Linux

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 149.78 seconds
team@nslabu:~$
```

8. **The annotated snippet of your tcpdump showing the IP ID sequence hole.**

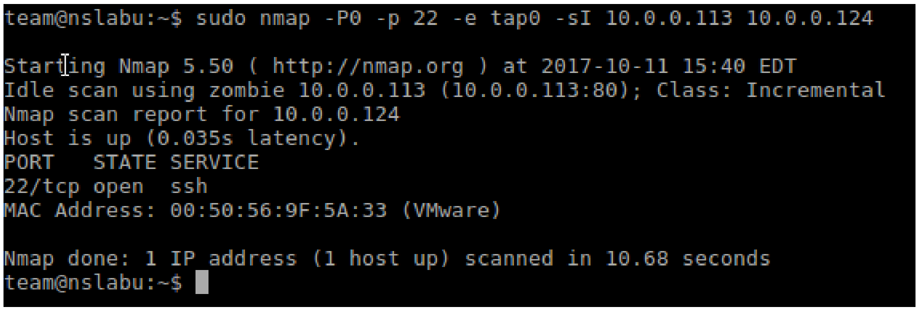


```
team@nslabu:~$ sudo tcpdump -v -i tap0 icmp[icmptype] == icmp-echoreply
tcpdump: listening on tap0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:13:25.170330 IP (tos 0x0, ttl 128, id 26472, offset 0, flags [DF], proto ICMP (1), length 84)
    knoxville.nslab > 10.0.0.17: ICMP echo reply, id 3885, seq 1, length 64
15:13:26.159935 IP (tos 0x0, ttl 128, id 26473, offset 0, flags [DF], proto ICMP (1), length 84)
    knoxville.nslab > 10.0.0.17: ICMP echo reply, id 3885, seq 2, length 64
15:13:27.164155 IP (tos 0x0, ttl 128, id 26474, offset 0, flags [DF], proto ICMP (1), length 84)
    knoxville.nslab > 10.0.0.17: ICMP echo reply, id 3885, seq 3, length 64
15:13:28.163296 IP (tos 0x0, ttl 128, id 26475, offset 0, flags [DF], proto ICMP (1), length 84)
    knoxville.nslab > 10.0.0.17: ICMP echo reply, id 3885, seq 4, length 64
15:13:29.167969 IP (tos 0x0, ttl 128, id 26476, offset 0, flags [DF], proto ICMP (1), length 84)
    knoxville.nslab > 10.0.0.17: ICMP echo reply, id 3885, seq 5, length 64
15:13:30.170716 IP (tos 0x0, ttl 128, id 26477, offset 0, flags [DF], proto ICMP (1), length 84)
    knoxville.nslab > 10.0.0.17: ICMP echo reply, id 3885, seq 6, length 64
15:13:31.173480 IP (tos 0x0, ttl 128, id 26478, offset 0, flags [DF], proto ICMP (1), length 84)
    knoxville.nslab > 10.0.0.17: ICMP echo reply, id 3885, seq 7, length 64
15:13:32.187038 IP (tos 0x0, ttl 128, id 26479, offset 0, flags [DF], proto ICMP (1), length 84)
    knoxville.nslab > 10.0.0.17: ICMP echo reply, id 3885, seq 8, length 64
15:13:33.176471 IP (tos 0x0, ttl 128, id 26480, offset 0, flags [DF], proto ICMP (1), length 84)
    knoxville.nslab > 10.0.0.17: ICMP echo reply, id 3885, seq 9, length 64
15:13:34.180520 IP (tos 0x0, ttl 128, id 26481, offset 0, flags [DF], proto ICMP (1), length 84)
    knoxville.nslab > 10.0.0.17: ICMP echo reply, id 3885, seq 10, length 64
15:19:56.505932 IP (tos 0x0, ttl 128, id 26507, offset 0, flags [DF], proto ICMP (1), length 84)
    knoxville.nslab > 10.0.0.17: ICMP echo reply, id 3983, seq 1, length 64
15:19:57.501794 IP (tos 0x0, ttl 128, id 26508, offset 0, flags [DF], proto ICMP (1), length 84)
    knoxville.nslab > 10.0.0.17: ICMP echo reply, id 3983, seq 2, length 64
15:19:58.506325 IP (tos 0x0, ttl 128, id 26509, offset 0, flags [DF], proto ICMP (1), length 84)
    knoxville.nslab > 10.0.0.17: ICMP echo reply, id 3983, seq 3, length 64
```

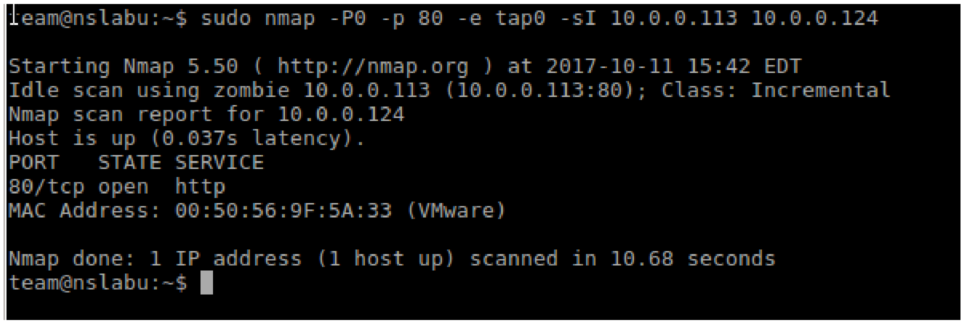
9. **The output of your nmap idle scan.**



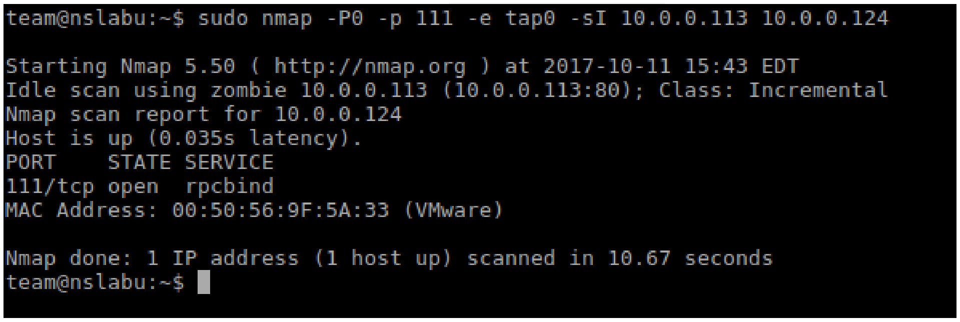
```
team@nslabu:~$ sudo nmap -P0 -p 443 -e tap0 -sI 10.0.0.113 10.0.0.124

Starting Nmap 5.50 ( http://nmap.org ) at 2017-10-11 15:39 EDT
Idle scan using zombie 10.0.0.113 (10.0.0.113:80); Class: Incremental
Nmap scan report for 10.0.0.124
Host is up (0.021s latency).
PORT    STATE           SERVICE
443/tcp closed|filtered https
MAC Address: 00:50:56:9F:5A:33 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 10.86 seconds
team@nslabu:~$
```



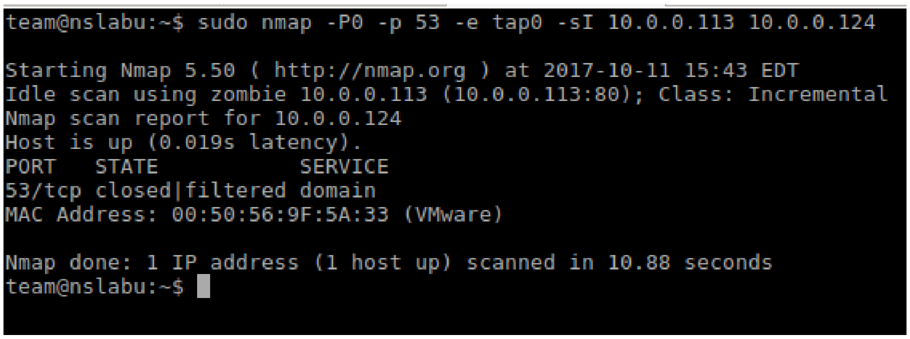
```
team@nslabu:~$ sudo nmap -P0 -p 22 -e tap0 -sI 10.0.0.113 10.0.0.124

Starting Nmap 5.50 ( http://nmap.org ) at 2017-10-11 15:40 EDT
Idle scan using zombie 10.0.0.113 (10.0.0.113:80); Class: Incremental
Nmap scan report for 10.0.0.124
Host is up (0.035s latency).
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:50:56:9F:5A:33 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 10.68 seconds
team@nslabu:~$
```



```
team@nslabu:~$ sudo nmap -P0 -p 80 -e tap0 -sI 10.0.0.113 10.0.0.124

Starting Nmap 5.50 ( http://nmap.org ) at 2017-10-11 15:42 EDT
Idle scan using zombie 10.0.0.113 (10.0.0.113:80); Class: Incremental
Nmap scan report for 10.0.0.124
Host is up (0.037s latency).
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:50:56:9F:5A:33 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 10.68 seconds
team@nslabu:~$
```



```
team@nslabu:~$ sudo nmap -P0 -p 111 -e tap0 -sI 10.0.0.113 10.0.0.124

Starting Nmap 5.50 ( http://nmap.org ) at 2017-10-11 15:43 EDT
Idle scan using zombie 10.0.0.113 (10.0.0.113:80); Class: Incremental
Nmap scan report for 10.0.0.124
Host is up (0.035s latency).
PORT    STATE SERVICE
111/tcp open  rpcbind
MAC Address: 00:50:56:9F:5A:33 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 10.67 seconds
team@nslabu:~$
```



```
team@nslabu:~$ sudo nmap -P0 -p 53 -e tap0 -sI 10.0.0.113 10.0.0.124

Starting Nmap 5.50 ( http://nmap.org ) at 2017-10-11 15:43 EDT
Idle scan using zombie 10.0.0.113 (10.0.0.113:80); Class: Incremental
Nmap scan report for 10.0.0.124
Host is up (0.019s latency).
PORT   STATE           SERVICE
53/tcp closed|filtered domain
MAC Address: 00:50:56:9F:5A:33 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 10.88 seconds
team@nslabu:~$
```

**10. What method does nmap use by default to ping a host?**

By default, nmap performs a SYN scan. Though it substitutes to a connect scan if the user does not have proper privileges to send raw packets. While using nmap unprivileged users can only execute FTP bounce scan and connect scans.

**11. Describe how you could use icmp_ratelimit kernel parameter in Linux to slow down a UDP scan.**

The icmp_ratelimit kernel parameter limits the maximum rate at which ICMP packets are sent to a target. In other words, it is the time the kernel waits between sending two ICMP packets. By default, it is set to 1000 and can be totally disabled if set to 0.

By increasing the value of this parameter, the UDP scan can be slowed down.

12. **Which nmap scan typically runs faster, -sS or -sT? Why?**

    The -sS (TCP SYN scan) typically runs faster than the -sT (TCP connect scan). The SYN scan can scan thousands of ports per second on a network without being hampered by restrictive firewalls. This is also known as half-open scanning because, we don't open a full TCP connection. We send a SYN packet as if we are going to connect and then wait for a response. Depending on the response the ports are categorized into 'open', 'closed' and 'filtered'.

    But in case of the TCP connect scan, instead of writing raw packets nmap asks the operating system to establish a connection with the target machine and port by issuing a connect system call. The system call completes connection to the open target ports rather than performing the half-open reset as done in the SYN scan. This takes longer and requires more packets to gather the same information. It is also not very stealthy as the target machine may log the connection.

13. **In general, if any port scanner sends a datagram to a specific UDP port on a system and receives NO response, what can be concluded without any other information? (Hint: see the nmap man page, and consider networks which use firewalls.)**

    There are various states in which a TCP/UDP port can be – OPEN, CLOSED etc. One of the states is FILTERED where the port is open but packet filtering prevents the NMAP probe from reaching the port.

    Such type of filtering can be done by a firewall device, or rules configured in a router or a host. When a nmap is performed on such ports, it usually does not give back a reply or sometimes gives a message Destination Unreachable.

14. **When running an idle scan against a victim, what happens if a specific port's SYN packets are dropped by the victim's firewall? How does this look to the attacker as compared to an open or closed port? If the scan target were running a tar-pit on every un-used TCP port, how effective would an idle scan be? For more background on this last question, you may want to search for "iptables TARPIT" on the web.**

    The idle scan uses the IP ID (fragment identification number) of the zombie host to determine whether the port on the target machine is open or closed. The attacker first probes the zombie hosts IP ID and records it, it then fabricates a SYN packet from the zombie and sends it to the desired port on the target. Then it probes the IP ID of the zombie again. The state of the port is determined by comparing the IP IDs of the zombie host. If the IP ID is incremented by 2 that means the port on the target system is open. If it has been incremented by 1 then the target port is either closed or filtered.

    If the victim's firewall is dropping the SYN packets then the zombie host will not receive the SYN/ACK packet from the victim's port and the IP ID will not be incremented. So the attacker will see an increase of just 1 in the IP ID and assume that the port is either closed or filtered.

    If the target is running a tar-pit on every un-used TCP port, then the attacker will think they are all closed. This is because, tap-pit implements the idea of 'greylisting' users. That is, if any connection request comes from an unseen IP address then the firewall drops the first connection. A legitimate user will try again but an attacker will be discouraged by this.

    Even if the zombie host being used by the attacker is known to the system the tar-pit firewall will delay the connection for some time and the attacker will either loose interest or will conclude that the port is not responding and is either closed or filtered.

15. **There are a number of ways that IP stacks can be written to reduce or eliminate the information leak of system-wide incremental IP IDs. How does Linux's IP stack defend against this? Name two techniques. See the "OS Vendors" section in this previously mentioned reference. How do these help defend against side-channel attacks?**

    Incremental IP IDs make idle scans possible. If the zombie hosts IP ID is incremented any way other than an incremental fashion, then the attacker will have no way to tell if the ports were open or closed.

    Different Linux systems take different approaches to tackle this problem. Solaris uses peer-specific IP ID values. This severely limits the information an attacker can gain from the zombie host. In Linux 2.4 systems the IP IDs are set to zero and the DF (don't fragment) bit is also set to true, so IP ID fragmentation doesn't take place at all.

    Another approach is to use completely randomized IP ID sequences. The same random IP ID will not be repeated in a short time span. These techniques make it very difficult for the attacker to use idle scanning and make use of the incremental IP ID flaw in the system to scan other targets using the system using incremental method as a zombie host.

16. **Describe your results using ZMap scanning the virtual network. Discuss the differences between nmap and ZMap, in terms of design, functionality, techniques, and performance.**

    Command -

    ```
    sudo zmap -i tap0 -G ae:f4:23:74:08:33 -p 80 -o output.txt 10.0.0.64/26
    ```

    Design & Functionality –

    Zmap has optimized probing, does not store state of each connection (stateless) and hence does not retransmit packets that are lost.

    One of the other major difference is that Nmap is ideal for scanning multiple open ports over a small number of hosts whereas Zmap is optimized to probe a single port over a very large number of hosts.

    Performance – Zmap can scan the entire IPv4 public address space over 1300 time faster than Nmap.