EXP:08	NMAP to Discover Live Hosts Using Nmap Scans (ARP, ICMP, TCP/UDP) on the TryHackMe Platform

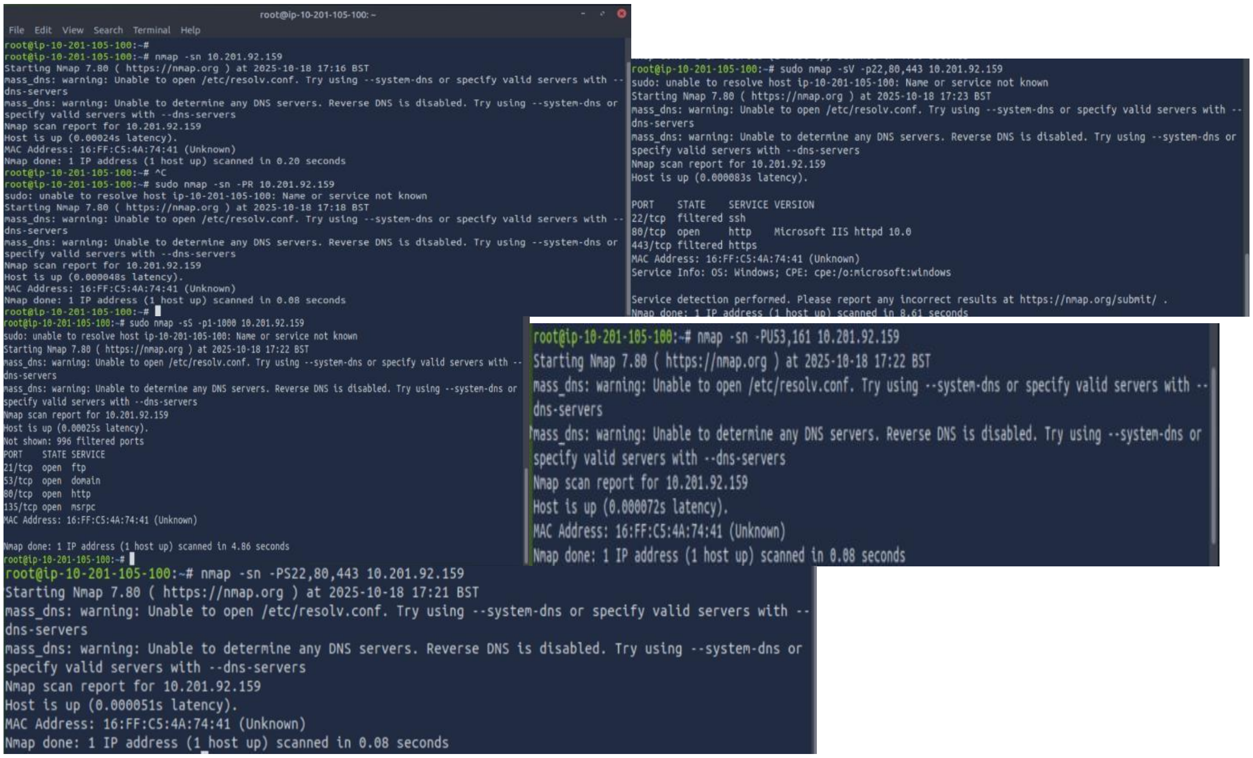
Aim

To use the **Nmap** tool to discover live hosts and analyze network services using various scan types (ARP, ICMP, TCP/UDP).

Algorithm / Procedure

1. **Access** the TryHackMe platform environment (or a similar controlled lab environment).
2. **Execute** an ARP scan (`nmap -sn -PR`) on the local subnet to discover active hosts.
3. **Execute** an ICMP echo request scan (`nmap -sn -PE`) to discover hosts that respond to ping.
4. **Perform** a TCP SYN scan (`nmap -sS`) on a target host to identify open ports.
5. **Perform** a UDP scan (`nmap -sU`) on a target host to identify open UDP services.
6. **Analyze** the results of each scan to understand the host's status and running services.

Output:

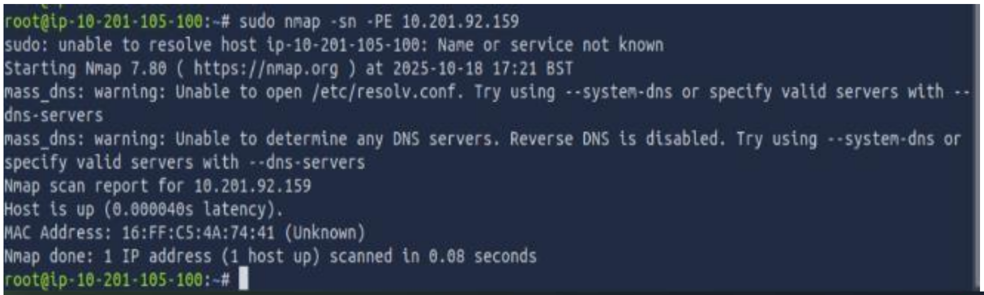

root@ip-10-201-105-100: ~
File Edit View Search Terminal Help

```
root@ip-10-201-105-100:~#
root@ip-10-201-105-100:~# nmap -sn 10.201.92.159
Starting Nmap 7.80 ( https://nmap.org ) at 2025-10-18 17:16 BST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --
dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or
specify valid servers with --dns-servers
Nmap scan report for 10.201.92.159
Host is up (0.00024s latency).
MAC Address: 16:FF:C5:4A:74:41 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
root@ip-10-201-105-100:~# ^C
root@ip-10-201-105-100:~# sudo nmap -sn -PR 10.201.92.159
sudo: unable to resolve host ip-10-201-105-100: Name or service not known
Starting Nmap 7.80 ( https://nmap.org ) at 2025-10-18 17:18 BST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --
dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or
specify valid servers with --dns-servers
Nmap scan report for 10.201.92.159
Host is up (0.000048s latency).
MAC Address: 16:FF:C5:4A:74:41 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
root@ip-10-201-105-100:~#
root@ip-10-201-105-100:~# sudo nmap -sS -p1-1000 10.201.92.159
sudo: unable to resolve host ip-10-201-105-100: Name or service not known
Starting Nmap 7.80 ( https://nmap.org ) at 2025-10-18 17:22 BST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --
dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or
specify valid servers with --dns-servers
Nmap scan report for 10.201.92.159
Host is up (0.00025s latency).
Not shown: 996 filtered ports
PORT    STATE SERVICE
21/tcp  open  ftp
53/tcp  open  domain
80/tcp  open  http
135/tcp open  msrpc
MAC Address: 16:FF:C5:4A:74:41 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 4.86 seconds
root@ip-10-201-105-100:~#
```

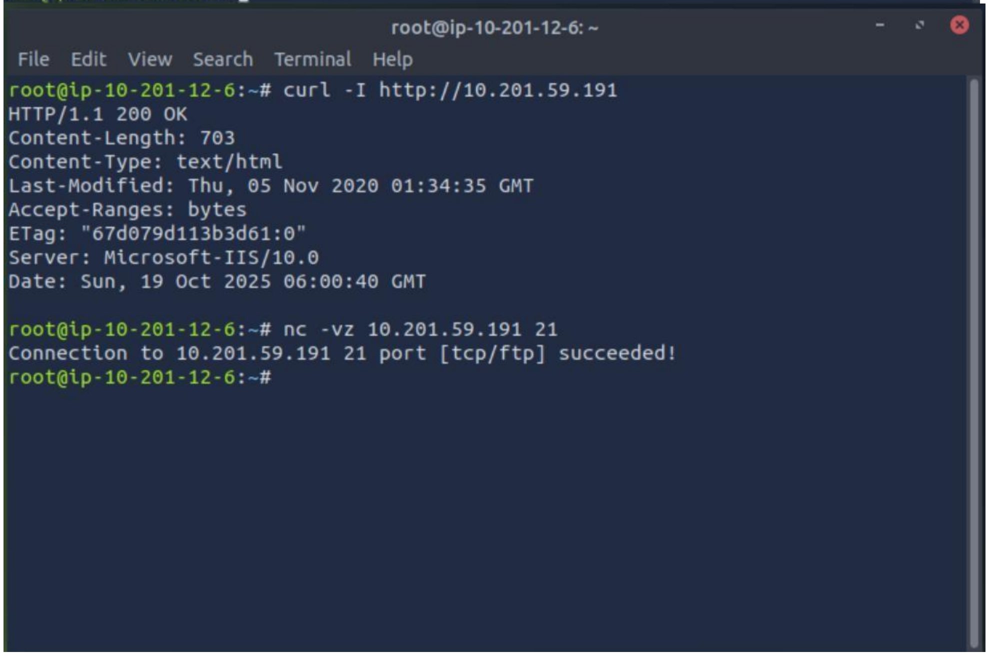
```
root@ip-10-201-105-100:~# sudo nmap -sV -p22,80,443 10.201.92.159
sudo: unable to resolve host ip-10-201-105-100: Name or service not known
Starting Nmap 7.80 ( https://nmap.org ) at 2025-10-18 17:23 BST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --
dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or
specify valid servers with --dns-servers
Nmap scan report for 10.201.92.159
Host is up (0.000083s latency).

PORT    STATE    SERVICE VERSION
22/tcp  filtered ssh
80/tcp  open     http    Microsoft IIS httpd 10.0
443/tcp filtered https
MAC Address: 16:FF:C5:4A:74:41 (Unknown)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.61 seconds
```

```
root@ip-10-201-105-100:~# nmap -sn -PU53,161 10.201.92.159
Starting Nmap 7.80 ( https://nmap.org ) at 2025-10-18 17:22 BST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --
dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or
specify valid servers with --dns-servers
Nmap scan report for 10.201.92.159
Host is up (0.000072s latency).
MAC Address: 16:FF:C5:4A:74:41 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

```
root@ip-10-201-105-100:~# nmap -sn -PS22,80,443 10.201.92.159
Starting Nmap 7.80 ( https://nmap.org ) at 2025-10-18 17:21 BST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --
dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or
specify valid servers with --dns-servers
Nmap scan report for 10.201.92.159
Host is up (0.000051s latency).
MAC Address: 16:FF:C5:4A:74:41 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```



```
root@ip-10-201-105-100:~# sudo nmap -sn -PE 10.201.92.159
sudo: unable to resolve host ip-10-201-105-100: Name or service not known
Starting Nmap 7.80 ( https://nmap.org ) at 2025-10-18 17:21 BST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --
dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or
specify valid servers with --dns-servers
Nmap scan report for 10.201.92.159
Host is up (0.000040s latency).
MAC Address: 16:FF:C5:4A:74:41 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
root@ip-10-201-105-100:~# 
```



```
root@ip-10-201-12-6:~# curl -I http://10.201.59.191
HTTP/1.1 200 OK
Content-Length: 703
Content-Type: text/html
Last-Modified: Thu, 05 Nov 2020 01:34:35 GMT
Accept-Ranges: bytes
ETag: "67d079d113b3d61:0"
Server: Microsoft-IIS/10.0
Date: Sun, 19 Oct 2025 06:00:40 GMT

root@ip-10-201-12-6:~# nc -vz 10.201.59.191 21
Connection to 10.201.59.191 21 port [tcp/ftp] succeeded!
root@ip-10-201-12-6:~#
```

Result

Nmap was successfully used to perform various network scans. Live hosts were discovered, and the status of TCP and UDP ports was analyzed, demonstrating the utility of Nmap for network reconnaissance.