

Submitted By Gurbaksh Lal

Roll No.: 2023PCS2029

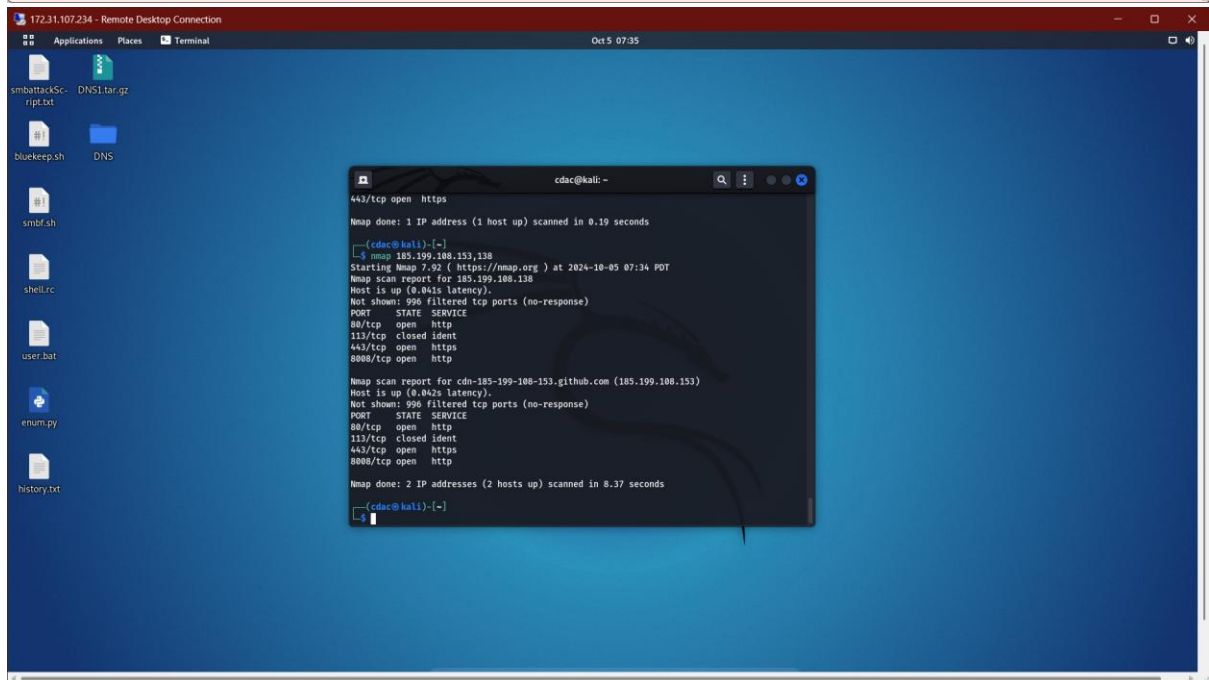
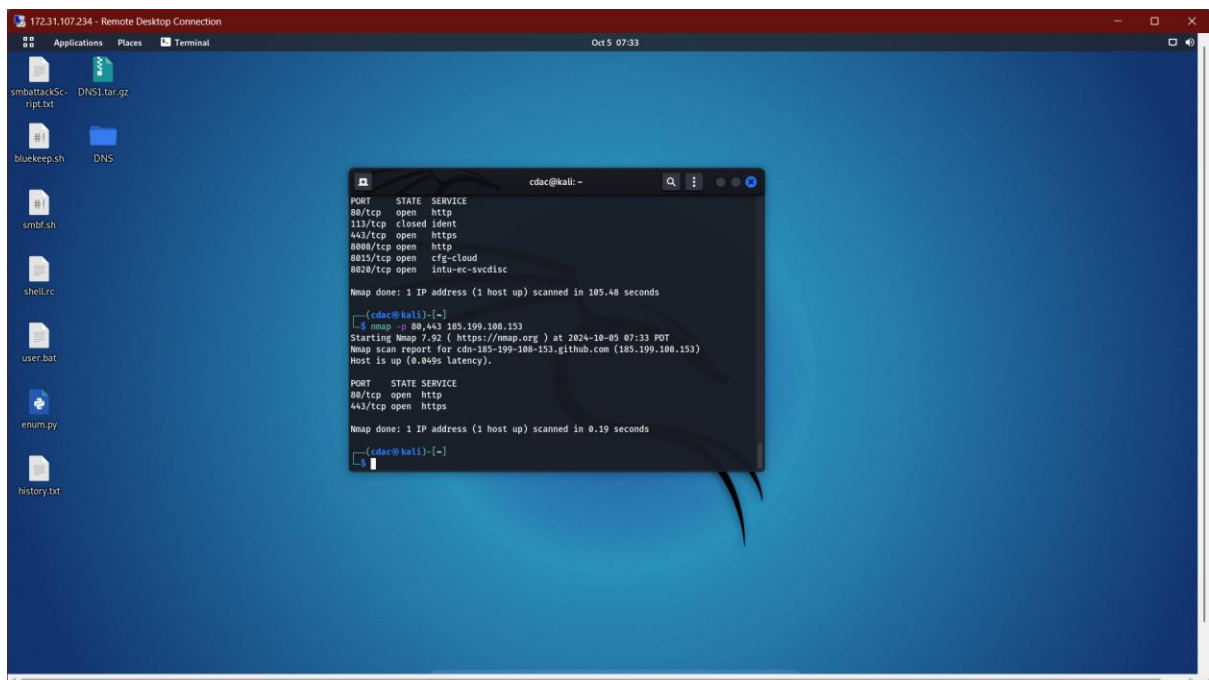
User id: gurbaksh.lal.pg23@nsut.ac.in

The screenshot shows a Kali Linux desktop environment with a blue background. On the left sidebar, there are icons for 'smbattackScript.txt', 'DNS1.tar.gz', 'bluekeep.sh', 'DNS', 'smbf.sh', 'shell.rc', 'user.bat', 'enum.py', and 'history.txt'. The top bar indicates a 'Remote Desktop Connection' to '172.31.107.234' at 'Oct 4 12:35'. A terminal window is open in the center, displaying the following Nmap scan results:

```
cdac@kali: ~  
[cdac@kali]~  
$ nmap www.cdac.in  
Starting Nmap 7.92 ( https://nmap.org ) at 2024-10-04 12:34 PDT  
Nmap scan report for www.cdac.in (196.1.1.30)  
Host is up (0.025s latency).  
Other addresses for www.cdac.in (not scanned): 2405:8a00:6029::45  
Not shown: 996 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
80/tcp    open  http  
113/tcp   closed ident  
443/tcp   open  https  
8000/tcp   open  http  
  
Nmap done: 1 IP address (1 host up) scanned in 4.10 seconds  
[cdac@kali]~  
$ nmap 185.199.108.153  
Starting Nmap 7.92 ( https://nmap.org ) at 2024-10-04 12:34 PDT  
Nmap scan report for cdn-185-199-108-153.github.com (185.199.108.153)  
Host is up (0.040s latency).  
Not shown: 996 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
80/tcp    open  http  
113/tcp   closed ident  
443/tcp   open  https  
8000/tcp   open  http  
  
Nmap done: 1 IP address (1 host up) scanned in 5.10 seconds  
[cdac@kali]~  
$
```

The screenshot shows the same Kali Linux desktop environment as the previous one, but at 'Oct 4 12:46'. The terminal window displays the following Nmap scan results:

```
cdac@kali: ~  
[cdac@kali]~  
$ nmap 185.199.108.153  
Starting Nmap 7.92 ( https://nmap.org ) at 2024-10-04 12:34 PDT  
Nmap scan report for cdn-185-199-108-153.github.com (185.199.108.153)  
Host is up (0.040s latency).  
Not shown: 996 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
80/tcp    open  http  
113/tcp   closed ident  
443/tcp   open  https  
8000/tcp   open  http  
  
Nmap done: 1 IP address (1 host up) scanned in 5.10 seconds  
[cdac@kali]~  
$ nmap -i- 185.199.108.153  
Starting Nmap 7.92 ( https://nmap.org ) at 2024-10-04 12:37 PDT  
Nmap scan report for cdn-185-199-108-153.github.com (185.199.108.153)  
Host is up (0.041s latency).  
Not shown: 65529 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
80/tcp    open  http  
113/tcp   closed ident  
443/tcp   open  https  
8000/tcp   open  http  
8015/tcp   open  cifs-cloud  
8020/tcp   open  intu-ec-svcdisc  
  
Nmap done: 1 IP address (1 host up) scanned in 105.23 seconds  
[cdac@kali]~  
$
```



```
172.31.107.234 - Remote Desktop Connection
Applications Places Terminal
Oct 5 07:40
cdac@kali: ~

Nmap done: 2 IP addresses (2 hosts up) scanned in 8.37 seconds

--(cdac@kali)-[~]
_ _ $ nmap 185.199.108.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2024-10-05 07:36 PDT
Nmap scan report for 185.199.108.0
Host is up (0.043s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
113/tcp   closed ident
443/tcp    open  https
8080/tcp   open  http

Nmap scan report for 185.199.108.1
Host is up (0.043s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
113/tcp   closed ident
443/tcp    open  https
8080/tcp   open  http

Nmap scan report for 185.199.108.2
Host is up (0.043s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
113/tcp   closed ident
443/tcp    open  https
8080/tcp   open  http

Nmap scan report for 185.199.108.3
Host is up (0.042s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
113/tcp   closed ident
443/tcp    open  https
8080/tcp   open  http

Nmap scan report for 185.199.108.4
Host is up (0.043s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
113/tcp   closed ident
443/tcp    open  https
8080/tcp   open  http

Nmap scan report for 185.199.108.5
```

```
172.31.107.234 - Remote Desktop Connection
Applications Places Terminal
Oct 5 07:40
cdac@kali: ~

smbattackerSc-ript.txt DNS: target
bluekeep.sh DNS
smbf.sh
shell.rc
user.bat
enum.py
history.txt

Nmap scan report for 185.199.108.253
Host is up (0.046s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
113/tcp   closed ident
443/tcp    open  https
8080/tcp   open  http

Nmap scan report for 185.199.108.254
Host is up (0.046s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
113/tcp   closed ident
443/tcp    open  https
8080/tcp   open  http

Nmap scan report for 185.199.108.255
Host is up (0.041s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
113/tcp   closed ident
443/tcp    open  https
8080/tcp   open  http

Nmap done: 256 IP addresses (256 hosts up) scanned in 217.47 seconds

--(cdac@kali)-[~]
_ _ $
```

