Assignment: Active Banner Grabbing

Submitted By: Tayyab

Site: techjuice.pk

IP Address: 172.67.138.208

Open ports to scan: 80,443

Closed ports to scan: 21,22

Initial Scan to check ports:

```
┌──(anon㉿kali)-[~]
└─$ sudo nmap -p 21,22,80,443 172.67.138.208

[sudo] password for anon:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-28 00:50 PKT
Nmap scan report for 172.67.138.208
Host is up (0.051s latency).

PORT    STATE    SERVICE
21/tcp  filtered ftp
22/tcp  filtered ssh
80/tcp  open     http
443/tcp open     https

Nmap done: 1 IP address (1 host up) scanned in 1.67 seconds
```

Test 1: A TCP packet with the SYN and ECN-Echo flags enabled is sent to an open TCP port.

```
┌──(anon㉿kali)-[~]
└─$ sudo nmap --scanflags SYN,ECN -p80,443  172.67.138.208

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-28 00:50 PKT
Nmap scan report for 172.67.138.208
Host is up (0.031s latency).

PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
```

Test 2: A TCP packet with no flags enabled is sent to an open TCP port. This type of packet is a NULL packet.

```
┌──(anon㉿kali)-[~]
└─$ sudo nmap -sN -p 80,443 172.67.138.208

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-28 00:52 PKT
Nmap scan report for 172.67.138.208
Host is up (0.0011s latency).

PORT    STATE         SERVICE
80/tcp  open|filtered http
443/tcp open|filtered https

Nmap done: 1 IP address (1 host up) scanned in 1.33 seconds
```

Test 3: A TCP packet with the URG, PSH, SYN, and FIN flags enabled is sent to an open TCP port.

```
┌──(anon㉿kali)-[~]
└─$ sudo nmap --scanflags URG,PSH,SYN,FIN -p 80,443 172.67.138.208

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-28 00:53 PKT
Nmap scan report for 172.67.138.208
Host is up (0.040s latency).

PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
```

Test 4: A TCP packet with the ACK flag enabled is sent to an open TCP port.

```
┌──(anon㉿kali)-[~]
└─$ sudo nmap -sA -p 80,443 172.67.138.208

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-28 00:53 PKT
Nmap scan report for 172.67.138.208
Host is up (0.0015s latency).

PORT    STATE      SERVICE
80/tcp  unfiltered http
443/tcp unfiltered https

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```

Test 5: A TCP packet with the SYN flag enabled is sent to a closed TCP port.

```
┌──(anon㉿kali)-[~]
└─$ sudo nmap -sS -p 21,22 172.67.138.208

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-28 00:53 PKT
Nmap scan report for 172.67.138.208
Host is up (0.0012s latency).

PORT   STATE    SERVICE
21/tcp filtered ftp
22/tcp filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 1.35 seconds
```

Test 6: A TCP packet with the ACK flag enabled is sent to a closed TCP port.

```
┌──(anon㉿kali)-[~]
└─$ sudo nmap -sA -p 21,22 172.67.138.208

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-28 00:54 PKT
Nmap scan report for 172.67.138.208
Host is up (0.0011s latency).

PORT   STATE      SERVICE
21/tcp unfiltered ftp
22/tcp unfiltered ssh

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
```

Test 7: A TCP packet with the URG, PSH, and FIN flags enabled is sent to a closed TCP port.

```
┌──(anon㉿kali)-[~]
└─$ sudo nmap --scanflags URG,PSH,FIN -p 21,22 172.67.138.208

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-28 00:55 PKT
Nmap scan report for 172.67.138.208
Host is up (0.0010s latency).

PORT   STATE    SERVICE
21/tcp filtered ftp
22/tcp filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 1.36 seconds
```