Nmap Firewall Spoofing

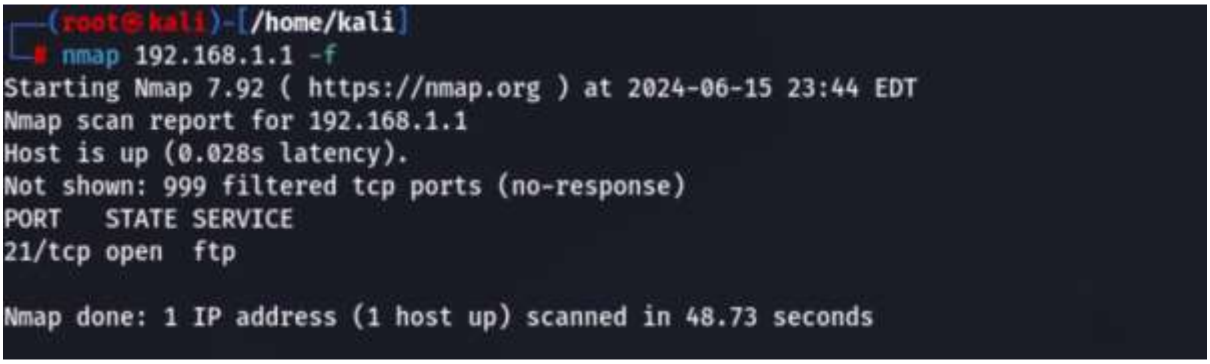
Nmap offers various techniques for firewall and intrusion detection system (IDS) evasion, commonly referred to as firewall spoofing. These techniques help network administrators and security professionals conduct more accurate security assessments by bypassing defensive measures that may block or alter scan results. Firewall spoofing techniques involve manipulating packet attributes and using stealth scanning methods to avoid detection and blocking by firewalls and IDS.

One of the common methods is the TCP SYN scan (`-sS`), also known as half-open scanning, which initiates a TCP connection without completing the handshake, making it less likely to be logged by the target system. Another technique is using decoys (`-D`), where Nmap sends scan packets from multiple spoofed IP addresses, complicating the task of identifying the real source of the scan. The `-f` option fragments packets, making it harder for firewalls and IDS to recognize and block the scan. Additionally, Nmap supports IP spoofing (`-S`) to send packets with a forged source address, making it appear as if the scan is coming from a different IP. The `--badsum` option sends packets with incorrect checksums, which are ignored by many firewalls but still processed by the target OS, helping bypass some filtering rules.

These techniques, among others, allow Nmap to conduct stealthy and efficient scans, providing security professionals with the ability to assess the security posture of networks and identify vulnerabilities that might otherwise go undetected due to firewall and IDS protections.

Examples: -

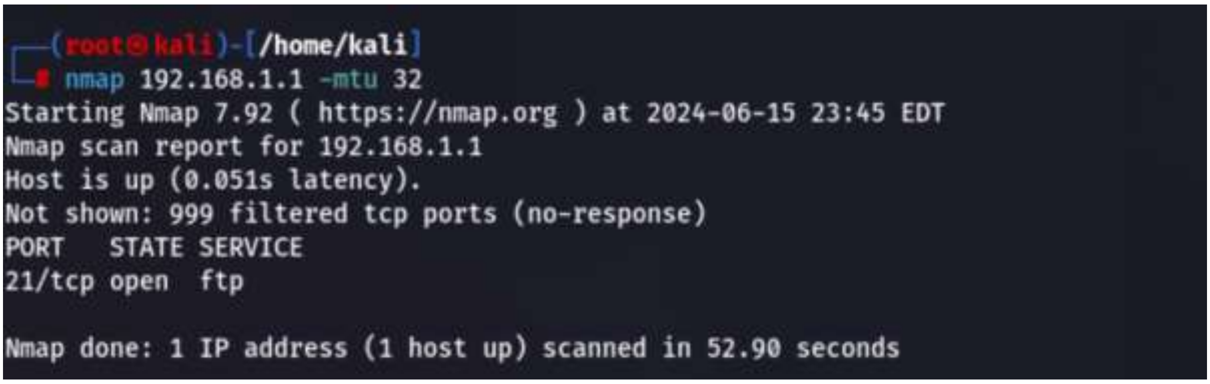
1. Here we requested scan (including ping scans) use tiny fragmented IP packets. It is harder for packet filters.



```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.1.1 -f
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-15 23:44 EDT
Nmap scan report for 192.168.1.1
Host is up (0.028s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
21/tcp open  ftp

Nmap done: 1 IP address (1 host up) scanned in 48.73 seconds
```

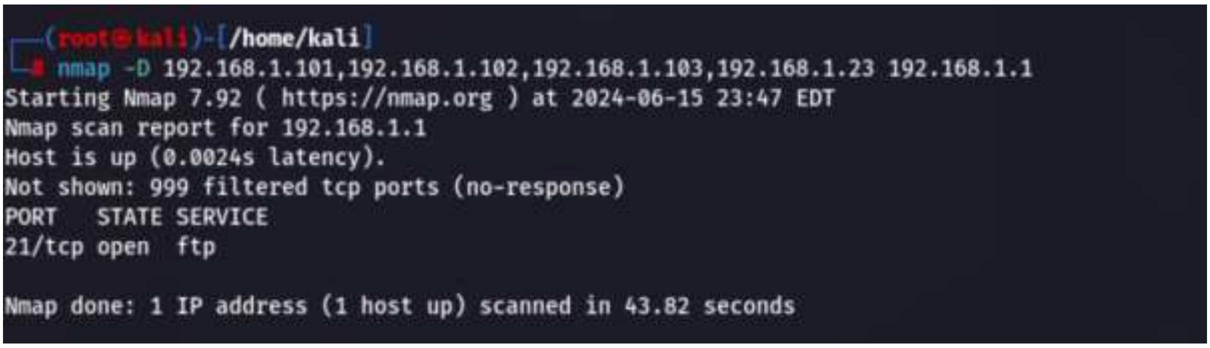
2. In this example we, set our own offset size i.e. 32.



```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.1.1 -mtu 32
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-15 23:45 EDT
Nmap scan report for 192.168.1.1
Host is up (0.051s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
21/tcp open  ftp

Nmap done: 1 IP address (1 host up) scanned in 52.90 seconds
```

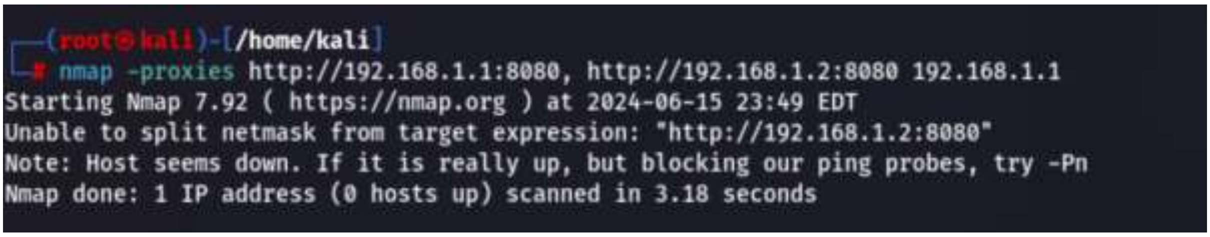
3. This -D Flag is used to send scans from spoofed IPs.



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -D 192.168.1.101,192.168.1.102,192.168.1.103,192.168.1.23 192.168.1.1
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-15 23:47 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0024s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
21/tcp open  ftp

Nmap done: 1 IP address (1 host up) scanned in 43.82 seconds
```

4. To relay connections through HTTP/SOCKS4 proxies we will use the -proxies flag.



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -proxies http://192.168.1.1:8080, http://192.168.1.2:8080 192.168.1.1
Starting Nmap 7.92 ( https://nmap.org ) at 2024-06-15 23:49 EDT
Unable to split netmask from target expression: "http://192.168.1.2:8080"
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.18 seconds
```