Scanning beyond Firewall & IDS

Before going further into this section, i should aware of the fact that these techniques might work in a CTF and controlled environment however the scanning techniques here does not guarantee results in real life as defensive technologies like Firewalls and IDS are very much evolved now and can most of the time thwart massive nmap scan packets. So, we have to realistic while performing these techniques on real websites.

On that note, lets get started.

- **Packet Fragmentation** - Packet Fragmentation refers to the splitting of a probe packet into several smaller packets called fragments while sending it to a network.

To perform this technique, we will use nmap -f flag.

```
sudo nmap -sS -sV -f IP
```

- **Source Port Manipulation** - Source port manipulation refers to manipulating actual port numbers with common port numbers in order to evade firewall or IDS.

Suppose a firewall only allow traffic to the network from port 80 (HTTP) only. In that case, we can use Source Port manipulation technique to send our traffic via port 80 to bypass the firewall rule.

To perform this, we can use nmap -g flag.

```
sudo nmap -g 80 IP
```

- **IP address decoy** - When performing a network scan, our real IP address is used as the source of the scan packets. So, this makes it easy for firewalls and IDS to detect and block the scan.

To avoid this, we can use IP address decoy technique. We can create random or specified decoy IP address with the help of nmap and then scan the target, in that way. Firewall will get confused which IP address to block and which to allow.

We can do this using two methods - one is the random one where we can specify a number and nmap will automatically create that much of random IP addresses to scan.

The other one is manual entrying the decoy IPs. This could be beneficial when you want to paint a target to a particular person or computer holding a particular IP address.

Lets see how we can perform the same. First we will look into the random one.

```
sudo nmap -D RND:10 IP
```

To entry the decoys manually. We just have to type them like

```
sudo nmap -D 192.168.29.110 192.168.29.111 192.168.29.112 192.168.29.113
192.168.29.114 IP
```

Keep in mind, that the decoy technique is not foolproof - Some firewalls and IDS can still detect that your real IP is sending more packets than the decoys. Using IP fragmentation and other evasion techniques in addition to decoys provides better results

- **Creating Custom Packets** - Firewalls are designed to inspect network traffic and block packets that match certain criteria, like particular content or data. Nmap scan probes has a particular kind of signature which these firewalls has adapted over the years. To bypass this filtering of our packets, we can append random data in our scans to confuse the firewall. Hence, bypassing it.

```
sudo nmap IP --data 0xinventyourshit

sudo nmap IP --data-string "Hack the Planet, Boisss"
```

- **Using proxies with nmap** - As we have already set up our proxychains with Tor. We can also use it to perform nmap scan on target and hiding our IP address eventually.

In the real world, there can be a issue with Tor as most of the websites on the internet block or scrutinise tor traffic. So, its better use residential proxies rather than tor to have better speed and consistent results.
