Advanced Computer Networks

SYN Flood Attack

Malicious actors can run a Denial of Service attack on a target IP address using a SYN-Flood attack – initiating many half-open TCP handshakes from many source IP addresses.

You were chosen to head the team of cyber-attack defenders – at your disposal is a Wireshark capture file recorded during the attack. You need to write a Python script that identifies the IP addresses of the attackers and saves them to a file.

https://data.cyber.org.il/networks/SYNflood.pcapng

Note:

1. Within your Python script, use Scapy to analyze the packets.
2. Scapy can read pcap files using the `rdpcap` command. For example:

```
pcapFile = rdpcap("SynFloodSample.pcap")
```

3. Packets can then be passed using a for loop such as:

```
for pkt in pcapFile:
    …
```

Good luck!

Capture file credit - https://blog.packet-foo.com/

Image generated by Avi Treistman on openart.ai