SPRING 2019

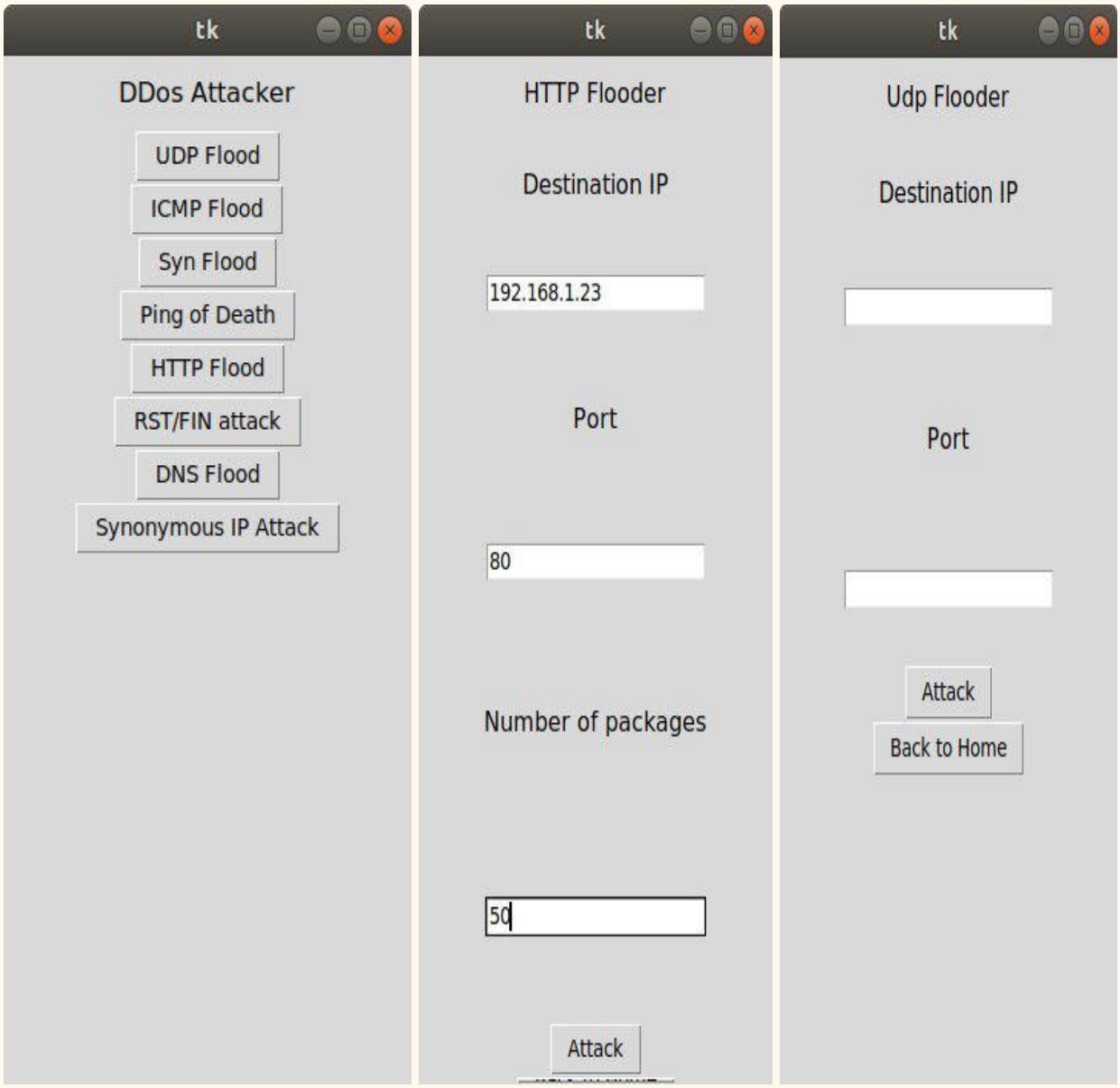
CS479 Project Report

Introduction to Cyber Security

Sara Jammal
Selin Özdaş
Berke Soysal
Cevat Barış Yılmaz

Project Type: DDoS Attack Tool

User Interface

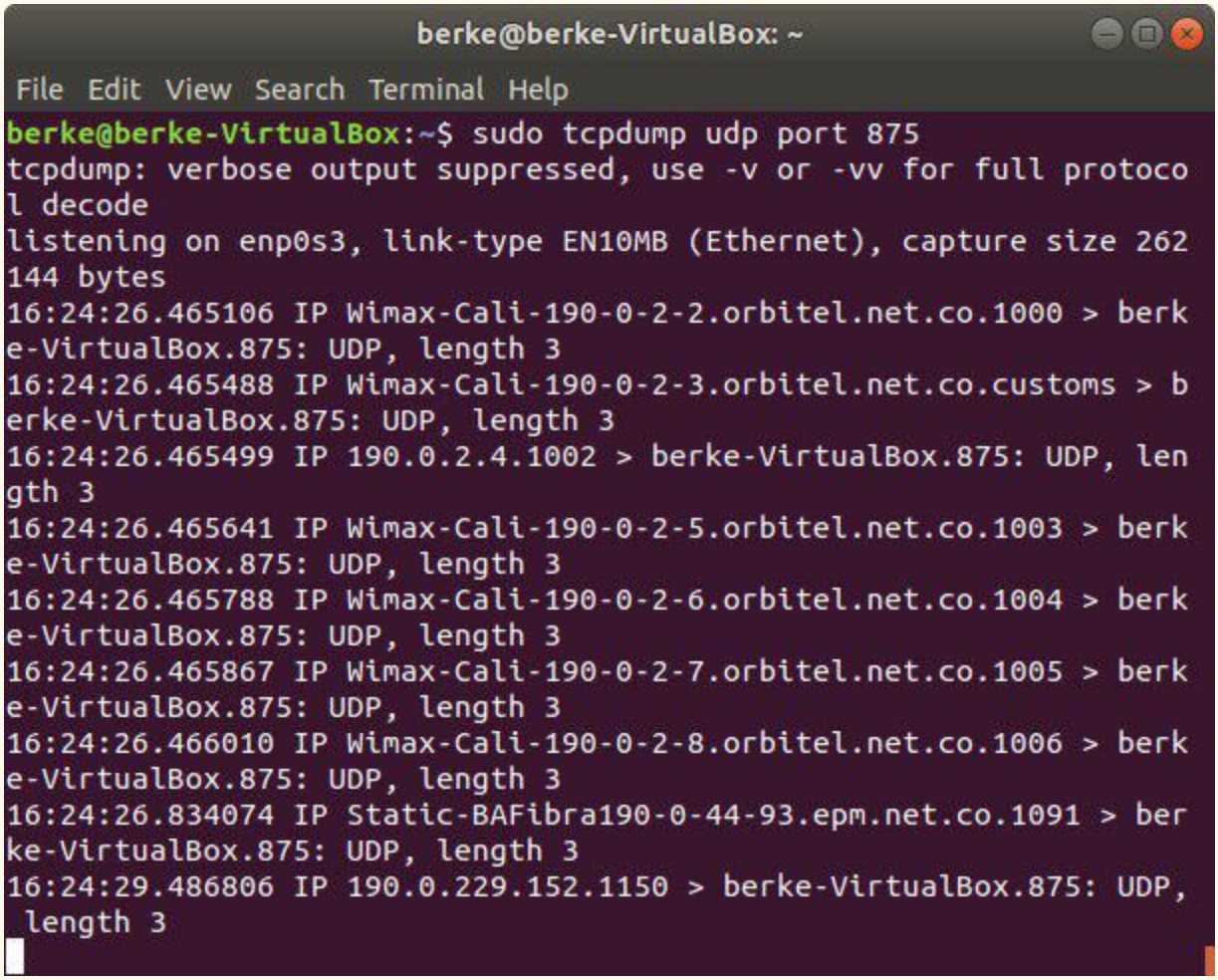


Attack Types

For our DDoS attack tool, we have implemented the following attacks. You can see the indicator of compromise screenshots of the attacks after the description of the attack:

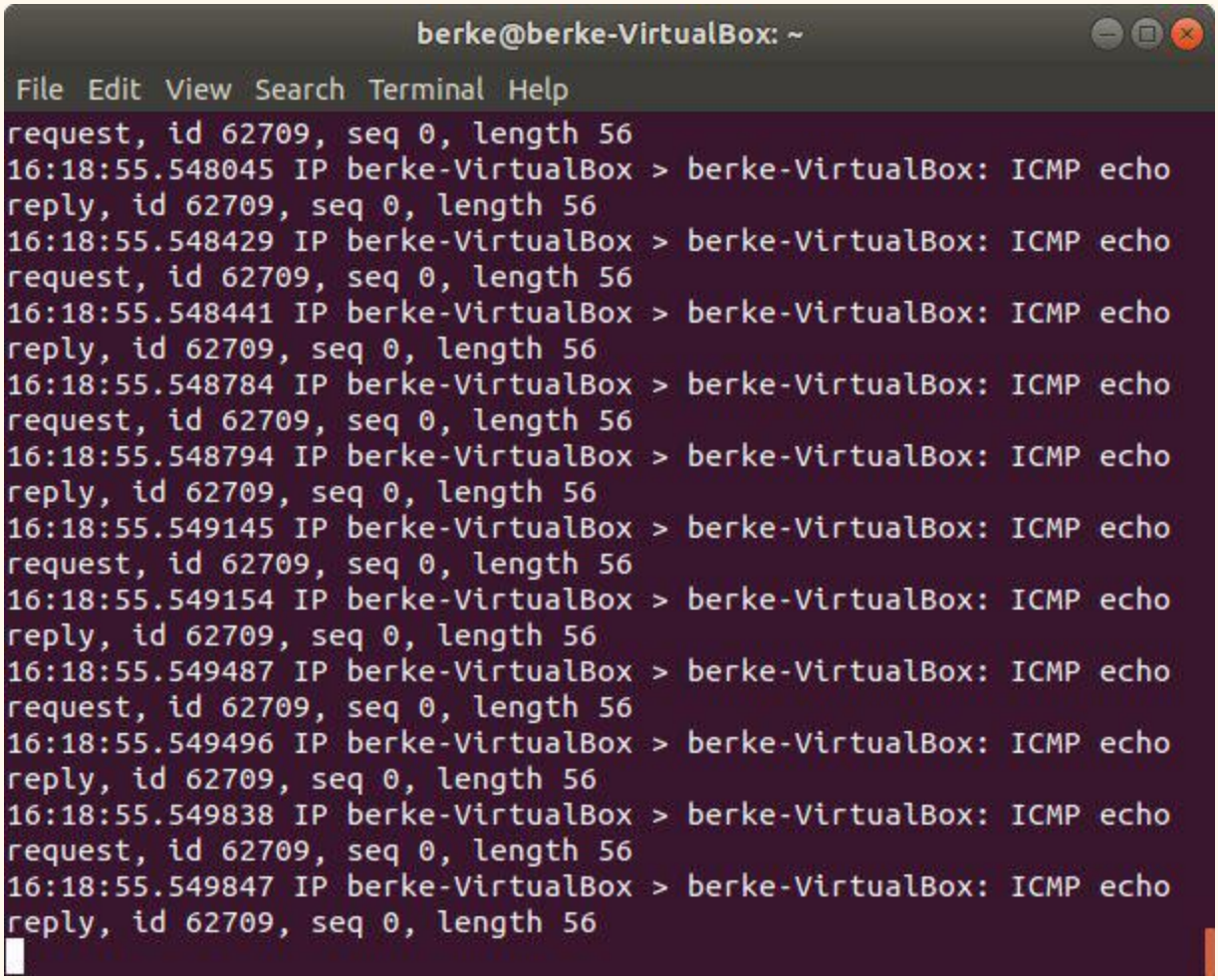
UDP Flood:

This attacks are created with sending a server a flood of User Datagram Protocol(UDP) packets.



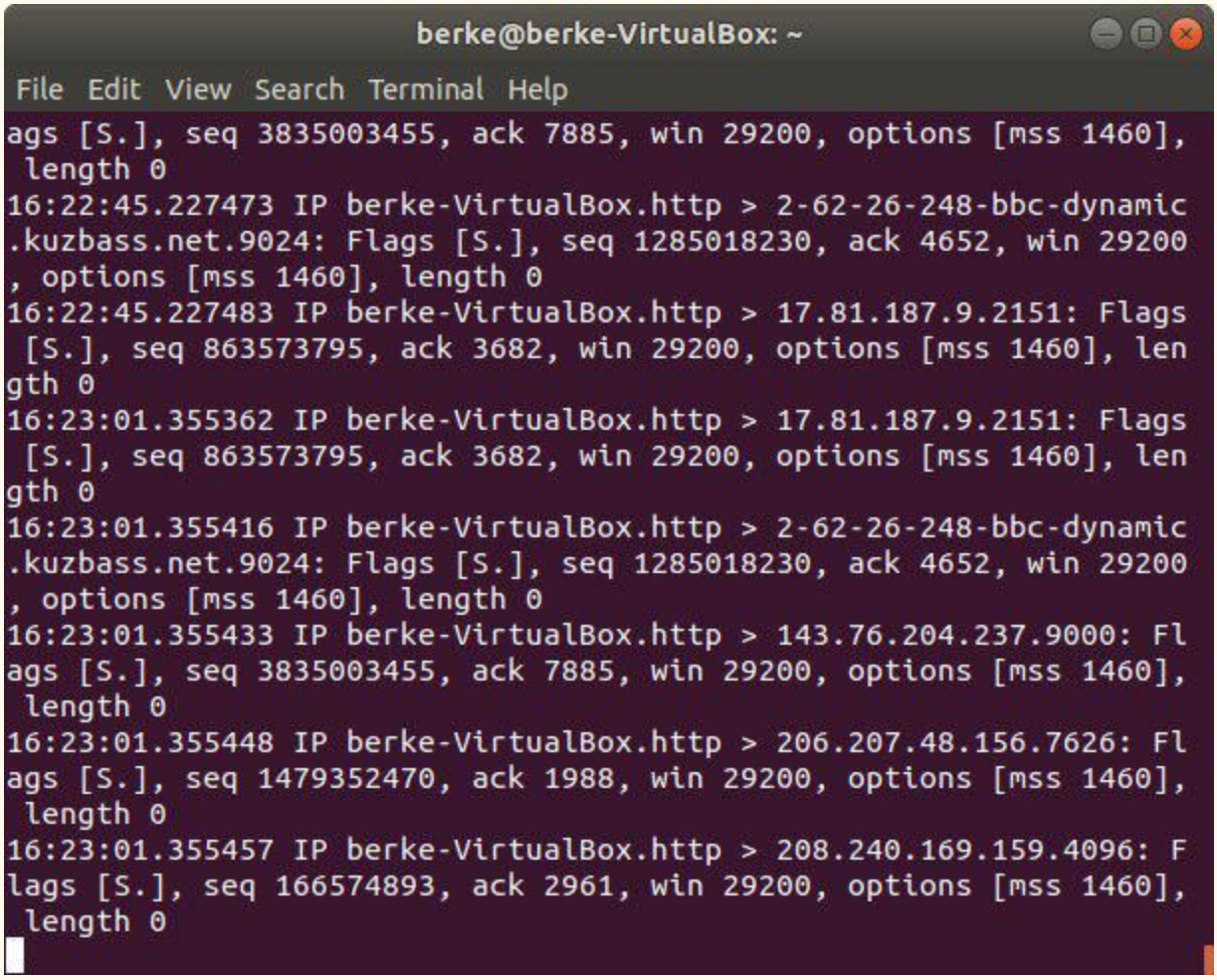
ICMP(ping) Flood:

This attack is similar to above one, an ICMP attack is executed by sending floods of ICMP Echo Request(ping) packets without waiting for reply, that results in a slow response for other users of the server.



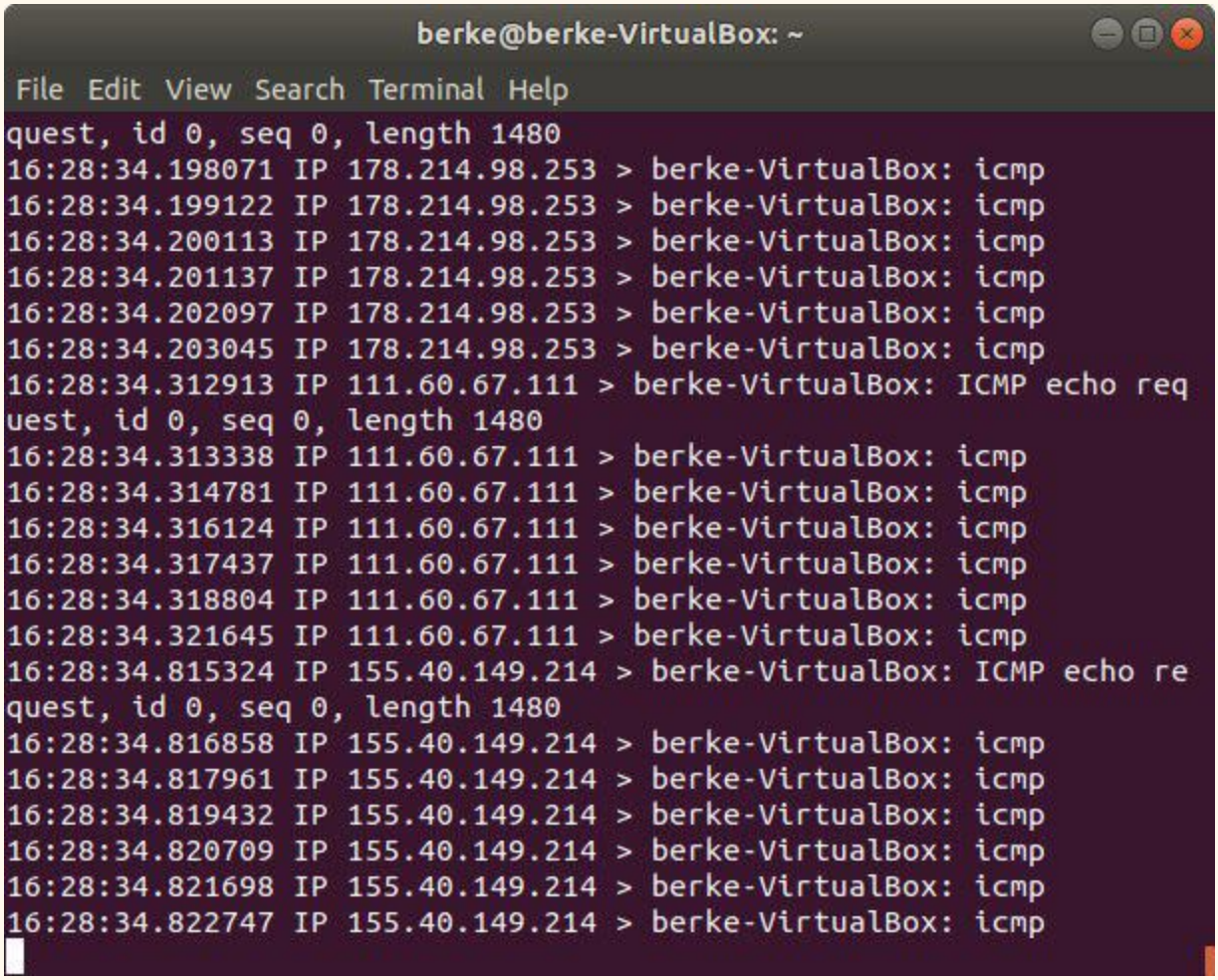
SYN Flood:

The tool is able to make SYN Flood attacks. It will exploit the weakness of TCP connection sequence ("three-way-handshake"). It sends numerous SYN packets to server, but it does not respond to server's SYN-ACK packets. As you can see there are SYN packets coming to the server with spoofed IP's.



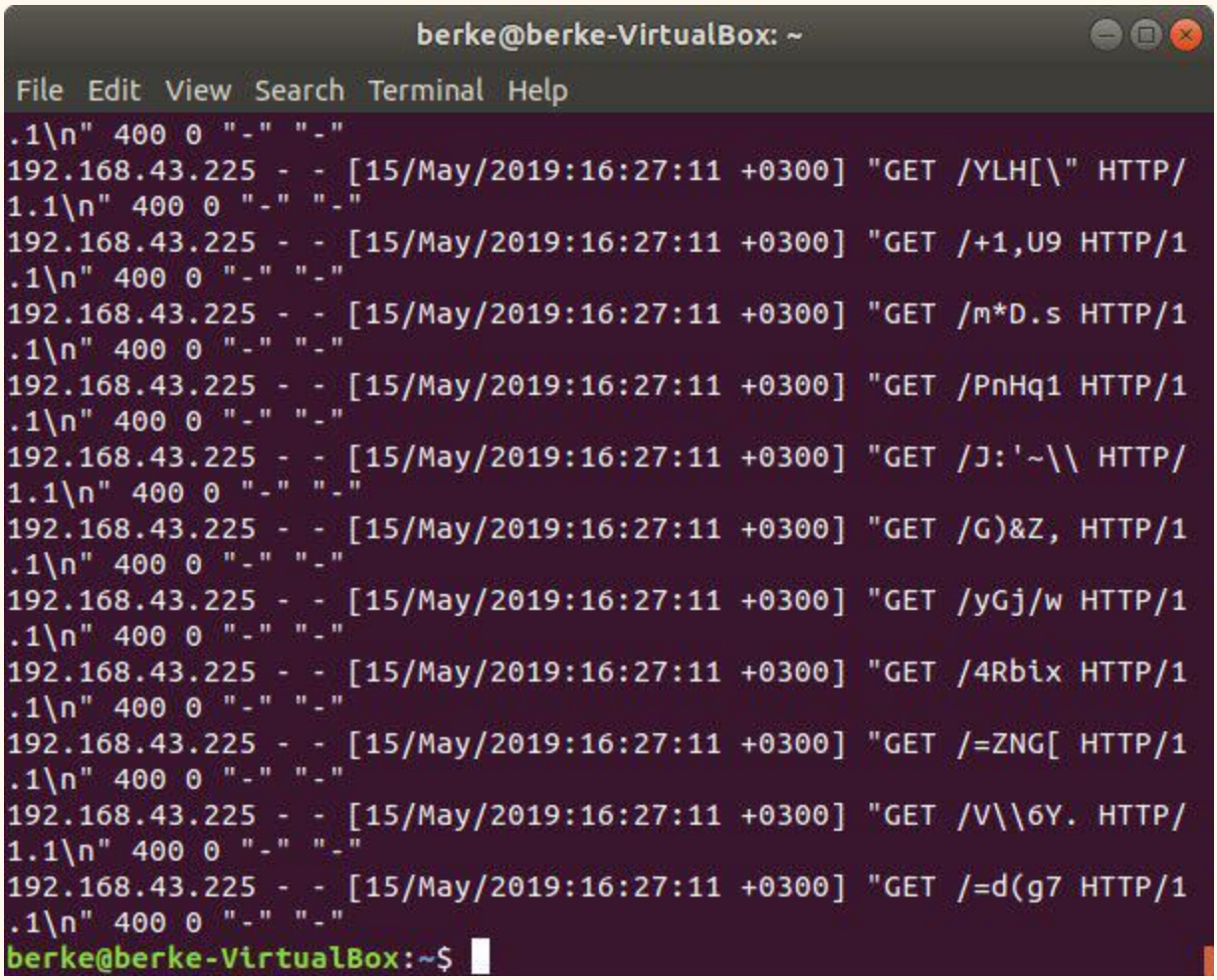
Ping of Death:

A ping of death attack is carried out by sending malicious pings to a computer. It will send a computer a packet that bigger than the maximum packet length of IP packet, 65,535 bytes. This will result in memory overflow for victim computer.



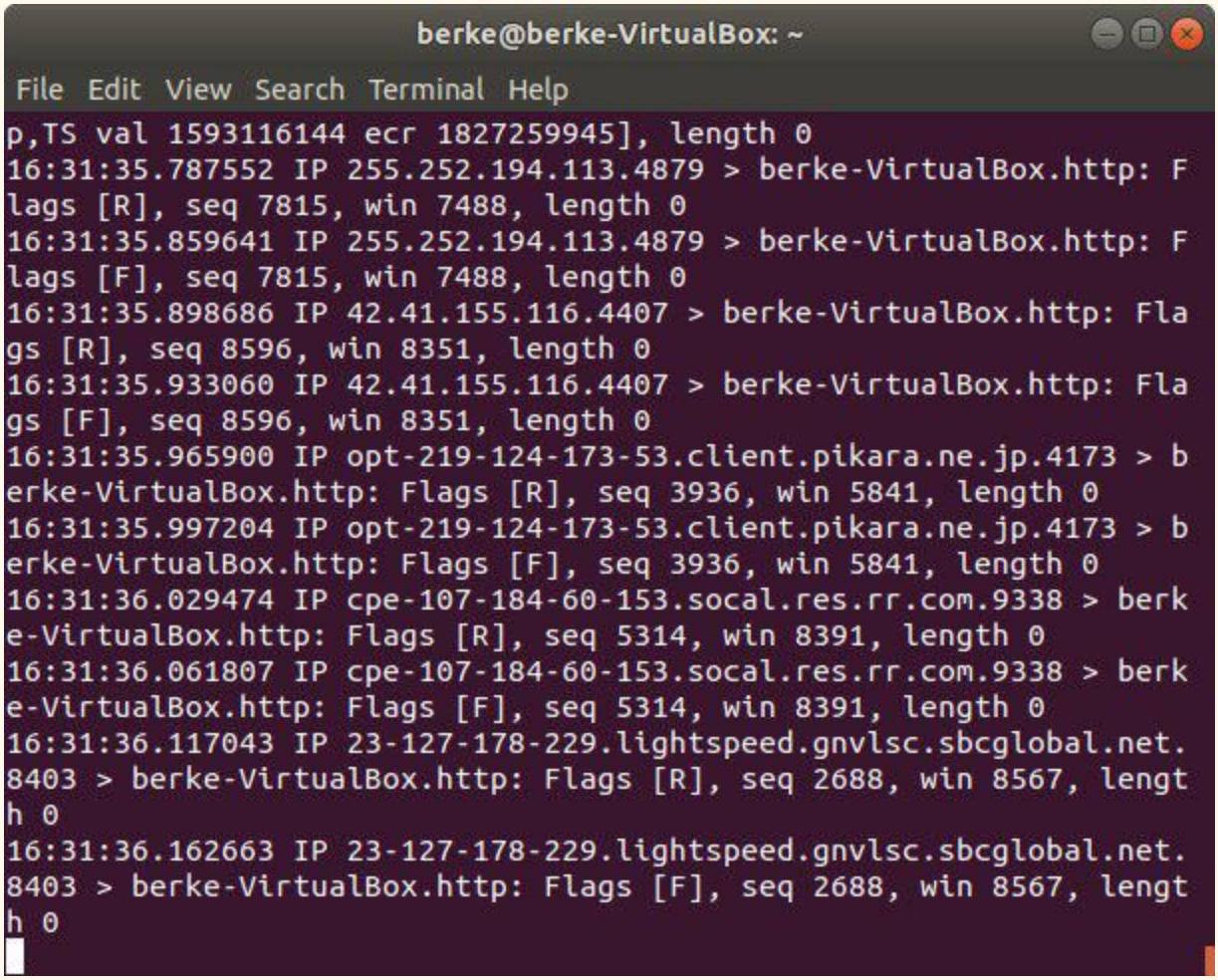
HTTP Flood:

Attacker sends legitimate HTTP Get/Post Request, and it will force the server to allocate maximum resources possible with every request it sends.



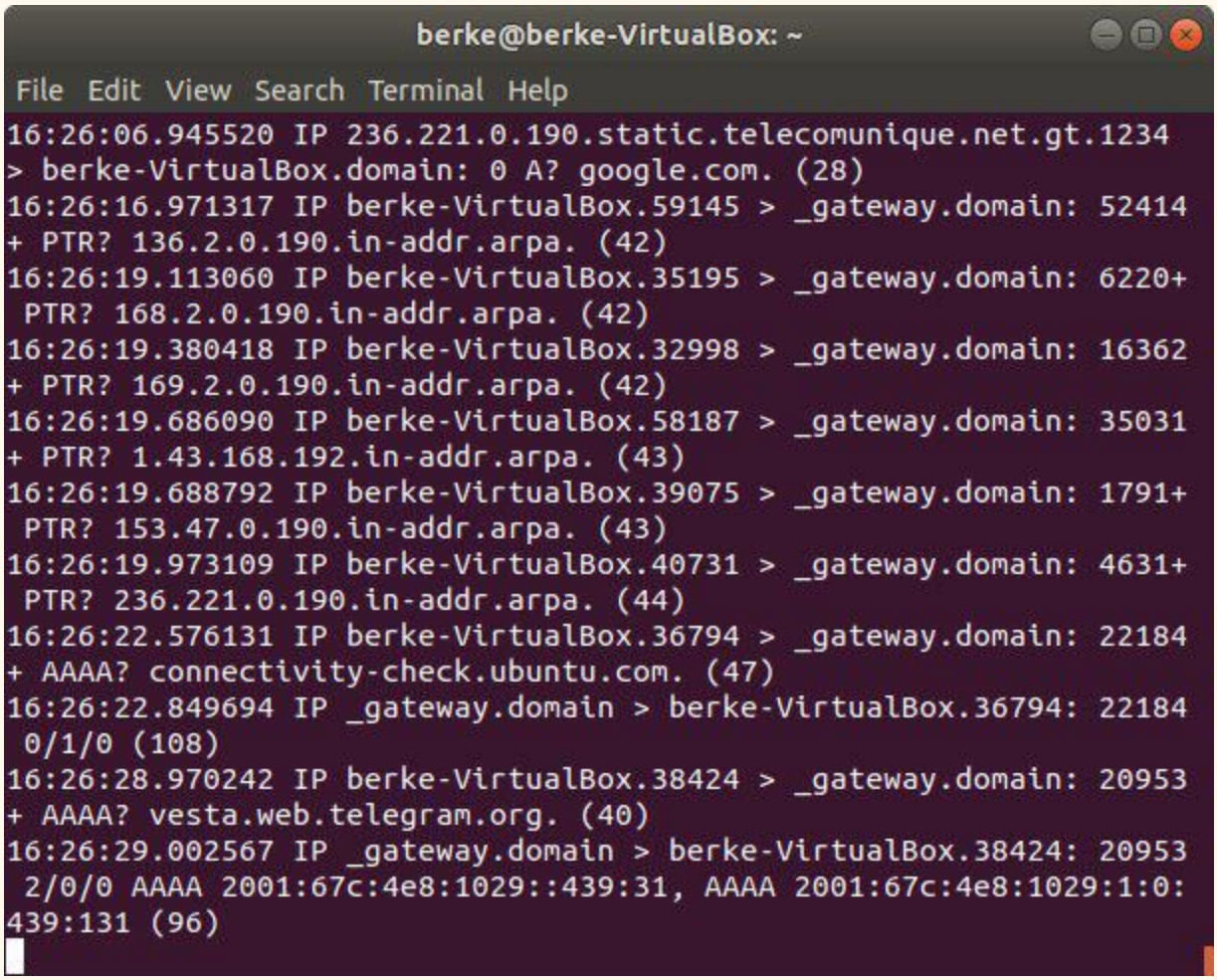
RST/FIN Flood:

In an RST/FIN Flood attack, attacker sends a large number of spoofed RST/FIN packets that do not belong to any session on the target server.



DNS Flood:

Flood a DNS server with DNS requests to prevent it from serving actual users properly.



Synonymous IP attack(LAND Attack):

A large number of TCP-SYN packets carrying the target server's Source IP and Destination IP are sent to the target server. The host server starts using additional system resources (RAM, CPU, etc.) to process each of the packets.