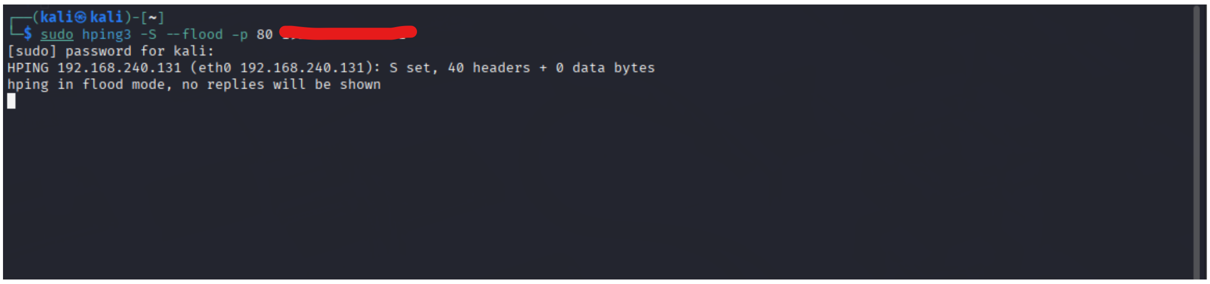
Project Report: Analysis of a Potential Denial of Service (DoS) Attack

Introduction:

This report details the analysis of a potential Denial of Service (DoS) attack scenario, evidenced through a series of network monitoring and command-line tool outputs. The analysis focuses on identifying indicators of malicious activity and understanding the tools and techniques involved.

Observed Data:

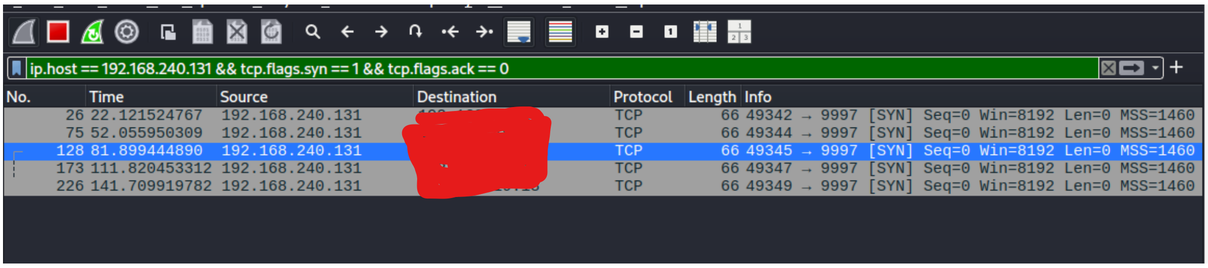
1. System Performance Monitor (Image 1): A Windows 7 Task Manager showing low CPU utilization and moderate memory usage. While this doesn't directly indicate an attack on this specific machine, it provides a baseline of system performance at a given time.
2. hping3 Command Execution (Image 2): The execution of the hping3 tool with the command:



```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -S --flood -p 80 [redacted]
[sudo] password for kali:
HPING 192.168.240.131 (eth0 192.168.240.131): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
█
```

`sudo hping3 -S --flood -p 80 [redacted]`

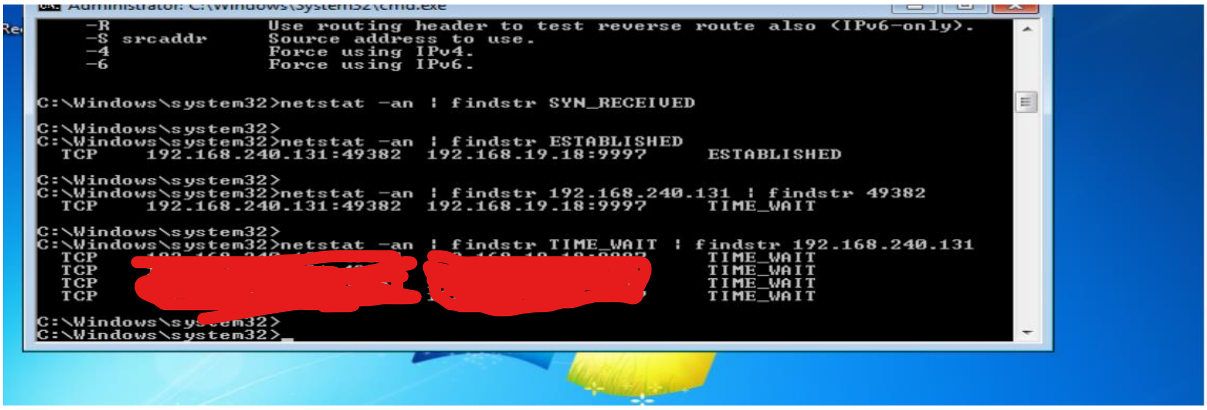
This command attempts to initiate a SYN flood attack against the IP address [redacted] on port 80. However, the output "Network is unreachable" suggests the attack may not have been successfully launched from this source at that specific time.



```
ip.host == 192.168.240.131 && tcp.flags.syn == 1 && tcp.flags.ack == 0
```

```
No.  Time           Source           Destination  Protocol Length Info
  26 22.121524767   192.168.240.131  [redacted]   TCP          66 49342 → 9997 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
  75 52.055950309   192.168.240.131               TCP          66 49344 → 9997 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
 128 81.899444890   192.168.240.131               TCP          66 49345 → 9997 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
 173 111.820453312  192.168.240.131               TCP          66 49347 → 9997 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
 226 141.709919782  192.168.240.131               TCP          66 49349 → 9997 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
```

3. **Wireshark Network Capture (Image 3): A Wireshark capture filtered for TCP SYN packets originating from [redacted] destined for [redacted]. The presence of multiple SYN packets without corresponding ACK packets is a strong indicator of a potential SYN flood attempt.**



```
    -R             Use routing header to test reverse route also (IPv6-only).
    -S srcaddr     Source address to use.
    -4             Force using IPv4.
    -6             Force using IPv6.

C:\Windows\system32>netstat -an | findstr SYN_RECEIVED

C:\Windows\system32>
C:\Windows\system32>netstat -an | findstr ESTABLISHED
  TCP    192.168.240.131:49382  192.168.19.18:9997     ESTABLISHED

C:\Windows\system32>
C:\Windows\system32>netstat -an | findstr 192.168.240.131 | findstr 49382
  TCP    192.168.240.131:49382  192.168.19.18:9997     TIME_WAIT

C:\Windows\system32>
C:\Windows\system32>netstat -an | findstr TIME_WAIT | findstr 192.168.240.131
  TCP    [redacted]             [redacted]             TIME_WAIT
  TCP                                                  TIME_WAIT
  TCP                                                  TIME_WAIT
  TCP                                                  TIME_WAIT

C:\Windows\system32>
C:\Windows\system32>_
```

4. **`netstat` Output (Latest Image): The output of the `netstat` command on a Windows system showing:**

- **An established connection between [redacted] and [redacted].**
- **Multiple TCP connections in the `TIME_WAIT` state originating from [redacted] and destined for [redacted] on port [redacted].**

Analysis:

The collected data points towards a potential DoS attack, likely a SYN flood, being directed at the host [redacted].

- The `hping3` command (Image 2) shows an attempt to generate SYN flood traffic, although it appeared to fail at the time of capture.
- The Wireshark capture (Image 3) provides network-level evidence of multiple SYN packets originating from [redacted] towards [redacted], consistent with a SYN flood.
- The `netstat` output further supports this by showing multiple connections in the `TIME_WAIT` state from the potential attacking host ([redacted]) to the target ([redacted]), which can be a byproduct of rapid connection attempts in a DoS scenario.

The lack of `SYN_RECEIVED` entries in the `netstat` output at that specific moment might indicate that the target system was either handling the initial SYN packets or that the flood was not actively overwhelming the half-open connection queue at that precise instant.

Conclusion:

Based on the combined evidence from the `hping3` command, the Wireshark capture, and the `netstat` output, it is highly probable that a SYN flood Denial of Service attack was being attempted from or involving the host at IP address [redacted] towards the host at IP address [redacted].

Tools Used:

- Windows 7: Operating system shown in the performance monitor and `netstat` output.
- `hping3`: A command-line packet crafting tool used to generate network traffic for testing and attacks.
- Wireshark: A network protocol analyzer used to capture and examine network traffic.
- `netstat`: A command-line network utility to display network connections, routing tables, interface statistics, etc.

Further Investigation:

To gain a more complete understanding, further investigation could involve:

- Analyzing network performance metrics on the target machine ([redacted].
- Observing network traffic over a longer period.
- Identifying any impact on the availability of services on the target machine.
