Introduction to Malware Analysis

Term Project (10 points)

Partner: Andy Pen

Instructions

Read the entire <u>Vulnserver TRUN Exploitation</u> 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:

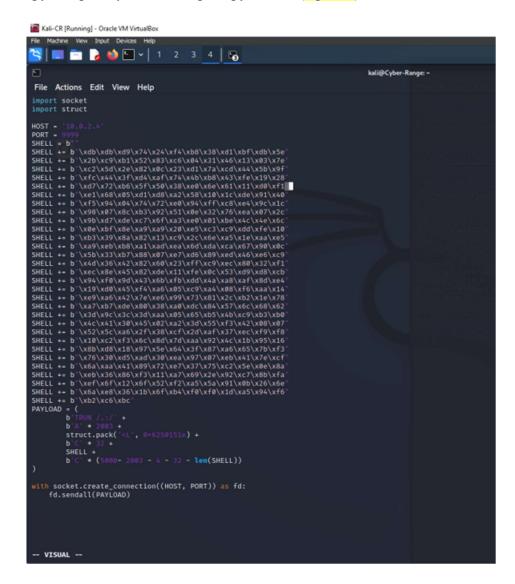
1. Explain how the TRUN command of Vulnserver/vchat can be exploited. (2 points)

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)



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