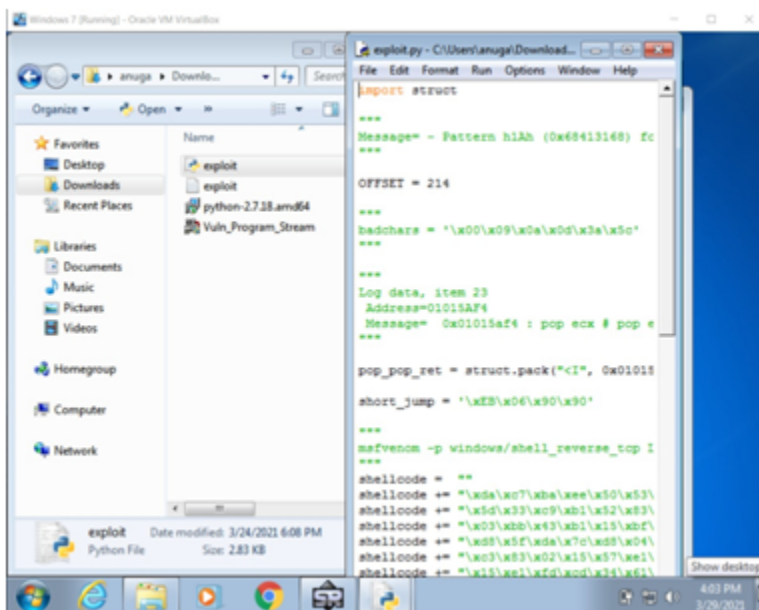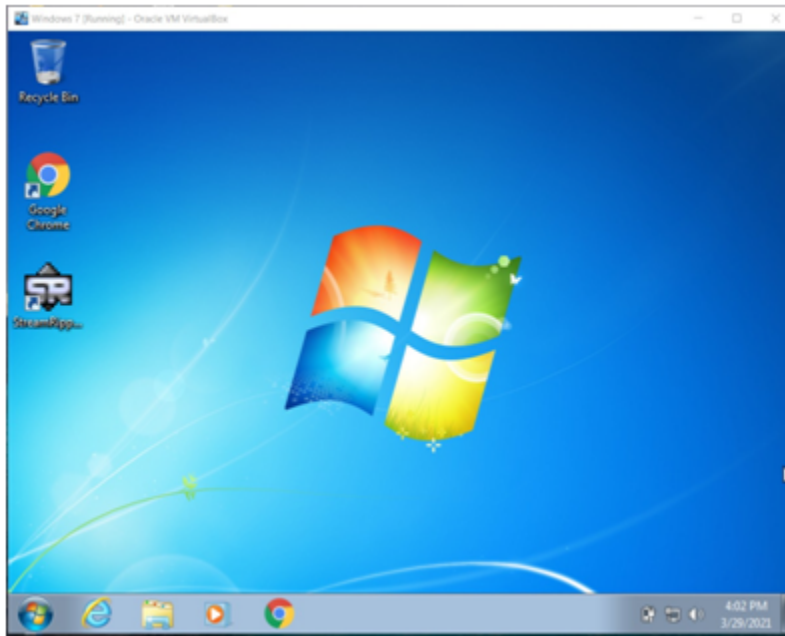**NAME : ANUGA SRIKAR REDDY REG**
NO : 18BCE7122

SLOT : L3+L4
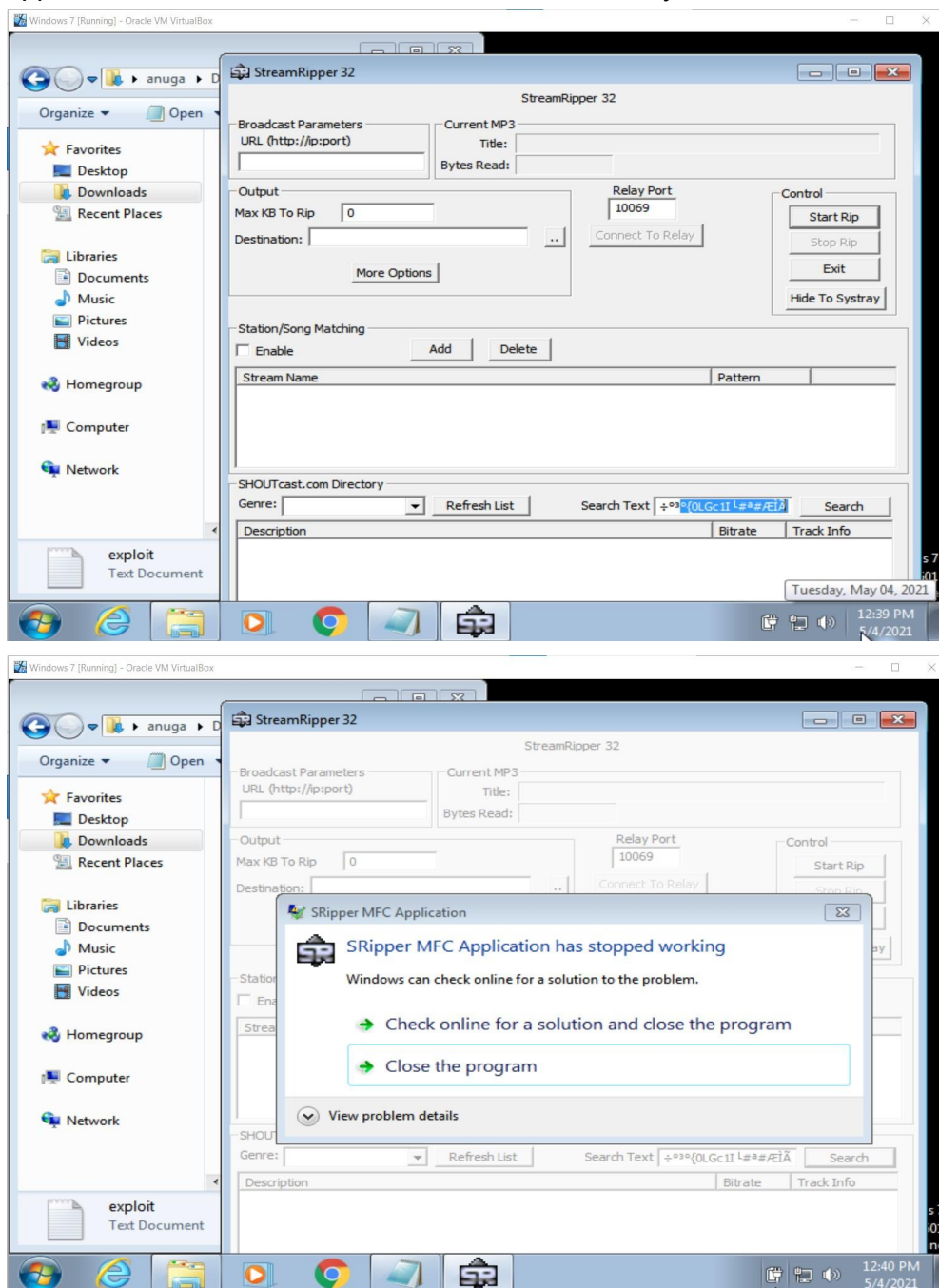
Exploiting:

➢ After extraction of Vulln.zip in Windows 7 instance

➢ After executing exploit.py and opening the payload(exploit.txt)
➢ Copy the payload into the search box of Streamripper32.

➢ Application crashed due to buffer overflow vulnerability.

```
Administrator: C:\Windows\System32\cmd.exe - diskpart

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

C:\Windows\system32>diskpart

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