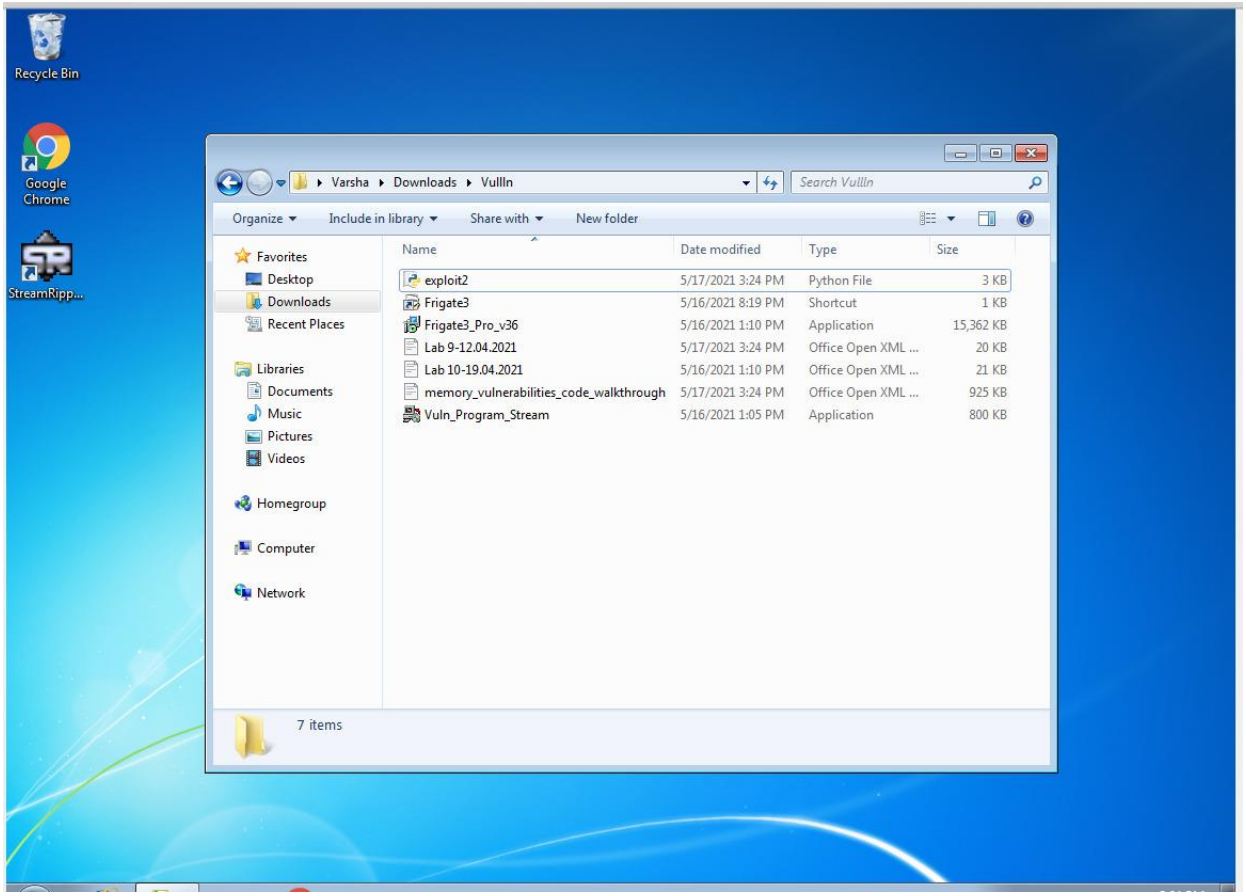
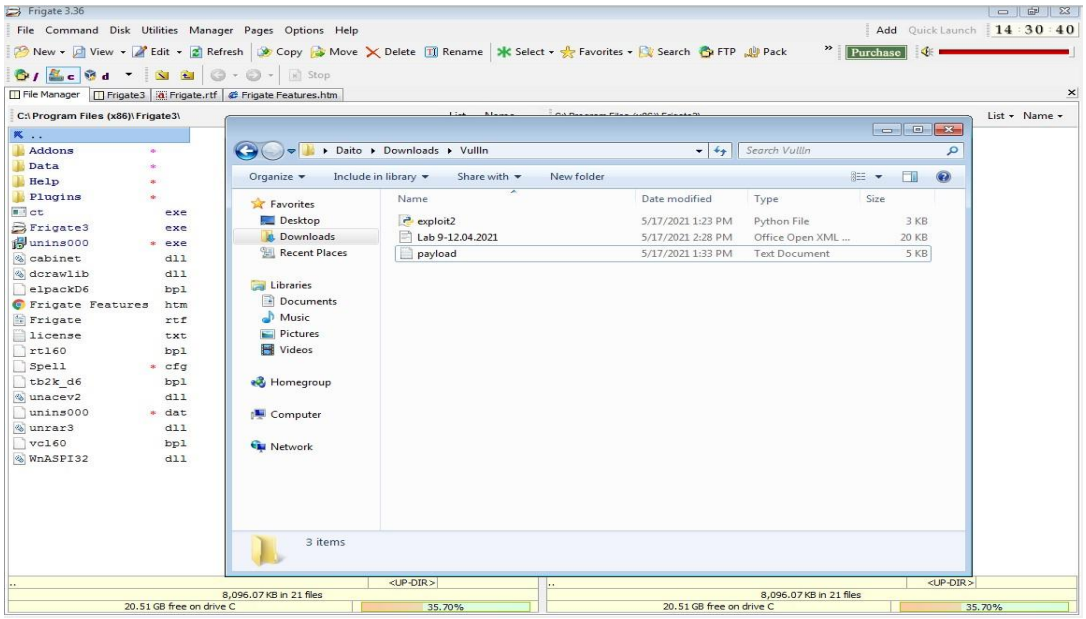
Lab Assignment -9

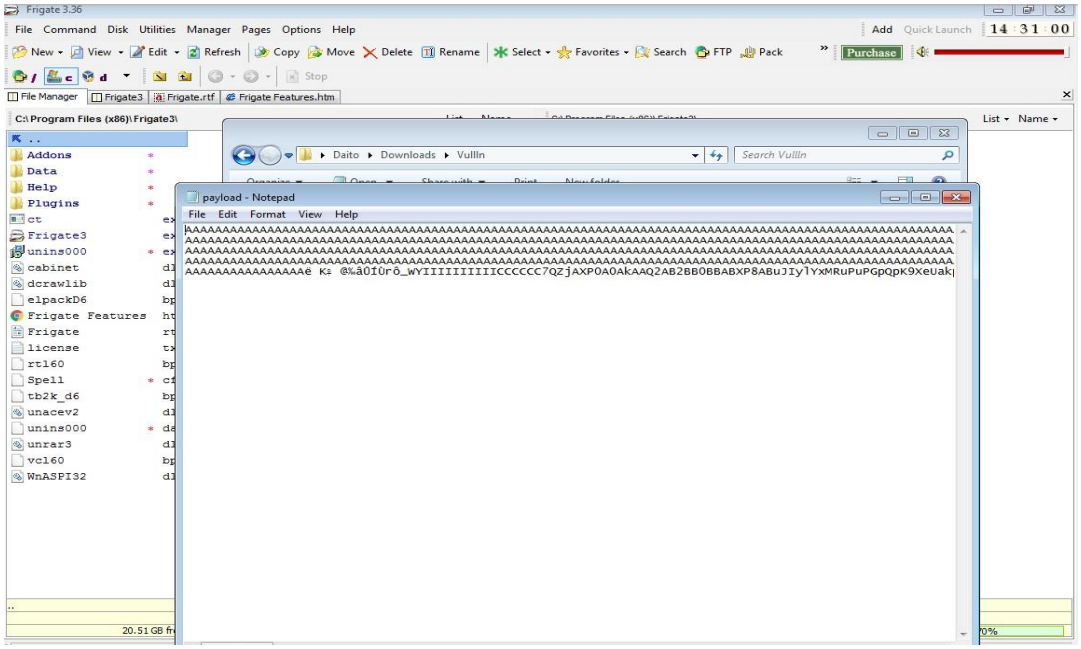
Name : D.Vakuladevi
Reg.No.: 19BCE7061
Slot : L39-40

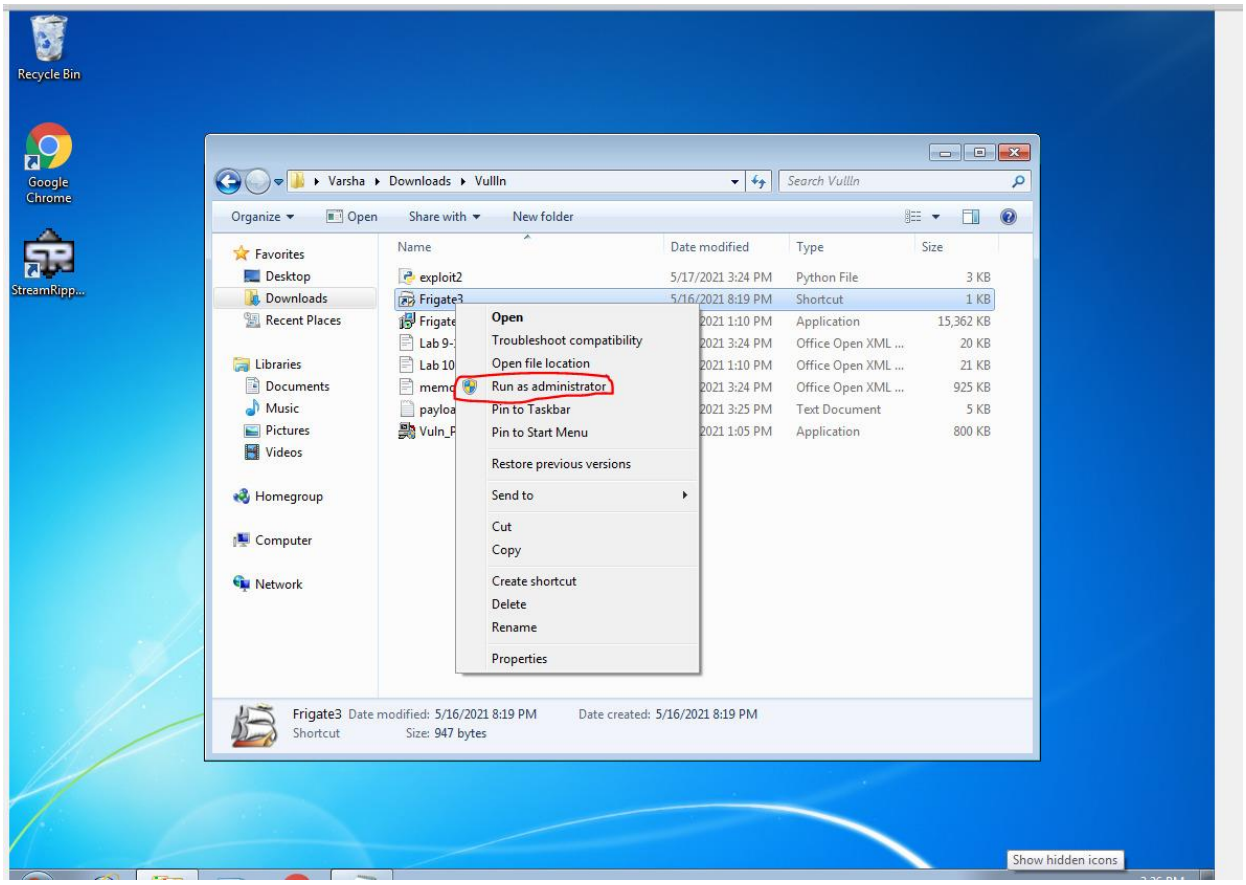
Working with the memory vulnerabilities

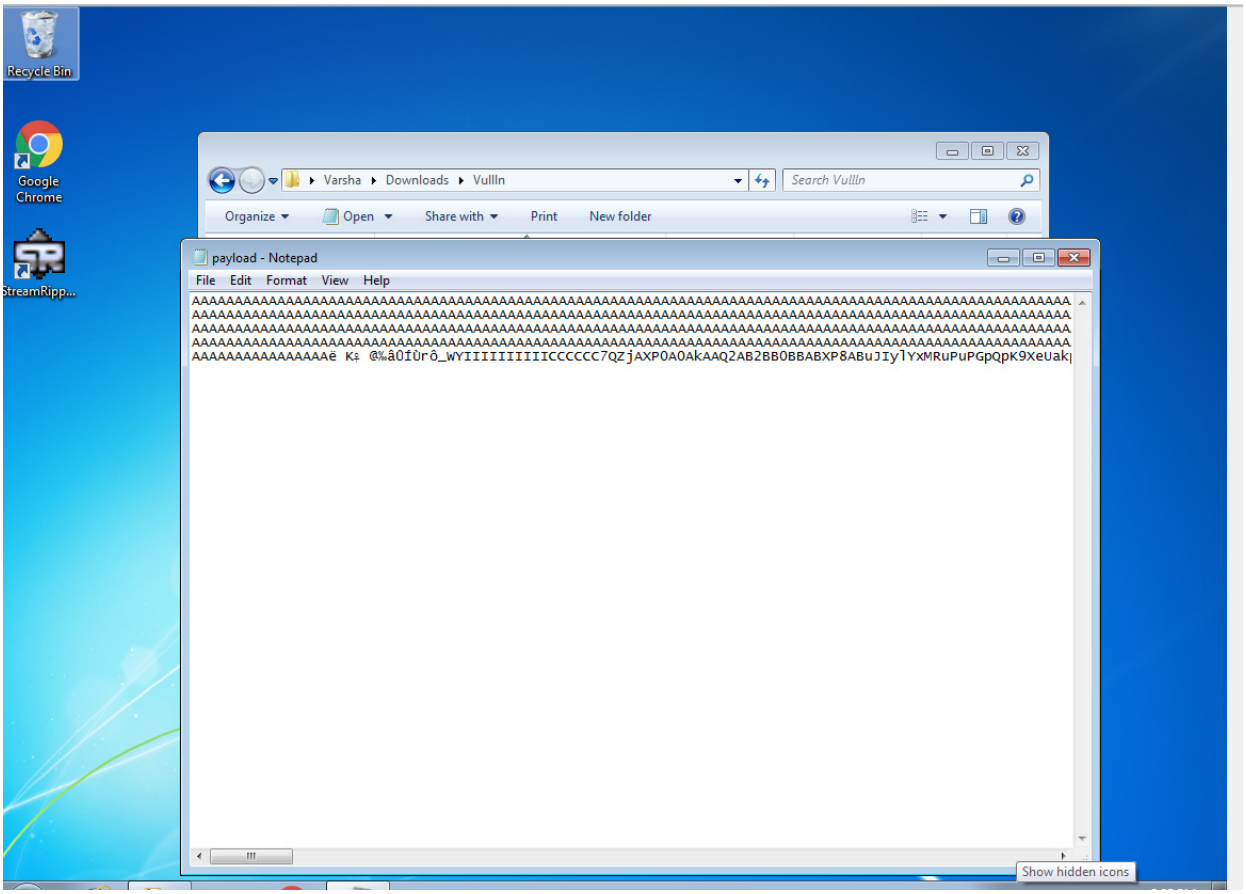
1)Install Frigate3 on Windows 7 VM: Frigate3 UI and Execute the exploit2.py to generate the payload_cmd.txt file.

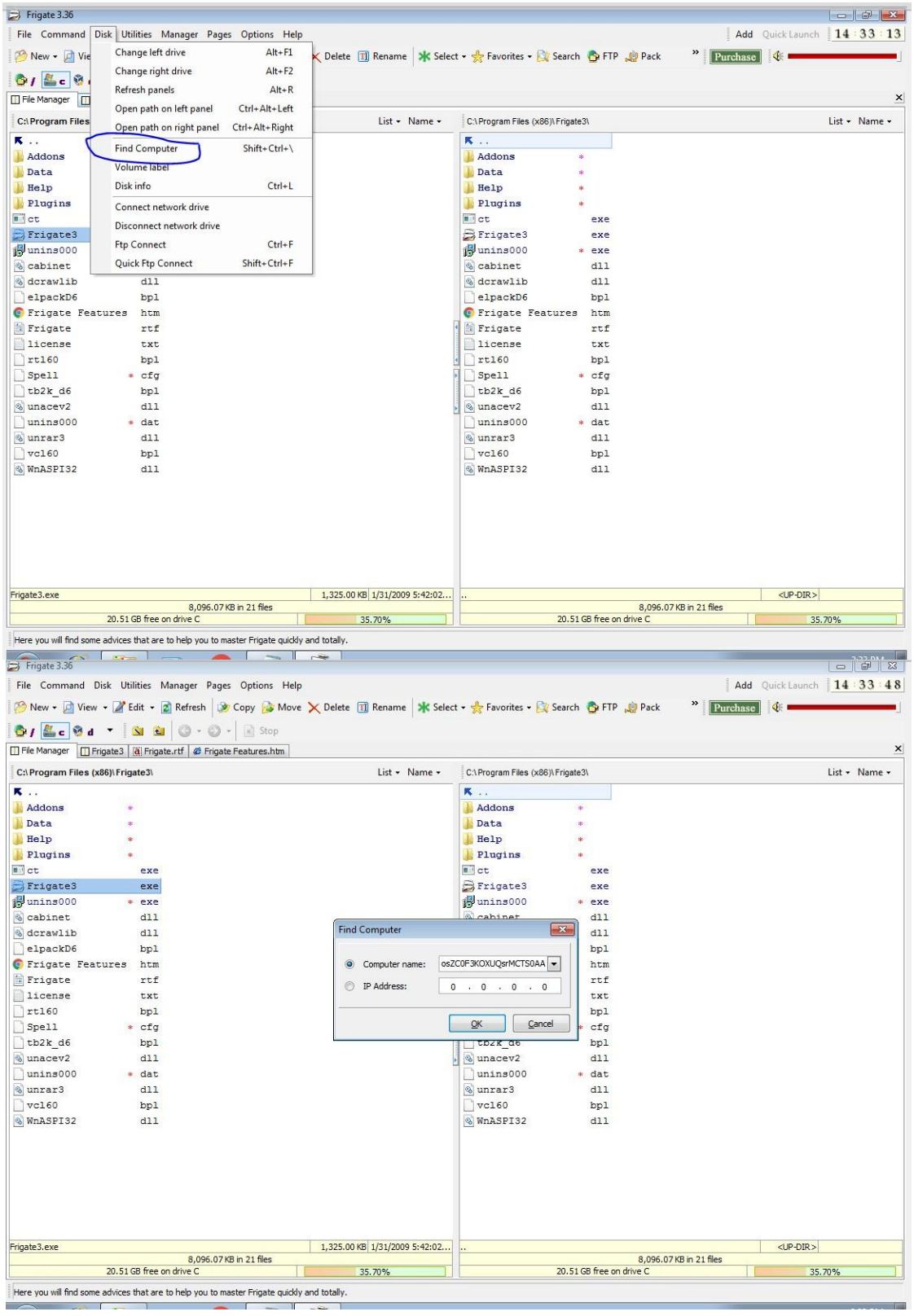




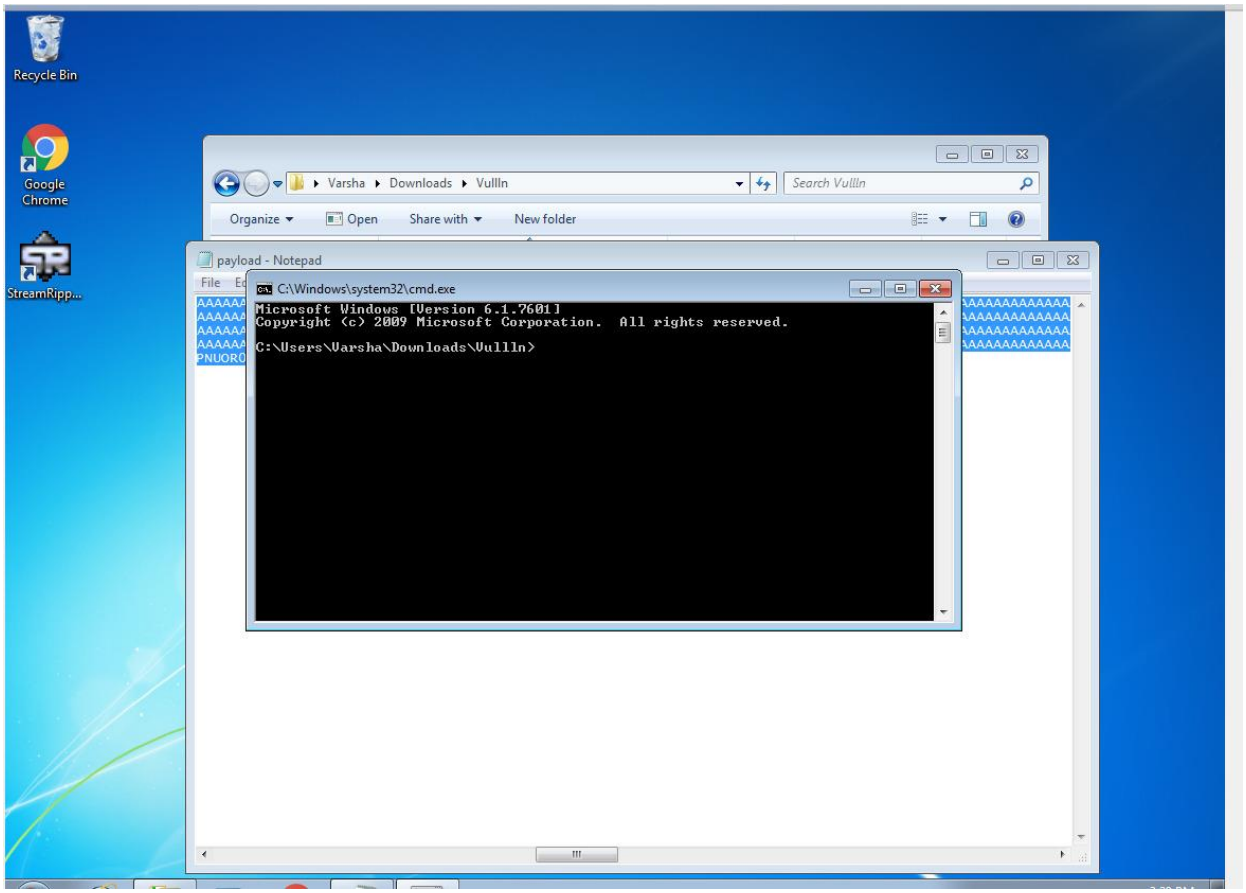

Frigate 3.36
File Command Disk Utilities Manager Pages Options Help
Add Quick Launch 14:31:00
New View Edit Refresh Copy Move Delete Rename Select Favorites Search FTP Pack Purchase
Stop
File Manager Frigate3 Frigate.rtf Frigate Features.htm
C:\Program Files (x86)\Frigate3\
List Name
Daito Downloads Vulln
Search Vulln
payload - Notepad
File Edit Format View Help
AAAA



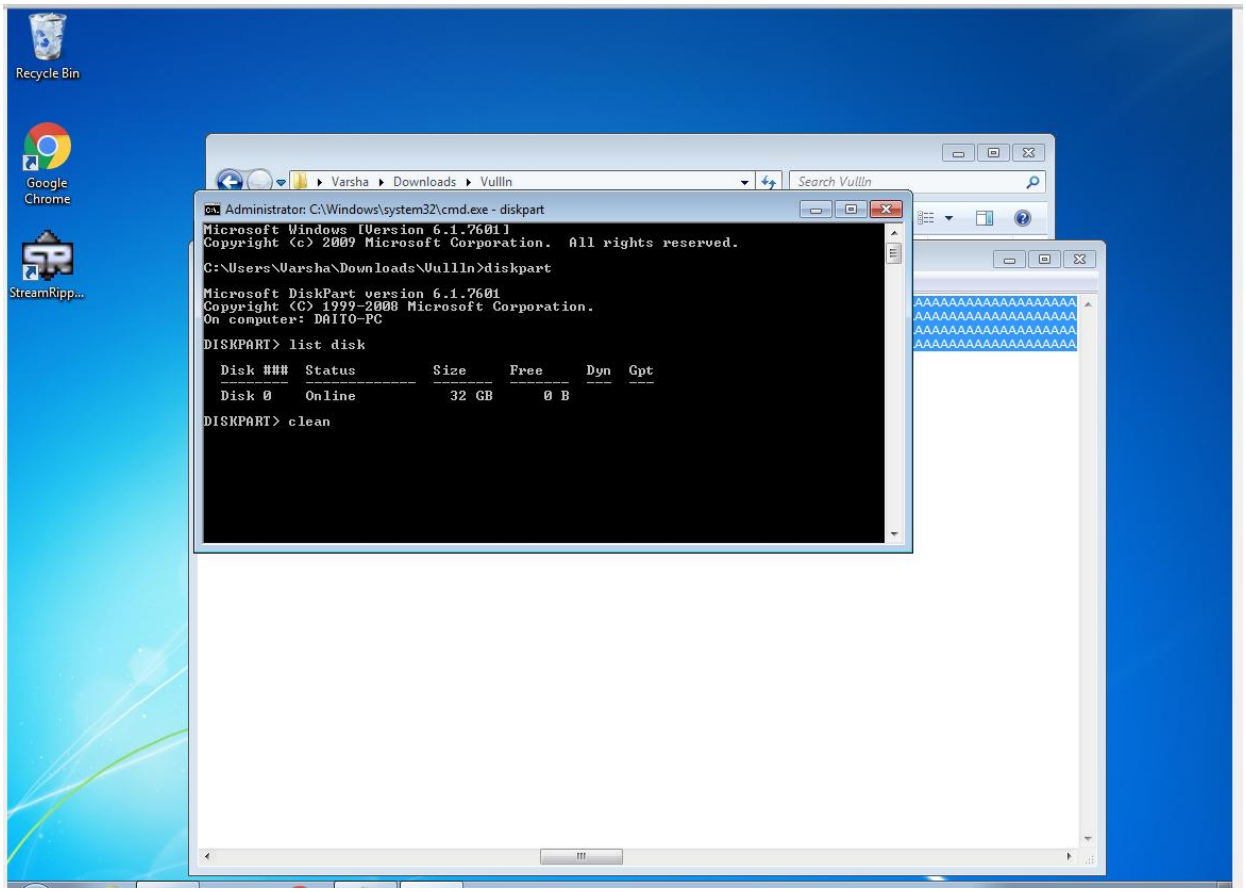

Recycle Bin
Google Chrome
StreamRipp...
Varsha ▸ Downloads ▸ VulnIn
Search VulnIn
Organize
Open
Share with
Print
New folder
payload - Notepad
File Edit Format View Help
AAAA



3)The CMD that opens after crashing the application is opened with elevated privileges.

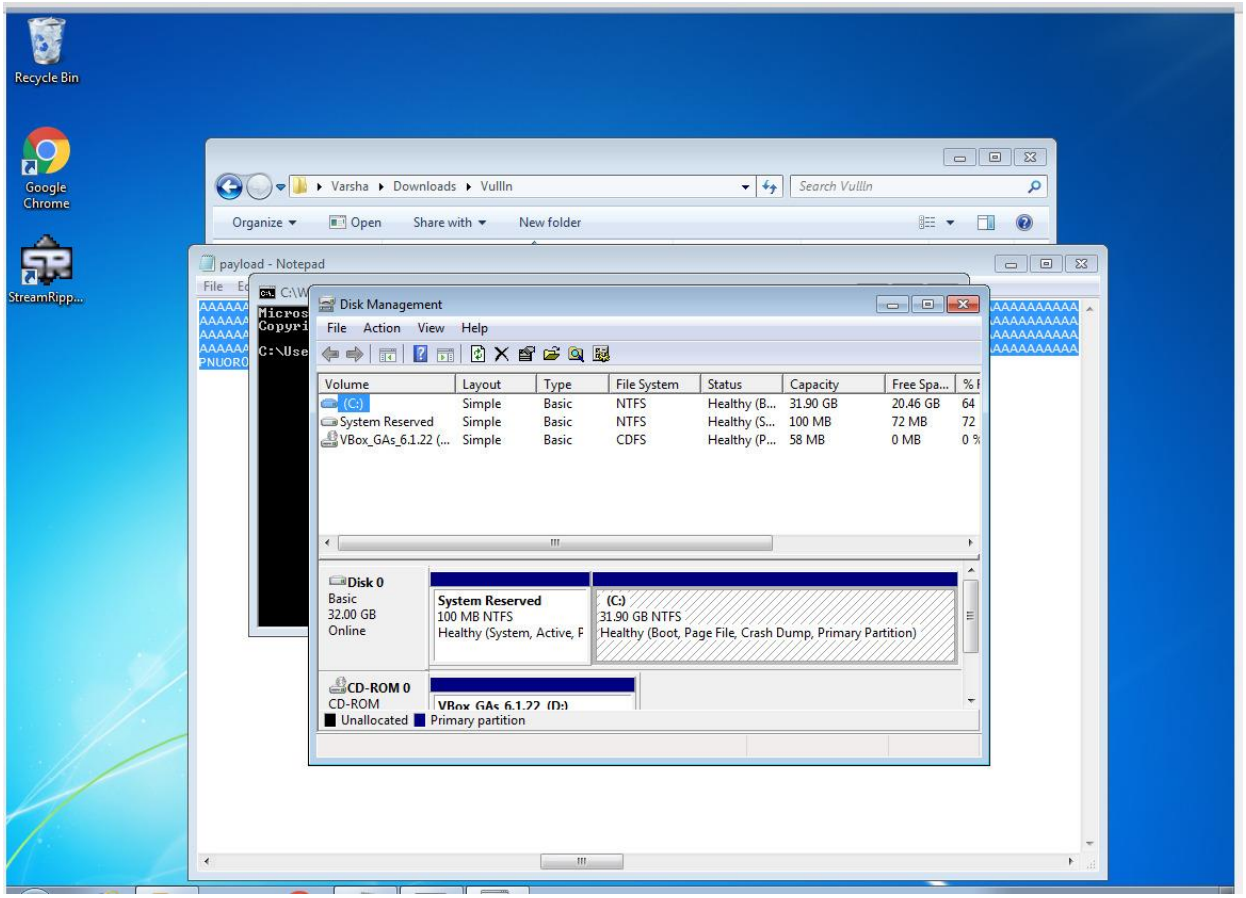


4)Type diskpart and follow the screenshots



5)From the diskpart prompt, type clean and press Enter. The drive's partition, data, and signature is now removed. You will return to the diskpart prompt. Warning: Once you type clean and hit enter the drive will be erased.

Check the drive in Device management:


Recycle Bin
Google Chrome
StreamRipp...
Varsha ▸ Downloads ▸ VullIn
Search VullIn
Organize
Open
Share with
New folder
payload - Notepad
Disk Management
File Action View Help
Volume Layout Type File System Status Capacity Free Spa... %
(C:) Simple Basic NTFS Healthy (B... 31.90 GB 20.46 GB 64
System Reserved Simple Basic NTFS Healthy (S... 100 MB 72 MB 72
VBox_GAs_6.1.22 (... Simple Basic CDFS Healthy (P... 58 MB 0 MB 0 %
Disk 0
Basic
32.00 GB
Online
System Reserved
100 MB NTFS
Healthy (System, Active, P
(C:)
31.90 GB NTFS
Healthy (Boot, Page File, Crash Dump, Primary Partition)
CD-ROM 0
CD-ROM
Unallocated
Primary partition