

# SECURE CODING CSE2010

19BCN7034

## Working with memory vulnerabilities

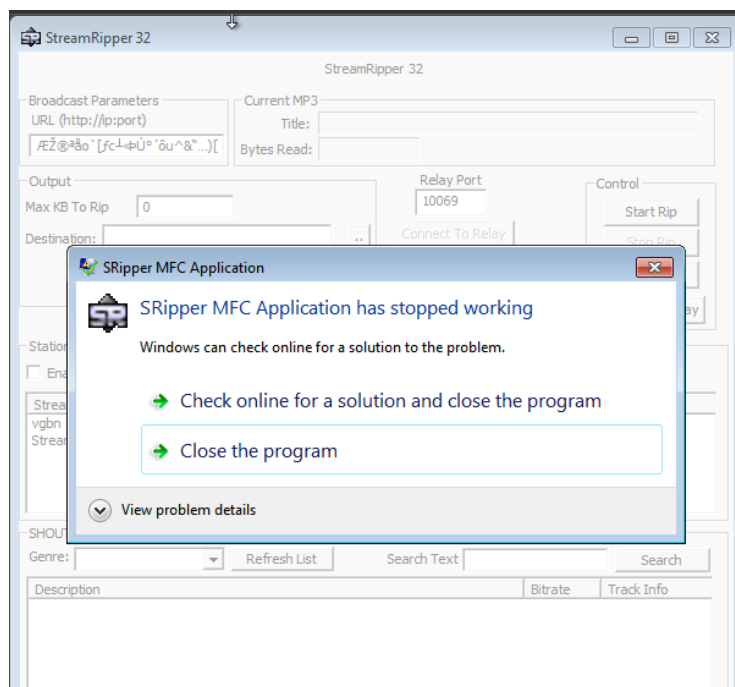
### TASK

- Crash the Vuln Program Stream program and try to erase the hdd.

After running the exploit.py we get a payload



And now this payload causes the programs to stop running



## Erasing the hdd



A screenshot of a Windows Command Prompt window titled "Administrator: Command Prompt". The window shows the execution of the diskpart utility to erase a hard drive. The commands entered are: `diskpart`, `list disk`, `select disk 0`, and `clean`. The output shows the diskpart version, copyright information, and a table of disks. The table has columns for Disk ###, Status, Size, Free, Dyn, and Gpt. It shows one disk (Disk 0) with a size of 60 GB and 0 B free space. The `clean` command is successful, with the message "DiskPart succeeded in cleaning the disk."

```
C:\Windows\system32>diskpart
Microsoft DiskPart version 6.2.9200
Copyright (C) 1999-2012 Microsoft Corporation.

DISKPART> list disk

   Disk ###  Status             Size       Free      Dyn  Gpt
   -----  -
   Disk 0     Online              60 GB         0 B

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

DISKPART> clean

DiskPart succeeded in cleaning the disk.
```