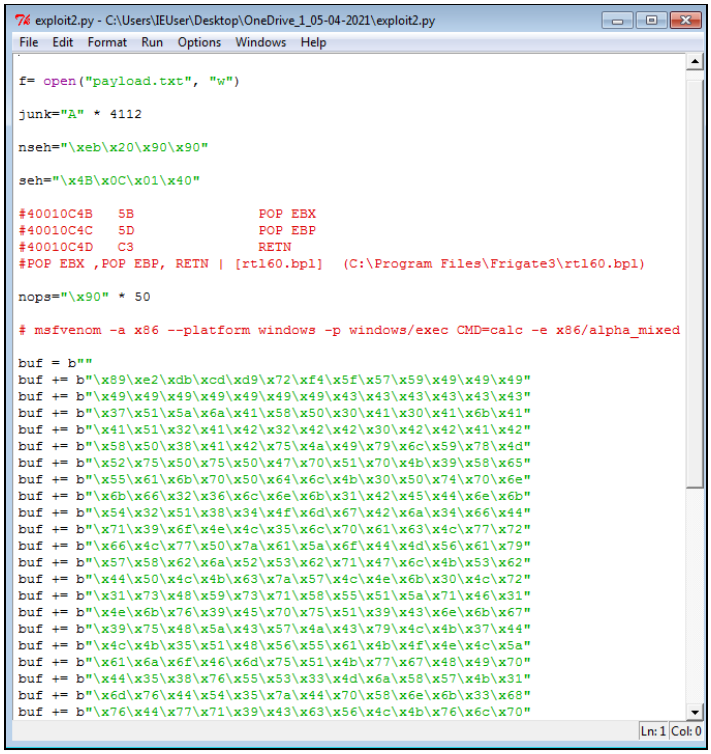
Secure Coding

Lab experiment - Working with the memory vulnerabilities – Part III

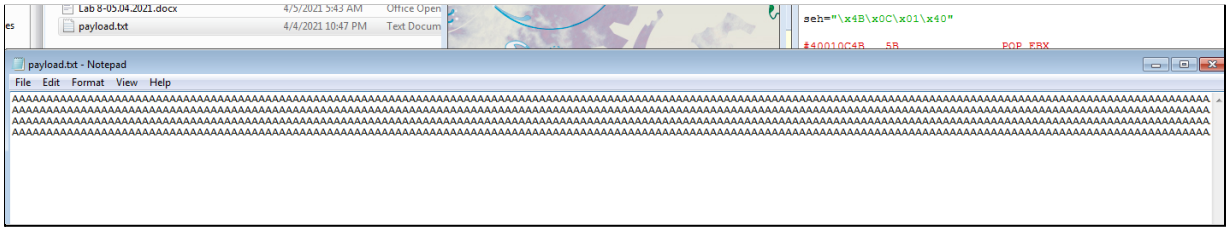
Task

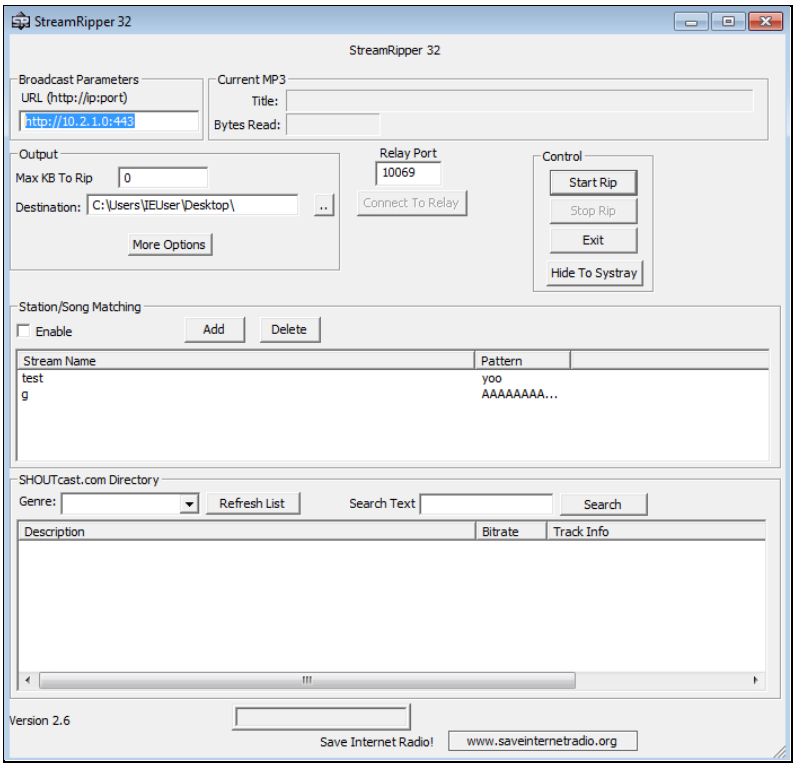
- Download Vulln.zip from teams.
- Deploy a virtual windows 7 instance and copy the Vulln.zip into it.
- Unzip the zip file. You will find two files named exploit.py and Vuln_Program_Stream.exe
- Download and install python 2.7.* or 3.5.*
- Run the exploit script II (exploit2.py) to generate the payload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

Running the script

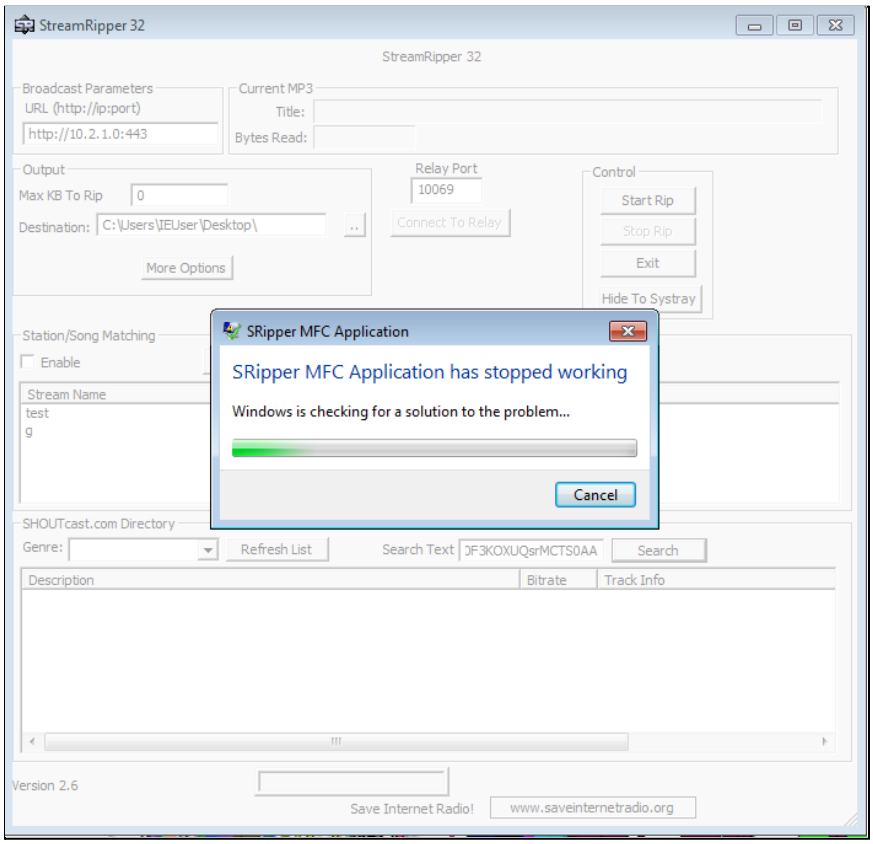


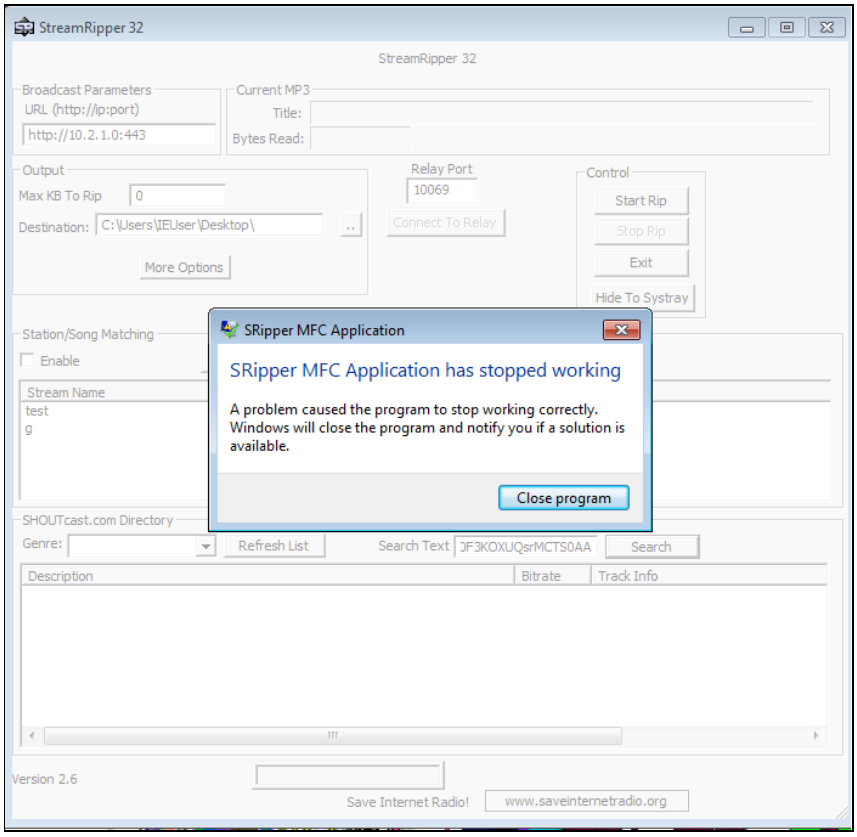
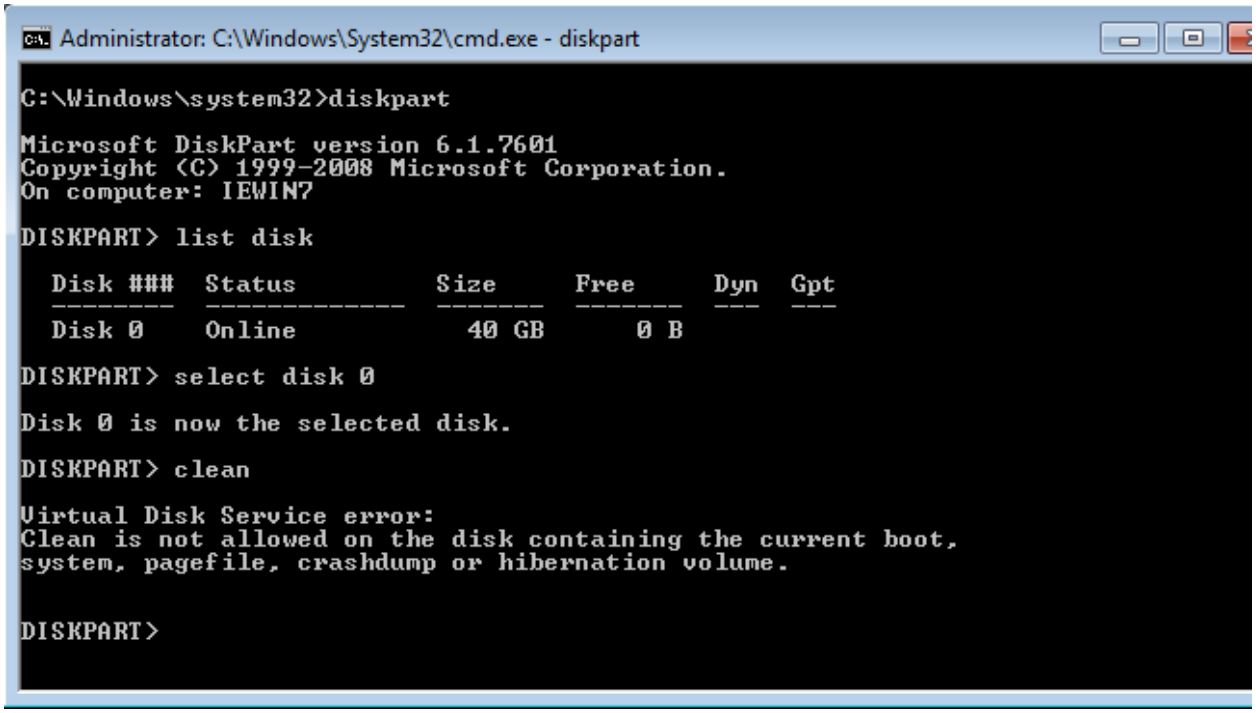
Generated the payload


Lab 8-05.04.2021.docx 4/5/2021 5:43 AM Office Open
payload.txt 4/4/2021 10:47 PM Text Docum
seh="\x4B\x0C\x01\x40"
#40010C4B 5B POP EBX
payload.txt - Notepad
File Edit Format View Help
AAAA


StreamRipper 32
StreamRipper 32
Broadcast Parameters
URL (http://ip:port)
http://10.2.1.0:443
Current MP3
Title:
Bytes Read:
Output
Max KB To Rip
0
Destination:
C:\Users\IEUser\Desktop\
More Options
Relay Port
10069
Connect To Relay
Control
Start Rip
Stop Rip
Exit
Hide To Systray
Station/Song Matching
Enable
Add
Delete
Stream Name
Pattern
test
yoo
g
AAAAAAAA...
SHOUTcast.com Directory
Genre:
Refresh List
Search Text
Search
Description
Bitrate
Track Info
Version 2.6
Save Internet Radio!
www.saveinternetradio.org

App crashes


StreamRipper 32
StreamRipper 32
Broadcast Parameters
URL (http://ip:port)
http://10.2.1.0:443
Current MP3
Title:
Bytes Read:
Output
Max KB To Rip
0
Destination:
C:\Users\IEUser\Desktop\
More Options
Relay Port
10069
Connect To Relay
Control
Start Rip
Stop Rip
Exit
Hide To Systray
SRipper MFC Application
SRipper MFC Application has stopped working
Windows is checking for a solution to the problem...
Cancel
Station/Song Matching
Enable
Stream Name
test
g
SHOUTcast.com Directory
Genre:
Refresh List
Search Text
JF3KOXUQsrMCTS0AA
Search
Description
Bitrate
Track Info
Version 2.6
Save Internet Radio!
www.saveinternetradio.org



Trying to erase hdd using diskpart