# CONTENTS

1. INTRODUCTION 1

1.1 Kali Linux 1

1.2 Penetration Testing 2

2. EASYSPLOIT 2

2.1 Introduction 2

2.2 Installation 3

3. STEPS FOR HACKING MAC OS

3.1 Commands to Exploits Mac OS

4. HOW TO PREVENT ATTACK

5. CONCLUSION 8

6. REFERENCE 9

# 1. INTRODUCTION

## 1.1 KALI LINUX

Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering.

It was developed by Mati Aharoni and Devon Kearns of Offensive Security through the rewrite of Backtrack. Kali Linux was released on the 13th march, 2013 as a complete, top to bottom. Rebuild of Backtrack Linux, adhering completely to Debian development standards.

## 1.2 PENETRATION TESTING

Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit. For example, an audit or an assessment may utilize scanning tools that provide a few hundred possible vulnerabilities on multiple systems. A Penetration Test would attempt to attack those vulnerabilities in the same manner as a malicious hacker to verify which vulnerabilities are genuine reducing the real list of system vulnerabilities to a handful of security weaknesses.

**Benefits of Penetration Testing**

- Intelligently manage vulnerabilities
- Avoid the cost of network downtime
- Meet regulatory requirements and avoid fines
- Preserve corporate image and customer loyalty

# 2. EASYSPLOIT

## 2.1 INTRODUCTION

**EASYSPLOIT** is an advanced pentesting framework which is a metasploit automation. The tool can compile the viruses with popular payloads and then compile the resulting file to run a specific platform – Microsoft Windows, Android or Mac OS X. The hacking utility runs as a simple script which uses interactive menus to guide the user into creating their custom malware.

Easysploit is a very easy tool for generating the backdoor or payload. Another the best thing of this tool is, your creating payload by using this tool can execute on windows, Linux, mac and android as well.

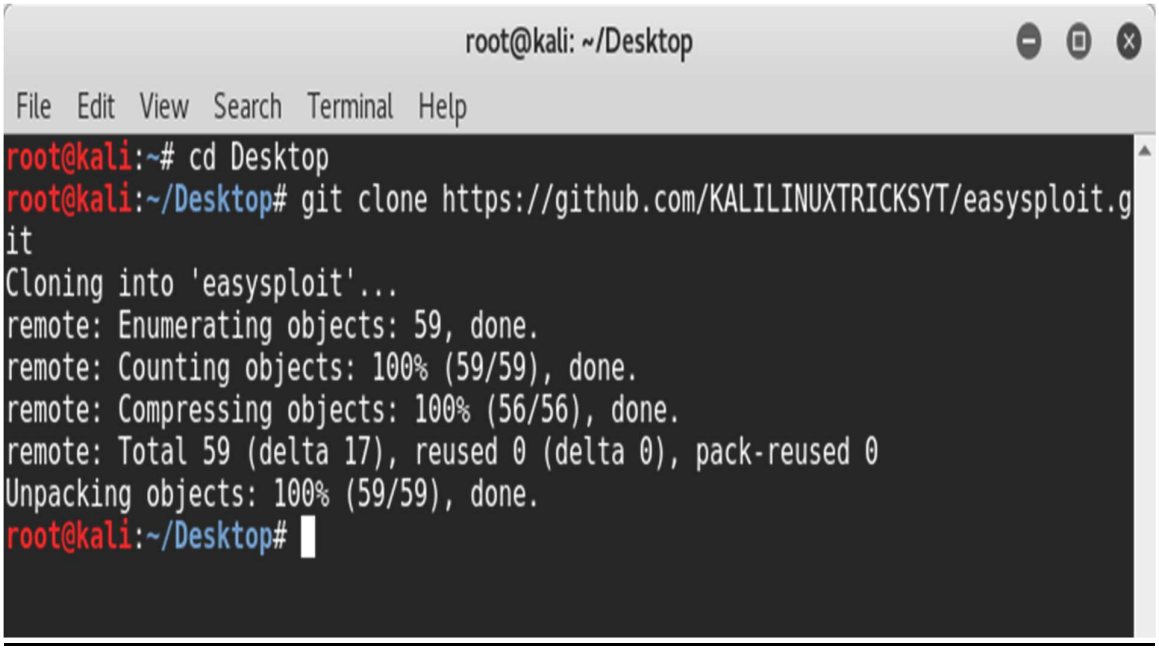
**Requirements**

- You have installed kali linux on your system
- Having some basic knowledge of kali linux
- The downloading link of Easysploit tool
- working internet connection
- A static IP address

# 2.2 INSTALLATION

- We will download the folder from *GitHub* with the git clone command:

  git clone **https://github.com/KALILINUXTRICKSYT/easysploit.git**

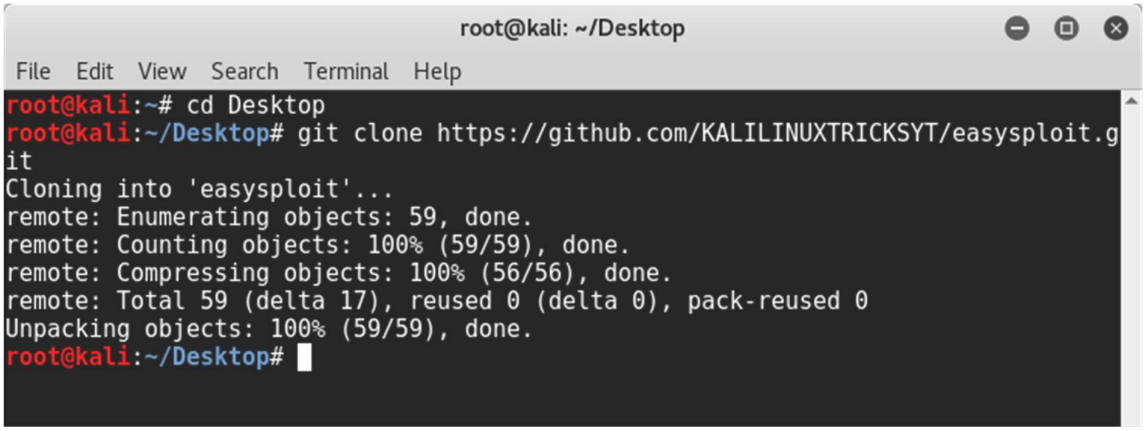


# 3. STEPS FOR HACKING MAC OS

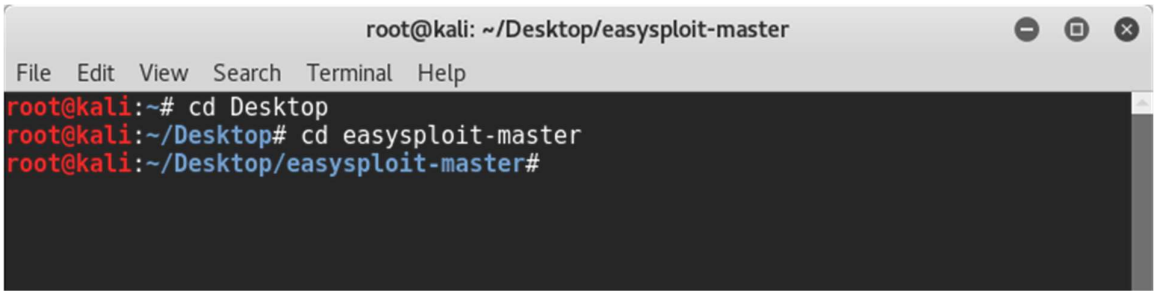
**Step 1:**

After the Easysploit downloaded, got a new folder The easysploit-master on your desktop. Move to that folder.

- *#cd Desktop*
- **#cd easysploit-master**



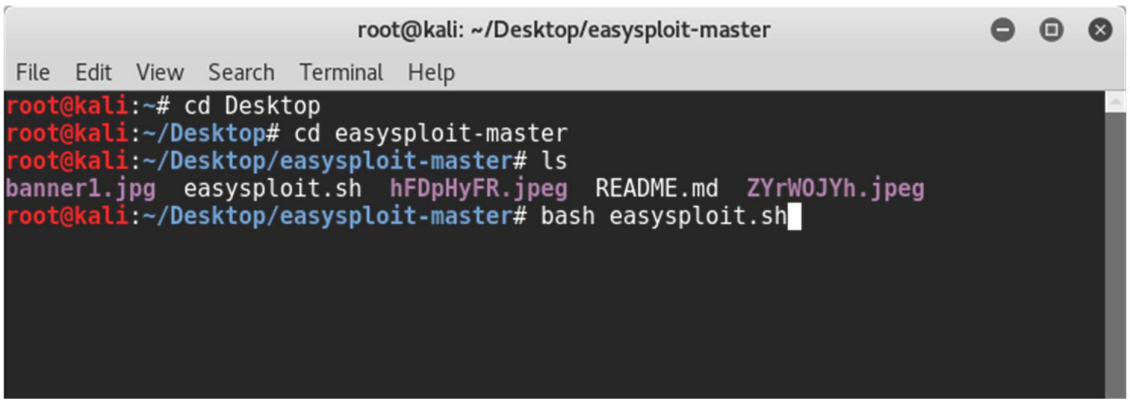

- Change directory to easysploit-master give the command: **cd easysploit-master**



**Step 2:**

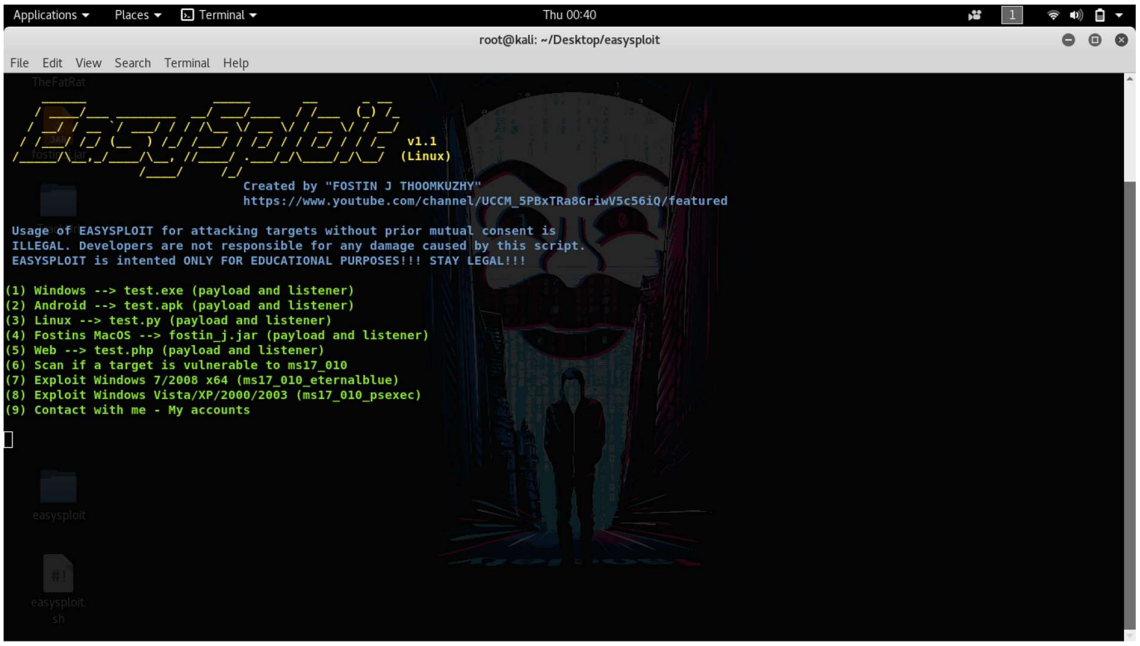
- Install the necessary dependencies using the command:

**./easysploit.sh**



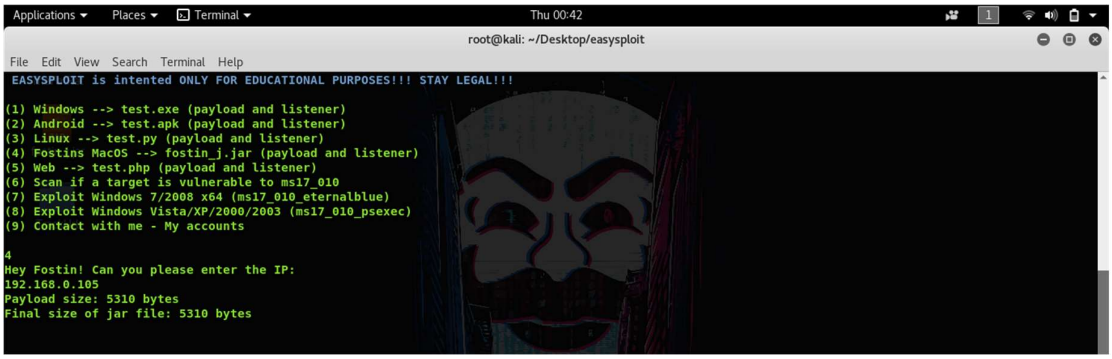

**Step 3:**

- For selecting the operating system: **Choose 4 for Mac OS**



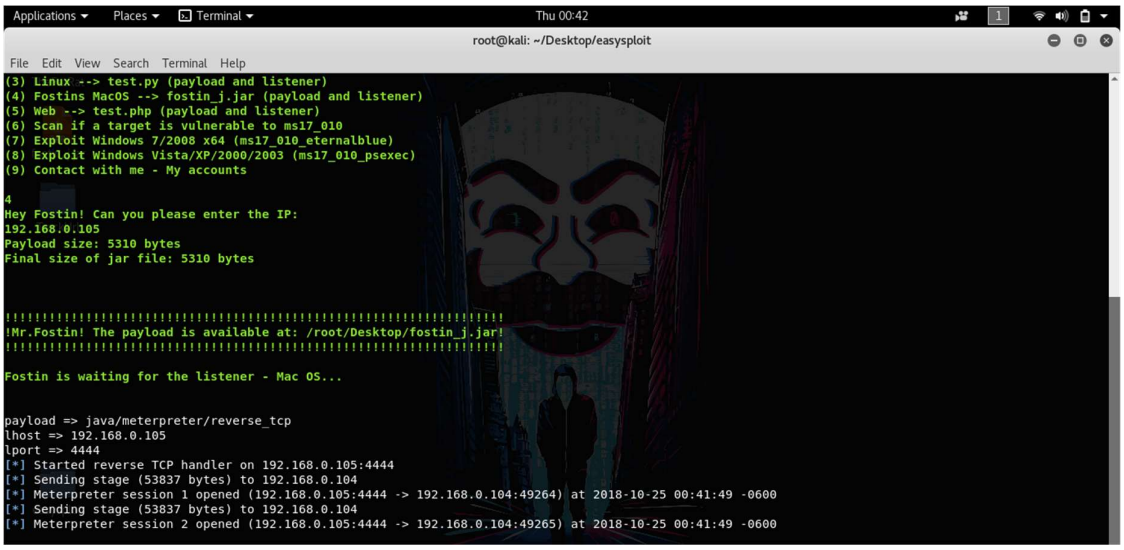
**Step 4:**

- To execute the program set **your IP**



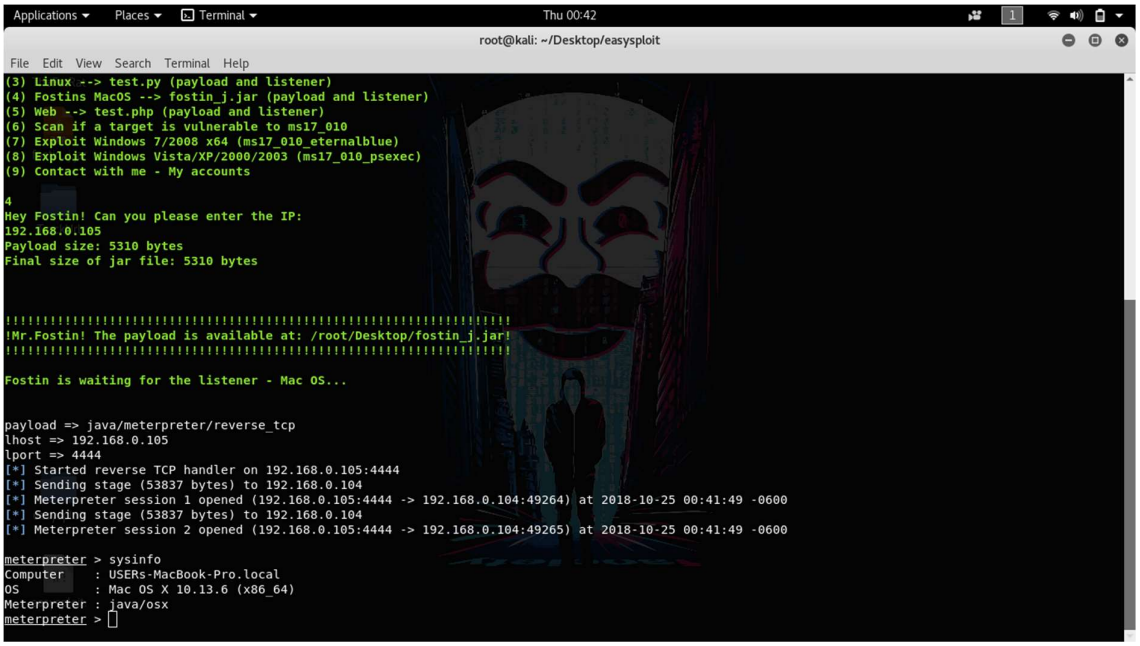

**Step 5:**

- Payload is generated as **fostin_j.jar** for Mac OS



## Step 6:

- Copy the payload to the victim system and run the application to get a connection with hacking system.



## 3.1 Commands to Exploits Mac OS

- **sysinfo –** Gets information about the remote system, such as OS
- **screenshot** – Create a screenshot of the interactive desktop.
- **pwd -** Print working directory.
- **search –** search for files.
- **mkdir –** Make directory.
- **rm** – remove the specified file.
- **rmdir** – Remove directory.
- **download** - Download a file or directory.
- **upload** - Upload a file or a directory.
- **cat** – Read the contents of a file to the screen.
- **localtime** – Display the targeted system's local date and time.

## HOW TO PREVENT ATTACK

This is the reason why we recommend that everyone should use a quality anti-spyware solution. These specialized software products can both remove all active dangerous infections on the host's computer and also protect them at all times.

- Continues updating of the system
- Continues check for vulnerability
- Don't allow downloading any apps from cloud websites or fake websites.
- Don't install apps with unknown resources enabled option.
- Use antivirus in your devices.
- Don't click any random link while surfing the internet.
- Never download unwanted src, doc, pdf, apk file from unknown source.

# 5. CONCLUSION

The backdoor application when installed and turned on the system allows attacker to read, write and modify data. Cautions are.

- Keep your System up to date.
- Installing antivirus software on your System.
- Firewall can prevent backdoor attacks.
- Don’t click any random link while surfing the internet.

# 6. REFERENCES


- https://github.com/KALILINUXTRICKSYT/easysploit
- https://docs.kali.org/introduction/what-is-kali-linux
- https://www.youtube.com/watch?v=UOUry9ov9rM
- https://www.youtube.com/watch?v=9J479dModb8