Task-1:

Kali Linux - Hands-on:

Practice basic to advance Linux commands and try to install Kali Linux tools from GitHub in your Kali Linux and use it to perform any type of attack.

Target site : http://testphp.vulnweb.com/

Some of the basic to advance linux commands:

1.ls	11.ln	21.top	31.lscpu,pci,usb
2.cd	12.find	22.kill	32.ifconfig
3.pwd	13.chmod	23.pkill	33.netstat
4.mkdir	14.chown	24.grep	34.ss
5.rm	15.chgrp	25.uname	35.ssh
6.cp	16.umask	26.whoami	36.scp
7.mv	17.tar	27.df	37.wget
8.touch	18.gzip	28.du	38.curl
9.cat	19.zip	29.free	39.git clone
10.head	20.ps	30.uptime	40.apt-get etc

Some of the tools i have exported from github:

I have cloned some tools like:

- 1.phoneinfoga
- 2.breacher
- 3.scapy
- 4.yerisinia
- 5.embomber
- 6.h8mail
- 7.I-see-you
- 8.pentbox
- 9.ufonet
- 10 raven-storm
- 11.ufonet etc..

```
[root@parrot]-[/home/lonewolf]
                                                              ufonet
92.168.126.252 Documents hashes.txt pentbox
                                                   sha.lst
                Downloads I-See-You phoneinfoga sh.txt
                                                              Videos
                                      Pictures
                                                   spiderfoot WhatBreach
1.pcap
                dump.pcap Music
c2.pcap
                EmBomber
                          my.txt
                                      Public
                                                   Templates
                                                              yersinia.log
                                      Raven-Storm tools
Desktop
                h8mail
                                                              zphisher
    oot@parrot]-[/home/lonewolf]
```

We are using a tool called: EmBomber/Zero-attacker

```
[lonewolf@parrot]-[~]
  $15
192.168.126.252 Downloads
                        I-See-You
                                    Pictures
                                               Templates
                                                            zphisher
Breacher dump.pcap Music
                                    Public
                                                tools
                                 Raven-Storm ufonet
c1.pcap
              EmBomber
                         my.txt
                                  sha.lst Videos
c2.pcap
              h8mail
                         path
Desktop
              hashes.txt pentbox
                                    sh.txt
                                               WhatBreach
Documents
              iplocator phoneinfoga spiderfoot yersinia.log
-[lonewolf@parrot]-[~]
  scd EmB*
-[lonewolf@parrot]-[~/EmBomber]
Banner.txt EmBomber.py README.md
-[lonewolf@parrot]-[~/EmBomber]
  - $cd Zero*
 [lonewolf@parrot]-[~/EmBomber/Zero-attacker]
 - $1s
 .jpg info.py
                 LICENSE requirements.txt zero.py
                                                    zero-tool.py
2.jpg install.bat README.md start.bat
                                          Zero-Tool
  [lonewolf@parrot]-[~/EmBomber/Zero-attacker]
  $./start.bat
```

```
THEADME IT GPL-10 liberse

BY: Zero Offens Security

1: Zero-Tools (Hacking Tools) in a law 2: Zero-Paid-Tools on of a device 3: Info (about-us)

> 1 Installation

Fur the following command for full installation:
```

```
1. Ip-Scanner 7. Sub-Domain-Scanner 2. Discord-Nuke 8. DDOS-TOOL 3. Subdirectory-Scanner 9. Discord-Token-Grabber 4. Email-Boomber 9. 10. Keylogger 5. Phone-Locator 11. Web-Crawler 6. Port-Scanner 12. Reverse-Shell 12. Reverse-Shell 13. Reverse-Shell 14. Reverse-Shell 15. Reverse-Shell 16. Reverse-Shell 16. Reverse-Shell 16. Reverse-Shell 17. Reverse-Shell 17. Reverse-Shell 18. Reverse-S
```

```
Request sent!
Request sent!into lo and
Request sent!
Request sentillation
Request sent!
Request sent!
Request sent!
Request sent!
Request sent!
Request sent!
```

Attack is carried out in this way and we can see it on wireshark:

