Class Instruction

1. Please make sure you download the **Redhat8** virtual machine and **Kali** virtual machine (if you do not have one) from the following link:
    Redhat8: https://drive.google.com/open?id=0BzkPm4m1AGy4N3Z4TldfNXRudlU
    Kali: https://www.offensive-security.com/kali-linux-vmware-virtualbox-image-download/

2. **Import** the virtual machines that you downloaded into your VMware software (such as VMware Workstation, VMware Fusion, and VMware Player, *etc.*).

3. Make sure those two virtual machines are in the same network. To do that right click the virtual machine in VMware software, go to **Settings…—> Network Adapter.** Make sure both of them have the same settings

4. In **Redhat8** to check the IP address using command:

```
$ /sbin/ifconfig
```

5. Upload the netcat installer, **nc-1.10-15mdk.i586.rpm** and **es-nweb.zip** files into **Redhat8**. For OSX and Linux, you can use **scp** command (For reference: http://www.hypexr.org/linux_scp_help.php), for Windows you can use **WinSCP** (https://winscp.net/eng/download.php)

6. For install Login **Redhat8** as **root** (password should be empty by default), find the uploaded installer. Run the following command in terminal:

```
$ rpm -i nc-1.10-15mdk.i586.rpm
```

7. To install nweb login as **john**, and find the uploaded zip file. Type the following command:

```
$ unzip es-neweb.zip
$ tar xvf nweb.tar
$ gcc -o nweb nweb.c
```

8. Make sure the system can generate core dump file, by type the following command:

```
$ ulimit -c unlimited
```

9. To run the nweb, type the following command:

```
$ ./nweb 8888 .
```

10. Make sure the nweb application is running by type the following command:

```
$ ps -aux | grep nweb
```

11. To crash the nweb application, open a terminal on Kali, type the following command. replace the [length] with a actual number such as 1200, replace the [IP_address] with your **Redhat8** IP address

```
$ perl -e “print ‘GET /’. ‘A’x [length] . ‘ HTTP/1.1’” | nc [IP_address] 8888
```

GDB cheatsheet

$ gdb -core [core_dump]	gdb analysis the core dump
$ gdb attach [pid]	gdb attach to an running pid

In GDB

$ continue	continue normal execution
$ step	go the next instruction, diving into function
$ next	go to next instruction, but do not dive into functions
$ info registers	print the names and values of all registers
$ backtrace	examine the stack
$ exit	exit GDB debugger
$ x/#of words to display	dump memory content

For more command please reference to: http://darkdust.net/files/GDB%20Cheat%20Sheet.pdf

Metasploit

- Launch Metasploit framework by the following command:

```
$ msfconsole
```

- The payload we are going use is **payload/linux/x86/shell_reverse_tcp** with **x86/alpha_mixed encoder**
- You can use **use** command and **show options** to setup variables. For more information please reference to the Metasploit manual: http://www.cse.usf.edu/~xou/msf_user_guide.pdf
- You might also need tools such as **pattern_create.rb** and **pattern_offset.rb**, of which you can find in the following path:

/usr/share/metasploit-framework/tools/exploit/