Complete Ethical Hacking Bootcamp: Zero To Mastery

zerotomastery.io

Resources For EachTool We Will Use(Attacks/Exploits Are Not Listed):

For Information Gathering:

1) Whatweb -https://tools.kali.org/web-applications/whatweb
2) theHarvester - https://tools.kali.org/information-gathering/theharvester
3) Red Hawk - https://github.com/Tuhinshubhra/RED_HAWK
4) Sherlock - https://github.com/sherlock-project/sherlock
5) Our Own Email Scraper - - https://mega.nz/folder/sMoUmTDI#SVy3plBr4DzTQEeaOgbCxw

Decryption key for Mega link - SVy3plBr4DzTQEeaOgbCxw

For Scanning:

6) Netdiscover - https://kalilinuxtutorials.com/netdiscover-scan-live-hosts-network/
7) Nmap - https://nmap.org/
8) Zenmap - https://nmap.org/zenmap/

For Vulnerability Analysis:

9) Nmap Scripts - https://nmap.org/book/man-nse.html
10) Google - https://www.google.com/
11) Searchsploit - https://www.exploit-db.com/searchsploit
12) Nessus - https://www.tenable.com/products/nessus

For Python Coding Project #1 - Portscanner:

13) Our Own Portscanner - https://mega.nz/folder/sMoUmTDI#SVy3plBr4DzTQEeaOgbCxw

For Exploitation & Gaining Access:

14) Msfconsole - https://www.offensive-security.com/metasploit-unleashed/msfconsole/
15) Routersploit - https://github.com/threat9/routersploit

For Gaining Access(Viruses,Trojans,Payloads..):

16) Msfvenom - https://www.offensive-security.com/metasploit-unleashed/msfvenom/
17) Veil - https://github.com/Veil-Framework/Veil-Evasion
18) TheFatRat - https://github.com/Screetsec/TheFatRat
19) Hexeditor - https://itsfoss.com/hex-editors-linux/

For Python Coding Project #2:

20) Our Own Backdoor - - https://mega.nz/folder/sMoUmTDI#SVy3plBr4DzTQEeaOgbCxw
21) Our Own Server - - https://mega.nz/folder/sMoUmTDI#SVy3plBr4DzTQEeaOgbCxw

For Website Application Penetration Testing:

22) Dirb - https://tools.kali.org/web-applications/dirb
23) Burpsuite - https://portswigger.net/burp
24) Hydra - https://tools.kali.org/password-attacks/hydra
25) DVWA - https://www.cyberpunk.rs/dvwa-damn-vulnerable-web-application

For Python Coding Project #3 - Bruteforcer, Directory Discovery:

26) Our Own Bruteforcer - https://mega.nz/folder/sMoUmTDI#SVy3plBr4DzTQEeaOgbCxw
27) Our Own Directory Discover Program - https://mega.nz/folder/sMoUmTDI#SVy3plBr4DzTQEeaOgbCxw

For Man In The Middle - MITM:

28) Bettercap - https://www.bettercap.org/
29) Ettercap - https://www.ettercap-project.org/
30) Scapy - https://scapy.net/

For Wireless Access Point Cracking:

31) aircrack-ng - https://www.aircrack-ng.org/
32) airodump-ng - https://www.aircrack-ng.org/doku.php?id=airodump-ng
33) aireplay-ng - https://www.aircrack-ng.org/doku.php?id=aireplay-ng
34) Hashcat - https://hashcat.net/hashcat/

References For Certain Lectures:

1) Downloading Virtual Box & Kali Linux Lecture:

VBox Download - https://www.virtualbox.org/
Kali New Version Download - https://www.kali.org/downloads/
Old Kali Versions - http://old.kali.org/kali-images/

2) Linux Operating System Section:

Linux filesystem explained - https://www.linux.com/training-tutorials/linux-filesystem-explained/
Basic Terminal Commands - https://ubuntu.com/tutorials/command-line-for-beginners#1-overview

3) Gathering Emails Using theHarvester & Hunter.io:

Hunter Website - https://hunter.io/

4) Finding Usernames With Sherlock:
Sherlock Tool - https://github.com/sherlock-project/sherlock

5) Bonus - Email Scraper Tool in Python 3:
email-scraper.py - https://mega.nz/folder/sMoUmTDI#SVy3plBr4DzTQEeaOgbCxw

6) Installing Vulnerable Virtual Machine:
Metasploitable - https://information.rapid7.com/download-metasploitable-2017.html?LS=1631875

7) Coding a Portscanner in Python 3:
portscanner.py - https://mega.nz/folder/sMoUmTDI#SVy3plBr4DzTQEeaOgbCxw

8) Setting Up Vulnerable Windows 10:
Rufus - https://rufus.ie/

9) Crashing Windows 10 Machine Remotely:
https://github.com/ButrintKomoni/cve-2020-0796
https://github.com/jiansiting/CVE-2020-0796

10) Exploiting Windows 10 Machine Remotely:
https://github.com/ZecOps/CVE-2020-0796-RCE-POC

11) TheFatRat Payload Creation:
https://github.com/Screetsec/TheFatRat

12) Python Coding Project #2 - Backdoor:
backdoor.py - https://mega.nz/folder/sMoUmTDI#SVy3plBr4DzTQEeaOgbCxw
server.py - https://mega.nz/folder/sMoUmTDI#SVy3plBr4DzTQEeaOgbCxw

13) ShellShock Exploitation:
Shellshock VM - https://pentesterlab.com/exercises/cve-2014-6271/course

14) Bruteforcer in Python:
bruteforce.py - https://mega.nz/folder/sMoUmTDI#SVy3plBr4DzTQEeaOgbCxw

15) Hidden Directory Discovery:
directories.py - https://mega.nz/folder/sMoUmTDI#SVy3plBr4DzTQEeaOgbCxw

16) Practice Note:
HackTheBox - https://www.hackthebox.eu/

17) Bug Bounty Note:
BugCrowd - https://www.bugcrowd.com/