Software Hardware List

Chapter number	Software required (With version)	Free/Proprietary	If proprietary, can code testing be performed using a trial version	If proprietary, then cost of the software	Download links to the software	Hardware specifications	OS required
1	The harvester	Free	NA	NA	http://www.sampleURl.com	Common Unix with 2GB RAM	Kali linux
1	Tor Browser for Windows	Free	NA	NA	https://www.torproject.org/download/download-easy.html.en#windows	2GB RAM	windows
1	exiftool	Free	NA	NA	https://www.sno.phy.queensu.ca/~phil/exiftool/index.html	2GB RAM	Kali Linux
1	Nexpose	Proprietary	Yes for 30 days	NA	https://www.rapid7.com/products/nexpose/	2GB RAM	Windows
2	LinEnum	Free	NA	NA	https://github.com/rebootuser/LinEnum	2GB RAM	Kali linux
2	Nmap	free	NA	NA	https://nmap.org/download.html	2GB RAM	windows
3	SDNPWN	free	NA	NA	https://github.com/smythtech/sdnpwn	2GB RAM	Kali linux
4	Empire	Free	NA	NA	https://github.com/EmpireProject/Empire	2GB RAM	Kali linux
5	Docker	Free	NA	NA	https://download.docker.com	2GB RAM	UBUNTU 16.04
6	Jenkins	Free	NA	NA	https://jenkins.io	2GB RAM	UBUNTU 16.04
6	Zed Attack Proxy (ZAP)	Free	NA	NA	https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project	2GB RAM	Kali linux
7	Metasploit	Proprietary	Yes	NA	https://www.rapid7.com/products/metasploit/download/	2GB RAM	windows
7	The Veil Framework	Free	NA	NA	https://github.com/Veil-Framework/Veil	2GB RAM	Kali linux
7	Nishang	Free	NA	NA	https://github.com/samratashok/nishang	2GB RAM	Kali linux
9	dual-tone multifrequency (DTMF)	Free	NA	NA	http://www.polar-electric.com/DTMF/	2GB RAM	windows
9	vomit	Free	NA	NA	http://vomit.xtdnet.nl/	2GB RAM	Kali Linux
9	Viproy VoIP Penetration Testing Kit (v4)	Free	NA	NA	https://github.com/fozavci/viproy-voipkit	2GB RAM	Kali Linux
9	SIGPLOIT – TELECOM SIGNALING EXPLOITATION FRAMEWORK	Free	NA	NA	https://github.com/SigPloiter/SigPloit	2GB RAM	Kali Linux
11	The Router Exploitation Framework	Free	NA	NA	https://github.com/reverse-shell/routersploit	2GB RAM	Kali Linux
12	BinWalk	Free	NA	NA	https://github.com/ReFirmLabs/binwalk/	2GB RAM	Kali Linux
12	firmwalker	Free	NA	NA	https://github.com/craigz28/ firmwalker	2GB RAM	Kali Linux

Detailed installation steps (software-wise)

The steps should be listed in a way that it prepares the system environment to be able to

test the codes of the book.

1. **The harvester:**
    1. git clone `https://github.com/laramies/theHarvester`
    2. cd theHarvester
    3. ./theHarvester
2. **Tor Browser for Windows**
    1. https://www.torproject.org/download/download-easy.html.en#windows
    2. Run the executable
3. **Exiftool:**
    1. https://www.sno.phy.queensu.ca/~phil/exiftool/index.html
    2. tar -xzf Image-ExifTool-10.76.tar.gz
    3. cd Image-ExifTool-10.76
    4. make
    5. make install
    6. ./exiftool
4. **Nexpose:**
    1. https://www.rapid7.com/products/nexpose/
5. **LinEnum:**
    1. git clone `https://github.com/rebootuser/LinEnum`
    2. cd LinEnum
    3. ./LinEnum.sh
6. **Nmap:**
    1. https://nmap.org/download.html
    2. Run the installation executable nmap.exe
7. **SDNPWN:**
    1. git clone `https://github.com/smythtech/sdnpwn`
    2. cd sdnpwn

3. ./sdnpwn.py

8. **Empire:**
    1. git clone `https://github.com/EmpireProject/Empire`
    2. cd Empire
    3. ./setup/install.sh
    4. ./Empire.
9. **Docker:**
    1. curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -
    2. sudo add-apt-repository "deb [arch=amd64] https://download.docker.com/linux/ubuntu $(lsb_release -cs) stable"
    3. sudo apt-get update
    4. sudo apt-get install -y docker-ce
10. **Jenkins:**
    1. apt-get install Jenkins
11. **Zed Attack Proxy (ZAP):**
    1. https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
    2. Download ZAP
12. **Metasploit:**
    1. curl https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/config/templates/metasploit-framework-wrappers/msfupdate.erb > msfinstall && chmod 755 msfinstall && ./msfinstall
    2. ./msfconsole
13. **The Veil Framework:**
    1. git clone https://github.com/Veil-Framework/Veil
    2. ./setup.sh
    3. ./Veil.py
14. **The Router Exploitation Framework**
    1. git clone https://github.com/reverse-shell/routersploit
    2. cd routersploit

3. ./rsf.py

15. **BinWalk:**
    1. git clone https://github.com/ReFirmLabs/binwalk/
    2. cd binwalk
    3. ./deps.sh
16. **firmwalker:**
    1. git clone https://github.com/craigz28/ firmwalker
    2. cd firmwalker
    3. ./firmwalker.sh
17. **dual-tone multifrequency (DTMF):**
    1. visit http://www.polar-electric.com/DTMF/
    2. install the downloaded .exe file
18. **vomit :**
    1. http://vomit.xtdnet.nl/
    2. download the release version
19. **Viproy VoIP Penetration Testing Kit (v4) :**
    1. git clone https://github.com/fozavci/viproy-voipkit
    2. Copy "lib", "modules" and "data" folders' to Metasploit folder in your system
20. **SIGPLOIT – TELECOM SIGNALING EXPLOITATION FRAMEWORK:**
    1. git clone https://github.com/SigPloiter/SigPloit
    2. cd bin
    3. ./SiGploit.py