

Offensive Penetration Testing Resource List

Instructor Name: Alejandro Guinea

Instructor Website: <https://www.linkedin.com/in/alejandro-guinea-36533636>

Teaching Assistant: Tahir Ibrahim - <https://www.linkedin.com/in/tahir-ibrahim/>

Course Resource List

- Kali Linux
 - Kali Linux is an operating system used to perform attacks in the exercises shown on the course
 - <https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/>
- Bee-box
 - Custom VM pre-installed with bWAPP vulnerabilities
 - <https://sourceforge.net/projects/bwapp/files/bee-box/>
- Vulnhub - XSS & MySQL FILE
 - XSS exploitation
 - MySQL injection with FILE privilege
 - <https://www.vulnhub.com/entry/pentester-lab-xss-and-mysql-file.66/>
- Vulnhub - Wallabys nightmare
 - <https://www.vulnhub.com/entry/wallabys-nightmare-v102.176/>
- VulnServer
 - Used on the buffer overflow module
 - <https://github.com/stephenbradshaw/vulnserver>
- The above resources were used during the course and would be recommended to download to follow along with the course

Cybrary Labs List

- Module 3 Hackers Main Tools
 - Nmap
 - www.cybrary.it/catalog/cybrscore/scanning-and-mapping-networks

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

CYBRARY

- Wireshark
 - <https://www.cybrary.it/catalog/cybrscore/wireshark/>
- TCPdump
 - <https://www.cybrary.it/catalog/cybrscore/tcpdump/>
- Module 4 Information Gathering
 - Nmap Scanning
 - <https://app.cybrary.it/browse/cybrscore/preliminary-scanning>
 - Port Scanning
 - <https://www.cybrary.it/catalog/cybrscore/specialized-linux-port-scans/>
 - Vulnerability Scanning
 - <https://app.cybrary.it/browse/cybrscore/vulnerability-scan-analysis>
 - Google Hacking
 - <https://app.cybrary.it/browse/cybrscore/open-source-collection>
 - Enumeration
 - <https://app.cybrary.it/browse/learn-on-demand/use-banner-grabbing-techniques-to-enumerate-services-on-a-linux-server>
- Module 5 Exploits
 - XSS
 - <https://app.cybrary.it/browse/cybrscore/introduction-to-owasp-top-ten-a7-cross-site-scripting-scored>
 - SQL Injection
 - <https://app.cybrary.it/browse/lab/sql-injection>
- Module 6 Buffer Overflow
 - <https://app.cybrary.it/browse/cybrscore/analyze-structured-exception-handler-buffer-overflow-exploit>
- Module 7 Privilege Escalation
 - <https://app.cybrary.it/browse/learn-on-demand/escalate-privileges-in-linux>
 - <https://app.cybrary.it/browse/learn-on-demand/configure-standard-permissions-in-linux>
 - <https://app.cybrary.it/browse/learn-on-demand/configuring-acl-permissions-on-files>
- Module 8 Pen Test Simulation
 - <https://app.cybrary.it/browse/cybrscore/comprehensive-threat-response>

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

CYBRARY

Extra Resources

- Kioptrix 2014
 - <https://www.vulnhub.com/entry/kioptrix-2014-5,62/>
- FristiLeaks 1.3
 - <https://www.vulnhub.com/entry/fristileaks-13,133/>
- Stapler 1
 - <https://www.vulnhub.com/entry/stapler-1,150/>
- VulnOS 2
 - <https://www.vulnhub.com/entry/vulnos-2,147/>
- SickOs 1.2
 - <https://www.vulnhub.com/entry/sickos-12,144/>
- Brainpan 1
 - <https://www.vulnhub.com/entry/brainpan-1,51/>
- HackLAB Vulnix
 - <https://www.vulnhub.com/entry/hacklab-vulnix,48/>
- DevRandom Scream
 - <https://www.vulnhub.com/entry/devrandom-scream,47/>
- pWnOS 2.0
 - <https://www.vulnhub.com/entry/pwnos-20-pre-release,34/>
- SkyTower 1
 - <https://www.vulnhub.com/entry/pwnos-20-pre-release,34/>
- DC416
 - CTF challenges
 - <https://www.vulnhub.com/series/dc416,99/>
- PwnLab init
 - <https://www.vulnhub.com/entry/pwnlab-init,158/>
- Mr-Robot 1
 - <https://www.vulnhub.com/entry/mr-robot-1,151/>
- IMF 1
 - <https://www.vulnhub.com/entry/imf-1,162/>

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.