ZROC 102

30-day training program on Practical Security Researching

Zumaroc Education
30-day Cybersecurity Researcher Training
Class Time: Monday – Thursday, 5pm – 7pm (WAT, EST)

OSCP certified Instructor
learn@zumaroc.com
Office Hours, by appointment

Course Overview:

This curriculum is designed to work you from the ground up to becoming bug bounty player. You will learn most of the important tools and techniques used to test the security of applications and network. Students will learn how to use professional tools to practice enumerating and exploiting known vulnerabilities as well as discovering new "bugs". This course will also look at reporting and responsible disclosure, to ensure the delivery of competent security penetration test / bug discovery reports with concise description, evidence and recommendation.

Learning Outcomes:

On the successful completion of the course, students will learn:

1. How to perform basic foot printing and reconnaissance.
2. Network and service enumeration on a wide variety of systems and services.
3. Vulnerability Analysis and exploitation techniques.
4. Privilege escalation techniques.
5. How to test for and exploit OWASP top 10 web application vulnerabilities.
6. How to write quality bug / penetration testing reports.

Course Requirements/Graded Components:

1. Class attendance 10%
2. Final Simulation Exam and Report 90%

Course Outline

Module	Outline	Days Start: 5:00pm End: 7:00pm
1	○ Course Resources ○ Link to external resources ○ Disclaimer ○ Introduction - Introduction and course overview ○ Frequently asked questions ○ Being a hacker ○ Note keeping - Effective note keeping and Pentest reporting. ○ Networking refresher ○ IP addresses ○ MAC addresses ○ TCP, UDP, and the Three-Way Handshake ○ Common Ports and Protocols ○ Lab setup ○ Installing VirtualBox, Kali Lab setup ○ Registering for ZrocCyberSec, HTB, Tryhackme, Portswigger Academy	Monday
	• Introduction to Linux ○ Exploring Kali Linux ○ Navigating the File System ○ Users and Privileges ○ Common Network Commands ○ Viewing, Creating, and Editing Files ○ Starting and Stopping Kali Services ○ Scripting with Bash	Tuesday
	○ Hacking Methodology ○ Reconnaissance ○ Scanning ○ Gaining Access ○ Maintaining Access ○ Clearing Tracks	Wednesday
	○ Passive Information Gathering (Reconnaissance) ○ Overview ○ Identifying our target ○ Hunting for subdomains (theharvester, knockpy, amass)	

	○ Whois enumeration ○ Google hacking ○ Shodan ○ Researching potential vulnerabilities ○ Introduction to Bug Bounty (Bug crowd & Hackerone, Zroccybersec) ○ Introduction to Grading Scale	Thursday
	○ Scanning and Enumeration ○ Scanning with Nmap o ○ Enumerating HTTP HTTPS ○ Enumerating SMB ○ Enumerating SSH ○ Enumerating SMTP ○ Enumerating NFS	Monday
	○ Exploitation Basics ○ Manual Exploitation ○ Automated Exploitation ○ Reverse and Bind shells	Tuesday
2	○ Linux Privilege Escalation ○ Understanding Permissions ○ Privilege Escalation Tools ○ Kernel Exploits ○ Weak File Permissions ○ Sudo ○ SUID executables	Wednesday
	○ Windows Privilege Escalation ○ Privilege Escalation Tools ○ Kernel Exploits ○ SE attacks ○ Stored Credentials ○ Trusted Service Paths ○ Vulnerable Services	Thursday
	○ Practice Labs	Friday
3	○ Testing Common Web Application Vulnerabilities ○ Introduction to BurpSuite ○ Login attacks and authorization bypass ○ Broken Authentication ○ Sensitive Data Exposure overview ○ Parameter manipulation and IDOR ○ Broken access control	Monday
	○ Testing Common Web Application Vulnerabilities ○ Brute forcing and rate limiting ○ Parameter Manipulation and account takeover	Tuesday

	○ Logic attack defenses ○ Exploiting file uploads ○ Cross origin Resource Sharing (CORS)	
	○ Testing Common Web Application Vulnerabilities ○ Remote File Inclusion (RFI) ○ Local File Inclusion (LFI) ○ Insecure Deserialization	Wednesday
4	○ Testing Common Web Application Vulnerabilities ○ Cross-site request forgery (CSRF) ○ Account takeover using CSRF ○ Anti-CSRF token implementation ○ Bypassing CSRF protection ○ Examples	Thursday
	○ Practice Labs	Friday
	○ Testing Common Web Application Vulnerabilities ○ Cross-site scripting (XSS) ○ Testing for Reflected XSS ○ Testing for stored XSS ○ Testing for DOM XSS ○ WAF bypass techniques	Monday
	○ Testing Common Web Application Vulnerabilities ○ Server-side request forgery (SSRF) ○ Subdomain takeover ○ Command Injection ○ HTML Injection ○ Directory Traversal ○ Missing/insufficient SPF record	Tuesday
	○ Documenting and Report Writing ○ Vulnerability Disclosure Report Writing ○ Pen Test Report Writing ○ Sample Report Template	Wednesday
	○ Final Simulation exams HTB	Thursday
	○ Final Report Submission	Saturday

Prerequisites

While the skills mentioned below are not mandatory, they would make the course easier to comprehend and follow.

1. Basic Linux and command line understanding.
2. Basic programming / scripting understanding (e.g. python or bash)
3. Familiarity with Kali Linux.

Course Policies

Virtual Classroom Culture

Success in this course will depends on your attitude and eagerness to learn. In order to get the most from the class, students are required to:

1. Sign into the virtual class on time.
2. Stay for the entire duration of the class.
3. Be fully present in the class as distractions will only have adverse effects for the students.
4. Always come to the class with computers. The use of mobile phones to join the class meetings is strongly discouraged.

Integrity

Since your assignments, quizzes, and exams will be conducted in an open-book, open-note format. All work on assignments, quizzes, and exam should be your own. Submitting someone else's work as your own is a serious form of academic dishonesty. You should always give credit, and site sources appropriately. In your journey to be a cyber security expert this is especially important.

Attendance

Live sessions are for Questions & Answers, please watch the recording before coming to class. Class is for Questions concerning the contents taught. You can also reach out via the Discord channel.

Responsibility

Everyone in the training is expected to participate in all assigned activities and to work hard to develop a mastery of the InfoSec and OffSec concepts that are presented in the mini lectures. Your participation in class discussions and your submissions of assignments and completions of quizzes and exam should provide tangible evidence that you have achieved a sophisticated understanding of OffSec concepts.

Students are responsible for all assignments, even if they are absent. Late papers, failure to complete the readings assigned for class discussion, and lack of preparedness for in-class discussions and presentations will jeopardize your successful completion of this course.

Certificate of Completion

ONLY STUDENTS WHO GET **A FINAL SCORE OF 70%** AND ABOVE WILL BE ISSUED A CERTIFICATE OF COMPLETION

Contact Information

Instructor:	OSCP certified Instructor
Training Number:	ZB102: 30-day training program on Practical Security Researching
Semester:	Rolling, starts first Monday of the new month
Email Address:	For private communications, email me learn@zumaroc.com (preferred)

Online Resources

Links	Descriptions
Oracle VM VirtualBox https://www.offensive-security.com/kali-linux-vm-vmware-virtualboximagedownload/	Free and open-source hosted hypervisor Kali image download
http://keepnote.org/ https://www.giuspen.com/cherrytree/ https://www.notion.so/	KeepNote is a note taking application that works on Windows, Linux, and MacOS X. A hierarchical note taking application, featuring rich text and syntax highlighting. Notion is an application that provides components such as notes, databases, kanban boards, wikis, calendars and reminders.
https://getgreenshot.org/downloads/	Free and open-source screenshot program for Microsoft Windows

ZrocCyberSec Researcher Account Registration

ZrocCyberSec homepage: https://zumaroc.com/signup/start

Registration as a researcher is **MANDATORY**

HackTheBox(HTB) Account Registration

HTB homepage: https://www.hackthebox.eu/individuals You will need to register using your personal email.
VIP subscription (it cost GBP 10) is **PAID** **subscription is advised**.

Tryhackme Account Registration

Tryhackme homepage: https://tryhackme.com/signup **PAID** subscription is advised.

Portswigger Academy

Portswigger registration page: https://portswigger.net/users/register

How You Will Be Evaluated

Your final training grade will be determined according to the following formula:

GRADING SCALE***

Grades Scored Between	Will Equal
70% to 100%	PASS
0% and Less Than 70%	FAIL