Ekene Joseph

Penetration testing, Malware Analysis, vulnerability analysis and web administrator
Lagos
cybervaultsecurities.io@gmail.com
+2348062948524

Professional Summary

I bring over seven years of expertise in information security with a strong focus on cyber security and penetration testing .

I have conducted penetration testing, phishing simulations, and vulnerability assessments for web servers and networks across government agencies, financial institutions, and corporate enterprises, ensuring robust security against evolving threats.

i am an expert in penetration testing using kali linux, i have a project on udemy which focuses on penetration testing with kali linux OS, with practicals on a virtual lab.

Link to projects are found below

https://www.udemy.com/user/ekene-joseph-6/

https://medium.com/@Ekenejoseph

https://www.udemy.com/course/learn-cyber-security-from-scratch-no-coding-experience/?couponCode=LETSLEARNNOW

https://m.youtube.com/@cybervolt-j6s

https://www.linkedin.com/in/ekene-joseph-135908198/

These are my skills and part of the topics in my Udemy course and youtube channel:

- webserver vulnerability assessment OWASP
- Python in cyber security
- cybersecurity automation using python
- Virtualization
- webserver directory enumeration
- Nessus
- Owasp-zap
- Burp suite
- Using Burp suite to exploit common vulnerabilities.
- SQLI detection and exploitation with burp suite
- XSS scanning and exploitation with burp suite
- LFI scanning and exploitation with burp suite
- Metasploit frame work
- Nmap scanning techniques
- Nmap scripting engine as a vulnerability scanner
- Vulnerability scanning
- subdomain enumeration
- RCE detection and exploitation
- stealth scanning techniques with Nmap

Willing to relocate: Anywhere

Work Experience

instructor at Udemy (penetration testing)

Udemy

October 2024 to Present

As a cybersecurity instructor on Udemy, I have designed and delivered a comprehensive, hands-on course in penetration testing, guiding learners from a beginner to an advanced level. This course equips students with the practical skills to understand and counteract black-hat hacking tactics, empowering them to think like a hacker while mastering professional techniques to secure systems effectively. The curriculum is tailored to help aspiring security experts excel in the cat-and-mouse dynamics of cybersecurity, transforming them into adept professionals in the field.

Blending practical work with solid theoretical training, we take you from the basics of ethical hacking through to mastery, giving you the training you need not just to hack, but also to secure against a hack.

While the theory is important, we understand that it can also be dry and uninspiring. For this reason, this course is packed with examples that you can follow. This practical focus starts from the beginning, where we will teach you about penetration testing and show you how to install the software required, and jump right into cyber security

Throughout, you will analyze and exploit various systems from regular websites through to sprawling networks, along with hacking servers and clients. More than just hacking, you'll also learn how to conduct efficient penetration testing techniques.

This approach gives you the foundational education that you need not just to hack any given system, but also to secure it, with each module covering both sides of the coin.

Researcher (Remote)

Cybervolt-Lagos, GU

October 2019 to Present

- I engage in penetration testing and ethical hacking services and training.
- I engage in scanning, enumeration and exploitation of web application vulnerabilities.
- I used tools like Burp suite, Nmap, Metasploit framework, Nessus, owasp-zap, wire shark
- i used python to automate several tasks
- I researched on current vulnerabilities and malwares and ways in which they are exploited to gain root or shell, these
- I document in a professional report, to be submitted to IT.
- i did malware analysis, malware encryption,
- i did malware extension exploitation (from .exe to .doc or .xls) after encryption to pentest email security.
- i worked with terminal based malware in kali linux, and rats with GUI on windows.

Penetration tester and web administration (remote)

Cybervolt-Lagos, GU

June 2019 to Present

I run vulnerability assessment, automated and manual penetration testing on web applications, and web servers and also offer solutions to risks and vulnerabilities found.

i develop malware, exploit its extension and encrypt it to carry out phishing assessments.

I Implement and Maintain of windows DNS and DHCP services.

I used Kali Linux Operating system to run penetration tests on web servers and networks , with tools like, nmap, burpsuite pro, nessus scanner, hydra, john the riper, dirb, e.t.c

I used wire shark tool to analyze and investigate PCAP files, to check if malware activities are immenient

I tested webservers for OWASP Top 10 (SQL Injection, cross site scripting vulnerability, remote code execution vulnerability, local file inclusion vulnerability) and other vulnerabilities.

I used Hash algorithms and scripts to check integrity of files (File integrity monitoring).

I created an integrity baseline of target files/folders using the SHA-512 hashing algorithm.

I continuously made comparison of actual file vs. baseline and raised alarm if any change is noticed

I used power shell script to extract metadata from windows event viewer to be forwarded to third party API in order to derive geo location data.

I installed and configured Nessus essentials to run vulnerability scans on windows 10 host.

I engage in latest vulnerability research and ways to exploit them as well as mitigate them, I work with a team of other pen testers alike.

I engage with Costumers some times to explain a vulnerability or fixture.

i have also created and managed web servers for my clients, which includes domain name purchase, web hosting and management, website development (wordpress) and website adminstration, and i also help them to secure the website.

Penetration tester and Ethical hacking instructor

Cybervolt-Lagos

2022 to 2024

I teach penetration testing with Kali Linux to students using virtual box which includes,

reconnaissance, scanning, vulnerability assessment, exploitation, and reporting.

i focused primarily on web-application testing, i tailored a course that is designed to check all aspects of the web application's functionality, including looking for bugs with usability, compatibility, security, and general performance.

i also majored on OWASP top 10 vulnerability.

i teach students on how to use major pentesting tools like:

Nmap, Burp suite, jack the riper, Hydra, Metasploit, Wire shark e.t.c.

i also take them through capture the flag walk-through using vulnhunb to help students understand the general security landscape of webservers

instructor (on site) and Penetration tester (remote)

Okona industries-Lagos

March 2020 to February 2022

i instruct and educate staffs and company personnel on cyber security best practices in handling companies digital infrastructure like emails and websites, i educate staffs on current hacking trends and methods used by hackers to gain unauthorized access in to domain servers or computers.

i run penetration tests on their digital infrastructures like webservers and emails.

i used different malwares and trojans to launch a controlled phishing attacks on emails to access their security posture.

i some cases i exploit the extentions of these malwares from exe to doc or jpg, to access the security mail boxes.

i use burp suite on webservers to test for different vulnerabilities like RFI, LFI, XSS scripting, e.t.c according to OWASP top 10

Education

Grade A in Penetration testing with kali linux (offensive security)
Cybrary-Lagos
January 2023 to August 2023

Certificate of traning in Penetration testing
Cybrary, Inc.-Riverdale, MD
August 2021 to August 2022

certificate of training in cyber security for industrial control systems (ICS)
National Cybersecurity & Communications Integration Center Industrial Control Systems U.S. Department of Homeland Security-Washington, DC
May 2019 to May 2020

WAEC 'A' Level in Sciencce
Gateway Schools-Lagos
February 2005 to September 2009

Post-secondary (technical & vocational) in Kali Linux operating systems and Micro computing
zenith computer school-Lagos
August 2005 to May 2009

Skills

- perimeter hardening and risk mitigation
- web application Penetration testing
- Malware exploitation and cryptology
- fluent in wireshark
- Vulnerability research
- vulnerability assessment and information gathering
- Fluent with burp suite
- Email server penetration testing and phishing assessment
- Digital forensics
- penetration testing with kali linux
- Malware Analysis

Links

https://www.linkedin.com/in/ekene-joseph-135908198/

https://medium.com/@Ekenejoseph

https://www.udemy.com/course/learn-cyber-security-from-scratch-no-coding-experience/?couponCode=LETSLEARNNOW

https://m.youtube.com/@cybervolt-j6s

Certifications and Licenses

The West African Senior School Certificate Examination

Present

Gateway schools, Lagos

Certificate in Advanced Penetration testing

Present

Certificate of completion in Advanced Penetration testing Training
Cybrary - Greenbelt Park, MD, USA

Certificate of Completion on Cyber security within IT and ICS domains

Present

CISA - Certificate by US department of homeland security - for completion of the course on cyber security within IT and ICS domains.

3801 Nebraska Ave NW, Washington, DC 20528, United States