Kerolos Nagi Whaba

Penetration Tester

+201221509055 | kerlosnagi072@gmail.com | linkedin.com/kerolos-nagi | github.com/KerolosNagi

PROFESSIONAL SUMMARY

- Motivated security professional specializing in penetration testing and vulnerability assessment. Skilled in identifying and analyzing web and network vulnerabilities with a strong understanding of OWASP Top 10 and core security principles. Trained in ethical hacking and red teaming. Dedicated to enhancing organizational security and developing advanced expertise in penetration testing and security analysis.

Education

Egyption E-Learning University - EELU Egypt

Bachelor's Degree: Computers and information technology, GPA 3.06 *Sep 2021 – Jun 2025*

Graduation project +A

Experience

Red Team Penetration Tester Oct 2025 – Jan 2026

Digital Egypt Youth – HireReady Initiative *National Telecom Institute, NTI*

- Linux Administration: Administered RHEL-based Linux systems, including user and group management, file permissions, service management, networking configuration, virtualization, and Bash scripting
- Python Programming - Automation: Developed Python scripts for automation and data processing, applying functions, loops, and Object-Oriented Programming (OOP) concepts to solve practical problems
- Networking - Security Fundamentals: Implemented IP networking concepts, firewall configurations, and basic cryptographic techniques to enhance system security.
- Web Application Penetration Testing: Identified and exploited common web vulnerabilities such as SQLi, XSS, CSRF, SSRF, insecure file uploads, broken authentication and access control, path traversal, CORS misconfigurations, and OS command injection
- Network Penetration Testing: Conducted network scanning, enumeration, exploitation, privilege escalation, malware analysis, Denial of Service (DoS) testing, social engineering attacks, and wireless security assessments
- Mobile Application Security Testing: Tested Android applications for security vulnerabilities and applied secure coding and testing best practices
- Hands-On Labs - Practical Experience: Gained hands-on experience through virtual lab environments, applying Linux administration, Python automation, networking, and penetration testing techniques

Projects

Graduation Project | *Full-Stack Web Application* Oct 2024 – May 2025

- Built and security-tested a full-stack web application using React, Spring Boot, and MySQL
- Ensured seamless user experience with responsive design, interactive UI, and optimized backend performance.
- Implemented authentication, authorization, and performed manual security testing during development.
- Identified and fixed common web vulnerabilities while maintaining a production-ready codebase.

Training - Certifications

Red Teaming, Ethical Hacking, Bug Hunting and Penetration Testing Jul 2025 – Oct 2025

- Completed hands-on cybersecurity training covering Linux+, network exploitation, and real-world offensive security scenarios.
- Trained with industry-standard tools including Nmap, Nessus, Acunetix, Metasploit, and Burp Suite for reconnaissance, vulnerability assessment, and exploitation.
- Gained practical experience through PortSwigger Web Security Academy labs, focusing on modern web vulnerabilities and exploitation techniques
- Acquired foundational exposure to Active Directory attack paths, including enumeration, privilege escalation, and lateral movement techniques.

Android Application Security - Mobile Penetration Testing — Black Belt Edition Jan 2026 – in progress

- Completed advanced hands-on training in Android application penetration testing and reverse engineering, focusing on identifying and exploiting real-world mobile vulnerabilities.
- Performed static and dynamic analysis of Android applications including APK decompilation, AndroidManifest analysis, and SMALI code inspection.
- Utilized industry tools such as ADB, Frida, JADX, APKTool, and Burp Suite for runtime instrumentation, network interception, and vulnerability validation.
- Practiced exploiting Android components and common mobile weaknesses including exported activities, insecure data storage, intent manipulation, authentication bypass, and SSL pinning bypass.
- Applied practical mobile penetration testing workflows including vulnerability discovery, exploitation, and security assessment aligned with the OWASP Mobile Top 10.

SANS SEC560 – Enterprise Penetration Testing - SANS Institute apr 2026 – in progress

- Comprehensive penetration testing planning, scoping, and reconnaissance
- In-Depth Scanning and Initial Access
- Assumed Breach, Post-Exploitation, and Passwords
- Domain Domination, Azure Annihilation, and Reporting
- Penetration Testing Workshop

Technical Skills

Networking : CCNA Switching, Routing, and Wireless Essentials
Languages-scripting: Java, Python, Linux Commands, SQL(MySql), JavaScript, HTML
Tools:
-Conducted network reconnaissance and service enumeration using Nmap, uncovering exposed ports and outdated services across enterprise systems.
-Leveraged Metasploit to validate critical vulnerabilities and demonstrate real-world exploit impact during penetration tests.
-Analyzed network traffic with Wireshark to detect malicious beaconing, data exfiltration attempts, and protocol misconfigurations.
Soft Skills:: Communication, Team Collaboration, Problem Solving, Adaptability, Leadership, Time Management, Attention to Detail, Emotional Intelligence, Creativity, Interpersonal Skills