ABDELAAL ATIF ABDELGHAFFAR

Qatar, Doha • (974) 77493028 • abdelaalatif253@gmail.com • linkedin.com/in/abdelaal-abdelghaffar

OBJECTIVE

Cybersecurity professional with a strong interest in ethical hacking, penetration testing, vulnerability analysis, and network security. Hard-working, energetic, personable, and technical-minded individual. Possess exceptional customer service and communication skills with the strong ability to multitask and resolve issues quickly with utmost confidentiality. I am currently in a cybersecurity role where I continue to develop and learn new abilities while contributing to the overall success of the organization with over 4 years of experience and ongoing. I also possess:

- Experience in scripting languages including Python and Bash.
- Excellent task management. Ability to handle multiple projects simultaneously.
- Experience with security toolkits such as Kali Linux, Metasploit, and Burp Suite Pro.
- Proficient in translating information from technical to executive/management terminology
- Good knowledge of the operation of different cyber security frameworks such as ISO 27001, NIST, PCI DSS, NISCF and SWIFT CSP.

EDUCATION

Future University – Bachelor's, Computer Science (Honors)

- GPA: 3.29/4.0

CERTIFICATIONS

- CompTIA Security+ 701
- Network Security Associate (NSE 1, 2)
- (ISC)2 Certified in Cybersecurity
- OSCP (Soon July 2024)

EXPERIENCE

Electronic Banking Services (EBS Co. Ltd),
Onsite/Khartoum, SD November 2022 - Present
Cyber Security Engineer

- Developed a complete Security Operations Center platform from ground up using Open-Source Wazuh platform, along with other integrations Virustotal, Yara rules, and theHive to automate workflows and remediation.
- Extensive experience replicating malware in closed and isolated environment to track their activity and match them to specific IOCs for later tracking, logging and triaging with security solutions.
- Analyzed attack pattern and came up with mitigations that were implemented in our incident response plan and playbooks.
- Created custom rules for SIEMs and security solutions on the spot to enhance posture against recent threats such as the recent SSH critical vulnerability affecting more than 90% of servers and services across the world.
- Proficient in Bash and Python, developed custom scripts to automate tasks.
- Extensive knowledge of the MITREATTACK framework and other threat feeds from public and private feeds to supplement analyze that data to determine APT's TTPs.
- Performed comprehensive grey and black box testing, identified vulnerabilities, then recommended appropriate resolution methods.

- Pioneered installation of new cutting-edge cyber threat intelligence platform to efficiently and effectively stay pro-actively ready for cyber threats.
- Performed extensive vulnerability assessments using multiple tools such as Nmap, OpenVAS, Nessus, Burp suite & Zaproxy.
- Experienced at writing professional for executives reporting vulnerabilities and recommending mitigations and fixes for security vulnerabilities and weakness along with follow-ups with clients and teams.

Bank of Khartoum, Onsite/Khartoum, SD June 2022 to October 2022
IT Security Officer

- Engage in a variety of penetration testing assessments including network (internal and external), web application.
- Developed comprehensive company-wide IT security best practices, ensuring compliance with industry standards and regulations.
- Documented security breaches and assessing the damage using effective Incident Response playbooks we have put in place.
- Identified and fixed vulnerabilities to maintain a high-security standard, utilizing various tools and techniques.
- Familiarity with network protocols, firewalls, and security technologies.
- Strong analytical and problem-solving skills.

PROJECTS

Personal Cyber Security Blog, Online October 2023
Link: https://0xd3d5ec.github.io

- My personal blog that highlights projects I have worked on, CTF's and other cyber security content that I believe makes a difference.

OpenCTI, Offline January 2023
Main Engineer Implementor

- OpenCTI platform that enhances the cyber team capabilities to **track down APT's** tactics, techniques and procedures (TTPs) to build a **pro-active approach** to cyber defenses.

Wazuh SOC Platform, Offline January 2023
Main Engineer Implementor

- Configuration and enhancement of the SOC platform with **extra plugins** and **custom rule detections**.

Attack & Defend Lab, Offline September 2023
Personal Lab

- Build an attack and defend lab utilizing the popular open-source IDS tool **Security Onion** configuration for building a defense IDS and IPS tool for monitoring different MITRE&ATTACK techniques and how they traverse and how to detect them specially in north south traffic environments. As for the attack methods I have utilized the **Red Atomic Framework** for adversary simulation of most modern known MITRE&ATTACK tactics, techniques and procedures.

Snort, Offline August
2021
Personal Lab

- Snort Installation and configuration as intrusion detection system and intrusion prevention system with log forwarding to Splunk.

Suricata, Offline May 2021
Personal Lab

- Suricata acting as an intrusion detection system (IDS) Setup and configuration to forward logs to Wazuh SIEM.

OPNsense May 2023
Personal Lab

- Open-source configured firewall with IPS, IDS, CrowdSec and WAF configuration using reverse-proxy and NAXSI.

Recognitions

CyberTalents Security Scholarship (Digital Forensics & Incident Response Track)
NCSA Penetration Testing Accreditation for Consumers

CTFs

White Hat Desert, 3rd Place Red Teaming Competition March 2024
White Hat Desert, 3rd Place Blue Teaming Competition March 2024
13th Place, Digital Forensics CTF August 2021
77th Place, Reverse Engineering CTF August 2021

Volunteerism

Ministry of Interior Affairs October
2018
Data Entry

Languages

Arabic – Fluent, Native tongue language
English – Fluent, bilingual (IELTS 7.0 Holder)

Skills

Python, Bash, PowerShell, Vulnerability Assessment, Penetration Testing, Malware Analysis (Static and Behavioral), SOC monitoring and investigations, IPS, IDS, WAF, DLP, Wireshark PCAP, Tcpdump, Metasploit, Nessus, OpenVAS, Nmap NSE/Nmap, Firewalls.