Mohamed Saber AbdElgwad Ali

+201225084795 · MohamedSaber.THunter@gmail.com · www.linkedin.com/in/Mohamed Saber · https://github.com

7 Al-Islam Moharram Bek . Alexandria .Egypt

SUMMARY

A passionate Cyber Security Specialist with a strong focus on both offensive (red team operation) and defensive (SOC analyst) aspects of cybersecurity. Through dedicated self-learning, I have developed expertise in Security Operations, Threat Detection, Incident Response, and Security Information and Event Management (SIEM). I have honed my skills using tools like Qradar , Splunk , Volatility , SandBoxing and others while working on various self-directed projects and hands-on labs. My continuous learning journey has been further enriched by completing a comprehensive cybersecurity Scholarship from “Kayfa,” which deepened my knowledge of both red and blue teaming strategies. This self-driven approach reflects my commitment to mastering the field of cybersecurity.

EDUCATION

Bachelor of Science in Cybersecurity — **Sep 2022 – Present (Expected Graduation: Jun 2026)**
Alexandria University

- Focus: Cybersecurity, Network Security, Penetration Testing, Digital Forensics, Incident Response, Malware Analysis, Operating Systems, and Programming.
- GPA: Excellent (3.7/4.0).
- **Relevant Projects:**
  - **Proactive Malware Detection and Incident Response:**
    1. Simulated malware execution and detection using Sysmon, Splunk, and Suricata HIDS.
    2. Investigated malicious processes and network interactions using Threat Intelligence platforms (e.g., VirusTotal) and sandboxing tools.
    3. Conducted memory dump analysis with Volatility and Yara to identify and mitigate advanced persistent threats.
    4. Followed a structured incident response process to restore systems and strengthen network policies.

  - **System Simulation:Advanced Network Defense and Threat Mitigation:**
    1. Designed a realistic system simulation replicating a corporate network environment using Linux Virtual Machines, a pfSense Firewall, SIEM solutions, and Host-Based Intrusion Detection Systems (HIDS).
    2. Simulated various attack scenarios to assess system vulnerabilities and measure defense efficacy, leveraging tools such as Splunk and Suricata for threat detection and analysis.
    3. Implemented comprehensive defense mechanisms, including Role-Based Access Control (RBAC), password hashing, and proactive security measures, to mitigate risks and improve incident response capabilities.

SOC Professional Analyst — **Jun 2024 - Dec 2024**
Kayfa Platform
Completion of the SOC Professional Analyst pathway, which included:

- Network and Security Fundamentals
- Microsoft Windows Active Directory
- Linux Fundamentals
- Introduction to SOC Analysis and Management
- SOC Monitoring Using Splunk SIEM
- QRadar Professional Pathway
- Splunk SIEM Case Studies
- DFIR & Case Studies

Digital Forensics Training **Oct 2024 - Des 2024**
CyberTalents and Information Technology Institute (ITI)

- Comprehensive understanding of the Cyber Kill Chain, MITRE ATT&CK, and digital evidence collection techniques.
- Proficient in forensic imaging with tools like FTK Imager and analyzing Windows artifacts (e.g., registry, Prefetch files).
- Skilled in network traffic analysis with Wireshark and Snort, and memory forensics for live process investigation.
- Advanced log analysis expertise using Windows Event Logs, Sysmon, and Splunk for reports and dashboards.
- Hands-on experience with industry-standard tools and methodologies for digital forensics and incident investigation.

Networking Intern **March 2023 - June 2024**
Skill Dynamics

- Successfully earned the CCNA (Cisco Certified Network Associate) certification, validating expertise in networking.
- Gained knowledge in network fundamentals, including protocols, infrastructure, and services.
- Proficient in configuring and verifying switches, VLANs, inter-switch communications, and IP routing technologies.
- Implemented and verified IP services like DHCP, NAT, and ensured network security measures.
- Acquired foundational skills in network automation and programmability.

Penetration Testing Course **Jan 2023 - Aug 2023**
Teaching Planet – American Board Giza Governorate Agent

- Conducted penetration testing on networks, operating systems, and applications.
- Performed vulnerability analysis, scans, and system remediation.
- Gained proficiency in Linux/Unix systems and command-line interfaces.
- Learned Bash scripting, Python scripting, and exploiting vulnerabilities.
- Developed knowledge of security standards and compliance requirements.

CERTIFICATIONS

Kayfa

- Network and Security Fundamentals
- Windows Active Directory
- Linux Fundamentals
- Introduction to SOC Analysis and Management
- SOC Monitoring Using Splunk SIEM
- QRadar Professional Pathway
- Splunk SIEM Case Studies
- DFIR & Case Studies

Comptia

- Linux+ course (Self learning)
- Network+ course (Self learning)

SANS

- Summit 2023.
- SANS 450 Course (Self learn).
- SANS 508 Course (Self learn).
- SANS 555 Course (Self learn).
- SANS 503 Course (Self learn).
- Human Risk Management.
- DFIR Summit.

Books

- Up-to-Down Approach in Networking
- Practical Malware Analysis
- SANS 450: Blue Team Fundamentals Security Operations and Monitoring
- SANS 508: Advanced Incident Response, Threat Hunting, and Digital Forensics
- SANS 503: Intrusion Detection In-Depth

KEY COMPETENCIES

- QRadar
- Splunk
- ELK
- Volatility(2&3)
- Autopsy
- YARA
- Cisco Talos
- MISP
- Zeek
- Nessus
- Qualys
- Wireshark
- Metasploit
- Burp Suite
- Nmap
- Kali Linux
- Active Directory
- Windows Server
- Linux Administration
- Python
- PowerShell
- The-Hive
- Cortex
- Wazuh
- Snort
- Floss
- Ghidra
- Any-Run
- Virus-Total
- Arsenal