# Omar Sleem Khwat

## Contacts

- Cairo, Egypt – Phone: +20 111 664 8335
- Omar.khwat@gmail.com
- https://www.linkedin.com/in/omarsleem/

## Education

**Faculty of engineering: Systems & computer Engineering Department**

**Al-Azhar University**

## Professional Summary

A skilled security professional with expertise in both offensive and defensive security, backed by a strong foundation in Systems & Computer Engineering. With certifications like OSCP, CRTP, and hands-on experience in penetration testing, red teaming, and digital forensics, I specialize in Windows Active Directory exploitation, and advanced red-teaming techniques. Additionally, I bring valuable defensive skills in SOC operations, threat hunting, and incident response. Eager to leverage my red teaming experience and blue team knowledge to identify, assess, and mitigate cybersecurity threats effectively in a dynamic red teaming environment.

## Skills

### Offensive Skills:

- **Windows Active Directory Exploitation**: Conducting attacks on Windows Active Directory environments, identifying weaknesses, and exploiting vulnerabilities for privilege escalation**.**
- **Privilege Escalation Techniques (Windows and Linux):** Identifying and exploiting privilege escalation vulnerabilities on both Windows and Linux systems to elevate access rights**.**
- **Lateral Movement and Pivoting:** Techniques for moving laterally within a network, establishing footholds, and maintaining access across compromised systems.
- **Persistence Mechanisms:** Implementing persistence strategies to maintain access to compromised systems, including the use of startup programs, services, and other backdoor methods.
- **Post-Exploitation Techniques:** Advanced skills in controlling compromised systems, gathering valuable information, and maintaining access over time.
- **Penetration Testing Methodologies:** Applying comprehensive penetration testing techniques, from reconnaissance and scanning to exploitation and post-exploitation activities.

### Defensive Skills:

- **Security Monitoring and SIEM Operations with Splunk**: Configuring, managing, and utilizing Splunk for comprehensive Security Information and Event Management (SIEM), including monitoring, alerting, and analysis of security events to detect and respond to threats
- **Threat Hunting & Threat Intelligence :** Proactively searching for indicators of compromise (IOCs) and anomalous activities in network and endpoint logs, utilizing threat intelligence and analytics to enhance detection capabilities and improve proactive defense strategies
- **Incident Response:** Responding to security incidents with techniques for detecting, analyzing, and containing attacks.
- **Log Analysis and Management:** Analyzing logs from various sources (e.g., network devices such as, servers, applications) for security incidents.
- **Phishing Analysis and Email Investigation**: Identifying and investigating phishing attacks and other email-based threats , as i practiced on open source projects that demonstrated real life phishing campaign
- **Network Traffic Analysis:** Analyzing network traffic for signs of compromise, intrusion attempts, or anomalous activities **in** network devices such as ( IPS , IDS , WAF , Proxy , email security gateways )
- **Real-World Digital Forensics**: Practical skills in real-world forensic investigations, including acquiring and analyzing volatile memory, disk data, and network traffic on Windows systems to track malicious activities and uncover evidence of intrusions.

## Courses

## Essential Courses

- **Network+ (CompTIA):** Fundamental networking skills, including network configuration, management, and Services.
- **Security+ (CompTIA)**: Comprehensive understanding of essential cybersecurity principles
- **Linux for Hackers (Book):** Practical skills in using Linux for security and hacking purposes, with a focus on command-line tools and scripting.
- **PowerShell for Pentesters (Pentester Academy)** : covering exploitation, privilege escalation, post-exploitation, and integrating tools like Metasploit for advanced security tasks using PowerShell
- **MCSA:** Training on administering and configuring Microsoft technologies, such as Windows Server, Active Directory
- **HTTP The Definitive Guide (Book - Part 1)**: Comprehensive knowledge of the HTTP protocol, covering its architecture, methods, status codes, and security implications.

## offensive courses

- **Certified Red Team Professional (CRTP):** Windows Active Directory exploitation, privilege escalation, and lateral movement techniques
- **Offensive Security Certified Professional (OSCP):** In-depth experience with penetration testing methodologies, exploiting vulnerabilities, and advanced post-exploitation techniques
- **Persistence, Pivoting, and Lateral Movement (TCM Security)**: In-depth training on persistence strategies, pivoting through networks, and lateral movement techniques.
- **Privilege Escalation Techniques (Book)**: In-depth understanding of privilege escalation methods on Windows and Linux systems, including identifying misconfigurations and exploiting system weaknesses.
- **Windows Privilege Escalation (TCM Security):** Techniques to identify and exploit privilege escalation vulnerabilities on Windows
- **Linux Privilege Escalation (TCM Security):** Skills to elevate privileges on Linux systems using various techniques
- **eLearnSecurity Junior Penetration Tester (eJPTv2):** Foundations in penetration testing with hands on labs in penetration testing process

## Defensive courses

- **SOC Analyst Training with Splunk (60 hours, Udemy):** Comprehensive training on using Splunk for security monitoring, alerting, and analysis
- **Effective Threat Investigation for SOC Analysts (Book)**: Techniques for conducting threat investigations, identifying indicators of compromise (IOCs), and performing comprehensive threat analysis.
- **Digital Forensics and Incident Response - Tactical Edition (Black Hat USA 2022)**: Covers acquiring and analyzing digital evidence from volatile memory and on-disk artifacts, tracking attacker activity, and incident response strategies in real-world investigations
- **Practical Threat Intelligence and Data-Driven Threat Hunting (Book)**: Strategies for leveraging threat intelligence and analytics to proactively identify and mitigate threats.
- **Practical Windows Forensics (TCM Security):** Windows forensics techniques, including memory and disk analysis
- **SOC101 (TCM Security):** Email investigation & Phishing analysis, Network security monitoring and Network traffic analysis Log analysis and Management , threat hunting, and SIEM operations

# Hands On

- **GOAD Lab (Orange Cyberdefense):** Successfully installed and solved the Game of Active Directory Lab to gain hands-on expertise in advanced Active Directory exploitation, lateral movement, and post-exploitation strategies, simulating real-world adversarial scenarios.
- **TryHackMe and CyberDefenders**: Completed various hands-on labs and challenges covering topics like penetration testing, privilege escalation, Active Directory exploitation, and digital forensics.
- **Boss of the SOC (Splunk)**: Participated in SOC-themed Splunk exercises, including threat detection, incident response, and log analysis such as web defacement and ransomware investigation
- **VulnHub**: Worked on vulnerable machines to practice skills in penetration testing, system exploitation, and post-exploitation techniques.
- **Hack The Box:** Engaged with a vulnerable machines and scenarios to develop penetration testing and red team skills.
- **Let's Defend:** Practiced defensive techniques, incident detection, and SOC analyst skills in simulated environments.
- **Website Development and Security Testing**: Built a website for a client in Australia and conducted web security testing to ensure the site's security and resilience against potential threats.