Issac Abraham

Texas | +14695140926 | issacabraham15@gmail.com | www.linkedin.com/in/issacabraham15

PROFESSIONAL SUMMARY

PJPT-certified cybersecurity professional with hands-on experience in offensive security labs and a solid foundation in real-world attack simulation techniques. Proficient in system hardening, basic exploit development, and vulnerability assessments using Kali Linux. Academically grounded with a focus on **AI in cybersecurity**, bringing a modern perspective to threat detection and adversary emulation. Highly adaptable and analytical, with a strong passion for penetration testing and a clear trajectory toward red team specialization.

EDUCATION

UNIVERSITY OF WOLLONGONG **Dubai, U.A.E**

Bachelor of Computer Science, Cyber Security *Graduation Date: Feb 2025*

OUR OWN ENGLISH HIGH SCHOOL – BOYS' BRANCH **Sharjah, U.A.E**

High School Diploma in Science *Graduation Date: Jun 2021*

CERTIFICATIONS

- Practical Junior Penetration Tester (**PJPT**)

WORK EXPERIENCE

Distinct Infotech Solutions **Dubai, U.A.E**

Cybersecurity Analyst / Penetration Tester *Apr 2025 - Present*

- Simulated real-world cyberattacks to assess organizational security posture, identifying system, network, and application vulnerabilities, and proposing tailored remediation plans.
- Conducted internal and external penetration tests using Kali Linux, enhancing detection and response capabilities across critical infrastructure.
- Performed vulnerability assessments using tools like Nessus, OpenVAS, and Nmap, documenting findings and prioritizing risk-based remediation actions.
- Tested web applications with Burp Suite and executed MITM attacks with Responder, uncovering misconfigurations and insecure protocols.
- Collaborated with IT and compliance teams to implement best practices, resulting in stronger firewall configurations, patch management, and endpoint defenses.
- Developed and refined mitigation strategies post-assessment, reducing threat exposure and reinforcing system hardening procedures.
- Documented security findings and proposed remediation aligned with compliance standards.
- Utilized Wireshark and Metasploit for network traffic analysis and exploit validation, verifying patch effectiveness and configuration integrity.

Star Impex Industries LLC **Dubai, U.A.E**

IT Support *Jun 2023 - Nov 2023*

- Provided technical support to 30+ employees, resolving 90% of reported hardware, software, and network issues on the first attempt, minimizing downtime.
- Installed, configured, and maintained 30+ company devices, including operating systems, Microsoft Office 365, and enterprise applications, reducing software-related disruptions.
- Assisted in user account management, handling 50+ access requests and password resets, while enforcing security measures like firewalls, antivirus, and endpoint protection.
- Monitored system security and compliance, escalating high-risk issues, contributing to a decrease in security incidents and improved policy adherence.
- Managed and tracked 30+ IT assets (laptops, printers, and peripherals), optimizing resource allocation and improving equipment lifecycle efficiency by 20%.

PROJECT EXPERIENCE

HOME LAB

Active Directory Setup and Penetration Testing *Jan 2025 - Apr 2025*

- **Objective:** Set up a server environment to practice Active Directory management and network configuration while assessing common vulnerabilities and exploits and mitigations.
- **Tools and Technologies**:
  - Virtualization Platform: VMware Workstation 17 Pro
  - Server OS: Windows Server 2022
  - Client Systems: Windows 10 Enterprise
  - Attacking System: Kali Linux
  - Administrative Tools: Active Directory Users and Computers, Group Policy Management Console (GPMC)
  - Vulnerability Scanning and Exploitation Tools: Nmap, Nessus, Nikto, Metasploit.
- **Tasks Completed:**
  - Installed and configured Windows Server on a VMware virtual machine.
  - Set up and managed Active Directory, including creating and managing users, groups, and OUs.
  - Configured DNS and static IP addresses.
  - Implemented Group Policy Objects (GPOs) for various administrative tasks.
  - Set up file sharing and network resources.
  - Used a plethora of methods to scan and exploit vulnerabilities (LLMNR Poisoning, Responder Hash Capture, SMB Relay Attack, IPv6 Attacks, ldapdomaindump, Bloodhound, Pass Attacks, Kerberoasting, Token Impersonation, LNK File Attacks, Mimikatz)

HACKERSPREY **Dubai, U.A.E**

Web CTF

- Co-ordinated with a team of 5 members to analyse and exploit web vulnerabilities hosted by Hackersprey.
- Exploited vulnerabilities such as SQL Injection, Broken File Access, Broken Access control, HTML injection.
- Secured 3rd rank as a team in finding 50% of the flags and scoring 100 points in the CTF by finding vulnerabilities in a website.

SKILLS

Technical: Cyber Security, Active Directory, Vulnerability Scanning and Assesment, Penetration Testing, Python (Programming Language), Operating Systems (Kali Linux, Windows), Active Directory Exploitation

Soft: Communication, Problem-solving, Adaptability, Ethical Judgement, Attention to Detail