**Mohammad Gabr**

**Cyber Security Engineer**

***A Cybersecurity professional with a passion for Penetration Testing, a CTF Player and, a PowerShell Expert.***

**Email: Mohammad.magdy.gabr@hotmail.com**

**Phone: 0111-227-4215**

**LinkedIn: linkedin.com/in/Mohammad-gabr-775751bb**

**Education:**

**[2012 – 2017] Bachelor's Degree in Communication & Information Engineering Helwan University**

**Experience:**

**[01/2021 – Present] Cyber Security Engineer**

**WorldPosta / Roaya IT Solutions**

**Tasks:**

1. Evaluating all aspects of the organization’s security posture and targeting the areas of high risk.

2. Performing regular assessments of Web Application & Network security.

3. Providing timely response to any incidents.

4. Educating staff and increasing Cyber Security Awareness.

5. Hardening both Windows & Linux hosts.

6. Hardening & Security Administration of Active Directory.

7. Firewall Administration & Implementing best practices for Network Security.

8. Developing PowerShell Scripts for Security, Monitoring, Administration, Reporting & Automation.

**Achievements:**

***Developed a fully-automated PowerShell engine to run various scripts on a regular basis to:***

1. Detect Software & Service Installations, Security Event Log Clears, Scheduled task creation within the domain.

2. Detect High-Privilege Group Changes, Password Changes & Local Security Group Changes.

3. Detect Unauthorized Logins & PowerShell Usage on domain computers and carrying out automated response (user disable, password change, local & AD group membership removal, session termination).

4. Track AD user bad password count, locked out users within the domain.

5. Ensure LAPS & Antivirus Endpoints are installed on all domain computers.

6. Monitor all running processes, sessions, services, shares, local users, network connections & scheduled tasks.

7. Generate reports for Disk Usage, Network Bandwidth, VCenter virtual machines (using VMWare PowerCLI) and other important information for Administration teams.

**[08/2020 – 11/2020] OSCP Labs & Exam Attempt**

**Offensive Security**

1. Applied the main concepts of hacking: Recon, Exploitation, Privilege Escalation, Lateral Movement & Persistence.

2. Used a variety of attacks: SQLi, LFI/RFI/Directory traversal, XSS, OS Injection, Brute-Forcing, Active Directory (Password Spraying, Kerberoasting, Pass-the-hash, Credential Dumping, Hash Cracking etc.), Buffer Overflows & using/modifying public exploits from ExploitDB and other sources to achieve RCE.

3. Achieved a complete compromise of all the Public, Developer, IT & Admin networks in under 24 days.

4. Provided a full lab report detailing the exploitation process as well as remediations to the found vulnerabilities.

**[12/2018 – 12/2020] Senior IT Operations Engineer**

**Centro Global Solutions**

**Tasks:**

1. Supervision of the Support Team (over 1200 end-users).

2. Point of Escalation for tickets that breach SLA.

3. Active Directory administration.

4. PowerShell Script Development.

5. Mentoring junior engineers.

**Achievements:**

***Developed an interactive toolkit in PowerShell to help increase the efficiency of the Support & Systems Administration teams. It could:***

1. Query various pieces of computer information remotely

2. Execute commands

3. Deploy software

4. Query and Carry out basic AD Administration Tasks

**[8/2017 - 12/2018] Customer Support**

**Vodafone UK / Teleperformance Egypt**

**Skills:**

1. Web Application Penetration Testing

2. Network & Active Directory Penetration Testing

3. Firewall Administration

4. Scripting [PowerShell/Python/Bash]

5. Regular Expressions

**Highlights:**

1. Discovered a Bypass for Windows Applocker policy and reported it to Microsoft's Security Response Center. (linkedin.com/pulse/applocker-policy-bypass-using-runas-mohammadgabr/)

2. Achieved rank #77 worldwide on TryHackMe platform (05/2020).

**Languages:**

1. Arabic (Native)

1. English (Native)

2. French (Good)

**Interests:**

1. Web Application Security

2. Network & Active Directory Security

3. Red Teaming