George Abou Assaleh

Computer Science Engineering Student — Cybersecurity & Digital Forensics

GitHub — LinkedIn — Email

— Beirut, Lebanon

Summary

Motivated Computer Science student with hands-on experience in **cybersecurity**, **DFIR**, **malware analysis**, and **threat hunting**. Skilled in **Linux/Windows exploitation**, **web application security**, and **Capture-the-Flag (CTF)** competitions. Proficient in security tools, scripting, and log analysis, seeking to contribute analytical and technical skills in a cybersecurity or software internship.

Education

B.Eng. in Computer Science, American University of Beirut *2021 – Expected 2026*

- GPA: 3.7 / 4.0

Technical Training & Coursework

- Advanced penetration testing on **Linux/Windows systems**: privilege escalation, **Active Directory exploitation**, kernel-level attacks
- Web application assessments: **SQLi**, **XSS**, custom exploits, and automation scripts
- **CTF challenges** and DC machines: problem-solving under time pressure
- **Malware analysis** and reverse engineering; memory/disk forensics for attack reconstruction
- Full incident response lifecycle: threat identification, containment, eradication, recovery, and reporting
- Mobile device forensics (iOS/Android) and network traffic analysis using **Wireshark**, **Nmap**, **Metasploit**
- Specialized skills: exploit development, AD persistence, rootkit analysis, forensic artifact recovery, malware behavior, and AV evasion

Projects

For comprehensive walkthroughs and further information, please visit my portfolio website: georgeAA03.github.io

- **CTF Challenges — AUB**
  - Exploited Linux/Windows systems and **Active Directory environments**
  - Performed malware analysis, reverse engineering, and scripting for flags
- **DFIR Project (Ongoing) — AUB**
  - Forensic investigation of simulated cyber incidents
  - Memory/disk analysis and log correlation for reconstructing attack timelines
- **Final Year Project (Ongoing) — AUB**
  - Building a cybersecurity monitoring and threat detection system using **ELK Stack** (**Elasticsearch**, **Logstash**, **Kibana**)
  - Replicating and extending Regi & Kaur's work with **machine learning** for automated anomaly and attack detection
  - Enhances real-time log analysis, incident correlation, and visualization to improve DFIR efficiency

Awards

- **Donor-Funded Full Tuition Scholarship — AUB**: Competitively awarded; covered full tuition expenses
- **Jusoor AUB Full Scholarship**: Competitive full-tuition scholarship for Syrian students, awarded for top academic performance; in my case, covered additional academic expenses beyond tuition
- **Dean's Honor List** (continuous)

Skills

- Security: Linux/Windows Pentesting, **DFIR**, AD Exploitation, Threat Hunting
- Tools: **Nmap**, **Metasploit**, Burp Suite, **Wireshark**, Volatility, Autopsy, Splunk
- Programming: **Python**, Bash, PowerShell, C++, Java
- Platforms: VMware, Docker, Git
- Languages: English (Fluent), Arabic (Fluent), French (Intermediate)

Interests

CTFs, Exploit Research, Malware Analysis, Football & Basketball

References

Dr. Hussein Bakri
Senior Lecturer, Department of Electrical & Computer Engineering
Bechtel Engineering Building, Room 526, Ext: 3616
Relationship: Creator and lecturer of **Ethical Hacking 1, Ethical Hacking 2, and DFIR**
hb102@aub.edu.lb

Dr. Ali Chehab
Professor & Chairperson, Department of Electrical & Computer Engineering
Bechtel Engineering Building, Room 416, Ext: 3487
Relationship: Cybersecurity FYP Advisor
chehab@aub.edu.lb