





# Mohammadreza Sarayloo

📍 Tehran, Iran ☎ +98 930 281 1868 ✉ mo.sarayloo@gmail.com 🖥 <https://signorrayan.github.io>

---

Education	<b>B.Sc. in Computer Engineering - Information Technology</b> <i>Azad University, Central Tehran Branch (IAUCTB)</i>  <b>Tehran, Iran</b> <i>Sep 2016 - Jul 2021</i> <b>Thesis:</b> Implement a security architecture to detect threats in the network and web-based attacks using IDS and SIEM, <ul style="list-style-type: none"><li>150 credits program with GPA <b>3.11/4.00</b>. GPA of the last 69 credits is <b>3.78/4.00</b></li><li><b>Selected courses:</b> Artificial Intelligence and Expert Systems (20/20) - Database Design (20/20) - Information Technology Project Management (20/20) - Internet Engineering (19/20) - Computer Networks (18.5/20) - Systems analysis and design (17/20) - Compiler Design Fundamentals (17/20)</li></ul>
Research Interests	<ul style="list-style-type: none"><li>CyberSecurity</li><li>Big Data</li><li>Information Security</li><li>Machine Learning</li><li>Web Application Security</li><li>Privacy and Access Control</li></ul>
Personal Projects and Contributions	<b>Hashlookup Forensic Analyser</b>  <i>Oct 2021 - present</i> <p>Participating in this project to improve performance and implement automated python tests using bandit, flake8, mypy, isort, and black. This tool can help a digital forensics investigator to know the context and origin of specific files during investigation using hash lookup.</p> <b>RedTeam Web Application Toolkit</b>  <i>Aug 2021 - present</i> <p>The RedTeam Toolkit is an open-source django offensive web-application that provides offensive tools that the security specialist can use as part of a red-team to identify vulnerabilities. Currently it supports the following modules:</p> <ul style="list-style-type: none"><li>Scan ports and vulnerabilities/CVEs on the target</li><li>Livehosts (scan all live hosts in the network scale)</li><li>DirScan (scan all directories on a target)</li><li>CVE Description (CveID Search)</li><li>SSH Dictionary password guessing</li><li>RDP User and Password guessing</li><li>WebApps Section<ul style="list-style-type: none"><li>Apache Path Traversal PoC ( CVE-2021-41773 )</li><li>Web Crawler for gathering URLs</li><li>SubDomain Enumeration</li><li>HTTP Verb Tampering</li></ul></li><li>Windows Section<ul style="list-style-type: none"><li>Microsoft Exchange ProxyShell PoC (CVE-2021-34523, CVE-2021-34473, CVE-2021-31207 )</li></ul></li></ul> <b>Splunk SIEM queries for Fortiweb and Fortigate assets</b>  <i>Oct 2021</i> <p>a set of Splunk queries and visualizations for FortiWeb and Fortigate assets, which may aid SOC analysts and security experts in spotting anomalous behavior in splunk.</p>

**Experience**Teaching Experience**Teacher Assistant****Tehran, Iran***Azad University, Central Tehran Branch (IAUCTB)*

- **Linux Operational System Labs (6 labs)** *Oct 2021 - present*  
Under supervision of **Prof. Nayereh Zaghari**  
Responsibilities: Head Teaching Assistant, Teacher in Problem-Solving
- **Image Processing project of B.Sc. students** *Apr 2020 - Aug 2020*  
Under supervision of **Prof. Nayereh Zaghari**  
Responsibilities: Problem-Solving in python programming language
- **Engineering Economics Course** *Feb 2020 - Jul 2020*  
Under supervision of **Prof. Mohammad Mahdi Motevali**  
Responsibilities: Teacher in Problem-Solving, Documenting students progress

Professional Experience**SOC Tier-1 Security Analyst****Tehran, Iran***Faraz Pajouhan**Apr 2021 - present*

- Working as a contractor on various of projects including KianDigital Company (Fintech industry) and Iran Railways (Subdivision of Iran Ministry of Roads and Urban Development).
- Investigating and analyzing ransomware using digital forensics.
- Monitor and analyze logs and events daily, to determine whether any events could constitute a genuine security incident.
- Performing security monitoring, reviewing, investigating and reporting the events generated by the SIEM.
- Create queries, panels and design monitoring dashboards and visualizations to detect real-time attacks in the SIEM systems such as Splunk.
- Working with Red-Team tools to detect vulnerabilities in case of Linux systems, web-applications, services and protocols.
- Linux server administration in some cases such as monitoring SIEM collectors health and create some configs to work easier with kubernetes and containers.

**SIEM Plugin Developer****Tehran, Iran***Faraz Pajouhan**Dec 2020 - Apr 2021*

- SIEM Administration.
- Developing SIEM knowledge base (KB) and implementing security usecases.
- Collect and normalize security logs to make them easier to understand and extract important information.
- Developing log analysis patterns.
- Monitoring SIEM collectors health in some cases (on linux servers).
- Working with Splunk SIEM and create panels and dashboards to monitor events.
- Create some configs to work easier with kubernetes and containers (for SIEM) on linux servers.

- Monitoring SIEM collectors health in some cases (on linux servers).
- Normalize security logs and extract important information to make them easier to understand .
- Developing log analysis patterns.
- Learn a lot from SOC layer 2 and layer 3 security analysts which helped me grow.

- Skills**
- **Linux:** System Administration, Auditing, Selinux, SSH hardening, WebServer hardening, PAM
  - **Programming:** Skilled in Python3, SQL. Familiar with: BashScript, HTML, CSS
  - **Technologies:** Django, Splunk SIEM, PostgreSQL, Suricata, OPNSense, Docker, Git
  - **Other Skills:** Log Analysis, Network+, Regular expression, Digital Forensics

- Courses and Certificates**
- |  |                 |
|--|-----------------|
| <b>Linux Security (LPIC3-303)</b>  | <i>Sep 2021</i> |
| <i>Private Course under supervision of <b>Mohammad Hosein Askari</b></i> |                 |
| <b>Splunk Beginner</b>   | <i>Sep 2021</i> |
| <i>Udemy</i>   |                 |
| <b>Computer Network Security</b>   | <i>Sep 2021</i> |
| <i>Udemy</i>   |                 |
| <b>Linux Network Professional (LPIC-2)</b>                               | <i>Apr 2021</i> |
| <i>Fanavaran Anisa</i>   |                 |
| <b>Learn to code with python</b>   | <i>Jul 2020</i> |
| <i>Udemy</i>   |                 |
| <b>PostgreSQL Course</b>   | <i>Jul 2020</i> |
| <i>Udemy</i>   |                 |
| <b>Cybersecurity Course</b>  | <i>May 2020</i> |
| <i>Udemy</i>   |                 |
| <b>Linux Lpic-1</b>  | <i>Jan 2019</i> |
| <i>IEEE Iran Section</i>   |                 |
| <b>Network +</b>   | <i>Jan 2019</i> |
| <i>IEEE Iran Section</i>   |                 |

- Languages**
- Persian:** Native proficiency
- English:** Full professional proficiency *IELTS Score: Will be taken March 2022*

- References**
- Prof. Mohammad Mahdi Motevali**  
 Instructor at the Department of Computer Engineering of the IAUCTB  
[mmotevali@iauctb.ac.ir](mailto:mmotevali@iauctb.ac.ir)
- Mohammad Hosein Askari** (Linkedin)  
 Security instructor at Fanavaran Anisa  
 CyberSecurity Manager at Linux-Zone.org  
[security@linux-zone.org](mailto:security@linux-zone.org)
- Prof. Nayereh Zaghari**  
 Instructor at the Department of Computer Engineering of the IAUCTB  
 (Academic email address is currently unavailable)  
[nasrin.zaghari@gmail.com](mailto:nasrin.zaghari@gmail.com)