





Mohammadreza Sarayloo

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

Education	B.Sc. in Computer Engineering - Information Technology <i>Azad University, Central Tehran Branch (IAUCTB)</i>  Tehran, Iran <i>Sep 2016 - Jul 2021</i>
	<p>Thesis: Implement a security architecture to detect threats in the network and web-based attacks using IDS and SIEM,</p> <ul style="list-style-type: none">• 148 credits program with GPA 3.11/4.00. GPA of the last 69 credits is 3.78/4.00• Selected courses: 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)
Research Interests	<ul style="list-style-type: none">• CyberSecurity • Big Data • Information Security • Machine Learning• Web Application Security • Privacy and Access Control
Personal Projects and Contributions	<p>Hashlookup Forensic Analyser  <i>Oct 2021 - present</i></p> <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> <p>RedTeam Web Application Toolkit  <i>Aug 2021 - present</i></p> <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">• Scan ports and vulnerabilities/CVEs on the target• Livehosts (scan all live hosts in the network scale)• DirScan (scan all directories on a target)• CVE Description (CveID Search)• SSH Dictionary password guessing• RDP User and Password guessing• WebApps Section<ul style="list-style-type: none">◦ Apache Path Traversal PoC (CVE-2021-41773)◦ Web Crawler for gathering URLs◦ SubDomain Enumeration◦ HTTP Verb Tampering• Windows Section<ul style="list-style-type: none">◦ Microsoft Exchange ProxyShell PoC (CVE-2021-34523, CVE-2021-34473, CVE-2021-31207) <p>Splunk SIEM queries for Fortiweb and Fortigate assets  <i>Oct 2021</i></p> <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>

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