

Mohammadreza Sarayloo

📍 Tehran, Iran ☎ +98 930 2811868 ✉ mo.sarayloo@gmail.com 🌐 <https://signorrayan.github.io>


Education

Azad University, Central Tehran Branch (IAUCTB) 

Tehran, Iran

B.Sc. in Computer (Information Technology) Engineering

Sep 2016 - Jul 2021

Thesis: Implementing a security architecture for detecting threats on the network and web-based attacks using IDS and SIEM under supervision of **Dr. Mohsen Jahanshahi** 

- 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

- CyberSecurity • Big Data • Information Security • Machine Learning
- Web Application Security • Privacy and Access Control

Projects and Contributions

Hashlookup Forensic Analyser 

Oct 2021 - present

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.

RedTeam Web Application Toolkit 

Aug 2021 - present

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:

- 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
 - Apache Path Traversal PoC (CVE-2021-41773)
 - Web Crawler for gathering URLs
 - SubDomain Enumeration
 - HTTP Verb Tampering
- Windows Section
 - Microsoft Exchange ProxyShell PoC (CVE-2021-34523, CVE-2021-34473, CVE-2021-31207)

Splunk SIEM queries for Fortiweb and Fortigate assets 

Oct 2021

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.

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 **Dr. Nayereh Zaghari**
Responsibilities: Head Teaching Assistant, Teacher in Problem-Solving
- **OpenCV project of B.Sc. students** *Apr 2020 - Aug 2020*
Under supervision of **Dr. Nayereh Zaghari**
Responsibilities: Problem-Solving in python programming language
- **Engineering Economics Course** *Feb 2020 - Jul 2020*
Under supervision of **Dr. Mohammad Mahdi Motevali**
Responsibilities: Teacher in Problem-Solving, Documenting students progress

Professional Experience

SOC Tier-1 Security Analyst**Tehran, Iran**

FarazPajouhan

Apr 2021 - present

- Investigating and analyzing ransomware using digital forensics.
- Working with files encrypted by Eking and Phobos ransomwares.
- 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.
- Create python scripts to collect some information about attackers such as Full IP ranges and their foundation name.

SIEM Plugin Developer**Tehran, Iran**

FarazPajouhan

Dec 2020 - Apr 2021

- Collect and normalize security logs to make them easier to understand and extract important information.
- Monitoring Security Information And Event Management 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.

SIEM Plugin Developer intern**Tehran, Iran**

FarazPajouhan








Oct 2020 - Dec 2020

- Monitoring SIEM collectors health in some cases (on linux servers).
- Normalize security logs and extract important information to make them easier to understand .
- Learn a lot from SOC Tier-2 and Tier-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, Docker, Git
- **Other Skills:** Log Analysis, Suricata, OPNSense, Network+, Regular expression, Zabbix, Digital Forensics

Courses and Certificates

Linux Network Professional (LPIC-2) 	<i>Apr 2021</i>
<i>Fanavaran Anisa</i>	
Linux Server Administration 	<i>Jan 2021</i>
<i>Udemy</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 soon***References****Dr. Mohammad Mahdi Motevali** 

Instructor at the Department of Computer Engineering of the IAUCTB
mmotevali@iauctb.ac.ir

Dr. Nayereh Zaghari

Instructor at the Department of Computer Engineering of the IAUCTB
(Academic email address is currently unavailable)

Mohammad Hosein Askari 

CyberSecurity Manager at Linux-Zone.org
security@linux-zone.org