

Mohammadreza Sarayloo

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

Education

Azad University, Central Tehran Branch (IAUCTB) 

Tehran, Iran

BS 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

- Information Security • Big Data • CyberSecurity • 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 project is for analyse a forensic target (such as a directory) to find and report files found and not found from CIRCL hashlookup public service. This tool can help a digital forensic investigator to know the context, origin of specific files during a digital forensic investigation.

RedTeam Web Application Toolkit 

Aug 2021 - present

The Red Team 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 options:

- 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 (Being updated, other major CVEs PoC will be added)
 - Microsoft Exchange ProxyShell PoC (CVE-2021-34523, CVE-2021-34473, CVE-2021-31207)

Implementation some Linux commands in Python

Jul 2020

As a hobby, I implemented some Linux commands in Python to learn how they work.

CRUD app using Python and PostgreSQL

Jul 2020 - Sep 2020

My first project with Python and PostgreSQL involved authenticating users (Sign-up and Sign-in) to manage contact information.

Experience

Teacher Assistant

Tehran, Iran

Azad University, Central Tehran Branch (IAUCTB)

- TA of Linux Operational System Labs (6 labs) *Oct 2021 - present*
 Under supervision of **Dr. Nayereh Zaghari**
 Responsibilities: Head Teaching Assistant, Teacher in Problem-Solving
- TA of Engineering Economics course *Feb 2020 - Jul 2020*
 Under supervision of **Dr. Mohammad Mahdi Motevali**
 Responsibilities: Teacher in Problem-Solving, Documenting students progress

SOC Tier-1 Security Analyst

Tehran, Iran

FarazPajouhan

Apr 2021 - present

- 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

FarazPajouhan

Tehran, Iran

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

FarazPajouhan

Tehran, Iran

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

Courses and certificates

Linux Network Professional (LPIC-2) 


Fanavar Anisa

Apr 2021

Linux Server Administration 

Udemy

Jan 2021

Learn to code with python 

Udemy

Jul 2020

PostgreSQL Course 

Udemy

Jul 2020

Cybersecurity Course 

Udemy

May 2020

Linux Lpic-1

IEEE Iran Section

Jan 2019

Network +

IEEE Iran Section

Jan 2019

Languages**Persian:** Native proficiency**English:** Full professional proficiency*IELTS Score: Will be taken soon***References****Dr. Mohammad Mahdi Motevali** 

Instructor Department of Computer Engineering of IAUCTB

mmotevali@iauctb.ac.ir**Mohammad Hosein Askari** 

CyberSecurity Manager at Linux-Zone.org

security@linux-zone.org