Mohammadreza Sarayloo

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

Education

B.Sc. in Computer (Information Technology) Engineering **Tehran, Iran**

Azad University, Central Tehran Branch (IAUCTB) ↗ *Sep 2016 - Jul 2021*

Thesis: Implement a security architecture to detect threats in the network and web-based attacks using IDS and SIEM, under supervision of **Prof. 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.

Implementation some linux commands in python ↗ *Jul 2020*

CRUD app using python and postgresql based on authentication↗ *Jul 2020 - Sep 2020*

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

- **OpenCV 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*

- 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**
Faraz Pajouhan *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**
Faraz Pajouhan *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, Suricata, OPNSense, Docker, Git
- **Other Skills:** Log Analysis, Network+, Regular expression, Digital Forensics

Courses and Certificates

Linux Network Professional (LPIC-2) ↗ *Apr 2021*
Fanavaran Anisa

Linux Server Administration ↗ *Jan 2021*
Udemy

Learn to code with python ↗ *Jul 2020*
Udemy

PostgreSQL Course ↗ *Jul 2020*
Udemy

Cybersecurity Course ↗ *May 2020*
Udemy

Linux Lpic-1 ↗ *Jan 2019*
IEEE Iran Section

Network + ↗ *Jan 2019*
IEEE Iran Section

Languages

Persian: Native proficiency

English: Full professional proficiency *IELTS Score: Will be taken soon*

References

Prof. Mohammad Mahdi Motevali ↗
Instructor at the Department of Computer Engineering of the IAUCTB
mmotevali@iauctb.ac.ir

Prof. Nayereh Zaghari ↗
Instructor at the Department of Computer Engineering of the IAUCTB
(Academic email address is currently unavailable)
nasrin.zaghari@gmail.com

Mohammad Hosein Askari ↗
CyberSecurity Manager at Linux-Zone.org
security@linux-zone.org