Mohammadreza Sarayloo

Tehran, Iran mo.sarayloo@gmail.com https://signorrayan.github.io

Experience

Professional Experience

Security Operation Center Analyst — **Tehran, Iran**
Ayandeh Bank — *Jan 2022 - Present*

- Monitor and analyze logs and events daily to determine whether any circumstances could constitute a genuine security incident.
- Python scripting to monitor assets and integration with Telegram bot.
- Performing security monitoring, reviewing, investigating, and reporting the events generated by the SIEM.
- Web application and network Threat Hunting and Penetration Testing.
- Sysmon and Windows threat hunting.
- Working with FortiGate, FortiWeb, Zeek, Suricata, Sysmon, Windows logs.

SOC Tier-1 Analyst — **Tehran, Iran**
Faraz Pajouhan — *Mar 2021 - Jan 2022*

- 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).
- Performing security monitoring, reviewing, investigating and reporting the events generated by the SIEM.
- Vulnerability detection in case of Linux systems, web-applications, services and protocols.

SIEM Plugin Developer — **Tehran, Iran**
Faraz Pajouhan — *Oct 2020 - Mar 2021*

- Two months (Oct - Dec) Internship.
- SIEM Administration, developing SIEM knowledge base (KB) and implementing security usecases.
- Collect logs and developing log analysis patterns to make them easier to understand and extract important information.
- Monitoring SIEM collectors health in some cases (on linux servers).

Teaching Experience

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

- **Linux Operational System Labs (6 labs)** — *Oct 2021 - Jan 2022*
  Responsibilities: Head Teaching Assistant, evaluate students project, teacher in problem-solving, create quizzes.
- **Image Processing project of B.Sc. students** — *Apr 2020 - Aug 2020*
  Responsibilities: Problem-Solving in python programming language

Personal Projects & Contribution

Splunk Threat Hunting ↗
Apr 2022 - present

This repository contains some of my Splunk queries for threat hunting in multiple assets, such as Fortigate, Zeek, Suricata, Sysmon, and Windows Event logs.

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 written in Python that provides offensive tools which 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
- Live hosts (scan all live hosts in the network scale)
- Dir Scan (scan all directories on a target)
- CVE Description (CveID Search)
- SSH password guessing
- RDP user and password guessing
- WebApps Section
  - Apache Path Traversal Scanner (CVE-2021-41773, CVE-2021-42013)
  - Web Crawler for gathering URLs
  - SubDomain Enumeration
  - HTTP Verb Tampering
- Windows Section
  - Microsoft Exchange ProxyShell Scanner (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

Skills

- **Programming:** Python3, SQL
- **Linux:** System Administration, Auditing, Selinux, SSH hardening, WebServer hardening
- **Technologies:** Django, Splunk SIEM, PostgreSQL, Suricata
- **Other Skills:** Log Analysis, Network+, Regular expression
- **Familiar with:** Docker, Git, GitHub Actions, ThreatHunting, Bashscript, HTML, CSS

Education

B.Sc. in Computer Engineering - Information Technology **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,

- 150 credits program with GPA **3.11/4.00**. GPA of the last 69 credits is **3.78/4.00**

Courses and Certificates

Linux Security (LPIC3-303)	*Sep 2021*
Splunk Begineer↗	*Sep 2021*
Computer Network Security↗	*Sep 2021*
Linux Network Professional (LPIC-2) ↗	*Apr 2021*
PostgreSQL Course↗	*Jul 2020*
Cybersecurity Course↗	*May 2020*
Linux Lpic-1↗	*Jan 2019*

Languages

Persian: Native proficiency

English: Full professional proficiency *IELTS Academic:* ***6 (B2)***