Mohsen Esfandyari Doulabi

Tehran, Iran
+98 (912) 963 6229
Mohsen.e.doulabi@gmail.com
https://Mohsen-esfandyari.github.io

Research Interests

- Software Security
- System Security
- Programming
- Malware Analysis
- Deep Learning

Education

B.Sc. in Computer Engineering, Azad University *2017 - 2022*

- **Overall GPA:** 3.3
- **GPA of Last 4 Semesters:** 3.94
- **Final Project:** Implementing an application security platform to improve the programmers secure-coding ability. *Supervised By: Dr.Gholami*
- **Project Summary:** As we move forward into the 21st century, the security of the internet has become an integral part of everyday life, affecting aspects of our lives in a practical manner. Numerous security bugs are published daily on the internet, and the reason behind these security concerns is developers' low-security knowledge. This security platform provides valuable information to developers by using practical examples of web security bugs and then clarifies how to mitigate these bugs. So, in order to design and implement secure systems, they must understand the details of attacks. For instance, they will fully understand the usual bugs, root causes, and what they affect, and with the knowledge they have concerning security, they can then figure out how to prevent these bugs from happening in the future.

Honors and Awards

- Top 7% of the Nationwide universities entrance exam in the field of Mathematics and Physics. *2017*
- Outstanding Computer Engineering Student in last two semesters based on each semester`s GPA, Azad University *2022*
- Within Top 25 Computer Engineering students according to academic works and overall GPA, Azad University *2022*
- 1st Place - Tehran Province - U16 Professional soccer league *2013*
- 3rd Place - Tehran Province - High schools` volleyball league *2016*

Grades in selected academic courses

- Artificial Intelligence: 20/20 (ranked 1st)
- Object Oriented Designing: 20/20 (ranked 1st)
- Designing programming languages: 20/20 (ranked 1st)
- Designing of digital systems: 20/20 (ranked 1st)
- Human-Computer Interaction: 19.5/20 (ranked 2nd)
- Operating System: 18.2/20 (ranked 3rd)
- Designing Algorithms: 17/20 (ranked 3rd)
- Internet Engineering: 17/20 (ranked 5th)

Research Experience

Detecting network attack using machine learning

October 2017- December 2018
Azad University

The main goal of this project was to conduct extensive research on the security and performance of website hosting solutions in Linux environments. This goal was designed and implemented a novel approach using deep learning techniques to detect and analyze the network communications between C&C servers and their victims by inspecting sent/received packets in a sandbox environment. Also, this system was developed with C++ and Python to create a large-scale platform for analyzing PCAP files and then to detect network attack patterns.

Teaching Assistance

Discrete Mathematics	*Dr. Tabibi* *Fall 2017*
Artificial Intelligence	*Dr. Dami* *Fall 2019*
Operating System	*Dr. Alavi Abhari* *Fall 2019*
Internet Engineering	*Dr. Mahdi* *Fall 2020*
Human-computer Interaction	*Dr. Dami* *Spring 2021*
Object Oriented Design of systems	*Dr. Delara* *Spring 2021*
Designing Programing Languages	*Dr. Delara* *Fall 2021*

Internships

Research on recent methods for detecting next-generation of application and network attacks

Supervisor: Dr. Gholami
summer 2021

Company: City Development and Innovation Corporation

Description: This project's focus was on creating autonomous censors in a computer networks, which improves the detection of next-generation cyber-attacks based on MITRE ATTACK framework information and traffic analysis.

Publications

M. Mosleh, M. Esfandyari, A. Mohammadi Izad, H.Fathi. An automated approach for Android malware detection by static analysis, under review.

Description: Due to the widespread use of the Android operating system, Android malware and malicious codes have increased noticeably. These malware types can be installed and run without the user's knowledge and afford numerous opportunities for attackers. Unfortunately, due to the presence of general countermeasures to detect malware, they can be easily evaded by simple code transformations. Therefore, this research project has been designed to develop a learning-based detection framework that is efficient, effective, and reliable to generate accurate results. Our static analysis is divided into several parts, including opcode-based methods, a method that analyses executables to extract function calls, and an analysis of permission requirements.

Presentations

Counting people with image processing

September 2019
Azad University

Description: This project, was developed to count people in a picture utilizing an Object Detection algorithm (HOG + Linear SVM) to better detect people based on a pre-trained model. Since each student in the class had to develop a project to pass the course successfully, this was my final project for the Artificial Intelligence course that I presented by requesting the professor.

Steganography

September 2020
Azad University

Description: This presentation consisted of several parts. First, the definitions and history of steganography, and then, all types of steganography were presented to the students. After giving the basic information, a simple tool was developed based on the LSB model by utilizing Python language. Therefore, using this tool, a simple message was hidden and unhidden in a PNG file, as everyone predicted.

Installing and managing network services

September 2020
Azad University

Description: This presentation consisted of two main parts: DNS and VPN services. First, information about two services was given to the attendants, and then, the explained services were installed and managed on both Linux and Microsoft servers. Finally, to check the correct work of each service, students connected to VPN servers and some laptops asked for some domain IPs from the DNS server.

Simulating real hacking scenarios

January 2021
Azad University

Description: Since this presentation was part of a security seminar at Azad University, it was undoubtedly like a real hacking scenario for guests. First, the project started with scanning a network IP range, and then with scanning all ports of each up host, trying to find hosts` vulnerabilities began. Therefore, by using a couple of exploit frameworks and well-known tools, exploiting and gaining access from the victim host were done. Then, to show what types of disasters could happen by suspicious access to a server, all kinds of administrators` commands were requested to the exploited host.

Academic Experience

Webinars

1- Looking in-depth at cybersecurity related occupations

August 2022
Azad University

- Introducing Cybersecurity.
- Definition behind red and blue teams.
- Main parts of each team.
- Specific requirements to find a job in Cybersecurity.

2- How to improve a website safety

September 2022
Azad University

- Introducing Penetration Testing.
- Introducing all types of penetration testing.
- Introducing Web and Mobile Penetration testing.
- Explaining ways to find a vulnerability in a website.

- Explaining SQL Injection and IDOR attacks
- Explaining how to exploit SQL Injection and IDOR attacks

3-Making private application and tools by utilizing Python

September 2022
Azad University

- Introducing Python language.
- Explain how to write a simple python code.
- Explain how to find SQL Injection and IDOR vulnerabilities on a host.
- Explain how to exploit SQL Injection and IDOR attacks
- Introducing what is Malware.
- Developing simple Linux and windows malwares to create backdoor and execute commands.
- Explain how to exploit SQL Injection and IDOR attacks on a network range.

Books

1-How to perform a complete website penetration testing based on OWASP WSTG

- **Publication:** Naghoos Press
- **state:** In progress
- **Language:** Persian

Work Experience

Security Engineer

2021 - Present

SHAHR BANK, IRAN

- Performing Application (web & mobile) and Network Penetration test.
- Hardening Servers and Services.
- Checking for Latest CVEs and patch the vulnerabilities.
- Developing security systems to analyze servers’ availability.
- Performing vulnerability assessment.
- Managing network Antivirus and EDR.
- Teaching security concepts to the developers.

SOC Tier2

2020 - 2021

APK-GROUP, IRAN

- Detecting live Attacks on the servers and network.
- Analyzing malwares behaviors in sandboxes.
- Performing vulnerability assessment.
- Performing Network Penetration test.
- Monitoring network`s Input/output traffic.
- Developing security systems to analyze servers’ availability.
- Analyzing the various devices Logs.
- Hardening Servers and Services.

Network Engineer *2019 - 2020*
SHATEL, IRAN

- Manage Linux and Microsoft servers.
- Monitoring Servers` states.
- Managing DNS, DHCP, and VPN services.
- Solving the network clients' issues.

Professional Skills

Security	BurpSuite, Nmap, IDA Pro, Ghidra, Metasploit, Nuclei, Nessus, Tcpdump, FFUF, Acunetix
Programming Language	C, C++, Python, Go, Assembly, Bash Script, MATLAB
Operating-System	Microsoft windows (Servers, Clients), Linux (Redhat and Debian bases), OS X
Web Application	Html, CSS, JavaScript, PHP
Virtualization & Clouds	VM-ware, Virtual Box, Docker, AWS
API	SOAP, Rest, GraphQL, Postman
Database	Database: MySQL, MSSQL
General	Microsoft Office Word, Excel, PowerPoint

Languages

IELTS:

- **Date**: November 2022
- **Overall**: 7.5
- **Listening:** 8.5, **Speaking:** 7.0, **Reading:** 7.0, **Writing:** 6.5

GRE:

- **Date:** Will be taken on October 30th

Hobbies

Sports:	Soccer, Basket Ball, Swimming, Volleyball
Others:	Video Games, Programming, Bug Bounty, Movies, Books, Musics

References

Dr. Sina Dami
Assistant Professor, Department Chair of Computer Science
WTIAU, Tehran, Iran
Email: dami@wtiau.ac.ir
Phone: +98 (912) 021 8552

Dr. Maryam Gholami
Deputy dean of the faculty, Instructor
WTIAU, Tehran, Iran
Email: gholami@wtiau.ac.ir
Phone: +98 (912) 536 1974

Dr. Changiz Delara
Assistant Professor, Computer Science
WTIAU, Tehran, Iran
Email: Delara.c@wtiau.ac.ir
Phone: +98 (912) 739 0904

Dr. Masoud Alavi Abhari
Visiting Instructor
WTIAU, Tehran, Iran
Email: Msa.6553@gmail.ir
Phone: +98 (912) 524 9256