Mohammad Reza Sabeti Zadeh
Born in 20/02/1991
Single - Military Service Completion Certificate
Narmak – Tehran
021 – 77 82 79 51
0920 – 317 9321
mohammadrezasabetizadeh@gmail.com
https://www.linkedin.com/in/mohammad-reza-sabeti-zadeh-70a2531a4

Education

Bachelor's Degree of Network Engineering
(University of Applied Science and Technology (2015 -2017)

Completed one dissertation in final year:
Launch Data Center

Certificates

- International

ICSI | CNSS Certified Network Security Specialist
Credential Number: 18046475
ISCI | Cyber Security Essentials
Credential Number: 12ss31twtt

NSE 1 – Certification Number: tUvU5Fy0qr
NSE 2 – Certification Number: H615BMC9GB
Fortinet Security 6.2

Awards

Splunk User Behavior Analytics
Splunk 7.x Fundamentals Part 1
Splunk Infrastructure Overview
10 Introduction to SignalFx Microservices APM (Previous Gen)
01 The SignalFx Solution

Cyber Threat Hunting W/S

CompTIA Security+ Certificate Number: C-e576117e2c-f861b0

- Internal

EC-Council CEH v10
EC-Council CEH v11
EC-Council CHFI v9
EC-Council ECSA v10

Offensive Security OSCP (PWK)
Offensive Security OSWP (WIFU)

ISO/ISC 27001 Fundamental (ISMS) TUV Academy

McAfee Device Control Workshop
Install and Implementing MEP Workshop

SANS Sec 580 Metasploit Kung Fu
SANS Sec 573 Automating Information Security with Python
SANS Sec 504 Hacker Tools, Techniques, Exploits, and Incident Handling
SANS Sec 542 Web App Penetration Testing and Ethical Hacking
SANS For 500 Windows Forensic Analysis
SANS For 572 Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response
SANS For 508 Advanced Incident Response, Threat Hunting and Digital Forensics
SANS Sec 555 SIEM with Tactical Analytics
SANS Sec 503 Intrusion Detection In-Depth

Cisco Certified Network Associate v2 Workshop
Cisco Certified Network Professional (Switch)
Cisco Certified Network Professional (Route)
Cisco Certified Network Associate

Microsoft Certified Solutions Expert 2012 R2

Linux Professional Institute – LPIC1

CompTIA Network Plus

Skills

Language

Persian (native)
English read and write so good

Offensive, Defensive, Network and Computer

Threat Hunting via ELK , Splunk
Cyber Threat Intelligence
Threat Management
Log Analyzing via ELK, Suricata, Bro
Normalization via REGEX and GROKE
Managing Log Broker (Rabbit-MQ)
Incident Response and Handling
Analyzing and Responsibility via RTIR
Analysis Attack and implementation
MITRE ATT&CK and Kill Chain
LAB for Implementing Attack and USE CASE
Sand box and Malware Analysis
SIEM Infrastructure
SOC Infrastructure
Best Practice for reporting
Design and create dashboards for all assets in SOC
Data Analysis
Log Analysis and management (Normalization)
Microsoft Logs and Event ID – SYSMON
Traffic and flow Analysis
OWASP Solutions
Penetration test with KALI and Parrot OS
Exploit Network and Web
Scanning Network and Web for Reconnaissance and Vulnerability
Nmap and Metasploit Framework
Network consulting and design and implementation
Install and Configuring APACHE Web server
Install and Configuring Microsoft windows server (2003 & 2008 & 2012)
Install and Configuring any LINUX family
Configuring ADDS,DNS,DHCP and Etc.
Install and Configuring any Hypervisor (ESXi , Hyper-V and Etc.)
Configuring Router and Switch (CISCO)
Design and Implementation of Local Wireless Networks

Work

Teaching SANS and Cyber Security Courses in Douran Academy

- SANS SEC503 Communications Regulatory Authority (CRA) of The I.R. of Iran

Teaching SANS and Cyber Security Courses in Cando

- SANS SEC504
- SANS SEC401 (Mellat Bank, Danayan Broker)
- SANS SEC301 (Mellat Bank, Danayan Broker)
- CEH v11
- PWK
- Security+ (Mellat Broker, Registration of Real Estate)
- And More Public Classes

Teaching SANS Security Courses in Vista

- SANS SEC555 (Communications Regulatory Authority (CRA) of The I.R. of Iran)
- SANS SEC450 (Communications Regulatory Authority (CRA) of The I.R. of Iran)
- SANS SEC503
    - (Mobin Petrochemical Co., Ministry of Economic Affairs and Finance)
- SANS SEC511
    - (Mobin Petrochemical Co., Ministry of Economic Affairs and Finance)
- SANS SEC504
    - (Mobin Petrochemical Co., Ministry of Economic Affairs and Finance)

Cyber Security Consultant

- Some Government Agencies

Cyber Security Analyst at Soorin (December 2021 – Present)
Amin Avid Broker SIEM Design, Install and Implementing (Splunk) (April 2022)
Petrochemical Organization(s) Arya Sasol Install and Implementing SIEM (April 2022)
Petrochemical Organization(s) Arya Sasol Customize SYSMON Configuration (April 2022)
Petrochemical Organization(s) Arya Sasol Threat Hunting (January 2022)
IRISA Purple Teaming (December 2021)

- Use Cases And IOC

Malware Threat Hunting Kowsar Insurance (August 2021)
VOIP Forensic at IKCO (August 2021)
MSSP Manager at APK-Group Amn Pardazan Kavir (July 2021 - December 2021)
MSSP Manager at Day Insurance (July 2021 - December 2021)
MSSP Manager at Kowsar Insurance (July 2021 - December 2021)

MSSP Manager at Qarz Al-Hasaneh Mehr Iran Bank (July 2021 - December 2021)
MSSP Manager at Chadormalu Industrial Co (July 2021 – December 2021)
Training new employees in APK-Group Amn Pardazan Kavir
SOC Analyst at APK-Group Amn Pardazan Kavir (January 2020 – July 2021)
SOC Analyst at IAC Iran Airport Company (January 2020 – July 2021)
Hardware and Network Expert At IRIB Cyber Space (September 2018- January 2020)
IT manager at Moj Pardaz (October 2017 – December 2018)
IT manager at Hunter Part (January 2018 – March 2018)
University of Applied Science and Technology 2016 TA :

- Managing the delivery of a message
- Mobile and Wireless Networking Workshop
- Virtual Machine
- Installation of inter-organizational networks

Hardware technician and Help desk at Aerospace Company (2013-2015)
ELECOMP with CyberTech (2011)
Hardware technician and Help desk at Pardazeshgaran Pishgam (2006)
Hardware technician at Hadi System (2005)