حسن خالقی راد

متخصص امنیت شبکه، برنامه نویسی

۰۹۳۵۴۰۸۱۸۹۱

تهران، پیروزی

h.khaleghirad@ut.ac.ir

https://www.linkedin.com/in/hassan-khaleghi-rad-

توانایی ها

- امنیت شبکه و فارنزیک
- SOC
- DevOps
- Embedded System
- مهندسی معکوس
- تست نفوذ
- امنیت و رمزنگاری
- لینوکس
- برنامه نوسی

زبان ها

- ✓ انگلیسی: عالی
- ✓ آلمانی: متوسط

علایق

- ✓ مطالعه و پژوهش
- ✓ رانندگی/ طبیعت گردی

درباره من:

من حسن خالقی راد دانشجوی دکتری مهندسی کامپیوتر دانشگاه تهران دارای ۱۳ سال سابقه کار در زمینه برنامه نویسی روی پلتفرم های مختلف سازمانی و تلکام، امنیت شبکه و صنعتی، فایروال، SOC، برنامه نویسی ابزار SIEM، تلکام، تولید اپلیکیشن های همراه اول، برنامه نویس USSD Gateway برنامه نویسی سیستم Embedded، لینوکس و امنیت لینوکس، رمزنگاری، راه اندازی آزمایشگاه امنیتی سیستم های کنترل صنعتی و تدریس مفاهیم امنیت و شبکه هستم.

ویژگی های من:

- سختکوش و با پشتکار
- علاقه به یادگیری
- انعطاف پذیری بالا
- کار گروهی
- مدیر
- قدرت حل مسئله
- مسئولیت پذیر
- با تجربه بالا
- آگاه و بروز

تحصیلات

دکتری – گرایش مهندسی کامپیوتر

دانشگاه تهران

از ۱۳۹۹ تاکنون

کارشناسی ارشد – گرایش مهندسی کامپیوتر

دانشگاه شهید بهشتی

از ۱۳۹۰ تا ۱۳۹۲

کارشناسی – گرایش مهندسی کامپیوتر

دانشگاه صنعتی سجاد

از ۱۳۸۵ تا ۱۳۸۹

تجربیات حرفه ای:

از فروردین ۱۴۰۳ تاکنون:

شرکت پرداخت الکترونیک سداد

تخصصی: SOC

وظایف: کارشناس مسئول مدیریت آسیب پذیری

توسعه ابزار تشخیص تقلب و پولشویی با یادگیری ماشین

- SOC Splunk
- Vulnerability Assessment
- Tenable SC- Nessus and Endpoincentral
- AI MLTK Machine learning in Splunk
- Develop Splunk Plugins
- **نوشتن اسکریپت‌های Python و Bashبرای خودکارسازی اسکن‌های دوره‌ای آسیب‌پذیری در سیستم‌ها و شبکه‌ها**
- **طراحی و توسعه اسکریپت‌های خودکار برای تحلیل آسیب‌پذیری‌ها و فیلتر کردن false positive ها با استفاده از تکنیک‌های خودکارسازی درPython**
- **استفاده از APIهای ابزارهای اسکن مانند Nessus API یا EndpointCentral API برای یکپارچه‌سازی فرآیندهای اسکن با سایر سیستم‌ها و پایگاه‌های داده داخلی**
- **طراحی و پیاده‌سازی خودکارسازی فرآیندهای Patch Managementبرای شناسایی و اعمال وصله‌ها با استفاده از اسکریپت‌های خودکار**
- **یکپارچه‌سازی ابزارهای اسکن آسیب‌پذیری با سیستم‌های مدیریت نظارت (SIEM) برای گزارش‌دهی لحظه‌ای و خودکار تحلیل آسیب‌پذیری‌ها**
- **مدیریت چرخه کامل آسیب‌پذیری‌ها، ارزیابی مداوم امنیت و اجرای اسکن‌های دوره‌ای برای شناسایی آسیب‌پذیری‌های جدید تهیه گزارش و داشبوردهای امنیتی و گزارش‌دهی به مدیریت درباره وضعیت امنیتی سازمان.**

- تحلیل تهدید و ریسک، ترکیب اطلاعات آسیب‌پذیری با تهدیدهای روز دنیا.(threat intelligence) و ارزیابی ریسک سازمان بر اساس آسیب‌پذیری‌های موجود.
- همکاری در تست نفوذ و ارزیابی امنیتی و پشتیبانی یا اجرای تست‌های نفوذ داخلی و خارجی همچنین تحلیل نتایج تست و هماهنگی برای رفع مشکلات.
- مستندسازی فرآیندها و رویه‌ها، ایجاد و نگهداری ازRunbook ها، SOPها و استانداردهای داخلی امنیت.
- آگاهی از چارچوب‌ها و استانداردها و تسلط به استانداردهایی مثل ISO 27001, NIST, OWASP Top 10برای تحلیل آسیب‌پذیری.

از سال ۱۴۰۲ تاکنون:

شرکت آرین

تخصصی: برنامه نویسی، امنیت، DevOps

وظایف: مدیر IT

پروژه های اجرا شده:

- API Gateway WSO2
- USSD برنامه خرید شارژ، پرداخت قبض و بسته اینترنت
- ETL Server application
- *800# Ads SMS Blocking
- BSS/OCS
- SMS Firewall
- BI: Crytal Report from MySQL Database from OCS/BSS Server

از سال ۱۳۹۸ تا ۱۴۰۲:

شرکت پرتو آبی

تخصصی:

متخصص امنیت و برنامه نویسی در زمینه تلکام و شبکه، برنامه نویسی سیگنالینگ مخابرات M3UA، مهندسی معکوس، برنامه نویسی، امنیت شبکه، رمزنگاری اپلیکیشن های ارتباط با همراه اول از قبیل خرید شارژ *۱۲۱#، امنیت سخت افزار و نرم افزار، برنامه CRM

نوشتن برنامه سیگنالینگ شبکه M3UA, SCTP, SIGTRAN

وظایف:

توسعه دهنده نرم افزارهای تلکام و تامین امنیت شبکه ارتباطی با همراه اول

پروژه های اجرا شده:

- امنیت سخت افزار و لینوکس پنهان
- برنامه نویسی پلتفرم های جاوایی برنامه ها و اپلیکشن های خرید شارژ همراه اول
- توسعه اپلیکشن های NGP, USSD GATEWAY, PWA, EMS, OSS,
- نوشتن برنامه USSD Gatewayنوشتن برنامه پروتکل مخابراتی SS7 Stack
- تولید ابزار با متد میکرو سرویس در پلتفرم Spring Boot Java
- رمزنگاری تمام اپلیکیشن های نوشته شده برای ارتباط با همراه اول
- رفع تمام نواقص امنیتی در سطح بسیار بالا، بالا، و متوسط از تمامی نرم افزارهای خرید شارژ همراه اول مانند نقض امنیتی خرید شارژ توسط چند نفر با یک TOKEN
- مهندسی معکوس و استخراج اطلاعات از بردهای مخابراتی شرکت های تولید کننده اصلی
- برنامه نویسی Linux Embedded System و FPGA VHDL & Verilog

- برنامه نویسی Front-End Angular برای تمامی اپلیکیشن ها Configuration, Log Analyzer در سمت همراه اول

۱۳۹۶ تا ۱۳۹۸

شرکت: پرنیان

تخصصی:

امنیت سخت افزار و نرم افزار در شبکه ، تست نفوذ، و امنیت سیستم های صنعتی

وظایف:

متخصص امنیت شبکه و سیستم های اسکادا در زیر ساخت های حیاتی مانند نفت و گاز، آب و فاضلاب، مخابرات و ارتباطات و صنعت برق

پروژه های اجرا شده:

ممیزی ISMSشبکه و سیستم های اسکادا در زیر ساخت های حیاتی مانند نفت و گاز، آب و فاضلاب، مخابرات و ارتباطات و صنعت برق

- برنامه نویسی پروتکل های S7comm, DNP3, IEC 104, ModbusTCP
- تدوین چک لیست ارزیابی امنیتی، راه اندازی SOC
- پیاده سازی سیستم لاگ گیری در SIEM
  - برنامه نویسی سیستم های Embedded و سرور و فرانت اند
  - ASP .Net Core
  - C/C++/C#
  - Java Spring Boot
  - Front-End Angular
  - FPGA VHDL & Verilog
  - پایتون (Crawler)
  - یادگیری ماشین و یادگیری عمیق
- نوشتن پروتکل ارتباطی صنعتی S7comm و ارتباط با PLC S7-300, 400 و خواندن اطلاعات حافظه و بلاک های دیتا PLC
- نوشتن برنامه IDS برای کنترل ترافیک شبکه صنعتی

- متخصص امنیت سخت افزار و نرم افزار و توسعه برنامه های برای سیستم های Embedded System لینوکس
- ترجمه تمامی استانداردهای امنیتی و پروتکل های امنیتی نظیر NISTIR 7628، NIST-800-53r4، ISA 99، NERC

۱۳۹۰ تا ۱۳۹۶

شرکت: امنیت فناوری اطلاعات

تخصصی:

امنیت شبکه، امنیت پروتکل و نوشتن پروتکل های صنعتی و دانگل ارتباطی دو شبکه ICS/IT تست نفوذ، ارزیابی ریسک، ارزیابی دارایی، برنامه نویسی و فارنزیک شبکه

وظایف:

مشاور ارشد امنیت و شبکه امنیتی، امنیت ICS

پروژه های اجرا شده:

- Siemens PLC/DCS S7-300/400, oT/IT Security
- برنامه نویسی ,Embedded System، C/C++/C#، Java، Angular
- فارنزیک شبکه
- تست نفوذ Pen-Testing
- طراحی و تولید IDS/IPS، Firewall
- Risk Assessment, Log Analyzer, SOC, SIEM

۱۳۹۵ تا ۱۳۹۶

شرکت: کیا موتورز

تخصصی:

مهندسی معکوس، امنیت شبکه، برنامه نویسی سیستم های Embedded ، سنسور، شبکه خودرو،

وظایف:

برنامه نویسی و تست نفوذ شبکه صنعتی

پروژه های اجرا شده:

- برنامه نویسی کامپیوترهای خودروهای کیا موتورز، هیوندا، بنز و بی ام و
- تولید سیستم عامل های Embedded
- نوشتن کنترلر پروتکل شبکه CAN Network
- عیب یابی کامپیوترهای ECU خودروهای وارداتی
- نوشتن برنامه تست سنسورهای گیربکس اتومات CVT

۱۳۸۹ تا ۱۳۹۰

شرکت: داده پردازی باور

تخصصی:

شبکه، سخت افزار، الکترونیک، برنامه نویسی نرم افزار، برنامه نویس سیستم Embedded، ASSEMBLY/C/C++/C#

وظایف:

برنامه نویسی برد الکترونیکی، طراحی برد

پروژه های اجرا شده:

- برنامه نویسی بردهای الکترونیکی برای چهار راه هوشمند
- برنامه نویسی سیستم های سخت افزاری
- برنامه نویسی Embedded System Board
- نرم افزار های مبتنی بر کاربر با C#
- پردازش سیگنال دوربین آنالوگ
- ارتباط رادیویی
- تخصص در پردازش سیگنال های تلویزیونی PAL, NISC
- شبکه ارتباطی با سنسورهای الکترونیکی و مگنتی در شبکه هوشمند کنترل ترافیک
- برنامه نویسی FPGA VHDL & Verilog
- تست سخت افزار System-Verilog

تخصص های من:

- **SOC:** Vulnerability Assessment, Splunk
- **Programming Language**: JAVA, Nodejs, Python, JavaScript, Angular, Assembly 86x, C/C++/C#, ASP.Net , HTML/CSS, TypeScript
- **DevOps**: Docker, Kubernetes, Git, CI/CD, OpenShift Container Platform
- **Message Handling**: RabbitMQ, Zookeeper Kafka, Redis, Apache nifi
- **Databases**: **MySQL**, SQL Server, Oracle, PostgreSQL
- **Machine Learning**: NLP, TensorFlow, scikit-learn, Anaconda, PyCharm, PyTorch,
- **JAVA Spring Boot**: Spring-Security, Hibernate JPA, JDBC, Microservice
- **BI:** Crystal Report, Tableau, PowerBI
- **Firewall**: SMS Firewall, Industrial and Telecom Protocol Firewall
- **Linux**: Kali Linux, Fedora, Ubuntu 22/18/16, CentOS 7, Remnux
- **Embedded Linux**: RTOS, Yocto Project, VxWorks
- **Reverse Engineering**: Gidra, IDA Pro, Ninja, Cutter

- **Web Service**: Nginx, Tomcat, Apache
- **Networking**: FTP/SFTP, DNS, HTTP, HTTPS, SSL/TLS, SSH
- **Infrastructure Monitoring**: Zabbix, Grafana, Elastic Search
- **Security**: Network Security, OWASP, IDS, IPS, Nmap, Burp Suite
- **Penetration Testing**: Embedded Devices, OS
- **Blockchain**: Bitcoin, Ethereum, DAG, IOTA, Ganache, Truffle, Remix, Solidity, Smart Contract
- **Telecom Core**: OCS/BSS Web API
- **Process Management**: BPMN, BPMS
- **Cryptography**: symmetric key encryption, asymmetric key encryption, public-key encryption, hash Function
- **Cyber Security Standard**:
    - 1. NIST Special Publication 800-53
    - 2. ISO/IEC 27001
    - 3. CIS Controls (Formerly SANS Top 20)
    - 4. NIST Cybersecurity Framework (NIST CSF)
    - 5. PCI DSS (Payment Card Industry Data Security Standard)
    - 6. HIPAA Security Rule
    - 7. GDPR (General Data Protection Regulation)
    - 8. SOC 2 (System and Organization Controls 2)
    - 9. NERC
    - 10. ISA99

سابقه تدریس:

- درس شبکه لیسانس دانشگاه تهران
- معماری کامپیوتر دانشگاه شهید بهشتی و صنعتی سجاد
- ریاضیات ۱ و۲ و ریاضی مهندسی دانشگاه سجاد

- تدریس کورس های امنیت شبکه: SANS SEC 410, SEC612, FOR610, FOR710
- تدریس برنامه نویسی انگولار، جاوا، C/C++/C#, Assembly
- تدریس استانداردهای امنیتی NIST, ISA, IEC64432
- تدریس دوره توسعه و ارائه دوره های آموزشی امنیتی و آگاهی امنیتی

پروژه ها و دانش:

- برنامه نویس USSD Gateway
- برنامه نویسی سیگنالینگ شبکه M3UA, SIGTRAN, SCTP
- برنامه نویسی Embedded System
- طراحی اولین فایروال ICS IDS/IPS.
- طراحی و پیاده سازی SOC و تولید ابزار SIEM
- نگارش و تدوین بزرگترین روشگان امنیتی (چک لیست های امنیتی) در زیر ساخت های کشور نظیر بانکداری، نفت و گاز و پتروشیمی، آب و فاضلاب برق، حمل و نقل بر اساس معتبرترین استانداردهای امنیتی جهان
- مهندسی معکوس سخت افزار و نرم افزار.
- فارنزیک شبکه و پرتکل
- پیاده سازی ابزار لاگ گیری و تحلیل لاگ
- پیاده سازی ابزار الستیک سرچ برای فرآیند خواندن لاگ
- آشنایی کامل با مفاهیم پروتکل، TCP/IP، HTTP، SMB، فریم ورک MITRE
- برنامه نویسی پایتون، Bash Linux
- تدریس دوره آموزشی SANS ICS410 و Security +
- SANS FOR610، FOR610، SEC410، SEC504،
- بهترین دانش در مورد استاندارد امنیتی SCADA NISTIR 7628، NIST-800-53r4، ISA 99، NERC و غیره
- دانش بالا در مورد حملات به یک شبکه
- ۱۳ سال تجربه در امنیت شبکه و پیاده سازی ابزار شبکه

- ارائه چک لیست ارزیابی ریسک امنیتی
- کارشناس فایروال صنعتی و سیستم های IDS و IPS

زمینه مورد علاقه من برای تحقیق:

- یادگیری عمیق در IDS/IPD (سیستم های تشخیص نفوذ/سیستم های پیشگیری از نفوذ)
- Ad-hoc Network VANET
- امنیت شبکه بلاک چین Blockchain Ethereum
- طراحی فایروال شبکه
- SOC و پیاده سازی ابزار SIEM
- امنیت شبکه و امنیت سخت افزار
- تجزیه و تحلیل تروجان سخت افزاری
- یادگیری ماشین و یادگیری عمیق ماشین
- امنیت شبکه
- شناسایی حملات CAN هدفمند در داخل خودرو
- توسعه و ارائه دوره های آموزشی امنیتی و آگاهی امنیتی
- Traditional SIEMها، Vulnerability Scannerها، ابزارهایPenetration Testing ، ابزارهای IPS/IDS، سیستم هایLog Management
- Machine Learningو Advanced Behavior Analytics ، Treat Huntingو built-in incident response و همچنینSOC automation
- بررسی وجود BackDoor در سیستم های پردازنده صنعتی
- بهترین دانش در مورد دستگاه های صنعتی (مثلاً حسگرها، محرک ها و ...)
- مدیریت احراز هویت و مجوز، مدیریت رمز عبور و دسترسی مبتنی بر نقش به حساب‌ها.
- مدیریت الزامات در دسترس بودن، الزامات عملکرد، آسیب پذیری های سیستم عامل و مسائل پهنای باند.