SABRI SALEH HASSANYAH

SENIOR INFORMATION SECURITY

CONTACT

+966 56 985 9955

king.sabri@gmail.com

www.SabriSaleh.info

INTERESTS

RED TEAMING

PENETRATION TESTING

EXPLOIT DEVELOPMENT

RESEARCH

KOWLEDGE SHARE AND TRAINING

LEADERSHIP

EDUCATION

B.S. Computer engineering

6th of October University

2002 – 2007

PROFILE

In this resume, I'm presenting my career path and some of the presentable experience I went through. In addition, as I professionally work, I'm always trying to add my vision to build better security assessment process with greater and doable solutions for risk mitigation. On the other hand, I focus on people behavior that might affect information security in the customers' environment.

My goal at this stage is to work with, build and lead a team of professional offensive security engineers that can be head to head with advanced adversaries for more secure environments.

EXPERIENCE

Offensive Technical Team Lead

TechArch | Riyadh – KSA | 2018 – Present

Working hand by hand with customers to find the best fitting security services and solutions. Working on getting the best of our services especially in red teaming and penetrations testing with leading my team to get the best effort with best results. Help management to understand the current/trending security services and how to compete.

- Develop and maintain services' methodology, implementation approach and processes, and deliverable standards
- Responsible about team's services performance, quality and lead new strategies for improvements
- Ensure the team works & deliver in compliance with defined processes.
- Assist in recruitment, performance evaluation, promotion, retention and termination activities
- Identify skill gaps and lead appropriate training to team (soft and technical)
- Develop division budgets and operate within them
- Empower team to participate in community services
- Studying Information Security market
- Creating and Enhancing security services quality and efficiency
- Leading and orchestrate technical projects, tasks and processes
- Evaluating and tuning consultants knowledge and skills
- Red teaming and penetration testing
- Red teaming and penetration testing
- R & D
- Secure Source code-review
    - Java applications
    - .Net applications
- Architecture and configurations review
- Security training:
    - penetration test
    - advanced web application attacks
    - Offensive Ruby – Ruby for penetration testers and red teamers
    - security awareness
- Pre-sales activities

CERTIFICATIONS

OSCE – Offensive Security Certified Expert

OSCP – Offensive Security Certified Professional

GWAPT – GIAC Web Application Penetration Tester

CEH – Certified Ethical Hacker

RHCE – Red Hat Certified Engineering

CCNA – Cisco Certified Network Associate

MCITP EA – Microsoft Certified IT Professional Enterprise Administrator

SKILLS

Platforms:
Linux (Ubuntu, Redhat, Debian), windows (Win7,8-2003, 2012, 2016).

Security tools:
nmap, burpsuite, acunetix, netsparker, metasploit, gfi network, nessus, ossim, snort, ossec, iptables, etc.

Prog languages:
Ruby(mainly), rails, bash, python, java, powershell, c++, assembly.

Databases:
mysql, mongodb, postgress, oracle, mssql.

Virtualiztion & cloud:
VMware, docker, virtual box, azure, OpenShift.

Communication skills:
Excellent written and verbal communication, Excellent presentation and negotiation skills, Team player and leader, well body language understanding and reactions.

EXPERIENCE

Sr. Information Security consultant and team lead

TechArch | Riyadh – KSA | 2014 – 2016

Working hand by hand with customers to find the best fitting security services and solutions. Working on getting the best of our services especially in red teaming and penetrations testing with leading my team to get the best effort with best results. Help management to understand the current/trending security services and how to compete.

- Technical Team Lead
- Red teaming and penetration testing
- Services and consultation development
- R & D
- Source code-review
- Architecture and configurations review
- Security training:
    - penetration test
    - advanced web application attacks
    - security awareness
- Pre-sales activities

Sr. Information Security Engineer

Ministry of high Education (MOHE) | Riyadh – KSA | 2013 – 2014

Full responsibility for vulnerability assessment and penetration testing. Responsibility include contact and meet development teams to find best fixes and spread awareness. In addition, the ability to involve security assessments in early development stages.

- Web and mobile penetration testing.
- Network and system penetration testing.
- Following up vulnerabilities fixes.
- Training and awareness.

Information Security Officer

Advanced Operations Technology (AOT) | Riyadh – KSA | 2010 – 2013

Hold accountability for planning, administering and monitoring the effectiveness of information security policies, programs, and procedures. Coordinate design, deployment, testing and upgrading of enterprise security and disaster recovery solutions, including installation and configuration of network security devices.

- Linux Firewall (iptables) administrator
- Apply information technology security programs, policies, and procedures.
- Administer and maintain end user accounts, permissions, and access rights.
- Monitoring and managing firewall, IPS and firewalls logs and operations.
- Investigate security breaches and vulnerability incidents.
- Conduct Penetration Testing.
- Enforce the ISO-20000 standard controls & Pass Certificate Auditing.
- Enforce Tadawul (Saudi Stock Exchange for Trading) Security controls.
- Develop and maintain a Business Continuity and Disaster Recovery plan.
- Build operation guidelines for different network security devices.

Linux Administrator

Innovative Application Co. Ltd (IAC) | Riyadh – KSA | 2009 – 2010

Developed, assembled and administered infrastructure for startup Web-hosting companies. Installed, configured and administered Linux servers. Provided consultation and training regarding Linux hosting services. Implemented security patches in response to identified vulnerabilities. Interfaced with clients in providing Linux-systems support, troubleshooting and training.

- Implementation, Installation, and Deployment for all kind of Linux Servers.
    - Web, database and mail servers
    - DNS, DHCP, VoIP, LDAP, Proxy and firewall servers,
    - Fax, iSCSO, LVM, NAS servers
- Troubleshooting and Solving client Linux services related problems.
- Linux training instructor.

PUBLICATIONS

Rubyfu book – Author of Ruby programming for pentester and red-teamer book.

SELinux book – Practical introduction to SELinux.

MD5 algorithm book – A book explains MD5 algorithm in academic but simple approach

Security4arabs.com – Co-founder and writer in on of most know infosec Arabic websites.

LinuxAC.org – Writer (former moderator) at biggest Open-source arabic community.

ATTENDED COURSES

BlackHat | Advanced Web Attacks and Exploitation – Advanced Web application exploitation and exploit chaining that always leads to OS shell.

BlackHat | Advanced Windows Exploitation – Advanced Windows exploitation and memory mitigation bypass.

BlackHat | Adversary Tactics: Red Team Ops – Advanced Red Team TTPs for real-world and complex environment scenarios.

TRAINING EXPERIENCE

Teaching is an art of knowledge sharing and it should be more realistic and informative. My philosophy of teaching is not just sharing topics, it's sharing experience, since most of the information nowadays are freely available on the internet and what people seek are organized information, experience-based knowledge, and instance answeres.

King Saud University(KSU)

Professional training for professionals and students via Center of Excellence in Information Assurance (CoEA), I gave the following training courses:

- **Penetration testing Lab**

  Practical training converting all penetration testing stages concepts and required tools. The course includes practical lab with isolated environment includes AD, Firewall/Nat exploit development, etasploit exploitation and post exploitation then reporting.

- **InfoSec and Cyber Crimes**

  The course convers computer and networking fundamentals, basics of information security, computer crimes and national law, cyber war and its effects, introduction to digital forensics.

Saudi Telecom Co. (STC)

STC is the biggest telecom company in KSA and I gave the following training courses:

- **OWASP Top 10 (2013/2017) for DevOps**

  The course convers all OWASP top 10 risks that affect applications including web and mobile applications. The course's practical part differs based on audience category(developers, operations, security). In addition, I consider the business needs.

Advanced Web App Attacks

A Practical training course course converse advanced web applications attacks and manual testing includes SQLi, XSS, CSRF, RCE, File upload and writing exploits scripts for professionals and students given on behalf of a Jordon-based firm specialized in infsec training named isecurity.

PROGJECTS AND ACHIEVEMENTS

CVE-2015-7822, CVE-2015-7823

Multiple Vulnerabilities Kentico CMS 8.2.x

Rubyfu.net

Ruby for hackers and pentesters book. First and yet the only Ruby for hacker book ever.

Metasploit modules

Contribution with Auxiliary modules and bugfixes community support

Buffer overflow kit

Collection of many tools used in buffer overflow development in one place

Scenario based scripts

Many customs scenario-based scripts that being privately shared with customers

BurpSuite Extensions in Ruby

Ruby templates to speed up building Burp Extensions using Ruby

CVE in Ruby

Exploits written & ported to Ruby - no Metasploit

Ninja Firewall

Application converts a standalone Linux firewall to a failover Linux firewall. Handels all operational tasks on both server and network side including switches.

SQLmap tamper-api

SQLMap tamper api allows sqlmap to accept tamper scripts from all languages no just python.

Hacker's Note

A command-line tool creates gitbook compatible structure for pentest and read team projects documentation.

REFERENCES

References available upon request!

SOCIAL

@KINGSABRI

kingsabri

KINGSABRI

/ sabrisaleh