SafeKeep

RESUME: AAR & MPR

Strong Points

- 10 years of total experience in the domain of cyber security
- Missions in: Cyber Security Consulting, Network & Infrastructure, Web Application Security, loud Auditing, Network Security Firewalls, Automobile Sector, Smart Meters, Intrusion Detection Systems, Endpoint Security Suites, Penetration Testing
- Certifications: CISSP, CEH, CCSK v4, MCPT (GCP, AWS, Azure), AWS Solution Architect Associate, RHCE, RHCOA, NSE4, PCNSA, Network+, Security+, HP-Cisco, Project Management (UCI), etc.
- Methodologies: OWASP, NIST, First level security certification (CSPN) by the ANSSI

Expertise

- Infrastructure, network, web application vulnerability analysis
- Cloud audit and security optimisation
- Building and monitoring security solutions
- Installation and configuration of PKI infrastructures
- Incident management: Analysis of cyber attacks and technology watch, remediation of vulnerabilities, impact and root cause analysis
- Process monitoring and operational procedures
- Application security: code audits (Python) and penetration tests
- Management of KMS (embedded and on Cloud), encryption keys, digital certificates and cryptographic aspects and tests for compliance by ANSSI
- Skills: Python, JAVA, C++, Raspberry Pi, Kali Linux, Snort, Suricata, Security Onion (Virus scan and intrusion detection), etc.
- Tools: BurpSuite, Nessus, Rapid7, Appspider, Wireshark, Hydra, John, Dirbuster, Nikto, Sqlmap, Nmap, Hashcat, Openssl, Bash, etc.

Professional Experiences :

Cybersecurity Consulting :

- **On assignment for infrastructure and network security, web application security, and cloud security**

  - Vulnerability and security risk assessment of internal and external network infrastructure
  - Vulnerability and security testing of web applications
  - Audit of cloud environments (AWS, GCP, AZURE) for security optimization
  - Deliver internal technical report and external partner facing security audit reports
  - Inform stakeholders to observed security risks
  - Technical environment and methodologies: Kali Linux, bash, python, Hydra, Nmap, SQLmap, Burp Suite Pro, Wireshark, OWASP, Netcat, John the Ripper, Hashcat, Bacu, AWSBucketDump, Goolge Web Security Scanner, GCPBucketBrute, gcloud.

- **On assignment for customers in the automotive sector**

  - Pen-Test of connected cars (telematics), of their Cloud platform
  - Management of KMS, verifications of keys, certificates, etc.
  - Technical environment and methodologies: Kali Linux, bash, python, Hydra, Nmap, SQLmap, Burp Suite Pro, Wireshark, OWASP, Netcat, John the Ripper, Hashcat

- **On assignment for customers in the energy sector (Smart-Meter)**

  - Pen-Test of connected smart meters, from their Cloud platform. Smart meters use MQTT, DLMS-COSEM protocols for communications
  - Developed a fuzzing tool using Python, Paho, Radamsa for the MQTT evaluation and the configuration of MITM_relay, and BurpSuite for the MQTT Proxy.
  - Technical environment and methodology: CSPN by ANSSI and METAS (Switzerland), Kali Linux, Bash, Python, Hydra, Nmap, SQLmap, Burp Suite Pro, Wireshark, OWASP, Netcat, John the Ripper, Hashcat, Mosquitto for MQTT

Professional Experiences :

Cybersecurity Consulting :

- **On a development mission in the digital sector**

- Pen-Test of a tool that was used to perform a vulnerability scan developed with Python and Java on Ubuntu, the whole solution was in an ISO package.
- Technical environment and methodology: CSPN by ANSSI, Kali Linux, Ubuntu, Bash, Python, Hydra, Nmap, SQLmap, Burp Suite Pro, Wireshark, OWASP, Openssl

- **On assignment for clients in the IoT sector**

- Pen-Test of a set of four roller motors for smart home, four remote controls, and their gateway. IoT devices use Bluetooth low energy and the Zigbee protocol to communicate with each other.
- Development of a fuzzing tool using Python, Killerbee, Radamsa for ZigBee evaluation and engine configuration.
- Technical environment and methodology: Kali Linux, Bash, Python, Wireshark, Bumblebee, Killerbee, Bettercap, Btlejack for BLE (Bluetooth Low Energy).

- **On assignment for customers in the aviation sector**

- Fuzzing for MSTS, one of the components of the TopSky system.
- Black box test, to discover “zero-day” vulnerabilities, robustness, and efficiency of the MSTS system by simulating thousands of test scenarios.

- **On assignment for malware analysis solution**

- CLI tools take pcap / pcapng files as input and classify required information such as IPs, domain names, type of requests, and downloaded files. Also has the ability to read those coming from blacklisted databases and update them if a newly infected system is found.
- Tools used – Linux, Bash, Python, Scapy, Wireshark et malware-traffic-analysis.net/.

Professional Experiences :

Cybersecurity Consulting :

- **On assignment with firewall vendor Fortinet**

- Supervision of Fortinet Certification "Network Security Expert Level 4"
- Develop a virtual NSE4 lab for Fortinet NSE4 certifications and train two Eurecom students on these labs.
Authentication Firewalls, Security Policy, Logging & Monitoring - Eurocom and Fortinet
- Use of GNS3, the configuration of FortiGate (a new generation of firewalls), FortiAnalyser, FortiGuard, Linux endpoints (docker), GNS web & FTP servers.

- **On assignment for application layer firewall design**

- Developed a cluster of 6 VMs, with a centralized firewall between them, carried out using technologies such as iptables, local DNS, Snort, and Suricata while having configuration services such as Apache2, TFTP, etc.
    - Establishment of a laboratory with VMware including the following elements:
    - Installation and configuration of the hypervisor.
    - Installation of Windows and Debian servers.
    - Setting up and configuration of DNS, DHCP, TFTP, SSH, Proxy servers.
    - VLAN segmentation.
    - Network configuration (switching and routing).
    - Tests and supervision with Snort and Suricata.