ahmed.mkadem@eurecom.fr

Ahmed MKADEM

Avenue Foch, 75116, Paris

IT Security Engineer/Security researcher

https://www.linkedin.com/in/mkadema/

+33 768625678

Looking to attain a position as a malware analyst and exploits developer with a company that encourages the contribution to research in cybersecurity on software and hardware vulnerabilities and the use of analytical skills to achieve innovative solutions.

Working History

Since December 2018 **IT Security Engineer, XPO Logistics**

Intervene on cybersecurity incidents. Analyzing malwares to improve attacks detection techniques. Contribute to R&D for the enhancement of our internal tools. Automate (Scripting) repetitive tasks for incident detection.

(**Key words**: Incident detection, Malware analysis, Sandboxing, Reverse Engineering, Python, Shell).

March 2018 – Sep 2018 **Master Thesis internship R&D, GROUPE RENAULT: RENAULT SOFTWARE LAB**

Analyze the attack surface in the automotive world. Evaluate on a practical level each proposed solution through penetration tests and exploit attempts. Contributing to the decision to integrate each tested product and drawing up technical reports. Test bench: Raspberry Pi, Yocto Project.

(**Key words**: Code-reuse attacks, Control-Flow integrity, Return-Oriented Programming, Memory Corruptions, ARM shellcoding).

Education

2016-2018 **EURECOM Research Center and Engineering School - (ParisTech site Sophia Antipolis) - Double degree program**
Engineering degree in Security of Computer Systems and Communications.

2014-2016 **Higher School of Communication of Tunis (SUPCOM)**
Engineering degree, Telecommunication.

2012-2014 **Preparatory school for engineering studies**
Preparatory school, Math & Physics.

Academic Projects & Professional Certifications

Since Jan 2021 **[Certified Malware Reverser]** **GIAC Reverse Engineering Malware (GREM)**

Analyzing protected executable, Analysis of malicious documents/web-based malwares, Malware analysis using memory forensics, Windows malwares reverse engineering, Malware code and behavioral analysis. Verifiable certificate here.

Since Sep 2020 **[IN PROGRESS – 70% training done – expected in Feb 2021]** **Certified Exploit Developer, Elearnsecurity, ECXD**

Windows and Linux exploit development, Software vulnerability identification, Reverse engineering (x86, x64), Shellcoding, Software debugging, Linux and Windows anti-exploit bypass.

Oct 2017-Feb 2018 **X Window Memory Analysis, Memory Forensics Project (EURECOM)**

Study the internal structures of the window system protocol managing the screens on UNIX (X11). Propose a way to extract an information window from a given memory dump and implement the result a volatility plugin to reconstruct the application windows opened at the time memory snapshot. (Programming Languages: C & Python, Key words: Memory Forensic, Volatility tool) Source Code available here.

March 2017-June 2017 **Implementation of a cryptographic protocol for Cloud Security, (EURECOM)**

Implementation of a new multi-user searchable encryption protocol that allows customers to delegate their data to a Service Cloud Provider (CSP) and allow other users to search in their encrypted data without decryption.

(Programming Language: C/C++, Key words: Searchable encryption) Implemented research paper here.

Oct 2016-Feb 2017 **Secure Data Storage for Autonomous System, (EURECOM)**

Design a cryptographic protocol enforcing a secure storage of telemetry and sensed data during an autonomous system mission. Design of a cryptographic mechanism to protect these data in case of an interception of the system.

(Programming Language: C, Key words: Cross-compilation, AES encryption, Forward Secrecy)

Skills

Spoken languages: Arabic, English, French
Programming Languages: C/C++, Python, Shell, Assembly (ARM, x86)
Exploitation: Shellcoding, Linux & Windows anti-exploit bypass
System security: Reverse Engineering, Binary exploitation

Intrests

Football, Tennis Table, CTFs (Hacking competitions)