Jan Hoersch

IT Security Consultant, Penetration Tester

nv1t.github.io - keybase.io/nv1t - nv1t - @nv1t

Career Profile

I'm an IT Security Consultant & Penetration Tester with 10 years experience in IT Security and 6 years of professional experience in IT Security Consulting targeting various companies in FinTec, Chemical Industries, Banking, Automotive Industry. With at least basic knowledge in a wide variety of IT Security topics, my major focus is on penetration testing and reverse engineering of various devices. I'm highly motivated to learn new tricks, broaden my knowledge getting to know other work environments.

Core Competencies

Burp Suite, CANAPE, IDA Pro, CobaltStrike, Metasploit, Immunity, Wireshark, Linux/Unix Administration, Security Monitoring, Hardware Hacking (SPI, JTAG, etc.), Docker, Python, Bash, Lockpicking (pending)

Education

OSCE, Offensive Security	2017
MASPT, eLearnSecurity	2015
OSCP, Offensive Security	2014
IT Specialist for System Integration	2011-2013

Experience

Lead Security Consultant, Context Information Security Ltd. 2018-present

Penetrationtests (Web-Applications, Infrastructure, Mobile, Cloud, Code Review), scenario based tests and Redteams for various customers (FinTec, Chemical Industries, Banking, Automotive), internal tool development

IT Security Consultant, Securai GmbH 2014-2018

Performing penetration tests and reverse engineering tasks on mobile application, web applications and rich clients for various customers.

Network & Security Engineer, TMT GmbH & Co. KG 2011-2014

During 2.5 years as a trainee as a network engineer, i managed several tasks, mainly system programming, server monitoring as well as internal software audits based on network environment and web applications.

Founder, Kouponki 2011

During the 5-Euro-Business competition i founded with 4 fellow students the Kouponki GbR. With a lot of engagement we managed to win the comptetion with this start-up company.

Publications

I hate you, WD, blog.nv1t.me

Recovering a failing HDD by swapping the bios chips on a PCB and disabling the re-location list for faster transfer speed.

IoT Pentest - Der Weg von der Firmware zur Shell, Securai Blog

Demonstrating an IoT attack path from downloading firmware to remote code execution on the device.

Binary Patching von Java fuer Rich-Client Penetrationtests, Securai Blog

Patching Java Rich-Clients to circumvent checks during security assessments.

SQLi after order by in less than 22 chars, blog.nv1t.me

Solving a SQLi challenge by using the order by feature and known content.

IoT Security Nightmares - 20 minutes, 10 devices, Kaspersky Security Analyst Summit, 2017

Talk about easy exploitation of IoT devices and current state of responsible disclosure due to bad communication with vendors.

I like trains, MRMCD 2015

Accessing undocumented APIs from big companies is fun. Especially if you get loads of data to store and analyze from them.

Men who stare at bits (Part 2), 29th Chaos Communication Congress

Reverse Engineering of multiple RFID payment systems from different universities. Most of these systems were based on Mifare Classic Cards with custom encryption on the card.

Men who stare at bits, Sigint12

Reverse Engineering of one RFID payment system with custom encryption of the credit sector of the card.

Douding Document Sharing, blog.nv1t.me

Reverse Engineering of the Douding Document Sharing Network Reader

Projects

Standing Desk Interceptor - Reverse Engineering my standing desk to create more functionality. It consists of two UART Communication channels and a custom protocol running between two Microcontrollers.

iliketrains - Accessing undocumented APIs from big companies is fun. Especially if you get loads of data to store and analyze from them. (See publication for talk on this project)

FreeElmo - Reverse Engineering an Elmo Document Camera and writing MultiOS Client.

Personal

Birth date: 28. July 1988
Citizenship: German
Residence: Dresden, Germany

Last updated: August 2020