





ARMANDO HUESCA

Security Researcher | Penetration Tester
Security Engineer

CONTACT

+393xxxxxxx10 
armandohuesca@icloud.com 
linkedin.com/in/armandohuesca 
Turin, Italy 

EDUCATION

MASTER'S DEGREE: Computer and Communication
Networks Engineering.
Politecnico di Torino, Italy / 2013 — 2017
Faculty: Computer Science.

BACHELOR'S DEGREE: Telecommunications and
Electronics Engineering.
Havana Institute of Technology (CUJAE) / 2008 — 2013
Faculty: Telecommunications

LICENSES AND CERTIFICATIONS

OSCE
Offensive Security Certified Expert
Offensive Security / Dic 2019 — In progress...

OSWP
Offensive Security Wireless Professional
Offensive Security / Apr 2019 — Present

OSCP
Offensive Security Certified Professional
Offensive Security / Apr 2018 — Present

CVEs

CVE 2019-7217
CITRIX SHAREFILE USER ENUMERATION
URL: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7217>
30 Jan 2019

CVE 2019-7218
CITRIX SHAREFILE TWO FACTOR AUTHENTICATION
DOWNGRADE TO ONE FACTOR
URL: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7218>
30 Jan 2019

PERSONAL SUMMARY

Information Security Professional involved in vulnerabilities assessments and hacking activities. Passionate about discovering systems security breaches with the scope of turning them into impenetrable and secure systems.

WORK EXPERIENCE

PENETRATION TESTER | SECURITY ENGINEER
SKIT Cyber Security/ Dic 2016 — Present

Security analyst for conducting penetration test and vulnerability assessment activities with manual and automated application security testing tools.

POSITION RESPONSIBILITIES:

- Network Penetration Testing.
- Social Engineering
- Web Application & Wireless Pentesting
- Customer's internal & external infrastructure Vulnerability Assessment
- Mobile App Penetration Testing
- Reverse Engineering, Binary & Malware Analysis
- Antivirus Evasion Technics
- Embedded IoT Systems, CPE & TIR Vulnerability Assessments
- Fortinet Infrastructural Technical Support

Conducted offensive security trainings including theoretical and cyber-labs. Security Testing based on OWASP and OSSTMM Methodologies. Writer of security advisories and exploitation documentation following guidelines established by NIST (NVD) and exploits 0day.

SECURITY RESEARCHER
SYNACK Red Team/ Jun 2018 — Present

Security analyst for conducting penetration test and vulnerability assessment activities with manual and automated application security testing tools.

POSITION RESPONSIBILITIES:

- Security researcher and bug hunter in Web Applications, Infrastructure and Network areas.

NETWORK SECURITY EXPERT INTERNSHIP
SHORR-KAN IT ENGINEERING SRL / AUG 2016 (month)

Hands on Fortinet Infrastructural and Network Security Expert training focused on potential information and security vulnerabilities identification, incidence response and risk management.

POSITION RESPONSIBILITIES:

- Infrastructural and network perimeter protection through security policies implementation.
- Monitoring and management of Fortinet firewalls, Virtual Private Networks (VPNs).
- Intrusion Detection/Prevention Systems (IDS/IPS), reverse proxy and data loss prevention.

ARMANDO HUESCA

Security Researcher | Penetration Tester
Security Engineer

ORGANIZATIONS

INTERNATIONAL CONSORTIUM OF MINORITY
CYBER PROFESSIONALS ICMCP

Practitioner Supporter
Mar 2016 – Present

LINUX FOUNDATION

Individual Supported
Jun 2016 – Present

INTERNET SOCIETY ISOC

Collaborator
May 2014 – Present

PUBLICATIONS

ATTACKS AND PERFORATIONS OF SECURITY
PROTOCOLS IN WIFI NETWORKS

Telecommunications Department, ISPJAE, Havana,
Cuba, 2013.
ISSN:1729 3804

REFERENCES

Heidy Hernandez Breton - Software Engineer
“<https://www.linkedin.com/in/heidy-hernandez-breton>”

Antonio Fiorito - Head of Information Security
“<https://www.linkedin.com/in/antonio-fiorito-oscp-osce-22649023>”

INTERESTS

- Cyber Security
 - Traveling
- Space Exploration
 - Baseball
 - Running
- Technology

WORK EXPERIENCE CONTINUED

NSE ATTENDED COURSES:

-
- Fortinet NSE 1 Training: Network Security Technology Foundations.
- Fortinet NSE 2 Training: Network Security Solutions Training for Sales.
- Fortinet NSE 3 Training: Network Security Product Training for Sales.
- Fortinet NSE 4 Training: FortiGate Network Security Professional.

Fortinet NSE Institute

NETWORK ENGINEER INTERN

IXEM LABS FOUNDATION / SEP 2015 – JUL 2016

Concept design and implementation of a Secure Communication Infrastructure for high-speed mobile nodes focused on fast Trains technologies.

POSITION RESPONSIBILITIES:

- System administration and real time network monitoring.
- Behavioural assessment of Experimental Congestion Control Algorithms for Multipath-TCP over a ciphered environment.

SECURITY RESEARCH INTERNSHIP

RESEARCH CENTER OF INTEGRATED TECHNOLOGIES AND CYBER
SECURITY CITI / SEP 2012 – DIC 2012

Analysis and Penetration testing of Wireless security protocols. Wireless virtualised environment design and implementation. Stress test and brute-forcing attacks against WEB, WPA, WPA2 and WPS Wireless Security.

PERSONAL PROJECTS

PERFORMANCE ANALYSIS OF MULTIPATH-TCP PROTOCOL OVER SECURE TCP
FLOWS - THESIS PROJECT :

- Behavioral assessment and performance of experimental Congestion Control Algorithms for Multipath-TCP over different ciphered environments.
- Congestion Control Algorithms involved: OLIA, LIA, BALIA, wVegas, CUBIC.
- Technologies involved: MP-TCP protocol, IPsec Protocol, Basic VPN Security Architecture, Ubuntu Linux Distribution, Debian kernel development tools, VMware virtualization, Bash programming language

SECURITY VULNERABILITIES ASSESSMENTS ON WIRELESS LAN
TECHNOLOGIES

- Real time testing of Wireless Network Security Protocols. Management of the Network.
- Behavioral assessment of Wireless Technology under Denial of Service Attacks.
- Distribution used: Linux Backtrack 5.