europass Curriculum vitae

PERSONAL INFORMATION

André Lima

Melbourne (Australia)

andreflima@gmail.com

https://andrelima.info https://pentesterslife.blog/

Date of birth 15 Jan 1986 | Nationality Cape Verdean

PREFERRED JOB

Computer Security Researcher / Penetration Testing / Red Teaming

WORK EXPERIENCE

28 Jul 2018–Present

Senior Security Consultant

PS&C Group, Melbourne (Australia)

- Penetration Testing
- Coordinate Red Team engagements
- Research and tool development (bypass AV and other security controls)
- Physical recon and physical attack deployment

19 Jun 2017–28 Jul 2018

Senior Penetration Tester & Security Consultant

Pure Hacking PTY LTD, Melbourne (Australia)
https://www.purehacking.com/

- Penetration Testing
- Research

1 Oct 2016–13 Jun 2017

Team Leader Pentesting Team

Integrity S.A., Lisbon (Portugal)

- Coordinating team members
- Scheduling automated scans and its analysis
- Making sure analysis by different members render the same consistency throughout all clients' scans
- Mentoring junior team members
- Guiding the creation of vulnerability templates for reporting
- Develop scripts (python+bash on github) that assist in guaranteeing consistency and efficiency throughout the pentesting process

22 Jan 2011–13 Jun 2017

Penetration Tester

Integrity S.A., Lisboa (Portugal)
https://keepitsecure24.com/

- Penetration Testing
  - XSS, SQLi, CSRF, Indirect object references, LFI, RFI, file uploads, and other webapp testing while mostly using Burp Suite
  - Scanning (nmap, nessus), metasploit, exploit alteration for specific uses, and other infrastructure testing consistent with OSCP trainning
  - WEP detection and cracking, WPA/WPA2 bruteforcing, WPA-Enterprise Mitm attacks using patched freeradius server and other wireless testing
  - Forensics: File system, memory, online, and offline analysis

- Reporting on vulnerabilities and recommendations for their mitigation
- Information Security Consulting
  - Evaluation, recommendation, and implementation of security systems
  - ISO27001 consulting

22 Nov 2010–21 Jan 2011

Internship in Information Security Consulting

Integrity S.A., Lisboa (Portugal)
https://integrity.pt/

- Nagios monitoring management
- Cisco security network evaluation

EDUCATION AND TRAINING

11 Feb 2019–14 Feb 2019

Windows Kernel Rootkits: Techniques and Analysis, by Bruce Dang

OffensiveCon (by Blue Frost Security), Berlin (Germany)

- Machine architecture for kernel programmers
- Virtual memory management
- Interrupts and exceptions
- CPU security features
- Windows kernel architecture
- Kernel components (Ps, Io, Mm, Ob, Se, Cm, etc.)
- System mechanisms
- Debugging with WinDbg
- Rootkit techniques
- Driver development

Completion Certificate: https://andrelima.info/files/offensivecon19.jpg.

6 Aug 2018–7 Aug 2018

BlackHat USA 2018 - Fuzzing for Vulnerabilities

Huntress Labs - Black hat Trainer, Las Vegas (United States)

- Mutative fuzzing (radamsa) vs Generative fuzzing (Sulley, Spike)
- Dumb fuzzing (AFL)
- Smart fuzzing (Boofuzz, Langfuzz)
- Code coverage
- Instrumentation
- Corpus Distillation

Completion Certificate: https://andrelima.info/files/FFV.jpg

1 Sep 2009–Present

Masters in Computer Science

Instituto Superior de Engenharia de Lisboa, Lisboa (Portugal)

Computer Network Security, Networks and Services Integration, Multimedia Communication Networks and Services

1 Sep 2003–20 Feb 2009

Undergraduate degree in Computer Science

Média 14 valores

Instituto Superior de Engenharia de Lisboa, Lisboa (Portugal)

Computer Networks, Internet Networks, Advanced Network Technology, Information Security

Final Project: Toll devices and application's monitoring system

PERSONAL SKILLS

Mother tongue(s) Portuguese, crioulo

Foreign language(s)

	UNDERSTANDING		SPEAKING		WRITING
	Listening	Reading	Spoken interaction	Spoken production	
English	C2	C2	C2	C2	C2
French	B1	B1	A2	A2	A2
Spanish	A2	A2	A2	A1	A1

Levels: A1 and A2: Basic user - B1 and B2: Independent user - C1 and C2: Proficient user
Common European Framework of Reference for Languages

Communication skills

- Good communication skills aquired mostly through presentations and client interactions/projects. One of the presentations was at Sapo Codebits 2014 - http://videos.sapo.pt/PEh5sBKdDgMTPp2ZvluF

Job-related skills

eWPTX - eLearnSecurity Web Application Penetration testing; CREST Certified Registered Tester (CRT); **OSCP** - Offensive Security Certified Professional; Associate **CISSP** - CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL; **ISO 27001** Leading Auditor; **CCNA Security** (Implementing Cisco IOS Network Security) - IINS; Cisco Certified Network Associate - **CCNA**

Also contributed to the **Exploit Database and Google Hacking Database**, and **SecurityTube Linux Assembly (x64) Expert** (**SLAE64**).

Familiar with: Linux (Debian, Ubuntu), Mac OS X, and Windows systems.

Programming Languages: Python, Bash script, Assembly x86_64 and x86, C, C++, PHP

Tools/Software: Burp Suite Pro, Kali, Metasploit, Meterpreter, nasm, ld, gcc, gdb, WinDBG, Volatility, Nmap, IPTables Firewall, Nagios monitor (plugin development), amongst other specific tools.

Solid background in cryptography, operating systems and networks.

Other skills Cape Verde's basketball National under 16 Team - IV Jogos Desportivos da CPLP (Cidade da Praia 21 a 28 Julho 2002)