# ANDREA GIAIME BODEI

EU Italian Citizen

info@andreabodei.com

## SUMMARY

- Extensive knowledge of Intelligence and investigation principles and methods. Cyber-Crime, Cyber-Conflicts, Cyber-Warfare. Custom virus writing, microspy search, wiretap and data logging for police and governmental consulting.
- System, Network, Web and Mobile Ethical Hacking, Penetration Test. Vulnerability Assessment, Security Audit. Former Team Leader of the Telecom Italia's Tiger Team.
- Information Security Crime Investigator/Forensics expert for police and corporations. Previous experience in Fraud Management.
- IT security consultant, standards OSSTMM, OWASP, NIST, SANS, PCI-DSS.

**In Bolivia/Brazil/Cuba/France/Italy/Mexico/Peru/Qatar/SaudiArabia/Singapore//Spain/UK/USA** - with Banks, ISPs and Police/Governments.
Possible authorization for the NOS / Security Clearance (<u>no criminal record</u> / <u>no criminal inclinations</u>)

## PRESENT POSITION

- **Intelligence Framework Inc.**, USA. CEO and Developer of **INFRA** Security and Vulnerability Scanner
INFRA is the most powerful Vulnerability Scanner and Exploitation system with more than 500,000 plugins, an easy interface in many languages for scanning and exploiting. For Vulnerability Assessments, Penetration Testing and Intelligence, it can also connect to popular open source and commercial security softwares including Nessus, Burp Suite, Acunetix WVS, Rapid7 Nexpose and Metasploit. For governments, corporations and security companies.
www.infrascan.net

- **Seed Security LLC**, USA. CTO and Ethical Hacker. Vulnerability Assessment, Penetration Testing, Risk Assessment, SOC.
Currently working with several banks and government in Latin America. www.seed-security.com

- **FOX Media LLC**, USA. CTO and Ethical Hacker.
Security Manager        (Managerial level consulting)
Tiger Team              (Penetration Test, VA, Audit)
Intelligence Services   (BI, Forensics, Micro spy)
Virus writing           (Police/Government consulting)

- **Security Division SRL**, Italy. CTO and Ethical Hacker.
Vulnerability Assessment, Penetration Testing, Risk Assessment, SOC, Webreputation, architectural advising and patch management to a variety of corporate and governmental clients in Italy, France, UK. www.securitydivision.it

- **OKIJOB LLC**, USA. CTO and Ethical Hacker. Mobile Apps, development and security.

- **Efecto Ticket LLC**, USA. CTO, development and security.

  Consultant for Italian national law enforcement agencies; working with Carabinieri (Italian military police), Investigative Police, Counter-Terrorism and Guardia di Finanza (Italian military Police for economic frauds). Forensics, custom viruses, wiretapping and microspy. www.andreabodei.com

# ANDREA GIAIME BODEI

info@andreabodei.com

## CAREER

- **2015 - 2016** – Seed Security USA, CTO, Penetration Test and teaching in Spain, Peru, Qatar.
- **2014 - 2015** – Deloitte in Spain, Team leader Penetration Test and VA, Web applications, Mobile Applications, big netwoks, PCI-DSS, teaching Ethical Hacking.
- **2013 - 2014** - A2SECURE in Spain, Team leader Penetration Test and VA, Web applications, Mobile Applications, big netwoks, PCI-DSS, teaching Ethical Hacking.
- **2012 - 2013** - McAfee in Saudi Arabia, CyberWar Forensic/Crime Investigator, Intelligence in Saudi Arabia for the biggest hacker attack in the history of Internet. My contribution was essential to solve the case.
- **2007 - 2012** - Security Division S.r.l., CTO, Team leader Penetration Test and VA, Forensic and Security Consultant, Computer Forensic, Intelligence, malware searching, SOC, Windows and Linux administration.
- **2006 - 2007** - Telecom Italia, Team Leader Penetration Test and VA, Forensic and Security Consultant, TigerTeam, Governance Information Security (SEC.G.I.S. Rome, Italy). Penetration Testing for partners and clients of Telecom Italia in Italy, Brazil, Cuba and Bolivia. Windows and Linux administration.
- **2005 - 2006** - The Technology Partners, (Working at Telecom during the day, and TTP at night) Penetration Test activity for the italian government.
- **2004 - 2006** - Telecom Italia, Team Leader Penetration Test and VA, Forensic and Security Consultant, Windows and Linux administration (SEC.T.I.S. Rome, Italy). Italy, Brazil and for clients especially banks.
- **2003 - 2004** - Telecom Italia, Team Leader  Penetration Test and VA, Forensic and Security Consultant, Fraud Management (SEC.F.M. Rome, Italy). Investigating fraud against Telecom Italia. I've also been the only forensic analyst at the company. Windows and Linux administration.
- **2000 - 2003** – Zone-H / Domina Security, Penetration Test and VA, Forensic and Security Consultant, Rome and Milan, Italy. With this company we started the development of Zone-H.org

## TEACHING AND EDITORIAL

- **2017** - Teacher of Cyber Security, Seguval - Universidad del Valle de Atemajac Mexico.
- **2017** - Contributor of the financial newspaper "Milano Finanza", Italy.
- **2014** - Teacher of Ethical Hacking, Deloitte, Barcelona, Spain.
- **2013** - Teacher of Ethical Hacking, A2Secure, Barcelona, Spain.
- **2010** - Contributor of the periodic www.mensiletechnet.it
- **2008 -** Guest Professor - **"la Sapienza" University of Rome** "Investigation" course, "Criminal Anthropology" department. http://www.uniroma1.it
- **2007 -** Speaker - February 20 - **"la Sapienza" University of Rome** "Sicurezza Mobile". Andrea Bodei – "Secure Communication and Crypto Mobile". http://www.xakep.it/
- **2005** - Teacher - Zone-H.org Seminars "Hands on Hacking" Teacher and assistant in Italy and Estonia.
- **2005** - Editorial Staff Criminologia.org (Rome, Italy). News, manuals and help to organize courses about computer-related crimes. http://www.criminologia.org/
- **2004 -** Speaker - **"la Sapienza" University of Rome** "IT & Law" Speaker: Andrea Bodei "Simplicity of making an attack". I exposed some famous hacked sites analyzing techniques. http://seco.di.uniroma1.it/
- **2003** - Speaker - **"la Sapienza" University of Rome** "SecurITy@uniROMA1" Speaker: Andrea Bodei "Defacement, analysis of the most common digital crime". Demo: Attack skills presentation and examples. http://twiki.dsi.uniroma1.it/pub/Remus/WebHome/
- **2002** - Editorial Staff of ZoneH.org. Study and post of Advisories, News and Exploits. Cataloging and management of computer related crimes.
- **2001** - News, Advisories, exploits and contributes on Nessus, Packetstormsecurity.org, Securityfocus.com, Milw0rm.org, Exploit-DB (search=spax, search=spabam): Exploits of File Inclusion, XSS, Buffer Overflow.

# ANDREA GIAIME BODEI

EU Italian Citizen

info@andreabodei.com

## EDUCATION AND LANGUAGES

- La Sapienza University of Rome - Computer Sciences - Cert/Exam "cum laude"
- La Sapienza University of Rome - Criminology - Cert/Exam
- State University of New York - Cyber Warfare - Cert/Exam
- University of Adalaide - Cyber War, Surveillance and Security - Cert/Exam
- La Sapienza University of Rome - Multimedia publishing - Cert/Exam
- La Sapienza University of Rome - Public Law - Cert/Exam
- La Sapienza University of Rome - Social Psychology - Cert/Exam "cum laude"
- La Sapienza University of Rome - Sociology - Cert/Exam
- La Sapienza University of Rome - Theories and techniques of mass communication - Cert/Exam
- Digital forensic Cert - ICAA
- Computer Security Cert - ICAA
- Network Security Cert BB
- Information Technology Security Fundamentals Cert BB
- Unix Administration (general) Master BB
- Linux Administration (general) Cert BB
- CS-332 - Windows Server - NCSA
- Computer Technical Support Cert BB  CH-111 - Computer Hardware Technician - NCSA
- CH-101 - PC Basics – NCSA Information Technology Terminology Master BB
- Bash, Python programming
- La Sapienza University of Rome - English - Cert/Exam
- English C2.  Spanish C2. Italian C2.
- Member of Mensa Italia 3901

## SOFTWARE

- **Network Penetration Test**: **INFRA** Scan, Core Impact, Immunity Canvas, Metasploit,  BackTrack/Kali
- **Network VA**: Nessus/OpenVas, eEye Retina/SafetyLabs SSS, Nmap, Amap, GFI Languard, Nexpose
- **Web App/ServicesVA**: HP WebInspect, IBM Appscan, Acunetix WVS, Burp Suite, OWASP ZAP, w3af
- **URL Manipulation**: Burp Proxy/Suite, Vega, OWASP ZAP, Paros, Priamos, Spike, Acunetix WVS, w3af
- **DataBase Security**: AppSecurity AppDetectivePro, SafetyLabs DBS, Inguma, SQLninja, SQLmap, Havj
- **WiFi test**: Wifite/Aircrack-ng, airtools, Kismet, NetStumbler, WirelessTools, BackTrack/Kali, Core Impact
- **Password guessing**: THC Hydra, Brutus, HP/SPI WebBrute, IBM Authentication Tester, Wfuzz, nmap
- **Network Analysis**: Ethereal/Whireshark, Tcpdump, Ettercap, Dsniff, Cain & Abel, Nagios, Snort IDS
- **Computer Forensic**: EnCase, TCT/S!euthKit/Autopsy, AccessData FTK, dd/dcfldd/dc3dd, air-imager
- **Password cracking**: John the Ripper, LophCrack (LC5), Crack, Cain, Passware
- **RevEng/Debug/Code Review**: OllyDBG, HexEditor, Parasoft .TEST, HP/Fortify RATS/SCA, Flawfinder
- **Custom Virus**: Keylogging, screenshot, autoupdate, DNS redirect, Skype, antivirus/firewall, encryption
- **System administration**: MS Windows, Linux, BSD, Apache, MySQL, Postfix, PureFTPd, SSHd, Netfilter
- **WebApp admin**: Joomla/Virtuemart, Prestashop, MediaWiki, Roundcube, PhpFox, PHPmyadmin, EXO
- **Virtualization**: VMWare, QEMU, Sun/Oracle VirtualBox, MS VirtualPC, wine, crossover, cygwin
- **Encryption**: FreeOTFE/Truecrypt/BitLocker/LUKS-dm-crypt/ecryptfs, OpenVPN/PPTP/L2TP, GPG/PGP