PERSONAL DATA

First and Last Name: Victor Ruben Lacort Pellicer
Birthday: 9th - January - 1980, in Valencia (Spain)
Address: C/Escultor Jose Capuz, nº16 puerta 25 – 46006 Valencia (Spain)
Driving License: Tourism cars
Website: *http://mural.uv.es/vicrula*
E-Mail: Victor.Lacort@gmail.com
Phone: (+34) 636 80 47 81

ACADEMIC FORMATION

- 2002 - 2010: BSc & MSc in **Computer Engineering** - University of Valencia (ETSE-UV) - Spain.
- 2007 - 2010: BSc in **Communications Engineering** - University of Valencia (ETSE-UV) - Spain.

PROFESSIONAL CERTIFICATES

- Jan 2017: **ISO 27001:2013** Information Security Management Systems Internal Auditor - Bureau Veritas.

FURTHER TRAINING

- 2020: Master Automation with **Ansible and Puppet** – Udemy.
- 2020: Complete **Artificial Intelligence** Course with Python – Udemy.
- 2017: Pentesting with Kali **PWK** training Course for OSCP Examination – Offensive Security.
- 2016: Certified Information Systems Auditor **CISA** Course for Certificate Examination – ISACA.
- 2016: Cybersecurity Fundamentals **CSX** Course for Certificate Examination – ISACA.
- 2015: **Court IT Expert Opinion** Course – COIICV - Spain.
- 2014: **Avanced C++11/14** Course – Instituto de Fisica Corpuscular (IFIC-CSIC/UV) - Spain.
- 2012: **Cloud Computing** Course – Polytechnic University of Valencia (GRyCAP-UPV) - Spain.
- 2010: Diploma on University Professional Specialization in IBM Big Corporative Systems **(IBM System Z)**, 4th Edition – Postgraduate at University of Valencia (ADEIT-UV) – Spain.

PROFESSIONAL EXPERIENCE

- May 2022 – Nowadays: CEO, CISO, CTO (**Codevania S.L.U.**)
  - o IT Consultancy company, in parnership with TCS Spain for a client on the top of european pharmaceutical sector.
  - o Main activities: Linux systems administration and engineering, Infrastructure automation.
  - o Ansible, Jenkins, Jboss, Apache+WebDAV.

- Nov 2020 – Apr 2022: Cybersecurity Analist at CSIRT-CV (**S2Grupo – Generalitat Valenciana**)
  - o Blue Team (CND - Incident Analysis and Handling), Data automation (Python requests).
  - o IPS, NGFW (Paloalto), NIDS (Suricata), HIDS (OSSEC, Wazuh), ePO (McAffe), Ironport.
  - o High-interaction Honeypot (Cowrie, Inetsim, OpenFPC, smtpot, bind9 sinkhole), Graylog.

- Sep 2019 – Nov 2020: Fullstack developer and System/Security DevOps (**BETWEEN – ETRA I+D**)
  - o Technical consultant for Energy projects from European Commission (FLEXGRID, etc).
  - o Proxies for HTTPS and Backend Authentication (Traefik, Openresty(Nginx+Lua)).
  - o WebApps development (Meteor framework, Python microservices, Docker+Portainer).
  - o Ansible, MongoDB, Elasticsearch, Grafana, Flask/Django apps (Python), Jenkins builds.

- Nov 2018 – May 2019: Security Technician (**Instituto de Tecnología Informática ITI – IVACE/UPV**)
  - o Design and Development of ISO 27001:2013 Information Security Management System.

- May 2017 – May 2018: OpenStack Cloud Services installation and deployment:
  - o Member of R&D department at **Walhalla DataCenterServices** as SysAdmin, working on correct installation, configuration and parametization of new services for systems on TEST, DEV, PRE and PRO, in a DevOps role supporting developers' team (REST API).
  - o Mirantis: Fuel, Pacemaker, Ceph, RadosGw, Nova, Cinder, Neutron, Designate, Barbican.
  - o System Administration of TEST (VMware), DEV and PRE domains (CentOS, Ubuntu).
  - o Jenkins Pipeline installation, Python scripts for sys admin and Openstack env deploys.
- Nov 2011 – Dec 2015: GRID Computing Systems and Security Administration in High Energy Physics project, contracted by CSIC: ATLAS Spanish Tier-2 for CERN's Large Hadron Collider (LHC) Computing Grid (**Instituto de Física Corpuscular IFIC – CSIC/UV**). PRO with 500+ servers.
  - o Installation, operation, monitoring and maintenance of servers and services (Hardware, Linux RedHat, Kernel patching, PXE, DHCP, Puppet, RAIDs, Lustre, Apache, Tomcat, Cacti, Nagios, Ganglia, KVM, Middleware GRID, LDAP, Torque, Maui, Bastille, Nmap, OpenVAS, OpenSSH, PKI, Netfilter, TCP/IP, Subnets, perfSONAR, MySQL, and more).
  - o Sys Hardening, Firewalls, HIDS/NIDS, Vuln scan, Net Segmentation, Fail2Ban, SIEM, IPS
- 2011: Internships in Robotics Institute (**IRTIC – University of Valencia**), making reverse engineering over video stream from a DVR device, through IP networks.
  - o Usage of hexedit, Android SDK, Wireshark and ad-hoc tools.
  - o Analysis of binary streams and files for learning data structure.
- 2010: Final Year Project "Academic Linux Kernel Module Rootkit" at the **University of Portsmouth** (United Kingdom) - http://mural.uv.es/vicrula/Proyecto.pdf
  - o Software Development, System and Kernel Programming (Linux) technologies.
  - o Development of Linux Password Cracking tool (dictionary and brute force).
- 2005 – 2010: Freelance Applications Developer for enterprises (Win32/MFC, Java, web services) - http://www.santybus.com (HTML+CSS+PHP)
  - o Software Development, Operating Systems and Programming Languages technologies.
- Sep 2002 – Jun 2007: Systems Technician at "**Ramón y Cajal**" public school, Xirivella (Valencia).
  - o Microcomputing repair, installation of Windows systems and LAN/WLAN networks.
- Jun 2004 – Jul 2005: Translation technical reviser to spanish (Magazines): Hakin9 (cibersecurity), Linux+DVD (open source software), PHP Solutions (web programming), and Software Developers Journal (monographics). **Software.com.pl** publishing (Poland).

PROFESSIONAL PROFILE

- ***IT Systems Engineer:*** Used to work in datacenters, performing installation, operation, administration, monitoring, maintenance tasks of operating systems, applications, middleware, databases and data networks in different coupling levels, from individual servers and clusters to grid and cloud infrastructures. Efficient and secure architectures design, according to Defense In Depth concept (network segmentation, hardening, etc). Experienced on DevOps roles.

- ***IT Security Engineer:*** Transversal knowledge about IT security needs (Cybersecurity). Conducting penetration tests (public reconnaisance, infrastructure mapping, vulnerability scanning, resource enumeration, exploiting, password attacks, privilege escalation, pivoting, passive methods), vulnerability asessment, intruder detection, incident handling and forensic data recovery.

- ***Software Engineer:*** Wide knowledge about different programming paradigms, specialized on system programming (libraries, utilities, OS kernel, LKM), real time environments (hard & soft) and applications (scripts, multithreaded programs). Experienced on web programming. Software design and implementation through Unified Modeling Languaje (UML) and CASE tools.

TECHNOLOGIES AREA

Systems Engineering and Administration:
- Linux Administration (RedHat, Debian), Unix (SysV, BSD), Windows (NT, XP), Syslog-ng
- Scripting, Docker, Cgroups, LVM, GRUB, Linux Kernel patching/compiling, System hardening
- Ansible, Puppet, Tripwire, Nagios, Ganglia, Cacti, PXE boot, Init (Systemd, Upstart)
- PAM, Hashing (MD5, SHA), Cryptography (symmetric/asymmetric encryption), x.509 PKI/PMI
- Lustre, Ceph, SMB, NFS, SMTP, DNS, LDAP, DHCP, NTP, FTP, SSH, HTTP, Tomcat, tcpd, xinetd
- Pacemaker, PBS, Torque, Maui, RAID (software/hardware), Virtualization (KVM, VMware, Xen)
- Middleware GRID: Computing Element (CE), Worker Nodes (WN), Storage Element (SE), Storage Resource Manager (SRM, GridFTP, GridHTTP), Job Accounting (APEL), Information System (BDII).
- Cloud: OpenStack (HAproxy, CRM, REST APIs), Amazon Web Services (EC2, S3, EBS, ELB, RDS)

Cybersecurity:
- Methodologies: OSSTMM.v3, OWASP.v4, ENISA ETL, NIST Framework
- ISO 27000, InDepth Defense, Incident Handling, Intrusion Detection, Vulnerability Asessment
- Defense: Bastille, Stunnel, Tripwire, Samhain, Snort, OSSEC, Honeyd, SIEM (OSSIM)
- Firewalls: Netfilter (Arp/Eb/Iptables+conntrack), Cisco PIX/ASA, BSD pf
- Pentesting: Scoping, Engagement Rules, Permission Memo, Public Data Recon, Reporting
- Reconnaisance: whois, Dig, BiLE, GHDB
- Scanning: Nmap, Hping, Scapy, LFT, THC-Amap/Vmap, Netcat
- Sniffing: Tcpdump, Wireshark, Ettercap, THC-ipv6
- Wireless: Kismet, Aircrack-ng, THC-Wardrive
- Exploiting: Nessus, OpenVAS, Armitage, Metasploit, shellnoob
- Web: w3af, Nikto, Paros Proxy, BeEF, Burp Suite
- PW attacks: John the Ripper, THC-Hydra, Medusa, fgdump, Cain&Abel, Ophcrack
- Forensics: The Sleuth Kit + Autopsy, Rkhunter, Chkrootkit, ddrescue, ngrep, strace, strings

Networking:
- Network Design and Administration (VLANs, 802.3, 802.11), Internetworking, IPv6, SNMP, MTRG
- Router Management (Cisco IOS), Routing (RIP, IGRP, EIGRP, OSPF, IS-IS, BGP), 6to4
- Firewalls (stateful/less), IPS/IDS (Host/Net/WiFi), DMZ Topologies (Bastion Host, 2/3-Tier)
- ACLs, KDCs (Kerberos), SSL/TSL, SSTP, IPSec, VPNs, GRE Tunneling, honey[pots/nets]
- Proxies (SOCKS, Squid, Openresty(Nginx+Lua), Traefik), SSH Tunneling, Multicast, Multimedia

Operating Systems:
- Real Time Systems (QNX RTOS) and Real Time application development (hard/soft)
- Ncurses, Sockets, System & Loadable Kernel Modules (LKMs) Programming, SELinux, Apparmor
- IBM z/OS (Mainframes) – TSO, ISPF, OMVS, RACF, JES2, SDSF

Programming Languages:
- Object Oriented: C++98/11/14, Java, C#
- Imperatives: C, Fortran, Pascal, Matlab
- Declaratives: SQL, LISP, Prolog
- Scripting: Bash, Python, Ruby, Perl, Lua
- Assembler (8086, DLX, DLXV), VHDL
- IBM System Z (Mainframe): JCL, CLIST, REXX, COBOL + CICS + DB2

Software Development:
- UML, METRICA3, Pre/Post Specification, Asserts, Architectures (MVC, Document/View)
- DevOps: GitHub, Maven, Jenkins, Docker Swarm, Kubernetes
- Web Frameworks (Django, Flask), SW Repositories (CVS, SVN, Mercurial, GiT)
- Web Applications: HTML + CSS, PHP, JSP + Java Servlets + JavaBeans, Python, Meteor (Node.js)
- Messaging Protocols (REST, STOMP), SOA (RPC, CORBA, SOAP, Java RMI)
- Libraries (dynamic/static), Parallel Algorithms (MPI, Threads), POSIX (Cygwin)
- Android SDK / NDK, QML (Qt + Javascript), XML, JSON
- Artificial Intelligence (Heuristic, Neural Networks, Fuzzy Logic, Expert Systems)
- Machine Learning (Tensorflow), Deep Learning (Keras)
- Language Processors (Grammars and Parsing: Flex, Bison)

Databases:
- PL/SQL, SQLite, ODBC, JDBC, Pro C
- Design of Relational and Object-Relational Dbs, NoSQL Databases
- DBs Administration: Oracle 10g, MySQL, PostgreSQL, MariaDB, InfluxDB, MongoDB

Other:
- Dec 2013: Fist Aid Course – FREMAP Prevention Society
- Equipment assembly and repair (PCs, Blades, DiskServers, Thumpers, Networking)
- Industrial automation (relay diagrams, GRAFCET)
- Office automation: MS Office, LibreOffice, LaTeX, AsciiDoc

LANGUAGES

- English: Fluent
- Spanish: Native
- Catalan: Native

PERSONAL DESCRIPTION

I am an analytical, methodical, solving and disciplined person, occupationally diligent and quick learner. I consider myself specially oriented to technical tasks, familiar with DevOps culture, with good communication skills and used to teamwork.