Yan Marques de Cerqueira

Email : sec-authority@protonmail.com
Personal GitHub: https://github.com/yanmarques
College GitHub: https://github.com/marquesYan
Work GitHub: https://github.com/sec0uth

Educação

- **Southern Santa Catarina University** — Tubarão, SC
  Graduation in Computer Science — *Jan. 2017 – 2022*

Línguas

- Native Portuguese.
- Advanced English.
- Basic Spanish.

Interested in

- Security by isolation through virtualized systems.
- Open source projects and systems architecture.
- Automation of processes in software projects.
- Binary reverse engineering.
- *Exploits* and *rootkits* development.
- Qubes OS project due to security and personal use perspectives.
- *Assume breach* security model, implemented in Qubes OS.

Experience

- **Tecimob** — Tubarão, SC
  Software developer — *Jul. 2017 - Mar. 2019*
  - Identification and resolution of issues in PHP softwares.
  - Leading developer in a new API using Laravel and Postgresql.
  - Automation of project deployment in the production environment.
  - **Laravel**: Open source framework based on Symfony framework, for web application development following the Model-View-Controller architecture.
  - **React**: Open source library for development of user interfaces in websites.
  - **Postgresql**: Open source relational database management system.
  - **Nginx**: Web server that can act as a reverse proxy for websites and e-mail, load balancer and HTTP cache.
  - **AWS**: Virtualized computation service provided by Amazon.
  - **CI/CD**: Continuous integration and continuous delivery aims to provide automation in the steps for developing applications, such as building, test and deploy.
- **Service Provision** — Tubarão, SC
  Web Pentest — *2020*
  - Execution model based on *The Penetration Testing Execution Standard*.
  - Threat modeling taking into consideration the organization needs.
  - Identification of flaws reported in a document with the score calculated using the *Common Vulnerability Scoring System Calculator* from NIST.
  - The instructions and best practices for fixing the vulnerabilities were placed in an organized fashion inside a private GitHub repository.

- **DevOps - Network Automation** Remote
  Service Provision *Jan. 2022*
  - Adding support for new type of devices on existing features.
  - Using containers for facilitate deployments.
  - Work and improve every stage of the software development cycle.

Projects

- **Badcat**: (link) It is a tool intended to be used by Red Team engagements, in order to mimic APT (Advanced Persistent Threat) attacks. It hides the C2 (Command and Control) server by using Tor's Onion Services.
- **Studies about x86 architecture**: (link) Study and experiment area about one of the most used family of computer instructions set, Intel's x86 architecture.
- **Proxmox Template VMs**: (link) This tool brings the Template virtual machine concept from Qubes OS into Proxmox.
- **Qbackup**: (link) Reasonably secure automation of virtual machines backups for the QubesOS project.
- **Cibern3tico**: (link) A game about cyber attacks using Unity framework, in order to penetrate the virtual environment looking for a flag.
- **Tor-demo**: (link) Scripts to create a remote infrastructure of virtual machines aiming to simulate how the anonymous Tor network works.
- **Task automation in Cisco and Juniper routers**: (link) As part of a job interview, I developed a solution that automates the modification of certain configurations in remote routers.
- **The smallest route between two points for trucks**: (link) I together with college coleagues, we developed a solution using the original Dijkstra algorithm that finds ideal route for truck drivers taking into account route's trafficability, condition and stopping points.

Programming skills

- **Languages**: Python, Assembly x86_64, Javascript, PHP, Shell script, C, C#, Rust, Java, PowerShell, Dart, SQL
- **Technology**: Ansible, SaltStack, Git, Docker, Django, Flask, AWS e Azure Cloud Provider, PM2, Systemd, ELK, Laravel, React, Linux Kernel Module, Postgresql, Oracle Database, Mongodb, Unity Engine

Cyber security skills

- **Tools**: Wireshark, Aircrack, Responder, impacket framework, Nmap, Burp Suite, Gobuster, Wfuzz, Metasploit framework, Seclists, PEASS, Patator, Hydra, Sqlmap, Hashcat, John The Ripper, Maltego, GDB, EDB-Debugger, Ghidra, WinDBG
- **Virtualization**: QEMU, Xen
- **Modules**: Iptables, OpenBSD PF Firewall, AppArmor, Open-SSH server, Unbound, Dnsmasq, GnuPG, Xorg
- **Operating System**: Qubes OS, Fedora, Debian, Kali Linux, OpenBSD, Arch Linux, Cisco and Juniper Routers, Android
- **Cryptography**: RSA (link to proof of concept in Cibern3tico project), SHA3, AES, ED25519