Yan Marques de Cerqueira

Email : sec-authority@protonmail.com
GitHub Pessoal: https://github.com/yanmarques
GitHub Faculdade: https://github.com/marquesYan
GitHub Trabalho: https://github.com/sec0uth

Educação

- **Universidade do Sul de Santa Catarina** — Tubarão, SC
  Graduação em Ciência da Computação — *Jan. 2017 – 2022*

Línguas

- Português nativo.
- Inglês avançado.
- Espanhol básico.

Interesses

- Segurança por isolamento, através de virtualização.
- Arquitetura de sistemas e projetos de código aberto.
- Primitivas criptográficas contra o abuso de informações.
- Engenharia reversa de binários.
- Desenvolvimento de *exploits* e *rootkits*.
- Projeto Qubes OS pelas perspectivas de segurança e uso pessoal.
- Modelo de segurança *assume breach*, implementado no Qubes OS.

Experiência

- **Tecimob** — Tubarão, SC
  Desenvolvedor de Aplicações — *Jul. 2017 - Mar. 2019*
  - Identificação e resolução de problemas em PHP.
  - Desenvolvedor chefe de uma nova API em Laravel e Postgresql.
  - Automatização na atualização de código em ambiente de produção.
  - **Laravel**: Framework de código aberto baseada na framework Symfony, criada para o desenvolvimento de aplicações web seguindo a arquitetura Model-View-Controller.
  - **React**: Biblioteca de código aberto para criação de interfaces de usuário em páginas web.
  - **Postgresql**: Sistema de gerenciamento de banco de dados relacional de código aberto.
  - **Nginx**: Servidor web comumente utilizado como *proxy* reverso para web e e-mail, balanceador de carga e *cache* HTTP.
  - **AWS**: Serviço provido pela Amazon para computação virtualizada.
  - **CI/CD**: Integração contínua e entrega contínua buscam proporcionar automatização nas etapas de desenvolvimento de aplicações como na compilação, teste e entrega.
- **Prestação de serviço** — Tubarão, SC
  Pentest Web — *2020*
  - Modelo de execução baseado no *The Penetration Testing Execution Standard*.
  - Elaboração do *threat model* levando em consideração as necessidades da organização.
  - Identificação das falhas em um relatório com pontuação calculada usando o *Common Vulnerability Scoring System Calculator* da NIST.
  - Instruções e melhores práticas para correção das vulnerabilidades dispostas de forma organizada em *Issues* em um repositório privado no Github.

Projetos

- **Badcat**: (link) É uma ferramenta criada para engajamentos de *Read Teams*, com intuito de simular ataques APT (Advanced Persistent Threat). A ferramenta gera *backdoors* que mascaram o servidor C2 (Command and Control) através do uso de Tor Onion Services.
- **Estudos acerca da arquitetura x86**: (link) Área de estudos e experimentos sobre uma das mais utilizadas famílias do conjunto de intruções existentes, a arquitetura x86 da Intel.
- **Proxmox Template VMs**: (link) Traz o conceito de máquina virtual Template do projeto Qubes OS para o Proxmox.
- **Cibern3tico**: (link) Um jogo sobre ataques cibernéticos usando a ferramenta Unity, com o objetivo de invadir o ambiente virtual atrás de uma *flag*.
- **Automatização de tarefas em roteadores Cisco e Juniper**: (link) Como parte de uma entrevista de emprego, criei uma solução em Python e Ansible que possibilita a automatização de alterações na configuração de roteadores remotos.
- **Menor rota entre dois pontos para caminhões**: (link) Juntamente com colegas de faculdade, desenvolvemos uma solução utilizando o algoritmo Dijkstra original que encontra a rota ideal para caminheiros levando em consideração a sua trafegabilidade, condição e se possue pontos de parada.

Habilidades em programação

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

Habilidades em cibersegurança

- **Ferramentas**: 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
- **Virtualização**: QEMU, Xen
- **Módulos**: Iptables, OpenBSD PF Firewall, AppArmor, Open-SSH server, Unbound, Dnsmasq, GnuPG, Xorg
- **Sistemas Operacionais**: Qubes OS, Fedora, Debian, Kali Linux, OpenBSD, Arch Linux, Cisco IOS, Android
- **Criptografia**: RSA (prova de conceito no projeto Cibern3tico), SHA3, AES, ED25519