Igor Henrique Sousa de Andrade
Security Analyst

Rua Tertuliano de Castro, N° 1287, Bessa, João Pessoa – PB Solteiro, 32 anos
Telefone: (83) 999650-2851 / E-mail: igor@igorlnx.com
Linkedin: https://www.linkedin.com/in/igor-andrade-244221160/
Github https://github.com/igorhrq
Gist GitHub: https://gist.github.com/igorhrq
Site: https://igorlnx.com (Apenas em inglês)
Mantenedor do blog: https://debian-pb.org (Grupo de Usuários Debian da Paraíba)

CERTIFICAÇÕES

LPIC-1 – https://cs.lpi.org/caf/Xamman/certification/verify/LPI000391345/2m2anumjvr
Comptia Linux+ – Visualizar aqui
Plesk Onyx Professional – https://igorlnx.com/plesk-igorandrade.pdf
NSE 1 Network Security Associate (FORTINET) - https://igorlnx.com/NSE_1_Certificate.pdf
NSE 2 Network Security Associate (FORTINET) – https://igorlnx.com/NSE_2_Certificate.pdf
DevOps Essentials Professional by Certiprof - Download PDF
Scrum Foundation Professional by Certiprof - Download PDF
Imunify360 by cPanel University - Download Certificate
cPanel Professional Certification (CPP) – http://igorlnx.com/CWAandCPP.png
cPanel & WHM Administrator Certification (CWA) – http://igorlnx.com/CWAandCPP.png
KanBan Foundation Certificate (KIKF) ™ – http://igorlnx.com/kanban.pdf

FORMAÇÃO ACADÊMICA

Pós-Graduação em Segurança da informação - Unipê

Pós-Graduação em segurança da informação: 2016 - 2017 (Incompleto)

Redes de Computadores – Estácio

Curso superior em Redes de Computadores na Estácio de Sá da Paraíba: 2013 – 2016 (Completo)

ÁREAS DE INTERESSE

- Segurança da informação
  - Obfuscation
  - Análise de Vulnerabilidade
  - OS Hardening, Solutions Hardening
  - Auditing
- DevOps
  - Aplicação de patchs em massa e Configurações em massa e persistência
  - IaC
- Linux Administration
  - Shell Scripting
  - Python

EXPERIÊNCIA PROFISSIONAL

- *Janeiro 2019 – Atualmente* **HostDime Brasil**

  Site: https://hostdime.com.br

  Cargo: Analista de Segurança Júnior

  - Auditoria Avançada em contas cPanel/Plesk ou s/ painel, Identificação e Mitigação de abusos (Comprometimento de complexidade Alta geralmente ocorrido via aplicação (outdated) e de contas de e-mails na máquina remota ou script, identificação e mitigação de ataques brute-force, criação de regras mod-security se necessário ou ajustes a nível de firewall iptables/csf)
  - Auditoria de Tráfego Outbound/Inbound com nload/iptraf/netstat/lsof/cacti/zabbix ou Network Monitor (Windows) para ver spikes e uso de tráfego excessivo
  - Interação direta com o cliente através dos canais de atendimento (Ticket);

- Filtrar e resolver os problemas a partir de sua complexidade;
- Suporte Avançado em Soluções Personalizadas (Zimbra Mail, xcp-ng/xen, Docker, pfsense, lemp/lamp, open-vpn e fortigate)
- Migrações de alta complexidade (cPanel, E-mails, s/ painel, etc)
- Desenvolvimento de Scripts Shell/Bash para automatizar tarefas complexas e atacar demandas pertinentes: meu gist.github.com
- Aplicar Patchs de atualização em massa com Ansible/WinRM ou via WSUS(Windows)
- Estudo de novas soluções para trazer melhorias e atacar certas demandas que eventualmente possa escoar um problema frequente
- Planejamento de Capacidade em Ambientes Linux ou Windows para ofertar upgrades para clientes que possuam gargalos com o hardware/recurso atual.
- Criação de Políticas via Confluence(Knowledge Base) focadas na segurança de todos os ambientes/setores/soluções da Empresa tanto de clientes como soluções internas, enumerando todas as eventuais brechas/gaps e correção das mesmas conscientizando todos os colaboradores.
- Análise de Vulnerabilidades em sistemas internos com (Nessus, Qualys, nikto, arachni e nmap)
- Monitoramento com Zabbix para identificar vários comportamentos e se antecipar a problemas com os clientes (partição cheia, fila de e-mails alta, versões de softwares desatualizados e etc)

- *Março 2018 – Dezembro 2018* **HostDime Brasil**

  Site: https://hostdime.com.br

  Cargo: SysOps

  - Administração Avançada de ambientes Linux e Windows c/ ou s/ Painel Plesk/cPanel/CWP/LEMP/LAMP e seus respectivos serviços
  - Interação direta com o cliente através dos canais de atendimento (Ticket);
  - Filtrar e resolver os problemas a partir de sua complexidade;
  - Auditoria Avançada em contas cPanel/Plesk ou s/ painel, Identificação e Mitigação de abusos (Comprometimento de complexidade Alta geralmente ocorrido via aplicação (outdated) e de contas de e-mails na máquina remota ou script, identificação e mitigação de ataques brute-force, criação de regras mod-security se necessário ou ajustes a nível de firewall iptables/csf)
  - Auditoria de Tráfego Outbound/Inbound com nload/iptraf/netstat/lsof/cacti/zabbix ou Network Monitor (Windows) para ver spikes e uso de tráfego excessivo
  - Suporte Avançado em Soluções Personalizadas (Zimbra Mail, xcp-ng/xen, Docker, pfsense, lemp/lamp, open-vpn e fortigate)
  - Migrações de alta complexidade (cPanel, E-mails, s/ painel, etc)
  - Desenvolvimento de Scripts Shell/Bash para automatizar tarefas complexas e atacar demandas pertinentes: meu gist.github.com
  - Aplicar Patchs de atualização em massa com Ansible/WinRM ou via WSUS(Windows)
  - Estudo de novas soluções para trazer melhorias e atacar certas demandas que eventualmente possa escoar um problema frequente

- Planejamento de Capacidade em Ambientes Linux ou Windows para ofertar upgrades para clientes que possuam gargalos com o hardware/recurso atual.

Janeiro de 2016 – Janeiro 2018 **HostDime Brasil**

Site: https://www.hostdime.com.br

Cargo: Analista de Suporte Level II e III

- Administração Avançada de ambientes Linux e Windows c/ ou s/ Painel Plesk/cPanel/CWP/LEMP/LAMP e seus respectivos serviços
- Interação direta com o cliente através dos canais de atendimento (Ticket);
- Filtrar e resolver os problemas a partir de sua complexidade;
- Auditoria Intermediária em contas cPanel/Plesk ou s/ painel Identificação e Mitigação de abusos (Comprometimento de complexidade média geralmente ocorrido via aplicação (outdated) e de contas de e-mails na máquina remota ou script)
- Suporte em Soluções Personalizadas (Zimbra Mail, xcp-ng/xen, pfsense, lemp/lamp, open-vpn e fortigate)
- Desenvolvimento de Scripts Shell/Bash para automatizar tarefas e atacar demandas pertinentes: meu gist.github.com

- *Abril 2015 – Janeiro 2016* **HostDime Brasil**

Site: https://www.hostdime.com.br

Cargo: Analista de Suporte Level I

- Administração Intermediária de ambientes Linux e Windows c/ ou s/ Painel Plesk/cPanel/CWP/LEMP/LAMP e seus respectivos serviços
- Interação direta com o cliente através dos canais de atendimento (Telefone, Chat e Ticket);
- Filtrar e resolver os problemas a partir de sua complexidade;
- Elaboração de artigos e tutoriais internos e públicos para auxiliar os clientes. (ajuda.hostdime.com.br)
- Auditoria Básica em contas cPanel (Identificação e mitigação de SPAM de comprometimentos de baixa complexidade)

- *Janeiro 2015 – Abril 2015* **HostDime Brasil**

Site: https://www.hostdime.com.br

Cargo: Estagiário de Suporte

- Administração básica de ambientes Linux e Windows c/ ou s/ Painel Plesk/cPanel/CWP e seus respectivos serviços
- Interação direta com o cliente através dos canais de atendimento (Telefone, Chat e Ticket);
- Filtrar e resolver os problemas a partir de sua complexidade;
- Elaboração de artigos e tutoriais internos e públicos para auxiliar os clientes. (ajuda.hostdime.com.br)

HABILIDADES

- Linux Administration & Hardening;
- cPanel, Plesk, CWP, Imunify360, MagicSPAM, ClamAV, cpnginx, engintron, litespeed
- Apache, nginx, exim, postfix, varnish cache, imapsync
- KVM, xcp-ng e OVZ
- Docker + Swarm/Kubernetes;
- Bash/Shell Script/Regex;
- Zimbra Mail;
- wpscan, nmap, sqlmap, metasploit, clamav + yara rules, modsecurity, arachni, nessus, qualys, deepsecurity, owasp
- AWS ec2/s3
- iptables, csf, pfsense, endian(iptables), fortigate;
- git;
- Ferramentas Atlassian(JIRA e Confluence);
- MySQL, MariaDB e PostgreSQL;

IDIOMAS

- Inglês Fluente
- Espanhol Intermediário

CURSOS COMPLEMENTARES

- Pen Test: Técnicas de Intrusão em Redes Corporativas - Certificado
- Python para Iniciantes - Certificado
- Ferramentas de Automação DevOps Ansible, Chef e Puppet - Certificado
- Docker – Introdução a administração de Containers - Certificado