Igor Henrique Sousa de Andrade
SysAdmin & Security Analyst

Street: Tertuliano de Castro, Nº 1287
Neighborhood:Bessa
City: João Pessoa
State: Paraiba
Country: Brasil
Not Married, 33 Years old
Celphone: +55 (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 (Only English)
Maintainer of blog: https://debian-pb.org (Users of Debian from Paraíba)

CERTIFICATIONS

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
Cyber Security Foundation – CSFPC - https://igorlnx.com/certs/CSFPC.pdf
GitLab Certified Associate – Link to certificate

FORMATION

Graduate Course on Security Information - Unipê

Graduate Course Incomplete InfoSec- From: 2016 – To: 2017 (Incomplete)

Gratuation Computer Network – University Estácio de Sá

Graduation on Computer Network at Estácio de Sá – Paraíba | Brasil : From : 2013 – To: 2016 (Completed)

AREAS OF INTEREST

- Infosec
  - Obfuscation
  - Vulnerability Analysis
  - OS Hardening, Solutions Hardening
  - Auditing
- DevOps
  - mass patch, mass configuration and persistence
  - IaC

- Linux Administration
    - Shell Scripting
    - Python

Professional

- *November 2020 – Actually* **Endurance Group / NewFold Digital**

Site: https://newfold.com/

Role: SysOps

- Maintain core environment of HostGator LatAm(Company of the NewFold group) Updated, secure and stable;
- Administer current monitoring for better effectiveness as well as improvements in it;
- Identify any incident that is related to payments as well as correction, otherwise trigger responsible sectors, if the correction is not at the system level;
- Python and Shell scripting for core environment improvements;
- Creation of dashboards in grafana + zabbix to monitor the resources of the color machines and also the entire payment system used in the company
- Ensure up-to-date backups for if necessary used;
- Study of new solutions, design and improvement of current solutions when necessary, then implement for production;
- Filter and solve problems based on their complexity;
- Apply system-level update patches
- Core email server maintenance (Ensure delivery, reputation etc)
- Mass execution via ansible for configuration or patching/update

- *January 2019 – November 2020* **HostDime Brasil**

Site: https://hostdime.com.br

Role: Junior Security Analyst

- Advanced Audit on cPanel/Plesk accounts or without panel, Identification and Mitigation of abuse (High complexity compromise usually occurred via application (outdated) and email accounts on remote machine or script, identification and mitigation of brute-force attacks, creation modsecurity rules if necessary or firewall level adjustments iptables/csf)
- Outbound/Inbound Traffic Audit with nload/iptraf/netstat/lsof/cacti/zabbix or Network
- Monitor (Windows) to see spikes and excessive traffic usage
- Direct interaction with the customer through service channels (Ticket);
- Filter and solve problems based on their complexity;
- Advanced Support on Custom Solutions (Zimbra Mail, xcp-ng/xen, Docker, pfsense, lemp/lamp, open-vpn and fortigate)
- Highly complex migrations (cPanel, E-mails, w/o panel, etc)
- Development of Shell/Bash Scripts to automate complex tasks and attack pertinent demands: my gist.github.com
- Apply Bulk Update Patches with Ansible/WinRM or via WSUS(Windows)
- Study of new solutions to bring improvements and tackle certain demands that may eventually drain a frequent problem
- Capacity Planning in Linux or Windows Environments to offer upgrades for customers who have bottlenecks with current hardware/resource.
- Creation of Policies via Confluence (Knowledge Base) focused on the security of all environments/sectors/solutions of the Company, both for customers and internal solutions, listing all possible gaps/gaps and correcting them, making all employees aware.
- Vulnerability analysis in internal systems with (Nessus, Qualys, nikto, arachni and nmap)
- Monitoring with Zabbix to identify various behaviors and anticipate problems with customers (full partition, high email queue, outdated software versions, etc.)

- *March 2018 – December 2018* **HostDime Brasil**

Site: https://hostdime.com.br

Role: SysOps

- Advanced Administration of Linux and Windows environments w/ or without Panel Plesk/cPanel/CWP/LEMP/LAMP and its respective services
- Direct interaction with the customer through service channels (Ticket);

- Filter and solve problems based on their complexity;
- Advanced Audit on cPanel/Plesk accounts or without panel, Identification and Mitigation of abuse (High complexity compromise usually occurred via application (outdated) and email accounts on remote machine or script, identification and mitigation of brute-force attacks, creation modsecurity rules if necessary or firewall level adjustments iptables/csf)
- Outbound/Inbound Traffic Audit with nload/iptraf/netstat/lsof/cacti/zabbix or Network
- Monitor (Windows) to see spikes and excessive traffic usage
- Advanced Support on Custom Solutions (Zimbra Mail, xcp-ng/xen, Docker, pfsense, lemp/lamp, open-vpn and fortigate)
- Highly complex migrations (cPanel, E-mails, w/o panel, etc)
- Development of Shell/Bash Scripts to automate complex tasks and attack pertinent demands: my gist.github.com
- Apply Bulk Update Patches with Ansible/WinRM or via WSUS(Windows)
- Study of new solutions to bring improvements and tackle certain demands that may eventually drain a frequent problem
- Capacity Planning in Linux or Windows Environments to offer upgrades for customers who have bottlenecks with current hardware/resource.

January 2016 – January 2018 **HostDime Brasil**

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

Role: Technical Support Analyst Level II e III

- Advanced Administration of Linux and Windows environments w/ or without Panel Plesk/cPanel/CWP/LEMP/LAMP and its respective services
- Direct interaction with the customer through service channels (Ticket);
- Filter and solve problems based on their complexity;
- Intermediate Audit on cPanel/Plesk or non-panel accounts Identification and Mitigation of abuse (Medium complexity compromise usually occurred via application (outdated) and email accounts on the remote machine or script)
- Custom Solutions Support (Zimbra Mail, xcp-ng/xen, pfsense, lemp/lamp, open-vpn and fortigate)
- Shell/Bash/Python Script Development to automate tasks and attack pertinent demands: my gist.github.com

- *April 2015 – January 2016* **HostDime Brasil**

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

Role: Technical Support Level I

- Intermediate Administration of Linux and Windows environments w/ or w/o Panel
- Plesk/cPanel/CWP/LEMP/LAMP and its respective services
- Direct interaction with the customer through service channels (Telephone, Chat and Ticket);
- Filter and solve problems based on their complexity;
- Preparation of articles and internal and public tutorials to help customers. (ajuda.hostdime.com.br)
- Basic Audit on cPanel accounts (Identifying and mitigating SPAM of low complexity compromises)

- *January 2015 – April 2015* **HostDime Brasil**

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

Role: Technical Support Trainee

- Basic administration of Linux and Windows environments w/ or without Plesk/cPanel/CWP Panel and its respective services
- Direct interaction with the customer through service channels (Telephone, Chat and Ticket);
- Filter and solve problems based on their complexity;
- Preparation of articles and internal and public tutorials to help customers. (ajuda.hostdime.com.br)

SKILLS

- 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;
- Python;
- Zimbra Mail;
- wpscan, nmap, sqlmap, metasploit, clamav + yara rules, modsecurity, arachni, nessus, qualys, deepsecurity, owasp;
- AWS ec2/s3/cloudwatch;
- iptables, csf, pfsense, endian(iptables), fortigate;
- git, gitlab and github;
- Ferramentas Atlassian(JIRA, confluence, bitbucket and bamboo);
- MySQL, MariaDB, PostgreSQL, galera cluster and perconadb;
- Zabbix and Grafana;
- Bacula;
- CloudFlare;

IDIOMS

- Fluent English
- Spanish intermediary
- Portuguese (Native)

COMPLEMENTARY COURSES

- Pen Test: Intrusion Technical on Corporate Network - Certificate
- Python for beginners - Certificate
- Tools for DevOps Automation with Ansible, Chef and puppet - Certificate
- Docker – Introduction for Containers Administration - Certificate