# Igor Henrique Sousa de Andrade

**SysOps Senior at HostGator**


Street: Tertuliano de Castro, N° 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+ - https://www.certmetrics.com/comptia/public/verification.aspx?code=W8TJTBGX7Y6PFP97
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 – https://cmkr.co/pdf/downloads/?certificate_id=33703&sid=31013024&nrg_id=546811&test_id=980770&aid=4238890&utype=SD&cert_token=e6dbc42bcd6d7e21b9ac59ae99b29d6b&tprtoken=TDFG
Scrum Foundation Professional by Certiprof – Download PDF
Imunify360 by cPanel University – https://igorlnx.com/certs/
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 – https://badgr.com/public/assertions/XmwjQmezQqO6csk0jnJ_zQ?identity__email=igorhenriquehdbr@gmail.com

# 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

- **Observability**
  - APM's like DataDog, NewRelic
  - Friendly view with Grafana, and alerting with webhooks
  - Zabbix to infrastructure
  - Graylog for logs management (OpenSource option)

- **Infosec**
  - Vulnerability Analysis
  - Obfuscation
  - OS Hardening, Solutions Hardening
  - Auditing
- **DevOps**
  - IaC
  - mass patching, configuration and persistence
- **Linux Administration**
  - Shell Scripting
  - Python

# Professional

- *April 2022 – Actually* **HostGator LatAm / NewFold Digital**

*Site: https://newfold.com/*

**Role: SysOps Senior**

- ***Observability:*** *An observability plan was implemented with Datadog to monitor critical services using Synthetics tests, Browser tests, SSL Tests, and Dashboards. Query analysis was performed using the Datadog DPM tool, and triggers were created to alert the team via channel notifications. CloudWatch integration with Datadog was also set up, and a lambda function was created to collect logs from services and microservices on AWS.*
- ***Observability:*** *Creation of Python scripts to consume APIs or create APIs with Flask to display a JSON with the status of various required services in a Healthcheck format.*
- ***Observability:*** *Integration of Zabbix and Teams with a Python script, where all critical alerts from the core were sent to our room, separated only for the core group.*
- ***Observability:*** *I worked extensively with Grafana, promoting observability culture. I created a dashboard that monitored the entire payment flow of HostGator, from the generation of a simple invoice to a system that monitored customers with high balances. In addition to displaying data in a user-friendly format on Grafana, it also triggered critical alerts.*
- ***Observability:*** *Created several specific Python and Bash scripts for certain types of demands, for specific and low-criticality monitoring or requests from nearby teams.*
- ***Observability:*** *Integration of Zabbix + Grafana to monitor available resources of core machines, creating a dashboard for monitoring.*
- ***Migrações Complexas:*** *Elimination of various points of failure in the Billing LatAm infrastructure by migrating to a completely redundant environment with HAProxy and Galera Cluster, featuring redundancy of 2 nodes for HAProxy/Web service/Postfix, and 3 nodes for the Percona XtraDB Cluster.*
- ***Migrações Complexas:*** *Migration of environments for the Business Intelligence LatAm team, using solutions such as Pentaho, Qlik, Postgres, Hadoop, and others.*
- ***DevOps:*** *Mass execution via Ansible for configuring services, updating certificates, or applying patches/updates (usually security-related) across the 5 nodes of the Billing Brasil and Billing LatAm environment (Colombia, Mexico, and Chile).*
- ***DevOps:*** *Certificate updates for shared hosting environments via Puppet, as well as new configurations.*
- *Maintenance of the core email server (Ensuring delivery, reputation, etc.)*
- *Identify any incident related to payments and make corrections, otherwise contact the responsible departments. If the correction is not at the system level, escalate to the appropriate team.*
- *Study of new solutions, design and improvement of current solutions when necessary, and subsequently implement them in production.*
- Implementation of security solutions with CloudFlare, in addition to integration with Grafana.
- Integration of Azure AD + Grafana, where all Azure AD users were integrated as Grafana oAUTH, reducing security risks and centralizing logins. I also disabled the local login.

- November 2020 – March 2022 **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 anticipa

- 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;

- 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**

- Plesk/cPanel/CWP/LEMP/LAMP and its respective services
- Advanced Administration of Linux and Windows environments w/ or without Panel
- 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

- *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;
- Apache, nginx, exim, postfix, varnish cache, imapsync
- HAProxy (High Availability Cluster with easy scalability)
- KVM, Proxmox, XCP-Ng(Virtualization)
- Docker e OpenVZ; (Container)
- Datadog e Graylog (Observability Stack)
- Zabbix and Grafana (Observability Stack)
- Bash/Shell Script/Regex;
- Python (API Creation w/ Flask + Consume API and scripting)
- Zimbra Mail;
- wpscan, nmap, sqlmap, metasploit, clamav + yara rules, modsecurity, arachni, nessus, qualys, deepsecurity, owasp zap (Infosec Stack)
- iptables, csf, pfsense, endian(iptables), fortigate; (Infosec Stack)
- AWS (ec2/s3/cloudwatch/cloudformation/route53/lambda)
- git, gitlab and github;
- Ferramentas Atlassian(JIRA, confluence, bitbucket and bamboo);
- MySQL, MariaDB, PostgreSQL, PerconaDB
- Galera Cluster (PerconaXtraDB Cluster) ( High Availability MySQL Cluster)
- Bacula (Backup Management with Agent)
- CloudFlare (Security Tools/Observability and integration of Grafana Plugin)
- cPanel, Plesk, CWP, Imunify360, MagicSPAM, ClamAV, cpnginx, engintron, litespeed

## LANGUAGES

- Fluent English
- Spanish Intermediate
- Portuguese (native)

## COMPLEMENTARY COURSES

- Pen Test: Intrusion Technical on Corporate Network - https://igorlnx.com/certs/
- Python for beginners - https://igorlnx.com/certs/
- Tools for DevOps Automation with Ansible, Chef and puppet - https://igorlnx.com/certs/
- Docker – Introduction for Containers Administration – https://igorlnx.com/certs/
- Proxmox (Management of Virtual Machines w/ Proxmox) - https://igorlnx.com/certs/