**Análise de Segurança - Scan de portas abertas - licitasis.com**

**Ativo: licitasis.com**

**Analista: Jonas Pacheco  
Data: 02/07/2025**

**RESUMO EXECUTIVO**

**Classificação de Risco: ALTO**

O scan revelou 28 portas abertas com múltiplas vulnerabilidades críticas, incluindo exposição de serviços administrativos, bancos de dados desprotegidos e configurações inseguras. Ação imediata é necessária para mitigar os riscos identificados.

**VULNERABILIDADES CRÍTICAS IDENTIFICADAS**

**CRÍTICO - Exposição de Bancos de Dados**

**MySQL (Porta 3306) e PostgreSQL (Porta 5432) Expostos**

* **Risco**: Acesso direto aos bancos de dados pela internet
* **Impacto**: Vazamento de dados, manipulação de informações, comprometimento total da aplicação
* **CVE Relacionado**: CWE-200 (Information Exposure)

**CRÍTICO - Painel Administrativo Exposto**

**cPanel/WHM Acessível Externamente (Portas 2078, 2080, 2083, 2087, 2091, 2096)**

* **Risco**: Interface administrativa acessível pela internet
* **Impacto**: Controle total do servidor em caso de comprometimento
* **Detalhes**: Múltiplas interfaces de gerenciamento expostas

**CRÍTICO - SSH em Porta Não Padrão**

**OpenSSH na Porta 1157**

* **Risco**: SSH exposto com porta customizada (possível obfuscação)
* **Impacto**: Acesso root ao sistema via força bruta ou credenciais comprometidas

**VULNERABILIDADES DE ALTO RISCO**

**ALTO - Serviços de Email Múltiplos**

**Portas 25, 110, 143, 465, 587, 993, 995**

* **Risco**: Múltiplos vetores de ataque via email
* **Impacto**: Spam relay, phishing, comprometimento de contas de email

**ALTO - Serviços Não Identificados**

**Portas 2077, 2079, 2082, 2086, 2095, 5960, 10050**

* **Risco**: Serviços com fingerprints desconhecidos
* **Impacto**: Vetores de ataque não documentados

**ALTO - FTP Exposto**

**Pure-FTPd na Porta 21**

* **Risco**: Protocolo inseguro para transferência de arquivos
* **Impacto**: Interceptação de credenciais, vazamento de arquivos

**ANÁLISE DETALHADA DOS SERVIÇOS**

**Servidor Web (Portas 80/443)**

* **Serviço**: Apache httpd
* **Status**: Funcionando com SSL
* **Preocupação**: Versão não especificada, possíveis vulnerabilidades

**DNS (Porta 53)**

* **Serviço**: PowerDNS Authoritative Server 4.9.5
* **Status**: Versão identificada
* **Recomendação**: Verificar atualizações de segurança

**RPC (Porta 111)**

* **Serviço**: rpcbind 2-4
* **Risco**: Exposição de serviços RPC pode revelar informações do sistema

**RECOMENDAÇÕES CRÍTICAS DE IMPLEMENTAÇÃO**

**1. MITIGAÇÃO IMEDIATA - BANCOS DE DADOS**

**Ações Urgentes:**

*# Configurar firewall para bloquear acesso externo aos bancos*

iptables -A INPUT -p tcp --dport 3306 -s localhost -j ACCEPT

iptables -A INPUT -p tcp --dport 3306 -j DROP

iptables -A INPUT -p tcp --dport 5432 -s localhost -j ACCEPT

iptables -A INPUT -p tcp --dport 5432 -j DROP

**Configurações MySQL/MariaDB:**

*-- Desabilitar acesso remoto para root*

DELETE FROM mysql.user WHERE User='root' AND Host NOT IN ('localhost', '127.0.0.1', '::1');

*-- Remover usuários anônimos*

DELETE FROM mysql.user WHERE User='';

*-- Remover banco de teste*

DROP DATABASE IF EXISTS test;

FLUSH PRIVILEGES;

**2. SEGURANÇA DO PAINEL ADMINISTRATIVO**

**Implementar Autenticação Multi-Fator:**

* Configurar 2FA para todas as contas cPanel/WHM
* Restringir acesso por IP através de .htaccess ou firewall

**Configuração de Firewall Específica:**

*# Permitir apenas IPs administrativos*

iptables -A INPUT -p tcp --dport 2083 -s [IP\_ADMIN] -j ACCEPT

iptables -A INPUT -p tcp --dport 2087 -s [IP\_ADMIN] -j ACCEPT

iptables -A INPUT -p tcp --dport 2083 -j DROP

iptables -A INPUT -p tcp --dport 2087 -j DROP

**3. HARDENING DO SSH**

**Configuração SSH Segura (/etc/ssh/sshd\_config):**

*# Desabilitar root login*

PermitRootLogin no

*# Usar apenas chaves públicas*

PasswordAuthentication no

PubkeyAuthentication yes

AuthorizedKeysFile .ssh/authorized\_keys

*# Limitar tentativas*

MaxAuthTries 3

MaxSessions 2

*# Protocolo e criptografia*

Protocol 2

Ciphers aes256-ctr,aes192-ctr,aes128-ctr

MACs hmac-sha2-256,hmac-sha2-512

**4. CONFIGURAÇÃO DE FIREWALL ABRANGENTE**

**Script de Firewall Recomendado:**

#!/bin/bash

*# Política padrão - negar tudo*

iptables -P INPUT DROP

iptables -P FORWARD DROP

iptables -P OUTPUT ACCEPT

*# Permitir loopback*

iptables -A INPUT -i lo -j ACCEPT

*# Permitir conexões estabelecidas*

iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

*# Serviços essenciais*

iptables -A INPUT -p tcp --dport 80 -j ACCEPT *# HTTP*

iptables -A INPUT -p tcp --dport 443 -j ACCEPT *# HTTPS*

iptables -A INPUT -p tcp --dport 25 -j ACCEPT *# SMTP*

iptables -A INPUT -p tcp --dport 587 -j ACCEPT *# SMTP Submission*

*# SSH restrito (alterar IP\_ADMIN)*

iptables -A INPUT -p tcp --dport 1157 -s [IP\_ADMIN] -j ACCEPT

*# Salvar regras*

iptables-save > /etc/iptables/rules.v4

**5. MONITORAMENTO E LOGGING**

**Implementar SIEM Básico:**

*# Configurar rsyslog para centralizar logs*

echo "\*.\* @@syslog-server:514" >> /etc/rsyslog.conf

*# Monitorar tentativas de acesso*

fail2ban-client set sshd maxretry 3

fail2ban-client set sshd bantime 3600

**Monitoramento de Integridade:**

*# Instalar AIDE para monitoramento de arquivos*

aide --init

aide –check

Links úteis:

[A03 Injection - OWASP Top 10:2021](https://owasp.org/Top10/A03_2021-Injection/)

[WSTG - v4.2 | OWASP Foundation](https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/07-Input_Validation_Testing/05-Testing_for_SQL_Injection)

[OWASP Top Ten 2017 | A1:2017-Injection | OWASP Foundation](https://owasp.org/www-project-top-ten/2017/A1_2017-Injection.html)

[CWE - CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') (4.16)](https://cwe.mitre.org/data/definitions/89.html)