HARDENING DE SERVIDOR LINUX

Responsável: João Pedro Toledo Gonçalves

Data: 26/01/2026

MANUAL TÉCNICO - HARDENING DE SERVIDOR LINUX

Código: ITGENG 0010/26 | **Classificação:** CONFIDENCIAL
Responsável: João Pedro Toledo Gonçalves | **Data:** 26/01/2026

1. HISTÓRICO DE REVISÃO

Data	Versão	Descrição	Autor
26/01/2026	**1.0**	**Criação Inicial**	**João Pedro Toledo Gonçalves**

2. OBJETIVO

Aplicar práticas de segurança para reduzir a superfície de ataque em servidores Linux expostos ou críticos, focando em SSH, Proteção contra Força Bruta e Kernel Tuning.

3. PRÉ-REQUISITOS

[ ] Acesso Root.
[ ] **CRÍTICO:** Tenha uma chave SSH pública configurada e testada no servidor ANTES de desabilitar a senha.
[ ] Backup das configurações originais.

---

4. SEGURANÇA NO SSH (DESABILITAR SENHA)

O vetor de ataque mais comum é força bruta na porta 22.

1. [x] Edite o arquivo: `/etc/ssh/sshd_config`
2. [x] Garanta que as seguintes linhas existem e estão descomentadas:

```
      PermitRootLogin prohibit-password  # Ou 'no' (Recomendado criar usuario admin
separado)
      PubkeyAuthentication yes
      PasswordAuthentication no
      ChallengeResponseAuthentication no
```

3. [x] Valide a configuração: `sudo sshd -t`
4. [x] Reinicie o serviço:

• Debian/Ubuntu: `sudo systemctl restart ssh`

• RHEL/CentOS: `sudo systemctl restart sshd`
• Alpine: `sudo rc-service sshd restart`

> **IMPORTANTE**
> **IMPORTANTE:** Não feche a sessão atual sem abrir uma nova para testar se a chave funcionou. Se falhar, você perderá acesso remoto.

5. PROTEÇÃO CONTRA BRUTE-FORCE (FAIL2BAN)

O Fail2Ban monitora logs e bane IPs que erram a senha repetidamente.

Instalação:

• Debian/Ubuntu: `sudo apt install fail2ban`
• RHEL/CentOS: `sudo dnf install epel-release && sudo dnf install fail2ban`
• Alpine: `sudo apk add fail2ban`

Configuração Básica:

1. [x] Copie o arquivo padrão de config:

```
sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
```

2. [x] Edite `/etc/fail2ban/jail.local` e ative a proteção SSH:

```
[sshd]
enabled = true
port = ssh
filter = sshd
logpath = /var/log/auth.log ; (Ou /var/log/secure no RHEL)
maxretry = 3
bantime = 3600 ; (1 hora)
```

3. [x] Reinicie: `sudo systemctl restart fail2ban`
4. [x] Verifique: `sudo fail2ban-client status sshd`

6. AJUSTES DE KERNEL (SYSCTL)

Proteção contra ataques de rede (Spoofing, ICMP Redirects).

1. [x] Crie o arquivo: `/etc/sysctl.d/99-security.conf`
2. [x] Adicione:

```
# Desabilita redirecionamentos ICMP (Man-in-the-middle)
net.ipv4.conf.all.accept_redirects = 0
net.ipv6.conf.all.accept_redirects = 0

# Ignora pings de broadcast
net.ipv4.icmp_echo_ignore_broadcasts = 1

# Protecao contra Syn Flood
net.ipv4.tcp_syncookies = 1

# Log de pacotes suspeitos (Martian packets)
net.ipv4.conf.all.log_martians = 1
```

3. [x] Aplique: `sudo sysctl system`

7. DADOS TÉCNICOS

Serviço	Porta Padrão	Logs
SSH	**22/tcp**	**/var/log/auth.log (Deb) / /var/log/secure (RHEL)**
Fail2Ban	**N/A**	**/var/log/fail2ban.log**

8. VALIDAÇÃO FINAL

[ ] Tentar logar via SSH sem chave pede senha? (Deve falhar: "Permission denied (publickey)")
[ ] O Fail2Ban está rodando (`systemctl status fail2ban`)?
[ ] Errar a senha 3 vezes bane o IP? (Cuidado para não se banir, use 4G para testar).