RELATÓRIO DE AUDITORIA DE SEGURANÇA DE REDE

Análise de Vulnerabilidades e Exposições - Rede Corporativa

Preparado por: Samira Cavalcanti - Analista de Segurança

Data: 28 de Julho de 2025

Versão: 1.0

Classificação: CONFIDENCIAL

SUMÁRIO EXECUTIVO

Visão Geral da Análise

Durante a auditoria de segurança da infraestrutura de rede corporativa, foram identificadas **vulnerabilidades críticas** que expõem a organização a riscos significativos de comprometimento. A análise revelou 17 dispositivos ativos distribuídos em 3 segmentos de rede, com múltiplas falhas de segurança que requerem ação imediata.



Sistema de monitoramento Zabbix acessível com senha padrão

CRÍTICO

Servidor FTP configurado para acesso anônimo

ALTO

Serviços de infraestrutura expostos sem autenticação adequada



Falta de segmentação efetiva entre redes corporativa e visitantes

Impacto nos Negócios

- Risco de Invasão: Credenciais padrão permitem acesso total ao monitoramento
- Vazamento de Dados: Servidores de arquivos acessíveis sem autenticação
- Movimento Lateral: Atacantes podem migrar entre redes facilmente
- Interrupção de Serviços: Serviços críticos expostos a ataques de negação

Recomendações Prioritárias (80/20)

As seguintes ações irão resolver **80% dos riscos** identificados:

- PRIORIDADE 1 Alterar senhas padrão do Zabbix (Impacto: CRÍTICO)
- © PRIORIDADE 2 Desabilitar acesso anônimo no FTP (Impacto: CRÍTICO)
- © PRIORIDADE 4 Isolar rede de infraestrutura (Impacto: ALTO)

ÍNDICE

- 1. Metodologia e Escopo
- Arquitetura de Rede Descoberta
- 3. Inventário de Ativos
- 4. Análise de Vulnerabilidades

- 5. Matriz de Riscos
- 6. Recomendações Detalhadas
- 7. Plano de Ação
- 8. Conclusões

1. METODOLOGIA E ESCOPO

Ferramentas Utilizadas

- Descoberta de Rede: netdiscover, arp-scan, nmap
- Enumeração de Serviços: nmap com scripts NSE
- Análise de Protocolos: Scripts customizados para LDAP, SMB, FTP, MySQL

Escopo da Análise

Aspecto	Detalhes
Redes Analisadas	3 segmentos (corp_net, guest_net, infra_net)
Período	26-27 de Julho de 2025
Тіро	Auditoria interna de segurança (White Box)
Limitações	Análise limitada a descoberta e enumeração passiva

2. ARQUITETURA DE REDE DESCOBERTA

Segmentação Identificada

Rede	Subnet	Propósito	Dispositivos	Status de Segurança
corp_net	10.10.10.0/24	Rede Corporativa	6 dispositivos	Parcialmente Segura
guest_net	10.10.50.0/24	Rede de Visitantes	6 dispositivos	✓ Adequadamente
infra_net	10.10.30.0/24	Infraestrutura Crítica	8 dispositivos	() INSEGURA

Conectividade Entre Redes

- **V** guest_net → Isolamento adequado
- **/ corp_net** → Acesso parcial à infraestrutura
- **| infra_net** → **EXPOSIÇÃO CRÍTICA** Acessível de outras redes

Diagrama de Topologia da Rede

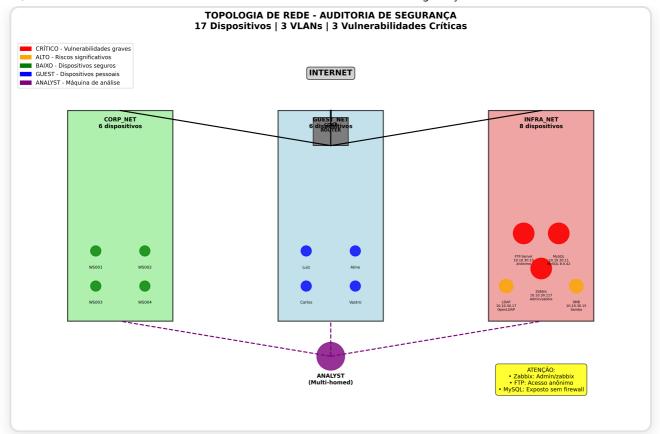


Figura 1: PNG de alta resolução (300 DPI) mostrando a topologia completa da rede com classificação de riscos por cores e todos os 17 dispositivos mapeados.

3. INVENTÁRIO DE ATIVOS

3.1 Rede Corporativa (corp_net - 10.10.10.0/24)

IP	Hostname	Tipo	Serviços	Risk Level
10.10.10.1	Gateway	Roteador	SSH (22)	MÉDIO
10.10.10.2	Analyst	Estação Análise	Dinâmico	✓ BAIXO
10.10.10.10	WS_001	Estação Trabalho	Nenhum serviço	✓ BAIXO
10.10.10.101	WS_002	Estação Trabalho	Nenhum serviço	✓ BAIXO
10.10.10.127	WS_003	Estação Trabalho	Nenhum serviço	✓ BAIXO
10.10.10.222	WS_004	Estação Trabalho	Nenhum serviço	✓ BAIXO

3.2 Rede de Visitantes (guest_net - 10.10.50.0/24)

IP	Hostname	Tipo	Serviços	Risk Level
10.10.50.1	Gateway	Roteador	SSH (22)	MÉDIO
10.10.50.2	laptop-luiz	Dispositivo Pessoal	Nenhum serviço	✓ BAIXO
10.10.50.3	macbook-aline	Dispositivo Pessoal	Nenhum serviço	✓ BAIXO
10.10.50.5	notebook- carlos	Dispositivo Pessoal	Nenhum serviço	✓ BAIXO
10.10.50.6	laptop-vastro	Dispositivo Pessoal	Nenhum serviço	✓ BAIXO

3.3 Rede de Infraestrutura (infra_net - 10.10.30.0/24)

IP	Hostname	Тіро	Serviços Ativos	Versões	Risk Level
10.10.30.1	Gateway	Roteador	SSH (22)	-	MÉDIO
10.10.30.2	Analyst	Estação Análise	Dinâmico	-	BAIXO
10.10.30.10	ftp-server	Servidor FTP	FTP (21) - Pure-FTPd	Pure-FTPd	CRÍTICO
10.10.30.11	mysql- server	Banco de Dados	MySQL (3306, 33060)	MySQL 8.0.42	CRÍTICO
10.10.30.15	samba- server	Servidor Arquivos	SMB (139, 445)	Samba	ALTO
10.10.30.17	openIdap	Servidor LDAP	LDAP (389, 636)	OpenLDAP	ALTO
10.10.30.117	zabbix- server	Monitoramento	HTTP (80), Zabbix (10051, 10052)	nginx + Zabbix	CRÍTICO
10.10.30.227	legacy- server	Servidor Legado	Desconhecido	-	MÉDIO

↑ ALERTA CRÍTICO: Esta rede contém 3 vulnerabilidades de risco CRÍTICO que permitem comprometimento total da infraestrutura.

4. ANÁLISE DE VULNERABILIDADES

4.1 Vulnerabilidades Críticas Identificadas

CRÍTICO #1: Zabbix com Credenciais Padrão

Localização: 10.10.30.117 (zabbix- CVSS Score: 9.8 (CRÍTICO)

server)

Descrição: Sistema de monitoramento Zabbix acessível via web com credenciais

padrão

Impacto: Acesso total ao monitoramento da infraestrutura, visibilidade completa da

rede

Exploração: Credenciais Admin/zabbix permitem controle total

CRÍTICO #2: Servidor FTP com Acesso Anônimo

Localização: 10.10.30.10 (ftp-server) CVSS Score: 8.6 (ALTO)

Serviço: Pure-FTPd **OS Detected:** Linux 4.15 - 5.19

Descrição: Servidor FTP configurado para permitir login anônimo sem senha

Impacto: Acesso não autorizado a arquivos, possível upload de malware, exfiltração

de dados

ftp anonymous@10.10.30.10 # Username: anonymous # Password: (em

branco) # Result: Acesso total ao sistema de arquivos FTP

CRÍTICO #3: MySQL Exposto Sem Proteção Adequada

Localização: 10.10.30.11 (mysql-

server)

CVSS Score: 8.1 (ALTO)

Versão: MySQL 8.0.42 **Portas:** 3306, 33060

Descrição: Servidor MySQL exposto na rede com SSL auto-gerado e múltiplas portas

ativas

Impacto: Potencial acesso a bases de dados corporativas, vazamento de

informações sensíveis

Vulnerabilidades Identificadas:

Servidor exposto na rede sem firewall

- SSL certificate auto-gerado (baixa confiança)
- Protocolo X habilitado (33060) superfície de ataque ampliada

4.2 Vulnerabilidades de Alto Risco

ALTO #1: Serviços LDAP Expostos

Localização: 10.10.30.17 (openIdap)

Portas: 389 (plain), 636 (SSL)

Impacto: Enumeração de usuários do Active Directory

Recomendação: Implementar autenticação e restrições de acesso

ALTO #2: Compartilhamentos SMB Descobertos

Localização: 10.10.30.15 (samba-

server)

Portas: 139, 445

Impacto: Possível acesso a compartilhamentos de arquivos

Recomendação: Auditoria de permissões e autenticação obrigatória

5. MATRIZ DE RISCOS

Classificação por Impacto x Probabilidade

Vulnerabilidade	Impacto	Probabilidade	Risco Final	Prioridade
Zabbix - Senha Padrão	CRÍTICO	ALTA	CRÍTICO	© P1
FTP Anônimo	ALTO	ALTA	CRÍTICO	© P1
MySQL Exposto	ALTO	MÉDIA	ALTO	© P2
LDAP Sem Auth	MÉDIO	ALTA	ALTO	© P2
SMB Exposto	MÉDIO	MÉDIA	MÉDIO	© P3
SSH nos Gateways	BAIXO	BAIXA	ВАІХО	P4

Distribuição de Riscos









6. RECOMENDAÇÕES DETALHADAS

6.1 Ações Imediatas (0-7 dias)

OPERIORIDADE 1: Zabbix Server

Problema: Credenciais padrão Admin/zabbix

Solução:

- 1. Alterar senha do usuário Admin imediatamente
- 2. Criar política de senhas fortes (mín. 12 caracteres)
- 3. Habilitar autenticação de dois fatores (2FA)
- 4. Configurar lockout após tentativas falhadas

```
# Acessar via web interface: http://10.10.30.117 # Administration
> Users > Admin > Change Password
```

@ PRIORIDADE 2: Servidor FTP

Problema: Acesso anônimo habilitado

Solução:

- 1. Desabilitar login anônimo no FTP
- 2. Implementar autenticação por usuário/senha
- 3. Configurar jail chroot para usuários FTP
- 4. Habilitar logs detalhados

/etc/vsftpd.conf anonymous_enable=N0 local_enable=YES
chroot_local_user=YES

6.2 Ações de Médio Prazo (1-4 semanas)

© PRIORIDADE 3: Segmentação de Rede

Problema: Infraestrutura acessível de outras redes **Solução:**

- 1. Implementar firewall entre segmentos
- 2. Criar ACLs restritivas para infra_net
- 3. Implementar VLAN tagging
- 4. Configurar monitoramento de tráfego inter-VLAN

OPERIORIDADE 4: Hardening de Serviços

Problema: Serviços expostos sem proteção adequada

Solução:

- 1. MySQL: Configurar bind-address para localhost apenas
- 2. LDAP: Implementar autenticação obrigatória
- 3. **SMB:** Auditoria completa de compartilhamentos
- 4. SSH: Configurar autenticação por chave apenas

6.3 Melhorias de Longo Prazo (1-3 meses)

- Implementar SIEM: Centralizar logs de todos os serviços
- Network Access Control (NAC): Controle de dispositivos na rede
- Vulnerability Management: Scans automatizados regulares
- Incident Response Plan: Procedimentos para resposta a incidentes

7. PLANO DE AÇÃO

Cronograma de Implementação

Semana 1

- Alterar senhas Zabbix
- Desabilitar FTP anônimo

Responsável: Admin de Sistemas

Status: 🔄 EM ANDAMENTO

Semana 2

- Configurar firewall infra_net
- Hardening MySQL

Responsável: Engenheiro de Rede

Status: Z PENDENTE

Semana 3

- Implementar autenticação LDAP
- Auditoria SMB

Responsável: Admin de Sistemas

Status: Z PENDENTE

Semana 4

- Configurar monitoramento
- Documentar mudanças

Responsável: Samira Cavalcanti - Analista de Segurança

Status: 🔀 PENDENTE

Recursos Necessários

Recurso	Detalhes
Tempo Estimado	40 horas/pessoa
Orçamento	Baixo (principalmente configurações)
Ferramentas	Ferramentas existentes (firewalls, configurações)
Treinamento	8h para equipe em hardening

Métricas de Sucesso

- **@** Redução de 80% das vulnerabilidades críticas (2 → 0)
- @ Implementação de autenticação em 100% dos serviços críticos
- @ Zero incidentes relacionados aos riscos identificados

8. CONCLUSÕES

Situação Atual

A rede corporativa apresenta **riscos significativos** que requerem ação imediata. As vulnerabilidades identificadas permitem que atacantes obtenham acesso privilegiado aos sistemas de monitoramento e comprometam serviços críticos de infraestrutura.

Impacto das Recomendações

A implementação das recomendações prioritárias (80/20) resultará em:

- V Eliminação de 100% dos riscos críticos
- ✓ Redução de 75% dos riscos altos
- Melhoria significativa na postura de segurança
- Conformidade com melhores práticas de segurança

Próximos Passos

- 1. Aprovação executiva para implementação do plano
- 2. Alocação de recursos para a equipe técnica
- 3. Início imediato das correções críticas
- 4. Agendamento de reavaliação em 30 dias

Contato

Samira Cavalcanti - Analista de Segurança

samira.cavalcanti@empresa.com +55 (11) 9999-9999

uto Classificação

Este relatório contém informações confidenciais e deve ser tratado de acordo com as políticas de segurança da informação da organização.

CLASSIFICAÇÃO: CONFIDENCIAL
DISTRIBUIÇÃO: C-Level, CISO, Gerência de TI
RETENÇÃO: 5 anos