Relatório Técnico de Mapeamento de Rede - Projeto Final

Autor: Ramon de Moraes Milhomem
Email: ramon.milhomen10@gmail.com
Telefone: (86) 99826-8185

Data: 24/07/2025

1. Objetivo

Este relatório tem como objetivo documentar o processo de mapeamento e diagnóstico de uma rede simulada com múltiplos segmentos (corporativo, infraestrutura e visitantes), identificando os ativos presentes, os serviços em execução e propondo recomendações para mitigação de riscos e melhoria da segurança da informação.

2. Estrutura das Redes Identificadas

A topologia foi segmentada em três redes lógicas distintas conforme abaixo:

- corp_net (10.10.10.0/24): Rede corporativa, onde estão as estações de trabalho.
- infra_net (10.10.30.0/24): Rede destinada a servidores de infraestrutura.
- guest_net (10.10.50.0/24): Rede de visitantes com notebooks pessoais conectados.

3. Inventário de Ativos

Rede Corporativa:
- WS_001 - 10.10.10.10 - MAC: 52:EE:7C:59:B6:DF
- WS_002 - 10.10.10.101 - MAC: 8E:69:C4:B4:71:44
- WS_003 - 10.10.10.127 - MAC: CE:9D:F1:16:DE:1E
- WS_004 - 10.10.10.222 - MAC: F2:72:AD:0D:8F:31

Infraestrutura:
- ftp-server - 10.10.30.10 - FTP (Pure-FTPd) - Linux 4.15-5.19
- mysql-server - 10.10.30.11 - Nao inspecionado
- samba-server - 10.10.30.15 - Nao inspecionado
- openldap - 10.10.30.17 - Nao inspecionado
- zabbix-server - 10.10.30.117 - Nao inspecionado
- legacy-server - 10.10.30.227 - Nao inspecionado

Visitantes:
- notebook-carlos - 10.10.50.2 - MAC: BE:80:1F:93:53:69
- laptop-luiz - 10.10.50.3 - MAC: 82:63:E7:DE:AB:01
- macbook-aline - 10.10.50.4 - MAC: DA:DF:54:8E:05:EF
- laptop-vastro - 10.10.50.5 - MAC: 76:40:DD:44:E6:FB

Relatório Técnico de Mapeamento de Rede - Projeto Final

4. Análise de Serviços e Sistemas

ftp-server (10.10.30.10):
- Serviço identificado: FTP (porta 21/tcp)
- Versão: Pure-FTPd
- Sistema Operacional: Linux 4.X-5.X
- Risco: FTP transmite dados sem criptografia, sujeito a interceptação e ataques de sniffing.

WS_001 (10.10.10.10):
- Todas as portas TCP estão fechadas (RESET).
- Indica a presença de firewall ou filtragem de pacotes.

5. Diagnóstico

- O ambiente apresenta segmentação de rede adequada, com sub-redes distintas para cada tipo de dispositivo.
- Foi identificado um serviço FTP exposto publicamente, o que representa risco de interceptação de credenciais e arquivos.
- Demais servidores não foram inspecionados a fundo, sendo necessária nova varredura com parâmetros adicionais (-sV, -A, etc.).

6. Recomendações Técnicas

- Substituir o serviço FTP por SFTP ou FTPS, garantindo criptografia dos dados.
- Realizar escaneamento mais profundo nos demais hosts para identificar serviços e vulnerabilidades.
- Implantar um firewall entre as sub-redes para isolar melhor os domínios de segurança.
- Reforçar o monitoramento com Zabbix e validar suas configurações.
- Aplicar auditoria no ambiente Docker e verificar as regras de NAT e bridge.

7. Conclusão

A análise identificou uma topologia organizada, com redes separadas por função. No entanto, a presença de um servidor FTP com serviço inseguro requer atenção imediata. Com as ações propostas, o ambiente pode ser tornado mais seguro e confiável, minimizando vetores de ataque e garantindo integridade dos dados em trânsito.