Análise de Segurança e Segmentação de Rede

Relatório Técnico

Autor: Lucas Seccatto

26 de julho de 2025

Sumário Executivo

Este relatório apresenta os resultados de uma análise de segurança realizada na rede do laboratório. A investigação revelou que a rede está dividida em três segmentos: um para funcionários, um para servidores e um para visitantes. Embora essa separação exista, foram encontradas falhas de segurança significativas que colocam a organização em risco.
O problema mais crítico é um servidor de monitoramento que utiliza um software severamente desatualizado, o que pode servir como uma porta de entrada para invasores. Além disso, foram identificados outros serviços que operam de forma insegura, expondo informações sensíveis, como senhas. A falta de um isolamento eficaz entre as redes agrava a situação, pois um ataque bem-sucedido em um ponto poderia facilmente se espalhar por todo o ambiente.
As ações recomendadas neste documento são cruciais para proteger a rede. A prioridade é a atualização imediata do servidor vulnerável e a implementação de regras de firewall para garantir que as redes fiquem devidamente isoladas umas das outras.

Objetivo

Analisar a rede do laboratório para entender como ela está organizada, quais serviços estão visíveis e se a separação entre as redes (segmentação) é segura, identificando possíveis riscos.

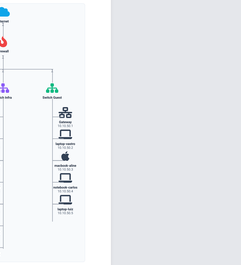
Escopo

O trabalho focou nas três redes encontradas no ambiente de laboratório:
`10.10.10.0/24` (corp_net)
`10.10.30.0/24` (infra_net)
`10.10.50.0/24` (guest_net)

Metodologia

A análise seguiu um passo a passo para investigar a rede de forma ativa:
1. **Descoberta de Ativos:** Primeiro, foram usadas ferramentas para encontrar quais computadores estavam ligados em cada rede.
2. **Varredura de Portas e Serviços:** Com a lista de computadores ativos, foram usadas as ferramentas `Portlcdn` e `nmap` para descobrir quais portas estavam abertas e quais programas (serviços) estavam rodando em cada uma.
3. **Análise de Riscos:** Cada serviço encontrado foi inspecionado manualmente para identificar problemas, como programas desatualizados, configurações perigosas ou protocolos que não usam criptografia.
4. **Documentação:** Todas as informações foram organizadas neste relatório, que inclui os problemas encontrados e as sugestões de correção.

Diagrama de Rede



Diagnóstico (Achados)

Mapeamento de Ativos por Rede

Nome da Rede	Sub-rede Descoberta	Finalidade Principal
`corp_net`	`10.10.10.0/24`	Rede corporativa para estações de trabalho
`infra_net`	`10.10.30.0/24`	Rede de infraestrutura e servidores
`guest_net`	`10.10.50.0/24`	Rede para dispositivos de visitantes

Achado 1: Programa Desatualizado em Servidor Importante (Risco Crítico)

Host/IP: `zabbix-server.projeto_final_opcao_1_infra_net` (`10.10.30.117`)
Serviço/Porta: `http` / `80/tcp`
Risco Identificado: O servidor que roda a aplicação Zabbix usa a versão `7.3.14` do PHP. Essa versão chegou ao seu **fim de vida** em 2021, o que significa que **ela não recebe mais correções de segurança**. Isso deixa o servidor vulnerável a muitas falhas já conhecidas, que podem permitir a um invasor executar comandos remotamente, tomar o controle total do servidor e usá-lo para atacar o resto da rede.
Evidência: Cabeçalho HTTP `X-Powered-By: PHP/7.3.14` retornado pelo servidor.

Achado 2: Uso de Protocolo Inseguro para Transferência de Arquivos (Risco Alto)

Host/IP: `ftp-server.projeto_final_opcao_1_infra_net` (`10.10.30.10`)
Serviço/Porta: `ftp` / `21/tcp`
Risco Identificado: O serviço de FTP está ativo. Este protocolo é antigo e perigoso porque envia usuários, senhas e todos os arquivos como texto simples, sem criptografia. Um invasor que consiga "escutar" o tráfego da rede poderá facilmente ler todas essas informações e ganhar acesso não autorizado.
Evidência: Porta `21/tcp` aberta, identificada pelo `Portscan`.

Achado 3: Vazamento de Informações sobre Serviços (Risco Médio)

Host/IP: `mysql-server` (`10.10.30.11`) e `openldap` (`10.10.30.17`)
Serviço/Porta: `mysql` / `3306/tcp` e `ldap` / `389/tcp`
Risco Identificado: O servidor de banco de dados e o de diretório respondem com informações detalhadas sobre suas versões e configurações. Por exemplo, o MySQL informa a versão exata (`8.0.43`) e o LDAP mostra parte da sua estrutura interna. Isso não é um erro grave por si só, mas ajuda um invasor a saber exatamente qual programa está rodando para procurar por falhas específicas dele.
Evidência: Respostas dos scripts `mysql-info` e `ldap-rootdse` do Nmap.

Recomendações

1. **Para o Achado 1 (Zabbix):** É fundamental atualizar o servidor Zabbix e, principalmente, o PHP para uma versão recente que ainda receba atualizações de segurança. A melhor solução seria usar a imagem Docker oficial e mais nova do Zabbix.

2. **Para o Achado 2 (FTP):** O serviço de FTP na porta 21 deve ser desativado. Para transferir arquivos, deve-se usar um protocolo seguro como o **SFTP**, que é criptografado.

3. **Para o Achado 3 (Vazamento de Informação):** Os servidores de MySQL e LDAP devem ser configurados para não dar tantas informações para quem não está autenticado. Além disso, o acesso a eles deveria ser bloqueado por um firewall, permitindo a conexão somente de outros servidores que realmente precisem desse acesso.

4. **Recomendação Geral de Segmentação:** É preciso criar regras de firewall para separar as redes de verdade. A rede de visitantes (`guest_net`) não deveria, em hipótese alguma, conseguir acessar as redes internas. O acesso da rede dos funcionários (`corp_net`) para a rede de servidores (`infra_net`) também deve ser muito restrito, permitindo acesso somente as que for estritamente necessário para o trabalho.

Plano de Ação (Modelo 80/20)

Ação	Impacto	Facilidade	Prioridade
Atualizar servidor Zabbix/PHP	Crítico	Média	**Crítica**
Criar regras de firewall entre as redes	Alto	Média	**Alta**
Desativar serviço FTP (porta 21)	Alto	Alta	**Alta**
Limitar informações de DB/LDAP	Média	Alta	Média

Conclusão

O ambiente do laboratório, embora dividido em três redes, possui falhas de segurança importantes. O programa desatualizado no servidor Zabbix e a falta de um bom isolamento entre as redes criam um risco real de invasão. Seguir as recomendações deste relatório, especialmente a atualização do Zabbix e a configuração do firewall, é o caminho correto para deixar o ambiente mais seguro.

Anexos

Referências do Projeto

Para consulta das evidências completas, incluindo os logs brutos das ferramentas de scan e os screenshots da análise, por favor, acesse o repositório oficial do projeto no Github:
https://github.com/lucasseccatto/kensei-cybersec-final-project