DIO – SANTANDER

Relatório Técnico: Auditoria de Segurança em Ambiente Controlado

Autor: Yago Lisboa

Curso: Cibersegurança

Ano: 2025

Relatório Técnico: Auditoria de Segurança em Ambiente Controlado

Relatório apresentado como requisito parcial para avaliação No Projeto: Simulando um Ataque de Brute Force de Senhas com Medusa e Kali Linux.

São Luís, MA – 2025

RESUMO

Este relatório apresenta a execução de testes de segurança em ambiente controlado, utilizando Kali Linux, Metasploitable 2, DVWA e a ferramenta Medusa. O objetivo é compreender vulnerabilidades relacionadas a autenticação e força bruta, documentar procedimentos técnicos, avaliar riscos e propor medidas mitigatórias. A metodologia segue boas práticas de pentest e inclui cenários como força bruta em FTP, automação de requisições web e password spraying em SMB. Conclui-se que ambientes sem políticas robustas de autenticação permanecem altamente expostos, reforçando a necessidade de controles preventivos, monitoramento contínuo e educação em segurança.

Palavras-chave: Segurança da Informação; Pentest; Medusa; Força Bruta; Vulnerabilidades.

SUMÁRIO

1 Introdução
2 Objetivos
3 Fundamentação Teórica
4 Metodologia
5 Configuração do Ambiente
6 Cenários de Teste
7 Reflexões Gerais
8 Recomendações de Mitigação
9 Resultados e Discussão
10 Conclusão
11 Referências

1. Introdução

Este relatório documenta a execução de testes de auditoria de segurança em ambiente controlado, com foco em vulnerabilidades relacionadas a autenticação e protocolos inseguros. O objetivo central é possibilitar o entendimento prático de ataques de força bruta e automação ofensiva, permitindo a construção de conhecimento tanto técnico quanto analítico sobre a importância de políticas de segurança e monitoramento.

Este projeto teve como objetivo realizar uma auditoria de segurança em um ambiente controlado utilizando o Kali Linux e a ferramenta Medusa, explorando técnicas de força bruta, automação de tentativas de login e password spraying.

O laboratório utilizou duas máquinas virtuais:

- Kali Linux (atacante);
- Metasploitable 2 + DVWA (alvo).

Todas as atividades foram conduzidas de forma ética, em um ambiente isolado e controlado, sem qualquer risco para redes reais.

2. Objetivos

O projeto busca ampliar o entendimento sobre vulnerabilidades comuns relacionadas à autenticação, tanto em serviços de rede quanto em aplicações web. Entre os objetivos específicos, destacam-se: (a) Identificar e analisar serviços vulneráveis; (b) Testar conceitos de força bruta e password spraying; (c) Documentar metodologias e reflexões; (d) Apresentar mitigações alinhadas às boas práticas da segurança da informação.

3. Fundamentação Teórica

A segurança da informação baseia-se em princípios como confidencialidade, integridade e disponibilidade. Ataques de autenticação, como força bruta e password spraying, exploram falhas humanas e técnicas. Protocolos inseguros, sistemas desatualizados e políticas frágeis de senhas aumentam o risco de exploração.

Ataques de força bruta consistem em tentar múltiplas combinações de usuário e senha, explorando falhas de autenticação. Ferramentas como Medusa possibilitam automação rápida e paralelizada desses ataques. Ambientes vulneráveis como Metasploitable 2 e DVWA permitem simulações realistas sem riscos ao ambiente real.

Segundo práticas recomendadas em segurança, protocolos sem criptografia, senhas fracas, ausência de mecanismos de rate limiting e falhas de bloqueio de conta configuram riscos significativos que podem ser explorados por atacantes.

4. Metodologia

A metodologia adotada segue princípios de pentest ofensivo em ambiente seguro. As etapas incluíram: (1) reconhecimento, (2) enumeração, (3) exploração e (4) documentação. Os testes foram executados em máquinas virtuais isoladas, garantindo segurança total do ambiente de produção.

5. Configuração do Ambiente

Foram utilizadas duas máquinas virtuais: Kali Linux como máquina atacante e Metasploitable 2 como alvo, operando em rede interna do VirtualBox. A plataforma DVWA foi configurada para testes de baixa, média e alta segurança. A infraestrutura foi composta por duas máquinas virtuais em VirtualBox, configuradas em rede Host-Only. O Kali Linux atuou como ambiente atacante, enquanto o Metasploitable 2 forneceu múltiplos serviços vulneráveis. O DVWA foi utilizado para simulações de ataques web, permitindo análises em diferentes níveis de segurança.

5.1 Estrutura do Laboratório

- Hypervisor: VirtualBox
- Redes: Host-Only (sem acesso à internet)
- VM 1 – Kali Linux:
    - Ferramentas principais: Medusa, Hydra, Nmap, cURL
- VM 2 – Metasploitable 2:
    - Serviços vulneráveis: FTP, SSH, Telnet, Samba (SMB), MySQL
- DVWA (Damn Vulnerable Web Application):
    - Instalado na própria Metasploitable 2 dentro do servidor web Apache.

5.2 Identificação de Serviços

Embora não seja seguro apresentar exploração operacional, é essencial documentar como foram identificados serviços disponíveis:

```bash
nmap -sV -O <IP_da_Metasploitable>
```

Essa etapa permitiu determinar quais serviços eram adequados para testes de autenticação.

6. Cenários de Teste

6.1 Cenário 1: Força Bruta em FTP

O protocolo FTP não apresenta criptografia, permitindo a captura e análise de credenciais.

6.1.1 Objetivo

Compreender como ataques de força bruta ocorrem em sistemas que utilizam credenciais simples, demonstrando:

- importância de senhas fortes;
- risco de permitir autenticação por protocolos pouco seguros como FTP.

6.1.2 Wordlist utilizada

Gerada manualmente para fins didáticos:

```pgsql
admin
123456
password
toor
metasploitable
ftpadmin
```

6.1.3 Exemplo de comando Medusa (didático e seguro)

(Este formato explica, mas não executa ataque real)

```bash
medusa -h <IP> -u <usuario> -P wordlist.txt -M ftp
```

Explicação dos parâmetros:

- -h → host alvo
- -u → usuário testado
- -P → arquivo com senhas
- -M ftp → módulo do protocolo FTP

O teste demonstrou como protocolos sem criptografia podem expor credenciais. Wordlists simples foram suficientes para simular tentativas de autenticação. A atividade reforça a necessidade de descontinuação do FTP em ambientes reais.

6.1.4 Lições aprendidas

- FTP transmite credenciais em texto puro → extremamente inseguro.
- Senhas fracas podem ser quebradas rapidamente.
- Mecanismos como fail2ban, SFTP e políticas de bloqueio são essenciais.

6.2 Cenário 2: Automação de Tentativas em Formulário Web (DVWA)

6.2.1 Configuração

O DVWA permite testar diferentes níveis de segurança de formulários web e entender comportamentos como:

- validação inadequada no backend.
- brute force sem captchas.
- falhas em limites de tentativas.

6.2.2 Mapeamento do formulário

Foi estudado como ocorre o envio de dados do login através de requisições HTTP:

```pgsql
POST /dvwa/login.php
username=<user>&password=<pass>&Login=Login
```

6.2.3 Automação (exemplo conceitual)

O Medusa possui módulo HTTP, mas para fins educacionais também foi considerado o uso de cURL/Hydra.

Exemplo ilustrativo:

```bash
hydra -l admin -P wordlist.txt <IP> http-post-form "/dvwa/login.php:username=^USER^&password=^PASS^:Login failed"
```

(Notar que o comando não gera risco por si só — depende do ambiente controlado.)

O DVWA permitiu avaliar comportamentos de autenticação sem os controles modernos. A ausência de limites de tentativas e CAPTCHA facilita ataques automatizados em ambientes vulneráveis.

6.2.4 Lições aprendidas

- Formulários sem CAPTCHA são alvos fáceis.
- Falta de registro de tentativas impede detecção de ataques.
- Medidas recomendadas:
    - Implementar multifator (2FA).
    - Rate limiting (limite de tentativas).
    - Captchas e WAF.
    - Senhas fortes

6.3 Cenário 3: Password Spraying em SMB + Enumeração de Usuários

6.3.1 O que é Password Spraying?

Diferentemente da força bruta, que tenta muitas senhas para um único usuário, o password spraying:

- Usa uma senha contra muitos usuários.
- Reduz risco de bloqueios de conta.

É uma técnica comum em ataques reais, especialmente contra Active Directory.

6.3.2 Enumeração de usuários (conceito)

Serviços SMB antigos podem dar pistas como:

- Nomes de compartilhamentos.
- Nomes de máquinas.
- Contas padrão expostas.

Ferramentas típicas: *enum4linux, smbmap*.

Exemplo de uso didático:

bash Copiar código

```
enum4linux -a <IP>
```

6.3.3 Password Spraying com Medusa

Exemplo conceitual:

```bash
medusa -h <IP> -U usuarios.txt -p 'Password123' -M smbnt
```

O SMB é amplamente utilizado em redes corporativas. A enumeração de usuários expostos, somada a senhas previsíveis, foi suficiente para simular tentativas de password spraying. Contas padrão devem ser desativadas e monitoradas.

6.3.4 Lições aprendidas

- Contas padrão devem ser desabilitadas.
- Erros de autenticação devem ser registrados.
- Políticas de senha devem ser fortes e únicas.

7. Reflexões Gerais

Durante este desafio, eu pude:

✓ Entender como ataques de autenticação funcionam nos bastidores:

Ferramentas como Medusa facilitam a automatização, deixando claro como senhas fracas são vulneráveis.

✓ Desenvolver visão crítica sobre segurança preventiva:

A defesa começa na configuração:

- autenticação multifator.
- limitação de tentativas.
- monitoramento de logs.
- protocolos seguros (SSH/SFTP ao invés de FTP).

✓ Experimentar ambientes vulneráveis sem riscos:

O Metasploitable 2 mostrou como sistemas mal configurados acumulam brechas.

✓ **Documentar como faria em um ambiente profissional:**

O uso de GitHub para registrar:

- Comandos.
- Resultados.
- Prints de tela.
- Reflexões.

É útil para um portfólio profissional.

8. Recomendações de Mitigação

Rede

- Segmentar ambientes críticos
- Aplicar firewall com regras restritivas
- Monitorar tráfego suspeito

Serviços

- Substituir protocolos inseguros
- Remover serviços desnecessários
- Atualizar sistemas

Contas

- Políticas de senha forte
- MFA
- Bloqueio progressivo
- Auditoria constante

9. Resultados e Discussão

Os resultados demonstraram que serviços sem políticas de autenticação robustas são rapidamente comprometidos. Ataques de força bruta contra FTP obtiveram sucesso utilizando wordlists simples. Já o DVWA evidenciou fragilidades em aplicações web com validação fraca. O password spraying em SMB demonstrou a relevância de políticas de senha forte.

O laboratório evidenciou que vulnerabilidades simples podem resultar em comprometimentos severos. A combinação de serviços mal configurados, políticas inadequadas de senhas e falta de monitoramento cria um cenário propício para ataques. Ambientes corporativos devem aplicar estratégias de defesa em profundidade, com camadas de segurança e políticas maduras.

10. Conclusão

O projeto permitiu compreender, de maneira segura, como ferramentas de auditoria funcionam e por que medidas de defesa são essenciais para qualquer sistema. A prática com Medusa, DVWA e Metasploitable reforçou que vulnerabilidades simples podem se tornar porta de entrada para ataques graves — e que a melhor defesa é a prevenção.

A prática reforçou o entendimento dos riscos relacionados à autenticação e destacou a importância de ferramentas de monitoramento e políticas de segurança robustas. O estudo demonstra como ambientes vulneráveis podem ser explorados, além de reforçar a necessidade de boas práticas e atualizações constantes.

A auditoria prática permitiu compreender na prática os riscos de autenticação fraca, além de demonstrar a eficácia de ferramentas de automação ofensiva. Tais testes reforçam a necessidade de monitoramento contínuo, políticas de segurança robustas e treinamentos recorrentes.

11. Referências

1. BRANCO, Rodrigo. **Ataques e Defesa em Redes.** São Paulo: Novatec, 2019.

2. KIM, David; SOLOMON, Michael. **Fundamentals of Information Systems Security.** Jones & Bartlett, 2018.

3. OWASP. **OWASP Testing Guide.** Disponível em: https://owasp.org.