

05

Wordlists

Transcrição

Na última aula inserimos manualmente possíveis nomes de usuários e senhas e tivemos sorte em descobrir uma combinação válida.

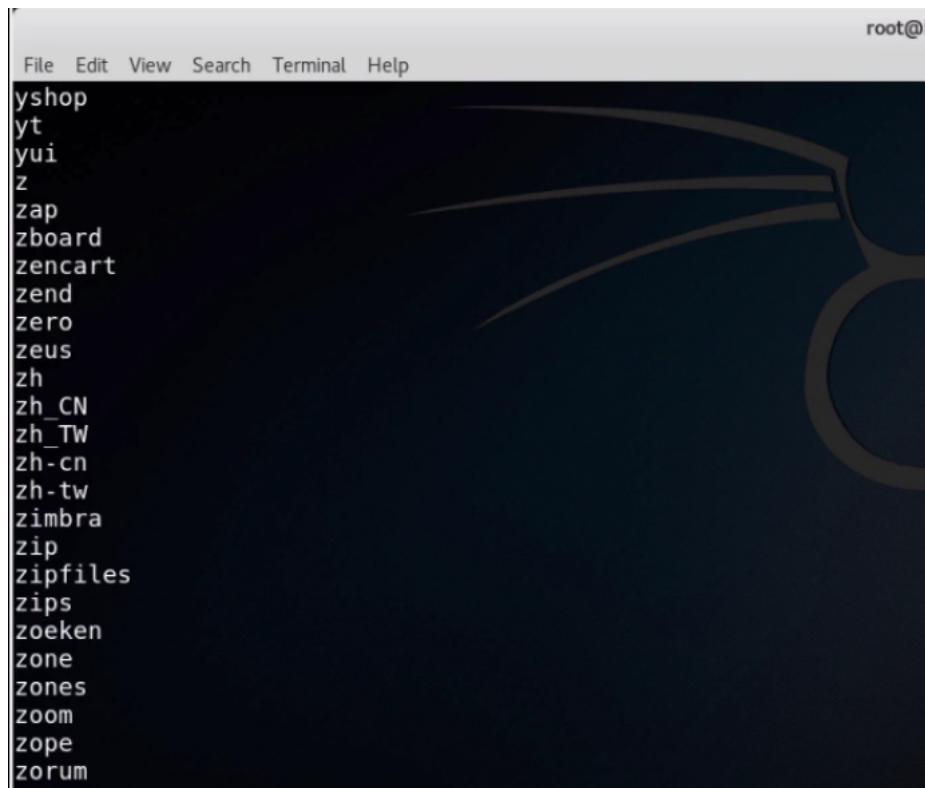
Para nos auxiliar, existem as *word lists*, listas que contêm diversas palavras para nomes e senhas comumente utilizadas e compiladas, dessa maneira, as chances de um ataque bem sucedido aumentam. O próprio Kali Linux possui algumas listas internas, portanto, escrevendo no Terminal, `locate /wordlists`, teremos uma grande quantidade de listas:

```
root@kali:~# locate /wordlists
/usr/share/wordlists
/usr/share/dirb/wordlists
/usr/share/dirb/wordlists/big.txt
/usr/share/dirb/wordlists/catala.txt
/usr/share/dirb/wordlists/common.txt
/usr/share/dirb/wordlists/euskera.txt
/usr/share/dirb/wordlists/extensions_common.txt
/usr/share/dirb/wordlists/indexes.txt
/usr/share/dirb/wordlists/mutations_common.txt
/usr/share/dirb/wordlists/others
/usr/share/dirb/wordlists/small.txt
/usr/share/dirb/wordlists/spanish.txt
/usr/share/dirb/wordlists/stress
/usr/share/dirb/wordlists/vulns
/usr/share/dirb/wordlists/others/best1050.txt
/usr/share/dirb/wordlists/others/best110.txt
/usr/share/dirb/wordlists/others/best15.txt
/usr/share/dirb/wordlists/others/names.txt
/usr/share/dirb/wordlists/stress/alphanum_case.txt
/usr/share/dirb/wordlists/stress/alphanum_case_extra.txt
/usr/share/dirb/wordlists/stress/char.txt
/usr/share/dirb/wordlists/stress/doble_uri_hex.txt
/usr/share/dirb/wordlists/stress/test_ext.txt
/usr/share/dirb/wordlists/stress/unicode.txt
/usr/share/dirb/wordlists/stress/uri_hex.txt
/usr/share/dirb/wordlists/vulns/apache.txt
```

Um dos arquivos acima é o `wordlists/common.txt`. Para verificar o que existe nessa lista escrevemos:

```
cat wordlists/common.txt
```

Teremos:



A screenshot of a terminal window titled 'root@kali' at the top right. The window has a dark background with a stylized cat logo on the right side. The menu bar at the top includes 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The main area of the terminal displays a list of words, likely a wordlist for a brute-force attack, including:

```
yshop  
yt  
yui  
z  
zap  
zboard  
zencart  
zend  
zero  
zeus  
zh  
zh_CN  
zh_TW  
zh-cn  
zh-tw  
zimbra  
zip  
zipfiles  
zips  
zoeken  
zone  
zones  
zoom  
zope  
zorum
```

Quanto maior a lista, maior a chance de sucesso no ataque!

O problema dessa estratégia é que alguns sistemas mais elaborados disponibilizam um número de tentativas para login limitado, justamente, para prevenir um site desse tipo de ataque.

Buscando na internet as palavras-chaves *wordlist brute force download* encontramos diversas listas disponíveis em fóruns e sites da internet. Além das listas mencionadas existem algumas que fazem referência a empresas específicas, mas dificilmente elas existem pré-prontas. Por exemplo, nós estamos no site *OWASP Multillidae*, portanto, é possível que exista uma senha ou usuário que estejam relacionados a palavra *Multillidae*, palavra que dificilmente encontraremos inclusa em alguma lista já pronta.

Assim, existe uma lista que pode ser elaborada através de uma pesquisa no próprio site. Para nos ajudar nisso existe a ferramenta, **Cewl**. Abrimos o terminal do Kali Linux e digitamos `cewl` e passamos a URL do site, "`http://192.168.1.37/multilidae/`" e, ainda, acrescentamos `-d 1`, pois isso delimita o nível de profundidade da pesquisa. Quanto maior o número, maior é a quantidade de valores que ele pesquisará. Teremos:

```
> cewl "http://192.168.1.37/multilidae/" -d 1
```

A página será mapeada e a partir dela construída uma lista baseada na realidade dessa empresa!

root@kali: ~

```
File Edit View Search Terminal Help
```

```
root@kali:~# cewl "http://192.168.1.37/mutillidae/" -d 1
CeWL 5.2 (Some Chaos) Robin Wood (robin@digi.ninja) (https://digi.ninja/)

User
the
Info
Injection
Lookup
HTML
File
Viewer
SQL
Test
Via
page
OWASP
Pen
PHP
php
XPath
Web
```