FICHA TRABALHO 4

MODALIDADE:	Aprendizagem +	Não aplicável	
CURSO:	Técnico de Cibersegurança		
UFCD:	Instalar e configurar ferramentas de análise e recolha de logs e evidências	CÓDIGO UFCD:	UC01485
FORMADOR/A:	Bruno Silva	DATA:	

OBJETIVOS

- Entender como funcionam os ataques de phishing
- Saber como usar ataques de força bruta e dicionários de palavras-passe com a aplicação John the Reaper (Kali Linux)

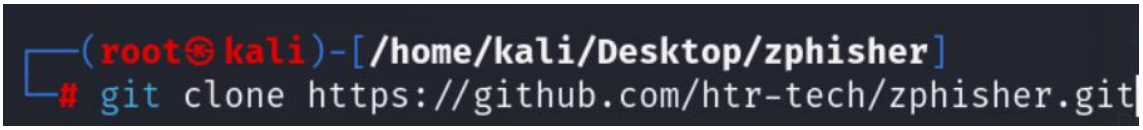
Parte 1 - Ataques de phising

Vamos construir uma rede social false (phising) para ver e compreender o vetor de ataque. Para tal, vamos realizar os seguintes passos:

1. Criar uma página de rede social falsa (como por exemplo um Facebook, linkedin, etc, onde vão ter um formulário com campos de introdução de informação)
2. O utilizador vai colocar os dados nesse formulário (do qual pensa que é verdadeiro);
3. Quando este submeter a informação no formulário, o atacante vai receber a informação e o utilizador vai ver uma página que a informar que algo aconteceu de errado ou que não conseguiu fazer o login na plataforma;

Este tipo de ataque é conhecido como **Sequestro de credenciais** que é uma variante de ataque por engenharia social.

1. Abra um terminal e faça login como root (isso é extramente vital para funcionar sem restrições);
2. Deve estar localizado na pasta Documents. Se ainda não está, deve aceder ao mesmo (cd Documents);
3. Fazer o clone do projeto zphisher. Coloque no terminal o comando:
   git clone https://github.com/htr-tech/zphisher.git



4. Entre dentro da pasta que clonou (cd zphisher) e liste o conteúdo da pasta de forma detalhada (comando ls -l);

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# cd zphisher

┌──(root㉿kali)-[/home/kali/Desktop/zphisher]
└─# ls -l
total 96
-rw-r--r-- 1 root root   187 Mar  3 14:53 Dockerfile
-rw-r--r-- 1 root root 35149 Mar  3 14:53 LICENSE
-rw-r--r-- 1 root root  7145 Mar  3 14:53 README.md
drwxr-xr-x 2 root root  4096 Mar  3 15:08 auth
-rwxr-xr-x 1 root root  1509 Mar  3 14:53 make-deb.sh
-rwxr-xr-x 1 root root   812 Mar  3 14:53 run-docker.sh
drwxr-xr-x 2 root root  4096 Mar  3 14:53 scripts
-rwxr-xr-x 1 root root 30928 Mar  3 14:53 zphisher.sh
```

5. Vamos tentar executar o programa executando o comando: ***./zphisher.sh***

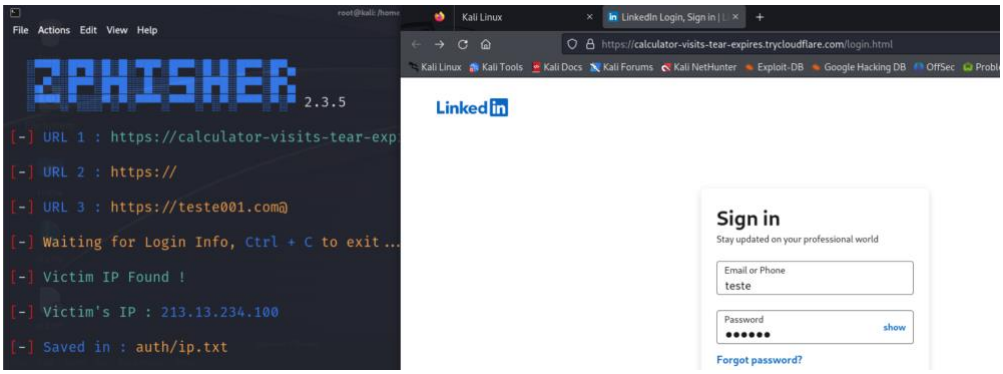
Nota Importante: Se der o erro "**permission denied**", temos de dar permissões para executar o programa. Como tal, insira o comando ***chmod 777 zphisher.sh***

De seguida, execute novamente o comando da aplicação:

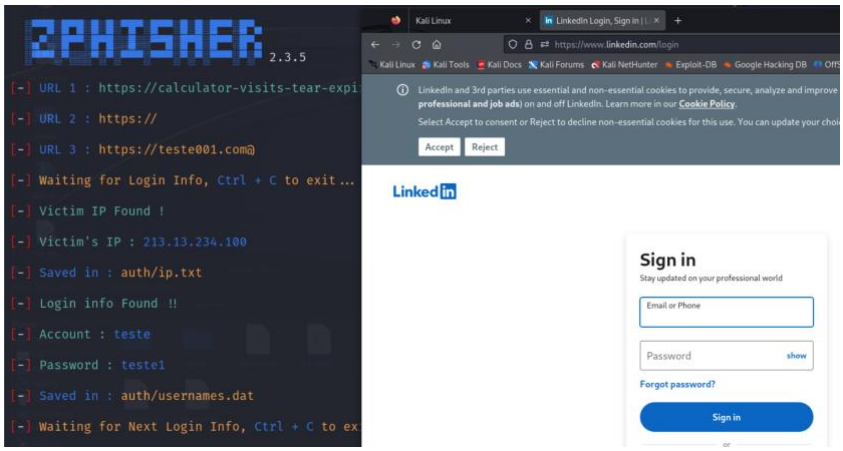
6. Agora selecionar a opção 1 (para criar uma página facebook) e pedir para criar o serviço na cloudefare (normalmente opção 2, para não ficar no servidor local):

7. Peça para não criar nenhum nome específico e de seguida temos o nosso serviço disponibilizado online (basta aceder ao link que foi disponibilizado e ver os registos na linha de comandos):

E assim temos a nossa página de pishing:



Depois de inserir a password, este volta a recarregar a página, mas, agora coloca o link verdadeiro da página para enganar o utilizador:



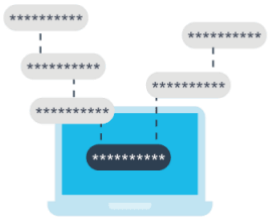
Parte 2 – John The Reaper (rar2john e rzr2zip)

Para fazer a autenticação nos websites e aplicações utilizamos um nome de utilizador e uma palavra-chave, que é uma das formas mais populares de autenticação nos websites, mas também podem ser aplicados para descobrir senhas de ficheiros compactados por password, de logins, entre outros.

Dois dos métodos mais famosos são:

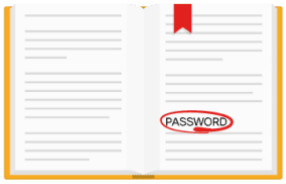
1 – Brute-Force Attacks

A maneira mais simples de obter acesso a um website protegido por senha são os ataques de força bruta, que fazem com que um atacante use todas as combinações possíveis de letras, números e símbolos até acertar a senha.



2 – Dictionary Attacks

Um atacante tenta sistematicamente cada palavra de um dicionário com as senhas mais utilizadas e outras combinações, na tentativa de invadir uma conta protegida por senha.



Descobrir passwords ficheiros rar/zip

- Para trabalhar com os ficheiros compactados em WIN RAR usar ***rar2john***
- Para trabalhar com os ficheiros compactados em ZIP usar ***rar2zip***

Nota importante 1: deve abrir o terminal e entrar em modo de administrador root;

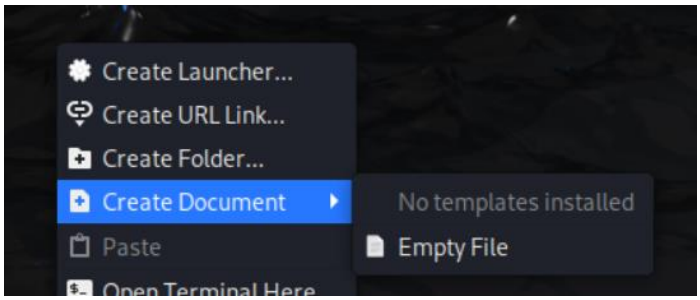
Nota importante 2: Verificar se o programa tem lista de passwords pré-definida. Se não tiver aceda a hiperligação: https://github.com/danielmiessler/SecLists/blob/master/Passwords/Software/john-the-ripper.txt em copie e abra o ficheiro que está na diretoria ***/usr/share/John/password.lst*** e cole os dados. Não esqueça de gravar o ficheiro com os novos dados.

Quando tentar descobrir os dados/passwords, pode indicar uma outra lista de passwords, indicando sempre que possível a localização da mesma antes de realizar o ataque:

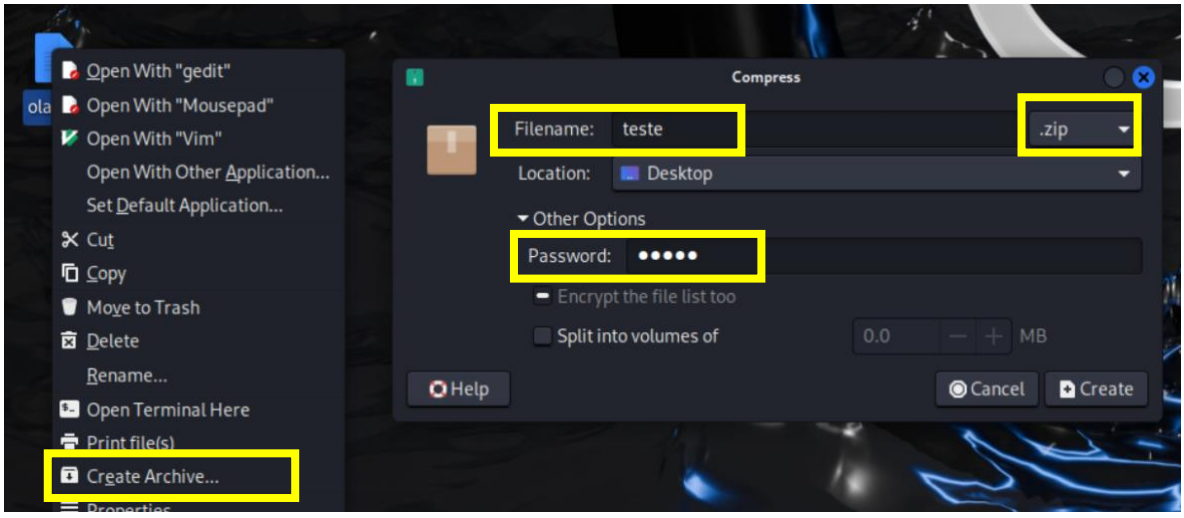
```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# john --wordlist=/usr/share/john/password.lst teste2.txt
```

Nota importante 3: Existem websites dedicados para verificar passwords e a medida que testa, guarda no repositório de informação. Um desses websites é o https://haveibeenpwned.com/Passwords

1. Crie 1 ficheiro de texto com o nome “ola.txt” e coloque alguma informação. Não esqueça de guardar a informação do ficheiro;



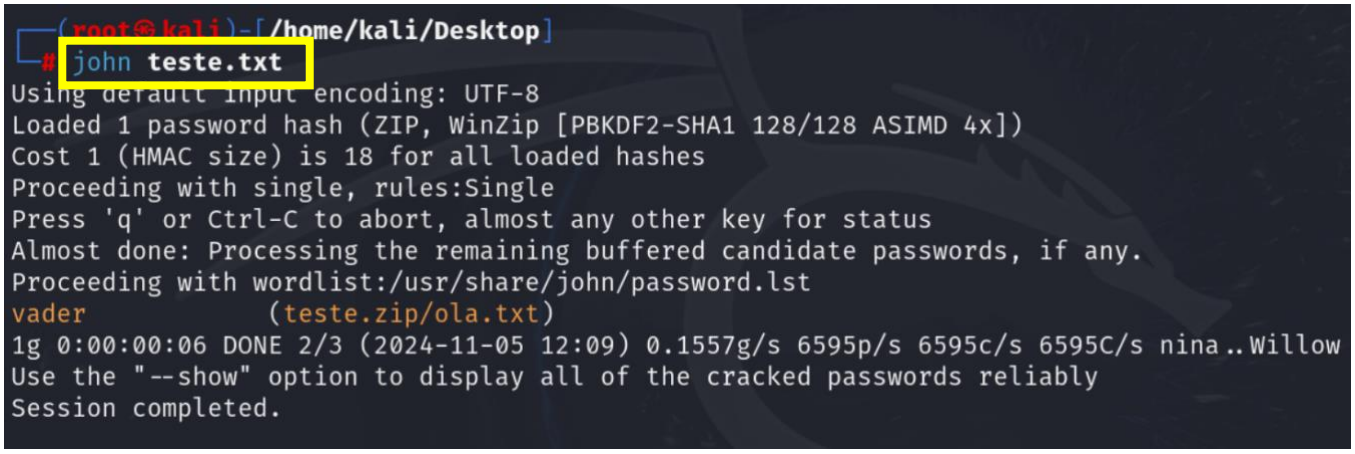
2. Faça a compactação do ficheiro em formato ZIP com o nome “teste”, com a extensão .zip, e clique na opção “Other options” para definir a password “vader”;



3. Vamos ao terminal e coloque a seguinte instrução: ***zip2john teste.zip > teste.txt*** para obter as informações internas da compactação do ficheiro

Resultado:

4. Testar o ataque e verificar o resultado com o comando: john teste.txt



5. Se já utilizou o passo 4, pode ver o histórico do que foi feito com o comando: **john teste.txt --show**