HackerDivulgation.com

DOCS

CUPP

Para explicar mejor el funcionamiento de esta herramienta se preparó un lab donde se simula que se tienen datos del administrador de un servidor ftp de una empresa. Estos datos se obtuvieron mediante técnicas de OSINT, se tienen sus nombres, username habitual, fecha de nacimiento; de la misma manera se tienen los datos de su esposa. Al investigar su vida en redes sociales se identificó que tomo varias fotos celebrando el ingreso a su nuevo trabajo, para fortuna en una de ellas se veía su terminal con el usuario ftp que resultó ser **ftpadmin**. Con esto se puede llegar a la conclusión de que es una persona muy despistada por lo que puede haber utilizado datos personales como su nombre o fecha de cumpleaños para su contraseña del usuario ftp.

Proyecto: CUPP-Common User Password Profiler - Github

Contenido

Instalación

Clonar el repositorio del proyecto.

```
sudo git clone https://github.com/Mebus/cupp.git
```

Ingresar al directorio.

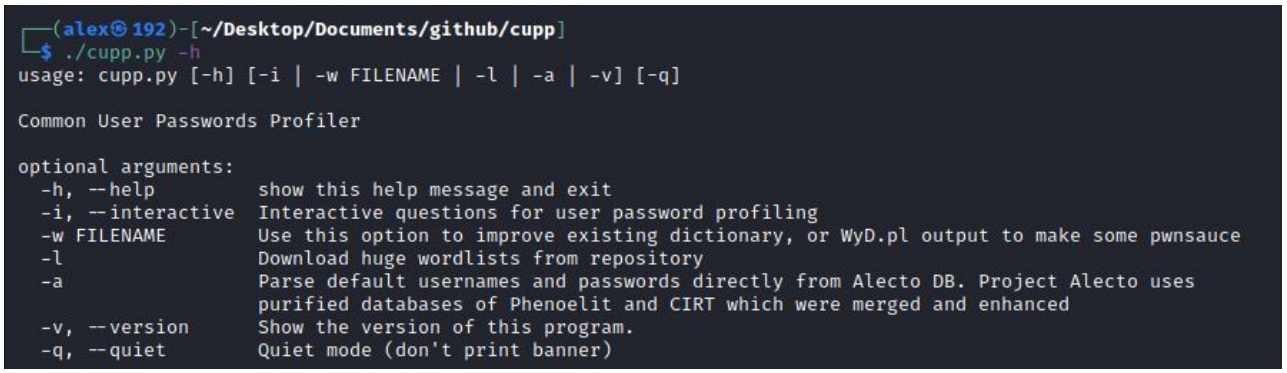
```
cd cupp/
```

Ejecutar el programa escrito en Python.

```
./cupp.py
```

Mostrar la ayuda del programa.

```
./cupp.py -h
```



USO

Con esta herramienta (*CUPP*) se generan las posibles contraseñas con los datos previamente recopilados mediante técnicas de OSINT e ingeniería social.
Con el argumento `-i` se ejecuta el programa, se deben ir colocando los datos según se soliciten.

```
./cupp.py -i
```

Hydra

Cuando se termina de colocar todos los datos se generará un archivo .txt en el directorio del programa donde estarán todas las contraseñas generadas. Con este archivo se puede realizar un ataque de fuerza bruta usando Hydra que es una herramienta preinstalada en Kali Linux.
Para esta herramienta seguir la siguiente sintaxis.

```
hydra -l ftpadmin -P passlist.txt ftp://IP_TARGET
```

En este caso se asume que se conoce el nombre de usuario, este parámetro se especifica con `-l`. En el parámetro `-P` se coloca la ruta del archivo .txt con las contraseñas generadas. Al final se coloca la dirección del objetivo, en este caso se trata de un servidor FTP.

Verificación

En caso de que el ataque de fuerza bruta sea exitoso, se mostrará la contraseña correcta y se detendrá el programa. Para ingresar al servidor y validar las credenciales obtenidas se hará lo siguiente.
Con la herramienta cliente `ftp` se puede acceder al servidor.

```
ftp IP_TARGET
```

Escribir el nombre de usuario.

```
ftpadmin
```

Escribir la contraseña obtenida con CUPP y validada por Hydra.

```
Alaor097610
```

Si todo se hizo correctamente se obtendrá acceso al servidor FTP.

Video

Video en YouTube donde se puede ver el funcionamiento de todas las herramientas en conjunto.

https://www.youtube.com/watch?v=17Jvn3fdiXs

Referencias

1. Repositorio del proyecto en Github. https://github.com/Mebus/cupp
2. Proyecto de Hydra. https://github.com/vanhauser-thc/thc-hydra