https://github.com/danialsfy

INTRODUCTION TO PASSWORD CRACKING

by

Danial Wajdi

CONTENTS

INTRODUCTION

- A password is a string of characters used to verify a user's identity and grant access to systems, applications, or data.

- A combination of letters, numbers, and symbols in a string for identity validation

- Linux - /etc/shadow
  Windows - C:\Windows\System32\config

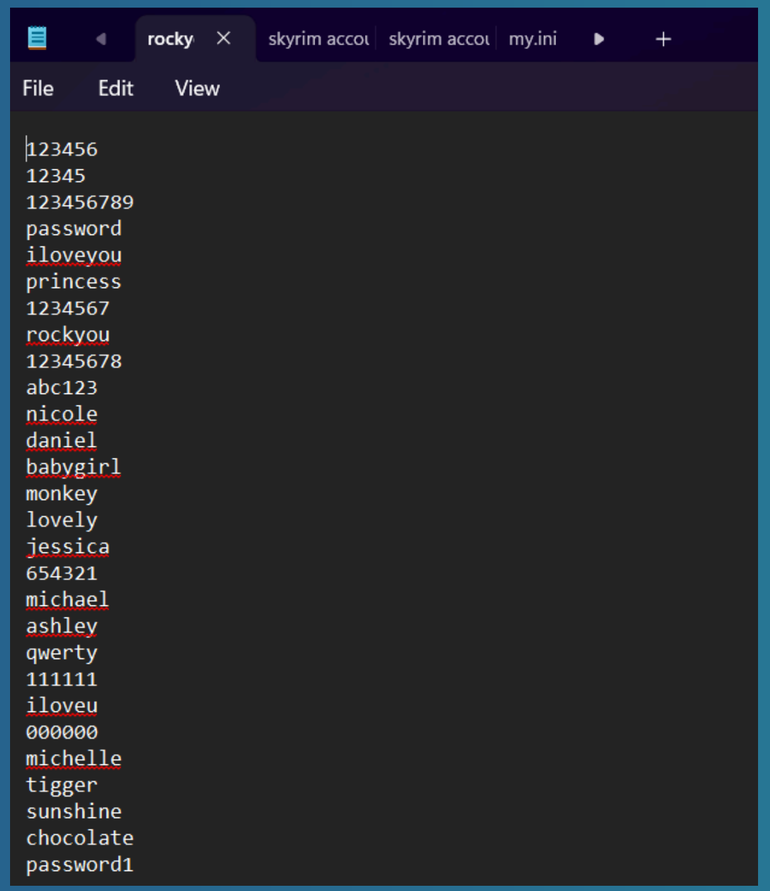
- Apply salt to prevent rainbow table attack

INTRODUCTION

- Time taken if use brute-force attack

Length of Password (Chars)	Only Numbers	Mixed Lower and Upper case alphabets	Mixed numbers, Lower and Upper case aplhabets	Mixed numbers, Lower and Upper case aplhabets , symbols
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	3 secs	10 secs
6	Instantly	8 secs	3 mins	13 mins
7	Instantly	5 mins	3 hours	17 hours
8	Instantly	3 hours	10 days	57 days
9	4 secs	4 days	153 days	12 years
10	40 secs	169 days	1 year	928 years
11	6 mins	16 years	106 years	71k years
12	1 hour	600 years	6k years	5m years
13	11 hours	21k years	108k years	423m years
14	4 days	778k years	25m years	5bn years
15	46 days	28m years	1bn years	2tn years
16	1 year	1bn years	97bn years	193tn years
17	12 years	36bn years	6tn years	14qd years
18	126 years	1tn years	374tn years	1qt years

- Dictionary attack



UNDERSTANDING THE HASHES

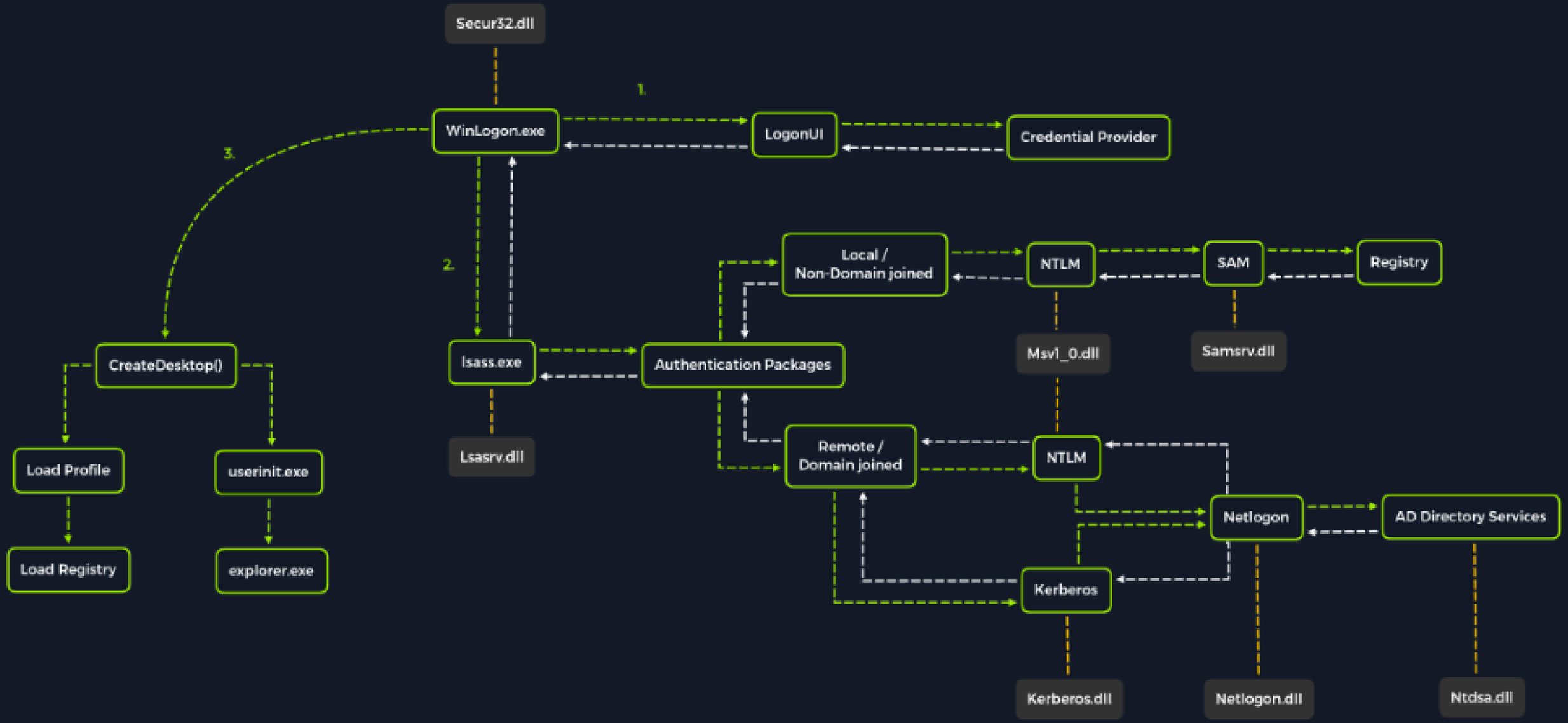
- /etc/shadow file format in kali linux

```
<username>:  <encrypted password>:  <day of last change>:  <min age>:  <max age>:  <warning period>:  <inactivity period>:  <expiration date>:  <reserved field>
```

```
kali:$y$j9T$ufXTBpN1QpgwlgqRFmb/B0$/.y0ybAF4iNQXniErsDWf9QSl2HZH7LnBeRHB4ZiQa9:20057:0:99999:7:::
```

ID	Cryptographic Hash Algorithm
1	MD5
$2a$	Blowfish
5	SHA-256
6	SHA-512
$sha1$	SHA1crypt
y	Yescrypt
gy	Gost-yescrypt
7	Scrypt

Windows Authentication Process



ATTACKER PERSPECTIVE

- On Linux, hashes are stored in /etc/shadow, accessible with root privileges.
- On Windows, password hashes are stored in the SAM file and can be extracted using tools like Mimikatz, secretsdump.py, or pwdump.
- On websites or apps, SQL injection or other vulnerabilities may reveal password hashes from databases.
- In breach scenarios, hackers may find publicly leaked password files or breach dumps.

PASSWORD CRACKING

- Process of converting a password hash back into the original plaintext password
- Offline : using stolen hash
- Online : repeatedly attempting logins
- Brute force, dictionary, rule-based

CRACKING TOOLS

John the Ripper

John is a fast, flexible, and easy-to-use password cracker. It works best for offline cracking and supports many hash types.

Hashcat

Hashcat is a powerful, GPU-accelerated password cracker known for its speed and flexibility. It supports over 300 hash types.

Hydra

Hydra is used for online brute force attacks on protocols like SSH, HTTP, FTP, and RDP.

JOHN THE RIPPER

Create a file

echo 'test:6P8qDneqBlAbONnLZ$nsIJldGytkaCT1pV6MWRl5QMYITKAhO2BvbobzGw1hy7.RJoveHwudF.dLKPuq0oBGpKAq8dN.9gHFPsskqzu0:0:0:99999:7:::' > test.txt

Run John

john --wordlist=/usr/share/wordlists/rockyou.txt test.txt

Show cracked password

john --show test.txt

Expected Output

test:123456:0:0:99999:7:::

HYDRA

Create a user

sudo adduser testuser
# Set password to 123456

Start SSH Service

sudo systemctl start ssh

Run Hydra

hydra -l testuser -P /usr/share/wordlists/rockyou.txt ssh://127.0.0.1

Expected Output

[22][ssh] host: 127.0.0.1 login: testuser password: 123456

HASHCAT

Create a hash file

5f4dcc3b5aa765d61d8327deb882cf99

Basic Dictionary Attack

hashcat -m 0 -a 0 hash.txt /usr/share/wordlists/rockyou.txt

Dsiplay Cracked Hash

hashcat -m 0 -a 0 hash.txt /usr/share/wordlists/rockyou.txt --show

Expected output

5f4dcc3b5aa765d61d8327deb882cf99:password

DEFENSE MITIGATIONS

Strong Password

Use long, random, and unique passwords.

Multi-factor Authentication

Adds a second layer (like SMS or app token) that passwords alone cannot bypass.

Rate Limiting

Protect online services from brute force attempts.

THANK YOU!