**🧠 1. WMIExec.py Nedir?**

**WMIExec.py**, Impacket araç setinin bir parçasıdır ve Windows sistemlerde **WMI (Windows Management Instrumentation)** protokolü üzerinden **uzak komut çalıştırma** imkânı sunar.

📌 SMB portu (TCP 445) üzerinden çalışır, hedef sistemde **administrative share (ADMIN$)** erişimi gerektirir.

**🎯 2. Ne İşe Yarar?**

| **Amaç** | **Açıklama** |
| --- | --- |
| ⚙️ Uzak Windows komutu | Hedef Windows sistemde komut çalıştırır |
| 📤 Komut çıktısını alır | stdout çıktısını çekip gösterir |
| 🧭 Lateral movement | Ağa sızıldıktan sonra yatay ilerleme |
| 🧪 Pentest / Red Team | İç ağ güvenliği testlerinde kullanılır |
| 🔒 NTLM auth ile çalışır | Kullanıcı adı/parola veya hash ile bağlantı kurabilir |

**⚙️ 3. Kurulum (Kali Linux / Impacket)**

**✅ 1. Impacket'i klonla ve kur:**

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**🚀 4. Kullanım Komutu**

**✅ Kullanıcı adı & parola ile:**

python3 wmiexec.py DOMAIN/USERNAME:PASSWORD@TARGET-IP

**✅ Hash ile (Pass-the-Hash):**

python3 wmiexec.py DOMAIN/USERNAME@TARGET-IP -hashes LMHASH:NTHASH

**📋 5. Örnek Kullanım**

python3 wmiexec.py WORKGROUP/administrator:Admin123@192.168.1.5

Terminal çıktısı:

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**🔄 6. Alternatiflere Göre Farkı**

| **Özellik** | **WMIExec.py** | **PsExec.py** | **SMBExec.py** |
| --- | --- | --- | --- |
| 🖥️ WMI kullanır | Evet | Hayır | Hayır |
| 📂 Disk yazmaz | Evet (fileless) | Hayır | Hayır |
| 🧭 Network görünürlüğü | Düşük | Orta | Düşük |
| 🔐 AV tespiti | Daha az tespit edilir | Daha fazla | Daha az |

**🔒 7. Gereksinimler**

* Hedef Windows sistemde **WMI servisi (Winmgmt)** açık olmalı
* Kullanılan hesap **admin yetkili** olmalı
* SMB (port 445) açık olmalı
* Windows Defender tarafından tespit edilme riski düşüktür ancak yine de **yasal kullanım şarttır**

**🎯 8. Öğrenim Kazanımları**

* Windows sistemlerde uzaktan komut çalıştırma mantığını öğrenme
* WMI protokolü ile yönetimsel işlemleri kavrama
* Impacket araçlarını tanıma ve iç ağda ilerleme tekniklerini öğrenme
* Red Team operasyonlarının uygulamalı temellerini anlama