**🎯 1. Fauxpersky Nedir?**

**Fauxpersky**, adını ünlü antivirüs yazılımı "Kaspersky"den esinlenerek almış, **sahte antivirüs görünümüne sahip bir keylogger** (tuş kaydedici) yazılımıdır.

📌 Özellikleri:

* Kullanıcıdan şüphe uyandırmadan çalışır
* GUI (grafik arayüz) ile antivirüs gibi davranır
* Arka planda tuş girişlerini kaydeder
* Python ile yazılmıştır
* Saldırgan bakış açısıyla “social engineering” + “malware” birleşimidir

**🔍 2. Ne İşe Yarar?**

| **Özellik** | **Açıklama** |
| --- | --- |
| 🎭 Antivirüs gibi görünür | Kurbanın şüphelenmesini önler |
| ⌨️ Keylogger işlevi | Girilen tuşları .txt dosyasına kaydeder |
| 🧪 Eğitim amaçlı | Social engineering ve zararlı yazılım analizi konularında kullanılır |
| 📦 Taşınabilir yapı | Tek bir Python dosyasıyla çalışır |
| 🛑 Antivirüsler tarafından tespit edilebilir | Amaç, bu tespit süreçlerini de öğretmektir |

**⚙️ 3. Kurulum (Kali veya Windows Üzerinden Hazırlık)**

Kali üzerinden hazırlanır, hedef sisteme (Windows) atılır.

**✅ 1. Gerekli kütüphaneler:**

pip3 install pynput pyinstaller

**✅ 2. Aracı GitHub’dan indir:**

ekran görüntüsü, metin, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.**✅ 3. .py dosyasını .exe haline getirme:**

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

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.Çıktı: dist/Fauxpersky.exe

Bu .exe dosyası hedef Windows sistemine taşınarak çalıştırılır.

**🚀 4. Kullanım**

**✅ 1. Hedef sistemde çalıştır:**

Fauxpersky.exe

* Kullanıcı, bir antivirüs arayüzüyle karşılaşır.
* Arka planda girilen tuşlar log.txt dosyasına kaydedilir.

**✅ 2. Log dosyasına erişim:**

C:\Users\victim\Documents\log.txt

Ya da: .exe ile aynı dizinde oluşur.

**📋 5. Örnek Terminal ve GUI Görünümü**

[\*] Fauxpersky launched...

[\*] Key logging started...

[\*] Log file updated: log.txt

👀 GUI ekranında “Fauxpersky Antivirus is active” gibi uydurma bir antivirüs arayüzü görüntülenir.

**🧠 6. Eğitim Amaçlı Kullanımı**

| **Alan** | **Açıklama** |
| --- | --- |
| 🧪 Malware eğitimi | Keylogger nasıl çalışır, nasıl gizlenir? |
| 🛡️ Blue Team eğitimi | AV tespiti, behavioral analysis |
| 👁️ Social Engineering | Kurbanı kandırarak zararlıyı çalıştırma senaryoları |
| 🧰 Red Team simülasyonları | Zararlı yazılım analizi üzerine teknik uygulamalar |

**🎯 7. Öğrenim Kazanımları**

* Keylogger mantığını teknik olarak kavrama
* PyInstaller ile Python dosyalarını zararlı formatlara çevirme
* GUI + zararlı mantığını birleştiren social engineering örneği
* Antivirüs tespiti ve AV bypass üzerine temel farkındalık
* Güvenli yazılım kullanımının neden önemli olduğunu anlama