**🧠 1. InSpy Nedir?**

**InSpy**, LinkedIn üzerinde arama yaparak bir şirkete ait çalışan, görev ve teknolojileri bulmaya yarayan **Python tabanlı bir OSINT aracıdır**.

* Şirketin çalışan listesi
* Çalışanların pozisyon ve görevleri
* Kullanılan teknolojiler (IT, yazılım, framework)

📌 Bu bilgiler özellikle **sosyal mühendislik saldırıları**, **phishing** ve **recon aşaması** için değerlidir.

**🎯 2. Ne İşe Yarar?**

| **Özellik** | **Açıklama** |
| --- | --- |
| 👤 Çalışan listesi çıkarma | LinkedIn üzerinden şirket çalışanlarını listeler |
| 📋 Görev/pozisyon bilgisi | Çalışanların rolleri ve departman bilgileri |
| 💻 Teknoloji tespiti | Profil bilgilerinden kullanılan teknolojileri belirleme |
| 🧠 OSINT veri toplama | Hedef şirket hakkında pasif bilgi toplama |

**⚙️ 3. Kurulum (Kali / Linux)**

**✅ 1. GitHub’dan indirme:**

git clone https://github.com/leapsecurity/InSpy.git

cd InSpy

**✅ 2. Bağımlılıkları yükleme:**

pip3 install -r requirements.txt

Python 3 kullanılması önerilir.

**🚀 4. Kullanım Komutları**

**✅ 1. Şirket çalışanlarını bulma:**

python3 inspy.py --emps "CompanyName"

**✅ 2. Belirli unvana göre arama:**

python3 inspy.py --emps "CompanyName" --title "Security Engineer"

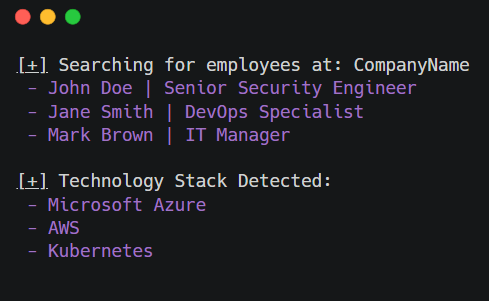
**✅ 3. Teknoloji bilgisi toplama:**

python3 inspy.py --tech "CompanyName"

**✅ 4. Çıktıyı dosyaya kaydetme:**

python3 inspy.py --emps "CompanyName" --outfile results.txt

**📋 5. Örnek Terminal Çıktısı**

****

**🧠 6. Kullanım Senaryoları**

| **Senaryo** | **Açıklama** |
| --- | --- |
| 🕵️‍♂️ Sosyal mühendislik | Phishing e-posta listesi hazırlama |
| 🛡️ Red Team ön keşif | Hedefte kullanılabilecek teknolojileri öğrenme |
| 🧠 OSINT araştırması | Şirket yapısını anlamak |
| 📊 Kurumsal risk analizi | Açık kaynakta ne kadar bilgi sızdığını görmek |

**🎯 7. Öğrenim Kazanımları**

* LinkedIn tabanlı OSINT tekniklerini öğrenme
* Hedef şirketin çalışan yapısını çıkarma
* Kullanılan teknolojileri analiz etme
* Sosyal mühendislik öncesi pasif bilgi toplama
* Python tabanlı OSINT araçlarının kullanımına hakimiyet