**🧠 1. Pwnagotchi Nedir?**

**Pwnagotchi**, WPA/WPA2 kablosuz ağlardan **el sıkışma (handshake)** paketlerini otomatik olarak toplayan, **yapay zekâ tabanlı** bir pentest cihazıdır.

* Raspberry Pi Zero W gibi küçük cihazlarda çalışır
* AI algoritmaları ile ağ keşfi ve handshake toplama optimizasyonu yapar
* Toplanan handshake’ler daha sonra **Hashcat, Aircrack-ng** gibi araçlarla kırılabilir

📌 Adını “Tamagotchi”den alır, cihaz öğrenmeye devam ettikçe “daha güçlü” hale gelir.

**🎯 2. Ne İşe Yarar?**

| **Özellik** | **Açıklama** |
| --- | --- |
| 📡 WPA/WPA2 handshake toplama | Kablosuz ağlardan el sıkışma paketlerini yakalar |
| 🧠 AI tabanlı öğrenme | Hangi ağlardan veri toplanacağını optimize eder |
| 📊 Ağ analizi | SSID, BSSID, sinyal gücü, şifreleme türü bilgileri |
| 🛠️ Offline parola kırma hazırlığı | Toplanan handshake dosyaları ile parola kırma |

**⚙️ 3. Donanım Gereksinimleri**

* **Raspberry Pi Zero W** veya Pi 3/4
* microSD kart (en az 8 GB)
* Uyumlu WiFi adaptörü (monitor mode + packet injection destekli)
* E-ink ekran (isteğe bağlı)
* Güç kaynağı (Powerbank vb.)

**🛠️ 4. Kurulum (Raspberry Pi)**

**✅ 1. Pwnagotchi imajını indir:**

* https://pwnagotchi.ai/ adresinden en güncel imajı indirin

**✅ 2. microSD karta yazın:**

sudo dd if=pwnagotchi.img of=/dev/sdX bs=4M status=progress

**✅ 3. config.toml dosyasını düzenleyin:**

* WiFi adaptör ayarları
* Cihaz ismi
* Mod (manual / auto / AI)

**✅ 4. Cihazı başlatın:**

* Raspberry Pi’yi güç kaynağına bağlayın
* E-ink ekranda durum bilgileri görünecektir

**🚀 5. Kullanım Modları**

| **Mod** | **Açıklama** |
| --- | --- |
| **Manual** | Sadece komut ile handshake toplar |
| **Auto** | Sürekli ağ taraması yapar ve handshake yakalar |
| **AI** | Öncelikli hedefleri seçerek en verimli handshake toplamayı sağlar |

**📋 6. Örnek Terminal Çıktısı**

ekran görüntüsü, metin, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**🧠 7. Kullanım Senaryoları**

| **Senaryo** | **Açıklama** |
| --- | --- |
| 🔍 WiFi güvenlik testi | WPA/WPA2 parola gücünü ölçmek |
| 🧪 Red Team saha çalışmaları | Hedef ağlardan handshake toplama |
| 🛡️ Blue Team farkındalığı | Kablosuz ağ güvenliğini iyileştirme |
| 📚 Eğitim ortamı | Aircrack-ng ve Hashcat uygulamaları için veri sağlama |

**🎯 8. Öğrenim Kazanımları**

* Kablosuz ağ güvenliğinin temellerini öğrenme
* WPA/WPA2 handshake mantığını kavrama
* AI destekli ağ keşif optimizasyonunu anlama
* Raspberry Pi üzerinde güvenlik test aracı çalıştırma