**🕵️‍♂️ Ghost Phisher Nedir?**

**Ghost Phisher**, Python ile yazılmış bir sosyal mühendislik aracıdır.  
Kali Linux gibi dağıtımlarda yer alan bu araç sayesinde:

* Sahte Wi-Fi erişim noktaları (Fake AP),
* Sahte giriş sayfaları,
* DNS spoofing,
* DHCP sunucusu oluşturma,
* ARP poisoning gibi birçok saldırı senaryosu denenebilir.

Ghost Phisher, GUI (grafiksel arayüz) ile çalışır ve kullanıcı dostu bir ortam sunar. Siber güvenlik eğitimlerinde **sosyal mühendislik ve ağ güvenliği farkındalığı** için kullanılır.

**🔧 Ghost Phisher Kurulumu**

Kurulumu oldukça kolaydır. Kali Linux’un eski sürümlerinde ön yüklü olabilir ancak yeni sürümlerde manuel kurulum yapılmalıdır.

**>>>>>>>Kali Linux Kurulum Komutları:<<<<<**

*sudo apt-get update*

*sudo apt-get install python-qt4*

*git clone https://github.com/savio-code/ghost-phisher.git*

*cd ghost-phisher*

*sudo python ghost-phisher.py*

metin, ekran görüntüsü, yazılım, multimedya yazılımı içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**🛠️ Ghost Phisher Kullanımı ve Tüm Modüller (Parametre Eşdeğeri)**

**✅ 1. Fake Access Point (Sahte Erişim Noktası)**

👉 Sahte bir Wi-Fi ağı oluşturur.  
**Kullanım:**

* Interface: Kablosuz ağ arayüzünü seç (örneğin: wlan0)
* ESSID: Yayın adı belirle (örneğin: “Ücretsiz WiFi”)
* Start AP: Başlat

Kullanım amacı: Hedefi kendi sahte ağına çekmek.

**✅ 2. HTTP Phishing Server (Sahte Sayfa Hosting)**

👉 Sahte giriş sayfalarını barındırır.  
**Alanlar:**

* IP address: Sunucunun yerel IP’si (genellikle 192.168.x.x)
* Phishing Page Location: Sahte login HTML sayfası (örnek: facebook.html)
* Log File: Kullanıcı giriş bilgilerini kaydedeceği dosya

Kullanım amacı: Hedef kullanıcıdan kullanıcı adı ve şifre toplamak.

**✅ 3. DHCP Server**

👉 IP, gateway, DNS bilgisi dağıtır (sahte ağ bağlantısı kurulurken kullanılır).  
**Parametreler:**

* Interface: Kullanılan ağ arayüzü
* Gateway IP: Saldırgan cihazın IP adresi
* DNS Server: Aynı IP olabilir
* IP range: 192.168.1.100–192.168.1.110 gibi

Kullanım amacı: Hedefe IP atanarak sahte ağdan internete yönlendirilmiş gibi gösterilir.

**✅ 4. DNS Spoofing**

👉 Hedefin girdiği alan adlarını sahte IP’ye yönlendirir.  
**Kullanım:**

* Domain: Örneğin facebook.com
* Redirect IP: Sahte sayfanın barındığı IP

Kullanım amacı: Hedef facebook.com yazdığında sahte giriş sayfası açılır.

**✅ 5. ARP Poisoning**

👉 Hedef ve ağ geçidi arasındaki trafiği ele geçirir (MITM).  
**Kullanım:**

* Target IP: Hedefin IP adresi
* Gateway IP: Modemin IP’si

Kullanım amacı: Hedefin tüm trafiğini görmek veya yönlendirmek.

**✅ 6. Credential Harvester (Log viewer)**

👉 Phishing saldırılarında gelen kullanıcı adı/şifreleri gösterir.  
**Gelen logları anlık olarak terminalde de görebilirsin.**

**📌 Kullanım Senaryosu (Sınıf Uygulaması İçin)**

**Öğrencilerin Ghost Phisher’ı test etmesi için örnek bir senaryo:**

1. **Kali Linux sisteminde aracı çalıştırın.**
2. **“Fake AP” özelliğiyle sahte Wi-Fi noktası oluşturun.**
3. **“Phishing Page Hosting” kısmında sahte bir giriş sayfası seçin (örnek HTML dosyası kullanılabilir).**
4. **DNS Spoofing modülünü aktif hale getirin.**
5. **Hedef cihazdan sahte Wi-Fi ağına bağlanarak phishing sayfasını açın.**
6. **Öğrenciler, terminalde gelen kullanıcı adı ve şifreleri gözlemlesin.**
7. **Deney sonrası analiz yapılarak etik farkındalık artırılsın.**

**🧠 Sonuç**

**Ghost Phisher, sosyal mühendislik araçlarının pratikte nasıl çalıştığını anlamak için çok değerlidir. Bu araç sayesinde:**

* **Ağ güvenliğinin zayıf noktaları gözlemlenebilir.**
* **DNS spoofing, phishing, ARP poisoning gibi kavramlar uygulamalı olarak öğretilebilir.**
* **Eğitim sırasında etik sınırlar ve yasal sorumluluklar mutlaka vurgulanmalıdır.**