**1. EvilNoVNC Nedir?**

**EvilNoVNC**, hedef kullanıcıyı bir **sahte uzak masaüstü (VNC) oturumuna yönlendirerek** kimlik bilgilerini veya davranışlarını yakalamaya yarayan, tarayıcı tabanlı bir **phishing framework**’üdür.

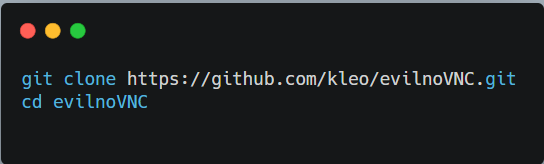
📌 Amaç: Kurbanı kandırarak sahte bir sistemde işlem yaptırmak → oturum, parola, MFA gibi bilgileri elde etmek.

**🧪 2. Nasıl Çalışır?**

* **NoVNC**: Gerçek bir uzak masaüstü arayüzü (HTML5/VNC)
* **EvilNoVNC**: Bu altyapıyı kullanarak **sahte masaüstü ortamı** sunar
* Kullanıcı tarayıcıda “gerçek bilgisayarmış” gibi sahte Windows/Linux ortamına yönlendirilir
* Her tıklama, yazı, parola, session token kayıt altına alınabilir

**⚙️ 3. Kurulum (Kali Linux)**

**✅ 1. GitHub’dan klonla**



**✅ 2. Kurulum scriptini çalıştır**

./setup.sh

📌 Script, noVNC, websockify, x11vnc, xfce4, tightvncserver gibi bileşenleri kurar.

**✅ 3. Sistemi başlat**

./start.sh

**🌐 4. Kullanım**

* Kurban şu URL’ye yönlendirilir:  
  http://<saldırgan-ip>:6080
* Açılan sayfada kurbana sahte masaüstü görünümü sunulur (örnek: sahte Windows login ekranı)
* Kurban bilgilerini girdiğinde veriler terminale loglanır veya logs/ dizinine yazılır

**📋 5. Örnek Terminal Çıktısı**

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**🎭 6. Senaryo Örneği**

🔹 **Oltalama E-Postası Gönder:**  
“Güvenlik politikası gereği uzak masaüstü oturumunuzu güncelleyin”  
Buton: “Giriş Yap” → EvilNoVNC linkine yönlendir

🔹 **Kurban Tıklarsa:**

* Sahte masaüstü açılır
* Oturum bilgisi girer
* Parola, oturum anahtarı veya davranış kaydı alınır

**🛠️ 7. Özellikler**

| **Özellik** | **Açıklama** |
| --- | --- |
| 💻 Tarayıcıdan erişim | NoVNC altyapısı ile doğrudan erişim |
| 🎭 Sahte masaüstü ortamı | Gerçek gibi görünen login ekranları |
| 🔒 Loglama | Tüm tuşlar ve işlemler kayıt altına alınır |
| 🧠 MFA geçişi (bazı senaryolarda) | Kullanıcının davranışını analiz etme |

**⚠️ 8. Etik ve Hukuki Uyarı**

* EvilNoVNC yalnızca **Red Team senaryoları**, **laboratuvar ortamları** ve **eğitim simülasyonlarında** kullanılmalıdır
* Gerçek kullanıcıları kandırmak, kimlik bilgisi toplamak **yasal suçtur**

**🎯 9. Öğrenim Kazanımları**

* Tarayıcı tabanlı kimlik avı saldırılarının nasıl planlandığını öğrenme
* Uzak masaüstü simülasyonu ile phishing tekniği uygulama
* Kullanıcı davranışı analizine dair temel bilgi edinme
* Red Team araçlarını etik sınırlar içinde deneyimleme