EAPHammer Aracı – Eğitimi Materyali

# 1. EAPHammer Nedir?

EAPHammer, WPA-Enterprise (özellikle EAP kimlik doğrulama) kullanan kablosuz ağlara yönelik Red Team saldırılarını gerçekleştirmek için kullanılan açık kaynaklı bir pentest aracıdır.  
  
Özellikle kimlik avı (phishing) yoluyla kullanıcı adı ve parola toplamaya, sahte EAP sunucuları oluşturmaya ve captive portal saldırılarına odaklanır.

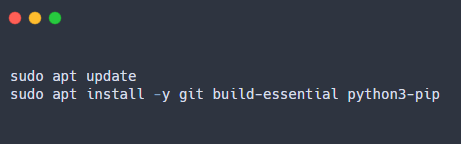
# 2. Hangi Amaçla Kullanılır?

- WPA2-Enterprise ağlarını test etmek  
- Evil Twin (sahte erişim noktası) saldırıları düzenlemek  
- Kullanıcı bilgilerini (kimlik bilgileri) toplamak  
- MSCHAPv2 üzerinden parola hash'lerini ele geçirmek  
- Captive portal saldırıları simüle etmek

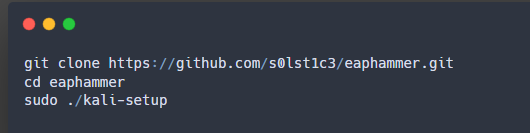
# 3. Kali Linux Üzerine Kurulum

EAPHammer, Kali Linux'a doğrudan kurulabilir ancak birkaç bağımlılık gerekebilir.

Gerekli Bağımlılıkları Kur:



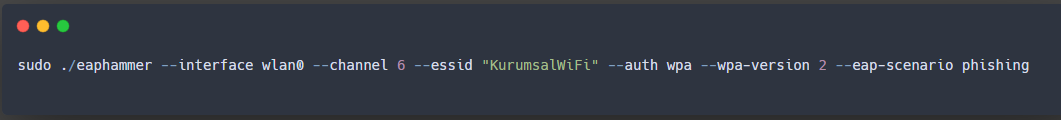
EAPHammer Kodunu Klonla ve Kur:



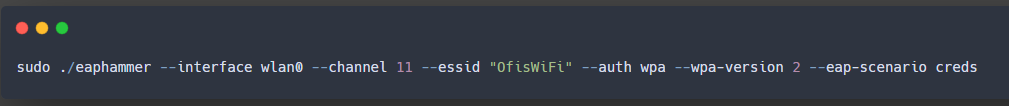
4. Temel Kullanım Örnekleri

Aşağıda bazı temel saldırı örnekleri verilmiştir.

1️⃣ WPA2-Enterprise Evil Twin Saldırısı (Kimlik Avı):

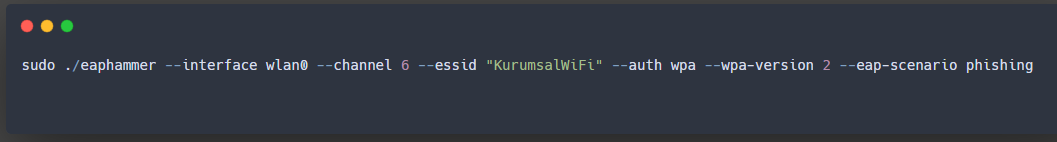


2️⃣ MSCHAPv2 Hash Toplama:

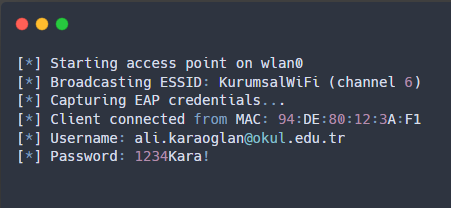


🔹 **Amacı:** WPA2-Enterprise WiFi ağlarına karşı sahte erişim noktası oluşturma ve kimlik bilgisi toplama

Komut: Evil Twin + Phishing

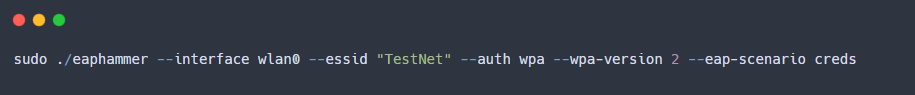


Çıktı:

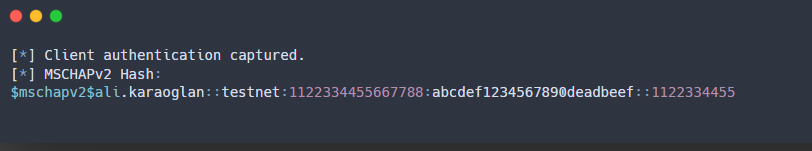


💡 Bu bilgiler düz metin veya hash olarak ele geçirilebilir.

Komut: MSCHAPv2 Hash Yakalama



Çıktı:



# 5. Örnek Saldırı Senaryosu

Senaryo:  
- Saldırgan, okulda kullanılan WPA2-Enterprise ağına benzer bir sahte erişim noktası kurar.  
- Öğrenciler bu sahte ağa bağlanınca kullanıcı adı ve parola bilgileri saldırganın terminalinde görünür.  
- Bu sayede kimlik avı başarıya ulaşmış olur.

# 6. Öğrenciler İçin Uygulama Görevleri

1. EAPHammer'ı Kali Linux'a kurun.

2. Kendi sahte WiFi ağınızı oluşturun (ESSID belirleyin).

3. Bir kullanıcıdan gelen bağlantı denemesini izleyin.

4. MSCHAPv2 hash çıktısını alın ve ekran görüntüsünü kaydedin.

5. Toplanan verilerin neler içerdiğini tartışın (etik kurallar vurgulanmalı).

# 7. Özet

Araç: EAPHammer

Amacı: WPA2-Enterprise ağlarda kimlik avı ve Evil Twin saldırıları

Platform: Kali Linux

Hedef: Kurumsal WiFi kullanıcıları

Kullanım Alanı: Red Team, Kablosuz Pentest, Güvenlik Eğitimi