**PACU**

**1. Nedir?**  
**Pacu**, Amazon Web Services (AWS) üzerinde güvenlik açıklarını test etmek için kullanılan **Red Team** (sızma testi) aracıdır.  
Modüler bir yapıya sahiptir, yani farklı saldırı senaryoları için eklentilerle çalışır.

Kısaca:  
- “Bir AWS hesabında hangi açıklar var?”  
- “Test et, analiz et ve açıkları ortaya çıkar.”  
- “Pacu bunu yapmanı sağlar.”



**2. Ne İşe Yarar?**

* Bir AWS hesabında **yanlış yapılandırılmış izinleri**, açık anahtarları, güvenlik açıklarını bulur.
* Kötü niyetli bir kişi sisteme erişim sağladığında neler yapabileceğini test etmek için kullanılır.
* Red Team bu aracı kullanarak “gerçek saldırgan gibi” davranır.
* Amaç: sistem zayıf noktalarını öğrenmek ve önlem almak.

➡️ Aynı zamanda IAM izinlerini analiz eder, veri sızdırma yollarını test eder.

**3. Neden Önemlidir?**

* Birçok kurum AWS kullanıyor ama yapılandırma hataları çok yaygın.
* Pacu sayesinde bu hatalar saldırganlar tarafından kullanılmadan önce tespit edilebilir.
* 🔐 Bu da daha güvenli bir bulut altyapısı anlamına gelir.
* Hem güvenlik uzmanları hem de öğrenciler için **bulut güvenliği eğitiminde** çok faydalıdır.

💡 Özellikle IAM (identity and access management – kimlik ve yetki yönetimi) hatalarında çok güçlüdür.

**4. Nasıl Kurulur? (Linux Örneği)**

Pacu, Python ile çalışır. Kurulumu oldukça basittir:

**# 1. Gerekli paketleri kur**

**sudo apt update && sudo apt install git python3-pip –y**

****

**# 2. Pacu'yu GitHub üzerinden klonla**

**git clone https://github.com/RhinoSecurityLabs/pacu.git**

**cd pacu**

****

**# 3. Bağımlılıkları yükle**

**pip3 install -r requirements.txt**

****

**# 4. Pacu'yu başlat**

**python3 pacu.py**

****

Başlangıçta bir AWS profil tanımlaman gerekir. AWS erişim anahtarlarını kullanarak Pacu'ya giriş yapabilirsin.

**5. Örnek Bir Anlatım:**  
Senin eline bir AWS erişim anahtarı geçti (örneğin bir sızma testi sırasında). Bu anahtarla sisteme girebilir misin? Ne kadar yetkin var? Hangi servislere ulaşabilirsin?

Pacu ile bunu test edebilirsin:

**# Pacu'yu başlat**

**python3 pacu.py**

**# AWS profilini gir (örneğin erişim anahtarı ve gizli anahtar)**

**# Modül listesini göster**

**list\_modules**

**# Örnek modül çalıştır: IAM izinlerini analiz et**

**run iam\_\_enum\_permissions**

**Sonuç:** Bu kullanıcı hangi haklara sahip? Hangi servislerde açıklar var? Bunları görmüş olursun.

⚠️ **Uyarı:**  
Pacu çok güçlü bir araçtır ve yalnızca **izinli ortamlarda, eğitim ve test amacıyla** kullanılmalıdır. Gerçek sistemlerde izinsiz kullanılması **yasal suçtur**.