**🔍 1. Rubeus Nedir?**

**Rubeus**, Windows ortamlarında Kerberos kimlik doğrulama protokolünü hedef alan, güçlü ve esnek bir **Kerberos ticket (bilet) manipülasyon aracıdır.**

📌 Red Team uzmanları tarafından kullanılır, özellikle **Active Directory (AD)** ortamlarında:

* Bilet çıkartma (ticket extraction)
* Sahte bilet oluşturma (ticket forging)
* Yetki yükseltme (privilege escalation)
* Post-exploitation işlemleri için

**🧰 2. Kullanım Amaçları**

| **Amaç** | **Açıklama** |
| --- | --- |
| 🎫 Ticket Dump | Sistemden biletleri çıkarma |
| 🔁 PTT (Pass-the-Ticket) | Başka bir kullanıcının biletiyle işlem yapma |
| 🔥 Kerberoasting | Hizmet hesaplarının hash'lerini elde etme |
| 🧂 AS-REP Roasting | Pre-auth devre dışı hesaplardan hash çekme |

**⚙️ 3. Kurulum**

Rubeus açık kaynak kodludur. Derlenmiş dosya ya da kaynak C# koduyla çalıştırılabilir.

**✅ Kaynak koddan indirmek:**

git clone <https://github.com/GhostPack/Rubeus.git>

**✅ Derleme sonrası elde edilir:**

* Rubeus.exe (standalone kullanım)
* veya Rubeus.cs dosyası (fileless çalıştırma için)

**💻 4. Temel Komutlar**

**🔍 Biletleri Görüntüle:**

Rubeus.exe klist

**📤 Biletleri Çıkar (Dump):**

Rubeus.exe dump

**🧩 Bilet Yükle (Pass-the-Ticket):**

Rubeus.exe ptt /ticket:ticket.kirbi

**🔓 Kerberoasting:**

Rubeus.exe kerberoast

**🔓 AS-REP Roasting:**

Rubeus.exe asreproast

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

Örnek terminal çıktısı

**🎯 5. Öğrenim Kazanımları**

* Kerberos sistemine genel bakış
* Ticket-based kimlik doğrulama kavramı
* Kerberoasting ve bilet enjeksiyon süreçleri
* Red Team operasyonlarında post-exploitation adımları