**HİLAL ÖKLÜK**

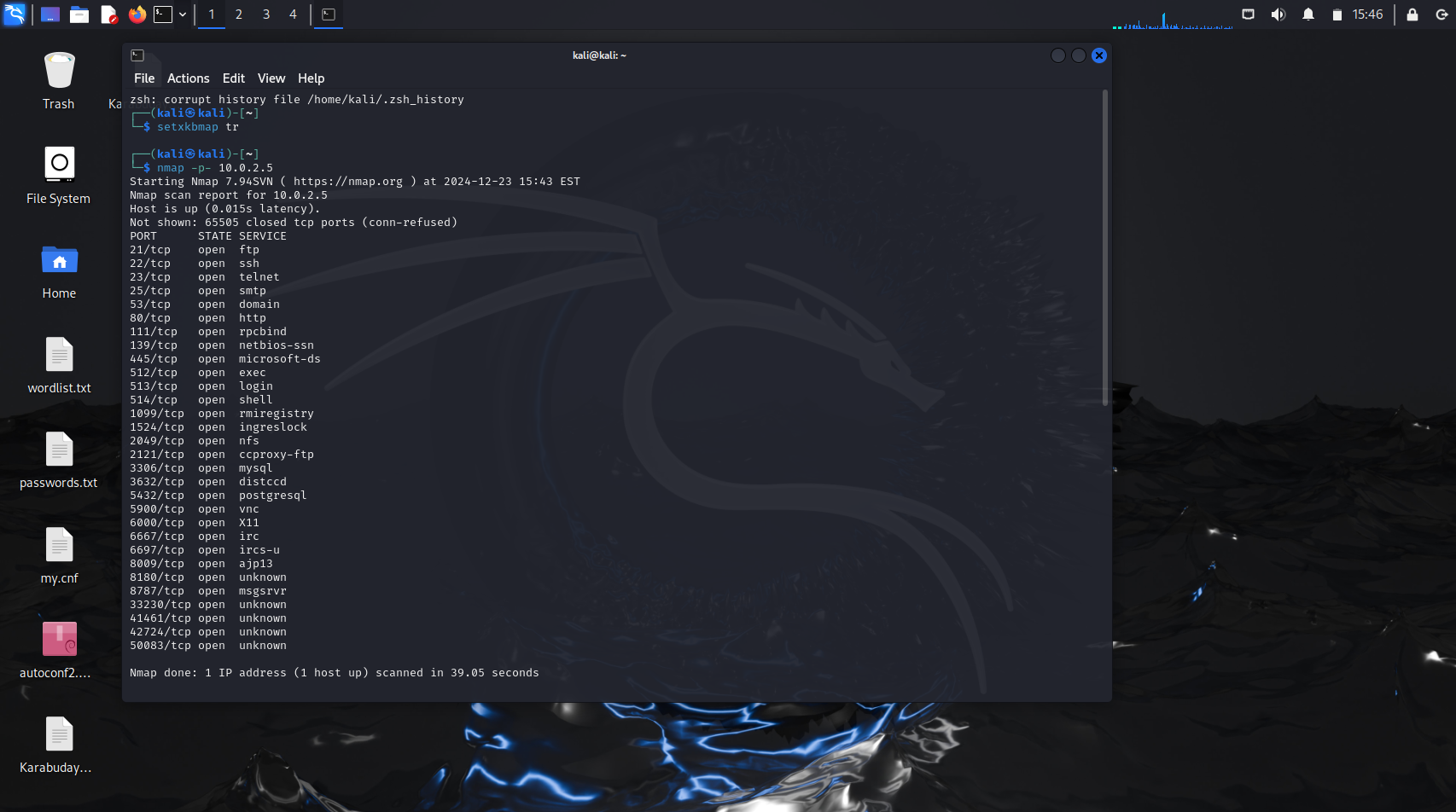
**213908251**

**SİBER GÜVENLİK - HYDRA İLE METASPLOITABLE’IN TELNET ŞİFRESİNİ KIRMA**

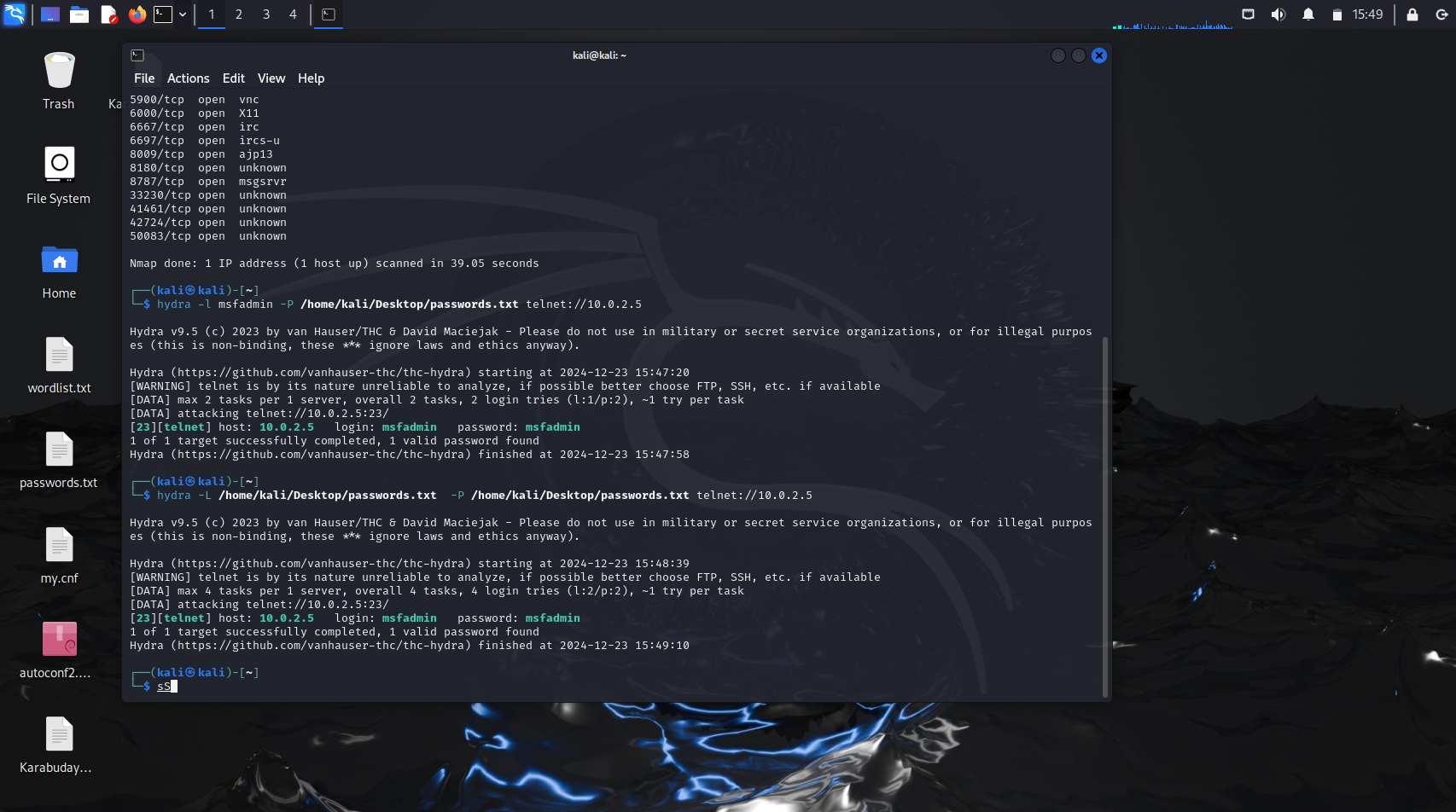
* **Projenin Amacı**: Metasploitable üzerinde bir güvenlik testi gerçekleştirilmesi.
* **Kullanılan Araçlar ve Yöntemler**: Hydra ile brute-force saldırısı, Telnet servisi üzerinden giriş.
* **Çalışmanın Adımları**: Nmap ile servislerin tespiti, Telnet servisinin seçimi ve Hydra ile parola kırma işlemi.
* **Sonuçlar**: Telnet şifresinin başarıyla kırıldığı ve ilgili oturuma erişildiği.

**Proje Adımları:**

* Öncelikle nmap ile Metasploitable’a ait tüm servislerin durumlarını inceledik. Ekran görüntüsünde şifresini kırmak istediğimiz telnet servisinin açık olduğunu görebiliyoruz.



* **Hydra ile Brute-Force Saldırısı:**
  + Hydra aracı kullanılarak, kullanıcı adı olarak "msfadmin" ve bir parola listesi (/home/kali/Desktop/passwords.txt) kullanılarak Telnet servisine brute-force saldırısı gerçekleştirildi.
  + Saldırı sonucu, kullanıcı adı: **msfadmin**, şifre: **msfadmin** olduğu tespit edilmiştir.



* Hydra ile brute-force saldırısı sonucu elde edilen kullanıcı adı ve şifre kullanılarak Telnet servisine giriş yapılmıştır. Sisteme **msfadmin** kullanıcısı ile giriş yapılmış ve başarıyla komut satırına erişilmiştir.

