**🧠 1. Netripper Nedir?**

**Netripper**, Windows işletim sisteminde **admin ayrıcalıkları olmadan** çalışan, ağ trafiğini şeffaf bir şekilde yakalayabilen ve bu trafik içinden **parola, oturum bilgileri gibi hassas verileri çıkartabilen** bir sızma testi aracıdır.

📌 Öne çıkan özellikler:

* Windows üzerinde arka planda çalışabilir
* Şifrelenmemiş protokollerden veri toplar (HTTP, FTP, IMAP vb.)
* Proses (process) tabanlı trafik dinleme
* Elde edilen verileri dosyaya kaydetme veya anlık görüntüleme

**🎯 2. Ne İşe Yarar?**

| **Özellik** | **Açıklama** |
| --- | --- |
| 📡 Ağ trafiğini yakalama | Hedef sistemdeki proseslerin internet trafiğini kaydeder |
| 🔑 Parola çıkarma | Şifrelenmemiş giriş bilgilerini bulur |
| 🕵️‍♂️ Oturum bilgisi toplama | Cookie, token, session verilerini yakalar |
| 🧪 Red Team testleri | Kullanıcı haberi olmadan veri toplama senaryoları |
| 🛡️ Blue Team farkındalığı | Ağ güvenliğinin önemini göstermek |

**⚙️ 3. Kurulum (Windows / Kali üzerinden hazırlık)**

**✅ 1. GitHub’dan indir:**

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

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.**✅ 2. Windows üzerinde derleme (Visual Studio veya mingw)**

* Kaynak kodu Windows ortamında derleyerek çalıştırılabilir .exe elde edilir.

**✅ 3. Kullanım için hedef sisteme aktarılır.**

**✅ 1. Mevcut prosesleri listeleme:**

Netripper.exe list

**✅ 2. Belirli bir prosesi dinleme:**

Netripper.exe sniff <PID>

**✅ 3. Tüm prosesleri dinleme:**

Netripper.exe sniff all

**✅ 4. Çıktıları dosyaya kaydetme:**

Netripper.exe sniff all > output.txt

**📋 5. Örnek Terminal Çıktısı**

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**🧠 6. Desteklenen Protokoller**

* HTTP (Basic / Form Auth)
* FTP
* IMAP / POP3
* SMTP
* Telnet

**🧪 7. Kullanım Senaryoları**

| **Senaryo** | **Açıklama** |
| --- | --- |
| 🔍 Red Team testleri | Hedef kullanıcı trafiğini şeffaf şekilde izleme |
| 🛡️ Blue Team farkındalığı | Hassas verilerin şifrelenmemiş taşınmasının risklerini göstermek |
| 🧪 Zararlı yazılım analizi | Keylogger / packet sniffer mantığının süreç tabanlı incelenmesi |
| 📚 Eğitim ortamı | Ağ güvenliğini uygulamalı göstermek |

**🎯8. Öğrenim Kazanımları**

* Process tabanlı ağ trafiği dinleme mantığını öğrenme
* Şifrelenmemiş protokollerin güvenlik risklerini anlama
* Pentest araçlarının Windows ortamında nasıl çalıştığını kavrama
* Blue Team bakış açısıyla veri koruma önemini fark etme