**🔍 1. TCPDump Nedir?**

**TCPDump**, terminal üzerinden çalışan, ağ trafiğini gerçek zamanlı olarak analiz etmeye yarayan güçlü bir **paket dinleme (sniffing)** aracıdır.

* Wireshark'ın metin tabanlı (CLI) karşılığıdır.
* Hafiftir, sunucu sistemlerde sıkça tercih edilir.
* Filtreleme, kayıt ve analiz işlemlerini hızlıca yapar.

🔧 Wireshark grafik arayüzlüdür, TCPDump ise komut satırı ile çalışır.

🔧 **2. Kurulum (Kali Linux)**

Kali Linux'ta genellikle yüklü gelir. Değilse:

sudo apt-get update

sudo apt-get install tcpdump

**📜 TCPDump – Temel Komut Listesi**

1. **Tüm trafiği dinle (varsayılan arayüzle):**  
   tcpdump
2. **Belirli bir arayüzü dinle (örnek: wlan0):**  
   tcpdump -i wlan0
3. **İlk 10 paketi göster:**  
   tcpdump -c 10
4. **Sadece HTTP (port 80) trafiğini dinle:**  
   tcpdump -i wlan0 port 80
5. **Belirli bir IP’ye ait tüm trafiği izle:**  
   tcpdump host 192.168.1.5
6. **Sadece belirli IP’ye giden (destination) trafiği izle:**  
   tcpdump dst host 192.168.1.5
7. **Sadece belirli IP’den gelen (source) trafiği izle:**  
   tcpdump src host 192.168.1.5
8. **Tüm DNS (port 53) sorgularını göster:**  
   tcpdump port 53
9. **Veriyi .pcap dosyasına kaydet (Wireshark ile açılabilir):**  
   tcpdump -i wlan0 -w kayit.pcap
10. **Kayıtlı .pcap dosyasını analiz et:**  
    tcpdump -r kayit.pcap

ekran görüntüsü, metin, yazılım, multimedya yazılımı içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**📊 4. Çıktı Yapısı Nasıldır?**

Örnek çıktı:

12:01:22.123456 IP 192.168.1.5.60000 > 142.250.74.206.443: Flags [S], seq 123456, win 65535, length 0

Anlamı:

* Zaman damgası
* Kaynak IP ve port > Hedef IP ve port
* TCP bayrağı (S: SYN, P: PSH, A: ACK vs.)
* Paket boyutu, sıra numarası

**⚠️ 6. Etik ve Güvenlik Uyarıları**

* TCPDump güçlü bir trafik analiz aracıdır.
* Yalnızca **izinli ortamlarda** ve **test ağlarında** kullanılmalıdır.
* Başka bireylerin ağına sızmak veya trafiğini kaydetmek **yasal suçtur.**

**🎯 7. Öğrencilerin Öğreneceği Şeyler**

* Gerçek zamanlı ağ trafiğinin yapısı
* TCP/IP protokolü nasıl işler
* IP, port, paket yönü (src/dst) kavramları
* Ağ analizi sadece grafik değil terminal tabanlı da yapılabilir
* .pcap dosyaları nedir, nasıl incelenir

**🧠 8. Sonuç**

* TCPDump ile ağ verisini filtrelemeyi, kaydetmeyi ve analiz etmeyi öğrenmiş olursun.
* Temel protokol bilgileri gelişir.
* Terminal tabanlı güvenlik analizi pratiği kazanılır.
* Ağ olaylarını anlamlandırmak için temel bir beceri edinilmiş olur.