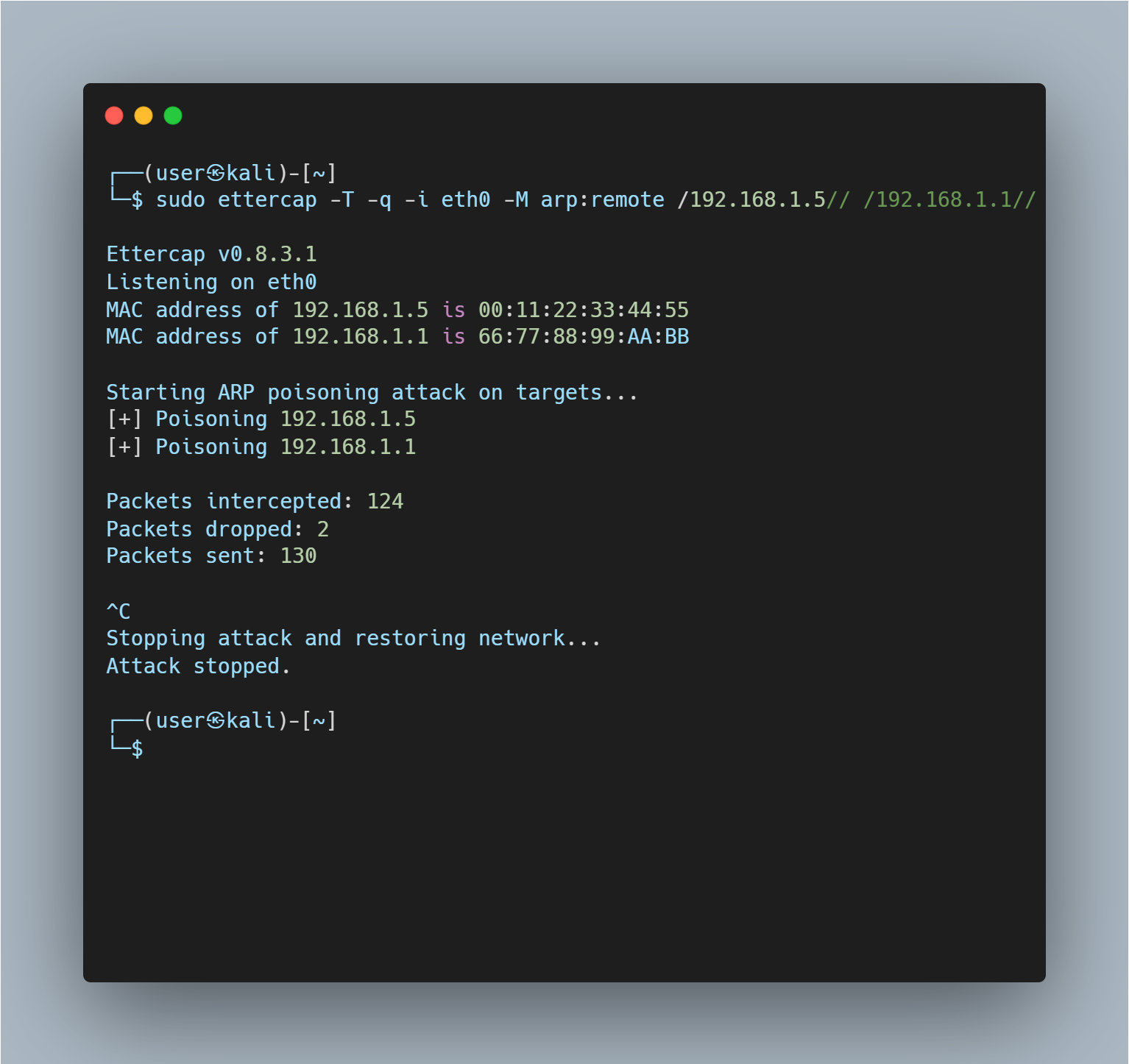
**Ettercap Nedir?**

Ettercap, ağ seviyesinde (Layer 2) çalışan güçlü bir Man-in-the-Middle (MitM) saldırı ve ağ analizi aracıdır. Hem aktif hem pasif modlarda kullanılabilir. Özellikle yerel ağdaki trafiği izlemek, değiştirmek veya engellemek için tercih edilir. Ettercap, ARP spoofing (zehirleme) ile hedef makineler arasındaki trafiği ele geçirip, gerçek zamanlı olarak veri toplamanıza veya müdahale etmenize olanak sağlar.

**Ettercap’in Temel Özellikleri**

* ARP Spoofing ile ağdaki iki cihaz arasına sızma
* HTTP, FTP, Telnet gibi protokollerde parolaları, oturum bilgilerini yakalama
* Paketleri analiz etme ve filtreleme
* Canlı trafik manipülasyonu (örneğin, web sayfalarında içerik değiştirme)
* Grafiksel (GUI) ve komut satırı (CLI) arayüz desteği



Bu çıktı:

* Ettercap sürümünü,
* Dinleme yapılan ağ arayüzünü,
* Hedeflerin MAC adreslerini,
* ARP zehirlenmesinin başladığını,
* Paket sayımlarını,
* İşlemin sonlandırıldığını gösteriyor.

**Kullanım Örneği**

Ağdaki cihazları keşfetme:

***sudo ettercap -T -q -M arp:remote /192.168.1.5/ /192.168.1.10/***

Bu komutla, 192.168.1.5 ve 192.168.1.10 IP adresleri arasında ARP spoofing yaparak trafiği ele geçirirsiniz.

Ettercap’i GUI modunda başlatmak: ***sudo ettercap -G***

Grafik arayüzünde hedef seçip saldırıyı kolayca başlatabilirsiniz.

**Eğitimde Kullanım Önerisi**

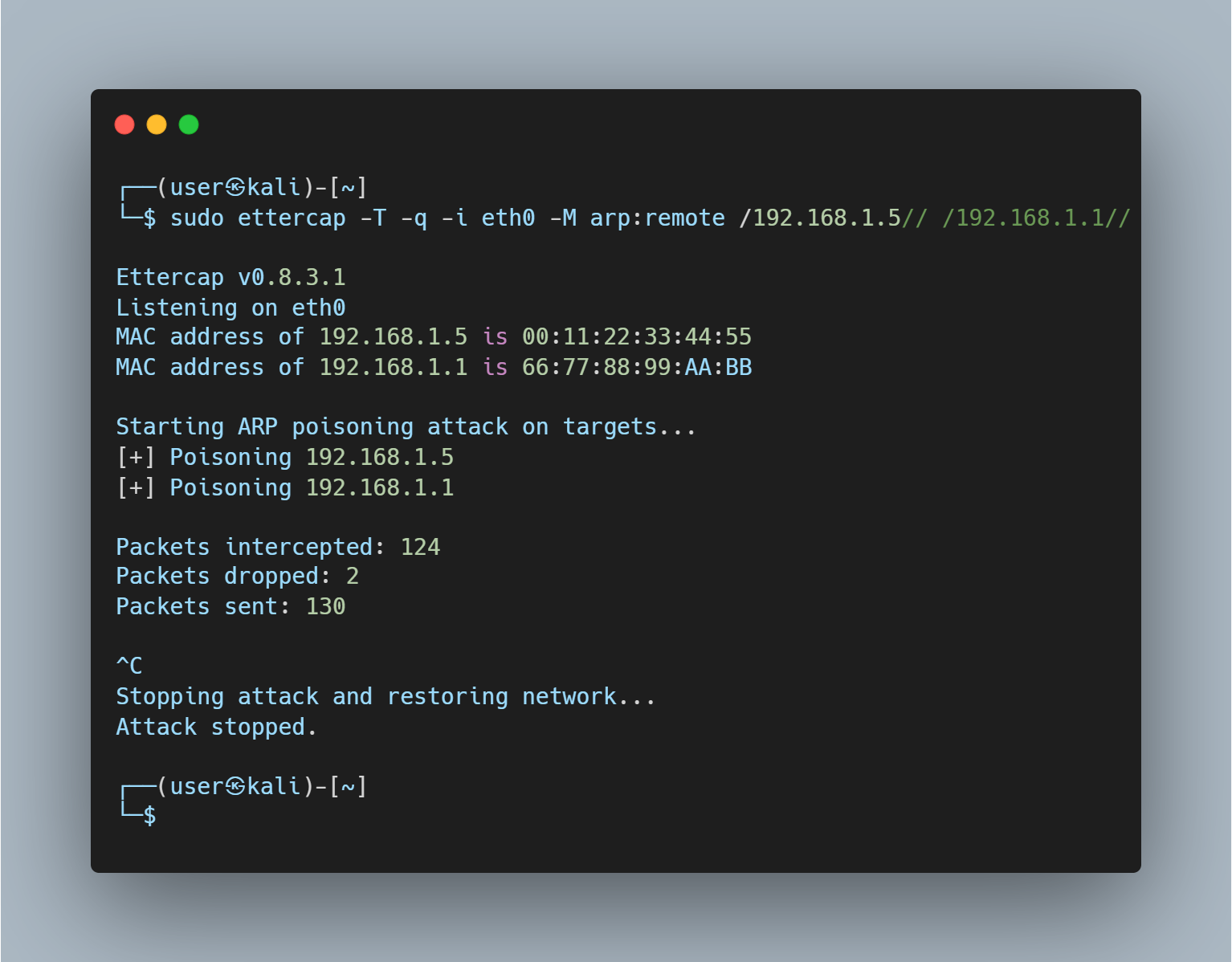
* Öğrencilere MitM saldırılarının nasıl yapıldığını ve ağ trafiğinin nasıl ele geçirildiğini anlatmak için ideal bir araçtır.
* Gerçek ağlarda trafiğin nasıl izlenip manipüle edildiğini göstermek için kullanılabilir.
* Parola veya kritik veri yakalama örnekleri ile saldırı senaryoları oluşturulabilir.

Ettercap, ağ protokolleri üzerinde derinlemesine analiz ve müdahale yapabilen kapsamlı bir Man-in-the-Middle (MitM) aracıdır. Çalıştığı katman, OSI modelinde Veri Bağlantı Katmanı (Layer 2) olduğu için, ağdaki cihazlar arasındaki paketleri doğrudan yakalayabilir ve değiştirebilir. Bu sayede, sadece dinleme değil, aynı zamanda veri manipülasyonu ve saldırı gerçekleştirme imkânı da sağlar.

ARP spoofing yöntemiyle ağdaki iki cihazın adreslerini birbirine yanlış tanıtarak, onların arasındaki trafiği kendisine yönlendirir. Ettercap, bu yöntemi kolaylaştıran otomatik araçlar sunar ve böylece hedefler arasındaki veri akışını pasif ya da aktif şekilde kontrol eder.

**Ettercap’in Kullanım Alanları**

* **Parola Yakalama:** FTP, HTTP, SMTP, POP3 gibi protokollerde şifreleri yakalayabilir.
* **DNS Spoofing:** Hedefin DNS sorgularını manipüle ederek sahte web sitelerine yönlendirme yapabilir.
* **HTTP Trafiği Manipülasyonu:** Web sayfalarına zararlı içerik enjekte etme, reklam değiştirme veya kullanıcı aktivitelerini izleme.
* **Protokol Analizi:** Ağ trafiğini gerçek zamanlı izleyip detaylı analiz yapma.
* **Kapsamlı Saldırı Senaryoları:** MITM ile güvenlik testlerinde senaryo tabanlı uygulamalar için tercih edilir.



Bu örnek çıktı şu aşamaları gösteriyor:

* Ettercap sürüm bilgisi ve ağ arayüzü
* ARP spoofing saldırısının başlatılması
* Hedef IP adreslerine ARP zehirlenmesi yapıldığı bildirimi
* Paket sayıları ve işlem detayları
* İşlemin Ctrl+C ile durdurulması ve ağın eski haline getirilmesi

**Ettercap Kullanırken Dikkat Edilmesi Gerekenler**

* Ettercap ağda trafiği manipüle ettiği için, kullanımı ağ performansını etkileyebilir.
* Etik ve yasal kurallar çerçevesinde, sadece izin verilen ağlarda kullanılmalıdır.
* Yanlış yapılandırma ağdaki diğer kullanıcıların bağlantısını kesebilir.
* Güncel Ettercap sürümleri ve yamaları takip edilmelidir, zira bazı ağ donanımları ARP spoofing saldırılarına karşı koruma sunar.

**Ettercap’i Kullanırken Pratik İpuçları**

* Öncelikle hedef ağda hangi IP adreslerinin aktif olduğunu belirlemek için ağ taraması yapın (örneğin, nmap).
* Ettercap’in GUI arayüzünü kullanmak, komut satırı yerine daha kolay hedef seçimi ve saldırı başlatma sağlar.
* Saldırı sırasında paket filtreleri kullanarak sadece belirli protokollere veya hedeflere odaklanabilirsiniz.
* Otomatik komut dosyaları (scripts) ile Ettercap’in yetenekleri artırılabilir.