Virtual Pirate Network (VPN)

written by Mert SARICA | 1 May 2014

Türkiye, 20 Mart 2014 tarihinde Twitter'a erişime engelleneyerek, dünyada Twitter'ı Çin'den sonra yasaklayan ikinci ülke olarak tarihe adına altın harflerle yazdırdı. Ardından Twitter yasağının nasıl aşılabileceği konusunda yazılı ve basılı görsel medya seferber oldu. Kısa bir süre içinde malum yasağın DNS tabanlı olduğu ve basit bir DNS değişikliği ile bu yasağın kolaylıkla atlatılabildiği anlaşıldı. Hatta bazı haber kanalları canlı yayında DNS değişikliğinin nasıl yapılabileceğini adım adım gösterdi. Canlı yayını kaçıranlar ise DNS adreslerini duvar yazılarından öğrenebildiler :)

Benim gibi, Android yüklü cep telefonundan Twitter'a girenler için bu yasağı atlatmak pek kolay olmadı çünkü rootlanmamış bir cihazda (Android 4.4.2) kullanılan 3G bağlantı için DNS değişikliği yapmak mümkün değildi. Buna karşı 2 yöntemden (cihazı rootlamak veya bir VPN hizmetinden faydalanmak) biri izlenebilirdi. Cihazı rootlamak beraberinde ilave güvenlik riskleri getireceğinden ötürü cihazımı rootlamaya hiçbir zaman sıcak bakmamıştım, Twitter yasağı nedeniyle de rootlamayı tercih etmedim. Ücretsiz bir VPN uygulaması ile VPN hizmetinden faydalanma kısmı ise pratik ve hızlı bir çözüm olarak görünse de, tüm uygulama trafiğimin bilinmeyen bir ağ üzerinden

gitmesine de gönlüm pek el vermiyordu. Wifi ayarları üzerinden DNS değişikliği yapılabildiği için bir süre Twitter'a cep telefonum ile WIFI ağlar üzerinden giriş yaptım.

Twitter yasağı şöyle böyle atlatılıyor diye TIB'in gözüne onlarca haber sokulduktan kısa bir süre sonra bu defa Twitter'ın IP adresleri yasaklanmaya başladı. Bu defa Twitter'ın yasaklanmayan IP adresleri üzerinden Twitter'a bağlanmak mümkün olabiliyordu fakat yine rootlanmamış bir Android cihaz için ip adresi – host eşleştirmesi yapmak (/etc/hosts) mümkün değildi. Bu defa kendi VPN sunucumu kurup onun üzerinden mi Twitter'ın yasaklanmamış IP adreslerine cep telefonu üzerinden bağlansam yoksa F-Secure'un Freedome VPN uygulamasını mı kullansam derken aklıma aylardır evde kuzu gibi yatan ve üzerinde Kali yüklü olan 2. Raspberry PI geldi. Kali üzerine OpenVPN sunucusu kurmak tam da gözümde büyürken Twitter üzerinden Gökhan POYRAZ'ın attığı bir tweet imdadıma yetişti. Gökhan'ın blogunda yer alan strongSwan VPN uygulaması kurulum adımlarından hızlıca geçtikten sonra Kali üzerinde başarıyla strongSwan'i kurdum. (GMP ve libgmp3c2_4.3.2+dfsg-1_armel.deb paketlerini ayrıca kurmam gerekti.)

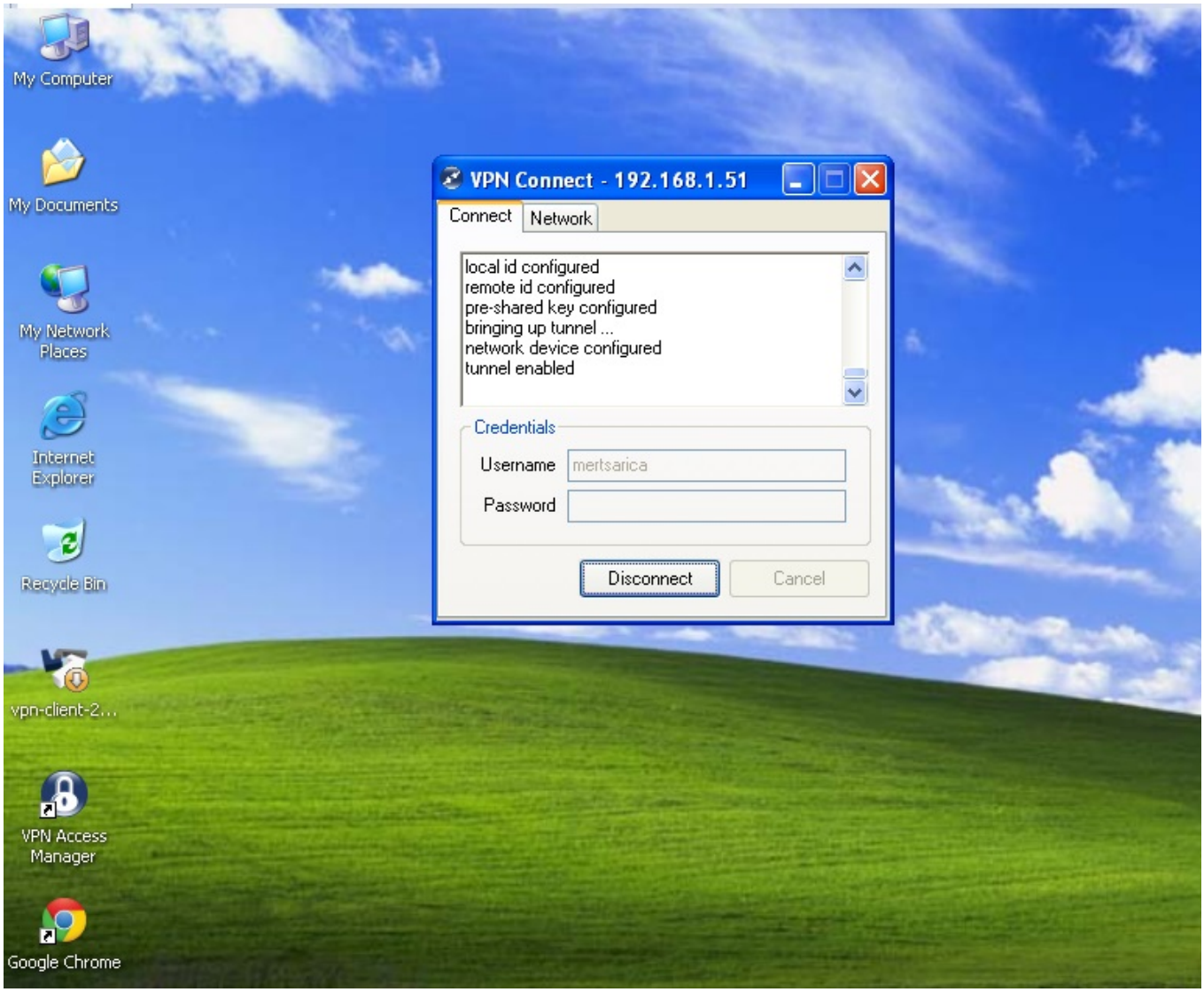
Herkesin elinin altında benim gibi VPN uygulaması kuracak hazır bir sistemi olmadığı için çoğu kimsenin ücretsiz VPN hizmetlerinden faydalandığını farkettim. Özellikle yakın çevremden gelen, hangi VPN uygulamasını yüklemeliyim ? Hangisi daha güvenli ? gibi sorular karşısında VPN kullanımının halk arasında ciddi derecede arttığını anladım. Tabii güvenilirliğinden emin olunamayan bir VPN üzerinden internet bağlantısı gerçekleştirmenin getirdiği riskleri, VPN'i sadece Twitter yasağını atlatmak için kullanan bir kullanıcı kitlesine anlatmak çok kolay olmadı.

Twitter yasağı nedeniyle VPN kullanımı arttıktan sonra güvenilir olmayan VPN sunucuları üzerinden şifrelerin çalındığı ile ilgili haberler okumaya başladık. Ardından bankalar, güvenilir olmayan VPN sunucuları üzerinden gerçekleştirilen bankacılık işlemlerinin tehlikeli olabileceği ile ilgili güvenlik bildirileri yayınlamaya başladılar.

Yeri gelmişken bankada çalışan bir güvenlik uzmanı olarak, bankaların müşterilerine sadece gerekli gördükleri zamanlarda (mevcut veya potansiyel güvenlik ihlalleri) güvenlik uyarıları gönderdiklerini, dolayısıyla bu tür uyarıların bir müşteri olarak büyük bir ciddiyetle dikkate alınması gerektiğini belirtmek isterim.

Bu esnada yakın bir arkadaşım, bu tür (güvensiz VPN sunucularının kullanımı) güncel konularla ilgili olarak neden birşeyler yazmadığım konusunda eleştiri oklarını bir bir üzerime atmaya başladı. Ben de hazır Kali üzerine VPN uygulaması kurmuşken, art niyetli kişilerce yönetilen bir VPN sunucusunun nasıl kullanıcıların internet bankacılığı şifrelerini çalabileceğini arkadaşıma göstermeye ve eleştirilerine bu yazı ile karşılık vermeye karar verdim.

Simülasyon için sanal makinede yüklü olan Windows XP işletim sistemi üzerine bir VPN istemcisi yüklemeye karar verdim. Kali işletim sistemi üzerinde yüklü olan strongsWan uygulaması ile bu istemciyi bağladıktan sonra Kali üzerinde sslstrip aracını port 8080 üzerinde çalıştırdım.



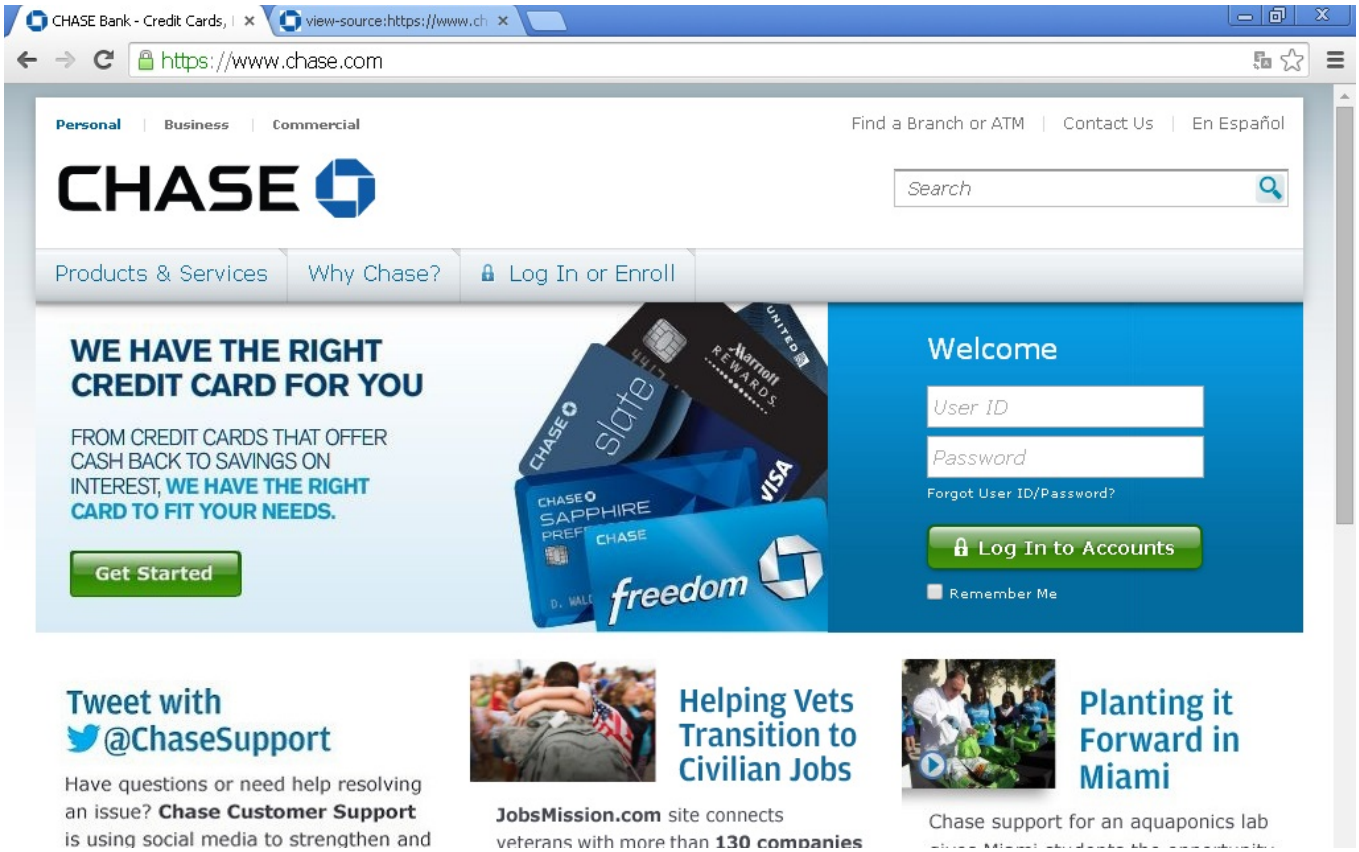
sslstrip aracı, http üzerinden gerçekleşen bir trafikte yer alan tüm https:// bağlantı adreslerini http:// ile değiştirerek kendisi üzerinden hedef sistem ile bağlantı kurarak ortadaki adam saldırısı (MITM) ile şifreleri çalabilmektedir.

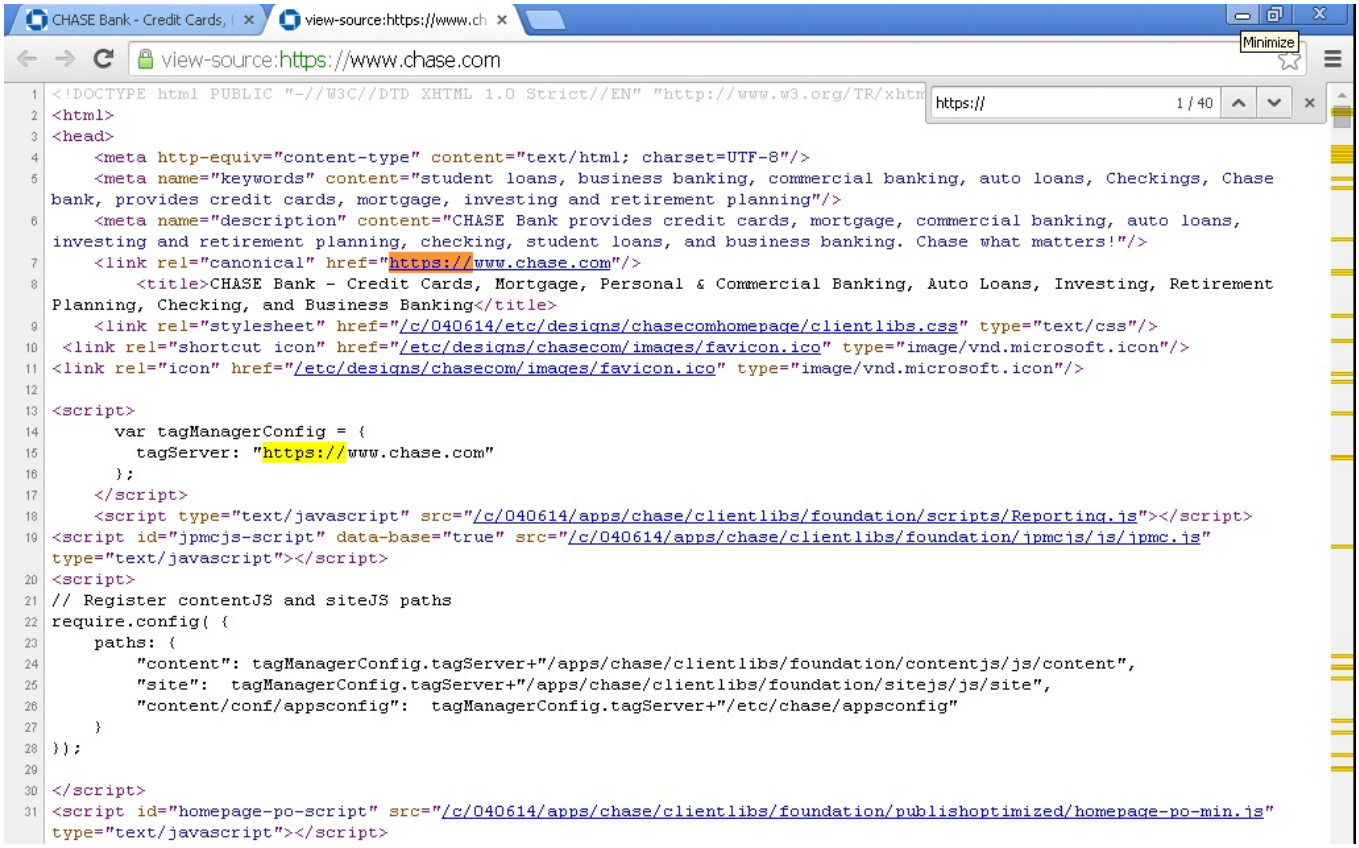
Ardından Gökhan POYRAZ'ın blog yazısında yer verdiği vpn.sh betik dosyasından NAT geçen 2 satırı silip yerine sslstrip aracı için iptables -t nat -A PREROUTING -p tcp –destination-port 80 -j REDIRECT –to-port 8080 satırını ekledim. Bu satır ile iptables'ın, port 80 üzerinden giden (outbound) http trafiğini sslstrip'in çalıştığı port 8080'e yönlendirip aracın tüm https:// bağlantıları http://'ye çevirmesini sağladım.

Raspberry | Kali ×

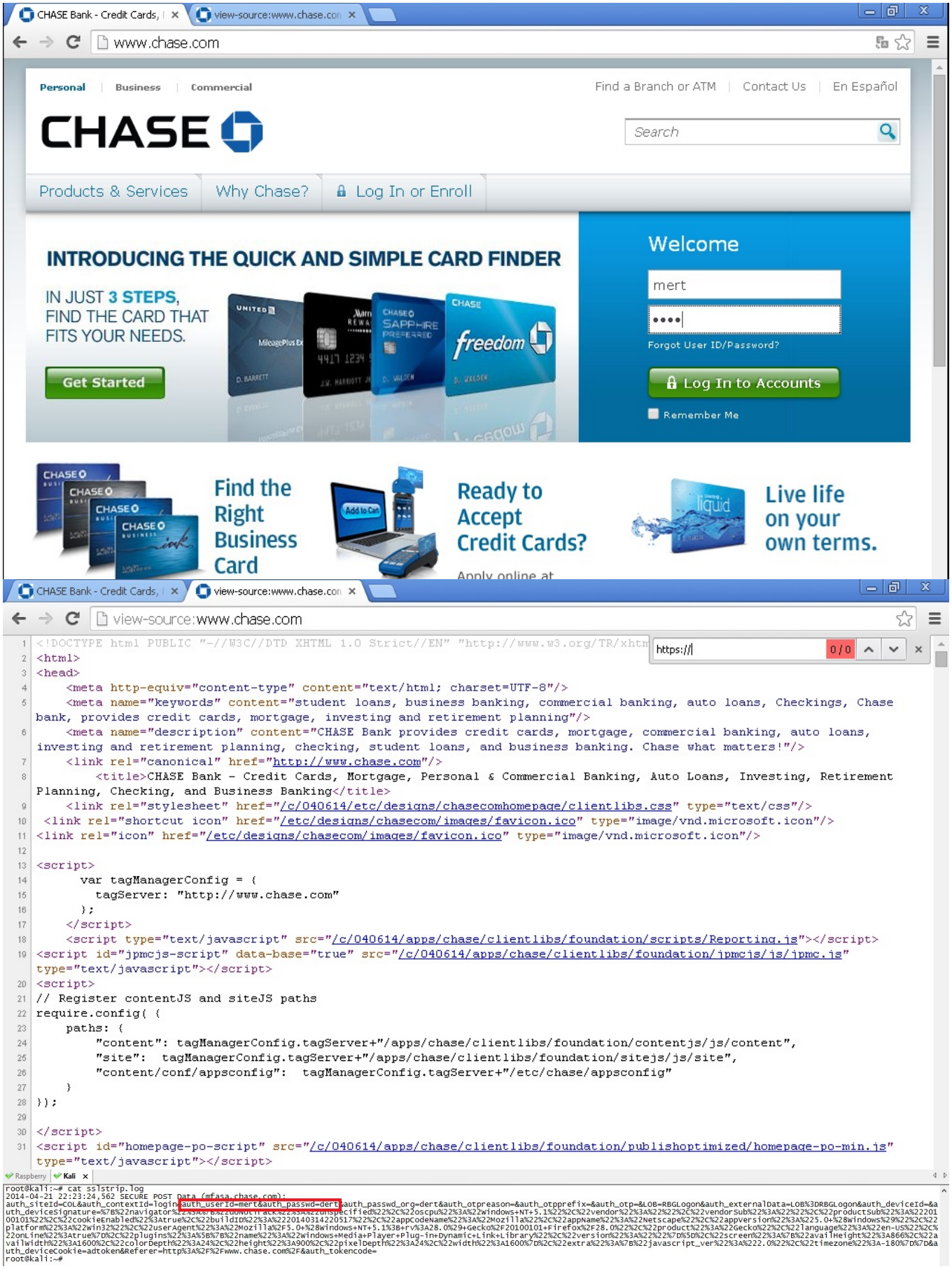
```
root@kali:/# cat /usr/local/bin/vpn.sh
#!/bin/bash
echo 1 > /proc/sys/net/ipv4/ip_forward
sleep 1
iptables -A FORWARD -o eth0 -i eth0 -s 10.71.80.0/24 -m conntrack --ctstate NEW -j ACCEPT
iptables -A FORWARD -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
# iptables -t nat -F POSTROUTING
# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080
sleep 1
/usr/local/sbin/ipsec start
root@kali:/#
```

Simülasyon için öncelikle XP ile Kali arasında VPN bağlantısını kestim. Ardından Chase Bank'ın web sitesine http://www.chase.com adresinden bağlanmak istediğimde sunucunun beni otomatik olarak https://www.chase.com adresine yönlendirdiğini gördüm. Kaynak kodu üzerinde https:// önekini (prefix) arattığımda 40 tane sonuç ile karşılaştım.





Ardından XP ile Kali arasında VPN bağlantısı kurduktan sonra Chase Bank'ın web sitesine http://www.chase.com adresinden bağlandığımda, araya giren sslstrip aracının bağlantıyı https://www.chasebank.com sitesine yönlendirmediğini gördüm. Kaynak kodu üzerinde de https:// öntakını arattığımda da 0 sonucu ile karşılaştım ve sslstripin aradaki adam saldırısını gerçekleştirmesi için kullanıcı adına mert şifre kısmına da dert yazdım. Son olarak sslstrip.log dosyasına baktığımda ise bu aracın girdiğim kullanıcı adı ve şifreyi kayıt dosyasına yazabildiğini görmüş oldum.



Bu simülasyon ile güvenilir olmayan bir VPN sunucusu üzerinde çalıştırılan/kullanılan çeşitli araçlar ve yöntemler ile art niyetli kişilerin şifrelerinizi kolaylıkla çalabileğini göstermiş olduğumu

düşünüyorum. Siz siz olun, bilmediğiniz bir VPN sunucusu kullanmadan önce başınıza neler gelebileceğini tekrar ama tekrar düşünün!

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.