Metasploit

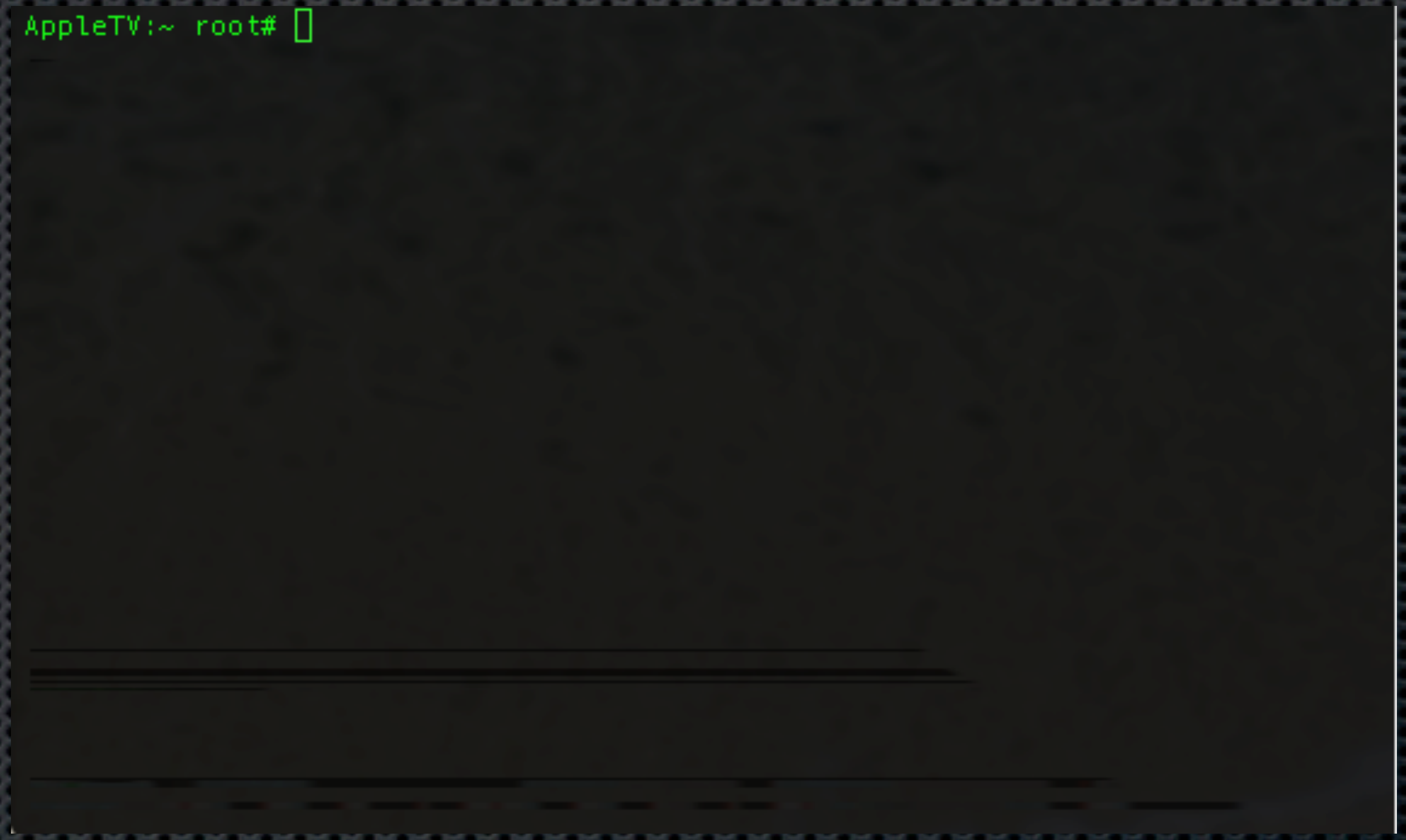
Hola , Soy Xc0d3 y uso mucho el Metasploit pero a mi megusta tenerle en todos mis dispositivos .

Yo uso sistema operativo Mac Os , Linux y en mis Device IOS

Hoy e pensado en instalarle en mi Apple TV 2G y decidí en hacer este tutoríal para si alguien lo querré Tenerle

1. Tenemos que tener Jailbreak en nuestro IDevice
Sabiendo que con Seas0nPass Tiene El puerto 22 SSH
abrierto solo tenemos que conectarnos a el.

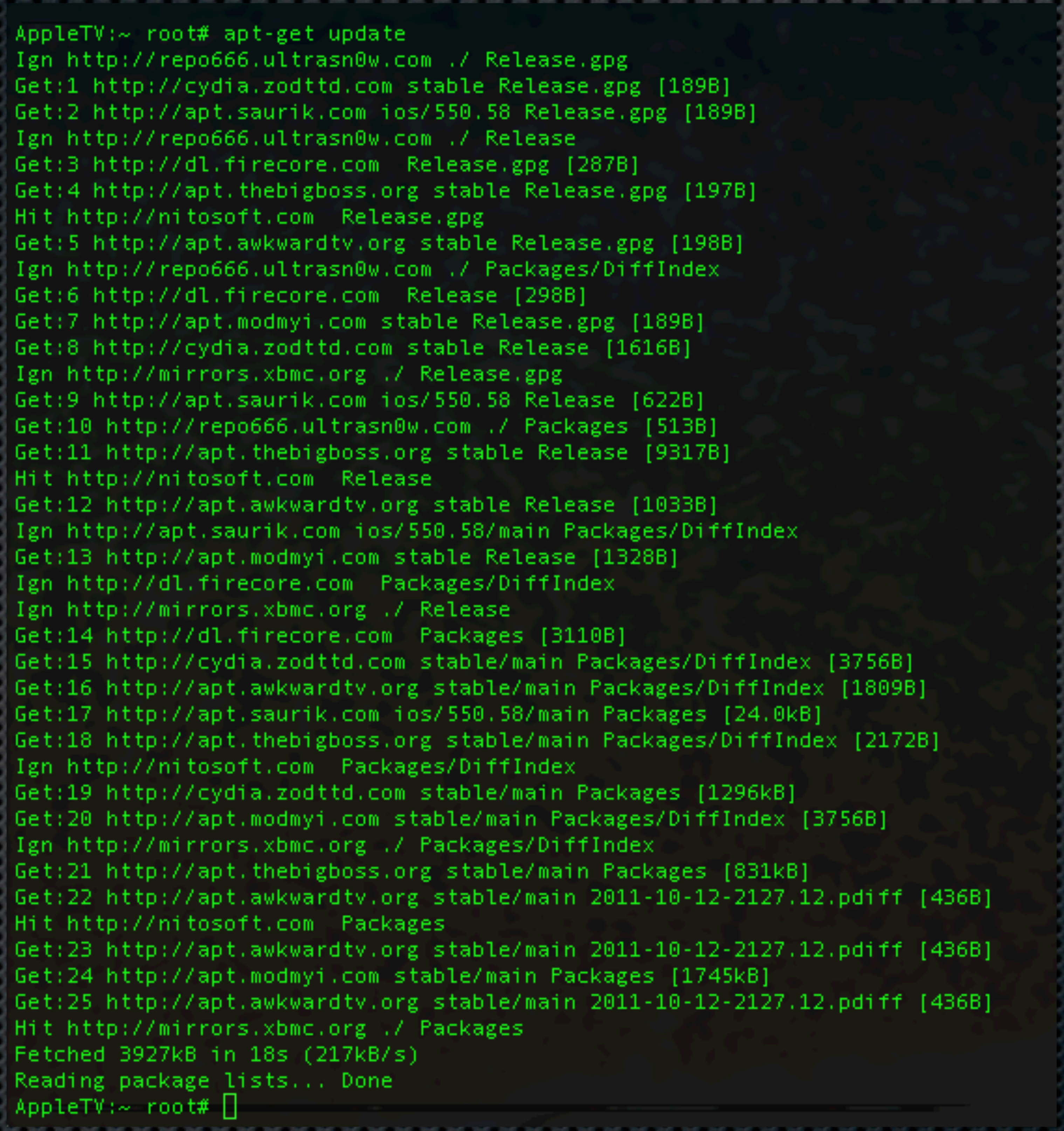
2 . Una vez Conectados al puerto 22 de nuestro Apple TV 2G no saldra lo siguente



```
AppleTV:~ root# ▯
```

Por defecto
Usuario : root
Contraseña : Aplpine

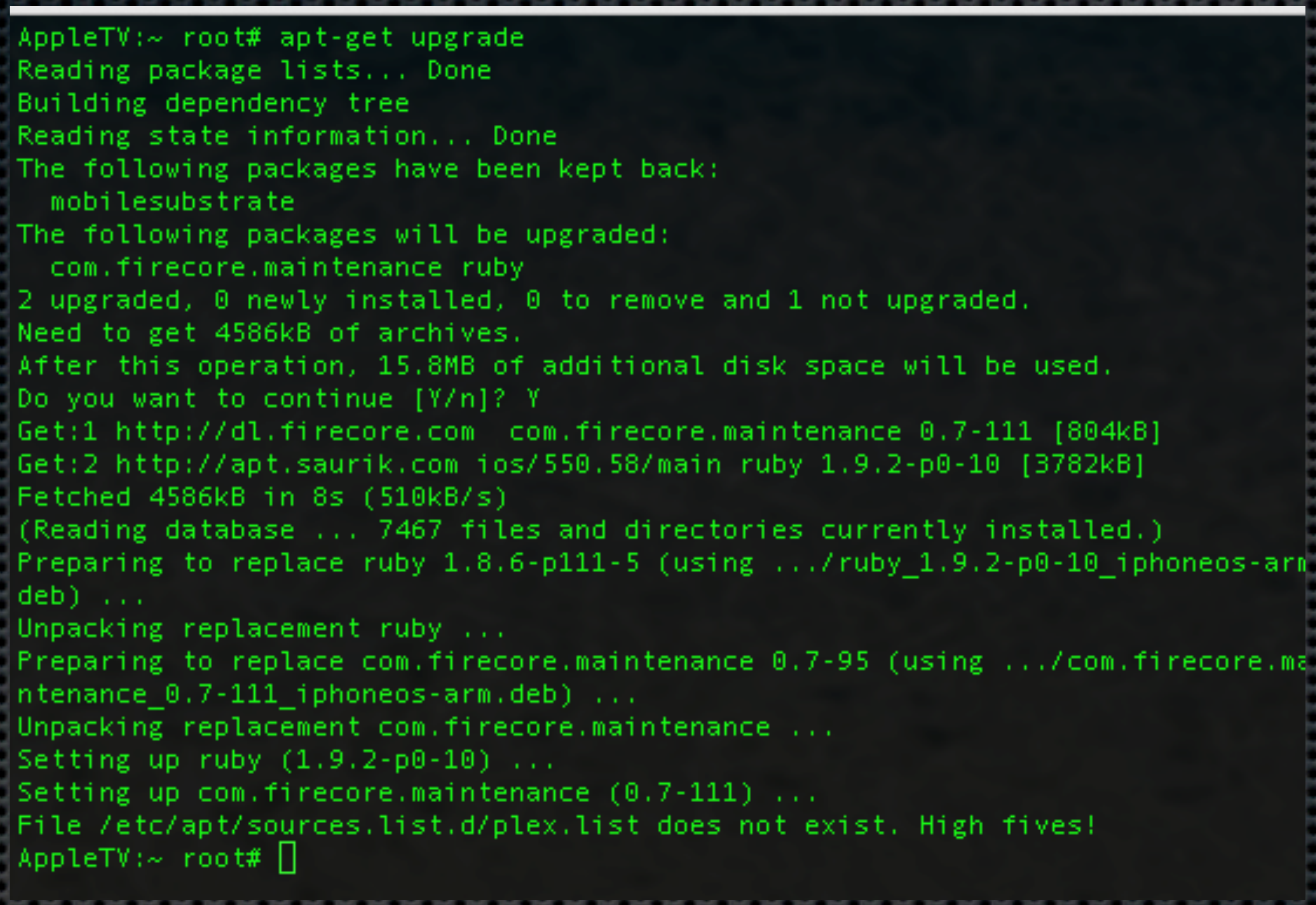
3 . Una vez que Estamos conectados en el Apple TV ponemos el siguete comando
apt-get update



```
AppleTV:~ root# apt-get update
Ign http://repo666.ultrasn0w.com ./ Release.gpg
Get:1 http://cydia.zodttd.com stable Release.gpg [189B]
Get:2 http://apt.saurik.com ios/550.58 Release.gpg [189B]
Ign http://repo666.ultrasn0w.com ./ Release
Get:3 http://dl.firecore.com  Release.gpg [287B]
Get:4 http://apt.thebigboss.org stable Release.gpg [197B]
Hit http://nitosoft.com  Release.gpg
Get:5 http://apt.awkwardtv.org stable Release.gpg [198B]
Ign http://repo666.ultrasn0w.com ./ Packages/DiffIndex
Get:6 http://dl.firecore.com  Release [298B]
Get:7 http://apt.modmyi.com stable Release.gpg [189B]
Get:8 http://cydia.zodttd.com stable Release [1616B]
Ign http://mirrors.xbmc.org ./ Release.gpg
Get:9 http://apt.saurik.com ios/550.58 Release [622B]
Get:10 http://repo666.ultrasn0w.com ./ Packages [513B]
Get:11 http://apt.thebigboss.org stable Release [9317B]
Hit http://nitosoft.com  Release
Get:12 http://apt.awkwardtv.org stable Release [1033B]
Ign http://apt.saurik.com ios/550.58/main Packages/DiffIndex
Get:13 http://apt.modmyi.com stable Release [1328B]
Ign http://dl.firecore.com  Packages/DiffIndex
Ign http://mirrors.xbmc.org ./ Release
Get:14 http://dl.firecore.com  Packages [3110B]
Get:15 http://cydia.zodttd.com stable/main Packages/DiffIndex [3756B]
Get:16 http://apt.awkwardtv.org stable/main Packages/DiffIndex [1809B]
Get:17 http://apt.saurik.com ios/550.58/main Packages [24.0kB]
Get:18 http://apt.thebigboss.org stable/main Packages/DiffIndex [2172B]
Ign http://nitosoft.com  Packages/DiffIndex
Get:19 http://cydia.zodttd.com stable/main Packages [1296kB]
Get:20 http://apt.modmyi.com stable/main Packages/DiffIndex [3756B]
Ign http://mirrors.xbmc.org ./ Packages/DiffIndex
Get:21 http://apt.thebigboss.org stable/main Packages [831kB]
Get:22 http://apt.awkwardtv.org stable/main 2011-10-12-2127.12.pdiff [436B]
Hit http://nitosoft.com  Packages
Get:23 http://apt.awkwardtv.org stable/main 2011-10-12-2127.12.pdiff [436B]
Get:24 http://apt.modmyi.com stable/main Packages [1745kB]
Get:25 http://apt.awkwardtv.org stable/main 2011-10-12-2127.12.pdiff [436B]
Hit http://mirrors.xbmc.org ./ Packages
Fetched 3927kB in 18s (217kB/s)
Reading package lists... Done
AppleTV:~ root# 
```

Tendremos que esperar unos segundos hasta que recarga dotos los sources de cydia

3 . Ahora tenemos que poner el siguente comando apt-get upgrade

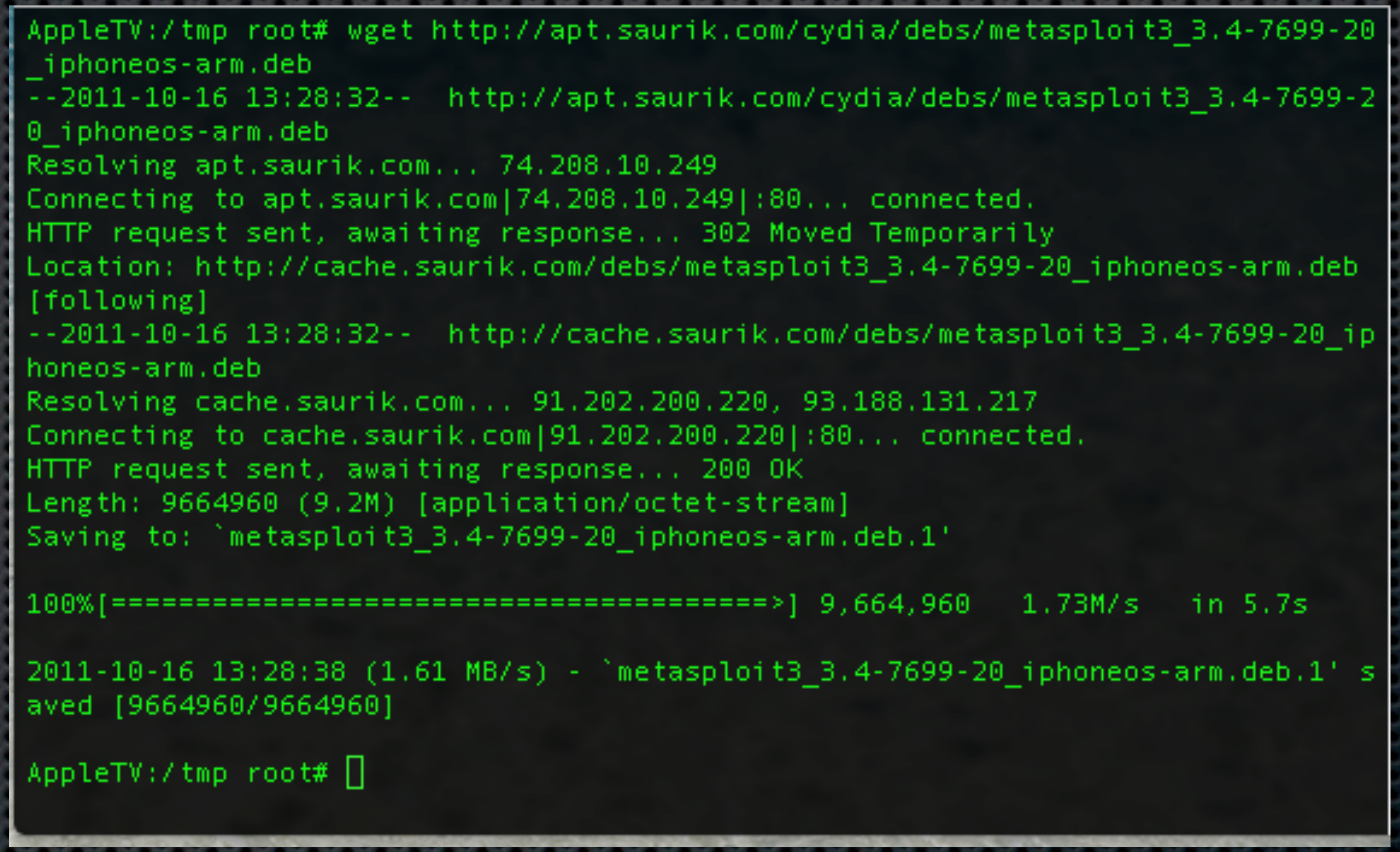


```
AppleTV:~ root# apt-get upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages have been kept back:
  mobilesubstrate
The following packages will be upgraded:
  com.firecore.maintenance ruby
2 upgraded, 0 newly installed, 0 to remove and 1 not upgraded.
Need to get 4586kB of archives.
After this operation, 15.8MB of additional disk space will be used.
Do you want to continue [Y/n]? Y
Get:1 http://dl.firecore.com  com.firecore.maintenance 0.7-111 [804kB]
Get:2 http://apt.saurik.com ios/550.58/main ruby 1.9.2-p0-10 [3782kB]
Fetched 4586kB in 8s (510kB/s)
(Reading database ... 7467 files and directories currently installed.)
Preparing to replace ruby 1.8.6-p111-5 (using .../ruby_1.9.2-p0-10_iphoneos-arm
deb) ...
Unpacking replacement ruby ...
Preparing to replace com.firecore.maintenance 0.7-95 (using .../com.firecore.ma
ntenance_0.7-111_iphoneos-arm.deb) ...
Unpacking replacement com.firecore.maintenance ...
Setting up ruby (1.9.2-p0-10) ...
Setting up com.firecore.maintenance (0.7-111) ...
File /etc/apt/sources.list.d/plex.list does not exist. High fives!
AppleTV:~ root# 
```

Si nos sale algo en plan
Do you want to continue [Y/n]?
damos Y

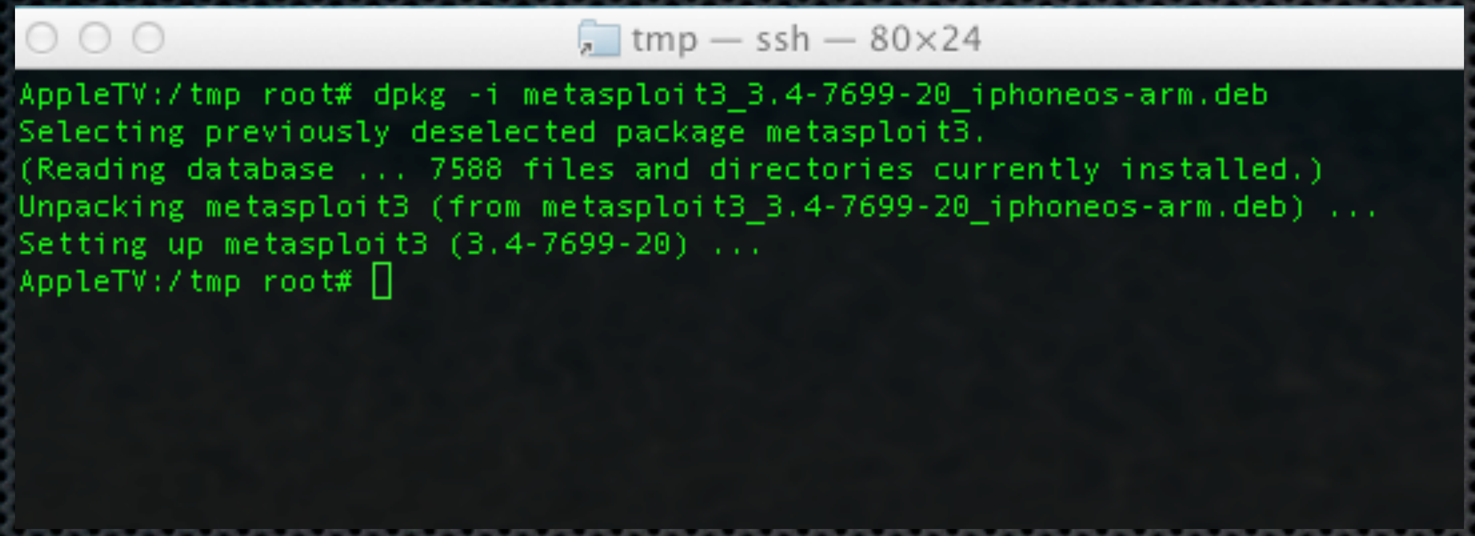
4 . vamos a la carpeta tmp
ponemos el siguente comando : cd /tmp/

Despues descargamos el Metasploit con el siguente comando
wget http://apt.saurik.com/cydia/debs/metasploit3_3.4-7699-20_iphoneos-arm.deb



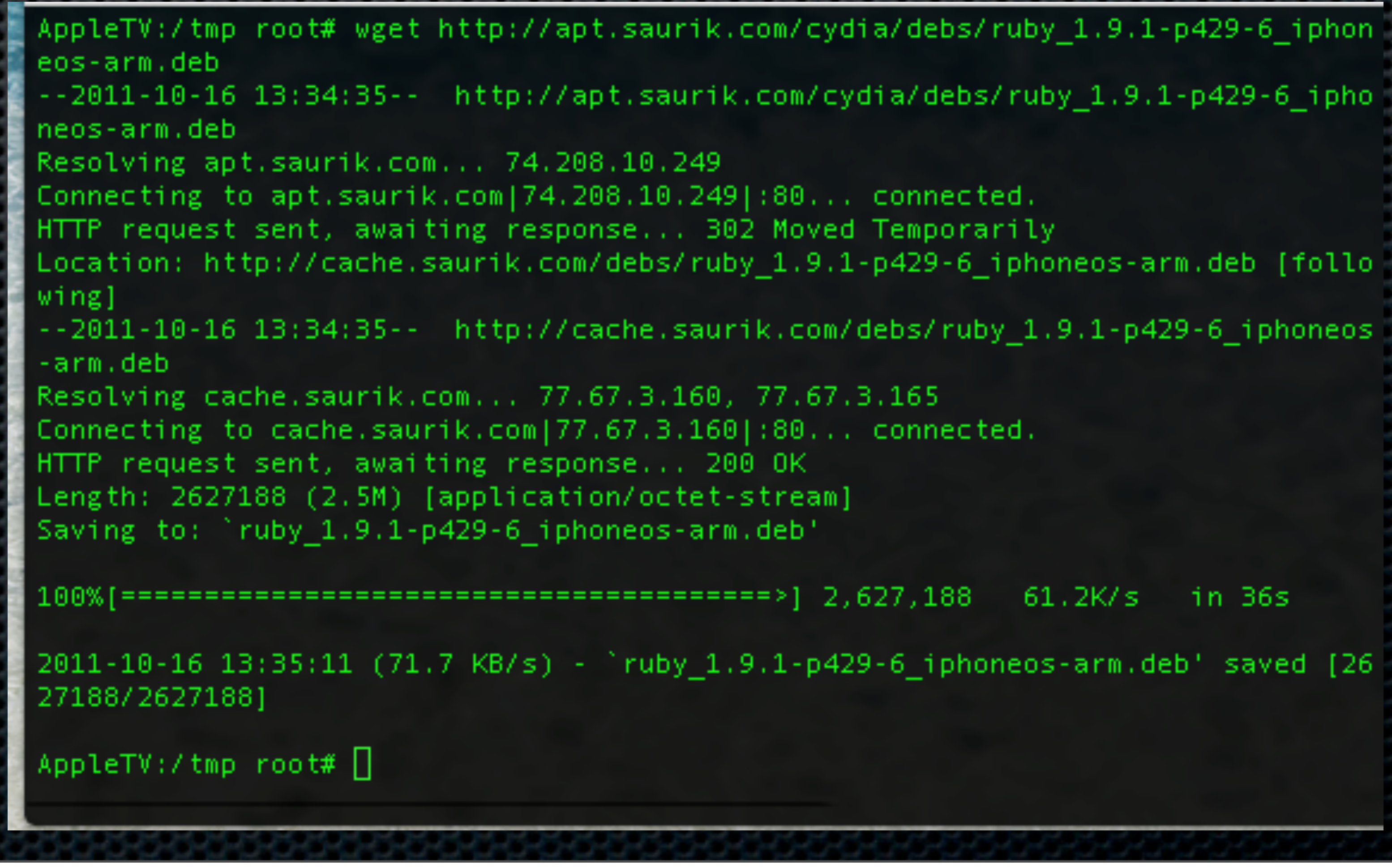
```
AppleTV:/tmp root# wget http://apt.saurik.com/cydia/debs/metasploit3_3.4-7699-20
_iphoneos-arm.deb
--2011-10-16 13:28:32--  http://apt.saurik.com/cydia/debs/metasploit3_3.4-7699-2
0_iphoneos-arm.deb
Resolving apt.saurik.com... 74.208.10.249
Connecting to apt.saurik.com|74.208.10.249|:80... connected.
HTTP request sent, awaiting response... 302 Moved Temporarily
Location: http://cache.saurik.com/debs/metasploit3_3.4-7699-20_iphoneos-arm.deb
[following]
--2011-10-16 13:28:32--  http://cache.saurik.com/debs/metasploit3_3.4-7699-20_ip
honeos-arm.deb
Resolving cache.saurik.com... 91.202.200.220, 93.188.131.217
Connecting to cache.saurik.com|91.202.200.220|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 9664960 (9.2M) [application/octet-stream]
Saving to: `metasploit3_3.4-7699-20_iphoneos-arm.deb.1'

100%[=======================================>] 9,664,960   1.73M/s   in 5.7s

2011-10-16 13:28:38 (1.61 MB/s) - `metasploit3_3.4-7699-20_iphoneos-arm.deb.1' s
aved [9664960/9664960]

AppleTV:/tmp root# 
```

5 . Ahora tenemos que instalar el Metasploit
ponemos el siguiente comando :
dpkg -i metasploit3_3.4-7699-20_iphoneos-arm.deb



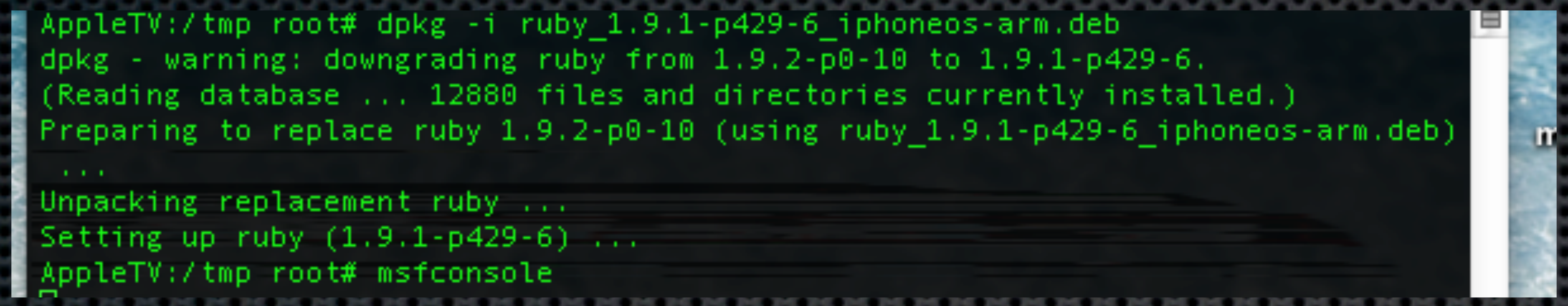
```
AppleTV:/tmp root# dpkg -i metasploit3_3.4-7699-20_iphoneos-arm.deb
Selecting previously deselected package metasploit3.
(Reading database ... 7588 files and directories currently installed.)
Unpacking metasploit3 (from metasploit3_3.4-7699-20_iphoneos-arm.deb) ...
Setting up metasploit3 (3.4-7699-20) ...
AppleTV:/tmp root# 
```

6 . Tenemos que descargar Ruby para que Metasploit funcione
wget http://apt.saurik.com/cydia/debs/ruby_1.9.1-p429-6_iphoneos-arm.deb



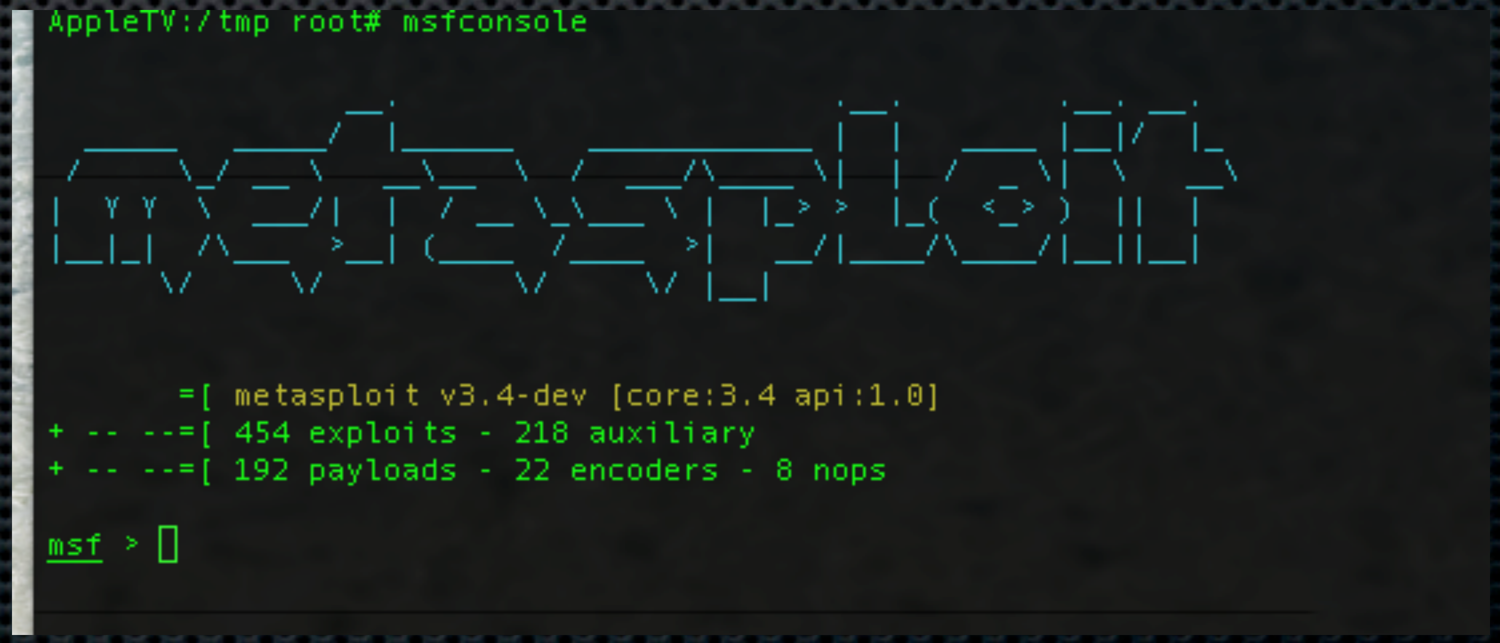
```
AppleTV:/tmp root# wget http://apt.saurik.com/cydia/debs/ruby_1.9.1-p429-6_iphon
eos-arm.deb
--2011-10-16 13:34:35--  http://apt.saurik.com/cydia/debs/ruby_1.9.1-p429-6_ipho
neos-arm.deb
Resolving apt.saurik.com... 74.208.10.249
Connecting to apt.saurik.com|74.208.10.249|:80... connected.
HTTP request sent, awaiting response... 302 Moved Temporarily
Location: http://cache.saurik.com/debs/ruby_1.9.1-p429-6_iphoneos-arm.deb [follo
wing]
--2011-10-16 13:34:35--  http://cache.saurik.com/debs/ruby_1.9.1-p429-6_iphoneos
-arm.deb
Resolving cache.saurik.com... 77.67.3.160, 77.67.3.165
Connecting to cache.saurik.com|77.67.3.160|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2627188 (2.5M) [application/octet-stream]
Saving to: `ruby_1.9.1-p429-6_iphoneos-arm.deb'

100%[======================================>] 2,627,188   61.2K/s   in 36s

2011-10-16 13:35:11 (71.7 KB/s) - `ruby_1.9.1-p429-6_iphoneos-arm.deb' saved [26
27188/2627188]

AppleTV:/tmp root# 
```

7 . Tenemos que instalar el Ruby , con el siguiente comando dpkg -i ruby_1.9.1-p429-6_iphoneos-arm.deb



```
AppleTV:/tmp root# dpkg -i ruby_1.9.1-p429-6_iphoneos-arm.deb
dpkg - warning: downgrading ruby from 1.9.2-p0-10 to 1.9.1-p429-6.
(Reading database ... 12880 files and directories currently installed.)
Preparing to replace ruby 1.9.2-p0-10 (using ruby_1.9.1-p429-6_iphoneos-arm.deb)
 ...
Unpacking replacement ruby ...
Setting up ruby (1.9.1-p429-6) ...
AppleTV:/tmp root# msfconsole
```

Ya por lo ultimo ejecutoamos Metasploit , con el siguiente comando msfconsole



```
AppleTV:/tmp root# msfconsole

                 __.                       .__.        .__. __.
  _____   _____/  |______    ____________ |  |   ____ |__|/  |_
 /     \_/ __ \   __\__  \  /  ___/\____ \|  |  /  _ \|  \   __\
|  Y Y  \  ___/|  |  / __ \_\___ \ |  |_> >  |_(  <_> )  ||  |
|__|_|  /\___  >__| (____  /____  >|   __/|____/\____/|__||__|
      \/     \/          \/     \/ |__|


       =[ metasploit v3.4-dev [core:3.4 api:1.0]
+ -- --=[ 454 exploits - 218 auxiliary
+ -- --=[ 192 payloads - 22 encoders - 8 nops

msf > 
```

Este Tutoríal lo he echo para la gente que querrá tener Metasploit en su Apple Tv , pero no me hago cargo de su mal uso ni los daños que puede provocar este programa

Echo Por

Xc0d3

**En **