# Hammered: https://cyberdefenders.org/blueteam-ctf-challenges/42

## #1 Which service did the attackers use to gain access to the system?

**Sol. ssh**

Ataque de contraseñas --> auth.log

```
$ grep -i "ssh" auth.log | grep -i "failed password" | wc -l
20338
```

## #2 What is the operating system version of the targeted system? (one word)

**Sol. 4.2.4-1ubuntu3**

```
$ grep -i linux dmesg
[    0.000000] Linux version 2.6.24-26-server (buildd@crested) (gcc version 4.2.4 (Ubuntu 4.2.4-1ubuntu3)) #1
SMP Tue Dec 1 18:26:43 UTC 2009 (Ubuntu 2.6.24-26.64-server)
[   29.245773] SELinux:  Disabled at boot.
[   30.725469] ACPI: BIOS _OSI(Linux) query ignored
[   30.725485] ACPI: Please send DMI info above to linux-acpi@vger.kernel.org
[   30.725486] ACPI: If "acpi_osi=Linux" works better, please notify linux-acpi@vger.kernel.org
[   31.195668] Linux Plug and Play Support v0.97 (c) Adam Belay
[   33.286041] Linux agpgart interface v0.102
[   33.896814] /build/buildd/linux-2.6.24/drivers/rtc/hctosys.c: unable to open rtc device (rtc0)
```

## #3 What is the name of the compromised account?

**Sol. root**

```
$ grep -E "Accepted|Failed" auth.log | grep -C 4 "Accepted password for root"
Mar 29 13:17:53 app-1 sshd[21426]: Accepted password for user1 from 76.191.195.140 port 40738 ssh2
Mar 29 13:23:46 app-1 sshd[21492]: Failed password for root from 10.0.1.2 port 51771 ssh2
Mar 29 13:24:07 app-1 sshd[21494]: Accepted password for user3 from 10.0.1.2 port 51773 ssh2
Mar 29 13:26:46 app-1 sshd[21552]: Failed password for root from 10.0.1.2 port 51780 ssh2
Mar 29 13:27:26 app-1 sshd[21556]: Accepted password for root from 10.0.1.2 port 51784 ssh2
Mar 29 23:39:05 app-1 sshd[26248]: Accepted password for user1 from 76.191.195.140 port 40654 ssh2
Mar 30 13:30:17 app-1 sshd[28893]: Accepted password for user1 from 208.80.69.74 port 33042 ssh2
Apr  1 11:20:58 app-1 sshd[4168]: Accepted password for user1 from 67.164.72.181 port 63021 ssh2
Apr  1 16:23:04 app-1 sshd[5001]: Accepted password for user3 from 10.0.1.2 port 53337 ssh2
--
Apr 19 05:41:42 app-1 sshd[8788]: Failed password for root from 219.150.161.20 port 46867 ssh2
Apr 19 05:41:42 app-1 sshd[8786]: Failed password for invalid user carlota from 219.150.161.20 port 46853 ssh2
Apr 19 05:41:42 app-1 sshd[8790]: Failed password for root from 219.150.161.20 port 46874 ssh2
Apr 19 05:41:42 app-1 sshd[8792]: Failed password for root from 219.150.161.20 port 47037 ssh2
Apr 19 05:41:44 app-1 sshd[8810]: Accepted password for root from 219.150.161.20 port 51249 ssh2
Apr 19 05:41:45 app-1 sshd[8802]: Failed password for invalid user monky from 219.150.161.20 port 50897 ssh2
Apr 19 05:41:46 app-1 sshd[8804]: Failed password for root from 219.150.161.20 port 51165 ssh2
Apr 19 05:41:46 app-1 sshd[8805]: Failed password for invalid user develop from 219.150.161.20 port 51210 ssh2
Apr 19 05:41:46 app-1 sshd[8809]: Failed password for invalid user carlotta from 219.150.161.20 port 51240 ssh2
--
Apr 19 05:42:25 app-1 sshd[9005]: Failed password for invalid user work from 219.150.161.20 port 36487 ssh2
Apr 19 05:42:25 app-1 sshd[9004]: Failed password for root from 219.150.161.20 port 36480 ssh2
Apr 19 05:42:25 app-1 sshd[9012]: Failed password for invalid user test123 from 219.150.161.20 port 36633 ssh2
Apr 19 05:42:25 app-1 sshd[9022]: Failed password for invalid user italtel from 219.150.161.20 port 36911 ssh2
Apr 19 05:42:27 app-1 sshd[9031]: Accepted password for root from 219.150.161.20 port 40877 ssh2
Apr 19 05:42:28 app-1 sshd[9028]: Failed password for root from 219.150.161.20 port 40721 ssh2
Apr 19 05:42:28 app-1 sshd[9029]: Failed password for invalid user website from 219.150.161.20 port 40720 ssh2
Apr 19 05:42:29 app-1 sshd[9032]: Failed password for invalid user test123 from 219.150.161.20 port 40880 ssh2
Apr 19 05:42:29 app-1 sshd[9025]: Failed password for invalid user carlota from 219.150.161.20 port 40682 ssh2
```

Empieza un ataque de contraseña contra ssh el 18 de abril a las 18:22:09

El 19 de abril se retoma a las 04:32:58 desde 203.81.226.86, desde 58.17.30.49 y 219.150.161.20. Es exitoso desde 219.150.161.20 a las 05:41:44:

```
Apr 19 05:41:44 app-1 sshd[8810]: Accepted password for root from 219.150.161.20 port 51249 ssh2
```

## 4# Consider that each unique IP represents a different attacker. How many attackers were able to get access to the system?cat a

**Sol. 6**

Si se cuentan las IPs desde las que se accede por sshh como root salen 18 IPs:

```
$ grep -i ssh auth.log | grep -i "Accepted" | grep root | awk '{print $11}' | sort -u | sort -n
10.0.1.2
94.52.185.9
121.11.66.70
151.82.3.201
188.131.22.69
188.131.23.37
190.167.70.87
193.1.186.197
61.168.227.12
122.226.202.12
151.81.204.141
151.81.205.100
190.166.87.164
190.167.74.184
219.150.161.20
222.66.204.246
201.229.176.217
222.169.224.197
$ grep -i ssh auth.log | grep -i "Accepted" | grep root | awk '{print $11}' | sort -u | sort -n | wc -l
18
```

Si restringimos la respuesta a aquellas IPs donde además de acceso como root hubo fallos de autenticación, la lista se reduce a 9. Con el comando diff o comm se pueden localizar las IPs que están en el fichero ENTRO (IPs con acceso por root) y ATACANTE (IPs con fallos de autenticación como root):

```
$ grep -i ssh auth.log | grep -i "Accepted" | grep root | awk '{print $11}' | sort -u | sort -g > ENTRO
$ grep -i ssh auth.log | grep -vi invalid | grep -i "failed" | grep root | awk '{print $11}' | sort -u | sort -
g > ATACANTE
$ diff -u ENTRO ATACANTE
--- ENTRO     2022-02-21 20:55:24.745199297 +0100
+++ ATACANTE  2022-02-21 20:55:33.220986778 +0100
@@ -1,18 +1,38 @@
+8.12.45.242
 10.0.1.2
+12.172.224.140
+24.192.113.91
+58.17.30.49
+59.46.39.148
+61.151.246.140
 61.168.227.12
+65.208.122.48
+78.38.27.21
+89.46.213.128
 94.52.185.9
+114.80.166.219
+116.6.19.70
 121.11.66.70
+122.102.64.54
+122.165.9.200
 122.226.202.12
-151.81.204.141
-151.81.205.100
-151.82.3.201
-188.131.22.69
```

```
+124.207.117.9
+124.51.108.68
+125.235.4.130
+173.9.147.165
 188.131.23.37
-190.166.87.164
-190.167.70.87
-190.167.74.184
-193.1.186.197
-201.229.176.217
+190.4.21.190
+200.72.254.54
+201.64.234.2
+203.81.226.86
+209.59.222.166
+210.68.70.170
+211.154.254.248
+217.15.55.133
+218.56.61.114
+219.139.243.236
 219.150.161.20
+220.170.79.247
 222.169.224.197
+222.240.223.88
 222.66.204.246
```

De esas IPs, revisando el fichero auth.log para cada una de ellas se puede deducir que:

- No asociadas a ataques de contraseña: 10.0.1.2, 94.52.185.9, 188.131.23.37
- Sí asociadas a ataques de contraseña: 61.168.227.12, 122.226.202.12, 121.11.66.70, 219.150.161.20, 222.169.224.197, 222.66.204.246

```
$ grep 10.0.1.2 auth.log  | grep root
Mar 29 13:23:46 app-1 sshd[21492]: Failed password for root from 10.0.1.2 port 51771 ssh2
Mar 29 13:26:46 app-1 sshd[21552]: Failed password for root from 10.0.1.2 port 51780 ssh2
Mar 29 13:27:26 app-1 sshd[21556]: Accepted password for root from 10.0.1.2 port 51784 ssh2

$ grep 222.66.204.246 auth.log  | grep root | head
Apr 19 10:41:42 app-1 sshd[27330]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh
ruser= rhost=222.66.204.246  user=root
Apr 19 10:41:45 app-1 sshd[27330]: Failed password for root from 222.66.204.246 port 51189 ssh2
Apr 19 10:41:46 app-1 sshd[27337]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh
ruser= rhost=222.66.204.246  user=root
Apr 19 10:41:48 app-1 sshd[27337]: Failed password for root from 222.66.204.246 port 51850 ssh2
Apr 19 10:41:50 app-1 sshd[27345]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh
ruser= rhost=222.66.204.246  user=root
Apr 19 10:41:51 app-1 sshd[27345]: Failed password for root from 222.66.204.246 port 52487 ssh2
Apr 19 10:42:02 app-1 sshd[27374]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh
ruser= rhost=222.66.204.246  user=root
Apr 19 10:42:03 app-1 sshd[27374]: Failed password for root from 222.66.204.246 port 54754 ssh2
Apr 19 10:42:05 app-1 sshd[27382]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh
ruser= rhost=222.66.204.246  user=root
Apr 19 10:42:07 app-1 sshd[27382]: Failed password for root from 222.66.204.246 port 55630 ssh2
...
```

## 5# Which attacker's IP address successfully logged into the system the most number of times?

### Sol. 219.150.151.20

```
$ grep -i "Accepted password" auth.log | awk '{print $9" - "$11}' | sort | uniq -c | sort -nr
     22 user1 - 76.191.195.140
     20 dhg - 190.166.87.164
     13 user3 - 10.0.1.2
      6 user1 - 65.88.2.5
      6 user1 - 208.80.69.74
      5 user2 - 71.132.129.212
```

```
      4 user3 - 10.0.1.4
      4 root - 219.150.161.20
      4 root - 188.131.23.37
      3 user3 - 192.168.126.1
      3 root - 190.166.87.164
      2 user3 - 208.80.69.69
      2 root - 122.226.202.12
      2 root - 121.11.66.70
      2 dhg - 190.167.74.184
      1 user3 - 65.195.182.120
      1 user3 - 208.80.69.74
      1 user1 - 67.164.72.181
      1 user1 - 65.195.182.120
      1 user1 - 208.80.69.70
      1 user1 - 166.129.196.88
      1 root - 94.52.185.9
      1 root - 61.168.227.12
      1 root - 222.66.204.246
      1 root - 222.169.224.197
      1 root - 201.229.176.217
      1 root - 193.1.186.197
      1 root - 190.167.74.184
      1 root - 190.167.70.87
      1 root - 188.131.22.69
      1 root - 151.82.3.201
      1 root - 151.81.205.100
      1 root - 151.81.204.141
      1 root - 10.0.1.2
      1 fido - 94.52.185.9
```

## #6 How many requests were sent to the Apache Server?

### Sol. 365

```
$ wc -l apache2/www-access.log
365 apache2/www-access.log
```

## #7 How many rules have been added to the firewall?

### Sol. 6

```
$ grep -i iptables auth.log
Apr 15 12:49:09 app-1 sudo:   user1 : TTY=pts/0 ; PWD=/opt/software/web/app ; USER=root ;
COMMAND=/usr/bin/tee ../templates/proxy/iptables.conf
Apr 15 15:06:13 app-1 sudo:   user1 : TTY=pts/1 ; PWD=/opt/software/web/app ; USER=root ;
COMMAND=/usr/bin/tee ../templates/proxy/iptables.conf
Apr 15 15:17:45 app-1 sudo:   user1 : TTY=pts/1 ; PWD=/opt/software/web/app ; USER=root ;
COMMAND=/usr/bin/tee ../templates/proxy/iptables.conf
Apr 15 15:18:23 app-1 sudo:   user1 : TTY=pts/1 ; PWD=/opt/software/web/app ; USER=root ;
COMMAND=/usr/bin/tee ../templates/proxy/iptables.conf
Apr 24 19:25:37 app-1 sudo:     root : TTY=pts/2 ; PWD=/etc ; USER=root ; COMMAND=/sbin/iptables -L
Apr 24 20:03:06 app-1 sudo:     root : TTY=pts/2 ; PWD=/etc ; USER=root ; COMMAND=/sbin/iptables -A INPUT -p
ssh -dport 2424 -j ACCEPT
Apr 24 20:03:44 app-1 sudo:     root : TTY=pts/2 ; PWD=/etc ; USER=root ; COMMAND=/sbin/iptables -A INPUT -p
tcp -dport 53 -j ACCEPT
Apr 24 20:04:13 app-1 sudo:     root : TTY=pts/2 ; PWD=/etc ; USER=root ; COMMAND=/sbin/iptables -A INPUT -p
udp -dport 53 -j ACCEPT
Apr 24 20:06:22 app-1 sudo:     root : TTY=pts/2 ; PWD=/etc ; USER=root ; COMMAND=/sbin/iptables -A INPUT -p
tcp --dport ssh -j ACCEPT
Apr 24 20:11:00 app-1 sudo:     root : TTY=pts/2 ; PWD=/etc ; USER=root ; COMMAND=/sbin/iptables -A INPUT -p
tcp --dport 53 -j ACCEPT
Apr 24 20:11:08 app-1 sudo:     root : TTY=pts/2 ; PWD=/etc ; USER=root ; COMMAND=/sbin/iptables -A INPUT -p
tcp --dport 113 -j ACCEPT
$ grep -i iptables auth.log | grep "ACCEPT" | wc -l
6
```

## #8 One of the downloaded files to the target system is a scanning tool. Provide the tool name.

### Sol. nmap

```
$ grep -i installed dpkg.log | cut -d " " -f 5 | sort -u
...
linux-libc-dev
lsb-build
make
nmap
po-debconf
python-celementtree
python-dateutil
python-elementtree
python-libxml2
python-rpm
python-tz
python-urlgrabber
rpm
shared-mime-info
sudo
tcl8.4
tcl8.5
tcl8.5-dev
tk8.4
tzdata
x11-apps
x11-common
x11-session-utils
x11-utils
x11-xfs-utils
x11-xkb-utils
x11-xserver-utils
xauth
xbase-clients
xinit
yum
$ grep -i installed dpkg.log | grep -i nmap
2010-04-24 19:38:15 status half-installed nmap 4.53-3
2010-04-24 19:38:16 status installed nmap 4.53-3
```

## #9 When was the last login from the attacker with IP 219.150.161.20? Format: MM/DD/YYYY HH:MM:SS AM

### Sol. 04/19/2010 05:56:05 AM

```
$ grep "219.150.161.20" auth.log  | grep -vi ssh
$ grep "219.150.161.20" auth.log  | grep -i "Accepted password"
Apr 19 05:41:44 app-1 sshd[8810]: Accepted password for root from 219.150.161.20 port 51249 ssh2
Apr 19 05:42:27 app-1 sshd[9031]: Accepted password for root from 219.150.161.20 port 40877 ssh2
Apr 19 05:55:20 app-1 sshd[12996]: Accepted password for root from 219.150.161.20 port 55545 ssh2
Apr 19 05:56:05 app-1 sshd[13218]: Accepted password for root from 219.150.161.20 port 36585 ssh2
```

El año se puede ver en access.log de Apache o en dpkg.log

## #10 The database displayed two warning messages, provide the most important and dangerous one.

### Sol. mysql.user contains 2 root accounts without password!

```
$ grep -i mysql daemon.log | grep -i warning
Mar 18 10:18:42 app-1 /etc/mysql/debian-start[7566]: WARNING: mysql.user contains 2 root accounts without
password!
Mar 18 17:01:44 app-1 /etc/mysql/debian-start[14717]: WARNING: mysql.user contains 2 root accounts without
```

```
password!
Mar 22 13:49:49 app-1 /etc/mysql/debian-start[5599]: WARNING: mysql.user contains 2 root accounts without
password!
Mar 22 18:43:41 app-1 /etc/mysql/debian-start[4755]: WARNING: mysql.user contains 2 root accounts without
password!
Mar 22 18:45:25 app-1 /etc/mysql/debian-start[4749]: WARNING: mysql.user contains 2 root accounts without
password!
Mar 25 11:56:53 app-1 /etc/mysql/debian-start[4848]: WARNING: mysql.user contains 2 root accounts without
password!
Apr 14 14:44:34 app-1 /etc/mysql/debian-start[5369]: WARNING: mysql.user contains 2 root accounts without
password!
Apr 14 14:44:36 app-1 /etc/mysql/debian-start[5624]: WARNING: mysqlcheck has found corrupt tables
Apr 18 18:04:00 app-1 /etc/mysql/debian-start[4647]: WARNING: mysql.user contains 2 root accounts without
password!
Apr 24 20:21:24 app-1 /etc/mysql/debian-start[5427]: WARNING: mysql.user contains 2 root accounts without
password!
Apr 28 07:34:26 app-1 /etc/mysql/debian-start[4782]: WARNING: mysql.user contains 2 root accounts without
password!
Apr 28 07:34:27 app-1 /etc/mysql/debian-start[5032]: WARNING: mysqlcheck has found corrupt tables
Apr 28 07:34:27 app-1 /etc/mysql/debian-start[5032]: warning  : 1 client is using or hasn't closed the table
properly
Apr 28 07:34:27 app-1 /etc/mysql/debian-start[5032]: warning  : 1 client is using or hasn't closed the table
properly
May  2 23:05:54 app-1 /etc/mysql/debian-start[4774]: WARNING: mysql.user contains 2 root accounts without
password!
$ grep -i mysql daemon.log | grep -i warning | awk -F " " '{for(i=6;i<=NF;i++) printf ("%s",$i " "); printf("\
n") }' | sort -u
warning : 1 client is using or hasn't closed the table properly
WARNING: mysqlcheck has found corrupt tables
WARNING: mysql.user contains 2 root accounts without password!
```

## #11 Multiple accounts were created on the target system. Which one was created on Apr 26 04:43:15?

### Sol. wind3str0y

```
$ grep useradd auth.log
Mar 16 08:12:13 app-1 useradd[4692]: new user: name=user4, UID=1001, GID=1001, home=/home/user4,
shell=/bin/bash
Mar 16 08:12:38 app-1 useradd[4703]: new user: name=user1, UID=1001, GID=1001, home=/home/user1,
shell=/bin/bash
Mar 16 08:12:55 app-1 useradd[4711]: new user: name=user2, UID=1002, GID=1002, home=/home/user2,
shell=/bin/bash
Mar 16 08:25:22 app-1 useradd[4845]: new user: name=sshd, UID=104, GID=65534, home=/var/run/sshd,
shell=/usr/sbin/nologin
Mar 18 10:15:42 app-1 useradd[5393]: new user: name=Debian-exim, UID=105, GID=114, home=/var/spool/exim4,
shell=/bin/false
Mar 18 10:18:26 app-1 useradd[6966]: new user: name=mysql, UID=106, GID=115, home=/var/lib/mysql,
shell=/bin/false
Apr 19 22:38:00 app-1 useradd[2019]: new user: name=packet, UID=0, GID=0, home=/home/packet, shell=/bin/sh
Apr 19 22:45:13 app-1 useradd[2053]: new user: name=dhg, UID=1003, GID=1003, home=/home/dhg, shell=/bin/bash
Apr 24 19:27:35 app-1 useradd[1386]: new user: name=messagebus, UID=108, GID=117, home=/var/run/dbus,
shell=/bin/false
Apr 25 10:41:44 app-1 useradd[9596]: new group: name=fido, GID=1004
Apr 25 10:41:44 app-1 useradd[9596]: new user: name=fido, UID=0, GID=1004, home=/home/fido, shell=/bin/sh
Apr 26 04:43:15 app-1 useradd[20115]: new user: name=wind3str0y, UID=1004, GID=1005, home=/home/wind3str0y,
shell=/bin/bash
```

## #12 Few attackers were using a proxy to run their scans. What is the corresponding user-agent used by this proxy?

### Sol. pxyscand/2.1

```
$ awk -F "\"" '{print $6}' apache2/www-access.log | sort | uniq -c
      8 -
    272 Apple-PubSub/65.12.1
```

```
     13 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
     15 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
      4 Mozilla/4.0 (compatible; NaverBot/1.0; http://help.naver.com/customer_webtxt_02.jsp)
     20 Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.6; en-US; rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3
      6 Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_2; en-us) AppleWebKit/531.21.8 (KHTML, like Gecko)
Version/4.0.4 Safari/531.21.10
      1 Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_2; en-us) AppleWebKit/531.22.7 (KHTML, like Gecko)
Version/4.0.5 Safari/531.22.7
      1 Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/532.5 (KHTML, like Gecko)
Chrome/4.1.249.1045 Safari/532.5
      3 Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/532.5 (KHTML, like Gecko)
Chrome/4.1.249.1059 Safari/532.5
      1 Mozilla/5.0 (Windows; U; Windows NT 5.1; es-ES; rv:1.9.0.19) Gecko/2010031422 Firefox/3.0.19
      3 pxyscand/2.1
     18 WordPress/2.9.2; http://www.domain.org
$ awk -F "\"" '{print $6}' apache2/www-media.log | sort | uniq -c
      9 iearthworm/1.0, iearthworm@yahoo.com.cn
     80 Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.6; en-US; rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3
     52 Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_2; en-us) AppleWebKit/531.21.8 (KHTML, like Gecko)
Version/4.0.4 Safari/531.21.10
     47 Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_2; en-us) AppleWebKit/531.22.7 (KHTML, like Gecko)
Version/4.0.5 Safari/531.22.7
     14 Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/532.5 (KHTML, like Gecko)
Chrome/4.1.249.1045 Safari/532.5
     13 Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/532.5 (KHTML, like Gecko)
Chrome/4.1.249.1059 Safari/532.5
     14 Mozilla/5.0 (Windows; U; Windows NT 5.1; es-ES; rv:1.9.0.19) Gecko/2010031422 Firefox/3.0.19
```