Challenge 5: Log Mysteries (intermediate)

(provided by Raffael Marty from the Bay Area Chapter, Anton Chuvakin from the Hawaiian Chapter, Sebastien Tricaud from the French Chapter) takes you into the world of virtual systems and confusing log data. In this challenge, figure out what happened to a virtual server using all the logs from a possibly compromised server.

The questions are a more open ended than past challenges. To score highly, we recommend to answer the following way:

□ Accuracy is highly encouraged to get the highest note
□ You must explain tools you used and how
□ If you use visualization tools such as afterglow, picviz, graphviz, gnuplot etc. explain why this was better (than other tools, than other visualization): such as good timeline representation etc.
□ Outline HOW you found things

Submission Template

Submit your solution at http://www.honeynet.org/challenge2010/ by 17:00 EST, Thursday, September 30th 2010. Results will be released on Thursday, October 21st 2010.

Name (required): William Söderberg	Email (required): william.soderberg@gmail.com
Country (optional): Sweden	Profession (optional): X Student _ Security Professional _ Other

1. Was the system compromised and when? How do you know that for sure?	Possible Points: 5

Tools Used: Python script I wrote: http://pastebin.com/xmTPSsm7
Awarded Points:

Answer

The system was definitely compromised. I know this for sure because I've analyzed the auth.log file with a script and found out that several brute force attackers eventually guessed the right root account password. Output of script in the end of document.

1. If the system was compromised, what was the method used?	Possible Points: 5

Tools Used: Aforementioned script
Awarded Points:

Answer

SSH Brute Force attacks was successfully launched against the system. They gained root access.

1. Can you locate how many attackers failed? If some succeeded, how many were they? How many stopped attacking after the first success? Possible Points: 5

Tools Used: Aforementioned python script
Awarded Points:

Answer

I'd say 31 attackers failed to gain access via brute force attempts/password guessing attempts on the sshd. 6 attackers succeeded with the brute force attempts. **My script reveals all this information.**
3 attackers ran a proxy scanner (from same subnet) called pxyscand against the server. I found this by running: **cat apache2/www-access.log | grep CONNECT**
12 attackers tried to use the web server as a proxy. All failed. I checked this by running **cat www-access.log | grep 'http://' | grep -v POST**. I then just quickly scanned through all the output of that command after unique IP's.

1. What happened after the brute force attack? Possible Points: 5
2.

Tools Used: cat, more, less, grep, google
Awarded Points:

Answer

Several user accounts was created. packet, dhg, messagebus, fido and wind3str0y. Software was installed. nmap, psybnc and eggdrop. Firewall rules was added. Following ports was added to ACCEPT incoming traffic: Port 53 TCP/UDP opened. Port 22 TCP... Port 113 TCP.

I found this by looking at the log files after the first successful brute force attack. I checked the daemon.log, auth.log, dpkg.log using more. I filtered out large amounts of data that was of no use for me using the grep -v command.

Like: cat auth.log | grep -v -i sshd | grep -v -i pam_unix > tmp

Then I used more to check the tmp file for date entries after the brute force attackers gained access.

1. Locate the authentication logs, was a bruteforce attack performed? if yes how many? Possible Points: 5

Tools Used: Aforementioned script
Awarded Points:

Answer

37 Brute Force attacks was performed against the SSH daemon. Some might not be a real brute force but just a few failed login attempts over a short period of time. People

trying a few passwords and then moving on. Not really what I'd like to call brute force. I used my script output to find this information.

1. What is the time line of significant events? How certain are you of the timing? Possible Points: 5

Tools Used: Aforementioned script and cat, more, less, grep, google
Awarded Points:

Answer

Attacker IP: 122.226.202.12
Apr 23 03:11:03 : root < Brute Force tool guesses right password
Apr 23 03:20:41 : root < 1st login by attacker
Attacker IP: 121.11.66.70
Apr 20 06:13:03 : root < Brute Force tool guesses right password
Apr 24 11:36:19 : root < 1st login by attacker
Attacker IP: 222.66.204.246
Apr 19 10:45:36 : root < Brute Force tool guesses right password
Attacker IP: 61.168.227.12
Apr 24 15:28:37 : root < Brute Force tool guesses right password
Attacker IP: 222.169.224.197
Apr 22 11:02:15 : root < Brute Force tool guesses right password
Attacker IP: 219.150.161.20
Apr 19 05:41:44 : root < Brute Force tool guesses right password
Apr 19 05:42:27 : root < 1st login by attacker
Apr 19 05:55:20 : root < 2nd
Apr 19 05:56:05 : root < 3rd

I am very certain of these timings. The attackers creates these accounts (cat auth.log | grep 'new user'):

```
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 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
```

1. Anything else that looks suspicious in the logs? Any misconfigurations? Other issues? Possible Points: 5

Tools Used: cat, more, less, grep, google
Awarded Points:

Answer

I found things mostly by looking in the log files to get the general feel of how the normal log entries looked like. Then I used grep -v to remove that normal output to scrutinize the not so normal entries.

The SSH daemon allows root login. I'd say that's a misconfiguration.
It also starts to listen to both IPv4 and IPv6 and thus results in this error message in the logs:

```
Apr 28 07:34:23 app-1 sshd[4615]: error: Bind to port 22 on
0.0.0.0 failed: Address already in use.
```

There's indications that sshd was flawed and that an attacker maybe tried to exploit the daemon:

```
Apr 21 12:12:24 app-1 kernel: : [237397.126529]
sshd[2798]: segfault at 0 rip 8048e33 rsp ffdf4600 error 4
```

Plenty of these segfaults are to be found in the logs. I was not able to determine if they were successful or not.

```
Apr 28 07:34:26 app-1 /etc/mysql/debian-start[4782]:
WARNING: mysql.user contains 2 root accounts without
password!
```

This is a security misconfiguration. It existed before the attackers gained access to the system.

apache2/www-error.log contains:

```
[Tue Apr 20 00:00:35 2010] [error] [client 193.109.122.33]
request failed: error reading the headers
[Fri Apr 23 10:34:42 2010] [error] [client 193.109.122.18]
request failed: error reading the headers
[Sat Apr 24 18:52:24 2010] [error] [client 193.109.122.15]
request failed: error reading the headers
```

cat apache2/www-access.log | grep CONNECT reveals:

```
193.109.122.56 - - [20/Apr/2010:00:00:01 -0700]
"CONNECT 72.51.18.254:6677 HTTP/1.0" 301 - "-"
"pxyscand/2.1" oFs91QoAAQ4AAAQFlmcAAAAL
1213441
193.109.122.57 - - [23/Apr/2010:10:34:20 -0700]
"CONNECT 72.51.18.254:6677 HTTP/1.0" 301 - "-"
"pxyscand/2.1" 1l730AoAAQ4AACkeBjsAAAAB 156351
193.109.122.52 - - [24/Apr/2010:18:51:52 -0700]
"CONNECT 72.51.18.254:6677 HTTP/1.0" 301 - "-"
"pxyscand/2.1" 54ydwAoAAQ4AAEHECacAAAAB
571386
```

The timestamps are equivalent enough. It's safe to assume that someone ran a network proxy scanner against the server.

cat www-access.log | grep 'http://' | grep -v POST

reveals several entries where attackers are trying to make the web service to act as a proxy. Entries like this:

```
221.192.199.35 - - [24/Apr/2010:05:00:50 -0700] "GET
http://www.wantsfly.com/prx2.php?hash=FABB83E72D135F
1018046CC4005088B36F8D0BEDCEA7 HTTP/1.0" 404
```

```
1466 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
5.0)" S4QF0woAAQ4AAEHECaMAAAAB 417959
```

The httpd returns 404 or 400 for all of these entries. Unsuccessful attempts.

1. Was an automatic tool used to perform the attack? if yes which one? Possible Points: 5

Tools Used:
Awarded Points:

Answer
A brute force tool was most definitely used. Which one I cannot tell.
A proxy scanner called pxyscand was used. Version 2.1. I found this by running this command: **cat apache2/www-access.log | grep CONNECT**.

1. What can you say about the attacker's goals and methods? Possible Points: 5

Tools Used: cat, more, less, grep, google and aforementioned script
Awarded Points:

Answer
The attacker's goals was to use the system as an IRC bouncer and possibly an attack platform. This is concluded by the following: The attacker downloaded and installed **psybnc-linux** and **eggdrop** as well as **nmap** on the system.

The attacker's methods was sloppy and careless. He/she generated large amounts of traces of his/hers presence on the system in the log files. He/she didn't care to delete them. He/she tried to change firewall rules without knowing how to do so. A good attacker would have done this in a virtual environment before trying it in a compromised system. Experimenting in a compromised system when it can be done elsewhere is sloppy.

Bonus. What would you have done to avoid this attack?

Possible Points: 5

Tools Used: http://cipherdyne.org/fwknop/
Awarded Points:

Answer
I would have implemented fwknop for the SSH daemon to prevent all the brute force attacks and exploitation attempts. I don't think fail2ban or changing port numbers are a good way to mitigate attacks. A persistent hacker will not be stopped by changing a port number which the service listens to. fail2ban won't stop an attacker that possesses a bot-net with a thousand or more infected machines as far as I know. I would also have changed sshd.conf to not accept root logins.

Script output

```
Total number of attackers: 37
Total number of successful attackers: 6
Total number of failed attackers: 31
Number of failed login attempts: 20319

Attacker IP: 217.15.55.133
Start time: Apr 22 14:15:25
End time: Apr 22 14:48:33
Login attempts: 427

Attacker IP: 122.165.9.200
Start time: Apr 26 07:18:09
End time: Apr 26 07:18:46
Login attempts: 7

Attacker IP: 173.9.147.165
Start time: Apr 23 20:06:09
End time: Apr 23 20:10:03
Login attempts: 145

Attacker IP: 203.81.226.86
Start time: Apr 19 04:32:58
End time: Apr 19 09:38:40
Login attempts: 79

Attacker IP: 58.17.30.49
Start time: Apr 19 05:18:38
End time: Apr 19 05:38:50
Login attempts: 263

Attacker IP: 219.139.243.236
Start time: Apr 26 06:10:17
End time: Apr 26 06:12:33
Login attempts: 28

Attacker IP: 122.226.202.12
Start time: Apr 23 03:06:17
End time: Apr 23 03:42:03
Login attempts: 513
Successful attempts: 2
Ratio: 0.00389863547758
Compromised account details:
Apr 23 03:11:03 : root
Apr 23 03:20:41 : root

Attacker IP: 124.51.108.68
Start time: Apr 24 10:26:54
End time: Apr 24 10:37:34
Login attempts: 158

Attacker IP: 200.72.254.54
Start time: Apr 19 10:01:08
End time: Apr 19 11:16:19
Login attempts: 26

Attacker IP: 190.4.21.190
Start time: Apr 20 16:27:47
End time: Apr 20 16:28:35
```

```
Login attempts: 10

Attacker IP: 121.11.66.70
Start time: Apr 20 05:48:07
End time: Apr 24 11:41:59
Login attempts: 1435
Successful attempts: 2
Ratio: 0.001393728223
Compromised account details:
Apr 20 06:13:03 : root
Apr 24 11:36:19 : root

Attacker IP: 222.66.204.246
Start time: Apr 19 10:41:41
End time: Apr 19 11:24:39
Login attempts: 1573
Successful attempts: 1
Ratio: 0.000635727908455
Compromised account details:
Apr 19 10:45:36 : root

Attacker IP: 222.240.223.88
Start time: Apr 20 06:26:20
End time: Apr 20 06:26:37
Login attempts: 3

Attacker IP: 61.168.227.12
Start time: Apr 24 15:26:00
End time: Apr 24 15:40:00
Login attempts: 213
Successful attempts: 1
Ratio: 0.00469483568075
Compromised account details:
Apr 24 15:28:37 : root

Attacker IP: 78.38.27.21
Start time: Apr 20 10:20:52
End time: Apr 20 10:21:14
Login attempts: 4

Attacker IP: 89.46.213.128
Start time: Apr 19 11:30:10
End time: Apr 19 11:40:32
Login attempts: 7

Attacker IP: 61.151.246.140
Start time: Apr 18 18:22:09
End time: Apr 18 18:22:55
Login attempts: 13

Attacker IP: 8.12.45.242
Start time: Apr 24 12:55:04
End time: Apr 24 14:49:42
Login attempts: 3037

Attacker IP: 220.170.79.247
Start time: Apr 20 14:15:41
End time: Apr 20 14:16:36
Login attempts: 15

Attacker IP: 65.208.122.48
Start time: Apr 26 08:23:47
```

```
End time: Apr 26 08:40:36
Login attempts: 306

Attacker IP: 211.154.254.248
Start time: Apr 24 03:19:02
End time: Apr 24 03:51:21
Login attempts: 455

Attacker IP: 125.235.4.130
Start time: Apr 20 02:48:10
End time: Apr 20 02:57:45
Login attempts: 113

Attacker IP: 124.207.117.9
Start time: Apr 23 17:20:53
End time: Apr 23 18:06:32
Login attempts: 650

Attacker IP: 116.6.19.70
Start time: Apr 25 00:54:38
End time: Apr 25 01:12:02
Login attempts: 180

Attacker IP: 59.46.39.148
Start time: Apr 20 10:24:18
End time: Apr 20 10:27:33
Login attempts: 51

Attacker IP: 218.56.61.114
Start time: Apr 23 12:44:50
End time: Apr 23 12:45:21
Login attempts: 9

Attacker IP: 222.169.224.197
Start time: Apr 22 11:01:29
End time: Apr 22 11:21:34
Login attempts: 646
Successful attempts: 1
Ratio: 0.0015479876161
Compromised account details:
Apr 22 11:02:15 : root

Attacker IP: 210.68.70.170
Start time: Apr 25 01:25:35
End time: Apr 25 01:35:34
Login attempts: 171

Attacker IP: 114.80.166.219
Start time: Apr 21 10:01:44
End time: Apr 21 10:07:51
Login attempts: 97

Attacker IP: 24.94.90.96
Start time: Apr 23 15:11:46
End time: Apr 23 15:11:58
Login attempts: 3

Attacker IP: 83.216.63.124
Start time: Apr 23 11:37:27
End time: Apr 23 11:37:37
Login attempts: 2
```

```
Attacker IP: 122.102.64.54
Start time: Apr 19 16:55:55
End time: Apr 22 00:23:11
Login attempts: 34

Attacker IP: 209.59.222.166
Start time: Apr 20 13:01:49
End time: Apr 20 13:07:48
Login attempts: 121

Attacker IP: 201.64.234.2
Start time: Apr 23 03:43:39
End time: Apr 23 04:13:32
Login attempts: 97

Attacker IP: 219.150.161.20
Start time: Apr 19 05:38:01
End time: Apr 19 08:58:54
Login attempts: 9259
Successful attempts: 4
Ratio: 0.000432012096339
Compromised account details:
Apr 19 05:41:44 : root
Apr 19 05:42:27 : root
Apr 19 05:55:20 : root
Apr 19 05:56:05 : root

Attacker IP: 24.192.113.91
Start time: Apr 19 13:05:47
End time: Apr 19 13:14:04
Login attempts: 168

Attacker IP: 12.172.224.140
Start time: Apr 20 12:43:03
End time: Apr 20 12:43:03
Login attempts: 1
```