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): Nikunj Shah	Email (required): nshah@prismmicrosys.com
Country (optional): United States of America	Profession (optional): Senior Support Engineer

1. Was the system compromised and when? How do you know that for sure?	Possible Points: 5
Tools Used: EventTracker 7.0 Awarded Points:	

Answer:

Yes the system was compromised. Examination of the /var/log/auth.log revealed password guessing attempts against the openssh daemon. Since the victim machine was attempting to scan other networks for SSH servers, it was reasonable to suppose it had been compromised by a guessed password, and in turn was probing for weak passwords.

Below logs will prove that attacker was tring to guess the password:

Apr 19 05:55:05 app-1 sshd[12933]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=219.150.161.20
Apr 19 05:55:06 app-1 sshd[12918]: Failed password for root from 219.150.161.20 port 42285 ssh2
Apr 19 05:55:06 app-1 sshd[12920]: Failed password for invalid user ftp123 from 219.150.161.20 port 42574 ssh2
Apr 19 05:55:06 app-1 sshd[12921]: Failed password for invalid user fred from 219.150.161.20 port 42600 ssh2
Apr 19 05:55:06 app-1 sshd[12924]: Failed password for invalid user coral from 219.150.161.20 port 42633 ssh2
Apr 19 05:55:06 app-1 sshd[12923]: Failed password for invalid user pauline from 219.150.161.20 port 42625 ssh2
Apr 19 05:55:06 app-1 sshd[12925]: Failed password for root from 219.150.161.20 port 42641 ssh2
Apr 19 05:55:06 app-1 sshd[12922]: Failed password for invalid user pauline from 219.150.161.20 port 42617 ssh2
Apr 19 05:55:07 app-1 sshd[12930]: Failed password for invalid user test from 219.150.161.20 port 42842 ssh2
Apr 19 05:55:07 app-1 sshd[12933]: Failed password for invalid user email from 219.150.161.20 port 42874 ssh2
Apr 19 05:55:08 app-1 sshd[12936]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=219.150.161.20 user=root
Apr 19 05:55:08 app-1 sshd[12938]: Invalid user ftp123 from 219.150.161.20

Above similar attacks were also tried from below ip addresses: (below are just some of the ip addresses)

- 219.150.161.20
- 222.66.204.246

- 121.11.66.70
- 222.169.224.197
- 122.226.202.12
- 121.11.66.70
- 61.168.227.12

Below log confirms that they are able to get into system with root 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
- Apr 23 03:11:03 app-1 sshd[13633]: Accepted password for root from 122.226.202.12 port 40892 ssh2
- Apr 23 03:20:41 app-1 sshd[13930]: Accepted password for root from 122.226.202.12 port 40209 ssh2
- Apr 24 11:36:19 app-1 sshd[24436]: Accepted password for root from 121.11.66.70 port 58832 ssh2
- Apr 20 06:13:03 app-1 sshd[26712]: Accepted password for root from 121.11.66.70 port 33828 ssh2
- Apr 22 11:02:15 app-1 sshd[7940]: Accepted password for root from 222.169.224.197 port 45356 ssh2
- Apr 19 10:45:36 app-1 sshd[28030]: Accepted password for root from 222.66.204.246 port 48208 ssh2
- Apr 24 15:28:37 app-1 sshd[31338]: Accepted password for root from 61.168.227.12 port 43770 ssh2

So to conclude,
Yes the system was compromised it was compromised at below date and time:

	Time of success	account	source ip address
-	4/19/2010 5:41:44 AM	root	219.150.161.20
-	4/19/2010 5:42:27 AM	root	219.150.161.20
-	4/19/2010 5:55:20 AM	root	219.150.161.20
-	4/19/2010 5:56:05 AM	root	219.150.161.20
-	4/23/2010 3:11:03 AM	root	122.226.202.12
-	4/23/2010 3:20:41 AM	root	122.226.202.12
-	4/20/2010 6:13:03 AM	root	121.11.66.70
-	4/24/2010 11:36:19 AM	root	121.11.66.70
-	4/22/2010 11:02:15 AM	root	222.169.224.197
-	4/19/2010 10:45:36 AM	root	222.66.204.246
-	4/24/2010 3:28:37 PM	root	61.168.227.12

Tools Used: EventTracker 7:

EventTracker consumed the logs and I ran the report on particular failure password events. Which gives us when that occurred what was the user name and what was the source ip address. Please refer to below sample reports generated by EventTracker 7.0 Santized log - Invalid logins from Existing User^39^1283955231.xls, Sanatized log - report for invalid user logons^41^1283955647.xls and Sanatized log - Accepted password^37^1283954925.xls reports. It also gives you count for total event for specific user name and specific ip address for summary.

Below is the sample from Santized log - Invalid logins from Existing User^39^1283955231.xls:

Santized log - Invalid logins from Existing User

Summary Report(s) :

Existing User	Total Event Occured
root	5479
mysql	44
games	35

backup	29
mail	27
nobody	25
lp	23
sshd	23

Ip Address	Total Event Occured
219.150.161.20	1685
121.11.66.70	1429
222.66.204.246	510
122.226.202.12	328
58.17.30.49	246
8.12.45.242	195
61.168.227.12	193
222.169.224.197	189
124.207.117.9	128
209.59.222.166	121
116.6.19.70	120
211.154.254.248	110
203.81.226.86	78
114.80.166.219	74
173.9.147.165	49

Detail Report :

Log Date Time	Existing User	Ip Address
4/15/2010 2:47:52 PM	user1	208.80.69.74
4/18/2010 6:22:09 PM	root	61.151.246.140
4/18/2010 6:22:13 PM	root	61.151.246.140
4/18/2010 6:22:17 PM	root	61.151.246.140
4/18/2010 6:22:20 PM	root	61.151.246.140
4/18/2010 6:22:24 PM	root	61.151.246.140
4/18/2010 6:22:28 PM	root	61.151.246.140
4/18/2010 6:22:32 PM	root	61.151.246.140
4/18/2010 6:22:36 PM	root	61.151.246.140
4/18/2010 6:22:39 PM	root	61.151.246.140
4/18/2010 6:22:43 PM	root	61.151.246.140
4/18/2010 6:22:47 PM	root	61.151.246.140
4/18/2010 6:22:51 PM	root	61.151.246.140
4/18/2010 6:22:55 PM	root	61.151.246.140
4/18/2010 9:51:56 PM	user3	10.0.1.4
4/18/2010 9:52:01 PM	user3	10.0.1.4
4/19/2010 4:32:58 AM	root	203.81.226.86
4/19/2010 4:33:03 AM	root	203.81.226.86
4/19/2010 4:33:08 AM	root	203.81.226.86

4/19/2010 4:33:13 AM	root	203.81.226.86
4/19/2010 4:33:18 AM	root	203.81.226.86
4/19/2010 4:33:23 AM	root	203.81.226.86
4/19/2010 4:33:28 AM	root	203.81.226.86
4/19/2010 4:33:33 AM	root	203.81.226.86
4/19/2010 4:33:38 AM	root	203.81.226.86
4/19/2010 4:33:44 AM	root	203.81.226.86
4/19/2010 4:33:50 AM	root	203.81.226.86
4/19/2010 4:33:55 AM	root	203.81.226.86
4/19/2010 4:34:00 AM	root	203.81.226.86
4/19/2010 4:34:04 AM	root	203.81.226.86
4/19/2010 4:34:09 AM	root	203.81.226.86
4/19/2010 4:34:14 AM	root	203.81.226.86
4/19/2010 4:34:20 AM	root	203.81.226.86

Below is the sample from Sanatized log - report for invalid user logons^41^1283955647.xls:

Sanatized log - report for invalid user logons

Summary Report(s) :

Invalid User	count	Event Id(Total Count)
admin	451	
test	282	
administrator	155	
123456	154	
12345	137	
123	133	
user	132	
qwerty	124	
oracle	124	
1234	117	
zxcvb	113	
users	105	
abc	95	
abcde	94	
tester	92	
abcd	90	
a	86	
Ip Address	**count**	
219.150.161.20	7574	
8.12.45.242	2842	
222.66.204.246	1063	
124.207.117.9	522	

222.169.224.197	457
217.15.55.133	382
211.154.254.248	345
65.208.122.48	300
122.226.202.12	185
124.51.108.68	154
210.68.70.170	135
24.192.113.91	135
173.9.147.165	96
125.235.4.130	85

Detail Report :

Log Date Time	Invalid User	Ip Address
4/19/2010 4:36:51 AM	tomcat	203.81.226.86
4/19/2010 5:19:10 AM	admin	58.17.30.49
4/19/2010 5:22:12 AM	tina	58.17.30.49
4/19/2010 5:22:16 AM	tom	58.17.30.49
4/19/2010 5:22:21 AM	tom	58.17.30.49
4/19/2010 5:22:26 AM	toor	58.17.30.49
4/19/2010 5:22:30 AM	tour	58.17.30.49
4/19/2010 5:22:34 AM	tour	58.17.30.49
4/19/2010 5:22:38 AM	tracy	58.17.30.49
4/19/2010 5:22:43 AM	tracy	58.17.30.49
4/19/2010 5:22:47 AM	user	58.17.30.49
4/19/2010 5:22:52 AM	www	58.17.30.49
4/19/2010 5:22:57 AM	www	58.17.30.49
4/19/2010 5:23:02 AM	admins	58.17.30.49
4/19/2010 5:38:01 AM	globus	219.150.161.20
4/19/2010 5:38:04 AM	Date Marine	219.150.161.20
4/19/2010 5:38:05 AM	condor	219.150.161.20
4/19/2010 5:38:08 AM	cadi	219.150.161.20
4/19/2010 5:38:08 AM	Date Marine	219.150.161.20
4/19/2010 5:38:09 AM	tomcat	219.150.161.20
4/19/2010 5:38:12 AM	cady	219.150.161.20
4/19/2010 5:38:12 AM	Date Marine	219.150.161.20
4/19/2010 5:38:13 AM	global	219.150.161.20
4/19/2010 5:38:15 AM	cai	219.150.161.20
4/19/2010 5:38:15 AM	Date Marine	219.150.161.20
4/19/2010 5:38:16 AM	upload	219.150.161.20
4/19/2010 5:38:19 AM	simoni	219.150.161.20

Below is the sample from Sanatized log - Accepted password^37^1283954925.xls reports:

Sanatized log - Accepted password

Summary Report(s) :

Authenticated User Name	Total Event Occured
user1	38
root	28
user3	24
dhg	22
user2	5
fido	1

Ip Address	Total Event Occured
190.166.87.164	23
76.191.195.140	22
10.0.1.2	14
208.80.69.74	7
65.88.2.5	6
71.132.129.212	5
188.131.23.37	4
219.150.161.20	4
10.0.1.4	4
192.168.126.1	3

Detail Report :

Log Date Time	Authenticated User Name	Ip Address
4/1/2010 11:20:58 AM	user1	67.164.72.181
4/1/2010 4:23:04 PM	user3	10.0.1.2
4/1/2010 9:12:32 PM	user1	76.191.195.140
4/2/2010 7:20:50 AM	user1	76.191.195.140
4/2/2010 12:42:31 PM	user1	76.191.195.140
4/14/2010 2:46:01 PM	user1	65.195.182.120
4/14/2010 2:51:05 PM	user3	65.195.182.120
4/15/2010 12:02:55 PM	user1	208.80.69.74
4/15/2010 2:43:56 PM	user1	208.80.69.74
4/15/2010 2:47:53 PM	user1	208.80.69.74
4/15/2010 7:48:38 PM	user1	76.191.195.140
4/15/2010 8:19:03 PM	user1	76.191.195.140
4/15/2010 8:29:16 PM	user1	76.191.195.140
4/16/2010 9:35:19 AM	user1	76.191.195.140
4/18/2010 6:07:35 PM	user3	10.0.1.2
4/18/2010 6:08:46 PM	user3	10.0.1.2
4/18/2010 6:29:30 PM	user3	10.0.1.4
4/18/2010 8:35:34 PM	user3	10.0.1.4
4/18/2010 9:52:03 PM	user3	10.0.1.4

4/18/2010 9:53:28 PM	user3	10.0.1.4
4/19/2010 5:41:44 AM	root	219.150.161.20
4/19/2010 5:42:27 AM	root	219.150.161.20
4/19/2010 5:55:20 AM	root	219.150.161.20
4/19/2010 5:56:05 AM	root	219.150.161.20
4/19/2010 9:59:27 AM	user1	76.191.195.140
4/19/2010 9:59:35 AM	user1	76.191.195.140
4/19/2010 10:45:36 AM	root	222.66.204.246
4/19/2010 10:46:50 AM	user1	208.80.69.74
4/19/2010 11:03:44 AM	root	201.229.176.217
4/19/2010 11:15:26 AM	root	190.167.70.87
4/19/2010 11:58:00 AM	user3	208.80.69.69
4/19/2010 2:28:32 PM	user3	208.80.69.69
4/19/2010 5:22:52 PM	user1	76.191.195.140

2. If the was compromised, what was the method used?	Possible Points: 5
Tools Used: EventTracker 7.0 Awarded Points:	
Answer The method was guessing attempts against the openssh daemon. Since the victim machine was attempting to scan other networks for SSH servers, it was reasonable to suppose it had been compromised by a guessed password, and in turn was probing for weak passwords.	

3. 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: EventTracker Awarded Points:	
Answer There were total 28 attackers out of these 22 attackers failed and 6 attackers were successful. 2 attackers from **121.11.66.70 and 222.66.204.246** attacked again after success rest of the 4 attacker stopped attacking after success. Tools User: EventTracker 7.0 again custom column analysis and Event Correlator provided help to find out the related between attacks and find out the attacked who attacked again. Please refer to sample report in Answer 1 generated by EventTracker 7.0 for Santized log - Invalid logins from Existing User^39^1283955231.xls, Sanatized log - report for invalid user logons^41^1283955647.xls and Sanatized log - Accepted password^37^1283954925.xls reports.	

4. What happened after the brute force attack?	Possible Points: 5
Tools Used:EventTracker 7.0 Awarded Points:	
Answer: I could not trace any logs after the attacker was able to succeed to get root password. One thing could be done is if the attacker had not really attempted to cover his or her tracks at all, this can make the analysis surprisingly quick and easy. For example, the *.bash_history* would be still intact and would have a complete list of commands that had been executed since the attacker logged on.	

5. Locate the authentication logs, was a brute force attack performed? If yes how many?	Possible Points: 5
Tools Used: Awarded Points:	

Answer
 	
Yes the brute force attack was performed. There were total 32 attacks performed. Out of these 22 attackers failed and 6 attackers were successful and 4 attackers attacked again.
 	
Below are the authentication logs start log and end log for the 32 attacks:
 	
- First attack from ip 61.151.246.140
  ○ (Start): Apr 18 18:22:09 app-1 sshd[5266]: Failed password for root from 61.151.246.140 port 52434 ssh2
  ○ (End): Apr 18 18:22:55 app-1 sshd[5290]: Failed password for root from 61.151.246.140 port 41764 ssh2
- Second attack from ip 203.81.226.86
  ○ (Start): Apr 19 04:32:58 app-1 sshd[6887]: Failed password for root from 203.81.226.86 port 48638 ssh2
  ○ (End): Apr 19 04:39:22 app-1 sshd[7055]: Failed password for root from 203.81.226.86 port 52246 ssh2
- Third attack from ip 58.17.30.49 and 219.150.161.20
  ○ (Start): Apr 19 05:18:38 app-1 sshd[7155]: Failed password for root from 58.17.30.49 port 39778 ssh2
  ○ (End): Apr 19 08:58:54 app-1 sshd[26986]: Failed password for invalid user emilie from 219.150.161.20 port 54595 ssh2
- Fourth attack from ip 200.72.254.54
  ○ (Start): Apr 19 10:01:08 app-1 sshd[27193]: Failed password for root from 200.72.254.54 port 58729 ssh2
  ○ (End): Apr 19 10:01:51 app-1 sshd[27217]: Failed password for root from 200.72.254.54 port 43467 ssh2
- Fifth attack from ip 222.66.204.246
  ○ (Start): Apr 19 10:41:41 app-1 sshd[27328]: Failed password for invalid user admin from 222.66.204.246	

port 50963 ssh2
    - (End): Apr 19 10:56:59 app-1 sshd[30242]: Failed password for root from 222.66.204.246 port 57237 ssh2
- Sixth attack **again** from ip 200.72.254.54
    - (Start): Apr 19 11:15:46 app-1 sshd[30378]: Failed password for root from 200.72.254.54 port 58764 ssh2
    - (End): Apr 19 11:16:19 app-1 sshd[30407]: Failed password for root from 200.72.254.54 port 40222 ssh2
- Seventh attack from **again** from ip 222.66.204.246
    - (Start): Apr 19 11:22:42 app-1 sshd[30435]: Failed password for invalid user admin from 222.66.204.246 port 55776 ssh2
    - (End): Apr 19 11:24:39 app-1 sshd[30758]: Failed password for invalid user uwe from 222.66.204.246 port 60995 ssh2
- Eighth attack from ip 24.192.113.91
    - (Start): Apr 19 13:05:47 app-1 sshd[31425]: Failed password for invalid user staff from 24.192.113.91 port 49583 ssh2
    - (End): Apr 19 13:14:04 app-1 sshd[31804]: Failed password for invalid user gopher from 24.192.113.91 port 45524 ssh2
- Ninth attack from ip 122.102.64.54
    - (Start): Apr 19 16:55:55 app-1 sshd[777]: Failed password for root from 122.102.64.54 port 51791 ssh2
    - (End): Apr 19 16:56:53 app-1 sshd[819]: Failed password for root from 122.102.64.54 port 56501 ssh2
- Tenth attack from ip 125.235.4.130
    - (Start): Apr 20 02:48:10 app-1 sshd[25155]: Failed password for root from 125.235.4.130 port 55681 ssh2
    - (End): Apr 20 02:57:45 app-1 sshd[25399]: Failed password for invalid user shop from 125.235.4.130 port 58837 ssh2
- Eleventh attack from ip 121.11.66.70
    - (Start): Apr 20 05:48:07 app-1 sshd[25819]: Failed password for root from 121.11.66.70 port 40766 ssh2
    - (End): Apr 20 06:44:33 app-1 sshd[29538]: Failed password for root from 121.11.66.70 port 56159 ssh2
- Twelfth attack from ip 78.38.27.21, 59.46.39.148
    - (Start): Apr 20 10:20:52 app-1 sshd[30434]: Failed password for root from 78.38.27.21 port 46115 ssh2
    - (End): Apr 20 10:27:33 app-1 sshd[30565]: Failed password for invalid user user from 59.46.39.148 port 59219 ssh2
- Thirteenth attack from ip 209.59.222.166
    - (Start): Apr 20 13:01:49 app-1 sshd[30989]: Failed password for root from 209.59.222.166 port 57061 ssh2
    - (End): Apr 20 13:07:48 app-1 sshd[31240]: Failed password for root from 209.59.222.166 port 59818 ssh2
- Fourteenth attack from ip 220.170.79.247
    - (Start): Apr 20 14:15:41 app-1 sshd[31405]: Failed password for root from 220.170.79.247 port 37610 ssh2
    - (End): Apr 20 14:16:36 app-1 sshd[31444]: Failed password for invalid user test from 220.170.79.247 port 41972 ssh2
- Fifteenth attack from ip 114.80.166.219
    - (Start): Apr 21 10:01:44 app-1 sshd[2174]: Failed password for root from 114.80.166.219 port 45970 ssh2
    - (End): Apr 21 10:07:51 app-1 sshd[2380]: Failed password for root from 114.80.166.219 port 58410 ssh2
- Sixteenth attack **again** from ip 122.102.64.54
    - (Start): Apr 22 00:22:14 app-1 sshd[4663]: Failed password for root from 122.102.64.54 port 37432 ssh2
    - (End): Apr 22 00:23:11 app-1 sshd[4695]: Failed password for root from 122.102.64.54 port 41345 ssh2
- Seventeenth attack from ip 222.169.224.197
    - (Start): Apr 22 11:01:38 app-1 sshd[7906]: Failed password for invalid user test from 222.169.224.197 port 26402 ssh2
    - (End): Apr 22 11:21:34 app-1 sshd[9369]: Failed password for invalid user kenvelo from 222.169.224.197 port 8129 ssh2
- Eighteenth attack from ip 217.15.55.133
    - (Start): Apr 22 14:15:25 app-1 sshd[10707]: Failed password for invalid user wwwweb from 217.15.55.133 port 44571 ssh2
    - (End): Apr 22 14:48:33 app-1 sshd[11646]: Failed password for invalid user bs from 217.15.55.133 port 34136 ssh2
- Nineteenth attack from ip 122.226.202.12, 201.64.234.2
    - (Start): Apr 23 03:06:17 app-1 sshd[13476]: Failed password for root from 122.226.202.12 port 51948 ssh2
    - (End): Apr 23 04:13:32 app-1 sshd[14867]: Failed password for root from 201.64.234.2 port 62643 ssh2

- Twentieth attack from ip 218.56.61.114
  - (Start): Apr 23 12:44:50 app-1 sshd[17154]: Failed password for invalid user test from 218.56.61.114 port 60332 ssh2
  - (End): Apr 23 12:45:21 app-1 sshd[17170]: Failed password for invalid user test from 218.56.61.114 port 32880 ssh2
- Twenty first attack from ip 124.207.117.9
  - (Start): Apr 23 17:20:53 app-1 sshd[17856]: Failed password for root from 124.207.117.9 port 43773 ssh2
  - (End): Apr 23 18:06:32 app-1 sshd[19265]: Failed password for invalid user will from 124.207.117.9 port 52594 ssh2
- Twenty second attack from ip 173.9.147.165
  - (Start): Apr 23 20:06:09 app-1 sshd[19569]: Failed password for invalid user globus from 173.9.147.165 port 52144 ssh2
  - (End): Apr 23 20:10:03 app-1 sshd[19886]: Failed password for invalid user escape from 173.9.147.165 port 59177 ssh2
- Twenty third attack from ip 211.154.254.248
  - (Start): Apr 24 03:19:02 app-1 sshd[20965]: Failed password for invalid user sales from 211.154.254.248 port 37871 ssh2
  - (End): Apr 24 03:51:21 app-1 sshd[21952]: Failed password for invalid user barone from 211.154.254.248 port 56633 ssh2
- Twenty fourth attack from ip 124.51.108.68
  - (Start): Apr 24 10:26:54 app-1 sshd[23126]: Failed password for root from 124.51.108.68 port 46942 ssh2
  - (End): Apr 24 10:37:34 app-1 sshd[23461]: Failed password for invalid user omega from 124.51.108.68 port 48142 ssh2
- Twenty fifth attack **again** from ip 121.11.66.70
  - (Start): Apr 24 11:10:35 app-1 sshd[23539]: Failed password for root from 121.11.66.70 port 38445 ssh2
  - (End): Apr 24 11:41:59 app-1 sshd[24629]: Failed password for root from 121.11.66.70 port 29129 ssh2
- Twenty sixth attack from ip 8.12.45.242
  - (Start): Apr 24 12:55:04 app-1 sshd[24803]: Failed password for root from 8.12.45.242 port 39118 ssh2
  - (End): Apr 24 14:49:42 app-1 sshd[31157]: Failed password for invalid user virtuoso from 8.12.45.242 port 38773 ssh2
- Twenty seventh attack from ip 61.168.227.12
  - (Start): Apr 24 15:26:00 app-1 sshd[31248]: Failed password for root from 61.168.227.12 port 55810 ssh2
  - (End): Apr 24 15:40:00 app-1 sshd[31715]: Failed password for root from 61.168.227.12 port 58972 ssh2
- Twenty eighth attack from ip 116.6.19.70
  - (Start): Apr 25 00:54:38 app-1 sshd[6484]: Failed password for root from 116.6.19.70 port 50886 ssh2
  - (End): Apr 25 01:12:02 app-1 sshd[6899]: Failed password for root from 116.6.19.70 port 35325 ssh2
- Twenty ninth attack from ip 210.68.70.170
  - (Start): Apr 25 01:25:35 app-1 sshd[6941]: Failed password for invalid user vmlinuz from 210.68.70.170 port 44122 ssh2
  - (End): Apr 25 01:35:34 app-1 sshd[7301]: Failed password for invalid user nagios from 210.68.70.170 port 34513 ssh2
- Thirtieth attack from ip 219.139.243.236
  - (Start): Apr 26 06:10:17 app-1 sshd[21176]: Failed password for root from 219.139.243.236 port 55823 ssh2
  - (End): Apr 26 06:12:33 app-1 sshd[21251]: Failed password for root from 219.139.243.236 port 58887 ssh2
- Thirty first attack from ip 122.165.9.200
  - (Start): Apr 26 07:18:09 app-1 sshd[22034]: Failed password for root from 122.165.9.200 port 41772 ssh2
  - (End): Apr 26 07:18:46 app-1 sshd[22046]: Failed password for invalid user oracle from 122.165.9.200 port 42938 ssh2
- Thirty second attack from ip 65.208.122.48
  - (Start): Apr 26 08:23:47 app-1 sshd[22662]: Failed password for invalid user skin from 65.208.122.48 port 59063 ssh2
  - (End): Apr 26 08:40:36 app-1 sshd[23433]: Failed password for invalid user esteban from 65.208.122.48 port 44707 ssh2

Below are the are the authentication logs for successful attack:

- 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
- Apr 23 03:11:03 app-1 sshd[13633]: Accepted password for root from 122.226.202.12 port 40892 ssh2
- Apr 23 03:20:41 app-1 sshd[13930]: Accepted password for root from 122.226.202.12 port 40209 ssh2
- Apr 24 11:36:19 app-1 sshd[24436]: Accepted password for root from 121.11.66.70 port 58832 ssh2
- Apr 20 06:13:03 app-1 sshd[26712]: Accepted password for root from 121.11.66.70 port 33828 ssh2
- Apr 22 11:02:15 app-1 sshd[7940]: Accepted password for root from 222.169.224.197 port 45356 ssh2
- Apr 19 10:45:36 app-1 sshd[28030]: Accepted password for root from 222.66.204.246 port 48208 ssh2
- Apr 24 15:28:37 app-1 sshd[31338]: Accepted password for root from 61.168.227.12 port 43770 ssh2

Tools Used EventTracker 7.0: Using Direct log Archiver EventTracker can consume auth.log file and then I ran a detailed report for all the attack audit events. It gave me complete details about who, what, when and from where was attack performed.

6. What is the timeline of significant events? How certain are you of the timing?	Possible Points: 5

Tools Used: EventTracker 7
Awarded Points:

Answer

Below is the start time and stop time of brute force attack event. I am 100% sure of the timing.

- First attacker from ip *61.151.246.140* started at 4/18/2010 6:22:09 PM and stopped at 4/18/2010 6:22:55 PM
- Second attacker from ip *203.81.226.86* started at 4/19/2010 4:32:58 AM and stopped at 4/19/2010 4:39:22 AM
- Third attacker from ip *58.17.30.49* and *219.150.161.20* started at 4/19/2010 5:18:38 AM and stopped at 4/19/2010 8:58:54 AM
- Fourth attacker from ip *200.72.254.54* started at 4/19/2010 10:01:08 AM and stopped at 4/19/2010 10:01:51 AM
- Fifth attacker from ip *222.66.204.246* started at 4/19/2010 10:41:41 AM and stopped at 4/19/2010 10:56:59 AM
- Fourth attacker **again** tried from ip *200.72.254.54* started at 4/19/2010 11:15:46 AM and stopped at 4/19/2010 11:16:19 AM
- Fifth attacker **again** tried from *ip 222.66.204.246* started at 4/19/2010 11:22:42 AM and stopped at 4/19/2010 11:24:39 AM
- Sixth attacker tried from ip *24.192.113.91* started at 4/19/2010 1:05:47 PM and stopped at 4/19/2010 1:14:04 PM
- Seventh attacker tried from ip *122.102.64.54* started at 4/19/2010 4:55:55 PM and stopped at 4/19/2010 4:56:53 PM
- Eighth attacker tried from ip *125.235.4.130* started at 4/20/2010 2:48:10 AM and stopped at 4/20/2010 2:57:45 AM
- Ninth attacker tried from ip *121.11.66.70* started at 4/20/2010 5:48:07 AM and stopped at 4/20/2010 6:44:33 AM
- Tenth attacker tried from *ip 78.38.27.21, 59.46.39.148* started at 4/20/2010 10:20:52 AM and stopped at 4/20/2010 10:27:33 AM
- Eleventh attacker tried from *ip209.59.222.166* started at 4/20/2010 1:01:49 PM and stopped at 4/20/2010 1:07:48 PM
- Twelfth attacker tried from ip 220.170.79.247 started at 4/20/2010 2:15:41 PM and stopped at 4/20/2010 2:16:36 PM
- Thirteenth attacker tried from ip *114.80.166.219* started at 4/21/2010 10:01:44 AM and stopped at 4/21/2010 10:07:51 AM
- Seventh attacker **again** tried from ip *122.102.64.54* started at 4/22/2010 12:22:14 AM and stopped at 4/22/2010 12:23:11 AM
- Fourteenth attacker tried from ip *222.169.224.197* started at 4/22/2010 11:01:38 AM and stopped at 4/22/2010

11:21:34 AM
- Fifteenth attacker tried from ip *217.15.55.133* started at 4/22/2010 2:15:25 PM and stopped at 4/22/2010 2:48:33 PM
- Sixteenth attacker tried from ip *122.226.202.12, 201.64.234.2* started at 4/23/2010 3:06:17 AM and stopped at 4/23/2010 4:13:32 AM
- Seventeenth attacker tried from ip 218.56.61.114 started at 4/23/2010 12:44:50 PM and stopped at 4/23/2010 12:45:21 PM
- Eighteenth attacker tried from ip *124.207.117.9* started at 4/23/2010 5:20:53 PM and stopped at 4/23/2010 6:06:32 PM
- Nineteenth attacker tried from ip *173.9.147.165* started at 4/23/2010 8:06:09 PM and stopped at 4/23/2010 8:10:03 PM
- Twentieth attacker tried from ip *211.154.254.248* started at 4/24/2010 3:19:02 AM and stopped at 4/24/2010 3:51:21 AM
- Twenty first attacker tried from ip 124.51.108.68 started at 4/24/2010 10:26:54 AM and stopped at 4/24/2010 10:37:34 AM
- Ninth attacker **again** tried from ip *121.11.66.70* started at 4/24/2010 11:10:35 AM and stopped at 4/24/2010 11:41:59 AM
- Twenty second attacker tried from ip 8.12.45.242 started at 4/24/2010 12:55:04 PM and stopped at 4/24/2010 2:49:42 PM
- Twenty third attacker tried from ip 61.168.227.12 started at 4/24/2010 3:26:00 PM and stopped at 4/24/2010 3:40:00 PM
- Twenty fourth attacker tried from ip 116.6.19.70 started at 4/25/2010 12:54:38 AM and stopped at 4/25/2010 1:12:02 AM
- Twenty fifth attacker tried from ip 210.68.70.170 started at 4/25/2010 1:25:35 AM and stopped at 4/25/2010 1:35:34 AM
- Twenty sixth attacker tried from ip 219.139.243.236 started at 4/26/2010 6:10:17 AM and stopped at 4/26/2010 6:12:33 AM
- Twenty seventh attacker tried from ip 122.165.9.200 started at 4/26/2010 7:18:09 AM and stopped at 4/26/2010 7:18:46 AM
- Twenty eighth attacker tried from ip 65.208.122.48 started at 4/26/2010 8:23:47 AM and stopped at 4/26/2010 8:40:36 AM

Below is the time when attacker was successful to get into the root account. I am 100% sure of timing.

Time of success	account	source ip address
4/19/2010 5:41:44 AM	root	219.150.161.20
4/19/2010 5:42:27 AM	root	219.150.161.20
4/19/2010 5:55:20 AM	root	219.150.161.20
4/19/2010 5:56:05 AM	root	219.150.161.20
4/23/2010 3:11:03 AM	root	122.226.202.12
4/23/2010 3:20:41 AM	root	122.226.202.12
4/20/2010 6:13:03 AM	root	121.11.66.70
4/24/2010 11:36:19 AM	root	121.11.66.70
4/22/2010 11:02:15 AM	root	222.169.224.197
4/19/2010 10:45:36 AM	root	222.66.204.246
4/24/2010 3:28:37 PM	root	61.168.227.12

7. Anything else that looks suspicious in the logs? Any misconfigurations? Other issues?	Possible Points: 5
Tools Used: EventTracker 7.0 Awarded Points:	
Answer: Below are the some of the issues: - Root access is not disabled	

- If you see 123.4.59.174 - - [19/Apr/2010:08:26:30 -0700] "GET http://proxyjudge1.proxyfire.net/fastenv HTTP/1.1" 404 1466 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" ldqydQoAAQ4AAEP5EvsAAAAF 2358754 log, the ip address 123.4.59.174 has to be block because they are trying to access some web data but they are getting 404 error code.
- There is nothing to worry about "+ ??? root:nobody" because those are by cron jobs.
- Observing this log Apr 20 12:26:08 app-1 sshd[30892]: reverse mapping checking getaddrinfo for 164.87.166.190.f.sta.codetel.net.do [190.166.87.164] failed - POSSIBLE BREAK-IN ATTEMPT!, I looks like 164.87.166.190.f.sta.codetel.net.do [190.166.87.164] is a valid system, to fix this add this entry into host files. Similary there are similar errors, add all those which are valid in host file so the log analysis becomes easy and we can find out potentially treat system easily.

8. Was an automatic tool used to perform the attack? If yes which one?	Possible Points: 5
Tools Used: EventTracker 7.0 Awarded Points:	
Answer Certainly seeing the pattern of brute force attack it is sure that either a tool or script was used for this attack. However during the attack there were some instances of success but looks like the tool was just guessing the password. Tool didn't do anything to system file or kernel drivers. So one could say that it could be either script or a tool with capability of just trying out different password on different user name.	

9. What can you say about the attacker's goals and methods?	Possible Points: 5
Tools Used:EventTracker 7.0 Awarded Points:	
Answer Attacker used an automated tool or script to start a brute force attack. The attacker used password guessing attempts against the openssh daemon. Since the victim machine was attempting to scan other networks for SSH servers, it was reasonable to suppose it had been compromised by a guessed password, and in turn was probing for weak passwords. The goal of the attack was simply to get into the system.	

Bonus. What would you have done to avoid this attack?	Possible Points: 5
Tools Used: EventTracker 7.0 Awarded Points:	
Answer 1. Hide systems running services such as SSH behind a firewall Connecting control systems components to the Internet is a significant risk. If a control system component does require Internet connectivity, such devices should be carefully deployed, and appropriate security measures should be implemented. Firewalls provide the capability to hide internal systems and define rules for communication with devices and between different network segments. Of critical importance to control systems is how the firewall is implemented. Many types of firewalls are available, and some research is required to ascertain what type of firewall is right for a given control architecture. Also, consider the use of virtual private networks (VPNs) to access services from outside the control system network, rather than opening up access through a firewall.	

2. Use strong passwords or public-key authentication

   Make password lengths long and combine letters, numbers, and special characters. For additional guidance, see Microsoft's "Strong passwords: How to create and use them."3 If the SSH server supports public-key authentication, consider using this as an option to static passwords.

3. Configure SSH servers to use a non-standard port

   SSH normally listens on TCP Port 22, but can be configured to listen on any other unused port. The TCP protocol provides 65,535 ports from which to select. The popular port scanning tool Nmap4 only scans a little over 1,600 ports by default, so by selecting a nonstandard high port number, SSH may not be detected by scans looking specifically for it.

4. Restrict access to SSH servers

   Only allow access from specific hosts rather than allowing access from anywhere.

5. Utilize Intrusion Detection/Intrusion Prevention (By EventTracker 7.0)

   EventTracker 7.0 provides Itrusion Detection correlation rules which can alert you on multiple authentication failures. Set up an email alert for Intursion detection and as a prevention EventTracker also provides an option to shutdown the server, so as soon as an intrusion is detected shut down the server or we can run any scripts which could prevent server from getting attacked.

6. Disable Root Access

7. Using 'iptables' to block the attack
   a. It is possible to set up iptables rules to block ssh attacks. The following ruleset will allow at most 3 connections per minute from any host, and will block the host for another minute if this rate is exceeded.
      i. iptables -A INPUT -p tcp --dport 22 -m state --state NEW -m recent --set \ --name SSH -j ACCEPT
      ii. iptables -A INPUT -p tcp --dport 22 -m recent --update --seconds 60 --hitcount 4 --rttl \ --name SSH -j LOG --log-prefix "SSH_brute_force. "
      iii. iptables -A INPUT -p tcp --dport 22 -m recent --update --seconds 60 \ --hitcount 4 --rttl --name SSH -j DROP

8. Using tcp_wrappers to block attacks
   a. It is possible to let the tcp wrapper library start a script whenever a connection is made, and let this script add rules to /etc/hosts.deny or /etc/hosts.allow, if the connecting host should be blocked.

9. Use EventTracker 7.0 Reports:
   a. In EventTracker 7.0 one can configure automatic schedule daily or hour reports like Sanatized log - Invalid logins from Existing User^39^1283955231.xls, Sanatized log - report for invalid user logons^41^1283955647.xls and Sanatized log - Accepted password^37^1283954925.xls reports (Please refer to sample reports in section 1) which could easily tell if the system is attacked and if yes is the system is compromised or not. Then one can perform proactive steps using these reports. This reports gives you complete meaningful information on who perform attacked, when was it and from where was the attack. After the analysis one can take all the required steps proactively.