

LOG

by Log Log

Submission date: 09-Nov-2018 02:37 PM (UTC+1300)

Submission ID: 1035668489

File name: logcaptureandeventcorrelation.docx (53.55K)

Word count: 1153

Character count: 6489

Name

Institution

Date

Log Capture and Event Correlation

Introduction

We are in an era where data security is of utmost importance in every industry. We have witnessed various network intrusions over the past decade where hackers penetrate networks either view sensitive information or encrypt information. A practical case where cyber-attack has been witnessed is the attack on the United Kingdom medical industry attack in mid-2017 where WannaCry virus was used to negatively affect the hospital systems (Dan, 2017). Log analysis is one of the countermeasures against malicious hacking practices today. Forensic investigators are some of the experienced personnel mandated to investigate these hacking cases.

Analysis

The log analysis was conducted using logwatch as the tool. Every detail relevant to the case has been discussed in detail in every paragraph. There were several cases of break-in attempts where different IP addresses were used by the attackers. All the successful break-in attempts have been indicated below (IP address and time of attack);

1. 61.168.227.12 made an attack on April 24th at 15:28:37
2. 122.226.202.12 made an attack on April 23rd at 03:11:03
3. 121.11.66.70 made an attack on April 20th at 06:13:03
4. 219.150.161.20 made an attack on April 19th at 05:41:44
5. 222.66.204.246 made an attack on April 19th at 10:45:36
6. 222.129.224.197 made an attack on April 22nd at 11:02:15

In any log analysis, certain criterion must be employed to determine the valid and false positive attacks. The network user may have forgotten his/her login credentials. A combination of hashes

in Perl to store IP data and some criteria were used to determine the attacks. In the forensic investigation, the following criteria were used to verify the successful attacks;

1. A number of logins had to be determined to identify which IP addresses had exceeded the set number. If the number is greater, the IP address is classified as an attacker's IP address.
2. If in any case invalid username was used, the attempt is considered as a break-in attempt.

The attackers used the brute-force attack method to gain entry. We can see various login attempts with varying credentials. A brute-force attack uses various login credentials in attempt to match the verified information in the system database. In our scenario, the brute-force attack was carried against the root user account. The root user seems to be the perfect account for any attack due to the privileged access it has in the system including database manipulation and total system control.

As previously indicated, we had six successful attacks on the system. In addition, 27 failed attacks were registered in the auth.log file. Therefore, the total number of system attacks was 33 in the same month on April. Following the criteria that was employed in the forensic analysis, the IP addresses of the failed break-in attempts and successful break-in attempts have been indicated in the table below;

Successful Break-In Attempts (6)	Failed Break-In Attempts (27)
---	--------------------------------------

121.11.66.70, 122.226.202.12, 61.168.227.12, 219.150.161.20, 222.66.204.246, 222.169.224.197.	61.151.246.140, 190.4.21.190, 218.56.61.114, 89.46.213.128, 122.165.9.200, 24.94.90.96, 8.12.45.242, 124.207.117.9, 211.154.254.248, 217.15.55.133, 65.208.122.48, 58.17.30.49, 116.6.19.70, 210.68.70.170, 24.192.113.91, 124.51.108.68, 173.9.147.165, 209.59.222.166, 125.235.4.130, 201.64.234.2, 114.80.166.219, 203.81.226.86, 59.46.39.148, 122.102.64.54, 219.139.243.236, 200.72.254.54, 220.170.79.247.
---	--

There were varying break-attempts times by the attackers. Below shows the number of break-in attempt times of individual attackers (IP addresses).

1. 122.226.202.12: 2 break-in attempts on 23rd April at 03:11:03 and 03:20:41
2. 61.168.227.12: 1 break-in attempt on 24th April at 15:28:37
3. 219.150.161.20: 4 break-in attempts on 19th April at 05:41:44, 05: 42:27, 05:55:20 and 05:56:05
4. 222.66.204.246: 1 break-in attempt on 19th April at 10:45:36
5. 222.169.224.197: 1 break-in attempt on 22nd April at 11:02:15
6. 121.11.66.70: 2 break-in attempts on April 20th at 06:13:03 and April 24th at 11:36:19

Two distinct actions happened after the brute-force attack on the system. Exim mail server was installed in the system and other existing programs replaced with others. The Exim server was also configured in the process. All these actions can be traced by viewing the term.log file found in the apt folder. A sample screenshot of these actions is displayed below;

```
Unpacking replacement exim4-daemon-light ...
Preparing to replace exim4 4.69-2 (using .../exim4_4.69-2ubuntu0.1_all.deb)
...
Unpacking replacement exim4 ...
Preparing to replace fuse-utils 2.7.2-1ubuntu2 (using .../fuse-utils_2.7.2-1ubuntu2.1_amd64.deb) ...
Unpacking replacement fuse-utils ...
Preparing to replace libfuse2 2.7.2-1ubuntu2 (using .../libfuse2_2.7.2-1ubuntu2.1_amd64.deb) ...
Unpacking replacement libfuse2 ...
Preparing to replace libpq5 8.3.9-0ubuntu8.04 (using .../libpq5_8.3.10-0ubuntu8.04_amd64.deb) ...
Unpacking replacement libpq5 ...
Preparing to replace sudo 1.6.9p10-1ubuntu3.5 (using .../sudo_1.6.9p10-1ubuntu3.7_amd64.deb) ...
Unpacking replacement sudo ...
Setting up libkrb53 (1.6.dfsg.3~beta1-2ubuntu1.4) ...

Setting up exim4-config (4.69-2ubuntu0.1) ...

Setting up exim4-base (4.69-2ubuntu0.1) ...
Installing new version of config file /etc/init.d/exim4 ...

Setting up exim4-daemon-light (4.69-2ubuntu0.1) ...
* Starting MTA      +[125G +[119G[ OK ]

Setting up exim4 (4.69-2ubuntu0.1) ...
```

The authentication logs are in the auth.log file. On completing the analysis of the file, brute-force attacks were evident. There were 27 failed attacks and 11 successful. The 11 successful attempts were carried out by 6 IP addresses as indicated below;

1. 122.226.202.12: 2 break-in attempts
2. 61.168.227.12: 1 break-in attempt
3. 219.150.161.20: 4 break-in attempts
4. 222.66.204.246: 1 break-in attempt
5. 222.169.224.197: 1 break-in attempt
6. 121.11.66.70: 2 break-in attempts

During the forensic analysis, the afterglow graph was employed. Afterglow graph is a useful reporting tool that indicates clear and accurate data including timelines. The individual timelines of the attacks have been indicated below;

1. 122.226.202.12: 2 break-in attempts on 23rd April at 03:11:03 and 03:20:41
2. 61.168.227.12: 1 break-in attempt on 24th April at 15:28:37
3. 219.150.161.20: 4 break-in attempts on 19th April at 05:41:44, 05: 42:27, 05:55:20 and 05:56:05
4. 222.66.204.246: 1 break-in attempt on 19th April at 10:45:36
5. 222.169.224.197: 1 break-in attempt on 22nd April at 11:02:15
6. 121.11.66.70: 2 break-in attempts on April 20th at 06:13:03 and April 24th at 11:36:19

There were no other suspicious activities identified except the ones discussed above. The fact that the attacks were carried in an efficient manner tells us that an automatic tool was used. In the networking world, we have various kinds of these tools including proxy scanners or simply Kali Linux pen-testing tools. The most probable tool used by the attackers was hydra. The method used by the attackers was brute-force attack where the main goal was to gain access to the root account and install malicious applications including the Exim server.

Installation of eggdrop program in the system proves that the attacker wanted the system to function as an IRC bouncer. The attackers left large traces of the attack logs thus were not careful in their attack. It was very easy to identify the attacks and point out who did it (IP addresses).

Conclusion

It is always important to enforce the standard network security guidelines in any network. If all the safety procedures were followed, the attack could have been prevented. Some of these prevention measures include using strong passwords, securing the SSH server and disabling port access to the root account. Every organization should follow these security guidelines so that the integrity of the system is not compromised.

References

² Mohit, . (2015). *Python penetration testing essentials: Employ the power of Python to get the best out of pentesting*. Birmingham, UK: Packt Publishing.

¹ Coleman, D. D., Westcott, D. A., Harkins, B., & Jackman, S. M. (2011). *CWSP Certified Wireless Security Professional Official Study Guide: Exam PW0-204*. New York, NY: John Wiley & Sons.

Clarke, G. E. (2012). *CompTIA network+: (exam N10-005)*. Berkeley, Calif: Osborne

Turvey, B. E., & Crowder, S. (2017). *Forensic investigations: An introduction*.

³ Korowajczuk, L. (2011). *LTE, WIMAX, and WLAN network design, optimization and performance analysis*. Chichester, West Sussex, U.K: Wiley.

Cryptography and network security. (2015).

LOG

ORIGINALITY REPORT

5%

SIMILARITY INDEX

3%

INTERNET SOURCES

0%

PUBLICATIONS

5%

STUDENT PAPERS

PRIMARY SOURCES

1

Submitted to Glasgow Caledonian University

Student Paper

2%

2

Submitted to University of Derby

Student Paper

1%

3

Submitted to Glyndwr University

Student Paper

1%

Exclude quotes Off

Exclude bibliography Off

Exclude matches Off