ITC8250 - Cyber Security Technologies I
Group Work 2

214322IV - Maëlie LEBARON
214366IV - Jordan Béziaud
214307IV - Vincent Rossignol
214319IV - Marine Hervet
214310IV - Victor Thévin

November 9, 2021

1 Why is rsyslogd not used by all server programs for logging? In particular, when should rsyslogd be avoided?

Logs are stored in **/var/log** which can cause the server to freeze if its partition becomes 100% full.

The way rsyslog uses permissions when generating the log files can allow local users to obtain information by reading /var/log/cron, and it can be sensitive information.

According to CVE details website, there is currently or there have been 18 known vulnerabilities which means that the tool should not be used in major or critical business infrastructures.

2 On bob, find out what the files /var/log/mail.log, /var/log/mysql/mysql.log and /var/log/dmesg are used for. Which programs use them? Configure MySQL so that its log information is stored in /var/log/mysql.log

- /var/log/mail.log:contains information from the mail server or email related services
- /var/log/mysql/mysql.log: contains information about actions performed on the server, requests and connections.
- /var/log/dmesg: contains messages from the **kernel ring buffer**, i.e. messages generated during the boot process and passed by the kernel

The oldest messages are deleted when the size is insufficient to store the new messages.

To configure MySQL so that **log information** is stored in /var/log/mysql.log, the MySQL configuration file must be modified: /etc/mysql/my.cnf by logging as root (this file is read-only otherwise).

The following lines must be added:

```
[mysqld]
general_log_file = /var/log/mysql/mysql.log
general_log = 1
```

The next step is to give ownership of the files in this directory to the mysql service:

```
chown mysql /var/log/mysql -Rf
```

3 How can you configure alice and bob so that all of bob's messages are logged by alice?

3.1 On Alice:

```
sudo nano /etc/rsyslog.conf
```

Then uncomment the two lines for TCP reception:

```
$ModLoad imtcp
$InputTCPServerRun 514
```

Restart the `rsyslog` service and allow reception of TCP traffic on port 514:

```
sudo service rsyslog restart
ufw allow 514/tcp
```

3.2 On Bob:

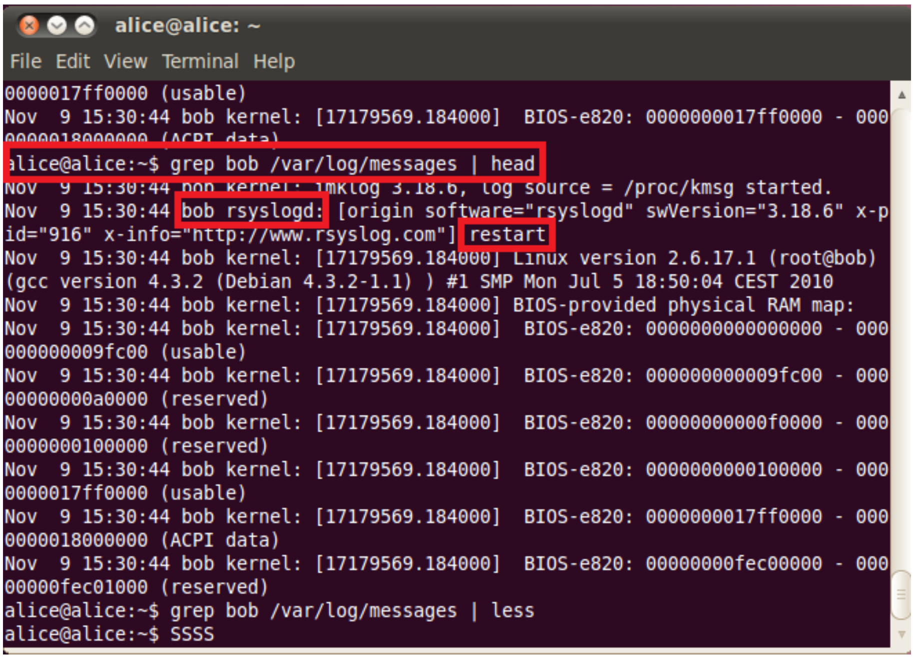
Creation of the file: `/etc/rsyslog.d/loghost.conf` and insertion of the following line:

```
touch /etc/rsyslog.d/loghost.conf
*.* @@alice:514
```

Find the remote logs on alice:

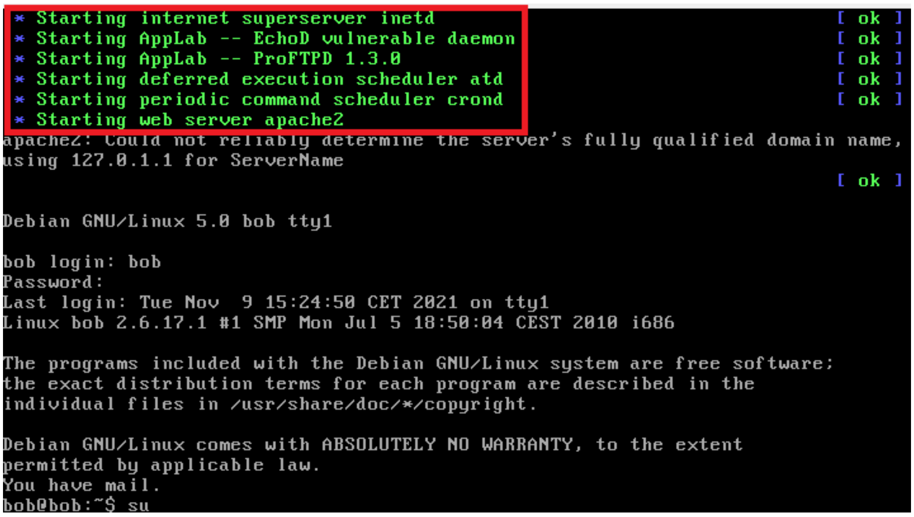
```
grep bob /var/log/messages
```

Which gives us as a result :



```
0000017ff0000 (usable)
Nov  9 15:30:44 bob kernel: [17179569.184000]  BIOS-e820: 0000000017ff0000 - 000
0000018000000 (ACPI data)
alice@alice:~$ grep bob /var/log/messages | head
Nov  9 15:30:44 bob kernel: imklog 3.18.6, log source = /proc/kmsg started.
Nov  9 15:30:44 bob rsyslogd: [origin software="rsyslogd" swVersion="3.18.6" x-p
id="916" x-info="http://www.rsyslog.com"] restart
Nov  9 15:30:44 bob kernel: [17179569.184000] Linux version 2.6.17.1 (root@bob)
(gcc version 4.3.2 (Debian 4.3.2-1.1) ) #1 SMP Mon Jul 5 18:50:04 CEST 2010
Nov  9 15:30:44 bob kernel: [17179569.184000] BIOS-provided physical RAM map:
Nov  9 15:30:44 bob kernel: [17179569.184000]  BIOS-e820: 0000000000000000 - 000
000000009fc00 (usable)
Nov  9 15:30:44 bob kernel: [17179569.184000]  BIOS-e820: 000000000009fc00 - 000
00000000a0000 (reserved)
Nov  9 15:30:44 bob kernel: [17179569.184000]  BIOS-e820: 00000000000f0000 - 000
0000000100000 (reserved)
Nov  9 15:30:44 bob kernel: [17179569.184000]  BIOS-e820: 0000000000100000 - 000
0000017ff0000 (usable)
Nov  9 15:30:44 bob kernel: [17179569.184000]  BIOS-e820: 0000000017ff0000 - 000
0000018000000 (ACPI data)
Nov  9 15:30:44 bob kernel: [17179569.184000]  BIOS-e820: 00000000fec00000 - 000
00000fec01000 (reserved)
alice@alice:~$ grep bob /var/log/messages | less
alice@alice:~$ SSSS
```

Figure 1: Selection of Bob's log in Alice's `/var/log/messages` file



```
 * Starting internet superserver inetd                                    [ ok ]
 * Starting AppLab -- EchoD vulnerable daemon                             [ ok ]
 * Starting AppLab -- ProFTPD 1.3.0                                       [ ok ]
 * Starting deferred execution scheduler atd                              [ ok ]
 * Starting periodic command scheduler crond                              [ ok ]
 * Starting web server apache2
apache2: Could not reliably determine the server's fully qualified domain name,
using 127.0.1.1 for ServerName
                                                                          [ ok ]

Debian GNU/Linux 5.0 bob tty1

bob login: bob
Password:
Last login: Tue Nov  9 15:24:50 CET 2021 on tty1
Linux bob 2.6.17.1 #1 SMP Mon Jul 5 18:50:04 CEST 2010 i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have mail.
bob@bob:~$ su
```

Figure 2: `shutdown -r now`

After rebooting bob's machine with `shutdown -r now`, we can see that `rsyslog` correctly reported the kernel reboot and successfully sent it to Alice's log file through TCP (port 514) ! We can thus get these informations on Alice's machine by looking at the log files with `grep bob /var/log/messages`

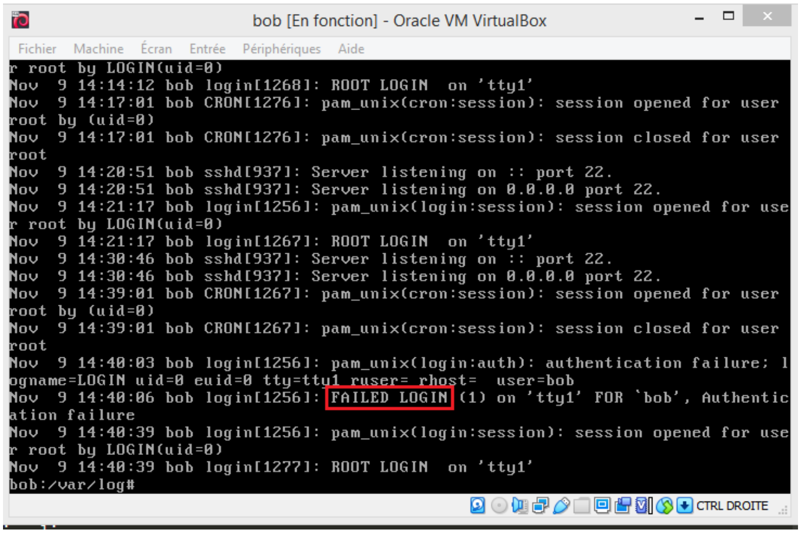
4 How would you design a system that makes it as difficult as possible for an adversary to compromise log information? Be creative in your solution!

To design a secured logging systems, the following tasks need to be applied :

- ***Securing the log files access***: Grant the right permissions to the authorized user for modifying / accessing the log files
- ***Securing the log content***: Sanitize (e.g. convert explicitly in string) the log messages / content to avoid user input, code injection & buffer overflow
- ***Securing the transmission***: Apply encryption on logs when transmitting them elsewhere, provide authenticity / integrity systems like computing checksum too
- ***Mitigating the damage***: Sending automatically the log message to a secure remote server before writing it to the log files so that the attacker can either delete all the logs or compromise them but there won't be any huge repercussions
- ***Preventing the damages***: Create `cronjob` to clean the compromised logs, create custom parsing with specific rules (remove entry with empty headers for example)

5 Search for entries that indicate login failures. What files do you have to check for this?

The authentication logs are located in `/var/log/auth.log`:



bob [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
CTRL DROITE

```
r root by LOGIN(uid=0)
Nov  9 14:14:12 bob login[1268]: ROOT LOGIN  on 'tty1'
Nov  9 14:17:01 bob CRON[1276]: pam_unix(cron:session): session opened for user
root by (uid=0)
Nov  9 14:17:01 bob CRON[1276]: pam_unix(cron:session): session closed for user
root
Nov  9 14:20:51 bob sshd[937]: Server listening on :: port 22.
Nov  9 14:20:51 bob sshd[937]: Server listening on 0.0.0.0 port 22.
Nov  9 14:21:17 bob login[1256]: pam_unix(login:session): session opened for use
r root by LOGIN(uid=0)
Nov  9 14:21:17 bob login[1267]: ROOT LOGIN  on 'tty1'
Nov  9 14:30:46 bob sshd[937]: Server listening on :: port 22.
Nov  9 14:30:46 bob sshd[937]: Server listening on 0.0.0.0 port 22.
Nov  9 14:39:01 bob CRON[1267]: pam_unix(cron:session): session opened for user
root by (uid=0)
Nov  9 14:39:01 bob CRON[1267]: pam_unix(cron:session): session closed for user
root
Nov  9 14:40:03 bob login[1256]: pam_unix(login:auth): authentication failure; l
ogname=LOGIN uid=0 euid=0 tty=tty1 ruser= rhost=  user=bob
Nov  9 14:40:06 bob login[1256]: FAILED LOGIN (1) on 'tty1' FOR `bob', Authentic
ation failure
Nov  9 14:40:39 bob login[1256]: pam_unix(login:session): session opened for use
r root by LOGIN(uid=0)
Nov  9 14:40:39 bob login[1277]: ROOT LOGIN  on 'tty1'
bob:/var/log#
```

Figure 3: `Failed login on Bobs machine`

6 What are the disadvantages of working with checksums? What is checked? What cannot be checked?

For checksums, the global sum is checked but the subunits are not. Thus, if there were errors in several subunits, this will not be detected if the sum is correct.

The authenticity of checksums can not be checked and the data may be corrupted if both the content and the checksum have been fraudulently changed.

If the checksum does not allows us to check the authenticity of logs, that means that logs can still be compromised without our knowledge. Therefore, we should use more than just checksum to verify the integrity of logs.

7 Why is this security relevant?

The logger allows comments to be added to the logs, which can be used to authenticate system events. Using logger with scripts also allows to monitor the running tasks on the system and add live information to the logs (real date for example).

8 Why may altered log entries be more dangerous than deleted ones?

When a log is deleted, you can notice it: if you know you should have logs, and you have nothing for a timestamp, you know some logs are missing.

If a log is altered, if it is done well, you have no trace of the alteration and nothing will indicate that the log has be modified. That means that a fraudulous action can be covered and nothing in the log will indicate it. Moreover, if you have full trust in your logs systems and the logs is altered, you will think that there is definitely no problems. An altered log is a false truth, and if one log is altered, you can trust none of the logs you have.