INSTITUTO SUPERIOR TÉCNICO

Departamento de Engenharia Informática

Forensics Cyber Security

MEIC / METI 2017-2018 – 1st Semester

Digital Forensics Report

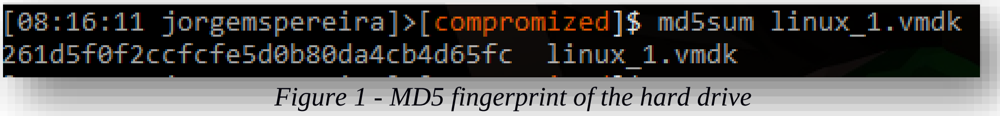
Luís Aguiar 80950 & Jorge Pereira 81428 & Filipe Azevedo 82468

1 Objectives of the investigation

In this case we were given an image of a hard drive collected from a server that is believed to have been infected by malware. We know that the file system is EXT3, and our job is to collect some evidences of that malware by analyzing the content of the log folder in that hard drive.

2 Artifacts for analysis

The only artifact that was given to us is that image of a hard drive collected from the server. Before starting our analysis, we verified if the image was not modified before it reaches us. After making a copy of it, we verified the md5 fingerprint of the file.



```
[08:16:11 jorgemspereira]>[compromized]$ md5sum linux_1.vmdk
261d5f0f2ccfcfe5d0b80da4cb4d65fc  linux_1.vmdk
```

Figure 1 - MD5 fingerprint of the hard drive

After this verification we attached the image to our workstation, with special care to not corrupt anything.

3 Evidence to look for

From here we proceeded with the investigation. We found that there were still many files within the directory from which we wanted to get information (*/var/log*). However, using some forensic investigation tools (such as **fls** and **icat**), we also found out that there were many files that had been deleted from that folder – namely the samba log (in the *samba* folder), the apache log (in the *httpd* folder), and 16 other files.

4 Examination details

With the information obtained we began to extract the deleted files using the tools referred previously. However, to facilitate analysis only the readable content of the files has been extracted from the files, and files that did not have content were not included either, although there are still some metadata about them. In total we were able to gather 22 files, some that even looked like log files, and the others that had suspicious content. A summary of the files' content can be found in the following table.

Name	Id	Size (bytes)	MD5	Description
cron	01	315	dbb04550b472206defc110c82afce44b	It looks like some manual for ADDLOG, we do not know if this is supposed to be the real content of the file.
dmesg	02	16384	c59428104fb9d66018093d4b91706fe5	It looks like a normal log.
ksyms.0	03	6468	9001623dc9a164f7e3b9053275105f1e	It looks like a normal log.
mailog.1	04	59137	cf1d1e50ed26092f8e45f567a8c1d0b8	Doesn’t appear to be a log file, contains some suspicious content.
rpmpkgs	05	187	0f893bec8e2e7622e58d8fdf96eaa24d	It looks like some manual for LISTLOGS, we do not know if this is supposed to be the real content of the file.
rpmpks.1	06	150	7721de6d08424d3f529f21a2a3be53dc	It looks like a normal log.
spooler.1	07	2551	fbacbac680750bb27b7bb0fc60d8aa47	Doesn’t appear to be a log file, contains some suspicious content.
xferlog	08	249	d53baa4ddd874dd83b6b616de7f4efb5	It looks like some manual for SETLEAVEMSG, we do not know if this is supposed to be the real content of the file.
xferlog.1	09	179	9db9bac6f1a7083b89a49880138453da	It looks like a normal log.
httpd/access_log	10	253	be649cf1a11b1e246b616ecd833a57ad	It looks like a normal access log.
httpd/access_log.1	11	3253	435d7995cfda4a26eec22846472e481b	Doesn’t appear to be a log file, contains some suspicious content.
httpd/error_log	12	23335716	61e73161df9da9171fbcf503ea01f075	It looks like a normal error log, but with a lot of errors in a short period of time.
httpd/ssl_engine_log	13	22795530	c4f6250faf7add9a0d97e863eb3737ff	It looks like a normal ssl engine log, but with a lot of errors in a short period of time.

samba/gustavo_.log.1	14	593	3ac4b68882e17b0d886f17e252e1de3b	It looks like some manual for ADDALOW, we do not know if this is supposed to be the real content of the file.
samba/ixia1600.log.1	15	416	72825dcd4c779f317331f6146b7f8197	It looks like some manual for ADDASK, we do not know if this is supposed to be the real content of the file.
samba/localhost.log	16	294	6298a9b536da65fdca3ec19e3da09df2	It looks like a bash script with three for loops which writes in a file with a suspicious name “hide.log”.
samba/localhost.log.1	17	236	6818c28c7333422b1d590d525c89383d	It looks like some manual for ADDBAN, we do not know if this is supposed to be the real content of the file.
samba/log.nmbd	18	201	62e5b4735a532142a51041a60e40823d	It looks like a normal log file.
samba/log.smbd	19	362	f0b78916f1994fc6d1d545e9692fa2ab	It looks like some manual for DELLOG, we do not know if this is supposed to be the real content of the file.
samba/main2000.log	20	233	cf964525e2a610d4b602ef8c5f072e23	It looks like some manual for DELAUTOOP, we do not know if this is supposed to be the real content of the file.
samba/main2000.log.1	21	537	7ec416697e55c012bb74632601297593	It looks like some manual for ADDDCC, we do not know if this is supposed to be the real content of the file.
samba/smbd.log.1	22	955	977f56a4c191cb055ca8525b51984e5e	It looks like some manual for ADDNETWORK, we do not know if this is supposed to be the real content of the file.

We also searched for examples of the samba and apache logs on the internet and found that the samba file usually contains the string “Allowed connection from”. With this knowledge, we then used **grep** tool to search for this string to try to find the samba logs on the unallocated regions of the disk. However, we couldn’t find any files that appeared to be logs, just some code with malware (rootkit). Since we didn’t find anything on the unallocated disk regions, we tried searching on the whole disk. On the whole disk we found several instances of the string “Allowed connection from” and decided to calculate the offset of this instances to find the file that had the string instances. We wrote the result in the file smbd.log. We were not able to find any logs from apache on either the unallocated regions of the disks or the rest of the disk. Information about the smbd.log file is in the table below.

Name	Id	Size (bytes)	MD5	Description
smbd.log	23	1057993	1d2436e234e954180b8fa15f46f3b961	Looks like a samba log file.

5 Analysis results

From the analysis of the files found on the disk log directory that was delivered to us, we found some files that have the normal file content in that directory. However, we also found unusual files since they contained code that is not normal in this directory which is only used to keep activity records of several applications. A more detailed analysis of the code found may be a starting point for future investigations, since it was also found suspicious code in the unallocated space of the disk. Despite this, since we couldn’t prove that it was located in the directory under investigation we didn’t feel it was relevant to include in this report.

6 Conclusions

In conclusion, we were able to find deleted files in the log directory, some of which had suspicious code that could indicate that the server was infected by a malware.

10th November 2017, Instituto Superior Técnico

Luís Aguiar - 80950

Jorge Pereira - 81428

Filipe Azevedo - 82468