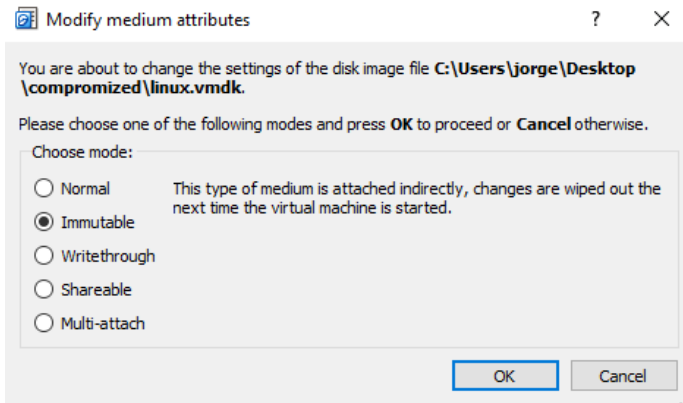
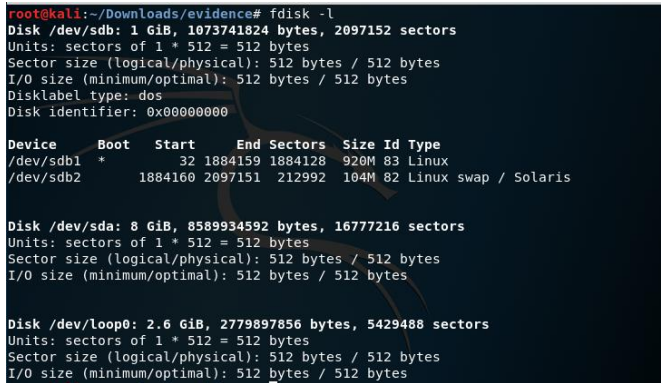


The Case of the Infected Server

Examination Log

Examiners: Luís Aguiar 80950, Jorge Pereira 81428, Filipe Azevedo 82468

Date / Time	Description
08-11-2017, 16h00	Luis, Filipe and Jorge calculated the md5 of the image of the disk, and verified that the file was not changed before it was delivered to them.
16h05	<p>They inserted the disk to the virtual machine with Kali Linux, and to ensure that the disk was not changed during the process, they set it as immutable. This was achieved by:</p>  <p>Figure 1 - Changing the disk to immutable</p> <p>By doing this the Virtual Box already changed some metadata from the disk however, its contents have not changed. “That can be validated with the vbindiff tool which highlights the differences of two binaries and shows that only physical characteristics of the geometry of the virtual disk are changed such as a number of cylinders, probably to match the Linux adapter.”. The md5 of the image was 10437d1eb6578307f957014b3b18e920.</p>
16h10	They started the virtual machine in forensic mode with the disk attached.
16h20	<p>They decided to use the fdisk tool to find out more information about the inserted disk.</p>  <p>Figure 2 - Some information about the disk</p>

16h30	<p>From there they decided to use the fls tool to navigate over the inodes on which there is still some metadata. They found the <i>var</i> folder, and inside it the <i>log</i> folder, both still allocated. However, in their interior, they noticed the following content:</p> <pre> root@kali:~/Downloads/evidence# fls /dev/sdb1 44613 r/r 44617: wtmp l/l 47173: messages r/r 46634: secure r/r 46901: maillog r/r 46902: cron r/r 46903: spooler r/r 46904: boot.log d/d * 46607(realloc): samba r/r * 46933(realloc): xferlog d/d * 46733(realloc): httpd r/r * 46901(realloc): dmesg r/r * 45307(realloc): ksyms.0 r/r * 46917(realloc): cron r/d * 46912(realloc): boot.log r/r * 46921(realloc): rpmpkgs r/d * 46937(realloc): messages.1 r/r * 47147(realloc): secure.1 r/r * 47148(realloc): maillog.1 r/r * 47149(realloc): spooler.1 r/r * 47150(realloc): boot.log.1 r/r * 47151(realloc): cron.1 r/r * 47152(realloc): rpmpkgs.1 r/r * 47158(realloc): xferlog.1 r/r * 46903(realloc): cron.1 r/r * 46616(realloc): rpmpkgs.1 r/r * 46634(realloc): xferlog.1 r/r * 45838(realloc): wtmp.1 </pre> <p><i>Figure 3 - Content inside the /var/log folder</i></p>
08-11-2017, 16h00	<p>They decided to try to extract traces of the files that had been deleted from the <i>var/log/</i> folder by using the icat tool to search the inodes that were previously allocated to those files, despite being now being allocated to other files/directories. For example, the command:</p> <pre>icat /dev/sdb1 46933</pre> <p>Will return the content of the file now allocated by the inode 46933 that was previously allocated to the “xferlog” file that was deleted from the folder.</p>
16h35	<p>They were able to extract the contents of some of the files from the inodes presented in the above table. The inodes 46607 and 46733 were previously allocated to a directory and they were also able to retrieve some of the content of the files that were inside those directories. The inodes that previously allocated the files “boot.log” and “messages.1” now allocate a directory, meaning that they were unable to recover information about those files. Some information about these files can be found in the table at the end of this Examination Log.</p>
16h40	<p>They then tried to find file server and web server logs. These logs correspond, respectively, to the log files of “samba” (smbd) and “apache” (httpd) which were installed on the server. They searched on the internet and found out that the logs of “samba” usually contained the string:</p> <p>“Allowed connection from”</p> <p>So they tried to use the grep tool to search for that string on the unallocated space of the disk, but</p>

	they didn't succeed, so they tried to search on the whole disk (not just in the unallocated space).
17h00	<p>The strings were found between byte number 567048224 and byte number 573466304. With this information they subtracted the byte numbers obtaining the number 6418080. Using the dd tool, they searched for 6148080 bytes since byte number 567048224 and wrote the result to the smbd.log file.</p> <pre>root@kali:~/Desktop# grep "Allowed connection from" text.str 567048224 Allowed connection from %s (%s) 567350624 Allowed connection from %s (%s) 568045344 Allowed connection from %s (%s) 568357664 Allowed connection from %s (%s) 568665632 Allowed connection from %s (%s) 569001920 Allowed connection from %s (%s) 569538912 Allowed connection from %s (%s) 570823488 Allowed connection from %s (%s) 571310016 Allowed connection from %s (%s) 571779872 Allowed connection from %s (%s) 572102336 Allowed connection from %s (%s) 572624352 Allowed connection from %s (%s) 573046080 Allowed connection from %s (%s) 573466304 Allowed connection from %s (%s) root@kali:~/Desktop# dd if=/dev/sdal count=6418080 skip=567048224 bs=1 > smbd.log</pre> <p><i>Figure 4 - Commands used to extract smbd file</i></p> <p>More information about this file can be found in the table at the end of this Examination Log.</p>

-- 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.
maillog.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 ADDALLOW, 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.
smbd.log	23	1057993	1d2436e234e954180b8fa15f46f3b961	Looks like a samba log file.