Markus Afonso, Devin Kandola
Set C
January 30, 2024

(Q1) Navigate to the folder where you can see logs on the Metasploitable2 VM. What are the different log files you see there?

```
msfadmin@metasploitable:/var/log$ ls
apache2   daemon.log    dmesg.2.gz  kern.log   mail.warn   samba
apparmor  debug         dmesg.3.gz  lastlog    messages    syslog
apt       dist-upgrade  dmesg.4.gz  lpr.log    mysql       tomcat5.5
auth.log  dmesg         dpkg.log    mail.err   news        udev
boot      dmesg.0       fsck        mail.info  postgresql  user.log
btmp      dmesg.1.gz    installer   mail.log   proftpd     vsftpd.log
msfadmin@metasploitable:/var/log$ _
```

auth.log: Contains authentication logs, for example successful logins, failed login attempts, and authentication mechanism used.

kern.log: contains information/logs related to the linux kernel such as errors and information to help diagnose issues related to the kernel.

syslog: A file that contains log information regarding your entire systems activity

mail.log: Contains logs of mail server activities if one is set up.

(Q2) What kind of logs are written to syslog file? (Explain the entires you see in the conf file)

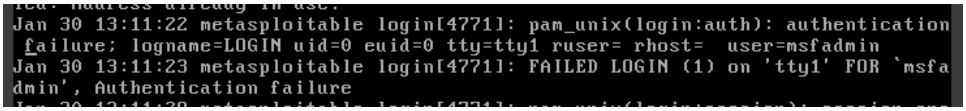
```
#  /etc/syslog.conf     Configuration file for syslogd.
#
#                       For more information see syslog.conf(5)
#                       manpage.

#
# First some standard logfiles.  Log by facility.
#

auth,authpriv.*                 /var/log/auth.log
*.*;auth,authpriv.none          -/var/log/syslog
#cron.*                         /var/log/cron.log
daemon.*                        -/var/log/daemon.log
kern.*                          -/var/log/kern.log
lpr.*                           -/var/log/lpr.log
mail.*                          -/var/log/mail.log
user.*                          -/var/log/user.log

#
```

```
# Logging for the mail system.  Split it up so that
# it is easy to write scripts to parse these files.
#
mail.info                       -/var/log/mail.info
mail.warn                       -/var/log/mail.warn
mail.err                        /var/log/mail.err

# Logging for INN news system
#
news.crit                       /var/log/news/news.crit
news.err                        /var/log/news/news.err
news.notice                     -/var/log/news/news.notice

#
# Some `catch-all' logfiles.
#
*.=debug;\
        auth,authpriv.none;\
        news.none;mail.none     -/var/log/debug
*.=info;*.=notice;*.=warn;\
        auth,authpriv.none;\
        cron,daemon.none;\
        mail,news.none          -/var/log/messages
_
```

Based on the entries of the conf file. The logs within the file include standard log files such as kern logs auth logs such as successful and unsuccesful logins. It also contains mail system log files that are further split. For example (mail.info, mail.warn, and mail.err).

(Q3) What kind of logs are written to auth.log file? (Explain the entires you see in the conf file)

Based on the entries of the conf file. The logs within the auth.log file include logs associated with auth and auth.priv. Seraching for 'failure' we can find the authentication failure when we used the wrong password:



(Q4) You might see some zipped files in the log folder (e.g. dmesg.1.gz,... in the following screenshot), the log rotation process generates these files.

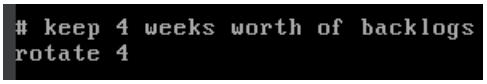
Log rotation is helpful to eliminiate and control larger files. It gives the ability to rotate files. If a log file gets to big a new file will be created and the new events wiill be written to it. Older log files are rotated across the system, but usually remain for auditing purposes.

(Q5) How often are logs rotated?

Log files are rotated weekly

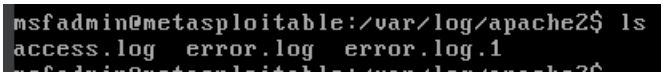
(Q6) How many old log files are kept?

Log files are kept for 4 rotations or 4 weeks. If we set rotations to daily, they'd be kept 4 days back.



(Q7) What kind of log files can you see there (apache2 folder)?

There are three log folders: access.log, error.log and error.log.1



access.log:

This log contains the requests made to the apache server

```
10.0.2.15 - - [16/Jan/2024:12:56:48 -0500] "OPTIONS / HTTP/1.1" 200 891 "-" "Moz
illa/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.2.15 - - [16/Jan/2024:12:56:48 -0500] "OPTIONS / HTTP/1.1" 200 891 "-" "Moz
illa/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.2.15 - - [16/Jan/2024:12:56:48 -0500] "OPTIONS / HTTP/1.1" 200 891 "-" "Moz
illa/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.2.15 - - [16/Jan/2024:12:56:48 -0500] "OPTIONS / HTTP/1.1" 200 891 "-" "Moz
illa/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.2.15 - - [16/Jan/2024:12:57:54 -0500] "GET / HTTP/1.0" 200 891 "-" "-"
10.0.2.15 - - [16/Jan/2024:12:57:54 -0500] "GET / HTTP/1.1" 200 891 "-" "-"
10.0.2.15 - - [16/Jan/2024:13:30:05 -0500] "GET / HTTP/1.0" 200 891 "-" "-"
10.0.2.15 - - [16/Jan/2024:13:32:36 -0500] "GET /nmaplowercheck1705429960 HTTP/1
.1" 404 301 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.or
g/book/nse.html)"
10.0.2.15 - - [16/Jan/2024:13:32:37 -0500] "GET /evox/about HTTP/1.1" 404 287 "-
" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.htm
l)"
10.0.2.15 - - [16/Jan/2024:13:32:36 -0500] "POST /sdk HTTP/1.1" 404 280 "-" "Moz
illa/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.2.15 - - [16/Jan/2024:13:32:37 -0500] "GET /HNAP1 HTTP/1.1" 404 282 "-" "Mo
zilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
10.0.2.15 - - [16/Jan/2024:13:32:36 -0500] "GET / HTTP/1.0" 200 891 "-" "-"
10.0.2.15 - - [16/Jan/2024:13:32:49 -0500] "GET / HTTP/1.0" 200 891 "-" "-"
10.0.2.15 - - [16/Jan/2024:13:32:49 -0500] "GET / HTTP/1.1" 200 891 "-" "-"
msfadmin@metasploitable:/var/log/apache2$
```

error.log:

This log contains the errors made during operations of the apache server.

```
[Tue Jan 16 12:56:41 2024] [error] [client 10.0.2.15] File does not exist: /var/
www/sdk
[Tue Jan 16 12:56:42 2024] [error] [client 10.0.2.15] File does not exist: /var/
www/robots.txt
[Tue Jan 16 12:56:44 2024] [error] [client 10.0.2.15] File does not exist: /var/
www/evox
[Tue Jan 16 12:56:44 2024] [error] [client 10.0.2.15] File does not exist: /var/
www/favicon.ico
[Tue Jan 16 12:56:45 2024] [error] [client 10.0.2.15] File does not exist: /var/
www/.git
[Tue Jan 16 13:32:36 2024] [error] [client 10.0.2.15] File does not exist: /var/
www/sdk
[Tue Jan 16 13:32:36 2024] [error] [client 10.0.2.15] File does not exist: /var/
www/nmaplowercheck1705429960
[Tue Jan 16 13:32:37 2024] [error] [client 10.0.2.15] File does not exist: /var/
www/HNAP1
[Tue Jan 16 13:32:37 2024] [error] [client 10.0.2.15] File does not exist: /var/
www/evox
[Tue Jan 23 13:35:07 2024] [notice] Apache/2.2.8 (Ubuntu) DAV/2 configured -- re
suming normal operations
[Sun Jan 28 22:52:44 2024] [notice] Apache/2.2.8 (Ubuntu) DAV/2 configured -- re
suming normal operations
[Tue Jan 30 13:11:13 2024] [notice] Apache/2.2.8 (Ubuntu) DAV/2 configured -- re
suming normal operations
msfadmin@metasploitable:/var/log/apache2$ _
```

error.log.1:

This log contains the archive/rotated logs and is currently empty

```
msfadmin@metasploitable:/var/log/apache2$ cat error.log.1
msfadmin@metasploitable:/var/log/apache2$
```

(Q8) What command gives you the number of log entries (lines) in this file?

We can use wc –l access.log to get the line count of the access.log file.

```
root@metasploitable:/var/log/apache2# wc -l access.log
2 access.log
```

(Q9) Take a screenshot of the logs and identify different parts of the log entries using this table:

```
root@metasploitable:/var/log/apache2# printf "" > access.log
root@metasploitable:/var/log/apache2# cat access.log
root@metasploitable:/var/log/apache2# cat access.log
10.0.2.15 - - [30/Jan/2024:13:37:11 -0500] "GET / HTTP/1.1" 200 891 "-" "Mozilla
/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
10.0.2.15 - - [30/Jan/2024:13:37:12 -0500] "GET /favicon.ico HTTP/1.1" 404 288 "
http://10.0.2.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Fire
fox/102.0"
root@metasploitable:/var/log/apache2# _
```

(Q10) How many IPs did you get from the previous step?

Just one, 10.0.2.15 which is the kali ip.

(Q11) Now, update the cut command (before piping it to uniq) to return the timestamps as well as the IPs to see how rapid these connections from the same IP were happening. What can you learn from this data?

Tons of requests within seconds of each other, all from the same ip, probably means that it is an attack.

```
      2 10.0.2.15 [30/Jan/2024:14:14:26
      2 10.0.2.15 [30/Jan/2024:14:14:29
      3 10.0.2.15 [30/Jan/2024:14:14:25
      3 10.0.2.15 [30/Jan/2024:14:14:26
      3 10.0.2.15 [30/Jan/2024:14:14:28
      4 10.0.2.15 [30/Jan/2024:14:14:20
      4 10.0.2.15 [30/Jan/2024:14:14:21
      5 10.0.2.15 [30/Jan/2024:14:14:11
      5 10.0.2.15 [30/Jan/2024:14:14:19
      5 10.0.2.15 [30/Jan/2024:14:14:24
      6 10.0.2.15 [30/Jan/2024:14:14:23
      7 10.0.2.15 [30/Jan/2024:14:14:22
      7 10.0.2.15 [30/Jan/2024:14:14:27
      8 10.0.2.15 [30/Jan/2024:14:14:12
      9 10.0.2.15 [30/Jan/2024:14:14:10
      9 10.0.2.15 [30/Jan/2024:14:14:13
      9 10.0.2.15 [30/Jan/2024:14:14:14
      9 10.0.2.15 [30/Jan/2024:14:14:15
     11 10.0.2.15 [30/Jan/2024:14:14:28
     15 10.0.2.15 [30/Jan/2024:14:14:16
     19 10.0.2.15 [30/Jan/2024:14:14:11
     23 10.0.2.15 [30/Jan/2024:14:14:17
     25 10.0.2.15 [30/Jan/2024:14:14:26
     28 10.0.2.15 [30/Jan/2024:14:14:18
root@metasploitable:/var/log/apache2# _
```

(Q12) Which user-agent has the maximum number of appearances? How can we find the IP addresses that used this user agent?

cat access.log | cut –d ‘”’ -f 1,6 | cut –d “ “ --complement –f 4,5 | uniq –c | sort –n

The first command cut –d ‘”’ -f 1,6 grabs the ip and date time stamp and agent.

The second cut –d “ “ --complement –f 4,5 cuts the date time stamp

uniq –c | sort –n finds unique lines and orders them appropriately.

```
root@metasploitable:/var/log/apache2# cat access.log | cut -d '"' -f 1,6 | cut -
d " " --complement -f 4,5 | uniq -c | sort -n
      2 10.0.2.15 - - "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
Firefox/102.0
    247 10.0.2.15 - - "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537
.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36
root@metasploitable:/var/log/apache2#
```