Logwatch and TCPDump

Written by Tyler Weiss 19 MAR 2024

Exercise 4 - Installing Logwatch

Run 'sudo apt install logwatch -y' to install program

```
rec0nrat@demoserver1:~$ sudo apt install logwatch -y
[sudo] password for rec0nrat:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
logwatch is already the newest version (7.5.6-1ubuntu1).
0 upgraded, 0 newly installed, 0 to remove and 21 not upgraded.
rec0nrat@demoserver1:~$
```

Exercise 5 - Basic Service Usage

Create a detailed report on the ssh service, using logwatch, by typing the following command: 'sudo logwatch --service sshd --detail high --range today --output stdout'

```
rec0nrat@demoserver1:~$ sudo logwatch --service sshd --detail high --range today --output stdout

 ################### Logwatch 7.5.6 (07/23/21) ####################
        Processing Initiated: Tue Mar 19 14:51:36 2024
        Date Range Processed: today
                              ( 2024-Mar-19 )
                              Period is day.
        Detail Level of Output: 10
        Type of Output/Format: stdout / text
        Logfiles for Host: demoserver1
 ##################################################################

 --------------------- SSHD Begin ------------------------

 SSHD Started: 2 Times

 Users logging in through sshd:
    rec0nrat:
       192.168.1.190 (MSI): 1 Time

 ---------------------- SSHD End ------------------------


 ###################### Logwatch End #########################

rec0nrat@demoserver1:~$
```

Exercise 6 Examining Logs Over Date Ranges

The following screen captures show reports produced by different protocols using multiple range and detail settings.

```
rec0nrat@demoserver1:~$ sudo logwatch --service sshd --detail low --range all --output stdout
[sudo] password for rec0nrat:

 ################### Logwatch 7.5.6 (07/23/21) ####################
        Processing Initiated: Tue Mar 19 15:09:35 2024
        Date Range Processed: all
        Detail Level of Output: 0
        Type of Output/Format: stdout / text
        Logfiles for Host: demoserver1
 ##################################################################

 -------------------- SSHD Begin ------------------------

 Network Read Write Errors: 1

 SSHD Killed: 1 Time

 SSHD Started: 26 Times

 Failed logins from:
    192.168.1.190 (MSI): 2 Times

 Users logging in through sshd:
    rec0nrat:
       192.168.1.190 (MSI): 11 Times

 **Unmatched Entries**
 error: kex_exchange_identification: Connection closed by remote host : 3 Times

 --------------------- SSHD End ------------------------


 ####################### Logwatch End #########################

rec0nrat@demoserver1:~$
```

```
rec0nrat@demoserver1:~$ sudo logwatch --service http  --detail high --range all --output stdout

 ################### Logwatch 7.5.6 (07/23/21) ####################
        Processing Initiated: Tue Mar 19 15:15:34 2024
        Date Range Processed: all
        Detail Level of Output: 10
        Type of Output/Format: stdout / text
        Logfiles for Host: demoserver1
 ##################################################################

 -------------------- httpd Begin ------------------------

 0.05 MB transferred in 17 responses  (1xx 0, 2xx 13, 3xx 0, 4xx 4, 5xx 0)
     7 Images (0.02 MB),
    10 Content pages (0.03 MB),

 Requests with error response codes
    404 Not Found
       /favicon.ico: 3 Time(s)
       /index.txt: 1 Time(s)

 -------------------- httpd End ------------------------


 ###################### Logwatch End #########################

rec0nrat@demoserver1:~$ sudo logwatch --service http  --detail high --range today --output stdout

 ################### Logwatch 7.5.6 (07/23/21) ####################
        Processing Initiated: Tue Mar 19 15:16:12 2024
        Date Range Processed: today
                              ( 2024-Mar-19 )
                              Period is day.
        Detail Level of Output: 10
        Type of Output/Format: stdout / text
        Logfiles for Host: demoserver1
 ##################################################################

 -------------------- httpd Begin ------------------------

 0.00 MB transferred in 1 responses  (1xx 0, 2xx 1, 3xx 0, 4xx 0, 5xx 0)
    1 Images (0.00 MB),

 -------------------- httpd End ------------------------


 ###################### Logwatch End #########################

rec0nrat@demoserver1:~$
```

```
rec0nrat@demoserver1:~$ sudo logwatch --service http  --detail medium --range "between -10 days and today" --output s
tdout

 ################### Logwatch 7.5.6 (07/23/21) ####################
        Processing Initiated: Tue Mar 19 15:19:37 2024
        Date Range Processed: between -10 days and today
                              ( 2024-Mar-09 / 2024-Mar-19 )
                              Period is day.
        Detail Level of Output: 5
        Type of Output/Format: stdout / text
        Logfiles for Host: demoserver1
 ##################################################################

 -------------------- httpd Begin ------------------------

 0.02 MB transferred in 9 responses  (1xx 0, 2xx 7, 3xx 0, 4xx 2, 5xx 0)
    3 Images (0.01 MB),
    6 Content pages (0.02 MB),

 Requests with error response codes
    404 Not Found
       /favicon.ico: 1 Time(s)
       /index.txt: 1 Time(s)

 -------------------- httpd End ------------------------


 ###################### Logwatch End #########################

rec0nrat@demoserver1:~$
```

Exercise 7 - View/Compare auth.log and logwatch Output

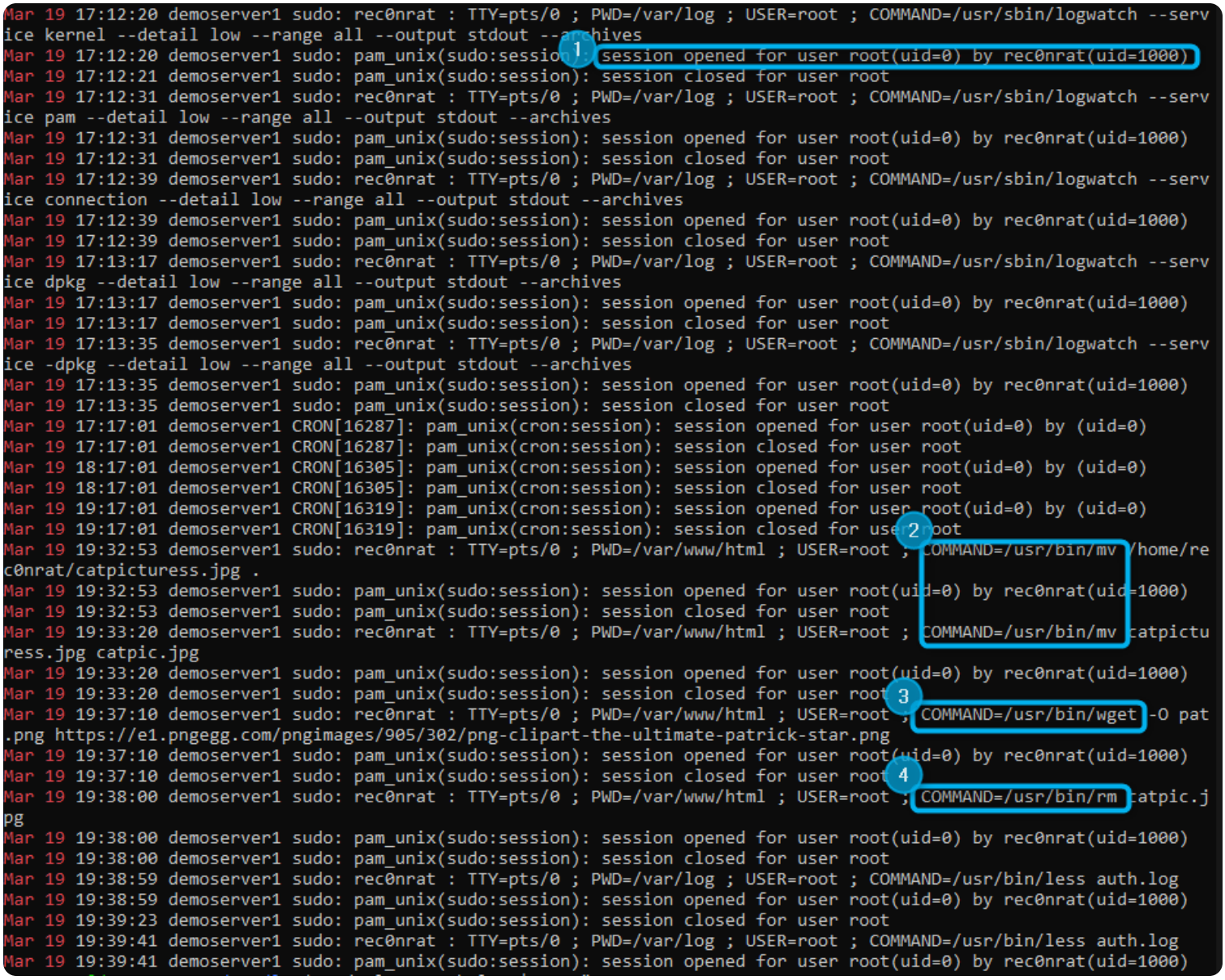
Task #1 - Review Raw Log Entries

1. Inspect the raw log entries in '/var/log/auth.log'
2. Generate a logwatch report for March 19th

Run the command 'sudo less auth.log |grep "Mar 19"' to output the log files for March 19th.

```
rec0nrat@demoserver1:/var/log$ sudo less auth.log |grep "Mar 19"
Mar 19 00:17:01 demoserver1 CRON[2277]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 19 00:17:01 demoserver1 CRON[2277]: pam_unix(cron:session): session closed for user root
Mar 19 01:17:01 demoserver1 CRON[2296]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 19 01:17:01 demoserver1 CRON[2296]: pam_unix(cron:session): session closed for user root
```

Only the logs from '17:12:00' to present will be analyzed.




```
Mar 19 17:12:20 demoserver1 sudo: rec0nrat : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/usr/sbin/logwatch --serv
ice kernel --detail low --range all --output stdout --archives
Mar 19 17:12:20 demoserver1 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by rec0nrat(uid=1000)
Mar 19 17:12:21 demoserver1 sudo: pam_unix(sudo:session): session closed for user root
Mar 19 17:12:31 demoserver1 sudo: rec0nrat : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/usr/sbin/logwatch --serv
ice pam --detail low --range all --output stdout --archives
Mar 19 17:12:31 demoserver1 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by rec0nrat(uid=1000)
Mar 19 17:12:31 demoserver1 sudo: pam_unix(sudo:session): session closed for user root
Mar 19 17:12:39 demoserver1 sudo: rec0nrat : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/usr/sbin/logwatch --serv
ice connection --detail low --range all --output stdout --archives
Mar 19 17:12:39 demoserver1 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by rec0nrat(uid=1000)
Mar 19 17:12:39 demoserver1 sudo: pam_unix(sudo:session): session closed for user root
Mar 19 17:13:17 demoserver1 sudo: rec0nrat : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/usr/sbin/logwatch --serv
ice dpkg --detail low --range all --output stdout --archives
Mar 19 17:13:17 demoserver1 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by rec0nrat(uid=1000)
Mar 19 17:13:17 demoserver1 sudo: pam_unix(sudo:session): session closed for user root
Mar 19 17:13:35 demoserver1 sudo: rec0nrat : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/usr/sbin/logwatch --serv
ice -dpkg --detail low --range all --output stdout --archives
Mar 19 17:13:35 demoserver1 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by rec0nrat(uid=1000)
Mar 19 17:13:35 demoserver1 sudo: pam_unix(sudo:session): session closed for user root
Mar 19 17:17:01 demoserver1 CRON[16287]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 19 17:17:01 demoserver1 CRON[16287]: pam_unix(cron:session): session closed for user root
Mar 19 18:17:01 demoserver1 CRON[16305]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 19 18:17:01 demoserver1 CRON[16305]: pam_unix(cron:session): session closed for user root
Mar 19 19:17:01 demoserver1 CRON[16319]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Mar 19 19:17:01 demoserver1 CRON[16319]: pam_unix(cron:session): session closed for user root
Mar 19 19:32:53 demoserver1 sudo: rec0nrat : TTY=pts/0 ; PWD=/var/www/html ; USER=root ; COMMAND=/usr/bin/mv /home/re
c0nrat/catpicturess.jpg .
Mar 19 19:32:53 demoserver1 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by rec0nrat(uid=1000)
Mar 19 19:32:53 demoserver1 sudo: pam_unix(sudo:session): session closed for user root
Mar 19 19:33:20 demoserver1 sudo: rec0nrat : TTY=pts/0 ; PWD=/var/www/html ; USER=root ; COMMAND=/usr/bin/mv catpictu
ress.jpg catpic.jpg
Mar 19 19:33:20 demoserver1 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by rec0nrat(uid=1000)
Mar 19 19:33:20 demoserver1 sudo: pam_unix(sudo:session): session closed for user root
Mar 19 19:37:10 demoserver1 sudo: rec0nrat : TTY=pts/0 ; PWD=/var/www/html ; USER=root ; COMMAND=/usr/bin/wget -O pat
.png https://e1.pngegg.com/pngimages/905/302/png-clipart-the-ultimate-patrick-star.png
Mar 19 19:37:10 demoserver1 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by rec0nrat(uid=1000)
Mar 19 19:37:10 demoserver1 sudo: pam_unix(sudo:session): session closed for user root
Mar 19 19:38:00 demoserver1 sudo: rec0nrat : TTY=pts/0 ; PWD=/var/www/html ; USER=root ; COMMAND=/usr/bin/rm catpic.j
pg
Mar 19 19:38:00 demoserver1 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by rec0nrat(uid=1000)
Mar 19 19:38:00 demoserver1 sudo: pam_unix(sudo:session): session closed for user root
Mar 19 19:38:59 demoserver1 sudo: rec0nrat : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/usr/bin/less auth.log
Mar 19 19:38:59 demoserver1 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by rec0nrat(uid=1000)
Mar 19 19:39:23 demoserver1 sudo: pam_unix(sudo:session): session closed for user root
Mar 19 19:39:41 demoserver1 sudo: rec0nrat : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/usr/bin/less auth.log
Mar 19 19:39:41 demoserver1 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by rec0nrat(uid=1000)
```

Run the command "sudo logwatch --detail medium --range "since 2024/03/19 17:12:00" --output stdout --ar
chives' to generate a logwatch report within the specified timeline to analyze.

```
rec0nrat@demoserver1:/var/log$ sudo logwatch --detail medium --range "since 2024/03/19 17:12:00" --output stdout --ar
chives

 ################### Logwatch 7.5.6 (07/23/21) ####################
        Processing Initiated: Tue Mar 19 20:08:07 2024
        Date Range Processed: since 2024/03/19 17:12:00
                              ( 2024-Mar-19 / 2024-Mar-19 )
                              Period is day.
        Detail Level of Output: 5
        Type of Output/Format: stdout / text
        Logfiles for Host: demoserver1
 ##################################################################
```

```
 --------------------- pam_unix Begin ------------------------

 cron:
    Sessions Opened:
       root(uid=0): 8 Time(s)

 sshd:
    Sessions Opened:
       rec0nrat(uid=1000): 1 Time(s)

 sudo:
    Sessions Opened:
       rec0nrat -> root(uid=0): 67 Time(s)

 systemd-user:
    Sessions Opened:
       rec0nrat(uid=1000): 1 Time(s)


 --------------------- pam_unix End -------------------------


 --------------------- Connections (secure-log) Begin ------------------------


 **Unmatched Entries**
    systemd-logind: Power key pressed.: 1 Time(s)
    systemd-logind: Powering Off...: 1 Time(s)
    systemd-logind: System is powering down.: 1 Time(s)

 --------------------- Connections (secure-log) End -------------------------


 --------------------- SSHD Begin ------------------------


 SSHD Started: 2 Times

 Users logging in through sshd:
    rec0nrat:
       192.168.1.190 (MSI): 1 Time

 --------------------- SSHD End -------------------------


 --------------------- Sudo (secure-log) Begin ------------------------


 rec0nrat => root
 ----------------
 /usr/bin/apt                    -   1 Time(s).
 /usr/bin/cat                    -   2 Time(s).
 /usr/bin/gzip                   -   2 Time(s).
 /usr/bin/less                   -   4 Time(s).
 /usr/bin/mv                     -   2 Time(s).
 /usr/bin/rm                     -   1 Time(s).
 /usr/bin/wget                   -   1 Time(s).
 /usr/sbin/logwatch              -  54 Time(s).

 --------------------- Sudo (secure-log) End -------------------------
```

The below list shows some of the correlations between the raw auth.log output and the report generated by logwatch. (matching entries are numbered in the screen captures):

1. Clearly shows that user 'rec0nrat' is logged in on a ssh session.
2. The 'mv' command was used twice to move image files.
3. The 'rm' command was used once to delete an image.
4. The 'wget' command was used once to download an image and save it as 'pat.png'

Exercise 8 - Syslog in Linux

Task #1

1. Configure syslog to send to the host OS

In order to forward syslog to a specific server the configuration file for rsyslog needs to be edited. Configuration files for syslog are located in the '/etc/rsyslog.d/' directory or the file '/etc/rsyslog.conf'. Adding '*.*@<server>:514' to the end of '/etc/rsyslog.conf' will send syslog to the specified server via UDP over port 514.

```
rec0nrat@demoserver1:/etc$ sudo vim rsyslog.conf
[sudo] password for rec0nrat:
```

```
#
# Where to place spool and state files
#
$WorkDirectory /var/spool/rsyslog

#
# Include all config files in /etc/rsyslog.d/
#
$IncludeConfig /etc/rsyslog.d/*.conf

*.*@192.168.1.210:514
:wq
```

```
rec0nrat@demoserver1:/etc$ tail rsyslog.conf
# Where to place spool and state files
#
$WorkDirectory /var/spool/rsyslog

#
# Include all config files in /etc/rsyslog.d/
#
$IncludeConfig /etc/rsyslog.d/*.conf

*.*@192.168.1.210:514
rec0nrat@demoserver1:/etc$
```

The rsyslog service must now be restarted for the changes to take effect.

```
rec0nrat@demoserver1:/etc$ sudo systemctl restart rsyslog.service
rec0nrat@demoserver1:/etc$
```

Task #2 - TCPdump

1. Using 'tcpdump', detect syslog traffic by running the following command:
   - `sudo tcpdump -i any udp port 514 -w syslog_traffic.pcap`
   - The command inspects for udp traffic, over any interface, on port 514 and writes the output to a .pcap file.

```
rec0nrat@demoserver1:~/RA-logs/Syslog$  sudo tcpdump -i any udp port 514 -w syslog_traffic.pcap
tcpdump: data link type LINUX_SLL2
tcpdump: listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes




^C3 packets captured
7 packets received by filter
0 packets dropped by kernel
rec0nrat@demoserver1:~/RA-logs/Syslog$
```

In order to read the .pcap file 'tcpdump -r <file>' must be used.

```
rec0nrat@demoserver1:~/RA-logs/Syslog$ ls
syslog_traffic.pcap
rec0nrat@demoserver1:~/RA-logs/Syslog$ sudo tcpdump -r syslog_traffic.pcap
reading from file syslog_traffic.pcap, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144
Warning: interface names might be incorrect
21:45:35.717380 lo    In  IP demoserver1.35423 > demoserver1.syslog: SYSLOG authpriv.info, length: 127
21:45:35.722244 lo    In  IP demoserver1.35423 > demoserver1.syslog: SYSLOG auth.info, length: 85
21:45:35.722258 lo    In  IP demoserver1.35423 > demoserver1.syslog: SYSLOG daemon.info, length: 80
rec0nrat@demoserver1:~/RA-logs/Syslog$
```