

**Name: Mosab Fathy Ramadan Mohamed**

**Group: B20-SD-01**

### **Lab 9: Logging and auditing**

1. What security monitoring tool will you forward your system logs to for security event detection? Give reasons for your choice.

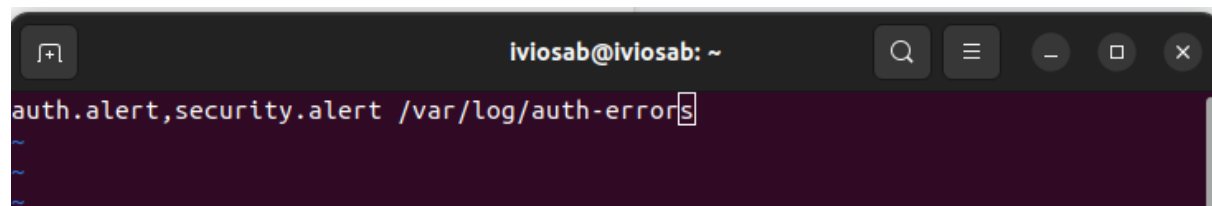
**Answer:**

Rsyslog: is an open-source software utility used on UNIX and Unix-like computer systems for forwarding log messages in an IP network. It implements the basic syslog protocol, extends it with content-based filtering, rich filtering capabilities, queued operations to handle offline outputs support for different module outputs, flexible configuration options and adds features such as using TCP for transport.

2. Configure rsyslogd by adding a rule to the newly created configuration file `/etc/rsyslog.d/auth-errors.conf` to log all security and authentication messages with the priority alert and higher to the `/var/log/auth-errors` file. Test the newly added log directive with the logger command. Verify it from rsyslog and journald perspectives by filtering the output.

**Answer:**

```
ivosab@ivosab:~$ sudo vim /etc/rsyslog.d/auth-errors.conf
```



```
ivosab@ivosab:~$ systemctl restart rsyslog
```

```
ivosab@ivosab:~$ logger -p auth.alert "Some test"
```

```
ivosab@ivosab:~$ sudo cat /var/log/auth-errors
```

Nov 6 20:38:28 ivosab ivosab: Some test

```

ivosab@ivosab:~$ journalctl -p alert
сен 29 18:13:27 ivosab kernel: BUG: kernel NULL pointer dereference, address:
сен 29 18:13:27 ivosab kernel: #PF: supervisor read access in kernel mode
сен 29 18:13:27 ivosab kernel: #PF: error_code(0x0000) - not-present page
-- Boot 13bd249b780e4573a31c7cb605072590 --
окт 09 03:18:27 ivosab kernel: watchdog: BUG: soft lockup - CPU#1 stuck for 22
-- Boot cd2296f2527544f4a5aea030901cec01 --
окт 21 01:56:23 ivosab kernel: BUG: kernel NULL pointer dereference, address:
окт 21 01:56:23 ivosab kernel: #PF: supervisor read access in kernel mode
окт 21 01:56:23 ivosab kernel: #PF: error_code(0x0000) - not-present page
-- Boot fd79d02b29e14a6690722ccbd562c4ea --
окт 30 13:08:25 ivosab sudo[429398]: ivosab : 2 incorrect password attempts
окт 30 18:23:13 ivosab sudo[458082]: ivosab : 2 incorrect password attempts
-- Boot 0d3b9acde5604bc6a704f4cceed2b114 --
ноя 06 20:38:28 ivosab ivosab[483282]: Some test
lines 1-14/14 (END)

```

```

ivosab@ivosab:~$ cat /var/log/auth.log | grep "Some test"
Nov 6 20:38:28 ivosab ivosab: Some test
ivosab@ivosab:~$

```

3. Install Apache web server and configure log rotate to rotate its web access log every six hours. Compress the rotated log files, and ensure that log rotate restarts the web server after rotating the logs. Manually execute the logrotate utility to test your configuration and show results.

### Answer:

```

ivosab@ivosab:~$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor prese
   Active: active (running) since Sun 2022-11-06 21:02:57 MSK; 10s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 487834 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/
 Main PID: 487838 (apache2)
    Tasks: 55 (limit: 19006)
   Memory: 5.0M
      CPU: 14ms
   CGroup: /system.slice/apache2.service
           └─487838 /usr/sbin/apache2 -k start
             └─487839 /usr/sbin/apache2 -k start
               └─487840 /usr/sbin/apache2 -k start

ноя 06 21:02:57 ivosab systemd[1]: Starting The Apache HTTP Server...
ноя 06 21:02:57 ivosab apachectl[487837]: AH00558: apache2: Could not reliably
ноя 06 21:02:57 ivosab systemd[1]: Started The Apache HTTP Server.
ivosab@ivosab:~$

ivosab@ivosab:~$ sudo mkdir /etc/mosab-logrotate.d
ivosab@ivosab:~$ sudo vim /etc/mosab-logrotate.d/mosab-web-rotate.conf

```

```

/var/log/apache2/access.log f
    daily
    missingok
    rotate 14
    compress
    delaycompress
    notifempty
    create 640 root adm
    sharedscripts
    prerotate
if [ -d /etc/logrotate.d/httpd-prerotate ]; then
    run-parts /etc/logrotate.d/httpd-prerotate
fi
endscript
postrotate
if pgrep -f ^/usr/sbin/apache2 > /dev/null; then
    invoke-rc.d apache2 reload 2>&1 | logger -t apache2.logrotate
fi
endscript

```

```

ivosab@ivosab:~$ sudo chmod 644 /etc/mosab-logrotate.d/mosab-web-rotate.conf

```

```

GNU nano 6.2 /tmp/crontab.zQ0usD/crontab *
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow   command
30 */6 * * * root logrotate -f /etc/mosab-logrotate.d/mosab-web-rotate.conf

```

```

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location

```

```

ivosab@ivosab:~$ cat /var/log/apache2/access.log
::1 - - [06/Nov/2022:21:09:10 +0300] "GET / HTTP/1.1" 200 3460 "-" "Mozilla/5.0
(X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safa
ri/537.36"
::1 - - [06/Nov/2022:21:09:10 +0300] "GET /icons/ubuntu-logo.png HTTP/1.1" 200 3
607 "http://localhost/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHT
ML, like Gecko) Chrome/106.0.0.0 Safari/537.36"
::1 - - [06/Nov/2022:21:09:11 +0300] "GET /favicon.ico HTTP/1.1" 404 487 "http:/
/localhost/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Ge
cko) Chrome/106.0.0.0 Safari/537.36"
ivosab@ivosab:~$ sudo logrotate -f /etc/mosab-logrotate.d/mosab-web-rotate.conf
ivosab@ivosab:~$ cat /var/log/apache2/access.log
ivosab@ivosab:~$

```

4. Create a bash script that continuously monitors the `/var/log/auth.log` file and triggers an alarm if there are three or more "authentication failure" in 30 seconds. The text `Three or more authentication failure in 30 seconds` should be appended to a log file `/var/log/alarm.log` everytime the alarm is triggered. Show test use case and results.

**Answer:**

```

#!/bin/bash
if [ "$EUID" -ne 0 ]
then echo "Please run as root"
exit
fi

REGEX="^([ a-zA-Z0-9]+[0-9][0-9]:[0-9][0-9]:[0-9][0-9]).*authentication failure.*"

buffer=()
tail -n0 -f /var/log/auth.log | while read -r line; do
# echo "$line"
if [[ $line =~ $REGEX ]]; then
buffer+=("${BASH_REMATCH[1]}")
# echo "${buffer[@]}"
if [[ "${#buffer[@]}" -ge 3 ]]; then
difference=$(( $(date -d "${buffer[2]}" +%s) - $(date -d "${buffer[0]}" +%s) ))
if [[ $difference -le 30 ]]; then
echo "Three or more authentication failure in 30 seconds" >> /var/log/alar
m.log
# echo "Three or more authentication failure in 30 seconds"
fi
# echo "${buffer[@]}"
buffer=("${buffer[@]:1}")
fi
fi
done
~

```

```

ivosab@ivosab:~$ cd /
ivosab@ivosab:/$ sudo bash script.sh
[sudo] password for ivosab:

```

```
ivosab@ivosab:/$ su
Password:
su: Authentication failure
ivosab@ivosab:/$ su
Password:
su: Authentication failure
ivosab@ivosab:/$
ivosab@ivosab:/$ su
Password:
su: Authentication failure
ivosab@ivosab:/$
```

```
ivosab@ivosab:/$ cat /var/log/audit.log
Three or more authentication failure in 30 seconds
Three or more authentication failure in 30 seconds
ivosab@ivosab:/$
```

5. How can you log all commands executed by every user on Linux systems. What utility will you use for this. Show how you configure this tool, and show the logs generated.

**Answer:**

```
ivosab@ivosab:~$ sudo vim /etc/rsyslog.d/bash.conf
```

```
ivosab@ivosab: ~
local7.* /var/log/commands.log
```

```
ivosab@ivosab:~$ sudo vim /etc/bashrc
ivosab@ivosab:~$
```

```
ivosab@ivosab: ~
export PROMPT_COMMAND='RETRN_VAL=$?;logger -p local7.debug "$(whoami) [$$]: $(history 1 | sed "s/^ [ ]*[0-9]\+[ ]*//" )"'
```

```
logger: unknown facility name: local
ivosab@ivosab:~$ source /etc/bashrc
ivosab@ivosab:~$
```

```
ivosab@ivosab:~$ sudo vim /etc/logrotate.d/syslog
ivosab@ivosab:~$
```

```
ivosab@ivosab: ~
/var/log/commands.log
```

```
ivosab@ivosab:~$ systemctl restart rsyslog
ivosab@ivosab:~$
```

```

ivosab@ivosab:~$ cat /var/log/commands.log
Nov  6 21:18:52 ivosab ivosab: ivosab [485470]: systemctl restart rsyslog
ivosab@ivosab:~$ cat /var/log/commands.log
Nov  6 21:18:52 ivosab ivosab: ivosab [485470]: systemctl restart rsyslog
Nov  6 21:19:26 ivosab ivosab: ivosab [485470]: cat /var/log/commands.log
ivosab@ivosab:~$ cat /var/log/commands.log
Nov  6 21:18:52 ivosab ivosab: ivosab [485470]: systemctl restart rsyslog
Nov  6 21:19:26 ivosab ivosab: ivosab [485470]: cat /var/log/commands.log
ivosab@ivosab:~$

```

6. Set up a centralized journald logging server `systemd-journal-remote`. Configure another machine as a client to forward its journal to the logging server.
  - Test your setup by running the `logger` utility on the client system and show the logs generated on the logging server.

### Answer:

```

ivosab@ivosab:~$ sudo apt install systemd-journal-remote

```

### Server:

```

ivosab@ivosab:~$ sudo systemctl enable systemd-journal-remote.socket
Created symlink /etc/systemd/system/sockets.target.wants/systemd-journal-remote.socket → /lib/systemd/system/systemd-journal-remote.socket.
ivosab@ivosab:~$ cp /lib/systemd/system/systemd-journal-remote.service /etc/systemd/system/
cp: Permission denied
ivosab@ivosab:~$ sudo cp /lib/systemd/system/systemd-journal-remote.service /etc/systemd/system/
ivosab@ivosab:~$
ivosab@ivosab:~$ sudo nano /etc/systemd/system/systemd-journal-remote.service
# change https to http
ivosab@ivosab:~$

```

```
iviosab@iviosab: ~  
GNU nano 6.2 /etc/systemd/system/systemd-journal-remote.service *  
# SPDX-License-Identifier: LGPL-2.1-or-later  
#  
# This file is part of systemd.  
#  
# systemd is free software; you can redistribute it and/or modify it  
# under the terms of the GNU Lesser General Public License as published by  
# the Free Software Foundation; either version 2.1 of the License, or  
# (at your option) any later version.  
  
[Unit]  
Description=Journal Remote Sink Service  
Documentation=man:systemd-journal-remote(8) man:journal-remote.conf(5)  
Requires=systemd-journal-remote.socket  
  
[Service]  
ExecStart=/lib/systemd/systemd-journal-remote --listen-http=3 --output=/var/lo  
LockPersonality=yes  
LogsDirectory=journal/remote  
MemoryDenyWriteExecute=yes  
NoNewPrivileges=yes  
  
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location  
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line  
# change https to http  
iviosab@iviosab:~$ sudo systemctl daemon-reload  
iviosab@iviosab:~$
```

Didn't have enough time please give me partial points