**QRADAR STEPS FOR OUR SCAP NODE**

* Determine the type of your Linux distribution ,our nodes have rsyslog configuration so below steps needs to be followed
* For redhat linux distribution alone these installation needs to be followed

1. yum install audit
2. service auditd start
3. chkconfig auditd on

create a file in this path /etc/audit/plugins.d/syslog.conf: and add these following lines

active = yes

direction = out

path = builtin\_syslog

type = builtin

args = LOG\_LOCAL6

format = string

Then restart the services:

• service auditd restart

• service syslog restart

in your /etc/rsyslog.conf conf file, you will need to add at the end of the file:

local6.\* @@<qradar\_collector\_ip\_address>

where <qradar\_collector\_ip\_address> is the IP of one of the IBM QRadar SIEM collectors per datacenter in the list of task 1

* For rsyslog, configure inside your /etc/rsyslog.conf as follows:

authpriv.\*;auth.\* action(type="omfwd" target="<qradar\_collector\_ip\_address>" port="514" protocol="tcp")

where <qradar\_collector\_ip\_address> is the IP of one of the IBM QRadar SIEM collectors per datacenter in the list of task 1

Then restart the service:

service rsyslog restart

* Our scap nodes have firewalld as the local firewall, by default logging is disabled, you can enable it by

sudo firewall-cmd --set-log-denied=all

Create a file called /etc/rsyslog.d/firewalld-dropped.conf

Add the configuration to pick up the drop and reject events from the message queue like the

following example:

:msg,contains,"\_DROP" /var/log/firewalld-dropped.log

:msg,contains,"\_REJECT" /var/log/firewalld-dropped.log

& stop

Ensure that the syslog binary configuration of your choice is configured to send the

facility/category of the newly created file towards the syslog destination defined in the

previous steps.

* We can debug the errors inside /var/log/messages file and also a log called firewalld\_dropped file should also be created
* We can confirm the configuration by checking if we have any error logs in /var/log/messages and go to Qradar team to confirm that they are getting the logs