**Student Name**: Dustin McClure

**Lab Name**: Legitimate Logging Logistics

I wanted to note here that none of the checks in this lab passed, but I am fairly certain that I configured everything to spec. Nearly two hours into the lab when I had the log server configured, all machines were successfully sending in their logs to this server, and all logs were exporting to desktop folders I noticed that the checks showed a last changed time of 7:03 PM (nearly 2 hours prior to the time of the screenshot). Screenshot included below:

Graphical user interface, application

Description automatically generated

**Documentation of Steps:** including commands used, config files edited, URL…

**Firewall**: <https://www.manageengine.com/products/firewall/help/configure-pfsense-firewalls.html>

It was pretty straightforward to configure the firewall to send logs to the remote syslog server on Domain-Controller.

Graphical user interface, text, application, email

Description automatically generated

I signed into the pfsense webconfigurator console at 172.16.30.250, enabled remote logging under **Status 🡪 System Logs 🡪 Settings**. After this was enabled, I set the source address to the production network, entered the log server address of 172.16.30.55:514, and made sure the only logs sent to the syslog server were System Events and Firewall Events.

**Fileshare**: <https://community.malforensics.com/t/how-to-configure-ubuntu-to-send-messages-to-a-remote-syslog-server/199>

It was also pretty simple to figure out sending syslog events from the Debian based systems.

I simply edited ***/etc/rsyslog.conf*** to include the following line, and then restarted the rsyslog service(***sudo service rsyslog restart***):

**\*.\* action(type="omfwd" target="172.16.30.55" port="514" protocol="udp" action.resumeRetryCount="100" queue.type="linkedList" queue.size="10000")**

**Domain-Controller**(Syslog Watcher and Eventlog Inspector):

Graphical user interface, application

Description automatically generatedA screenshot of a phone

Description automatically generated with medium confidenceGraphical user interface, text, application

Description automatically generated

Graphical user interface, application, table, Excel

Description automatically generatedOnce installing Syslog Watcher on the Domain Controller machine, it was pretty easy to get everything set up. I made sure to bind the service to the Domain Controller’s IPv4/IPv6 LAN ips(**Settings 🡪 Networking**), I set an export directory for log exports (**Settings 🡪 --Destination**), configured criteria for the export folder/export file format so that both were named after the source ip of the logs(**Settings 🡪 --Destination**), ensured that logs were encoded using utf-8 and exported in csv format(**Settings 🡪 --Destination**), and made sure that log levels info and above from all sources were exported to these logs(**Settings 🡪 -Export to Files**).

Graphical user interface

Description automatically generated

After configuring Syslog Watcher, I installed and configured Eventlog Inspector. I configured it to forward events to the log server (**Settings 🡪 Syslog**), to forward only events that were info level and above(**Settings 🡪 Syslog 🡪 Forwarding**).

**prod-joomla**: <https://community.malforensics.com/t/how-to-configure-ubuntu-to-send-messages-to-a-remote-syslog-server/199>

Text

Description automatically generatedIt was also pretty simple to figure out sending syslog events from the Debian based systems.

I simply edited ***/etc/rsyslog.conf*** to include the following line, and then restarted the rsyslog service(***sudo service rsyslog restart***):

**\*.\* action(type="omfwd" target="172.16.30.55" port="514" protocol="udp" action.resumeRetryCount="100" queue.type="linkedList" queue.size="10000")**

**Database**:

Graphical user interface

Description automatically generatedI installed and configured Eventlog Inspector. I configured it to forward events to the log server (**Settings 🡪 Syslog**), to forward only events that were info level and above(**Settings 🡪 Syslog 🡪 Forwarding**).

**What I Learned:**

In doing this lab, I learned how to do a couple of things that I had not previously done.

First, I learned how to configure the log server itself(Syslog Watcher). Installing it was a simple (double) click of the desktop icon. When I first launched Syslog Watcher I found the interface to be intuitive and the settings easy to locate and understand. Knowing that I would need the server to be reachable across the network by multiple systems, I headed to the network settings where I learned you could set the service up locally or bind it to an IP address and port so that it is available to remote machines needing to send their logs in. After figuring out networking to make the server available, I navigated to the export and destination sections. Here I learned how to format the subfolder name and file name using syslog variables so that both took on the name of the source IP from which the log originated. I also learned how to filter syslog exports by log level and log source using filter criteria.

Additionally, I learned how both Windows and Linux based systems handle sending their logs in to a centralized log server. With the Windows systems it was as easy as installing Eventlog Inspector, entering in the remote server’s IP address and log server port, and specifying which types of log events should be forwarded. I learned how to do all of these things simply by looking through Eventlog Inspector’s settings.

While configuring syslog forwarding for the Linux systems was still easy, it was a little more difficult to figure out than Windows. Initially I just edited rsyslog.conf to include ***\*.\* @@172.16.30.55*** at the top, but this didn’t work. After a little research, I learned that you have to enter an action line with configuration parameters in rsyslog.conf *(How to configure ubuntu to send messages to a remote syslog server, 2019)*. This action line includes the action type, target (syslog server ip), port(syslog server port), protocol(udp or tcp), and other parameters to fine tune the log forwarding process.

# References

*How to configure ubuntu to send messages to a remote syslog server*. (2019, February 6). Retrieved from Cyber Security Community: https://community.malforensics.com/t/how-to-configure-ubuntu-to-send-messages-to-a-remote-syslog-server/199