System Logging Protocol

In this exercise, you will learn to setup a syslog client in Ubuntu environment. Also, you will be inspecting syslog packets to explore their content and relate these to the protocol specifications defined in the syslog RFC.

I. Setting-up the syslog client in Ubuntu

* 1. Before starting up the Ubuntu virtual machine using VMWare, configure the network settings of the Ubuntu VM.
     1. Go to settings (right click the Ubuntu VM tab) 🡪 Network Adapter
     2. Network Connection 🡪 select ‘**Bridged: Connected directly to the physical network’**. Click OK.
  2. Run the Ubuntu VM.
  3. Normally, rsyslog is installed by default on a freshly installed Ubuntu 20.04.
     1. Check the status of the rsyslog by entering the following command:

|  |
| --- |
| # sudo service rsyslog status |

If the status isn’t active, you can always start it by running:

|  |
| --- |
| # sudo service rsyslog start |

1. If the status isn’t active, you can always start it by running: After the installation, do the steps in #3a and #3b.

|  |
| --- |
| # sudo apt-get update  # sudo apt-get install rsyslog |

* 1. Now, we need to edit the syslog configuration file. Enter the following command.

|  |
| --- |
| # sudo nano /etc/rsyslog.conf |

* 1. We need to configure the syslog server IP address. In this case, you need to enter your assigned IP address in your Host’s OS (not vm). Add a line before the Module section. Enter the following command. (See Fig. 1)

|  |
| --- |
| \*.\* @OS IP ADDRESS:514 |

* 1. Please remove the comment symbol (#) for the following lines: (See figure 1)

|  |
| --- |
| module(load="imudp") input(type="imudp" port="514") module(load="imtcp") input(type="imtcp" port="514") |

* 1. To save the configuration file, press “CTRL+X”, then type ‘Y’.
  2. We need to edit the firewall rules. Enter the following commands:

|  |
| --- |
| # sudo ufw allow 514/tcp  # sudo ufw allow 514/udp |

* 1. Lastly, restart the syslog service.

|  |
| --- |
| # sudo service rsyslog restart |

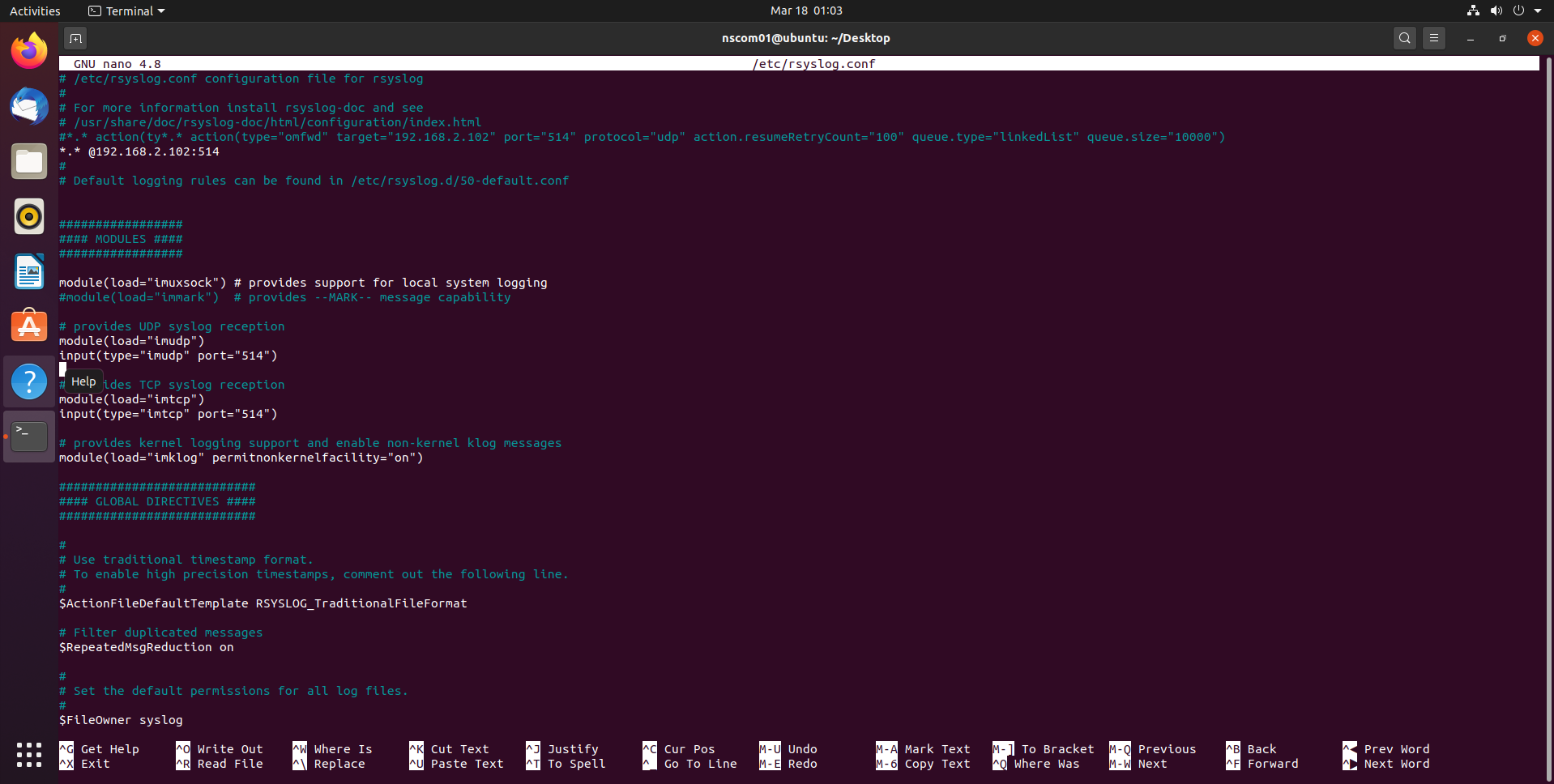
1. 

Figure 1: rsyslog.conf

II. Installing the tftpd64

* 1. Install the tftpd64, by downloading [here](https://bitbucket.org/phjounin/tftpd64/downloads/Tftpd64-4.64-setup.exe)
  2. After installing, run the application as administrator.
  3. Go to settings 🡪 GLOBAL, uncheck everything except Syslog Server
  4. Go to settings 🡪 SYSLOG, check Save syslog messages to file syslog.txt
  5. Then, restart the application.

III. Capturing the syslog packets

* 1. First, confirm connection from the Ubuntu VM to Host’s OS IP address, by sending four (4) ICMP messages. Attach a screenshot. **[1pt]**

|  |
| --- |
| # ping -c 4 xxx.xxx.xxx.xxx |
| Screenshot |

* 1. Go back to tftpd application. Click “Clear” buttong. Set the server interface to your host’s OS IP address by selecting from the drop-down menu then click on the syslog tab.
  2. Also, run the Wireshark application on the OS, setting the capture interface to your Ethernet Connection. Apply a filter by using the string ‘syslog’
  3. On the Ubuntu VM, do the following actions by checking messages logged in TFTPd:

Logout from the Ubuntu VM. Click the power button on the upper right side of the desktop. See the results in the tftpd64 application. Answer the following questions:

What is the most common priority # in the results? **[1 pt]**

|  |
| --- |
|  |

Attach a screenshot of the tftpd syslog results below. **[3pts]**

|  |
| --- |
| Screenshot |

Select a syslog entry and fill the information below.[**3pts**]

|  |  |
| --- | --- |
| Facility (Value and Interpretation) |  |
| Severity (Value and Interpretation) |  |
| Date and Time |  |
| Host |  |
| Source Process |  |

Your Ubuntu VM is currently logged out. Click your profile (do not enter password yet). Get the details of the second message generated. Attach a screenshot of the tftpd syslog results.**[3pts]**

|  |  |
| --- | --- |
| Facility (Value and Interpretation) |  |
| Severity (Value and Interpretation) |  |
| Date and Time |  |
| Host |  |
| Source Process |  |

|  |
| --- |
| Screenshot |

Log-in to your Ubuntu VM by entering password. Open a terminal and go back to tftpd, click ‘Clear’. Restart the syslog service (sudo service rsyslog restart). Get the details of the 3rd and 4th messages generated. [**6pts**]

|  |  |
| --- | --- |
| Facility (Value and Interpretation) |  |
| Severity (Value and Interpretation) |  |
| Date and Time |  |
| Host |  |
| Source Process |  |

|  |  |
| --- | --- |
| Facility (Value and Interpretation) |  |
| Severity (Value and Interpretation) |  |
| Date and Time |  |
| Host |  |
| Source Process |  |

Why do you think is it essential to include a priority field containing the facility and severity codes? [**1pt**]

|  |
| --- |
|  |

* 1. Stop the packet capture on Wireshark



* 1. Expand the network layer details of syslog packets captured and inspect contents

Based on the source and destination addresses of the packets, which host serves as syslog originator and which host serves as syslog collector? [**1pt**]

|  |
| --- |
|  |

* 1. Expand transport layer details of syslog packets captured.

What transport protocol and port number used to transfer syslog packets? [**1pt**]

|  |
| --- |
|  |

Are any of these packets acknowledged by the collector? [**1pt**]

|  |
| --- |
|  |

* 1. Inspect the raw data of the packets by looking at the Hex dump on the bottom most window pane of Wireshark.

Can you easily read the message content of syslog messages? [**1pt**]

|  |
| --- |
|  |

What does this imply in terms of security for the syslog protocol? [**1pt**]

|  |
| --- |
| . |

* 1. **Upload the generated syslog.txt with this document.** [**2pts**]