Project: System-to-System Log Forwarding using Rsyslog on Ubuntu

🚱 💻 By: Afroz Shaikh

Email: afrozshaikh8086@gmail.com

Overview

This project demonstrates how to configure **log forwarding** from one Ubuntu system to another using **rsyslog**. This technique is commonly used in **SOC environments**, **log management systems**, and **SIEM platforms** to centralize and monitor logs from multiple sources.

Prerequisites

- Ubuntu OS installed on both systems.
- rsyslog service enabled (default on most Ubuntu installs).
- Network connectivity between the source and destination systems.
- Root or sudo access.

Step-by-Step Configuration

1. Launch Terminal

Start by opening the terminal on your Ubuntu system.

2. Navigate to Configuration Directory

*Run the following command to go to the /etc directory:

```
splunk123@hackerzone:/etc$ cd /etc
```

This folder contains system-wide configuration files, including those for rsyslog.

3. Locate rsyslog Configuration

Use 1s to verify the presence of the configuration files:

```
splunk123@hackerzone: /etc
 plunk123@hackerzone:/etc$ cd
plunk123@hackerzone:/etc$ ls
  uduser.conf cryptsetup-initramfs gshadow-
lternatives crypttab gss
parmor dbus-1
                                                                                                locale.alias
                                                                     gss
hdparm.conf
host.conf
hostname
                                   dbus-1
debconf.conf
debian_version
                                                                                                localtime
                                                                      hosts
                                                                      hosts.allow
hosts.deny
                                                                                                login.defs
logrotate.conf
  indresvport.blacklist dhcpcd.conf
                                                                                                                        nsswitch.conf
oinkmaster.conf
                                                                                                lsb-release
                                                                                               lvm
machine-id
magic
magic.mime
                                                                                                                                                                                                             usb_modeswitch
vconsole.conf
                                                                                                                        opt
os-release
                                                                                               magic.mime overlayroot.conf
manpath.config PackageKit
mdadm pam.conf
  a-certificates.conf
                                   ethertypes
                                                                      issue.net
kernel
landscape
                                                                                                                                                                              sudoers.d
sudo_logsrvd.conf
                                                                                                                                                         resolv.conf
                                                                                                mdadm
mime.types
                                   fwupd
gai.conf
gnutls
groff
                                                                                                                                                         rsyslog.conf
                                                                                                                                                                                sysctl.conf
sysctl.d
sysstat
                                                                      ld.so.cache
ld.so.conf
ld.so.conf.d
legal
                                                                                                                                                                                                             zsh command not found
                                                                      libaudit.conf
                                                                                                mtab
                                                                                                                                                         sensors3.conf terminfo
                                                                                                multipath polkit-1
multipath.conf pollinate
 plunk123@hackerzone:/etc$
```

Look for:

- o rsyslog.conf
- o rsyslog.d/ directory

4. Edit the rsyslog Configuration

Open the config file with elevated privileges:

```
sudo nano /etc/rsyslog.conf

Add the following line at the end of the file:

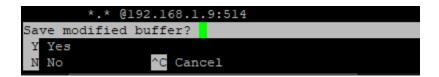
*.* @192.168.1.9:514

o *.* → forward all logs from all facilities and severity levels
o @ → indicates use of UDP (use @@ for TCP)
o 192.168.1.9:514 → destination IP and port of the log collector
```

```
splunk123@hackerzone: /etc
                                                                             /etc/rsyslog.conf *
 #module(load="immark") # provides --MARK-- message capability
# provides UDP syslog reception
#module(load="imudp")
#input(type="imudp" port="514")
# provides TCP syslog reception
#module(load="imtcp")
#input(type="imtcp" port="514")
# provides kernel logging support and enable non-kernel klog messages
module(load="imklog" permitnonkernelfacility="on")
*********************
#### GLOBAL DIRECTIVES ####
**********************
# Filter duplicated messages
$RepeatedMsgReduction on
# Set the default permissions for all log files.
$FileOwner syslog
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022
$PrivDropToUser syslog
$PrivDropToGroup syslog
# Where to place spool and state files
$WorkDirectory /var/spool/rsyslog
Include all config files in /etc/rsyslog.d/
$IncludeConfig /etc/rsyslog.d/*.conf
        *.* @192.168.1.9:514
```

5. Save and Exit

- o Press Ctrl + X
- Press y to confirm
- o Hit Enter to save



6. Restart rsyslog Service

sudo systemctl restart rsyslog

```
splunk123@hackerzone:/etc$ sudo nano /etc/rsyslog.conf
[sudo] password for splunk123:
splunk123@hackerzone:/etc$ sudo ./splunk restart rsyslog
```

Output

Now, logs from your system will be **forwarded in real time** to the destination system or SIEM platform for centralized analysis and monitoring.

- Ensure that port 514 is open on the destination.
- Use firewall-cmd or ufw to allow traffic if needed.
- Recommended: monitor /var/log/syslog to verify forwarding is working.

■ Use Cases

- Security Operations Centers (SOC)
- SIEM integration
- Lab-based log collection projects
- Centralized log monitoring