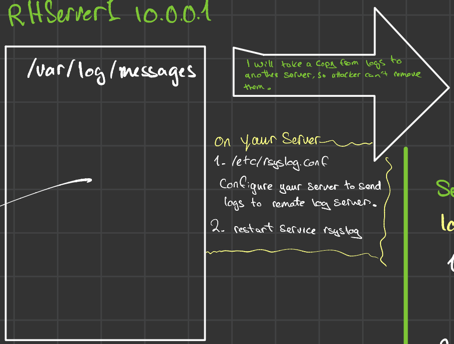
Our topic today : 1. Rsyslog (Remote system logs)
2- Archive and compress files

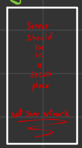
1- Rsyslog (Remote system logs)

/var/log/messages
tail -f /var/log/messages → read
journalctl → read all events & logs
journalctl -since yyyy-mm-dd → read logs since certain date
journalctl -b → read logs since system boot

RHServer1 10.0.0.1



RHServer3
10.0.0.3
Log Server



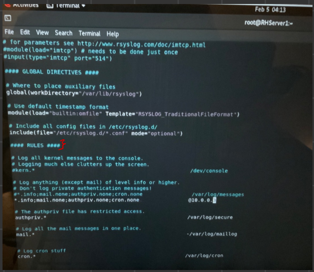
Attack
Hacked the system

In logs will be all actions saved.
attacker can delete logs easily.

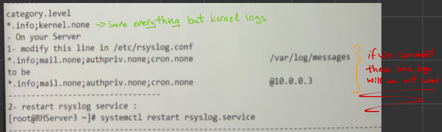
Service rsyslog enabled started

log Server Configuration:

1. firewall configuration
   ↳ allow rsyslog port (514 tcp/udp) or close it.
2. Configure rsyslog Service to recieve logs
   ↳ allow server to recieve logs by the configuration file /etc/rsyslog.conf
3. restart service rsyslog



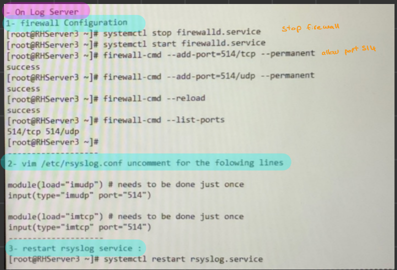
```
Activities   Terminal ▾                                   Feb 5 04:13
                                                    root@RHServer1:~
File  Edit  View  Search  Terminal  Help
# for parameters see http://www.rsyslog.com/doc/imtcp.html
#module(load="imtcp") # needs to be done just once
#input(type="imtcp" port="514")

#### GLOBAL DIRECTIVES ####

# Where to place auxiliary files
global(workDirectory="/var/lib/rsyslog")

# Use default timestamp format
module(load="builtin:omfile" Template="RSYSLOG_TraditionalFileFormat")

# Include all config files in /etc/rsyslog.d/
include(file="/etc/rsyslog.d/*.conf" mode="optional")

#### RULES ####

# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*                                                 /dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
#*.info;mail.none;authpriv.none;cron.none               /var/log/messages
*.info;mail.none;authpriv.none;cron.none                @10.0.0.3

# The authpriv file has restricted access.
authpriv.*                                              /var/log/secure

# Log all the mail messages in one place.
mail.*                                                  -/var/log/maillog

# Log cron stuff
cron.*                                                  /var/log/cron
```



```
category.level
*.info;kernel.none
- On your Server
1- modify this line in /etc/rsyslog.conf
*.info;mail.none;authpriv.none;cron.none          /var/log/messages
to be
*.info;mail.none;authpriv.none;cron.none          @10.0.0.3
--------------------------------
2- restart rsyslog service :
[root@RHServer3 ~]# systemctl restart rsyslog.service
```


A small problem is that all logs are saved in one file at /etc/log/messages

> grep Server_name /etc/log/messages
> grep Server_name /etc/log/messages > /root/server1.log



```
- On Log Server
1- firewall Configuration
[root@RHServer3 ~]# systemctl stop firewalld.service
[root@RHServer3 ~]# systemctl start firewalld.service
[root@RHServer3 ~]# firewall-cmd --add-port=514/tcp --permanent
success
[root@RHServer3 ~]# firewall-cmd --add-port=514/udp --permanent
success
[root@RHServer3 ~]# firewall-cmd --reload
success
[root@RHServer3 ~]# firewall-cmd --list-ports
514/tcp 514/udp
[root@RHServer3 ~]#
--------------------
2- vim /etc/rsyslog.conf uncomment for the folowing lines

module(load="imudp") # needs to be done just once
input(type="imudp" port="514")

module(load="imtcp") # needs to be done just once
input(type="imtcp" port="514")
--------------------
3- restart rsyslog service :
[root@RHServer3 ~]# systemctl restart rsyslog.service
```


→ systemctl stop firewall.service → stop firewall (bullshit)
→ firewall-cmd --add-port=514/tcp --permanent → allow certain ports
→ firewall-cmd --add-port=514/udp --permanent → " " "
→ firewall-cmd --reload
→ firewall-cmd --list-port

Note : if you want to save logs of specific level do following:

1. go to /etc/rsyslog.conf
2. make a new rule → (example) *.error /var/log/msg.errors
3. Save + restart service

2- Archive and compress Files

Archive	→ for Backup (copy of the file)	tar
Compress	→ for saving space (replace the file)	gzip , bzip2
Archive + Compress	→ both like winrar	zip

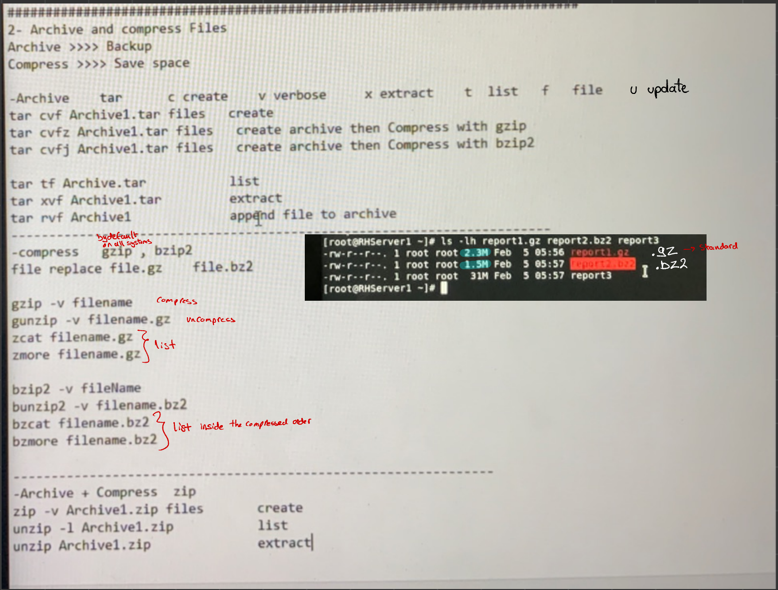
Archive f1, f2, f3 Backup in Archive1.tar

Compress f1 , f2 , f3 (1GB) replace in files.gz (500MB)

```
> ls -l -R /  > report1
> cp report1 report2
> cp report1 report3
> ls -lh report*
```

gzip is standard in any distribute

zcat / zmore } to read content of zip



```
##########################################################################
2- Archive and compress Files
Archive >>>> Backup
Compress >>>> Save space

-Archive    tar    c create    v verbose    x extract    t list    f file    u update
tar cvf Archive1.tar files    create
tar cvfz Archive1.tar files    create archive then Compress with gzip
tar cvfj Archive1.tar files    create archive then Compress with bzip2

tar tf Archive.tar            list
tar xvf Archive1.tar          extract
tar rvf Archive1              append file to archive
----------------------------------------------------------------------
-compress    gzip , bzip2     (bydefault on all systems)
file replace file.gz    file.bz2

gzip -v filename              compress
gunzip -v filename.gz         uncompress
zcat filename.gz   } list
zmore filename.gz  }

bzip2 -v fileName
bunzip2 -v filename.bz2
bzcat filename.bz2   } list inside the compressed order
bzmore filename.bz2  }

----------------------------------------------------------------------
-Archive + Compress  zip
zip -v Archive1.zip files       create
unzip -l Archive1.zip           list
unzip Archive1.zip              extract
```

```
[root@RHServer1 ~]# ls -lh report1.gz report2.bz2 report3
-rw-r--r--. 1 root root 2.3M Feb  5 05:56 report1.gz
-rw-r--r--. 1 root root 1.5M Feb  5 05:57 report2.bz2
-rw-r--r--. 1 root root  31M Feb  5 05:57 report3
[root@RHServer1 ~]#
```

.gz → standard
.bz2

Sudo = Super User do

→ in group user file at /etc/group

in the file you will find a group Wheel in redhat
Sudoers in another distribution

⇒ So if I added someone in this group, he can run commands as root

You can also go to file /etc/sudoers and add