



МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«МИРЭА –Российский технологический университет»

РТУ МИРЭА

Институт кибербезопасности и цифровых технологий

Кафедра КБ-4 «Интеллектуальные системы информационной безопасности»

Дисциплина «Технологии обеспечения информационной безопасности»

Отчет

о проделанной практической работе №5

Выполнил студент 1 курса

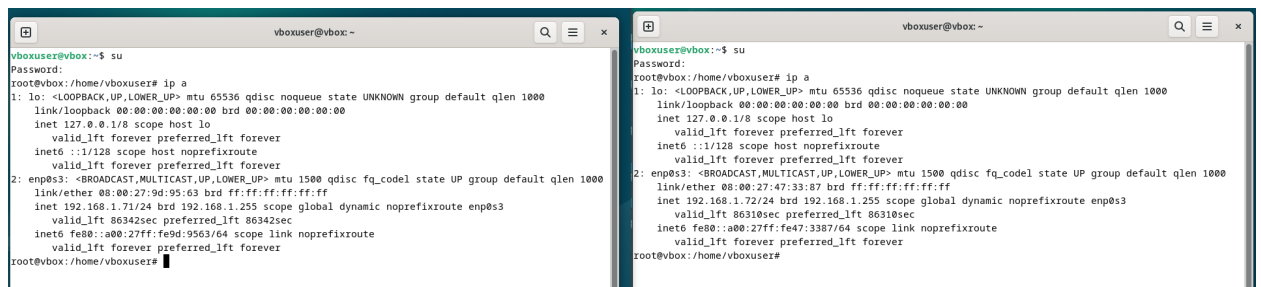
Группы: ББМО-02-24

Овечкин Александр Романович

Москва

2024

Созданы две машины с дебиан 12, на каждой включен сетевой мост Deb1(192.168.1.71)
Deb2(192.168.1.72)



The image shows two terminal windows side-by-side. The left window is for Deb1 (192.168.1.71) and the right window is for Deb2 (192.168.1.72). Both windows show the output of the 'ip a' command, displaying network interfaces and their configurations. In Deb1, the interface 'lo' is configured with IP 127.0.0.1 and 'enp8s3' is configured with IP 192.168.1.71. In Deb2, the interface 'lo' is configured with IP 127.0.0.1 and 'enp8s3' is configured with IP 192.168.1.72. Both windows also show the output of the 'ip netns exec' command, indicating that the network namespace is up and running.

Пинг с Deb2 Deb1

```
PING 192.168.1.71 (192.168.1.71) 56(84) bytes of data.  
64 bytes from 192.168.1.71: icmp_seq=1 ttl=64 time=0.812 ms  
64 bytes from 192.168.1.71: icmp_seq=2 ttl=64 time=0.656 ms  
64 bytes from 192.168.1.71: icmp_seq=3 ttl=64 time=0.694 ms  
64 bytes from 192.168.1.71: icmp_seq=4 ttl=64 time=0.639 ms  
64 bytes from 192.168.1.71: icmp_seq=5 ttl=64 time=0.661 ms  
^Z  
[13]+  Stopped                  ping 192.168.1.71
```

Пинг с Deb1 Deb2

```
-----  
PING 192.168.1.72 (192.168.1.72) 56(84) bytes of data.  
64 bytes from 192.168.1.72: icmp_seq=1 ttl=64 time=0.655 ms  
64 bytes from 192.168.1.72: icmp_seq=2 ttl=64 time=0.822 ms  
64 bytes from 192.168.1.72: icmp_seq=3 ttl=64 time=0.534 ms  
64 bytes from 192.168.1.72: icmp_seq=4 ttl=64 time=0.818 ms  
64 bytes from 192.168.1.72: icmp_seq=5 ttl=64 time=0.586 ms
```

На каждой из машин запущен rsyslog

```
Created symlink /etc/systemd/system/rsyslog.service - /lib/systemd/system/rsyslog.service.
Created symlink /etc/systemd/system/multi-user.target.wants/rsyslog.service - /lib/systemd/system/rsyslog.service.
Processing triggers for libc-bin (2.36-9+deb12u9) ...
Processing triggers for man-db (2.11.2-2) ...
root@vbox: /home/vboxuser# start rsyslog
bash: start: command not found
root@vbox: /home/vboxuser# systemctl start rsyslog
root@vbox: /home/vboxuser# systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; preset: enabled)
   Active: active (running) since Mon 2024-11-25 17:30:44 MSK; 1min 25s ago
TriggeredBy: ● syslog.socket
           Docs: man:rsyslogd(8)
                  man:rsyslog.conf(5)
                  https://www.rsyslog.com/doc/
   Main PID: 2647 (rsyslogd)
     Tasks: 4 (limit: 4631)
    Memory: 1.0M
       CPU: 28ms
   CGroup: /system.slice/rsyslog.service
           └─2647 /usr/sbin/rsyslogd -n -iNONE

Nov 25 17:30:44 vbox systemd[1]: Starting rsyslog.service - System Logging Service...
Nov 25 17:30:44 vbox rsyslogd[2647]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3)
Nov 25 17:30:44 vbox systemd[1]: Started rsyslog.service - System Logging Service.
Nov 25 17:30:44 vbox rsyslogd[2647]: [origin software="rsyslogd" swVersion="8.2302.0" x-pid="2647" x-info="https://www.rsyslog.com/doc"]
[lines 1-18/18 (END)]
```

```
Setting up libbstr0:amd64 (0.1.11-1) ...
Setting up libfastjson4:amd64 (1.2304.0-1) ...
Setting up liblognorm5:amd64 (2.0.6-4) ...
Setting up rsyslog (8.2302.0-1) ...
Created symlink /etc/systemd/system/rsyslog.service - /lib/systemd/system/rsyslog.service.
Created symlink /etc/systemd/system/multi-user.target.wants/rsyslog.service - /lib/systemd/system/rsyslog.service.
Processing triggers for libc-bin (2.36-9+deb12u9) ...
Processing triggers for man-db (2.11.2-2) ...
root@vbox: /home/vboxuser# systemctl start rsyslog
root@vbox: /home/vboxuser# systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; preset: enabled)
   Active: active (running) since Mon 2024-11-25 17:33:50 MSK; 30s ago
TriggeredBy: ● syslog.socket
           Docs: man:rsyslogd(8)
                  man:rsyslog.conf(5)
                  https://www.rsyslog.com/doc/
   Main PID: 2708 (rsyslogd)
     Tasks: 4 (limit: 4631)
    Memory: 3.3M
       CPU: 24ms
   CGroup: /system.slice/rsyslog.service
           └─2708 /usr/sbin/rsyslogd -n -iNONE

Nov 25 17:33:50 vbox systemd[1]: Starting rsyslog.service - System Logging Service...
Nov 25 17:33:50 vbox rsyslogd[2708]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3)
Nov 25 17:33:50 vbox rsyslogd[2708]: [origin software="rsyslogd" swVersion="8.2302.0" x-pid="2708" x-info="https://www.rsyslog.com/doc"]
```

Убираем комментирование с TCP UDP rsyslog.conf на каждой машине

```
GNU nano 7.2 /etc/rsyslog.conf
# /etc/rsyslog.conf configuration file for rsyslog
#
# For more information install rsyslog-doc and see
# /usr/share/doc/rsyslog-doc/html/configuration/index.html

#####
### MODULES ###
#####

module(load="imuxsock") # provides support for local system logging
module(load="imklog")   # provides kernel logging support
#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")

#####
### GLOBAL DIRECTIVES ###
#####

#
# Log anything besides private authentication messages to a single log file
#
*. *;auth,authpriv.none                -/var/log/syslog

#
# Log commonly used facilities to their own log file
#
auth,authpriv.*                        /var/log/auth.log
cron.*                                 /var/log/cron.log
kern.*                                 /var/log/kern.log
mail.*                                 /var/log/mail.log
user.*                                 /var/log/user.log

#
# Emergencies are sent to everybody logged in.
#
*.emerg                                :omusrmsg:*

#
# * * * @192.168.1.72:514
#
```

```
GNU nano 7.2 /etc/rsyslog.conf
# /etc/rsyslog.conf configuration file for rsyslog
#
# For more information install rsyslog-doc and see
# /usr/share/doc/rsyslog-doc/html/configuration/index.html

#####
### MODULES ###
#####

module(load="imuxsock") # provides support for local system logging
module(load="imklog")   # provides kernel logging support
#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")

#####
### GLOBAL DIRECTIVES ###
#####

#
# Log anything besides private authentication messages to a single log file
#
*. *;auth,authpriv.none                -/var/log/syslog

#
# Log commonly used facilities to their own log file
#
auth,authpriv.*                        /var/log/auth.log
cron.*                                 /var/log/cron.log
kern.*                                 /var/log/kern.log
mail.*                                 /var/log/mail.log
user.*                                 /var/log/user.log

#
# Emergencies are sent to everybody logged in.
#
*.emerg                                :omusrmsg:*

#
# * * * @192.168.1.72:514
#

template(name="RemoteLogs" type="string" string="/var/log/$HOSTNAME/$PROGRAMNAME.log")
# * * * RemoteLogs
# stop
```

На Deb1 включаем отправку логов на Deb2, так же дополняем на Deb 2 правила (Nano /etc/rsyslog.conf)

```
GNU nano 7.2 /etc/rsyslog.conf
#####
### RULES ###
#####

#
# Log anything besides private authentication messages to a single log file
#
*. *;auth,authpriv.none                -/var/log/syslog

#
# Log commonly used facilities to their own log file
#
auth,authpriv.*                        /var/log/auth.log
cron.*                                 /var/log/cron.log
kern.*                                 /var/log/kern.log
mail.*                                 /var/log/mail.log
user.*                                 /var/log/user.log

#
# Emergencies are sent to everybody logged in.
#
*.emerg                                :omusrmsg:*

#
# * * * @192.168.1.72:514
#
```

```
GNU nano 7.2 /etc/rsyslog.conf
includeConfig /etc/rsyslog.d/*.conf

#####
### RULES ###
#####

#
# Log anything besides private authentication messages to a single log file
#
*. *;auth,authpriv.none                -/var/log/syslog

#
# Log commonly used facilities to their own log file
#
auth,authpriv.*                        /var/log/auth.log
cron.*                                 /var/log/cron.log
kern.*                                 /var/log/kern.log
mail.*                                 /var/log/mail.log
user.*                                 /var/log/user.log

#
# Emergencies are sent to everybody logged in.
#
*.emerg                                :omusrmsg:*

#
# * * * @192.168.1.72:514
#

template(name="RemoteLogs" type="string" string="/var/log/$HOSTNAME/$PROGRAMNAME.log")
# * * * RemoteLogs
# stop
```

Рестартам rsyslog на каждой тачке и выводим статус , можно у заметить что Deb2 слушаем ещё и Deb1

```
vboxuser@vbox: ~
Nov 25 21:15:06 vbox systemd[1]: Starting rsyslog.service - System Logging Service...
Nov 25 21:15:06 vbox rsyslogd[2346]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) f
Nov 25 21:15:06 vbox rsyslogd[2346]: [origin software="rsyslogd" swVersion="8.2302.0" x-pid="2346" x-
Nov 25 21:15:06 vbox systemd[1]: Started rsyslog.service - System Logging Service.
lines 1-18/18 (END)
[7]+ Stopped systemctl status rsyslog
lines 1-18/18 (END)
root@vbox:/home/vboxuser# nano /etc/rsyslog.conf
root@vbox:/home/vboxuser# systemctl restart rsyslog
root@vbox:/home/vboxuser# systemctl status rsyslog
rsyslog.service - System Logging Service
Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; preset: enabled)
Active: active (running) since Mon 2024-11-25 21:20:33 MSK; 3s ago
TriggeredBy: ● syslog.socket
Docs: man:rsyslogd(8)
      man:rsyslog.conf(5)
      https://www.rsyslog.com/doc/
Main PID: 2370 (rsyslogd)
Tasks: 10 (limit: 4631)
Memory: 1.1M
CPU: 26ms
CGroup: /system.slice/rsyslog.service
        └─2370 /usr/sbin/rsyslogd -n -iNONE

Nov 25 21:20:33 vbox systemd[1]: Starting rsyslog.service - System Logging Service...
Nov 25 21:20:33 vbox rsyslogd[2370]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) f
Nov 25 21:20:33 vbox rsyslogd[2370]: [origin software="rsyslogd" swVersion="8.2302.0" x-pid="2370" x-
Nov 25 21:20:33 vbox rsyslogd[2370]: [origin software="rsyslogd" swVersion="8.2302.0" x-pid="2370" x-
lines 1-18/18 (END)

Nov 25 21:15:39 vbox rsyslogd[2785]: [origin software="rsyslogd" swVersion="8.2302.0" x-pid="2785" x-info=
Nov 25 21:15:39 vbox systemd[1]: Started rsyslog.service - System Logging Service.
root@vbox:/home/vboxuser# sudo ss -tulnp | grep "rsyslog"
udp UNCONN 0 0 0.0.0.0:514 0.0.0.0:* users:({"rsyslogd",pi
udp UNCONN 0 0 [::]:514 [::]:* users:({"rsyslogd",pi
tcp LISTEN 0 25 0.0.0.0:514 0.0.0.0:* users:({"rsyslogd",pi
tcp LISTEN 0 25 [::]:514 [::]:* users:({"rsyslogd",pi

root@vbox:/home/vboxuser# nano /etc/rsyslog.conf
root@vbox:/home/vboxuser# systemctl restart rsyslog
root@vbox:/home/vboxuser# systemctl status rsyslog
rsyslog.service - System Logging Service
Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; preset: enabled)
Active: active (running) since Mon 2024-11-25 21:21:00 MSK; 11s ago
TriggeredBy: ● syslog.socket
Docs: man:rsyslogd(8)
      man:rsyslog.conf(5)
      https://www.rsyslog.com/doc/
Main PID: 2812 (rsyslogd)
Tasks: 10 (limit: 4631)
Memory: 1.1M
CPU: 23ms
CGroup: /system.slice/rsyslog.service
        └─2812 /usr/sbin/rsyslogd -n -iNONE

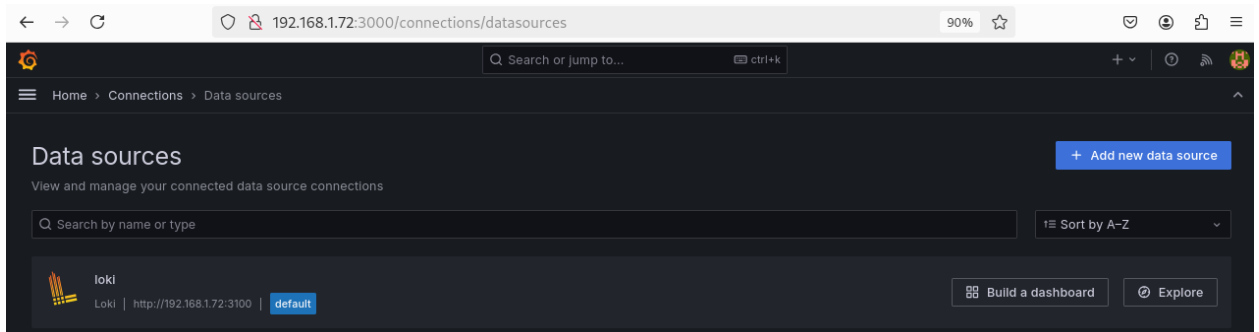
Nov 25 21:21:00 vbox systemd[1]: Starting rsyslog.service - System Logging Service...
Nov 25 21:21:00 vbox rsyslogd[2812]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) f
Nov 25 21:21:00 vbox rsyslogd[2812]: [origin software="rsyslogd" swVersion="8.2302.0" x-pid="2812" x-info=
Nov 25 21:21:00 vbox systemd[1]: Started rsyslog.service - System Logging Service.
root@vbox:/home/vboxuser# sudo ss -tulnp | grep "rsyslog"
udp UNCONN 0 0 0.0.0.0:514 0.0.0.0:* users:({"rsyslogd",pi
udp UNCONN 0 0 [::]:514 [::]:* users:({"rsyslogd",pi
```

Скачиваем и запускаем два докера “loki” и “Grafana”

```
oot@vbox:~# docker run -d --name=loki -p 3100:3100 grafana/loki:2.9.4
Unable to find image 'grafana/loki:2.9.4' locally
2.9.4: Pulling from grafana/loki
926b61bad3b: Pull complete
b0ef9568c4b: Pull complete
0420823e620: Pull complete
aefed802139: Pull complete
ac27bc4df5d: Pull complete
1eacff5fabb2: Pull complete
Digest: sha256:f379a20ce9dd815884ed6446aad8819b81a8ba4d36b548ca14be8cecb6c6bca0
Status: Downloaded newer image for grafana/loki:2.9.4
4f9da279d43dcba75b2e869e69959293cb294928646570c0ec7356c08318c3d
oot@vbox:~#
```

```
root@vbox:/loki# docker run -d --name=grafana -p 3000:3000 grafana/grafana
Unable to find image 'grafana/grafana:latest' locally
latest: Pulling from grafana/grafana
da9db072f522: Pull complete
eb724a2c4954: Pull complete
082ff8086b23: Pull complete
5d14cfaa511e: Pull complete
c05f507886b: Pull complete
16819baaa32d: Pull complete
557cb0193fc4: Pull complete
8821fea706d0: Pull complete
dfa49a55d740: Pull complete
915f3104e0f: Pull complete
Digest: sha256:fa801ab6e1ae035135309580891e09f7eb94d1abdbd2106bdc288030b028158c
Status: Downloaded newer image for grafana/grafana:latest
e099ae1fb6e7e6e9c6d58b455c13403f2aee1e43c254dcf66a64a85669621c17
root@vbox:/loki# docker ps
CONTAINER ID   IMAGE               COMMAND                  CREATED        STATUS        PORTS
ES
e099ae1fb6e7   grafana/grafana    "/run.sh"               11 seconds ago Up 9 seconds  0.0.0.0:3000-
fana
a4f9da279d43   grafana/loki:2.9.4  "/usr/bin/loki -conf..." 4 minutes ago  Up 4 minutes  0.0.0.0:3100-
i
root@vbox:/loki#
```

Заходим по адресу Deb 2 и порту выделенный Grafana и подцепляем туда Loki



Чтобы видеть логи с Deb 1 поставим на него promtail

```
root@vbox:~# wget https://github.com/grafana/loki/releases/download/v2.9.4/promtail-linux-amd64.zip
--2024-11-25 22:44:53-- https://github.com/grafana/loki/releases/download/v2.9.4/promtail-linux-amd64
.zip
Resolving github.com (github.com)... 140.82.121.4
Connecting to github.com (github.com)|140.82.121.4|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/129717717/8708e
eb0-9680-4eaa-8a41-444e5b6dc8de?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=releaseassetproducti
on%2F20241125%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20241125T194454Z&X-Amz-Expires=300&X-Amz-Sign
ature=fe1c3c90b0a77833806a9fad600ab8e1e1fa563718786632cdf6645806008b88&X-Amz-SignedHeaders=host&respon
se-content-disposition=attachment%3B%20filename%3Dpromtail-linux-amd64.zip&response-content-type=appli
cation%2Foctet-stream [following]
--2024-11-25 22:44:54-- https://objects.githubusercontent.com/github-production-release-asset-2e65be/
129717717/8708eeb0-9680-4eaa-8a41-444e5b6dc8de?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=relea
seassetproduction%2F20241125%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20241125T194454Z&X-Amz-Expires
=300&X-Amz-Signature=fe1c3c90b0a77833806a9fad600ab8e1e1fa563718786632cdf6645806008b88&X-Amz-SignedHead
ers=host&response-content-disposition=attachment%3B%20filename%3Dpromtail-linux-amd64.zip&response-con
tent-type=application%2Foctet-stream
Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.108.133, 185.199.11
1.133, 185.199.109.133, ...
Connecting to objects.githubusercontent.com (objects.githubusercontent.com)|185.199.108.133|:443... co
nnected.
HTTP request sent, awaiting response... 200 OK
Length: 26811203 (26M) [application/octet-stream]
Saving to: 'promtail-linux-amd64.zip.1'

promtail-linux-amd64.zip. 100%[=====>] 25.57M 23.7MB/s in 1.1s

2024-11-25 22:44:56 (23.7 MB/s) - 'promtail-linux-amd64.zip.1' saved [26811203/26811203]

root@vbox:~#
```

```
root@vbox:~# unzip promtail-linux-amd64.zip -d /usr/local/bin/promtail
Archive: promtail-linux-amd64.zip
  inflating: /usr/local/bin/promtail/promtail-linux-amd64
root@vbox:~# ls /usr/local/bin/promtail
promtail-linux-amd64
```

```
root@vbox:~# cp promtail-linux-amd64 /usr/local/bin/promtail
root@vbox:~# chnod +x /usr/local/bin/promtail
bash: chnod: command not found
root@vbox:~# chmod +x /usr/local/bin/promtail
root@vbox:~# mkdir /etc/promtail
root@vbox:~# touch /etc/promtail/config.yaml
root@vbox:~# nano /etc/promtail/config.yaml
root@vbox:~#
```

```
GNU nano 7.2 /etc/promtail/promtail.yaml *
server:
  http_listen_port: 9080
  grpc_listen_port: 0
positions:
  filename: /tmp/positions.yaml

clients:
  - url: http://192.168.1.72:3100/loki/api/v1/push

scrape_configs:
- job_name: system
  static_configs:
  - targets:
    - localhost
    labels:
      job: varlogs
      __path__: /var/log/*log
```

После редактирования всех файлов стартуем и проверяем статус, на этом моменте что-то пошло не так и к сожалению проблему найти не смог, поэтому логи не доходят до Loki

```
root@vbox:/etc/systemd/system# systemctl status promtail
* promtail.service - Promtail Service
   Loaded: loaded (/etc/systemd/system/promtail.service; enabled; preset: enabled)
   Active: failed (Result: exit-code) since Mon 2024-11-25 23:46:12 MSK; 815ms ago
   Duration: 3ms
   Process: 6863 ExecStart=/usr/local/bin/promtail -config.file=/etc/promtail/promtail.yaml (code=exited, status=203/EXEC)
   Main PID: 6863 (code=exited, status=203/EXEC)
   CPU: 3ms
```

