Task #1

It is necessary to prepare the audit.rules configuration file for the auditd service and configure the auditd and rsyslog services so that when attempting to access the shadow, sudoers, and passwd files from the /etc directory, the system sends the corresponding events to the remote syslog server. It is also necessary to configure sending events when attempting to change the system time.

Solution:

Setting up **a client using** OS as an example Ubuntu 2024.04.2:

1. First of all, you need to download the auditd and rsyslog packages using the command – sudo apt install auditd && sudo apt install rsyslog

2. After that, we configure the rules in the audit configuration file audit.rules, open it with the command - sudo nano /etc/audit/rules.d/audit.rules.

   We enter the rules into the file:

   # Monitoring access to critical files
   -w /etc/shadow -p wa -k shadow_access
   #Monitors the file /etc/shadow, records events if a file is written or its attributes are changed, marks the event with the shadow_access key to make it easier to search in the logs
   -w /etc/sudoers -p wa -k sudoers_access
   #Similarly for /etc/sudoers (file with sudo rights) and /etc/passwd (file with accounts)
   -w /etc/passwd -p wa -k passwd_access

   # Monitoring changes systemic time
   -a always,exit -F arch=b64 -S clock_ settime,settimeofday -k time_change
   #writes an event when exiting a system call (i.e. after the action is performed), filters for 64-bit systems, monitors calls to time-changing functions, marks time-changing events
   -a always,exit -F arch=b32 -S clock_ settime,settimeofday -k time_change
   #Does the same thing only for 32-bit systems

The end result should look like this:

```
  GNU nano 7.2                    /etc/audit/rules.d/audit.rules *

## Increase the buffers to survive stress events.
## Make this bigger for busy systems
-b 8192

## This determine how long to wait in burst of events
--backlog_wait_time 60000

## Set failure mode to syslog
-f 1

# Monitoring access to critical files
-w /etc/shadow -p wa -k shadow_access
-w /etc/sudoers -p wa -k sudoers_access
-w /etc/passwd -p wa -k passwd_access

# Monitoring changes in system time
-a always,exit -F arch=b64 -S clock_settime,settimeofday -k time_change
-a always,exit -F arch=b32 -S clock_settime,settimeofday -k time_change
```

3. Next, we configure the syslog plugin for auditd – sudo nano /etc/audit/plugins.d/syslog.conf

   Initially, the configuration file looks like this:

```
  GNU nano 7.2                    /etc/audit/plugins.d/syslog.conf *
# This file controls the configuration of the syslog plugin.
# It simply takes events and writes them to syslog. The
# arguments provided can be the default priority that you
# want the events written with. And optionally, you can give
# a second argument indicating the facility that you want events
# logged to. Valid options are LOG_LOCAL0 through 7, LOG_AUTH,
# LOG_AUTHPRIV, LOG_DAEMON, LOG_SYSLOG, and LOG_USER.

active = yes
direction = out
path = /sbin/audisp-syslog
type = always
args = LOG_INFO
format = string
```

We bring it to this form:

```
  GNU nano 7.2                    /etc/audit/plugins.d/syslog.conf
# This file controls the configuration of the syslog plugin.
# It simply takes events and writes them to syslog. The
# arguments provided can be the default priority that you
# want the events written with. And optionally, you can give
# a second argument indicating the facility that you want events
# logged to. Valid options are LOG_LOCAL0 through 7, LOG_AUTH,
# LOG_AUTHPRIV, LOG_DAEMON, LOG_SYSLOG, and LOG_USER.

active = yes
direction = out
path = /sbin/audisp-syslog
type = builtin
args = LOG_INFO
format = string
```

Activate the plugin by setting active = yes

Change in the type line always on builtin (always is an invalid value, the type parameter determines whether the plugin is «builtin» or «external». The «always» value is invalid here and may cause errors).

4. Setting up rsyslog

Now we need to configure rsyslog to forward auditd logs to a remote server.

Command : sudo nano /etc/rsyslog.d/audit_remote.conf

We enter the rules into the file:

For TCP forwarding
$ ModLoad imtcp
# Load module for TCP support
$ InputTCPServerRun 514
# Allow rsyslog to accept incoming connections via TCP on port 514

Filter events auditd By tag
:programname, isequal, "audit" @192.168.1.143:514
#All logs generated by audit d will be sent to remote server 192.168.1.143 via port 514 over UDP.

It should look like this:

```
  GNU nano 7.2                    /etc/rsyslog.d/audit_remote.conf
#TCP
$ModLoad imtcp
$InputTCPServerRun 514

#audit tag
:programname, isequal, "audit" @192.168.1.143:514
```

5. Restart services
   sudo systemctl restart auditd rsyslog

6. Checking audit rights
   sudo auditctl -l

```
ubuntuclient@UbuntuClient:/home$ sudo auditctl -l
-w /etc/shadow -p wa -k shadow_access
-w /etc/sudoers -p wa -k sudoers_access
-w /etc/passwd -p wa -k passwd_access
-a always,exit -F arch=b64 -S settimeofday,clock_settime -F key=time_change
-a always,exit -F arch=b32 -S settimeofday,clock_settime -F key=time_change
ubuntuclient@UbuntuClient:/home$
```

7. Let's run a test event (edit the file, add ## signs at the top and save)
   sudo nano /etc/shadow

```
Mar 20 03:18
ubuntuclient@UbuntuClient: /home
  GNU nano 7.2                    /etc/shadow *
##
root:*:20134:0:99999:7:::
daemon:*:20134:0:99999:7:::
bin:*:20134:0:99999:7:::
sys:*:20134:0:99999:7:::
sync:*:20134:0:99999:7:::
games:*:20134:0:99999:7:::
man:*:20134:0:99999:7:::
lp:*:20134:0:99999:7:::
mail:*:20134:0:99999:7:::
news:*:20134:0:99999:7:::
uucp:*:20134:0:99999:7:::
proxy:*:20134:0:99999:7:::
www-data:*:20134:0:99999:7:::
backup:*:20134:0:99999:7:::
list:*:20134:0:99999:7:::
irc:*:20134:0:99999:7:::
_apt:*:20134:0:99999:7:::
nobody:*:20134:0:99999:7:::
systemd-network:!*:20134:::::
```

8. Now let's check the local logs for the event
   sudo ausearch -k shadow_access

```
----
time->Thu Mar 20 03:18:25 2025
type=PROCTITLE msg=audit(1742415505.438:791): proctitle=6E616E6F002F6574632F736861646F77
type=PATH msg=audit(1742415505.438:791): item=1 name="/etc/shadow" inode=1051359 dev=08:02 mode=0100640 ouid=0 ogid=42
rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=PATH msg=audit(1742415505.438:791): item=0 name="/etc/" inode=1048577 dev=08:02 mode=040755 ouid=0 ogid=0 rdev=00:
00 nametype=PARENT cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=CWD msg=audit(1742415505.438:791): cwd="/home"
type=SYSCALL msg=audit(1742415505.438:791): arch=c000003e syscall=257 success=yes exit=3 a0=ffffff9c a1=588947fecda0 a2
=241 a3=1b6 items=2 ppid=4170 pid=4171 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts5 ses=3
 comm="nano" exe="/usr/bin/nano" subj=unconfined key="shadow_access"
----
```

The event actually happened

9. We will also do the same for the passwd and sudoers files.

```
Mar 20 03:25
ubuntuclient@UbuntuClient: /home
  GNU nano 7.2                    /etc/sudoers *
#####
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/>

# This fixes CVE-2005-4890 and possibly breaks some versions of kdesu
# (#1011624, https://bugs.kde.org/show_bug.cgi?id=452532)
Defaults        use_pty

# This preserves proxy settings from user environments of root
# equivalent users (group sudo)
#Defaults:%sudo env_keep += "http_proxy https_proxy ftp_proxy all_proxy no_proxy"

^G Help      ^O Write Out  ^W Where Is   ^K Cut       ^T Execute    ^C Location
^X Exit      ^R Read File  ^\ Replace    ^U Paste     ^J Justify    ^/ Go To Line
```

The event appears too

```
----
time->Thu Mar 20 03:25:14 2025
type=PROCTITLE msg=audit(1742415914.952:833): proctitle=6E616E6F002F6574632F7375646F657273
type=PATH msg=audit(1742415914.952:833): item=1 name="/etc/sudoers" inode=1049017 dev=08:02 mode=0100440 ouid=0 ogid=0
rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=PATH msg=audit(1742415914.952:833): item=0 name="/etc/" inode=1048577 dev=08:02 mode=040755 ouid=0 ogid=0 rdev=00:
00 nametype=PARENT cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=CWD msg=audit(1742415914.952:833): cwd="/home"
type=SYSCALL msg=audit(1742415914.952:833): arch=c000003e syscall=257 success=yes exit=3 a0=ffffff9c a1=5d7f9cf1cd10 a2
=241 a3=1b6 items=2 ppid=4205 pid=4206 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts5 ses=3
 comm="nano" exe="/usr/bin/nano" subj=unconfined key="sudoers_access"
```

Passwd

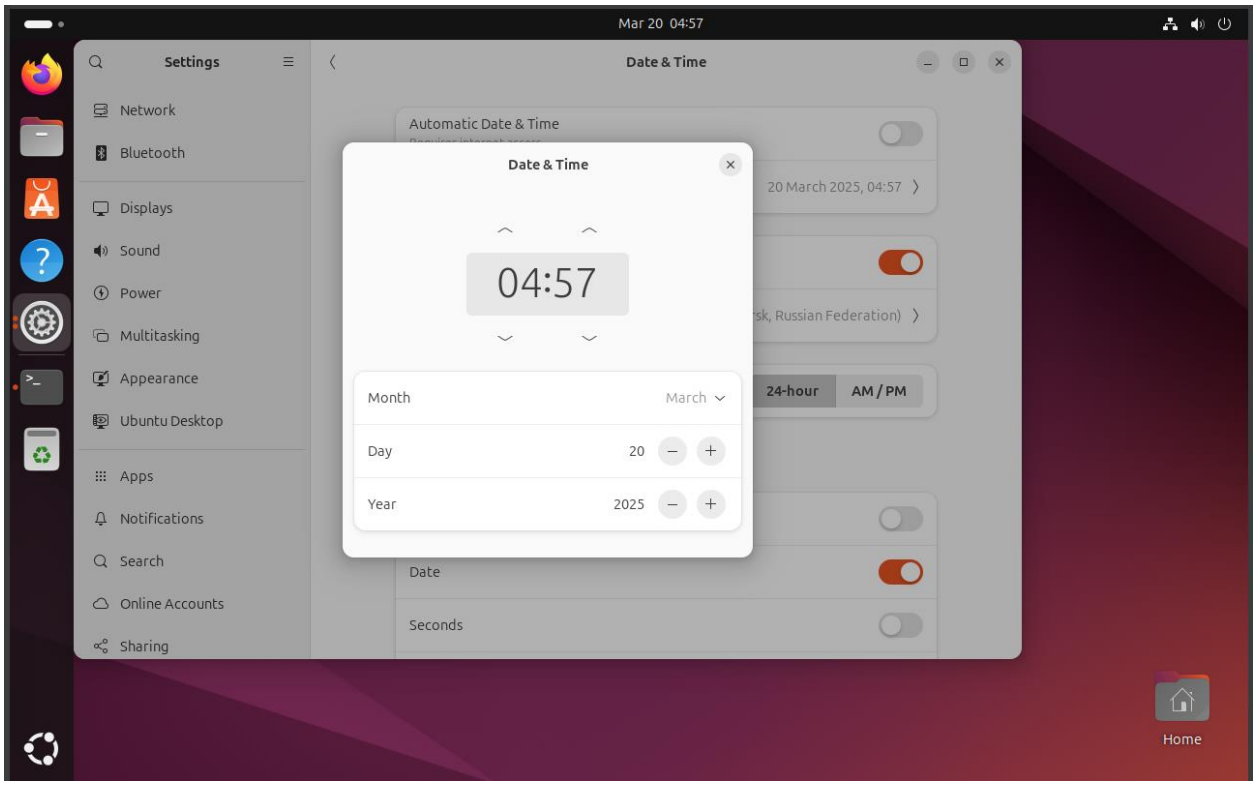
```
Mar 20 03:29
ubuntuclient@UbuntuClient: /home
  GNU nano 7.2                    /etc/passwd *
##
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin

^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify
```

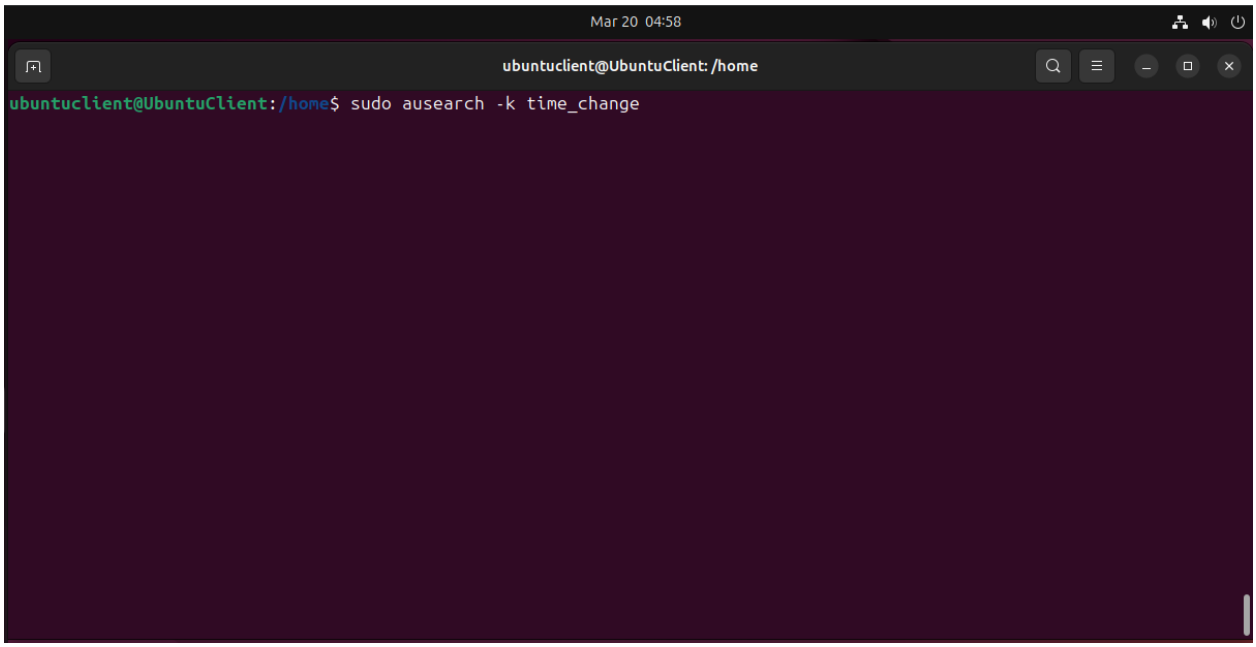
Event

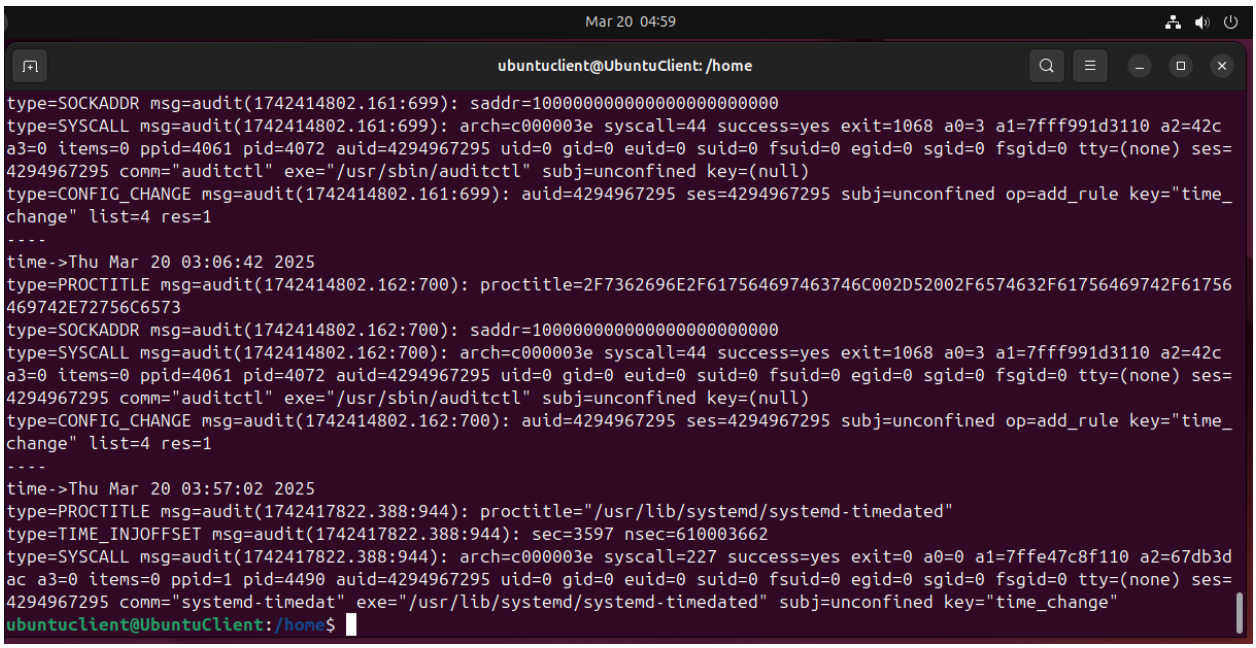
```
----
time->Thu Mar 20 03:30:34 2025
type=PROCTITLE msg=audit(1742416234.444:848): proctitle=6E616E6F002F6574632F706173737764
type=PATH msg=audit(1742416234.444:848): item=1 name="/etc/passwd" inode=1051377 dev=08:02 mode=0100644 ouid=0 ogid=0 r
dev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=PATH msg=audit(1742416234.444:848): item=0 name="/etc/" inode=1048577 dev=08:02 mode=040755 ouid=0 ogid=0 rdev=00:
00 nametype=PARENT cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=CWD msg=audit(1742416234.444:848): cwd="/home"
type=SYSCALL msg=audit(1742416234.444:848): arch=c000003e syscall=257 success=yes exit=3 a0=ffffff9c a1=55a3d07ca750 a2
=241 a3=1b6 items=2 ppid=4218 pid=4219 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts5 ses=3
 comm="nano" exe="/usr/bin/nano" subj=unconfined key="passwd_access"
```

We will also check events for time changes in the system, set the time an hour ahead



Events also appear





Now we need to configure **the server** also using the OS example Ubuntu 2024.04.2 **:**

1. Installing rsyslog
   sudo apt update && sudo apt install rsyslog

2. Editing the configuration file
   sudo nano /etc/rsyslog.conf

3. Let's uncomment the lines

   module(load="imudp")
   input(type="imudp" port="514")

   module(load="imtcp")
   input(type="imtcp" port="514")

4. We add the rule after the imudp, imtcp modules

   # Template for saving logs by hosts and programs
   $template RemoteLogs ,"/var/log/remote/%HOSTNAME%/%PROGRAMNAME%.log"

   # Apply template to all incoming messages
   . ?RemoteLogs

In the end it should look like this

```
root@Ubuntu: /var/log/remote/UbuntuClient
  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
#
# Default logging rules can be found in /etc/rsyslog.d/50-default.conf


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

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

#log template
$template RemoteLogs,"/var/log/remote/%HOSTNAME%/%PROGRAMNAME%.log"
*.* ?RemoteLogs

# provides kernel logging support and enable non-kernel klog messages
```

5. Create a directory for logs and give it permissions
   sudo mkdir -p /var/log/remote
   sudo chmod -R 755 /var/log/remote

6. Restart rsyslog after settings
   sudo systemctl restart rsyslog

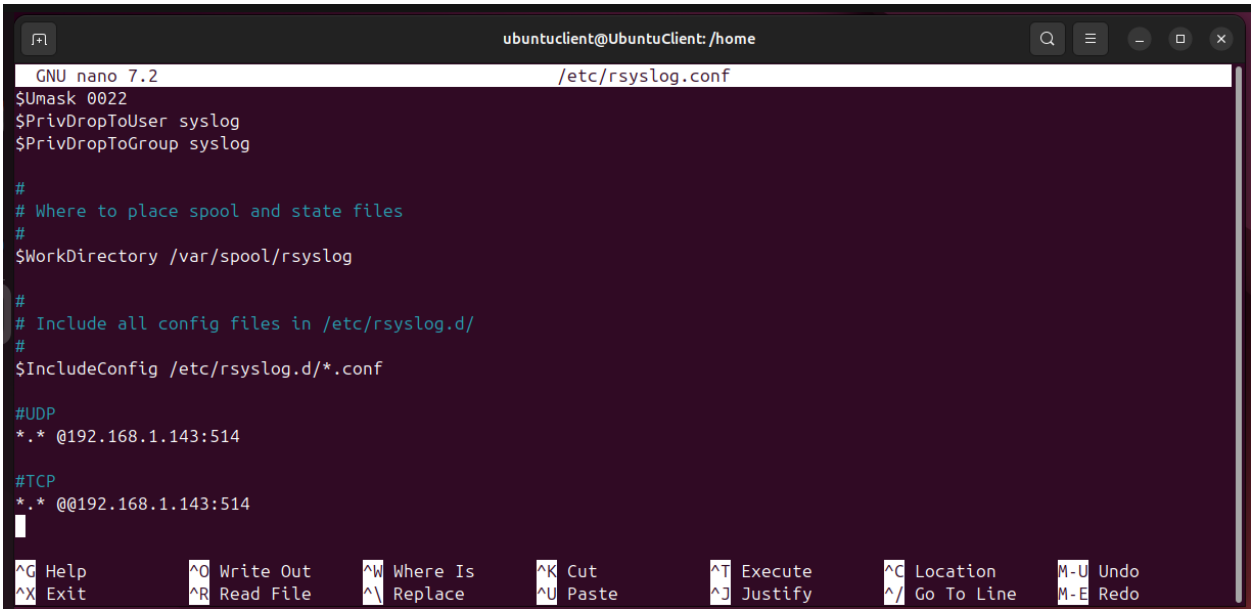
7. Configuring a firewall to accept tcp and udp protocols

   # For UDP
   sudo ufw allow 514/ udp

   # For TCP
   sudo ufw allow 514/ tcp

8. On **the client** , we also configure the rsyslog .conf file .
   Add to the end of the file

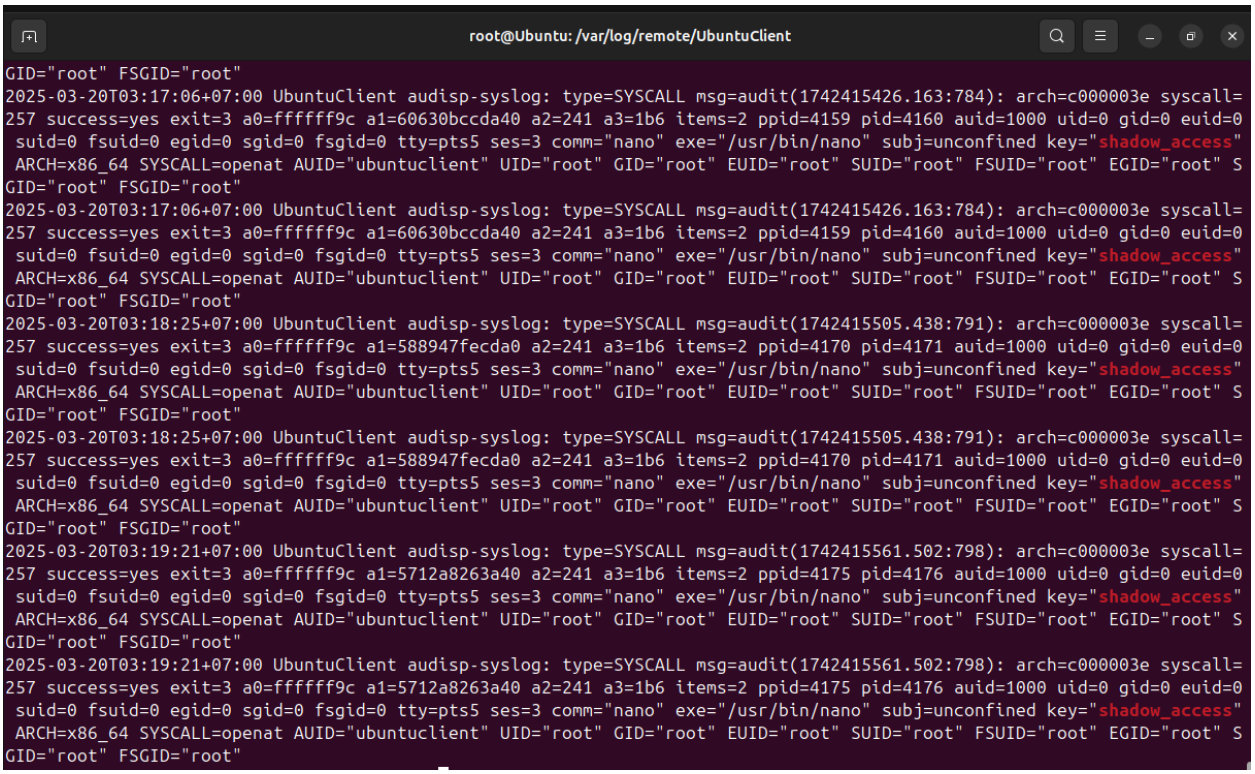
   . @192.168.1.143:514 # For UDP
   . @@192.168.1.143:514 # For TCP



9. Checking the operation of logging on **the server**

   From our settings it becomes clear that all remote client logs will be stored in a file at/var/log/remote/UbuntuClient/audisp-syslog.log

   Let's check the logs in the **shadow file** with the command grep ' shadow _ access ' /var/log/remote/UbuntuClient/audisp-syslog.log



Let's do the same for **sudoers**

```
Чт, 20 марта 04:19
root@Ubuntu: /var/log/remote/UbuntuClient
ses=4294967295 subj=unconfined op=add_rule key="sudoers_access" list=4 res=1 AUID="unset"
2025-03-20T02:30:23+07:00 UbuntuClient audisp-syslog: type=CONFIG_CHANGE msg=audit(1742412623.894:608): auid=4294967295
ses=4294967295 subj=unconfined op=add_rule key="sudoers_access" list=4 res=1 AUID="unset"
2025-03-20T03:06:42+07:00 UbuntuClient audisp-syslog: type=CONFIG_CHANGE msg=audit(1742414802.148:689): auid=4294967295
ses=4294967295 subj=unconfined op=remove_rule key="sudoers_access" list=4 res=1 AUID="unset"
2025-03-20T03:06:42+07:00 UbuntuClient audisp-syslog: type=CONFIG_CHANGE msg=audit(1742414802.159:697): auid=4294967295
ses=4294967295 subj=unconfined op=add_rule key="sudoers_access" list=4 res=1 AUID="unset"
2025-03-20T03:06:42+07:00 UbuntuClient audisp-syslog: type=CONFIG_CHANGE msg=audit(1742414802.148:689): auid=4294967295
ses=4294967295 subj=unconfined op=remove_rule key="sudoers_access" list=4 res=1 AUID="unset"
2025-03-20T03:06:42+07:00 UbuntuClient audisp-syslog: type=CONFIG_CHANGE msg=audit(1742414802.159:697): auid=4294967295
ses=4294967295 subj=unconfined op=add_rule key="sudoers_access" list=4 res=1 AUID="unset"
2025-03-20T03:24:06+07:00 UbuntuClient audisp-syslog: type=SYSCALL msg=audit(1742415846.797:819): arch=c000003e syscall=
257 success=yes exit=3 a0=ffffff9c a1=5b646a75c630 a2=241 a3=1b6 items=2 ppid=4200 pid=4201 auid=1000 uid=0 gid=0 euid=0
 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts5 ses=3 comm="nano" exe="/usr/bin/nano" subj=unconfined key="sudoers_access
" ARCH=x86_64 SYSCALL=openat AUID="ubuntuclient" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root"
SGID="root" FSGID="root"
2025-03-20T03:24:06+07:00 UbuntuClient audisp-syslog: type=SYSCALL msg=audit(1742415846.797:819): arch=c000003e syscall=
257 success=yes exit=3 a0=ffffff9c a1=5b646a75c630 a2=241 a3=1b6 items=2 ppid=4200 pid=4201 auid=1000 uid=0 gid=0 euid=0
 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts5 ses=3 comm="nano" exe="/usr/bin/nano" subj=unconfined key="sudoers_access
" ARCH=x86_64 SYSCALL=openat AUID="ubuntuclient" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root"
SGID="root" FSGID="root"
2025-03-20T03:25:14+07:00 UbuntuClient audisp-syslog: type=SYSCALL msg=audit(1742415914.952:833): arch=c000003e syscall=
257 success=yes exit=3 a0=ffffff9c a1=5d7f9cf1cd10 a2=241 a3=1b6 items=2 ppid=4205 pid=4206 auid=1000 uid=0 gid=0 euid=0
 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts5 ses=3 comm="nano" exe="/usr/bin/nano" subj=unconfined key="sudoers_access
" ARCH=x86_64 SYSCALL=openat AUID="ubuntuclient" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root"
SGID="root" FSGID="root"
2025-03-20T03:25:14+07:00 UbuntuClient audisp-syslog: type=SYSCALL msg=audit(1742415914.952:833): arch=c000003e syscall=
257 success=yes exit=3 a0=ffffff9c a1=5d7f9cf1cd10 a2=241 a3=1b6 items=2 ppid=4205 pid=4206 auid=1000 uid=0 gid=0 euid=0
 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts5 ses=3 comm="nano" exe="/usr/bin/nano" subj=unconfined key="sudoers_access
" ARCH=x86_64 SYSCALL=openat AUID="ubuntuclient" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root"
SGID="root" FSGID="root"
root@Ubuntu:/var/log/remote/UbuntuClient#
```

Passwd

```
Чт, 20 марта 04:21
root@Ubuntu: /var/log/remote/UbuntuClient
2025-03-19T04:21:52+07:00 UbuntuClient audisp-syslog: type=SYSCALL msg=audit(1742332912.030:3793): arch=c000003e syscall
=257 success=yes exit=3 a0=ffffff9c a1=5757a5be6540 a2=241 a3=1b6 items=2 ppid=11595 pid=11596 auid=1000 uid=0 gid=0 eui
d=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts4 ses=3 comm="nano" exe="/usr/bin/nano" subj=unconfined key="passwd_acce
ss" ARCH=x86_64 SYSCALL=openat AUID="ubuntuclient" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root
" SGID="root" FSGID="root"
2025-03-20T02:30:23+07:00 UbuntuClient audisp-syslog: type=CONFIG_CHANGE msg=audit(1742412623.887:601): auid=4294967295
ses=4294967295 subj=unconfined op=remove_rule key="passwd_access" list=4 res=1 AUID="unset"
2025-03-20T02:30:23+07:00 UbuntuClient audisp-syslog: type=CONFIG_CHANGE msg=audit(1742412623.887:601): auid=4294967295
ses=4294967295 subj=unconfined op=remove_rule key="passwd_access" list=4 res=1 AUID="unset"
2025-03-20T02:30:23+07:00 UbuntuClient audisp-syslog: type=CONFIG_CHANGE msg=audit(1742412623.895:609): auid=4294967295
ses=4294967295 subj=unconfined op=add_rule key="passwd_access" list=4 res=1 AUID="unset"
2025-03-20T02:30:23+07:00 UbuntuClient audisp-syslog: type=CONFIG_CHANGE msg=audit(1742412623.895:609): auid=4294967295
ses=4294967295 subj=unconfined op=add_rule key="passwd_access" list=4 res=1 AUID="unset"
2025-03-20T03:06:42+07:00 UbuntuClient audisp-syslog: type=CONFIG_CHANGE msg=audit(1742414802.148:690): auid=4294967295
ses=4294967295 subj=unconfined op=remove_rule key="passwd_access" list=4 res=1 AUID="unset"
2025-03-20T03:06:42+07:00 UbuntuClient audisp-syslog: type=CONFIG_CHANGE msg=audit(1742414802.160:698): auid=4294967295
ses=4294967295 subj=unconfined op=add_rule key="passwd_access" list=4 res=1 AUID="unset"
2025-03-20T03:06:42+07:00 UbuntuClient audisp-syslog: type=CONFIG_CHANGE msg=audit(1742414802.148:690): auid=4294967295
ses=4294967295 subj=unconfined op=remove_rule key="passwd_access" list=4 res=1 AUID="unset"
2025-03-20T03:06:42+07:00 UbuntuClient audisp-syslog: type=CONFIG_CHANGE msg=audit(1742414802.160:698): auid=4294967295
ses=4294967295 subj=unconfined op=add_rule key="passwd_access" list=4 res=1 AUID="unset"
2025-03-20T03:30:34+07:00 UbuntuClient audisp-syslog: type=SYSCALL msg=audit(1742416234.444:848): arch=c000003e syscall=
257 success=yes exit=3 a0=ffffff9c a1=55a3d07ca750 a2=241 a3=1b6 items=2 ppid=4218 pid=4219 auid=1000 uid=0 gid=0 euid=0
 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts5 ses=3 comm="nano" exe="/usr/bin/nano" subj=unconfined key="passwd_access"
 ARCH=x86_64 SYSCALL=openat AUID="ubuntuclient" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" S
GID="root" FSGID="root"
2025-03-20T03:30:34+07:00 UbuntuClient audisp-syslog: type=SYSCALL msg=audit(1742416234.444:848): arch=c000003e syscall=
257 success=yes exit=3 a0=ffffff9c a1=55a3d07ca750 a2=241 a3=1b6 items=2 ppid=4218 pid=4219 auid=1000 uid=0 gid=0 euid=0
 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts5 ses=3 comm="nano" exe="/usr/bin/nano" subj=unconfined key="passwd_access"
 ARCH=x86_64 SYSCALL=openat AUID="ubuntuclient" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" S
GID="root" FSGID="root"
root@Ubuntu:/var/log/remote/UbuntuClient#
```

Change of time

```
Чт, 20 марта 04:23
root@Ubuntu: /var/log/remote/UbuntuClient
ses=4294967295 subj=unconfined op=add_rule key="time_change" list=4 res=1 AUID="unset"
2025-03-20T02:30:23+07:00 UbuntuClient audisp-syslog: type=CONFIG_CHANGE msg=audit(1742412623.895:610): auid=4294967295
ses=4294967295 subj=unconfined op=add_rule key="time_change" list=4 res=1 AUID="unset"
2025-03-20T02:30:23+07:00 UbuntuClient audisp-syslog: type=CONFIG_CHANGE msg=audit(1742412623.895:611): auid=4294967295
ses=4294967295 subj=unconfined op=add_rule key="time_change" list=4 res=1 AUID="unset"
2025-03-20T03:06:42+07:00 UbuntuClient audisp-syslog: type=CONFIG_CHANGE msg=audit(1742414802.149:691): auid=4294967295
ses=4294967295 subj=unconfined op=remove_rule key="time_change" list=4 res=1 AUID="unset"
2025-03-20T03:06:42+07:00 UbuntuClient audisp-syslog: type=CONFIG_CHANGE msg=audit(1742414802.149:692): auid=4294967295
ses=4294967295 subj=unconfined op=remove_rule key="time_change" list=4 res=1 AUID="unset"
2025-03-20T03:06:42+07:00 UbuntuClient audisp-syslog: type=CONFIG_CHANGE msg=audit(1742414802.161:699): auid=4294967295
ses=4294967295 subj=unconfined op=add_rule key="time_change" list=4 res=1 AUID="unset"
2025-03-20T03:06:42+07:00 UbuntuClient audisp-syslog: type=CONFIG_CHANGE msg=audit(1742414802.162:700): auid=4294967295
ses=4294967295 subj=unconfined op=add_rule key="time_change" list=4 res=1 AUID="unset"
2025-03-20T03:06:42+07:00 UbuntuClient audisp-syslog: type=CONFIG_CHANGE msg=audit(1742414802.149:691): auid=4294967295
ses=4294967295 subj=unconfined op=remove_rule key="time_change" list=4 res=1 AUID="unset"
2025-03-20T03:06:42+07:00 UbuntuClient audisp-syslog: type=CONFIG_CHANGE msg=audit(1742414802.149:692): auid=4294967295
ses=4294967295 subj=unconfined op=remove_rule key="time_change" list=4 res=1 AUID="unset"
2025-03-20T03:06:42+07:00 UbuntuClient audisp-syslog: type=CONFIG_CHANGE msg=audit(1742414802.161:699): auid=4294967295
ses=4294967295 subj=unconfined op=add_rule key="time_change" list=4 res=1 AUID="unset"
2025-03-20T03:06:42+07:00 UbuntuClient audisp-syslog: type=CONFIG_CHANGE msg=audit(1742414802.162:700): auid=4294967295
ses=4294967295 subj=unconfined op=add_rule key="time_change" list=4 res=1 AUID="unset"
2025-03-20T04:57:00+07:00 UbuntuClient audisp-syslog: type=SYSCALL msg=audit(1742417822.388:944): arch=c000003e syscall=
227 success=yes exit=0 a0=0 a1=7ffe47c8f110 a2=67db3dac a3=0 items=0 ppid=1 pid=4490 auid=4294967295 uid=0 gid=0 euid=0
suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="systemd-timedat" exe="/usr/lib/systemd/systemd-time
dated" subj=unconfined key="time_change" ARCH=x86_64 SYSCALL=clock_settime AUID="unset" UID="root" GID="root" EUID="root
" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
2025-03-20T04:57:00+07:00 UbuntuClient audisp-syslog: type=SYSCALL msg=audit(1742417822.388:944): arch=c000003e syscall=
227 success=yes exit=0 a0=0 a1=7ffe47c8f110 a2=67db3dac a3=0 items=0 ppid=1 pid=4490 auid=4294967295 uid=0 gid=0 euid=0
suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="systemd-timedat" exe="/usr/lib/systemd/systemd-time
dated" subj=unconfined key="time_change" ARCH=x86_64 SYSCALL=clock_settime AUID="unset" UID="root" GID="root" EUID="root
" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
root@Ubuntu:/var/log/remote/UbuntuClient#
```

Task #2

In Active Directory users has attributes msRADIUSFramedIPAddress and msRASSavedFramedIPAddress. This attribute stores information about the IP-address that is assigned on the Dial-in tab in the user properties. You need to write a script in powershell that will list all Active Directory users who have this attribute filled in and convert the attribute value into a readable IP-address. For example, the value of the msRADIUSFramedIPAddress attribute -1062666676 corresponds to the IP address 192.168.254.76

Solution:

```
# Active module Directory

Import-Module Active Directory


#Function to convert integer to IP-address

function Convert-IntToIP {

   param(

      [int]$Integer

   )

   $bytes = [BitConverter]::GetBytes($Integer)

   [Array]::Reverse($bytes)

   return ([System.Net.IPAddress]::new($bytes)).ToString()

}


#Get all users with filled attributes

$users = Get-ADUser -Filter * -Properties msRADIUSFramedIPAddress, msRASSavedFramedIPAddress |

        Where-Object { $_.msRADIUSFramedIPAddress -or $_.msRASSavedFramedIPAddress }


#Processing and conclusion results

$result = foreach ($user in $users) {

   [PSCustomObject]@{

      Name             = $user.Name

      SamAccountName    = $user.SamAccountName

      FramedIP         = if ($user.msRADIUSFramedIPAddress) { Convert-IntToIP $user.msRADIUSFramedIPAddress } else {
$null }

      SavedFramedIP     = if ($user.msRASSavedFramedIPAddress) { Convert-IntToIP $user.msRASSavedFramedIPAddress }
else { $null }

   }

}


#Conclusion result V tabular format

$result | Format-Table - AutoSize
```

Explanation:

1. Import module : Loads the ActiveDirectory module to work with AD .

2. Function to convert number to IP :

- Convert-IntToIP converts a 32-bit integer to an IP address.

- [BitConverter]:: GetBytes() converts a number to an array of bytes (little - endian).

- [Array]:: Reverse() changes the byte order to big - endian (network format).

3. Getting users:

- Filter «-Filter *» selects all users.

- Properties loads the required attributes.

- Where-Object filters users with filled attributes.

4. Formation of the result:

- For each user, an object is created with a name, login and IP addresses.

- Conversion is performed only for non-empty attributes.

5. Output of results in a convenient tabular format.

Example output :

Name	SamAccountName	FramedIP	SavedFramedIP
User1	Ivan	192.168.1.100	10.0.0.50
User2	Vladimir	192.168.1.101	

Task #3

Write regular expressions For specified below events with devices :
a. <14>1 2019-11-29T13:09:07.000Z sco1s-vksu-01.sgp.ru KES|11.0.0.0 - 0000014f [event@23668
et='0000014f' tdn='Защита' etdn='Объект восстановлен из резервного хранилища' hdn='SCO1S-
VKSU-01' hip='10.47.0.120'] Тип события: Объект восстановлен из резервного хранилищаПрограмма: Kaspersky Endpoint Security для WindowsПрограмма\Путь: C:\Program
Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows\Пользователь: SGP\
Administrator (Инициатор)Компонент: ЗащитаРезультат\Описание: ВосстановленоОбъект: C:\
Users\Administrator.SGP\Desktop\eicar.comОбъект\Тип: ФайлОбъект\Путь: C:\Users\
Administrator.SGP\Desktop\Объект\Название: eicar.com

b. <189> Aug 29 12:06:07 cd5201-cm5448-15-1 TRAPMGR[trapTask]: traputil.c(721) 3833 %%
Session 0 of type 3 started for user admin connected from 172.16.11.56.\u0000

c. <188>2020/03/03 03:13:53 USG6330 %%01ATK/4/FIREWALLATCK(l): AttackType="Udp flood
attack", slot="11", cpu="0", receive interface="GE1/0/1 ", proto="UDP", src="180.226.100.160:59001 91.200.160.160:58003 5.140.90.120:51003 95.150.130.170:15007 ", dst="178.30.180.190:2008 178.30.180.190:16002 ", begin time="2020-1-1 9:11:31", end time="2020-2-2 2:12:52", total packets="20", max speed="29298", User="", Action="discard"

Solution:

a. **Regular expression for Kaspersky Endpoint Security event:**

   ^<(\d+)>1 (\d{4}-\d{2}-\d{2}T\d{2}:\d{2}:\d{2}\.\d{3}Z) (\S+) (\w+)\|([\d.]+) - (\w+) \[event@\d+ et='([^']+)' tdn='([^']+)' etdn='([^']+)' hdn='([^']+)' hip='([^']+)'\].*?Тип события:\s*(.*?)\s*Программа:\s*(.*?)\s*Программа\\Путь:\s*(.*?)\s*Пользователь:\s*(.*?)\s*Компонент:\s*(.*?)\s*Результат\\Описание:\s*(.*?)\s*Объект:\s*(.*?)\s*Объект\\Тип:\s*(.*?)\s*Объект\\Путь:\s*(.*?)\s*Объект\\Название:\s*(.*)$

   Extracted fields:

- Priority
- Timestamp
- Host
- Application (KES)
- Application version
- Event code (0000014f)
- et , tdn , etdn , hdn , hip from the parameter block
- Event Type, Program, Program Path, User, Component, Result, Object, Object Type, Object Path, Object Name

b. Regular expression for TRAPMGR event:

^<(\d+)> (\w{3}\s\d{1,2} \d{2}:\d{2}:\d{2}) (\S+) (\w+)\[(\w+)\]: (\w+\.c\(\d+\)) (\d+) %% (.*?)\\u0000$

Extracted fields:

- Priority
- Date and time (without year)
- Host
- Application (TRAPMGR)
- Process (trapTask)
- File and line (traputil.c(721))
- Event code (3833)
- Message (session and IP-address)

c. Regular expression for UDP flood attack :

^<(\d+)>(\d{4}/\d{2}/\d{2}\s\d{2}:\d{2}:\d{2})\s(\S+)\s%%(\S+):\s*AttackType="([^"]+)",\s*slot="([^"]+)",\s*cpu="([^"]+)",\s*receive\sinterface="([^"]+)",\s*proto="([^"]+)",\s*src="([^"]+)",\s*dst="([^"]+)",\s*begin\stime="([^"]+)",\s*end\stime="([^"]+)",\s*total\spackets="([^"]+)",\s*max\sspeed="([^"]+)",\s*User="([^"]*)",\s*Action="([^"]+)"$

Extracted fields:

- Priority
- Date and time
- Host
- Log ID (01ATK/4/FIREWALLATCK)
- Attack type, slot, CPU, interface, protocol, source and target IP:ports , start/end time, packets, speed, user, action.