

Задание №1

Необходимо подготовить конфигурационный файл audit.rules для службы auditd и настроить службы auditd и rsyslog таким образом, чтобы при попытке доступа к файлам shadow, sudoers и passwd из директории /etc, система отправляла соответствующие события на удаленный syslog-сервер. Также, необходимо настроить отправку событий при попытке изменения системного времени.

Решение:

Настройка **клиента** на примере OS Ubuntu 2024.04.2:

1. В первую очередь нужно скачать пакеты auditd и rsyslog командой – `sudo apt install auditd && sudo apt install rsyslog`
2. После этого мы настраиваем правила в конфигурационном файле audit.rules, открываем его командой - `sudo nano /etc/audit/rules.d/audit.rules`.

Вносим правила в файл:

```
# Мониторинг доступа к критическим файлам
-w /etc/shadow -p wa -k shadow_access
#Следит за файлом /etc/shadow, записывает события если происходит запись или
изменение атрибутов файла, помечает событие ключом shadow_access чтобы легче
было искать в логах
-w /etc/sudoers -p wa -k sudoers_access
#Аналогично для /etc/sudoers (файл с правами sudo) и /etc/passwd (файл с учетными
записями)
-w /etc/passwd -p wa -k passwd_access

# Мониторинг изменения системного времени
-a always,exit -F arch=b64 -S clock_settime,settimeofday -k time_change
#записывает событие при выходе из системного вызова (т. е. после выполнения
действия), фильтрует для 64-битных систем, следит за вызовами функций изменения
времени, ставит метку для событий изменения времени
-a always,exit -F arch=b32 -S clock_settime,settimeofday -k time_change
#Делает все тоже самое только для 32-битных систем
```

В итоге должно получиться так:

```
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. Далее настраиваем плагин syslog для auditd – `sudo nano /etc/audit/plugins.d/syslog.conf`

Изначально конфигурационный файл выглядит так:

```
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
```

Мы его приводим к такому виду:

```
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
```

Активируем плагин установив `active = yes`

Меняем в строке `type` `always` на `builtin` (`always` — это некорректное значение, параметр `type` определяет, является ли плагин встроенным (`builtin`) или внешним (`external`). Значение `always` здесь недопустимо и может вызвать ошибки).

4. Настройка rsyslog

Теперь нужно настроить `rsyslog`, чтобы он пересылал логи `auditd` на удаленный сервер.

Команда: `sudo nano /etc/rsyslog.d/audit_remote.conf`

Вносим правила в файл:

```
# Для TCP-пересылки
$ModLoad imtcp
# Загрузить модуль для поддержки TCP
$InputTCPServerRun 514
# Разрешить rsyslog принимать входящие подключения через TCP на порт 514

# Фильтр событий auditd по тегу
:programname, isequal, "audit" @192.168.1.143:514
#Все логи, сгенерированные программой auditd, будут отправлены на удаленный
сервер 192.168.1.143 через порт 514 по UDP.
```

Должно получиться так:

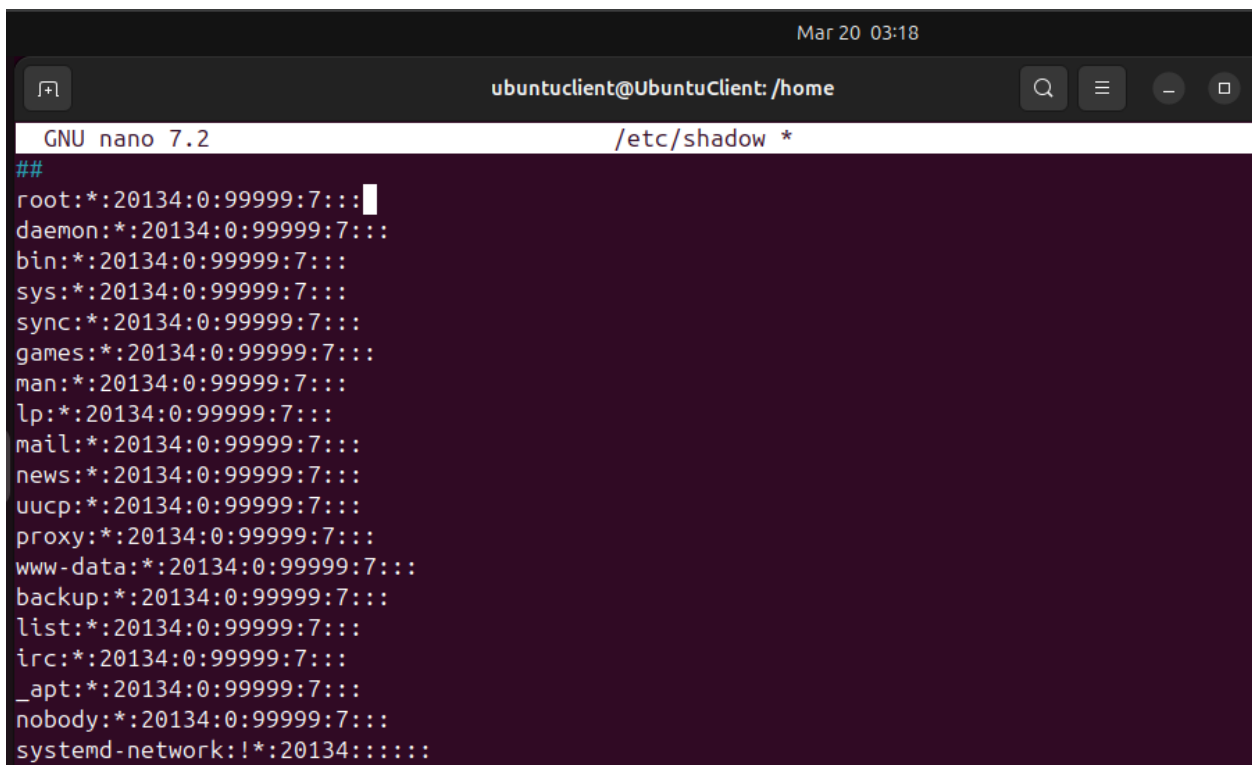
```
GNU nano 7.2 /etc/rsyslog.d/audit_remote.conf
#TCP
$ModLoad imtcp
$InputTCPServerRun 514

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

5. Перезапуск служб
`sudo systemctl restart auditd rsyslog`
6. Проверка аудит прав
`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. Выполним тестовое событие (отредактируем файл, добавим сверху знаки ## и сохраним)
`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-networkd:*:20134:0:99999:7:::
```

8. Теперь проверим локальные логи на событие
`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"
-----
```

Событие действительно произошло

9. Также сделаем тоже самое для файлов passwd и sudoers

```
Mar 20 03:25
ubuntucient@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:/v
# 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
```

Событие появляется тоже

```
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="/" 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

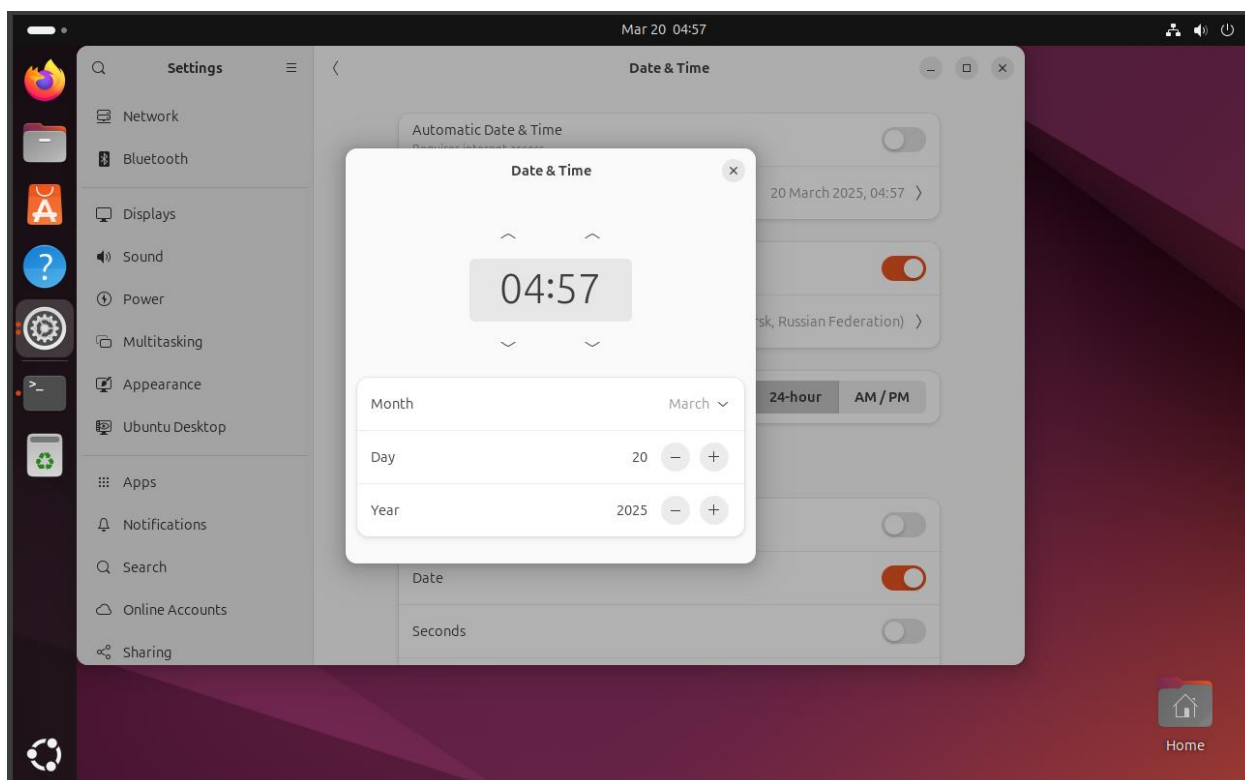
```
Mar 20 03:29
ubuntuclient@UbuntuClient: /home
GNU nano 7.2 /etc/passwd *
##
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
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
```

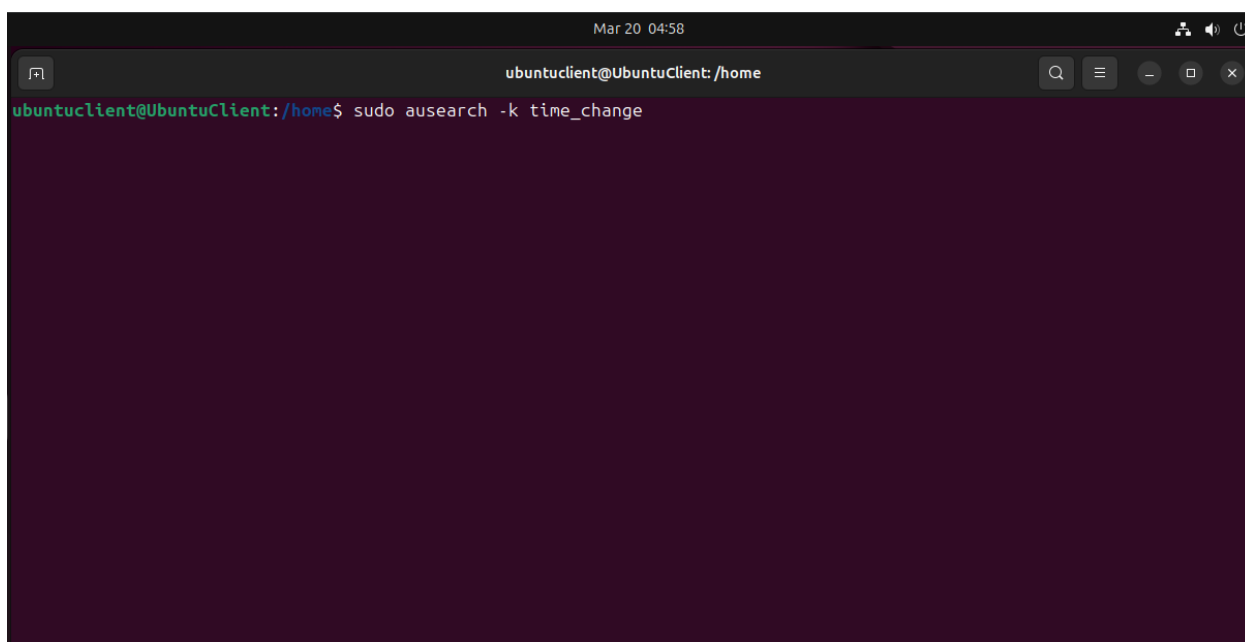
Событие

```
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"
```

А также проверим события на изменение времени в системе, установим время на час вперед



События также появляются



```
Mar 20 04:59
ubuntuclient@UbuntuClient: /home
type=SOCKADDR msg=audit(1742414802.161:699): saddr=1000000000000000000000000000000000
type=SYSCALL msg=audit(1742414802.161:699): arch=c000003e syscall=44 success=yes exit=1068 a0=3 a1=7fff991d3110 a2=42c
a3=0 items=0 ppid=4061 pid=4072 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=
4294967295 comm="auditctl" exe="/usr/sbin/auditctl" subj=unconfined key=(null)
type=CONFIG_CHANGE msg=audit(1742414802.161:699): auid=4294967295 ses=4294967295 subj=unconfined op=add_rule key="time_
change" list=4 res=1
-----
time->Thu Mar 20 03:06:42 2025
type=PROCTITLE msg=audit(1742414802.162:700): proctitle=2F7362696E2F617564697463746C002D52002F6574632F61756469742F61756
469742E72756C6573
type=SOCKADDR msg=audit(1742414802.162:700): saddr=1000000000000000000000000000000000
type=SYSCALL msg=audit(1742414802.162:700): arch=c000003e syscall=44 success=yes exit=1068 a0=3 a1=7fff991d3110 a2=42c
a3=0 items=0 ppid=4061 pid=4072 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=
4294967295 comm="auditctl" exe="/usr/sbin/auditctl" subj=unconfined key=(null)
type=CONFIG_CHANGE msg=audit(1742414802.162:700): auid=4294967295 ses=4294967295 subj=unconfined op=add_rule key="time_
change" list=4 res=1
-----
time->Thu Mar 20 03:57:02 2025
type=PROCTITLE msg=audit(1742417822.388:944): proctitle="/usr/lib/systemd/systemd-timedated"
type=TIME_INJ_OFFSET msg=audit(1742417822.388:944): sec=3597 nsec=610003662
type=SYSCALL msg=audit(1742417822.388:944): arch=c000003e syscall=227 success=yes exit=0 a0=0 a1=7ffe47c8f110 a2=67db3d
ac 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-timedated" subj=unconfined key="time_change"
ubuntuclient@UbuntuClient: /home$
```

Теперь надо настроить **сервер** также на примере OS Ubuntu 2024.04.2:

1. Установка rsyslog
`sudo apt update && sudo apt install rsyslog`

2. Редактируем конфигурационный файл
`sudo nano /etc/rsyslog.conf`

3. Раскомментируем строки

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

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

4. Вносим правило после модулей imudp, imtcp

```
# Шаблон для сохранения логов по хостам и программам
$template RemoteLogs,"/var/log/remote/%HOSTNAME%/%PROGRAMNAME%.log"
```

```
# Применить шаблон ко всем входящим сообщениям
*. * ?RemoteLogs
```


В итоге должно получиться так

```
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. Создаем директорию для логов и даём ей права
sudo mkdir -p /var/log/remote
sudo chmod -R 755 /var/log/remote
6. Перезапускаем rsyslog после настроек
sudo systemctl restart rsyslog
7. Настраиваем фаервол для приема tcp и udp протоколов

Для UDP

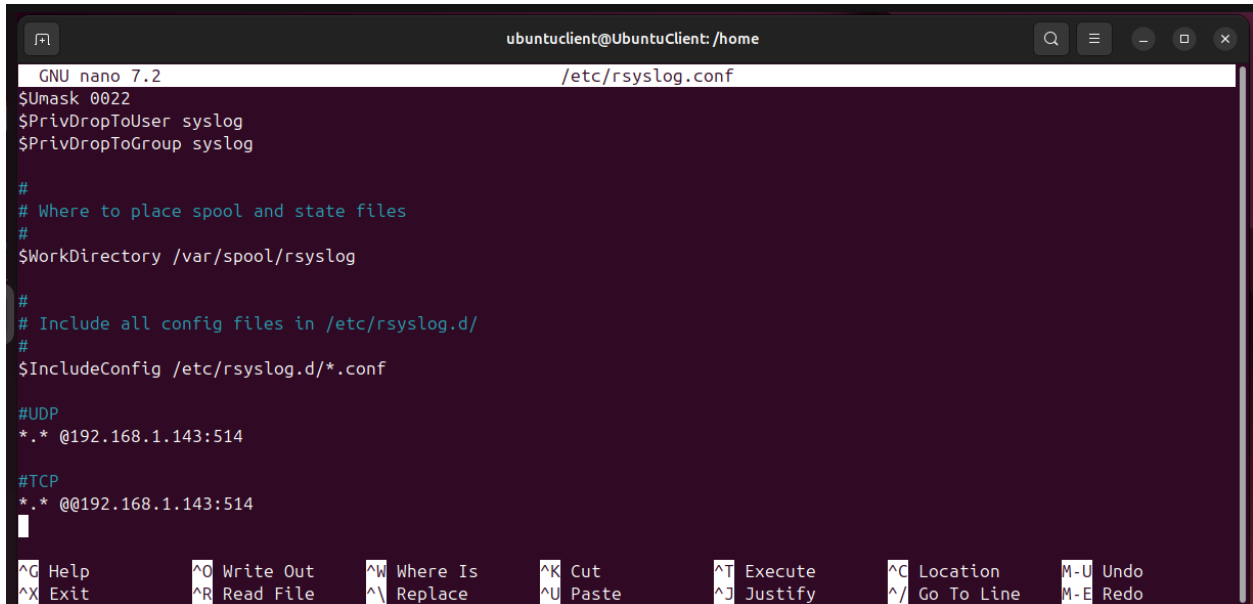
sudo ufw allow 514/udp

Для TCP

sudo ufw allow 514/tcp

8. На клиенте тоже настраиваем файл rsyslog.conf
Добавляем в конец файла

```
*. * @192.168.1.143:514      # Для UDP
*. * @@192.168.1.143:514    # Для TCP
```



```
GNU nano 7.2 /etc/rsyslog.conf
$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

#UDP
*. * @192.168.1.143:514

#TCP
*. * @@192.168.1.143:514
|
```

9. Проверка работы записи логов на сервере

Из наших настроек становится понятно что все логи удаленного клиента будут храниться в файле по пути /var/log/remote/UbuntuClient/audisp-syslog.log

Проверим логи по файлу shadow, командой `grep 'shadow_access' /var/log/remote/UbuntuClient/audisp-syslog.log`



```
root@Ubuntu: /var/log/remote/UbuntuClient
GID="root" FSGID="root"
2025-03-20T03:17:06+07:00 UbuntuClient audisp-syslog: type=SYSCALL msg=audit(1742415426.163:784): arch=c000003e syscall=
257 success=yes exit=3 a0=ffffff9c a1=60630bccda0 a2=241 a3=1b6 items=2 ppid=4159 pid=4160 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"
ARCH=x86_64 SYSCALL=openat AUID="ubuntuclient" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" S
GID="root" FSGID="root"
2025-03-20T03:17:06+07:00 UbuntuClient audisp-syslog: type=SYSCALL msg=audit(1742415426.163:784): arch=c000003e syscall=
257 success=yes exit=3 a0=ffffff9c a1=60630bccda0 a2=241 a3=1b6 items=2 ppid=4159 pid=4160 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"
ARCH=x86_64 SYSCALL=openat AUID="ubuntuclient" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" S
GID="root" FSGID="root"
2025-03-20T03:18:25+07:00 UbuntuClient audisp-syslog: 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"
ARCH=x86_64 SYSCALL=openat AUID="ubuntuclient" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" S
GID="root" FSGID="root"
2025-03-20T03:18:25+07:00 UbuntuClient audisp-syslog: 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"
ARCH=x86_64 SYSCALL=openat AUID="ubuntuclient" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" S
GID="root" FSGID="root"
2025-03-20T03:19:21+07:00 UbuntuClient audisp-syslog: type=SYSCALL msg=audit(1742415561.502:798): arch=c000003e syscall=
257 success=yes exit=3 a0=ffffff9c a1=5712a8263a40 a2=241 a3=1b6 items=2 ppid=4175 pid=4176 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"
ARCH=x86_64 SYSCALL=openat AUID="ubuntuclient" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" S
GID="root" FSGID="root"
2025-03-20T03:19:21+07:00 UbuntuClient audisp-syslog: type=SYSCALL msg=audit(1742415561.502:798): arch=c000003e syscall=
257 success=yes exit=3 a0=ffffff9c a1=5712a8263a40 a2=241 a3=1b6 items=2 ppid=4175 pid=4176 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"
ARCH=x86_64 SYSCALL=openat AUID="ubuntuclient" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" S
GID="root" FSGID="root"
```

Проделаем также для **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="ubuntucient" 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="ubuntucient" 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="ubuntucient" 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="ubuntucient" 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=5757a5b6e540 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="ubuntucient" 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="ubuntucient" 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="ubuntucient" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" S
GID="root" FSGID="root"
root@Ubuntu: /var/log/remote/UbuntuClient#
```

Изменение времени

```
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#
```

Задание №2

В Active Directory у пользователей есть атрибуты msRADIUSFramedIPAddress и msRASSavedFramedIPAddress. В данном атрибуте хранится информация об IP-адресе, который назначается на вкладке Dial-in в свойствах пользователя. Необходимо написать скрипт на powershell, который выведет список всех пользователей Active Directory, у которых заполнен данный атрибут и сконвертирует значение атрибута в читаемый IP-адрес. Например, значение атрибута msRADIUSFramedIPAddress -1062666676 соответствует IP-адресу 192.168.254.76

Решение:

```
# Импорт модуля Active Directory
```

```
Import-Module ActiveDirectory
```

```
# Функция для преобразования целого числа в IP-адрес
```

```
function Convert-IntToIP {  
    param(  
        [int]$Integer  
    )  
    $bytes = [BitConverter]::GetBytes($Integer)  
    [Array]::Reverse($bytes)  
    return ([System.Net.IPAddress]::new($bytes)).ToString()  
}
```

```
# Получение всех пользователей с заполненными атрибутами
```

```
$users = Get-ADUser -Filter * -Properties msRADIUSFramedIPAddress, msRASSavedFramedIPAddress |  
    Where-Object { $_.msRADIUSFramedIPAddress -or $_.msRASSavedFramedIPAddress }
```

```
# Обработка и вывод результатов
```

```
$result = foreach ($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 }  
}
```

```
# Вывод результата в табличном формате
```

```
$result | Format-Table -AutoSize
```

Пояснение:

1. Импорт модуля: Загружает модуль ActiveDirectory для работы с AD.
2. Функция преобразования числа в IP:
 - Convert-IntToIP конвертирует 32-битное целое число в IP-адрес.
 - [BitConverter]::GetBytes() преобразует число в массив байт (little-endian).
 - [Array]::Reverse() меняет порядок байт на big-endian (сетевой формат).
3. Получение пользователей:
 - Фильтр -Filter * выбирает всех пользователей.
 - Properties загружает нужные атрибуты.
 - Where-Object фильтрует пользователей с заполненными атрибутами.
4. Формирование результата:
 - Для каждого пользователя создается объект с именем, логином и IP-адресами.
 - Преобразование выполняется только для непустых атрибутов.
5. Вывод результатов в удобном табличном формате.

Пример вывода:

Name	SamAccountName	FramedIP	SavedFramedIP
----	-----	-----	-----
User1	Ivan	192.168.1.100	10.0.0.50
User2	Vladimir	192.168.1.101	

Задание №3

Напишите регулярные выражения для указанных ниже событий с устройств:

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"

Решение:

a. Регулярное выражение для события Kaspersky Endpoint Security:

```
^<(\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*(.*)$
```

Извлекаемые поля:

- Приоритет
- Временная метка
- Хост
- Приложение (KES)
- Версия приложения
- Код события (0000014f)
- et, tdn, etdn, hdn, hip из блока параметров
- Тип события, Программа, Путь программы, Пользователь, Компонент, Результат, Объект, Тип объекта, Путь объекта, Название объекта

b. Регулярное выражение для TRAPMGR события:

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

Извлекаемые поля:

- Приоритет
- Дата и время (без года)
- Хост
- Приложение (TRAPMGR)
- Процесс (trapTask)
- Файл и строка (traputil.c(721))
- Код события (3833)
- Сообщение (сессия и IP-адрес)

c. Регулярное выражение для атаки UDP flood:

```
^<(\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="([\^]+)"$
```

Извлекаемые поля:

- Приоритет
- Дата и время
- Хост
- Идентификатор лога (01ATK/4/FIREWALLATCK)
- Тип атаки, слот, CPU, интерфейс, протокол, исходные и целевые IP:порты, время начала/окончания, пакеты, скорость, пользователь, действие.