Домашнее задание к уроку №6 Криптография.

Группа: Cyb07-onl

Студент: Парфимович Алексей

1. Создание ключей SSH на Kali Linux.

Экспортировать открытый ключ на сервер Ubuntu Server. Настроить конфиг SSH для аутентификации по ключам. Выполнить подключение SSH по ключу, сохранить скрин экрана, после чего удалить соданные SSH ключи на ВМ Kali и Ubuntu.

Создание SSH-пары ключей на Kali Linux

Открыть терминал на Kali Linux и выполнить:

ssh-keygen -t ed25519 -C "parfimovich@tut.by"

Где

ed25519 — алгоритм шифрования (если ed25519 не поддерживается - можно использовать rsa -b 4096).

Далее:

- Задать путь для создания файлов ключей (по умолчанию ~/.ssh/id_ed25519).
- Задать парольную фразу (passphrase) для дополнительной защиты.

В результате будут созданы два файла:

- Приватный ключ ~/.ssh/id_ed25519
- Публичный ключ ~/.ssh/id_ed25519.pub

Копирование публичного ключа на сервер Ubuntu

В терминал выполнить:

ssh-copy-id -i ~/.ssh/id_ed25519.pub user@192.168.2.100

Где:

user — имя пользователя на Ubuntu-сервере

192.168.2.100 — IP-адрес сервера

```
┌──(user㉿kali)-[~]
└─$ ssh-keygen -t ed25519 -C "parfimovich@tut.by"
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/user/.ssh/id_ed25519):
Created directory '/home/user/.ssh'.
Enter passphrase for "/home/user/.ssh/id_ed25519" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/user/.ssh/id_ed25519
Your public key has been saved in /home/user/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:qY0be6H1eu1KFKFXBrEDb5ODv7Dcpo/gra1ajn+tauw parfimovich@tut.by
The key's randomart image is:
+--[ED25519 256]--+
|        . +oo    |
|         = *     |
|        o @      |
|         = =     |
|        S o      |
|       =o= .     |
|     .*o++=.     |
|     =+Bo=+ .    |
|    o=E*B=oo.    |
+----[SHA256]-----+

┌──(user㉿kali)-[~]
└─$ ssh-copy-id -i ~/.ssh/id_ed25519.pub user@192.168.2.100
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/user/.ssh/id_ed25519.pub"
The authenticity of host '192.168.2.100 (192.168.2.100)' can't be established.
ED25519 key fingerprint is SHA256:8xh50OE9fcNBTk4D9jvkiJK9d4qaQ+/C+57y07R9XOM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
user@192.168.2.100's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh -i /home/user/.ssh/id_ed25519 'user@192.168.2.100'"
and check to make sure that only the key(s) you wanted were added.


┌──(user㉿kali)-[~]
└─$
```

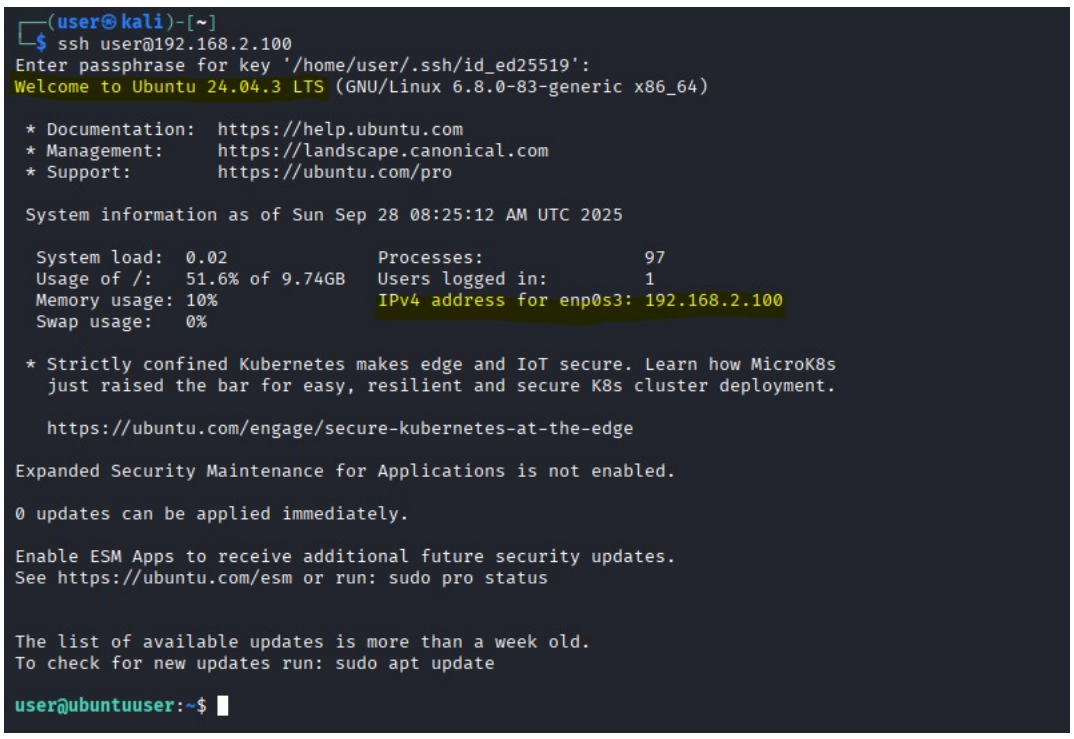
Проверка подключения

С ВМ Kali выполнить подключение к ВМ Ubuntu:

ssh username@ip_адрес_сервера

Далее:

- ввести passphrase
- выполнится вход без пароля



2. Установка 2FA с TOTP токеном на Ubuntu Server.

Выполнить конфигурацию и выдачу токена пользователю. Подключиться с ВМ Kali на ВМ Ubuntu с использованием TOTP, сделать скрин экрана.

Установка и настройка 2FA на Ubuntu-сервере

1. Обновить систему

Выпонить команду:

sudo apt update && sudo apt upgrade -y

2. Установить libpam-google-authenticator

Выполнить команду:

sudo apt install libpam-google-authenticator -y

Примечание:

- данный пакет реализует стандарт TOTP (RFC 6238) и совместим с любыми TOTP-приложениями (Google Authenticator, Authy, Microsoft Authenticator, FreeOTP и др.).

3. Запустить генератор TOTP для локального пользователя

Выполнить команду:

google-authenticator

Далее будут заданы вопросы (в конце строк приведены ответы):

- Do you want authentication tokens to be time-based (y/n)? → y
  на экране отобразятся QR-код, секретный ключ и список одноразовых аварийных кодов
- Do you want me to update your "~/.google_authenticator" file? → y
- Do you want to disallow multiple uses of the same authentication token? → y
- By default, tokens are good for 30 seconds... Do you want to increase the window? → n
- If the computer time is ever more than 1 minute off... Do you want to do so? → y

Необходимо обязательно сохранить QR-код (сфотографировать или сделать копию экрана), Секретный ключ (на случай, если не сможете отсканировать QR), 5 аварийных кодов

Файл ~/.google_authenticator будет создан автоматически с правильными правами.

4. Настроить PAM для использования 2FA в файле PAM для SSH:

Открыть файл:

sudo nano /etc/pam.d/sshd

Добавить в начало файла (сразу после @include common-auth):

auth required pam_google_authenticator.so

5. Настроить SSH-демона в файле конфигурации SSH

Открыть файл:
sudo nano /etc/ssh/sshd_config

Включить следующие параметры для использования пароля + 2FA:
KbdInteractiveAuthentication=yes
UsePAM=yes

Перезапусть SSH:
sudo systemctl restart ssh

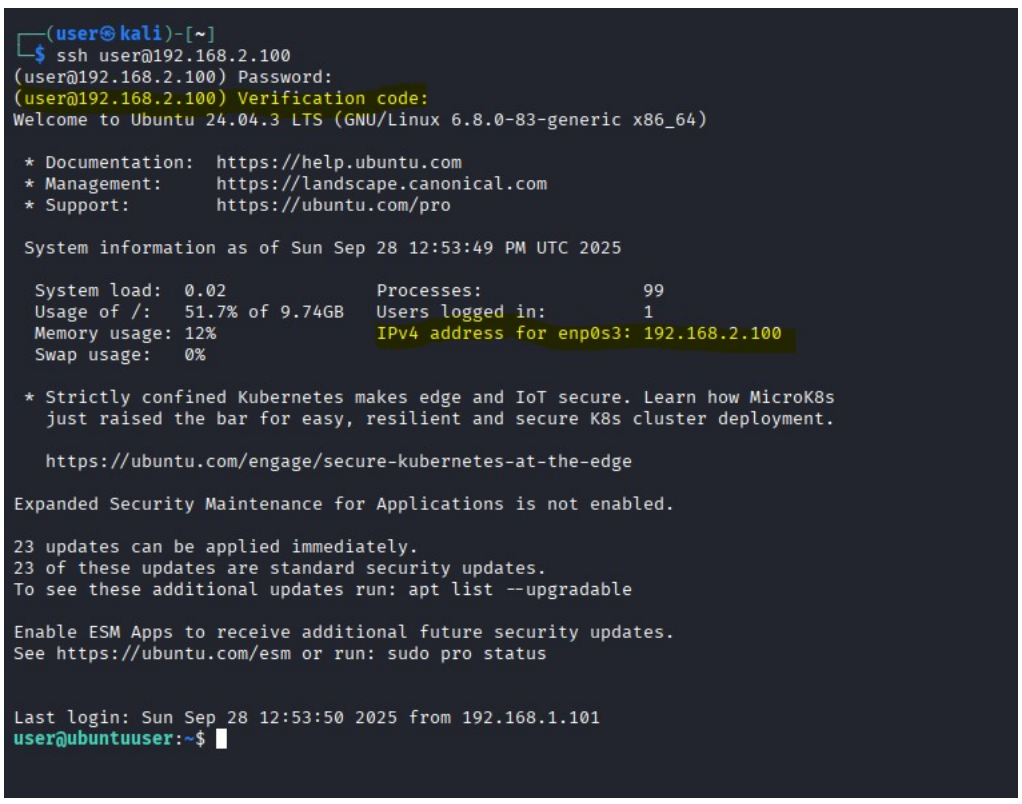
Настройка TOTP-приложения на клиенте

Установить TOTP-приложение на смартфон (Microsoft Authenticator)
Открыть приложение → «Добавить аккаунт» → «Сканировать QR-код».
Отсканировать QR-код, показанный на сервере при запуске google-authenticator,
или вручную ввести секретный ключ и указать тип «Time-based».

Теперь приложение будет генерировать 6-значные коды каждые 30 секунд.

Подключение с удалённой машины

Выполнить команду:
ssh user@192.168.2.100
Система запросит:
- Password (пароль пользователя)
- Verification code (TOTP-код из приложения)



3. На сервере Ubuntu развернуть и настроить ftp сервер(vsftpd).

Подключиться к FTP серверу с ВМ Kali и отправить туда любой файл, сохранить скрин об успешной отправке файла.

1. Установка vsftpd

```
sudo apt install vsftpd -y
```

2. Настройка vsftpd

Открыть конфигурационный файл:

```
sudo nano /etc/vsftpd.conf
```

Проверить установку параметров:

```
local_enable=YES  # Разрешить локальных пользователей
write_enable=YES  # Разрешить запись (загрузку файлов)
chroot_local_user=YES # Ограничить пользователей в их домашних каталогах (chroot)
allow_writeable_chroot=YES  # Запретить выход из домашнего каталога
anonymous_enable=NO # Отключить анонимный доступ
xferlog_enable=YES  # Включить логирование
xferlog_file=/var/log/vsftpd.log
```

Перезапустить службу:

```
sudo systemctl restart vsftpd
sudo systemctl enable vsftpd  # автозапуск при загрузке
```

Проверить статус службы:

```
sudo systemctl status vsftpd
```

```
user@ubuntuuser:~$ sudo systemctl status vsftpd
● vsftpd.service - vsftpd FTP server
     Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; enabled; preset: enabled)
     Active: active (running) since Sun 2025-09-28 13:53:12 UTC; 48s ago
    Process: 3372 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
   Main PID: 3374 (vsftpd)
      Tasks: 1 (limit: 2268)
     Memory: 712.0K (peak: 2.0M)
        CPU: 38ms
     CGroup: /system.slice/vsftpd.service
             └─3374 /usr/sbin/vsftpd /etc/vsftpd.conf

Sep 28 13:53:12 ubuntuuser systemd[1]: Starting vsftpd.service - vsftpd FTP server...
Sep 28 13:53:12 ubuntuuser systemd[1]: Started vsftpd.service - vsftpd FTP server.
user@ubuntuuser:~$
user@ubuntuuser:~$ ftp localhost
Connected to localhost.
220 (vsFTPd 3.0.5)
Name (localhost:user): user
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||23689|)
150 Here comes the directory listing.
226 Directory send OK.
ftp> _
```

3. Настройка брандмауэра (UFW)

Выполнить команды:

```
sudo ufw allow 20:21/tcp
sudo ufw allow 40000:50000/tcp  # для пассивного режима
```

4. Протестировать подключение

Подключение с локальной машины:

```
ftp localhost
```

Подключение с удалённой машины (Kali):

```
ftp 192.168.2.100
```

Загрузка-выгрузка файлов выполняется командами Put и Get

```
┌──(user㉿kali)-[~]
└─$ echo Hello Ubuntu!!! > test-hello.txt
echo Hello Ubuntuftp 192.168.2.100! > test-hello.txt

┌──(user㉿kali)-[~]
└─$ cat test-hello.txt
Hello Ubuntuftp 192.168.2.100!

┌──(user㉿kali)-[~]
└─$ ftp 192.168.2.100
Connected to 192.168.2.100.
220 (vsFTPd 3.0.5)
Name (192.168.2.100:user): user
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get test-hello.txt
local: test-hello.txt remote: test-hello.txt
229 Entering Extended Passive Mode (|||34231|)
550 Failed to open file.
ftp>
ftp> put test-hello.txt
local: test-hello.txt remote: test-hello.txt
229 Entering Extended Passive Mode (|||27684|)
150 Ok to send data.
100% |**********************************************************************************************|    31      219.37 KiB/s    00:00 ETA
226 Transfer complete.
31 bytes sent in 00:00 (4.89 KiB/s)
ftp>
```

4. В PfSense настроить блокирующее правило

Floating: src.ip=kali, dst.ip=ubuntu, dst.port=20,21, protocol=tcp.
Настроить логирование этого правила и сохранить скрин блокировки в логах.