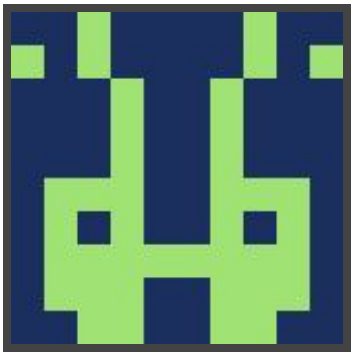


Lame

9th October 2017 / Document No D17.100.12

Prepared By: Alexander Reid (Arrexel)

Machine Author: ch4p

Difficulty: Easy

Classification: Official

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

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

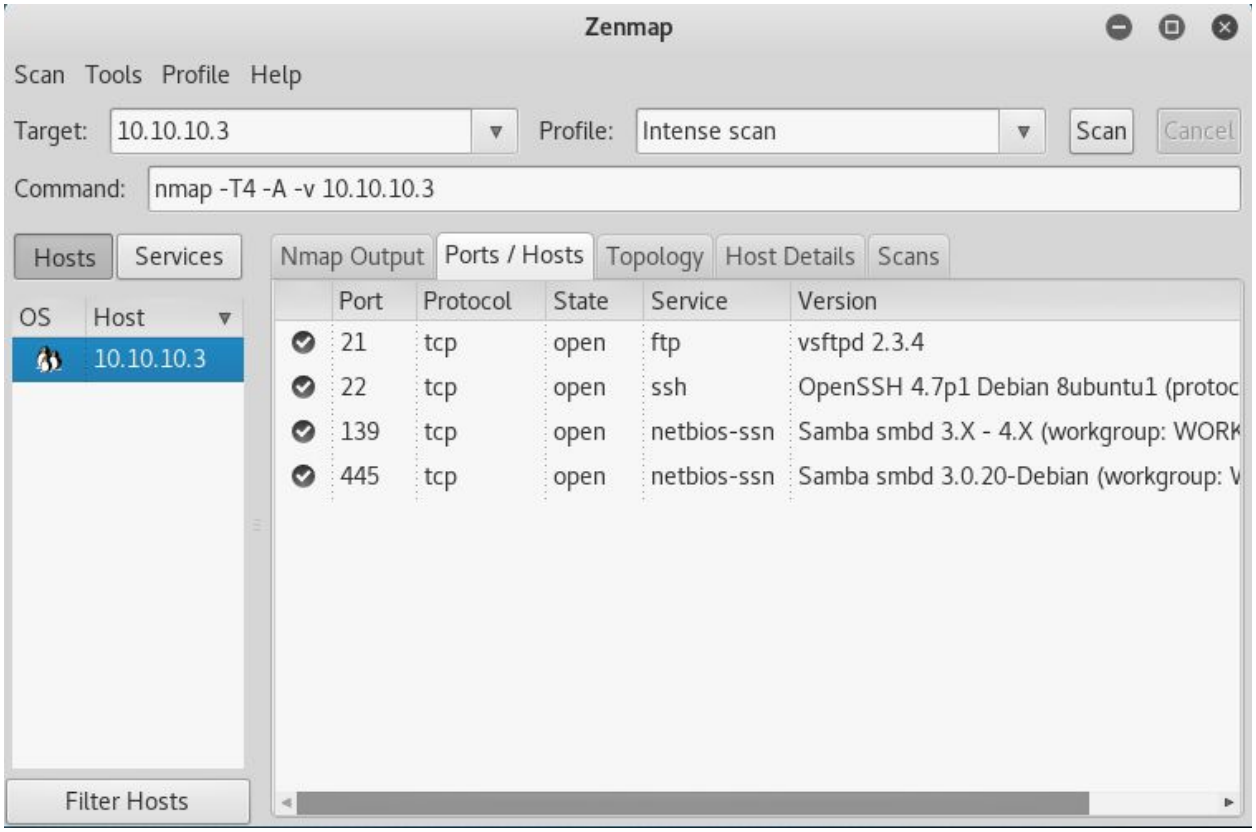
Skills Learned

- Identifying vulnerable services
- Exploiting Samba

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

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.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

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