Information Gathering

1) Checked open ports

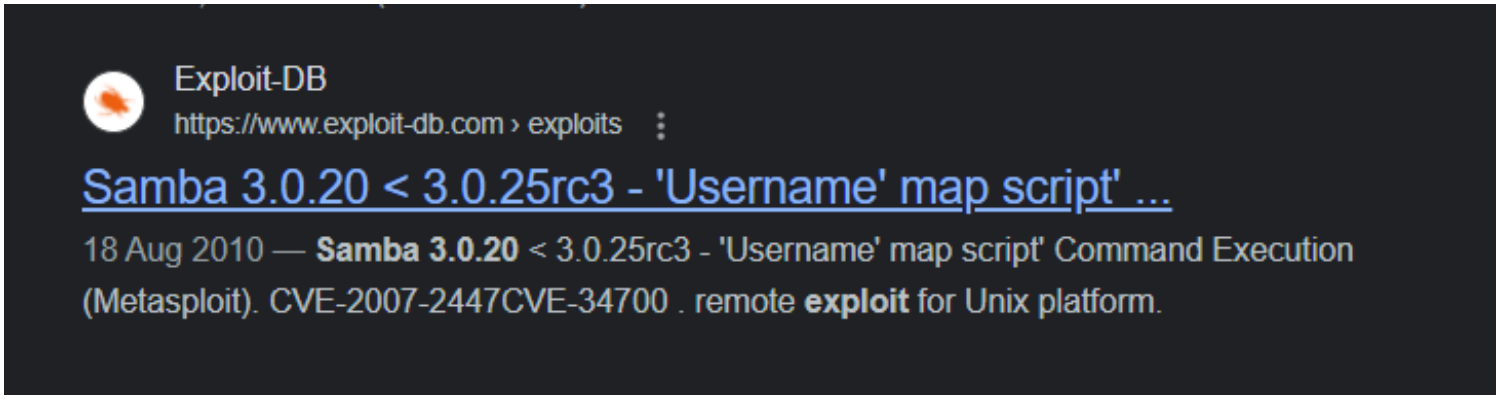
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap 10.10.10.3 --min-rate 1000 -sV -p-
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-18 23:19 IST
Nmap scan report for 10.10.10.3
Host is up (0.35s latency).
Not shown: 65530 filtered tcp ports (no-response)
PORT     STATE SERVICE     VERSION
21/tcp   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)
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

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)-[~]
└─$ sudo 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



Exploitation

1) Exploited with metasploit