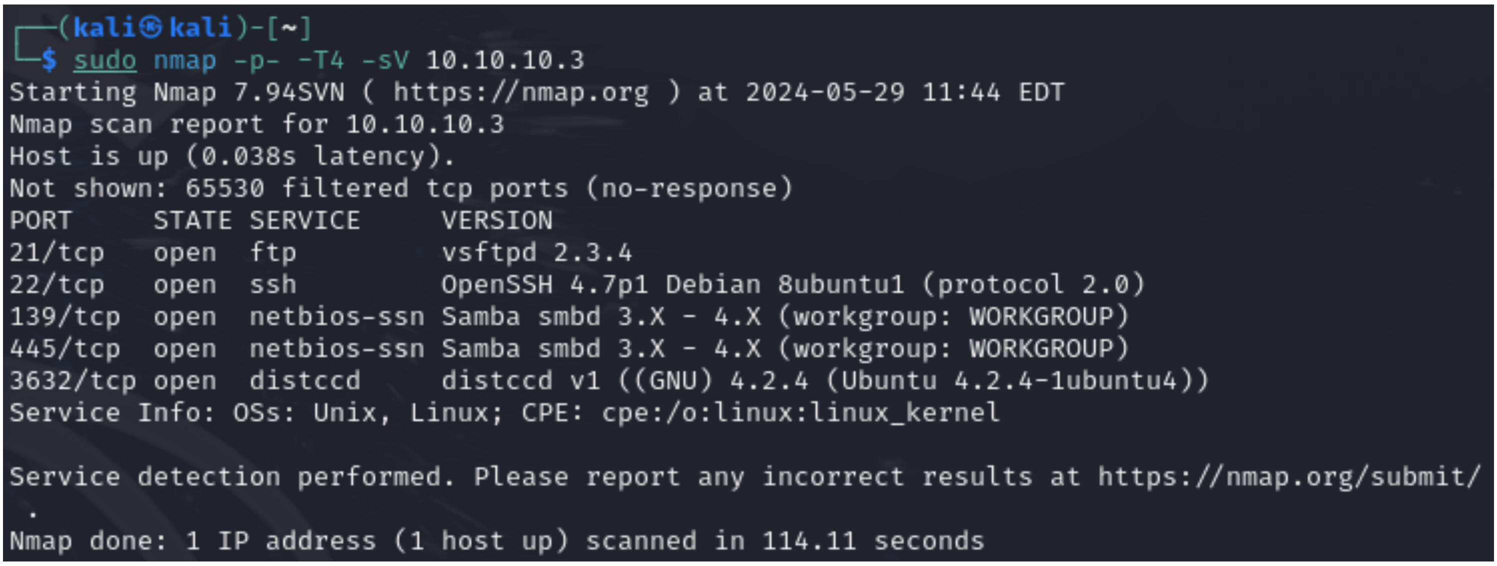
scanning

nmap



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- -T4 -sV 10.10.10.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-29 11:44 EDT
Nmap scan report for 10.10.10.3
Host is up (0.038s 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 114.11 seconds
```

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 2.6.23 (91%), DD-WRT v24-sp1 (Linux 2.4.36) (90%), Arris TG862G/CT cable modem (90%), Dell Integrated Remote Access Controller (iDRAC6) (90%), Linksys WET54GS5 WAP, Tranzeo TR-CPQ-19f WAP, or Xerox WorkCentre Pro 265 printer (90%), Linux 2.4.21 - 2.4.31 (likely embedded) (90%), Linux 2.4.27 (90%), Linux 2.4.7 (90%), Linux 2.6.22 (90%), Linux 2.6.27 - 2.6.28 (90%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

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 103.37 seconds

Metasploit

```
[*] 10.10.10.3:445      - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)
[*] 10.10.10.3:445      -   Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 10.10.10.3:         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

exploits

VSFTPD_v2.3.4

VSFTPD v2.3.4 Backdoor Command Execution

Not working
https://www.exploit-db.com/exploits/49757
https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor/

Samba_v3.0.20

https://www.exploit-db.com/exploits/16320
Based from exploit-db, use Metasploit module: exploit/multi/samba/usermap_script