**Task 2: Port Scanning and Banner Grabbing**

**Task 2: Port Scanning and Banner Grabbing**

* **Command:** Perform a port scan on an identified host and attempt banner grabbing to detect service details.
* **Example Command for Banner Grabbing:** nmap -sV -p 80 <target IP>
* **Report:** Describe the ports discovered, services running, and any banner information obtained.

1. **nmap -sV -p 80 192.168.0.170**

Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-20 15:32 +0530

Nmap scan report for 192.168.0.170

Host is up (0.0010s latency).

PORT STATE SERVICE VERSION

**80/tcp closed http**

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

Nmap done: 1 IP address (1 host up) scanned in 1.21 seconds

1. **nmap -sV -p 80,443 www.cisco.com**

Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-20 15:35 +0530

Nmap scan report for www.cisco.com (23.209.254.61)

**Host is up (0.0090s latency).**

Other addresses for www.cisco.com (not scanned): 2600:1417:73:588::b33 2600:1417:73:582::b33

rDNS record for 23.209.254.61: a23-209-254-61.deploy.static.akamaitechnologies.com

**PORT STATE SERVICE VERSION**

**80/tcp open http AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)**

**443/tcp open ssl/http AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)**

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

Nmap done: 1 IP address (1 host up) scanned in 13.39 seconds

1. KALI LINUX

nmap -sV -p- 192.168.65.130

Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-20 18:37 +0530

Nmap scan report for 192.168.65.130

**Host is up (0.00038s latency).**

All 65535 scanned ports on 192.168.65.130 are in ignored states.

**Not shown: 65535 closed tcp ports (reset)**

MAC Address: 00:0C:29:06:6B:CB **(VMware)**

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

Nmap done: 1 IP address (1 host up) scanned in 1.94 seconds

1. metasploitable-linux-2.0.0 – 192.168.65.131

**nmap -sV -p- 192.168.65.131**

Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-20 18:36 +0530

Nmap scan report for 192.168.65.131

Host is up (0.00038s latency).

Not shown: 65506 closed tcp ports (reset)

PORT STATE SERVICE VERSION

**21/tcp open ftp vsftpd 2.3.4**

22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

**23/tcp open telnet Linux telnetd**

**25/tcp open smtp Postfix smtpd**

**80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)**

111/tcp open rpcbind 2 (RPC #100000)

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)**

512/tcp open exec netkit-rsh rexecd

513/tcp open login?

514/tcp open tcpwrapped

1099/tcp open java-rmi GNU Classpath grmiregistry

1524/tcp open bindshell Metasploitable root shell

2049/tcp open nfs 2-4 (RPC #100003)

2121/tcp open ftp ProFTPD 1.3.1

3306/tcp open mysql MySQL 5.0.51a-3ubuntu5

3632/tcp open distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))

5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7

5900/tcp open vnc VNC (protocol 3.3)

6000/tcp open X11 (access denied)

6667/tcp open irc UnrealIRCd

6697/tcp open irc UnrealIRCd

8009/tcp open ajp13 Apache Jserv (Protocol v1.3)

8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1

8787/tcp open drb Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)

34537/tcp open java-rmi GNU Classpath grmiregistry

37365/tcp open status 1 (RPC #100024)

40497/tcp open mountd 1-3 (RPC #100005)

59626/tcp open nlockmgr 1-4 (RPC #100021)

MAC Address: 00:0C:29:90:CA:F0 (**VMware**)

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; **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 128.56 seconds

1. **REPORT**

Here's a structured **banner grabbing and vulnerability analysis report** based on your nmap -sV -p- 192.168.65.131 scan.

**🔐 Banner Grabbing & Vulnerability Assessment Report**

**Target IP:** 192.168.65.131  
**Scan Command Used:** nmap -sV -p- 192.168.65.131  
**Scan Time:** 2025-07-20 18:36 IST  
**Tool Used:** Nmap 7.97 (Version Detection Enabled)

**✅ 1. Banner Grabbing Summary**

The following table lists the open ports, detected service versions, and known associated risks:

| **Port** | **Service** | **Version** | **Banner/Notes** | **CVE/Threat** | **Risk Level** |
| --- | --- | --- | --- | --- | --- |
| 21 | FTP | vsftpd 2.3.4 | Vulnerable version | **CVE-2011-2523** – backdoor | 🔴 High |
| 22 | SSH | OpenSSH 4.7p1 | Outdated | Multiple CVEs (e.g., CVE-2008-4109) | 🟠 Medium |
| 23 | Telnet | Linux telnetd | Unencrypted login | Credential sniffing, brute force | 🔴 High |
| 25 | SMTP | Postfix smtpd | Email relay/open relay risk | CVE-2011-1720 | 🟠 Medium |
| 80 | HTTP | Apache 2.2.8 (Ubuntu) | Outdated, vulnerable to DoS, buffer overflow | **CVE-2007-6388**, CVE-2009-3555 | 🔴 High |
| 111 | RPCBind | v2 | NFS-related RPC service | Used in NFS attacks | 🟠 Medium |
| 139/445 | Samba | smbd 3.x - 4.x | Legacy SMB version | **CVE-2017-7494**, EternalBlue | 🔴 High |
| 512-514 | rsh, login | netkit-rsh, login | Rsh is insecure | Transmits cleartext credentials | 🔴 High |
| 1099 | Java RMI | GNU Classpath | Remote method invocation | RCE via deserialization | 🔴 High |
| 1524 | Bindshell | Metasploitable shell | Backdoor shell | Pre-installed backdoor | 🔴 High |
| 2049 | NFS | v2-4 | NFS share exposure | NFS misconfigurations | 🟠 Medium |
| 2121 | FTP | ProFTPD 1.3.1 | Multiple known vulnerabilities | CVE-2010-4221 | 🔴 High |
| 3306 | MySQL | 5.0.51a | Outdated DB | CVE-2008-2079, weak auth | 🟠 Medium |
| 5432 | PostgreSQL | 8.3.0 | Old version | CVE-2009-3230 | 🟠 Medium |
| 5900 | VNC | Protocol 3.3 | No auth by default | Unauthenticated access | 🔴 High |
| 6667/6697 | IRC | UnrealIRCd | Known trojanized version | **CVE-2010-2075** | 🔴 High |
| 8009 | AJP13 | Apache JServ | May allow ghostcat RCE | **CVE-2020-1938** | 🔴 High |
| 8180 | Tomcat | JSP Engine 1.1 | Likely vulnerable admin console | Weak creds, RCE | 🔴 High |

**⚠️ 2. Vulnerability Mapping (Sample References)**

| **CVE ID** | **Description** |
| --- | --- |
| **CVE-2011-2523** | vsftpd 2.3.4 backdoor vulnerability (port 21) |
| **CVE-2010-2075** | Trojan in UnrealIRCd (ports 6667/6697) |
| **CVE-2020-1938** | Apache Tomcat AJP Ghostcat vulnerability (port 8009) |
| **CVE-2017-7494** | Samba remote code execution (ports 139/445) |

**🛠️ 3. Recommendations**

| **Category** | **Recommendation** |
| --- | --- |
| **Patching** | Upgrade all outdated services: vsftpd, Apache, Samba, SSH, PostgreSQL, MySQL, ProFTPD |
| **Access Control** | Disable Telnet, RSH, and unsecured services; implement SSH-only access |
| **Firewalling** | Restrict access to critical services (e.g., MySQL, PostgreSQL) to trusted IPs only |
| **Authentication** | Enforce strong passwords and multi-factor authentication for SSH and admin portals |
| **Monitoring** | Enable logging and intrusion detection on all public-facing ports |
| **Service Hardening** | Disable unused ports and services (e.g., 1524 bindshell, 1099 RMI unless required) |

**📝 Conclusion:** The target host runs **multiple outdated and vulnerable services**, some with **known remote code execution (RCE) and backdoor vulnerabilities**. Immediate remediation is strongly advised, especially for FTP (21), Telnet (23), Tomcat (8180), Samba (139/445), and AJP (8009).