

# Lab 7 Task: Vulnerability Scoring & Analysis Using the \*Butler\* Pentesting Box

---

## Lab Task: Vulnerability Scoring & Analysis Using the *Butler* Pentesting Box

---

**Objective:** Analyze real vulnerabilities from the *Butler* VM walkthrough. Apply **CVSS scoring**, consult public databases (**NVD**, **Exploit-DB**), and recommend mitigations—without exploitation.

---

### Background Summary

The *Butler* machine (Windows-based) from involves two key phases:

#### 1. Initial Access

- Jenkins web interface on **port 8080**
- Default credentials: `Jenkins:Jenkins`
- **Groovy Script Console** used for **Remote Code Execution (RCE)** → `cmd.exe`

#### 2. Privilege Escalation

- **Unquoted Service Path** vulnerability in the `WiseBootAssistant` service
- Exploited to gain **SYSTEM** privileges

**Note:** This lab is **analysis-only**. No live exploitation permitted.

---

### Your Tasks

#### 1. Identify & Document Vulnerabilities

For **each** vulnerability below:

##### A. Jenkins RCE via Script Console

- **Vulnerability Type:** Misconfiguration + Weak Credentials + Dangerous Feature Exposure
- **Affected Software:** Jenkins (likely ≤ v2.54 or unpatched)
- **Actions:**
  - Search **NVD** (<https://nvd.nist.gov>) for relevant **CVE(s)** (e.g., “Jenkins script console CVE”)
  - Check **Exploit-DB** (<https://www.exploit-db.com>) for public exploits
  - Record:

- CVE ID (if found)
- Affected versions
- Exploit availability (Yes/No)

## B. Unquoted Service Path (WiseBootAssistant)

- **Vulnerability Type:** Windows Misconfiguration
- **Affected Component:** WiseBootAssistant service → C:\Program Files (x86)\Wise\WiseCare 365\BootTime.exe
- **Actions:**
  - Search NVD for “Unquoted Service Path” or **CVE-2015-2291** (example)
  - Confirm if this exact path/service has a CVE
  - Note OS requirements (Windows, service running as SYSTEM)

## 2. Apply CVSS v3.1 Scoring

For **each** vulnerability:

Field	Jenkins RCE	Unquoted Service Path
<b>CVE ID</b>	<input type="text"/>	<input type="text"/>
<b>CVSS Vector</b>	e.g., CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	e.g., CVSS:3.1/AV:L/AC:L/I:H/A:H
<b>Base Score</b>	<input type="text"/> / 10	<input type="text"/> / 10
<b>Severity</b>	<input type="checkbox"/> None <input type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High <input type="checkbox"/> Critical	<input type="checkbox"/> None <input type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High <input type="checkbox"/> Critical
<b>Justification</b>	Explain: Attack Vector (Network), Privileges (None), Impact (Full CIA loss)	Explain: Local attack, low privilege, runs as SYSTEM

 Use the official CVSS calculator: <https://www.first.org/cvss/calculator/3.1>

## 3. Simulated Impact Analysis

Write a short **business impact statement** for ACKme IT Services (fictional client):

*“If our helpdesk portal used Jenkins with default credentials and an exposed script console, an attacker could...”*

Include:

- Data at risk (user info, source code, configs)
- Potential for lateral movement
- Service disruption (e.g., ransomware via SYSTEM access)

Do this for **both** vulnerabilities.

---

## 4. Recommend Mitigations

Provide **two actionable mitigations per vulnerability**:

### Jenkins RCE

1. **Disable Script Console** in production Jenkins instances  
→ Jenkins > Manage Jenkins > *In-process Script Approval*
2. **Enforce strong authentication + Role-Based Access Control (RBAC)**  
→ Never use default credentials; integrate with SSO or LDAP

### Unquoted Service Path

1. **Quote all Windows service paths**  
→ Correct path: "C:\Program Files (x86)\Wise\Wise Care 365\BootTime.exe"
2. **Apply least privilege** to service accounts  
→ Services should **not** run as SYSTEM unless absolutely necessary

Bonus: Cite NIST SP 800-123 or CIS Windows Benchmarks if possible.

---

## Deliverable

Create a **Joplin note** titled:

Lab - Butler VM Vulnerability Scoring

Structure it as:

```
# Lab - Butler VM Vulnerability Scoring

## 1. Vulnerability Identification
...
## 2. CVSS Analysis
...
## 3. Impact Statement
...
## 4. Mitigation Recommendations
...
```

**Ethical Reminder:** This exercise is for **educational analysis only**. Never test systems without explicit authorization.