Penetration Test Report

TryHackMe - Basic Pentesting (practice)

Prepared by

Ambar Roy

Contact: ambarroy11@gmail.com

Report date: October 20, 2025

Engagement type: Practice / Training pentest (CTF-style)
Scope: Basic Pentesting lab on TryHackMe (single VM/challenge)
Tester: Freelance beginner security practitioner

Contents

Executive Summary

This report documents an educational penetration test performed against the TryHackMe *Basic Pentesting* room. The objective was hands-on practice of reconnaissance, enumeration, exploitation and post-exploitation. The tester performed directory and service enumeration, discovered credentials, obtained an initial shell as user `jan`, then escalated/shifted to user `kay` and retrieved the final flag.

Key outcomes:

- Directory enumeration revealed a `/development` directory with informative files.
- Service enumeration identified SMB; user enumeration via Samba revealed usernames.
- SSH credential for `jan` was discovered via password guessing and used for initial access.
- Local enumeration discovered an encrypted SSH private key for `kay`; passphrase was recovered and used to access `kay`.
- Final flag was retrieved under user `kay`.

1 Scope and Rules of Engagement

Scope

- Target: Basic Pentesting VM (TryHackMe)
- IP Address: 10.201.94.210
- Engagement type: Educational / CTF-style

Rules of Engagement

- Only the assigned VM was tested.
- No denial-of-service or destructive actions were performed.
- All findings are for educational purposes and reporting practice.

2 Methodology

The engagement followed a standard workflow:

1. Reconnaissance — identify public directories and services.
2. Enumeration — extract usernames, versions and files of interest.
3. Exploitation — use discovered credentials to gain access.
4. Post-exploitation — local enumeration, credential harvesting and lateral movement.
5. Reporting — document findings, evidence, impact and remediation.

Tools used

- `gobuster` for directory enumeration
- `nmap` for port/service discovery
- `enum4linux` for Samba-based enumeration

- `hydra` for password guessing against SSH
- `linpeas.sh` for local privilege-escalation discovery
- `ssh2john` and `john` for extracting and cracking SSH key passphrases
- `ssh`, `nc` and standard UNIX tools for shells and file access

3 Risk Rating Definitions

- **High:** Immediate risk — full system or credential compromise possible.
- **Medium:** Exploitable weakness that could lead to partial compromise.
- **Low:** Minor information disclosure or configuration issues.

4 Findings

Finding #1 — Reconnaissance and Directory Discovery

Finding #1: Discovery of `/development` directory and informative files Risk: Low

Affected Asset: http://10.201.94.210/development

Summary:
A web directory enumeration revealed the `/development` path which contained two text files (notes) that indicated configuration choices and that SMB had been enabled on the host.

Details and PoC:

```
gobuster dir -u http://10.201.94.210 -w /usr/share/dirbuster/wordlists/
    ↪ directory-list-2.3-medium.txt -t 100
```

`/development` contained two files:

- **j.txt** — Noted that an `/etc/shadow` hash was cracked and advised changing passwords (internal note).
- **dev.txt** — Notes referencing experimentation with Apache Struts (version 2.5.12) and a note that SMB had been configured.

Impact:
Low — information disclosure that helps guide further testing (e.g., check SMB and potentially Struts-related services).

Remediation:

- Remove internal notes and operational comments from publicly-accessible directories.
- Avoid storing sensitive operational details in webroot.

Finding #2 — Service Enumeration and Samba-based User Discovery

Finding #2: SMB detected and user accounts enumerated via enum4linux Risk: Medium

Affected Asset: 10.201.94.210:139,445

Summary:
A targeted service scan revealed SMB services; subsequent Samba-focused enumeration produced two usernames which were used in later attack steps.

Details and PoC: A full service scan was performed:

```
nmap -A 10.201.94.210
```

Notable services discovered:

- 22/tcp — OpenSSH 8.2p1
- 80/tcp — Apache 2.4.41
- 139/tcp, 445/tcp — Samba smbd 4.6.2
- 8009/tcp — AJP (Apache JServ)

- 8080/tcp — Apache Tomcat 9.0.7

Because Samba was detected, Samba enumeration was performed to enumerate shares and users. The exact command executed was:

```
enum4linux -a 10.201.94.210 | tee e4l.log
```

Output from `enum4linux` returned two discovered usernames:

jan and **kay**

Impact:
Medium — discovered usernames reduce the search space for credential-based attacks such as password guessing and credential stuffing.

Remediation:

- Limit SMB exposure to trusted networks and apply proper access controls.
- Monitor and audit SMB activity.
- Avoid revealing account names in public or unauthenticated services where possible.

Finding #3 — Initial Access: SSH Login as `jan` via Password Guessing

Finding #3: SSH access obtained for user `jan` via password guessing **Risk: Medium**

Affected Asset: 10.201.94.210:22

Summary:
Using discovered usernames from Samba enumeration, password guessing against SSH succeeded for user `jan` enabling an initial interactive shell on the host.

Details and PoC: Password guessing was performed with Hydra using a popular wordlist:

```
hydra -l jan -P /usr/share/wordlists/rockyou.txt ssh://10.201.94.210
```

Once the password was identified, SSH login was performed:

```
ssh jan@10.201.94.210 -p 22
```

Result:
A valid shell as user `jan` was obtained.

Impact:
Medium — low-privilege account compromise can be used for local enumeration and to attempt privilege escalation.

Remediation:

- Enforce strong password policies (length, complexity) and account lockout mechanisms.
- Implement multi-factor authentication for remote logins where possible.
- Monitor failed login attempts and alert on brute-force patterns.

Finding #4 — Lateral Movement: Cracking SSH Key Passphrase and Accessing `kay`

Finding #4: Encrypted SSH private key discovered and passphrase cracked to access user `kay` **Risk: High**

Affected Asset: Local (post-exploitation)

Summary:
While enumerating the compromised host as `jan`, an encrypted private key belonging to user `kay` was discovered. The passphrase was extracted by converting the key for John the Ripper and cracking it; the key was then used to SSH into the host as `kay`, and the final flag was retrieved.

Details and PoC: Local enumeration with linPEAS was performed to identify sensitive files and escalation vectors:

```
linpeas.sh | tee linlog.txt
```

An RSA private key file for `kay` was discovered (file name referenced as `kay_id_rsa`). The key was passphrase-protected, so the following steps were taken to recover it:

```
ssh2john kay_id_rsa | tee kay_pass.txt
john kay_pass.txt
```

`john` recovered the passphrase for the private key. The key was then used to authenticate as `kay`:

```
ssh -i kay_id_rsa kay@10.201.94.210
```

Upon successful login as `kay`, the final flag was located and retrieved:

```
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
```

Result:
Full access to user `kay` was achieved and the final flag retrieved.

Impact:
High — exposed private keys or improperly protected keys allow attackers to impersonate users and escalate privileges. Even if keys are encrypted, weak/guessable passphrases can be cracked offline.

Remediation:

- Store private keys securely and restrict filesystem permissions (e.g., `chmod 600`).
- Avoid leaving private keys in shared or world-readable directories.
- Use strong passphrases and consider hardware-backed key storage (YubiKey, etc.).
- Monitor for unexpected key files or transfers and rotate keys when compromise is suspected.

Appendices

Appendix A — Commands and Tools

```
# Directory enumeration
gobuster dir -u http://10.201.94.210 -w /usr/share/dirbuster/wordlists/
    ↪ directory-list-2.3-medium.txt -t 100

# Service enumeration
nmap -A 10.201.94.210

# Samba enumeration (explicit command used and logged)
enum4linux -a 10.201.94.210 | tee e4l.log

# SSH brute force (example)
hydra -l jan -P /usr/share/wordlists/rockyou.txt ssh://10.201.94.210

# Local enumeration
linpeas.sh | tee linlog.txt

# Convert SSH private key for john and crack passphrase
ssh2john kay_id_rsa | tee kay_pass.txt
john kay_pass.txt

# SSH login as kay using the private key
ssh -i kay_id_rsa kay@10.201.94.210
```

Contact and Notes

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

This report documents a TryHackMe lab-based educational penetration test. All findings are derived from the commands and steps executed during the engagement and are intended for training and remediation practice only.