Penetration Test Report

Client: TryHackMe
Prepared by: Lucio Rodrigues
Date: 11 August 2025
Assessment Type: Black Box Penetration Test

---

1. Executive Summary

The client engaged me to conduct a **black box penetration test** on the provided virtual environment, simulating the perspective of a malicious external actor with no prior knowledge of internal systems or credentials. The objective was to identify vulnerabilities, demonstrate exploitability, and retrieve two target flags - User.txt and Root.txt - as proof of compromise.

This assessment uncovered multiple security weaknesses across exposed services, including misconfigured SMB shares, sensitive file exposure, inadequate privilege separation, and privilege escalation vulnerabilities within the Windows environment. These issues, when chained together, allowed for ***complete system compromise***.

All identified vulnerabilities should be addressed promptly to reduce the risk of exploitation by malicious actors.

---

2. Scope

- **IP Address in Scope:** 10.10.156.108
- **Allowed Actions:**
    - Any tools or techniques permitted (manual exploitation prioritised first).
    - Locate and note all vulnerabilities found.
    - Submit flags as proof of exploitation.
    - Only the assigned target IP is in scope.
- **Objectives:**
    - User.txt flag.
    - Root.txt flag.

---

3. Methodology

This engagement followed a standard penetration testing methodology, adapted for a black box assessment:

1. **Reconnaissance**
    - Identified open ports and services using nmap.
    - Enumerated SMB shares, RPC services, and RDP endpoints.

2. **Enumeration**
    - Connected to SMB shares via smbclient.
    - Retrieved and decoded sensitive files (Base64).
    - Examined potential attack surfaces using both automated and manual methods.

3. **Exploitation**
    - Crafted a custom Windows reverse shell payload using msfvenom.
    - Uploaded payload via SMB and executed to establish a remote shell.

4. **Post-Exploitation & Privilege Escalation**
    - Ran `whoami /priv` for privilege escalation vector discovery.
    - Identified **SeImpersonatePrivilege** and exploited using PrintSpoofer to escalate to SYSTEM-level access.

5. **Flag Retrieval**
    - Extracted User.txt from user directory.
    - Extracted Root.txt from Administrator directory.

---

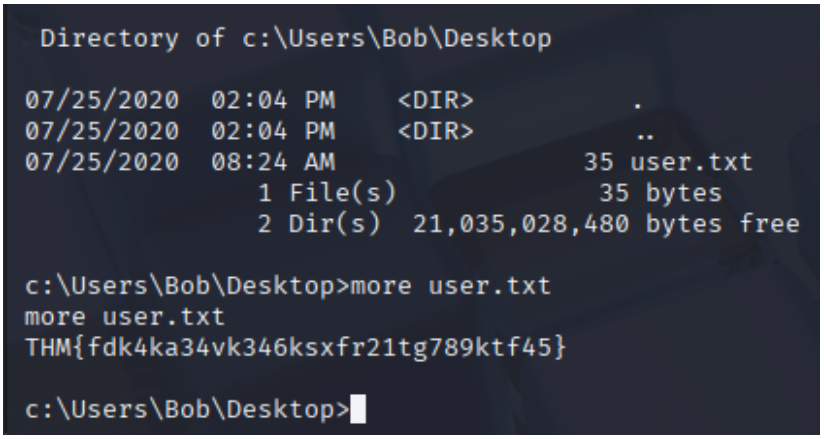
4. Vulnerability & Exploitation Assessment

Vulnerability	Severity	Description	Proof of Concept / Exploitation
SMB Share Misconfiguration	High	Accessible SMB shares allowed unauthenticated users to list and download files.	Connected with smbclient \\\\<targetIP>\\share and retrieved Base64-encoded data.
Sensitive Data Exposure	Medium	Retrieved Base64-encoded file contained sensitive instructions and system info.	Decoded using base64 -d to extract credentials/data.
Remote Code Execution via Uploaded Payload	High	SMB write permissions allowed direct upload of malicious executable.	Generated payload with msfvenom -p windows/shell_reverse_tcp and executed to gain a reverse shell.
Privilege Escalation via SeImpersonatePrivilege	**Critical**	SYSTEM privilege obtained using PrintSpoofer.	PrintSpoofer64.exe -i -c cmd.exe resulted in NT AUTHORITY\SYSTEM shell.

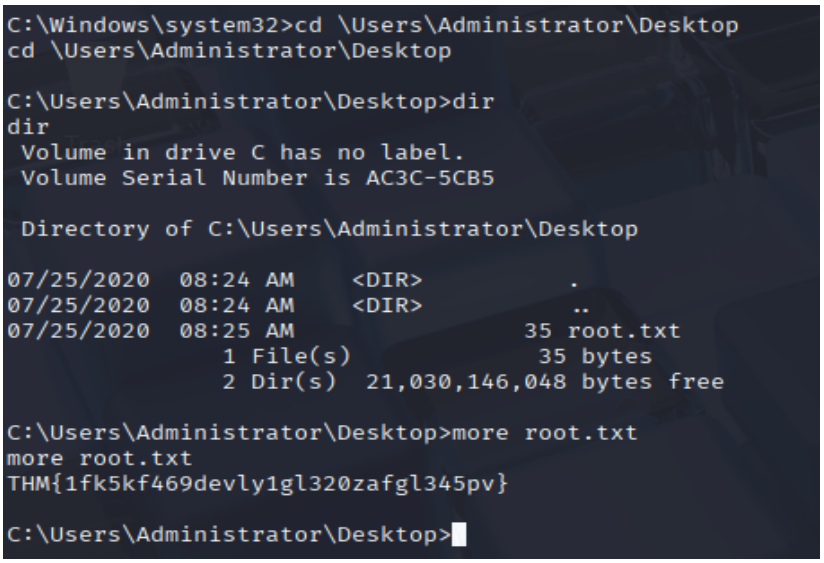
---

5. Proof of Exploitation

- **User Flag:**



- **Root Flag:**



---

6. Remediation Recommendations

1. **SMB Hardening**
    - Disable anonymous access to SMB shares.
    - Implement least privilege access controls.
    - Monitor SMB traffic for unauthorized access attempts.

2. **Secure Data Handling**
    - Avoid storing sensitive files in publicly accessible directories.
    - Ensure all sensitive data is encrypted in storage and transit.

3. **Privilege Management**
    - Restrict assignment of **SeImpersonatePrivilege** to only necessary accounts.
    - Regularly audit user privileges and remove unnecessary rights.

4. **Application Whitelisting**
    - Implement AppLocker or equivalent to block unauthorized executables.
    - Enable Controlled Folder Access to limit file modification.

5. **Patch & Update**
    - Keep Windows OS and services patched to mitigate known privilege escalation exploits like PrintSpoofer.

---

7. Conclusion

This black box penetration test demonstrated that an unauthenticated external attacker could compromise the target Windows environment **completely**, leveraging chained vulnerabilities from misconfigured services to SYSTEM-level privilege escalation.

By implementing the remediation recommendations provided, the organisation can significantly reduce the likelihood of similar successful attacks in the future.