Title : Capstone Penetration Testing Engagement

INTRODUCTION

This report documents the complete penetration testing engagement conducted on the TryHackMe Blue Room target (IP: 10.49.186.148). The focus was to apply comprehensive methodologies honed in previous modules to identify, exploit, and assess vulnerabilities across network, web applications, APIs, and host systems. Testing was performed over a 4-hour window with strict adherence to scope and ethical guidelines.

Key findings include open services on HTTP, SMB, and RDP, along with exploitable web application weaknesses, successful privilege escalation, and network protocol attacks enabling man-in-the-middle positioning and credential capture. All findings have been validated with supporting evidence and assigned critical CVSS scores, with detailed remediation recommendations to enhance the security posture.

SCOPE

Scope

- Target: TryHackMe Blue Room, IP 10.49.186.148
- Assessment Type: Full-scope penetration test encompassing network, application, API, and host layers
- Tools: nmap, Burp Suite, Responder, Ettercap, Wireshark, Python scripting, Linux native commands
- Out of Scope: Denial of service attacks, physical/social engineering
- Deliverables: Full PTES-aligned report, logged evidence, screenshots, remediation guidance

METHODOLOGY

The testing approach followed the PTES framework integrating reconnaissance, vulnerability analysis, exploitation, post-exploitation, and comprehensive reporting phases. Network scanning identified exposed ports and services; web and API endpoints were enumerated and tested for broken authentication and authorization vulnerabilities. Privilege escalation techniques were implemented leveraging service misconfigurations and SUID binaries. Network-level attacks, including SMB relay and ARP poisoning, were conducted to simulate real-world lateral movement and credential theft.

FINDING AND TECHNICAL DETAILS

Reconnaissance

- Nmap identified open ports 80 (HTTP), 445 (SMB), and 3389 (RDP)
- Web app directories and API endpoints enumerated with Gobuster and Burp Suite

Exploitation

- Web vulnerabilities exploited to gain initial shell access
- API vulnerabilities such as Broken Object Level Authorization (BOLA) and Broken Authentication demonstrated
- Privilege escalation via known Linux misconfigurations
- Man-in-the-middle attacks using Responder and Ettercap captured NTLM hashes and manipulated network traffic

Post-Exploitation

- Confirmed elevated privileges on target hosts
- Established persistence mechanisms
- Verified ability to pivot and access network resources

RISK AND IMPACT

The vulnerabilities discovered present critical risks to confidentiality, integrity, and availability of enterprise systems. Unauthenticated or low-privileged access escalated to system-level control facilitates data theft, service disruption, and potential compliance violations. The network attacks enable persistent man-in-the-middle positioning, allowing interception of sensitive user credentials and data. Immediate remediation is essential to prevent exploitation.

REMEDIATION & RECOMMENDATIONS

Patch all identified service misconfigurations
Harden web and API authentication & authorization logic
Disable legacy name resolution protocols (LLMNR/NetBIOS)
Enforce SMB signing and network segmentation
Strengthen monitoring and incident response capabilities

CONCLUSION

This capstone demonstrates the integration of technical knowledge and hands-on skills essential for effective penetration testing. The findings underscore the importance of layered defenses and continuous security validation to protect against both network and application level threats.

CYART

inquiry@cyart.io

www.cyart.io

Prepared by: Rushi Nalawade

Date: December 4, 2025