Elijah Hines

Mock Penetration Test & Security Assessment

Overview

This document is a detailed sanitized case study derived from an academic penetration testing engagement conducted in a controlled lab environment. All sensitive identifiers, IP addresses, credentials, flags, and exploit command details have been removed. The purpose of this document is to demonstrate penetration testing methodology, analysis depth, and professional reporting.

Engagement Scope

- External attacker simulation against a segmented lab network
- Assessment of Windows, Linux, and web application hosts
- Controlled, non-destructive testing only

Methodology

- Reconnaissance and service enumeration
- Vulnerability identification and validation
- Controlled exploitation to demonstrate impact
- Privilege escalation analysis
- Risk analysis and remediation development

Key Findings

- Remote code execution via vulnerable public-facing application
- Weak authentication controls enabling unauthorized access
- Insecure legacy service configurations leaking sensitive system data
- Local privilege escalation to administrative or SYSTEM-level access

MITRE ATT&CK; Alignment

- Observed activity was mapped to MITRE ATT&CK; techniques including active scanning,
- exploitation of public-facing applications, brute-force authentication, valid account abuse, privilege
- escalation, and ingress tool transfer.

Risk and Impact

The assessment demonstrated how multiple low- and medium-risk issues can be chained together to achieve full system compromise. Without proper controls, such attack paths could result in data exposure, service disruption, and persistent attacker access.

Remediation Themes

- Consistent patch management for operating systems and applications
- Hardened authentication and credential policies
- Restricted exposure of administrative services
- Improved logging and monitoring for detection

Ethics Notice

This project was conducted in a controlled educational lab environment. This document omits sensitive technical exploit details and is intended solely to demonstrate security assessment methodology and reporting practices.