vPENTEST

Internal Lab

AI ENHANCED EXECUTIVE SUMMARY

ABC Company

June 19, 2025

vPENTEST

Copyright

Confidentiality

This document contains company confidential information of a proprietary and sensitive nature. As such, this document should be afforded the security and handling precautions that a confidential document warrants. This document should have a controlled distribution to relevant parties only and should not be copied without written permission. vPenTest Partner treats the contents of a security audit as company confidential material and will not disclose the contents of this document to anyone without written permission.

Assessment Project Team

Below is a list of contacts that were involved in this engagement. Should you have any questions pertaining to the content of this document or any project and non-project-related items, please feel free to reach out to the necessary project contacts.

Primary Point of Contact	
Name:	Demo Consultant
Title:	Consultant
Office:	(844) 866-2732
Email:	support@vpentest.io

Executive Summary

The purpose of this internal network penetration test was to identify potential vulnerabilities within the organization's network infrastructure, simulating real-world malicious actors. The assessment targeted one hundred six (106) systems, with a total of twenty-four (24) systems found during the engagement. Additionally, thirteen (13) vulnerable systems were identified. The assessment identified several security vulnerabilities that require attention.

Initial host discovery was performed, followed by enumeration of HTTP, SSH, FTP, NFS, LDAP, RPC, MSSQL, HTTPS, SMB, and Redis services to identify misconfigurations and potential vulnerabilities. During testing, significant findings included configurations that could allow unauthorized access to sensitive data, as well as critical vulnerabilities such as ZeroLogon and EternalBlue, which pose serious risks if exploited.

Strengths

- Password security controls were effective, as password attacks did not result in unauthorized access.

Findings Summary

- The ZeroLogon vulnerability poses a significant risk as it allows unauthenticated attackers to gain domain administrator privileges on Windows Server systems. It is crucial to apply the security patches released by Microsoft immediately, as failing to do so could result in major security breaches.
- Systems vulnerable to MS17-010 (EternalBlue) present a serious concern, as successful exploitation allows attackers full access to the affected systems. Immediate security updates should be applied, and the organization's patch management program should be evaluated to prevent further vulnerabilities.
- SMTP NULL Session Authentication has been found enabled, allowing unauthorized access to SMB shares which could lead to data exposure. Disable this feature if not needed, and ensure that a strong authentication method is implemented for necessary services.
- Configuration issues in Microsoft Windows may lead to security risks, specifically in the lack of SMB signing which can make the environment susceptible to relay attacks. It is important to enforce SMB signing across systems via Group Policy to enhance security.
- Using FTP in its current form presents a risk as it transmits data in cleartext, exposing sensitive information during file transfers. If necessary for business, shift towards Secure FTP (SFTP) which protects data during transmission.

Closing Statement

The assessment found that password security controls were effective. However, vulnerabilities such as the ZeroLogon exploit, systems affected by MS17-010 (EternalBlue), and misconfigurations allowing SMTP NULL Session Authentication present significant risks for the organization, which operates in the education sector. If exploited, these vulnerabilities could potentially result in compromise of student/staff PII, breach of academic records, and reputational damage, depending on the criticality and purposes of the tested systems. Addressing these issues will enhance the overall security posture and protect sensitive information.

Engagement Scope of Work

Prior to beginning the assessment, vPenTest Partner and ABC Company agreed to a scope of work to define the specific assessment phases. The table below outlines the engagement scope of work and details entailed within each assessment phase that was conducted as part of this engagement.

Assessment Component	Assessment Phases
Internal Network Penetration Test	This assessment attempted to identify security threats that are exposed on the internal network environment. Threats identified within the internal environment are usually less severe than those of the external environment due to the limited exposure. → **Internal Network Penetration Test** - A penetration test was conducted to identify the potential impact of exploiting any identified vulnerabilities. Only exploits that are deemed safe were executed during this phase.

Engagement Statistics

The information below displays overall statistics that were recorded as part of this engagement. Following the statistics, vPenTest Partner has summarized all of the threats identified.

Internal Network Penetration Test

The information below provides a high-level overview of the assessment results recorded as part of this engagement. Following this section is a summary of all the threats identified and their potential risk to your organization.

Overall Severity Ranking

ASSESSMENT SCHEDULE

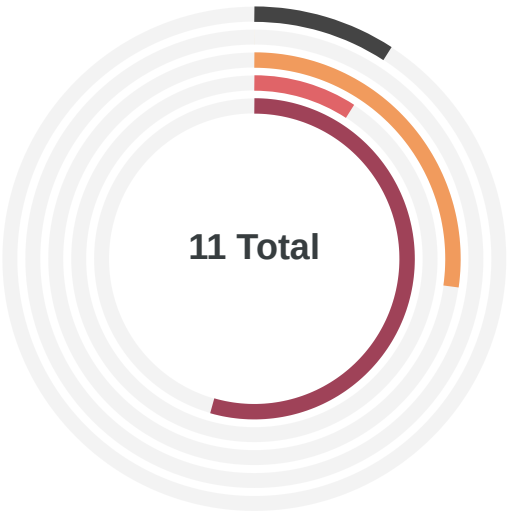
Thu, June 19, 2025
11:52 AM PT

Immediate remediation or mitigation is required. Exploitation of identified vulnerabilities require minimal effort from an attacker and pose a significant threat. A successful attack could result in unauthorized access to systems and/or valuable data.

Engagement Results Charts

To help ABC Company understand the severity of the threats identified during testing, vPenTest Partner has included an over-all summary chart below that displays a comparison of the report findings as well as the vulnerabilities that were discovered.

Internal Network Penetration Test Results



PenTest Findings

The following chart displays the overall severity of the report findings that were documented as part of the penetration testing efforts.

C	6	CRITICAL	H	1	HIGH
M	3	MEDIUM	L	0	LOW
I	1	INFO			

Engagement Results Summary

To summarize the results, vPenTest Partner has grouped all of the findings from the penetration test into rollup findings. These rollup findings can be used to quickly determine the root cause of the issues identified in the technical report. By implementing a remediation strategy for the findings based on the rollup issues identified below, ABC Company's security posture would be greatly improved.

Internal Network Penetration Test

Category	Summary
Password Deficiencies	The technical report presents findings related to password deficiencies. Weak and/or default passwords can have a significant impact on an organization as they typically allow an attacker to gain access to a particular system and/or resources. With access to systems and/or resources, this could eventually lead to elevated privileges, potentially granting access to confidential and/or sensitive documents.
Insecure Protocols	Testing identified instances of insecure protocols, which are essentially communication protocols that can potentially expose sensitive/confidential data in cleartext communications. A successful compromise against this weakness could lead to escalated privileges within the environment and could provide additional access to critical information systems and/or resources.
Patching Deficiencies	The tested environment contains patching deficiencies among systems and services. These issues could potentially result in a successful compromise, as each vulnerability contains multiple security weaknesses that an attacker may be able to exploit. Successful access may lead to unauthorized access to confidential data and/or systems.
Configuration Deficiencies	Configuration weaknesses were identified that could potentially lead to a successful compromise of systems and/or data within the tested environment. Although some of the configuration weaknesses may be exploitable in limited circumstances, the potential impact of a successful attack could be relatively high.
Egress Filtering Deficiencies	Testing identified that excessive services are accessible on the public Internet from the internal network environment. This could allow for an attacker to circumvent security controls by using alternative communication channels. Furthermore, a compromised system may be able to use such alternative communication channels to exfiltrate sensitive information.

Remediation Roadmap

For each assessment conducted, vPenTest Partner provided a remediation roadmap to help ABC Company understand the issues within the respective environment and the overall remediation strategies that should be implemented to resolve the issues identified during the penetration test. It should be noted that the remediation strategies below apply to multiple issues identified within the technical report and can greatly reduce the overall attack surface once successfully implemented.

Internal Network Penetration Test

Issue	Remediation Strategy
Configuration Deficiencies	Implement or improve a security configuration baseline that adheres to security best practices and industry standards such as National Institute of Standards and Technology (NIST). This security configuration baseline should ensure that no services and/or systems are deployed within the environment until a thorough configuration review has been performed.
Egress Filtering Deficiencies	Ensure that the organization's network firewalls restrict outbound access to the public Internet to services that are required for business operations. For services that are required for business operations, the organization should document these in a policy and procedure so that business justifications are communicated and understood within the organization. Any adjustments to these configurations should be documented in a change management program to establish an audit trail.
Insecure Protocols	Implement and/or improve a security configuration baseline within the organization that addresses the use of secure protocols. Insecure protocols pose a significant risk as the data being communicated is exposed in cleartext, allowing an attacker to discover potentially sensitive information. The organization should regularly perform scans that attempt to identify the use of insecure protocols to ensure that the configuration baseline is effective.
Patching Deficiencies	A patch management program should be implemented to ensure that both native and third-party services are up-to-date. Given today's evolving threat landscape and the frequency of security updates released for systems and services, patches should be applied on a weekly basis at a minimum. If the organization currently has a patch management program, it should be evaluated to identify any gaps that may have resulted in the patching deficiencies identified during testing.
Password Deficiencies	Implement a robust password policy that ensures all services and systems requiring authentication credentials adhere to the organization's stringent password complexity requirements. In some cases, the organization may have a system or service that is deployed and cannot have its authentication requirements managed via technical controls. The organization should ensure that configuration hardening baselines exist that address services and/or systems that cannot be centrally controlled. These services, along with those that can be controlled centrally, should have their passwords changed before being deployed within the environment.