Assignment 2

Vulnerability Analysis

Mansoor Hoshmand
ISEC2076

Table of Contents

Executive Summary

This vulnerability assessment, conducted in October 2025, evaluated the security posture of two workstations located in room D317. The primary objective was to identify existing vulnerabilities and assess their associated risks. The assessment consisted of two phases: (1) an **uncredentialed network scan**, performed without any user or administrative credentials to identify externally observable vulnerabilities; and (2) a **credentialed scan**, conducted using the workstations' built-in administrator account credentials to enable a more comprehensive analysis of configuration and privilege-level vulnerabilities.

Total Vulnerabilities from the Uncredentialed scan

A total of **4 medium-severity vulnerabilities** and **41 informational disclosures** were identified during the **uncredentialed scan** conducted on both workstations.

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	4	0	35

Total Vulnerabilities from the Credentialed scan

A total of 2 high-severity, 6 medium-severity vulnerabilities, and 226 informational disclosures were identified during the credentialed scan performed on both workstations

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	2	6	0	226

Vulnerability Severity Levels Explained

- **Critical (9–10):** vulnerabilities that are easily exploited and result in complete system compromise. Attackers can gain full control over the affected system.
- **High (7–8):** these pose a significant security risk, often easy to exploit and capable of causing data loss or major service disruption, though not full system control.
- **Medium (4–6):** vulnerabilities that present a moderate risk and may need specific conditions or user interaction to exploit.
- **Low (1–3):** these are low-impact or low-likelihood vulnerabilities, often involving minor misconfigurations or rare attack scenarios.
- **Informational (0):** these are not actual vulnerabilities but provide useful information about system configurations, software versions, or open services. While they pose no direct risk, they can help inform security decisions and highlight hygiene issues.

The most severe vulnerabilities are **outdated VMware Workstation versions** which contain multiple serious flaws that could let attackers **gain control of the system, run malicious code, or escalate privileges.** Additionally, the **WinVerifyTrust flaw (CVE-2013-3900)** allows attackers to **bypass signature checks**, enabling the delivery of fake but trusted malware. To protect system confidentiality, integrity, and availability, it is recommended that remediation efforts be prioritized according to the severity of each finding

Scope

Testing was conducted on two workstations in room D317 using a laptop running a virtual machine configured as the scanner.

Workstation	IP Address
Workstation 1	**172.16.136.133**
Workstation 2	**172.16.137.183**

Methodology

- The vulnerability scan was conducted using Nessus vulnerability scanner.
- Conducted two scans (Uncredentialed and Credentialed)
- Followed assignments instructions to complete the assessment.

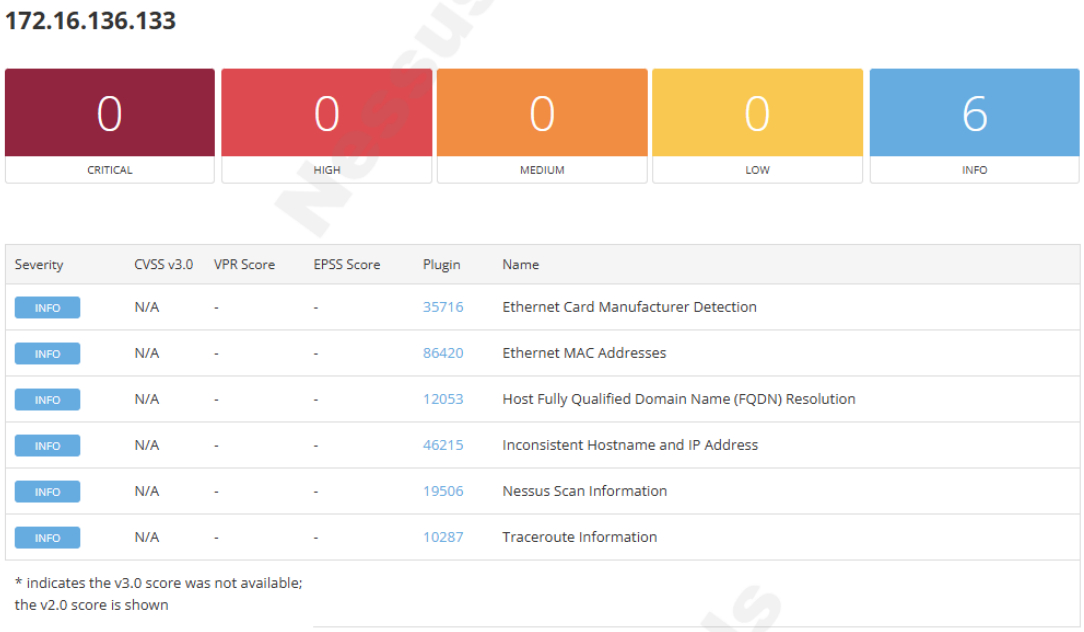
.

1. Uncredentialed scan results

A – Workstation 1 (IP:172.16.136.133)

After conducting a credentialed scan of this workstation, no low to critical vulnerabilities were detected. However, the scan did reveal six pieces of identifying information about the device or network. While these findings do not represent direct vulnerabilities, they could aid an attacker in the reconnaissance or planning stages of an attack. For detailed information on each finding, please refer to the accompanying HTML report.

Figure1: the image below shows the uncredentialed scan result for workstation 1.



172.16.136.133

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	0	0	6

Severity	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	-	46215	Inconsistent Hostname and IP Address
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	10287	Traceroute Information

* indicates the v3.0 score was not available; the v2.0 score is shown

B – Workstation 2 (172.16.137.183)

The scan for this workstation showed 4 medium categories of vulnerabilities with 35 information disclosures. Medium level threat means a moderate vulnerability not as severe as High or Critical, but still important to fix because it can be exploited by attackers under certain conditions. Below, we have explained all the medium categories of vulnerabilities and their threats. For detailed information on each finding, please refer to the accompanying HTML report.

Figure2: the image below shows the uncredentialed scan result for workstation 2.

172.16.137.183

0	0	4	0	35
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	-	157288	TLS Version 1.1 Deprecated Protocol
INFO	N/A	-	-	46180	Additional DNS Hostnames
INFO	N/A	-	-	39446	Apache Tomcat Detection
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information

1. **SSL certificate cannot be trusted (Medium Severity).**

   Having Digital certificates is a way to verify the identity of a website or a system. They are like digital identification cards confirming that the users are connected to legitimate trusted service. However, **untrusted certificates** present a significant risk to business operations and reputation. When a system or website uses an untrusted certificate, users may encounter security warnings or be blocked from accessing the site altogether. This not only disrupts access to essential services but also undermines user and customer confidence. Such vulnerabilities can be exploited by attackers to impersonate legitimate systems, intercept sensitive data, or deceive users into disclosing confidential information, leading to potential data breaches, fraud, and compliance failures. Over time, recurring warnings and security concerns can slowly damage organizational credibility, diminish trust, and strain business relationships. Resolving this issue is critical to maintaining a secure, trustworthy, and professional digital environment.

2. **SSL Self-Signed Certificate**

   A self-signed certificate is a digital certificate that is not issued by a trusted authority but instead created and signed by the organization itself. While this may be acceptable for internal testing, using self-signed certificates in production environments poses serious risks. They are not trusted by browsers or devices, often triggering security warnings or blocking access altogether. This undermines customer confidence and can disrupt service availability. More importantly, self-signed certificates make it easier for attackers to impersonate systems, intercept sensitive data, or carry out phishing attacks, as there is no trusted third party verifying the identity of the server. To maintain trust and ensure secure communication, it is critical to replace self-signed certificates with ones issued by a recognized certificate authority.

3. **TLS Version 1.0 Protocol Detection**

Transport Layer Security (TLS) is a cryptographic protocol that ensures data is encrypted and securely transmitted over networks. However, TLS version 1.0 is outdated and vulnerable to a known exploit called the BEAST attack (CVE-2011-3389). In this type of attack, a malicious actor can intercept and decrypt sensitive traffic between users and systems. For an organization, this presents significant risks, including unauthorized access to confidential data and the possibility of attackers redirecting users to malicious, impersonated websites. Continued use of TLS 1.0 weakens the overall security posture and can result in compliance failures, service disruptions, and damage to trust. It is essential for enterprises to disable outdated TLS versions and enforce modern, secure protocols such as TLS 1.2 or 1.3.

4. **TLS Version 1.1 Deprecated Protocol**

TLS 1.1, like TLS 1.0, is considered outdated due to weaknesses in its cryptographic design. These flaws make it easier for attackers to decipher encrypted communications, potentially exposing sensitive data transmitted between users and systems. If exploited, this can lead to data breaches, unauthorized access, and allow attackers to intercept or manipulate information in transit. Continued use of TLS 1.1 poses a security risk and may also result in non-compliance with modern security standards.

2. Credentialed scan results

A – Workstation 1 (IP:172.16.136.133)

During a credentialed scan conducted using the built-in administrator account, one high-severity and one medium-severity vulnerability were identified on Workstation 1. Additionally, the scan uncovered 104 informational findings. Although these are not direct vulnerabilities, they expose detailed system information that could aid attackers in the reconnaissance phase of a targeted attack. A comprehensive HTML report containing all findings is attached for reference.

Figure 3: the image below shows the credentialed scan result for workstation 1.

172.16.136.133

0	1	1	0	104
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
HIGH	7.5	8.1	0.0002	242128	VMware Workstation 13.0.x < 13.6.4 / 17.0.x < 17.6.4 Multiple Vulnerabilities (VMSA-2025-0013)
MEDIUM	5.5	6.6	0.7447	166555	WinVerifyTrust Signature Validation CVE-2013-3900 Mitigation (EnableCertPaddingCheck)
INFO	N/A	-	-	16193	Antivirus Software Check
INFO	N/A	-	-	92415	Application Compatibility Cache
INFO	N/A	-	-	34097	BIOS Info (SMB)
INFO	N/A	-	-	96533	Chrome Browser Extension Enumeration
INFO	N/A	-	-	152530	Cisco Packet Tracer Installed (Windows)
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)

1. **VMware Workstation 13.0.x < 13.6.4 / 17.0.x < 17.6.4 Multiple Vulnerabilities (VMSA-2025-0013)**

   A set of vulnerabilities disclosed in VMware's VMSA 2025 0013 advisory, including CVE 2025 41236, CVE 2025 41237, CVE 2025 41238, and CVE 2025 41239, present serious risks to organizations using VMware ESXi, Workstation, Fusion, and Tools. These flaws allow attackers with administrative access to a virtual machine to escape its boundaries and gain control over the host system, which often runs important applications and stores sensitive data. This could lead to theft of confidential information, installation of ransomware, shutdown of services, or spread across the network to compromise other systems. Although Nessus categorizes these vulnerabilities as High, Broadcom has assessed them as Critical with a severity score of 9.3 due to their potential impact. Systems that were assumed to be isolated and secure could become entry points for full scale attacks, making prompt patching and strong security practices essential to avoid disruption, data loss, and reputational damage.

2. **WinVerifyTrust Signature Validation CVE-2013-3900**

   CVE-2013-3900 can have serious technical impacts by undermining the integrity of digital signature validation in Windows. It allows attackers to append malicious code to signed executables without invalidating their signatures, effectively bypassing trust mechanisms. This can lead to remote code execution, unauthorized software installation, and the spread of malware across systems. Because the operating system treats these tampered files as trusted, traditional security tools may fail to detect or block them, increasing the risk of widespread compromise and persistent threats within affected environments. Microsoft's mitigation involves enabling the EnableCertPaddingCheck registry setting, which forces Windows to reject improperly padded certificates and restores the reliability of signature validation.

B – Workstation 1 (IP:172.16.137.183)

During a credentialed scan conducted using the built-in administrator account, 1 High and 5 medium-severity vulnerabilities were identified on Workstation 2 which have already been explained on pages 7, 8, 10.

Figure 4: the image below shows the credentialed scan result for workstation 2.

172.16.137.183

0	1	5	0	122
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
HIGH	7.5	8.1	0.0002	242128	VMware Workstation 13.0.x < 13.6.4 / 17.0.x < 17.6.4 Multiple Vulnerabilities (VMSA-2025-0013)
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	-	157288	TLS Version 1.1 Deprecated Protocol
MEDIUM	5.5	6.6	0.7447	166555	WinVerifyTrust Signature Validation CVE-2013-3900 Mitigation (EnableCertPaddingCheck)

References

- https://www.securew2.com/blog/the-dangers-of-self-signed-certificates
- https://www.upguard.com/blog/ssl-configuration#:~:text=your%20web%20server.-,Common%20SSL%20Misconfiguration%20Findings,features%20like%20SSL/TLS%20authentication.
- https://www.acunetix.com/blog/articles/tls-vulnerabilities-attacks-final-part/
- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/35877
- https://learn.microsoft.com/en-us/answers/questions/1182542/cve-2013-3900-winverifytrust-signature-validation