CyberMax Office of Information and Technology

Division of Information Security & Privacy Management

Security Assessment

Cat’s Company Vulnerabilities

July 28, 2023

## Table of Contents

[Table of Contents ii](#_Toc10020855)

[List of Tables ii](#_Toc10020856)

[List of Figures ii](#_Toc10020857)

[1. Executive Summary 3](#_Toc10020858)

[2. Background 3](#_Toc10020859)

[3. Assessment Scope 3](#_Toc10020860)

[4. Summary of Findings 3](#_Toc10020861)

[5. Summary of Recommendations 4](#_Toc10020862)

[2. Introduction 4](#_Toc10020863)

[1. Assessment Methodology 4](#_Toc10020864)

[2. Detailed Findings 5](#_Toc10020865)

[3. Methodology for the Security Control Assessment 5](#_Toc10020866)

[4. Methodology for Security Test Reporting 5](#_Toc10020867)

[3.1 Business Risks 7](#_Toc10020868)

[3.1.1 Moderate 8](#_Toc10020869)

[Assessed-2017-SCA-IA-2-12 8](#_Toc10020870)

[4. Documentation Lists 10](#_Toc10020871)

## List of Tables

[Table 1. Risk Level Definitions 5](#_Toc10020872)

[Table 2. Ease-of-Fix Definitions 6](#_Toc10020873)

[Table 3. Estimated Work Effort Definitions 7](#_Toc10020874)

[Table 4. CFACTS System Names 7](#_Toc10020875)

[Table 5. Documentation Requested 10](#_Toc10020876)

## List of Figures

[Figure 1. Reported Findings by Risk Level 3](#_Toc10020949)

[Figure 2. Open Findings by Risk Level 4](#_Toc10020950)

**2) Executive Summary**

A preliminary Nmap using a Kali machine has been done on 3 devices that are part of the scope of our research namely a Linux Ubuntu (172.16.14.52), a Windows Server (172.16.14.53) and Windows Workstation 1 (172.16.14.50). The objective of this scan is to observe the information a less experience attacker can see. It also highlights the preliminary information a more experiences attacker could see before potentially attacking Cat’s Company. Using the Nmap has a baseline, CyberMax will have a more in-depth search using OpenVas (GreenBone) to identify the vulnerabilities and provide solutions for each of the identified ones.

**4) Assessment Scope and NMAP results**

**Linux Ubuntu: 172.16.14.52**

Une image contenant texte, Police, capture d’écran

Description générée automatiquement

**Windows Server: 172.16.14.53**

Une image contenant texte, capture d’écran, Police, information

Description générée automatiquement

**Windows WorkStation 1: 172.16.14.50**

Une image contenant texte, capture d’écran, Police, information

Description générée automatiquement

**5) Summary of Findings Figure 1**

Une image contenant capture d’écran, texte, logiciel, Logiciel multimédia

Description générée automatiquementThe OpenVAS scan has uncovered 2 high risks and 2 moderate risks. 0 low risk have been identified when looking at the broad scope of each device. We will look deeper into each one of the devices in a later section. This section is meant to give a broad summary of what to focus our attention on. Which are the critical and high vulnerabilities.

**Linux Ubuntu vulnerabilities**

The scan on Ubuntu uncovered a vulnerability on port 9200/tcp. The vulnerability is a critical one and is the HTTP Brute Force Logins with Default Credentials Reporting. This vulnerability makes it easier for an attacker to penetrate the network by using any app/device to try as many passwords as possible in a short period of time. The scan uncovered the default credentials are on the Ubuntu device making it even more vulnerable. Changing the password for a 12 characters password with numbers and special characters will greatly mitigate the vulnerability.

Une image contenant texte, nombre, Police, logiciel

Description générée automatiquement**Figure 2**

The CVE-1999-0508 (Figure 2) identifies an account on a router, a firewall or other network devices has a default, null, blank or missing a password. Changing the current password or adding another one will prevent or greatly limit someone’s ability to infiltrate Cat’s Company System.

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement

<https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cve_id=CVE-1999-0508&isCpeNameSearch=false>

Add a High Vulnerability assessment for Ubuntu

**Figure 3**

Une image contenant texte, Police, nombre, capture d’écran

Description générée automatiquement

**Windows Workstation 1**

The scan on the Windows Workstation uncovered a critical vulnerability on the general/tcp port. The critical vulnerability is the Operating System (OS) End of life (EOL) Detection. This vulnerability indicated that the software vendor (windows in that instance) has stop providing updates, patches or any other support for that version of the software. An attacker could potentially exploit known or even newly discovered vulnerabilities in an EOL and gains unauthorized access or compromise the system’s security. The windows workstation 1 has the “DCE/RPC and MSRPC Services enumeration reporting” vulnerability on port 135/tcp. The latter vulnerability allows an attacker to gain more knowledge about the remote host. Although labeled has a lower risk that the previous one, this vulnerability allows the attacker to gather a great deal of information through reconnaissance and the scope of the potential damage could spread throughout Cat’s company. Filtering incoming traffic to and from this port or blocking the port would be possible effective mitigations.

Une image contenant texte, Police, nombre, ligne

Description générée automatiquement

The CVE-1999-0508 identifies an account on a router, a firewall or other network devices has a default, null, blank or missing a password. Changing the current password or adding another one will prevent or greatly limit someone’s ability to infiltrate Cat’s Company System. <https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cve_id=CVE-1999-0508&isCpeNameSearch=false>

**Winserver Scan 1**

The scan on the Windows Server (Winserver1) uncovered a “DCE/RPC and MSRPC Services Enumeration Reporting on port 135/tcp” the same vulnerability on port 135/tcp mentioned in the Windows Workstation 1. However, the Winserver also has a “SSL/TLS : Report Weak Cipher Suites” vulnerability on port 3389/tcp. Cipher Suites are meant to provide secure communication over a network ensuring confidentiality and integrity of data transmission. In other words, it is a two ways communication between the clients and our web browser, The communication is done through an exchange of “keys”. A Weak Cipher Suite may potentially allow someone to “brute force” the encryption key has mentioned above, or someone may perform a Cypher text attack and recover sensitive information by deduction without ever having to decrypt the data (man in the middle attack). A good solution would be to prevent any port in your system, but especially port 3389/tcp to accept services/communications from any of the Cipher Suites mentioned in the figure below (the Cypher Suites start with RC4).

Une image contenant texte, Police, nombre, capture d’écran

Description générée automatiquement

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Une image contenant texte, Police, ligne, nombre

Description générée automatiquement

Une image contenant texte, capture d’écran, Police, logiciel

Description générée automatiquement

<https://www.cvedetails.com/cve/CVE-2015-4000/?q=CVE-2015-4000>