Vulnerability Assessment Report

Target. Inc

July 2022

Target. Inc Consulting Services, LLC

TABLE OF CONTENTS

1. Executive Summary 3

1.1 Vulnerability Assessment Summary of Results 3

2. Vulnerability Assessment 4

2.1 Purpose 4

2.2 Scope 4

2.3 Methodology 4

2.4 Vulnerability Ranking 4

3. External Publicly Available Information (OSINT) 5

3.1 Search Engine Results 5

3.2 LinkedIn Results 6

4. Vulnerability Assessment Findings 6

4.1 Vulnerabilities in smb could allow remote code execution 6

4.2 Microsoft windows smb server ntlm multiple vulnerabilities 7

4.3 SMB brute force logins with default credentials 7

4.4 Vulnerabilities in smb server multiple vulnerability remote 8

4.5 DCE/RPC and MSRPC services enumeration reporting 8

Appendix A – References 9

# Executive Summary

Target. Inc was engaged by Yingwei Liu to perform an internal and external vulnerability assessment and presents the business and technical findings in this report. The assessment was conducted from 12 to 14, 2022.

## Vulnerability Assessment Summary of Results

The following was identified by Target. Icduring the course of the vulnerability assessment as the greatest risks to the organization’s information and systems.

* 1. In the first finding, the host missing a critical security update that prevent remote code execution to the SMB. This vulnerability may lead to potentials security risks to the target. Inc
* 2. In the second finding, the host is missing a critical security update. An input validation error exists while processing SMB requests and can be exploited to cause buffer overflow via a specially crafted SMB packet. A lack of cryptographic entropy when the SMB server generates challenges during SMB NTLM authentication and can be exploited to bypass the authentication mechanism. The potential security risk of this finding may relate to the man in the middle attack since the information does not encrypt during the transferring process.
* 3. In the third finding, there are numbers of known default credentials is tried to log in via SMB protocol. This is considered as the brute forces attack which may leads to the unauthorized access to the system.
* 4. In the fourth findings, this Host is missing a critical security update according to Microsoft Bulletin MS17-010.
* 5. In the fifth findings, distributed computing Environment / Remote Procedure calls or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

# Vulnerability Assessment

## Purpose

**The purpose of performing a vulnerability assessment is to provide a detailed and systematic review of security weaknesses in Taget.com. Also, it evaluates the security awareness for the potential vulnerability and provide recommendations for the vulnerability remediation process of Target.com.**

## Scope

OSINT conducted on the following Target.com external URLs:

* + <Https://www.target.com>
  + <Https://www.target.com/link>
  + <https://www.google.com/search?q=site:target.com+ext:sql+|+ext:dbf+|+ext:mdb>.
  + <https://www.google.com/search?q=site:target.com+ext:xml+|xt:conf+|+ext:cnf+|+ext:reg+|+ext:inf+|+ext:rdp+|+ext:cfg+|+ext:txt+|+ext:ora+|+ext:ini>.
  + <https://www.google.com/search?client=firefox-b-1-e&q=target>.
  + <https://www.google.com/search?q=site:target.com+intitle:index.of>.

Internal IP addresses scanned for vulnerabilities

* + Target.com IP address: 193.105.91.168.
  + The Harvester Target.com: 145.75.34.187.
  + (Actually scanned) Scanning and Enumeration:
    - 1. Zenmap: 10.0.0.10, 10.0.0.103.
    - 2. Nmap -T4 -A -V -oX 10.0.0.103, 108, 112.
    - 3. OpenVAS.

## Methodology

Target’s assessment methodology

The assessment methodology is a useful tool that helps users have a better understanding of the steps to perform a quality and successful vulnerability assessment of Target.com. A vulnerability assessment is a way to determine and classify security vulnerabilities in the Target web application. According to NIST-800-115, "Evaluating the types of security tests and examinations the organization will execute, developing an appropriate methodology, identifying the resources required, and structuring the assessment process to support expected requirements can mitigate the resource challenge. This gives the organization the ability to reuse pre-established resources such as trained staff and standardized testing platforms." Additionally, a well-designed vulnerability assessment methodology can improve the efficiency of the security examination process, reduce expenses, and identify potential vulnerabilities in the target.

The vulnerability assessment of the Target web application involves four different phases. The first phase is the guideline development phase, which includes defining the purpose of the vulnerability assessment. The second phase involves designing an approach to set up methods for collecting information about the target. In the third phase, information about the target's web applications is collected and analyzed. Finally, a vulnerability assessment report is generated for the target's web application. As Roddy Correa mentioned, "the proposed approach contemplates a three-phase process at the macro level of definition, execution, and results, where the core of the methodology is in the execution phase. It is fed by the results of static and dynamic analysis, which are verified and validated through a correlation of results. This allows us to establish scenarios manually, from an attacker's perspective, to discard false positives and identify possible false negatives. Additionally, we emphasize evaluating the access control of the applications in a particular way to increase the degree of vulnerability coverage, which allows for the most effective analysis."

The vulnerability assessment report is a review document that records all the vulnerabilities found in Target’s web application scanning and enumeration process. It is the result gathered from the vulnerability scanning lab and allows people to review and understand the network structure of Target’s web application. A comprehensive vulnerability assessment report helps improve the efficiency of vulnerability management and enables quick identification and remediation of vulnerabilities. According to Alberto Caponi, "In general, risk management is a crucial factor in the success of an organization. Several different groups are concerned with risk management in an organization to meet many business or regulatory requirements. The management of this risk should provide a general view of the organization through the cataloging of resources, identification of threats, and valuation of vulnerabilities."

The risk of vulnerability assessment includes identifying the potential loss resulting from the assessment. According to NIST 800-115, "A more reliable way of identifying the risk of vulnerabilities in aggregate is through penetration testing." Penetration testing simulates cyber-attacks against computer systems, web applications, and networks to identify vulnerabilities. It helps improve the security level of the company and raises security awareness among employees. Just like Jeremiah 46:27 states, "But fear not, O Jacob my servant, nor be dismayed, O Israel, for behold, I will save you from far away, and your offspring from the land of their captivity. Jacob shall return and have quiet and ease, and none shall make him afraid. “Vulnerability Ranking

The vulnerabilities are identified and ranked according to their potential threat to the Enterprise. The “risk factor” for each vulnerability identified is determined using the Common Vulnerability Scoring System (CVSS)2:

|  |  |
| --- | --- |
| Critical | CVSS score of 10 |
| High | CVSS score ranges (7.0 - 9.9) |
| Medium | CVSS score ranges (4.0 - 6.9) |
| Low | CVSS score ranges (1.0 - 3.9) |

It is recommended to immediately remediate any high or critical vulnerabilities due to the potential threat. Although, exploiting multiple medium or low vulnerabilities may also lead to a system compromise.

# External Publicly Available Information (OSINT)

During external reconnaissance, **Target.com** was able to find the following publicly available information using various reconnaissance tools.

## Search Engine Results

Details

|  |  |
| --- | --- |
| *These servers and email addresses were identified using the Bing search engine.* |  |
| *These servers and email addresses were identified using the Google search engine.* |  |
| *The information shown was identified using the Maltego tool.* |  |

Impact

These exposed public information helps the attacker to generate sufficient information about company’s network structure and employee’s private information. It helps the attacker to create further attack such as social engineering, DDOS, etc.

Recommendation

People need to pay attention to what they are posting online. Also, the company need to adjusting their security policy and provide security training for employees.

## LinkedIn Results

Details

|  |  |
| --- | --- |
| *These users were identified by manually searching through LinkedIn accounts.* |  |

Impact

Hacker can apply social engineering attack tactics based on the information that user post on the LinkedIn.

Recommendation

1. User should not post critical information that relates to the company.
2. User on LinkedIn should monitor other viewers activities.
3. Company should educate social engineering attack.

# Vulnerability Assessment Findings

During the vulnerability assessment Yingwei Liu was able to use Zenmap, Wireshark, OpenVAS to scan and enumerate Target. Inc web application.

## VULNERABILITIES IN SMB COULD ALLOW REMOTE CODE EXECUTION

Details

This host missing a critical security update that prevent remote code execution to the SMB.

|  |  |  |  |
| --- | --- | --- | --- |
| Host(s) | | CVSS | Severity |
| 10.0.0.103 | 9.3 | | High |

Impact

Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosures from the server.

Recommendation

Update the windows system and update the hotfixes

## Microsoft windows smb server ntlm multiple vulnerabilities

Details

The host is missing a critical security update. An input validation error exists while processing SMB requests and can be exploited to cause buffer overflow via a specially crafted SMB packet. A lack of cryptographic entropy when the SMB server generates challenges during SMB NTLM authentication and can be exploited to bypass the authentication mechanism.

|  |  |  |  |
| --- | --- | --- | --- |
| Host(s) | | CVSS | Severity |
| 10.0.0.103 | 10 | | High |

Impact

Successful exploitation will allow remote attackers to arbitrary code or cause a denial of service or bypass the authentication mechanism via brute force technique impact level.

Recommendation

Run Windows update and update the listed hotfixes or download and update mentioned hotfixes.

## SMB bRUTE fORCE lOGINS WITH dEFAULT cREDENTIALS

Details

A number of known default credentials is tried to log in via SMB protocol.

|  |  |  |  |
| --- | --- | --- | --- |
| Host(s) | | CVSS | Severity |
| 10.0.0.103 | 9 | | High |

Impact

potential account breach.

Recommendation

Change the password as soon as possible.

## Vulnerabilities in smb server multiple vulnerability remote

Details

This Host is missing a critical security update according to Microsoft Bulletin MS17-010.

|  |  |  |  |
| --- | --- | --- | --- |
| Host(s) | | CVSS | Severity |
| 10.0.0.103 | 9.3 | | HIGH |

Impact

Successful exploitation will allow remote attacker to gain the ability to execute code on the target server, also could lead to information disclosures from the servers.

Recommendation

Run windows update.

## DCE/RPC and MSRPC services enumeration reporting

Details

Distributed computing Environment / Remote Procedure calls or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

|  |  |  |  |
| --- | --- | --- | --- |
| Host(s) | | CVSS | Severity |
| 10.0.0.103 | 5.0 | | Medium |

Impact

An attacker may use this fact to gain more knowledge about the remote host.

Recommendation

Filtering incoming traffic to this port. Insert intrusion detection system and update firewall.

# Appendix A – References

Correa, R. A., Bermejo Higuera, J. R., Javier, B. H., Sicilia Montalvo, J. A., Manuel Sánchez Rubio, & Magreñán, Á. A. (2021). Hybrid Security Assessment Methodology for Web Applications.*Computer Modeling in Engineering & Sciences, 126*(1), 89-124. <https://doi-org.ezproxy.liberty.edu/10.32604/cmes.2021.010700>.

Caponi, A., & Leuti, M. (2019). A Web Platform for Integrated Vulnerability Assessment and Cyber Risk Management. Information, 10(7), 242. https://doi.org/10.3390/info10070242