Development and Simulation of CVE-2020-1472 Exploit

Created by :- Akash Rathod

Introduction

This project aims to develop and simulate the CVE-2020-1472 exploit, also known as Zerologon. The vulnerability affects all supported versions of Microsoft Windows Server and allows an attacker to bypass authentication and gain unauthorized access to the domain controller. The project involves developing a Python script that can exploit the vulnerability and simulate the attack against a vulnerable domain controller.

2. Overview of the impact of the vulnerability: The impact of CVE-2020-1472 is severe as it allows an attacker to take complete control of a network. If exploited, it could lead to data theft, ransomware attacks, and disruption of operations.
3. Importance of studying the vulnerability: It is crucial to study CVE-2020-1472 to understand the severity of the vulnerability and the potential impact on organizations. This knowledge can help system administrators and security professionals take steps to protect their networks.

Development:

To develop the CVE-2020-1472 exploit, we used the Python programming language and the
Impacket library, which is a collection of Python classes for working with network protocols. The exploit script uses a brute-force method to try to authenticate with the domain controller using all-zero challenge and credential values. If successful, the script can gain access to the domain controller and take over the network.

Background

- Description of Netlogon Remote Protocol (MS-NRPC): MS-NRPC is a remote procedure call (RPC) protocol used by Windows Server for authentication between clients and domain controllers.

- Explanation of the authentication process: The authentication process involves a series of steps, including establishing a secure channel, exchanging credentials, and verifying the authenticity of the credentials.
- Discussion of how the vulnerability allows for bypassing authentication: The vulnerability allows an attacker to use a vulnerable Netlogon protocol implementation to bypass the authentication process and gain administrative access to the domain controller.

Methodology

- Description of the lab environment used for testing: The lab environment should mimic a typical network infrastructure with domain controllers, clients, and servers.
- Explanation of the testing process: The testing process involves attempting to exploit the vulnerability using various methods, including using Metasploit or creating custom exploits.
- Discussion of the tools used for testing: The tools used for testing may include network sniffers, vulnerability scanners, and exploitation frameworks like Metasploit.

Results

- Presentation of the findings on CVE-2020-1472: The results should include a detailed description of the exploit, its success rate, and the level of access obtained.
- Identification of vulnerabilities or development of an exploit: The report should highlight any vulnerabilities found during the testing process, and if an exploit is developed, it should be detailed in the results section.
- Evidence to support the findings, including code snippets and screenshots: The report should include code snippets or screenshots to provide evidence of the findings.

Simulation:

To simulate the CVE-2020-1472 exploit, we set up a virtual machine running a vulnerable version of Windows Server and configured it as a domain controller. We then ran the exploit script against the virtual machine to test whether the vulnerability could be exploited. The script successfully authenticated with the domain controller and gained unauthorized access to the network, demonstrating the severity of the vulnerability.

Conclusion:

The CVE-2020-1472 vulnerability is a serious threat to organizations that use Microsoft Windows Server as their domain controller. It is essential to apply the security patch released by Microsoft to mitigate the risk of exploitation. This project has demonstrated the severity of the vulnerability and the ease with which it can be exploited, highlighting the importance of proactive vulnerability management and security patching.

Reference :

1 . https://tryhackme.com/room/zer010gon

2. https://github.c.om/SecuraBV/C-VE-2020-1472

3. Tom Tervoort of Secura - https://www.secura.com/pathtoimg.php?id=2055

4. Microsoft https://docs.microsoft.com/en-us/openspecs/windows protocols/ms-nrpc/7b9e31d
1-670e-4fc5-ad54-9ffff50755f9

5. Microsoft -

-8014-45ae-80af-cOecb06e2db9

6. https://raw.githubusercontent.com/SecuraBV/CVE-2020-1472/master/7erologon tes ter.py

7. https://learn.microsoft.com/en-us/openspecs/windows protocols/ms-nrpc/5ad9db9 f-7441-4ce5-8c7b-7b771 e243d32