

<> Code Issues 17 Pull requests 1 Actions Projects Security Insights

About

KrbRelayUp - a universal no-fix local privilege escalation in windows domain environments where LDAP signing is not enforced (the default settings).

- 📖 Readme
- 📈 Activity
- ★ 1.5k stars
- 👁 23 watching
- 🔗 202 forks

Report repository

Releases

No releases published

Packages

No packages published

Contributors 6



Languages



Simple wrapper around some of the features of [Rubeus](#) and [KrbRelay](#) (and a few other honorable mentions in the acknowledgements section) in order to streamline the abuse of the following attack primitive:

0. (Optional) New machine account creation ([New-MachineAccount](#))
1. Local machine account auth coercion ([KrbRelay](#))
2. Kerberos relay to LDAP ([KrbRelay](#))
3. Add RBCD privs and obtain privileged ST to local machine ([Rubeus](#))
4. Using said ST to authenticate to local Service Manager and create a new service as NT/SYSTEM. ([SCMUACBypass](#))

This is essentially a universal no-fix local privilege escalation in windows domain environments where LDAP signing is not enforced (the default settings).

UPDATE: [Here](#) is an excellent writeup by [@an0n_r0](#) on how to perform this attack manually (using the **original tools** for this attack path: [PowerMad/SharpMad](#), [KrbRelay](#), [Rubeus](#) and [SCMUACBypass](#))

I added some features to support this attack primitive using shadow credentials. Note this eliminates the need for adding (or owning) another machine account.

Note: this attack method bypasses the Protected Users (or 'Account is sensitive and cannot be delegated') mitigation due to the S4U2Self abuse.

1. Local machine account auth coercion ([KrbRelay](#))
2. Kerberos relay to LDAP ([KrbRelay](#))
3. Generate new KeyCredential and add it to the local machine account's 'msDS-
KeyCredentialLink' attribute. ([Whisker](#) and [KrbRelay](#))
4. Using said KeyCredential to obtain a TGT for the local machine account via PKInit.
([Rubeus](#))
5. Using the TGT to obtain privileged ST to local machine via S4U2Self and TGSSUB.
([Rubeus](#))

6. Using said ST to authenticate to local Service Manager and create a new service as NT/SYSTEM. ([SCMUACBypass](#))

UPDATE: [Here](#) is an excellent writeup by [@icyguider](#) on how to perform the ShadowCred method of this attack manually (using the **original tools** for this attack path: [KrbRelay](#), [Rubeus](#) and [SCMUACBypass](#)) along with the usage of [NimCrypt2](#) to pack the various tools and evade some detection by defensive mechanism.

Update - ADCS Web Enrollment Support

I added support for relaying Machine KRB auth to ADCS Web Enrollment (instead of LDAP). This eliminates the requirement of LDAP Signing not to be enforced in the domain since this attack does not relay to LDAP.

Note: *this attack method bypasses the Protected Users (or 'Account is sensitive and cannot be delegated') mitigation due to the S4U2Self abuse.*

1. Local machine account auth coercion ([KrbRelay](#))
2. Kerberos relay to ADCS (HTTP) ([KrbRelay](#) and [ADCSPwn](#))
3. Generate certificate request on behalf of the local machine account, submit it to ADCS Web Enrollment and finally retrieve the certificate for the local machine account ([ADCSPwn](#))
4. Using said certificate to obtain a TGT for the local machine account via PKInit. ([Rubeus](#))
5. Using the TGT to obtain privileged ST to local machine via S4U2Self and TGSSUB. ([Rubeus](#))
6. Using said ST to authenticate to local Service Manager and create a new service as NT/SYSTEM. ([SCMUACBypass](#))

Usage

KrbRelayUp - Relaying you to SYSTEM

FULL: Perform full attack chain. Options are identical to RELAY. Tool will relay to local Service Manager and create a new service as NT/SYSTEM.

RELAY: First phase of the attack. Will Coerce Kerberos auth from local machine account and relay it to ADCS Web Enrollment. Will obtain a TGT for the local machine account via PKInit. Will then use the TGT to obtain a privileged ST to local machine via S4U2Self and TGSSUB. Finally will use the ST to authenticate to local Service Manager and create a new service as NT/SYSTEM.

Usage: KrbRelayUp.exe relay -d FQDN -cn COMPUTERNAME [-c] [-cp PASSWORD] [-m] [-p] [-cls] [-c] [-cp] [-f] [-ca] [-https] [-cet]

| | | |
|------|------------|--------------------------------------------------|
| -m | (--Method) | Abuse method to use in after a successful relay. |
| -p | (--Port) | Port for Com Server (default=1.35.0.1) |
| -cls | (--Clsid) | CLSID to use for coercing Kerberos auth. |

RBCD Method:

| | | |
|-----|------------------------------|--------------------------------------------|
| -c | (--CreateNewComputerAccount) | Create new computer account for attacker. |
| -cn | (--ComputerName) | Name of attacker owned computer account. |
| -cp | (--ComputerPassword) | Password of computer account for attacker. |

SHADOWCRED Method:

| | | |
|----|---------------------|---------------------------------------------------------------------------|
| -f | (--ForceShadowCred) | Clear the msDS-KeyCredentialList attribute for the local machine account. |
|----|---------------------|---------------------------------------------------------------------------|

ADCS Method:

| | | |
|--------|-------------------------|------------------------------------------------|
| -ca | (--CAEndpoint) | CA endpoint FQDN (default = sametime.com) |
| -https | (--Https) | Connect to CA endpoint over secure connection. |
| -cet | (--CertificateTemplate) | Certificate template to request. |

SPAWN: Second phase of the attack. Will use the appropriate control to impersonate the user and create a new service as NT/SYSTEM.

Usage: KrbRelayUp.exe spawn -d FQDN -cn COMPUTERNAME [-cp PASSWORD] [-m] [-i] [-s] [-sc]

| | | |
|-----|--------------------|------------------------------------------------|
| -m | (--Method) | Abuse method used in RELAY phase. |
| -i | (--Impersonate) | User to impersonate. should be a domain user. |
| -s | (--ServiceName) | Name of the service to be created. |
| -sc | (--ServiceCommand) | Service command [binPath]. (default = cmd.exe) |

RBCD Method:

| | | |
|-----|--------------------------|--------------------------------------------|
| -cn | (--ComputerName) | Name of attacker owned computer account. |
| -cp | (--ComputerPassword) | Password of computer account for attacker. |
| -ch | (--ComputerPasswordHash) | Password NT hash of computer account. |

```
# SHADOWCRED | ADCS Method:
-ce (--Certificate)           Base64 encoded certificate or |
-cep (--CertificatePassword)  Certificate password (if appli
```

KRBSCM: Will use the currently loaded Kerberos Service Ticket to create a new service ticket for the specified service.

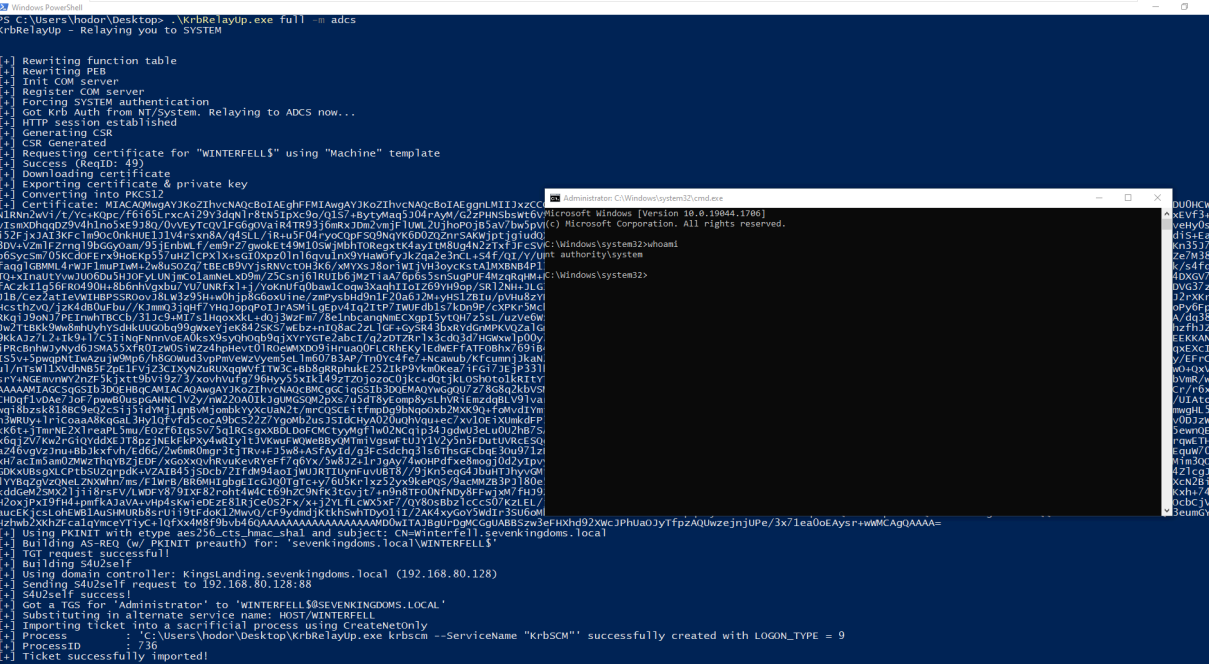
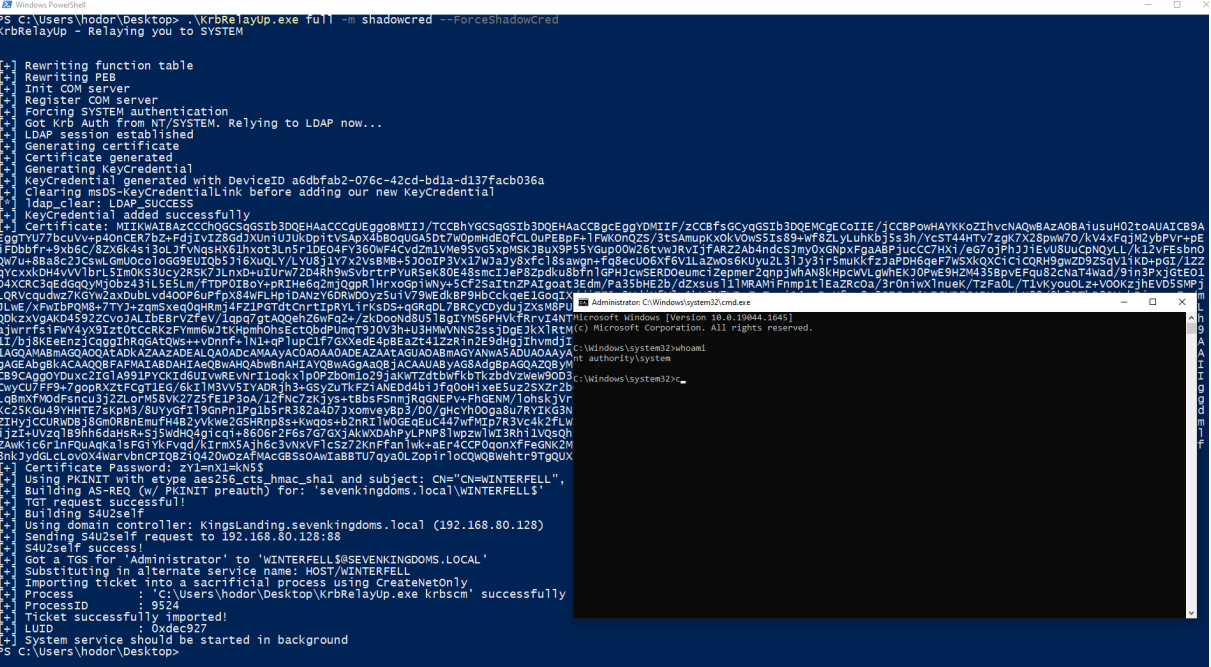
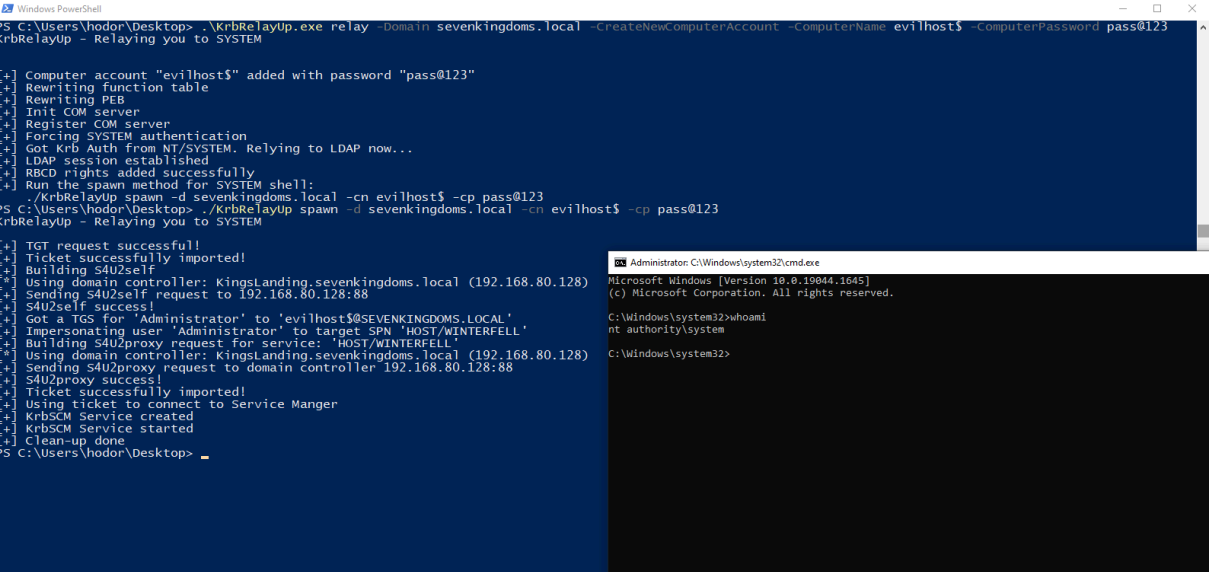
Usage: KrbRelayUp.exe krbscm <-s SERVICENAME> <-sc SERVICECOMMANDLINE>

```
-s (--ServiceName)           Name of the service to be created
-sc (--ServiceCommand)       Service command [binPath]. (default: %SystemRoot%\system32\cmd.exe)
```

General Options:

```
-d (--Domain)                 FQDN of domain. (Optional)
-dc (--DomainController)     FQDN of domain controller. (Optional)
-ssl                          Use LDAP over SSL. (Optional)
-n                             Use CreateNetOnly (needs to be enabled in Group Policy)
-v (--Verbose)                Show verbose output. (Optional)
```

Examples



TODO

- ☒ Code refactoring and cleanup!!!
- ☒ Add ShadowCred attack as a RELAY method
- ☐ Add TGTDELEG attack in SPAWN method to be used in Network Service->SYSTEM scenarios (potatoes alternative)
- ☒ Fix the issue I'm having trying to combine the RELAY and SPAWN methods into one run so it can be used as one complete command. Probably has something to do with the fact that both RELAY and SPAWN functionalities rely on hooks during the initialization of the COM Server (Once RELAY initializes its COM Server the SPAWN can't re-initialize it to place its hooks as well)

Mitigation & Detection

- Enforce LDAP Signing and LDAP Channel Binding to mitigate the relay of the machine account KRB auth to LDAP. This can be configured via the "Domain Controller: LDAP server signing requirements" GPO. (Thank you [Will Dormann](#) for your [tweet](#) on this matter)
- Make the attack requirements harder to obtain by setting the [MS-DS-Machine-Account-Quota attribute](#) in AD to 0, thus removing the ability of any user to add a new machine account to the domain. This is a dangerous default setting in AD - make sure you change it.
- Setting the flag "Account is sensitive and cannot be delegated" on all admin accounts (or put them in protected users) would make it so there is no account with the privileges required that can be delegated in order to complete the attack path. (Thanks to [Christoph Faltz](#) for this [tweet](#))
- Mitigation for ADCS Relay - Enforcing the use of TLS on the *certsrv* site and enabling **Extended Protection for Authentication (EPA)** in IIS will prevent the relay to ADCS. (Thanks to [Will Dormann](#) for pointing that out in his [tweet](#), this also was mentioned in [Dirk-jan Mollema](#) post on [Relaying Kerberos over DNS using krbrelayx and mitm6](#))
- Resources for possible monitoring and detection rules:
 - i. https://github.com/tsale/Sigma_rules/blob/main/windows_exploitation/KrbRelayUp.yml (@Kostastsale)
 - ii. <https://twitter.com/SBousseaden/status/1518976397364056071> (@SBousseaden). Mainly the rule about authentication to Service Manager via Kerberos from 127.0.0.1, Great Work!.
 - iii. https://www.linkedin.com/posts/john-dwyer-xforce_threathunting-threatdetection-blutteam-activity-6924739962131140608-py45/ (John Dwyer @TactiKoolSec)
 - iv. <https://twitter.com/cyb3rops/status/1519241598311321601> (@cyb3rops)

Acknowledgements

- [James Forshaw](#) for his research on [Kerberos relaying](#) and for figuring out how to [use Kerberos Service Tickets for LOCAL authentication to Service Manager](#) which was the missing piece of the puzzle in order to make this attack primitive **local only** (before that, we had to export the ST to a remote machine in order to use it and gain privileged access to our target machine). Also for his [New-MachineAccount](#) functionality which was used in this project.
- [Cube0x0](#) This project wouldn't exist without his amazing work on [KrbRelay](#) - a lot of code was taken from there and it made me gain a deeper understanding on how Kerberos Relaying works (I really recommend going through the code for anyone who wish to understand the concept better).
- [Elad Shamir](#) for his research on [Shadow Credentials](#) and his awesome tool [Whisker](#) - parts of his code (and of course [cube0x0](#)'s [KrbRelay](#) code) was used to add support for the Shadow Credentials attack in this tool.
- [Will Schroeder](#) and everyone who contributed to [Rubeus](#) which we all know and love. Basically all the RBCD-S4U functionality was taken from there. Also, for

- [Certify](#) and the [Certified Pre-Owned whitepaper](#) (credits goes to [Lee Christensen](#) as well) which was used when adding the ADCS Web Enrollment Relay option.

 - [batsec](#) and everyone who contributed to [ADCS Pwn](#). A lot of code related to the ADCS Web Enrollment Relay option was taken from this awesome tool.
 - [Michael Grafnetter](#) for his tool [DSInternals](#) which was used here to help with the Shadow Credentials functionality.
 - [Orange-Cyberdefense](#) for their work on [GOAD](#), the Active Directory research lab I

