Hacking Articles
Raj Chandel's Blog

Credential Dumping: DCSync Attack

posted in RED TEAMING on MAY 26, 2020 by RAJ CHANDEL

The most of the Organisation need more than one domain controller for their Active Directory and to maintain consistency among multiple Domain controller, it is necessary to have the Active Directory objects replicated through those DCs with the help of MS-DRSR refer as Microsoft feature Directory Replication Service (DRS) Remote Protocol that is used to replicate users data from one DC to another. Taking Advantage of this feature the attack abuse the MS-DRSR using Mimikatz-DCSYNC.

Table of Content

What is DCSYNC Attack

The Mimikatz DCSYNC-function allows an attacker to replicate Domain Controller (DC) behaviour. Typically impersonates as a domain controller and request other DC's for user credential data via GetNCChanges.

But compromised account should be a member of administrators, Domain Admin or Enterprise Admin to retrieve account password hashes from the others domain controller. As a result, the intruder will build Kerberos forged tickets using a retrieved hash to obtain any of the Active Directory 's resources and this is known as Golden Ticket attack.

Walkthrough on DCSYNC Attack

Mimikatz

So, here we have a normal user account, hence at present User, Yashika is not the member of any privileged account (administrators, Domain Admin or Enterprise Admin).

When the attacker attempts to execute the command MimiKatz-DCSYNC to get user credentials by requesting other domain controllers in the domain, this will cause an error as shown in the image. This is not possible.

So now we have granted Domain Admins right for user Yashika and now yashika has become the member of domain Admin Group which is also AD a privileged group.

We then confirmed this by listing the details of user Yashika 's group information and found that she is part of the domain admin group.

Now let ask for a credential for KRBTGT account by executing the following command using mimikatz:

```
lsadump::dcsync /domain:ignite.local /user:krbtgt
```

As a result, it will retrieve the KRBTGT NTLM HASH, this hash further can be used to conduct the very famous GOLDEN Ticket attack, read more about it from **here**.

Similarly, for every user account in the domain with the same command, we can obtain credentials. Here, it not only requests the current hash but also seeks to get the previous credentials stored.

```
lsadump::dcsync /domain:ignite.local /user:kavish
```

PowerShell Empire

If you want to conduct this attack remotely, PowerShell Empire is one of the best tools to conduct DCSYNC attack. Only you need to compromise the machine who is member privilege account (administrators, Domain Admin or Enterprise Admin) as shown here.

Now load the following module that will invoke the mimikatz Powershell script to execute the dcsync attack to obtain the credential by asking from an others domain controller in the domain. Here again, we will request for KRBTGT account Hashes and as result, it will retrieve the KRBTGT NTLM HASH.

```
usemodule credentials/mimikatz/dcsync_hashdump
set user krbtgt
execute
```

Likewise, the Empire has a similar module that retrieves the hash of the entire domain controller users account.

```
usemodule credentials/mimikatz/dcsync_hashdump
execute
```

Metasploit

If you have meterpreter session of the victim machine who account is member of domain admin, then here also you can execute Mimikatz-DCSYNC attack in order to obtain user's password.

If your compromised account is a member of the domain admin group, then without wasting time load KIWI and run following command:

```
dcsync_ntlm krbtgt
dcsync krbtgt
```

As a result, we found the hashes for krbtgt account and this will help us to conduct Golden Ticket attack for further.

ABOUT THE AUTHOR

RAJ CHANDEL

Raj Chandel is Founder and CEO of Hacking Articles. He is a renowned security evangelist. His works include researching new ways for both offensive and defensive security and has done illustrious research on computer Security, exploiting Linux and windows, wireless security, computer forensic, securing and exploiting web applications, penetration testing of networks. Being an infosec enthusiast himself, he nourishes and mentors anyone who seeks it.

PREVIOUS POST
← DEVRANDOM CTF:1.1 VULNHUB WALKTHROUGH

NEXT POST
LATERAL MOVEMENT: PASS THE TICKET ATTACK →

1 Comment

→
CREDENTIAL DUMPING: DCSYNC ATTACK

PORLOCKZZZ
June 8, 2020 at 8:13 am

Hello,
Thanks for your sharing.
Is there a github or somethings that i can establish my trainning environment?

REPLY ↓

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

Notify me of follow-up comments by email.

Notify me of new posts by email.

POST COMMENT

Search

ENTER KEYWORD

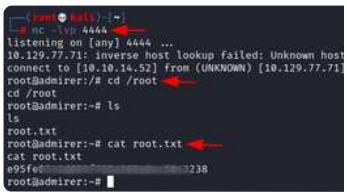
Subscribe to Blog via Email

Email Address

SUBSCRIBE

Join our Training Programs

Follow me on Twitter



Categories

- Cryptography & Stegnography
- CTF Challenges
- Cyber Forensics
- Database Hacking
- Footprinting
- Hacking Tools
- Kali Linux
- Nmap
- Others
- Password Cracking
- Penetration Testing
- Pentest Lab Setup
- Privilege Escalation
- Red Teaming
- Social Engineering Toolkit
- Uncategorized
- Website Hacking

- Window Password Hacking
- Wireless Hacking

Articles

Select Month