Tutorial for NTDS goodness (VSSADMIN, WMIS, NTDS.dit, SYSTEM)

November 21, 2013 | 2 Minute Read

Share:

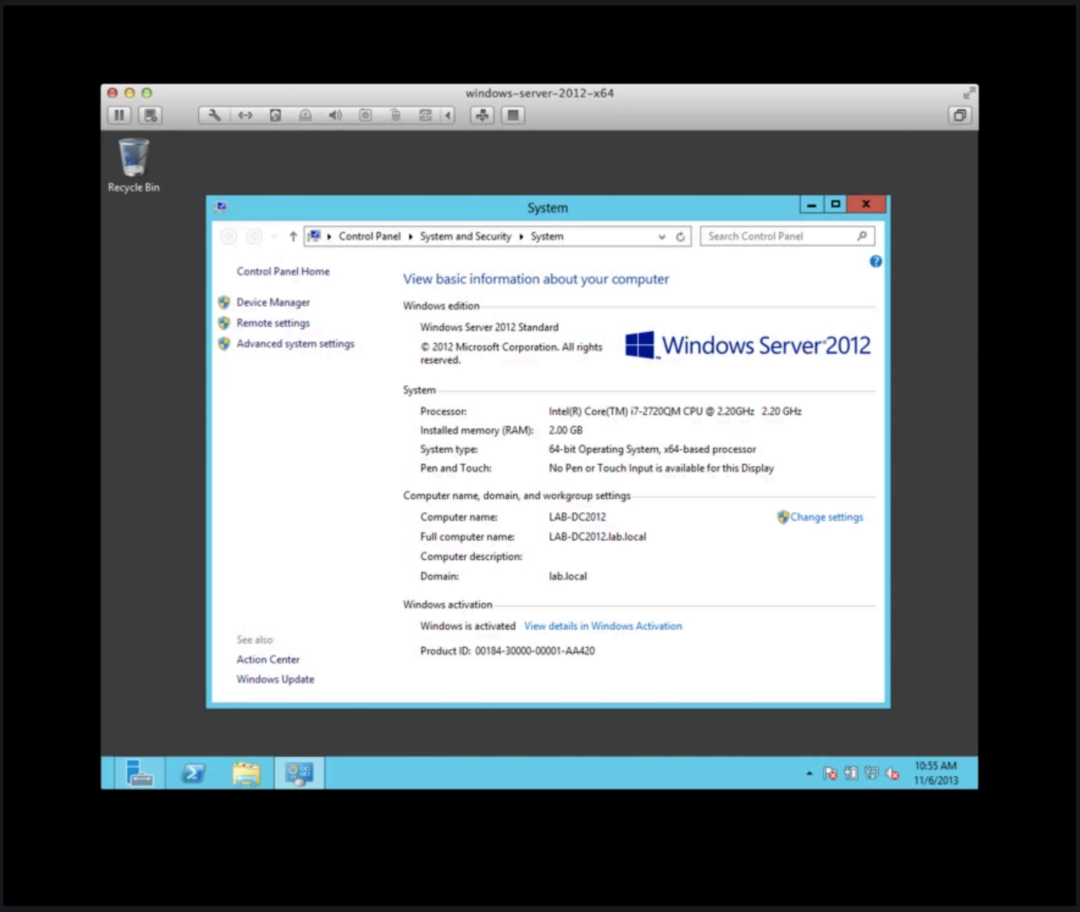
I recently performed an internal penetration test where the NTDS.dit file got me thousands of password hashes. After compromising unpatched Microsoft Windows computers on the client's domain, I gained access to a number of domain accounts. Below I'll explain how I did it.

The client had two domain controllers, one Windows 2003 and one Windows 2008. One of the domain accounts obtained via other

The NTDS.dit file is the Active Directory database. It stores all Active Directory information including password hashes.

Facebook Malvertising Epidemic – Unraveling a Persistent Threat: SYS01 →

I recreated the scenario, to demonstrate it on a Windows 2012 server.



View basic information about your computer

Windows edition

Windows Server 2012 Standard
© 2012 Microsoft Corporation. All rights reserved.

System

Processor: Intel(R) Core(TM) i7-2720QM CPU @ 2.20GHz 2.20 GHz
Installed memory (RAM): 2.00 GB
System type: 64-bit Operating System, x64-based processor
Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name: LAB-DC2012
Full computer name: LAB-DC2012.lab.local
Computer description:
Domain: lab.local

Windows activation

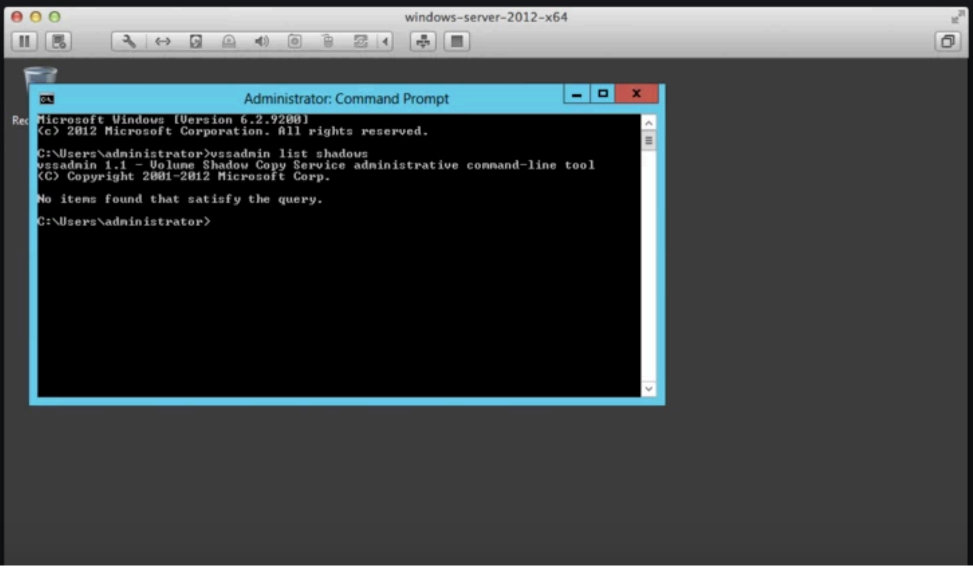
Windows is activated
Product ID: 00184-30000-00001-AA420

There are various ways of accessing the NTDS.dit file. It can't just be copied when it is in use (similar to a SAM file).

A technology that is included in Microsoft Windows itself is the Volume Snapshot Service or Volume Shadow Copy Service. It requires the partition to run NTFS, and it is the same technology used to
create a Windows backup or automatic system restore point.

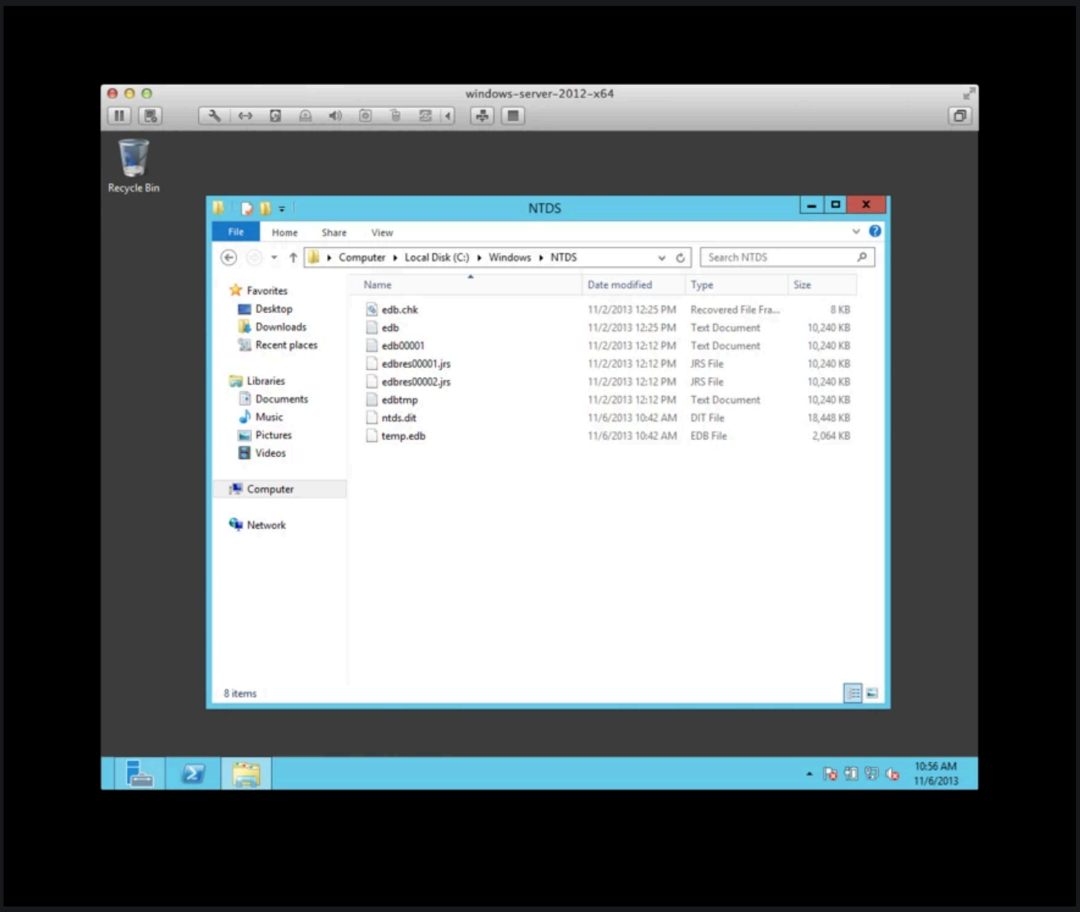
The command line utility I used was VSSADMIN.

The command determines whether there are current volume shadow copies that exist or if we need to create one:



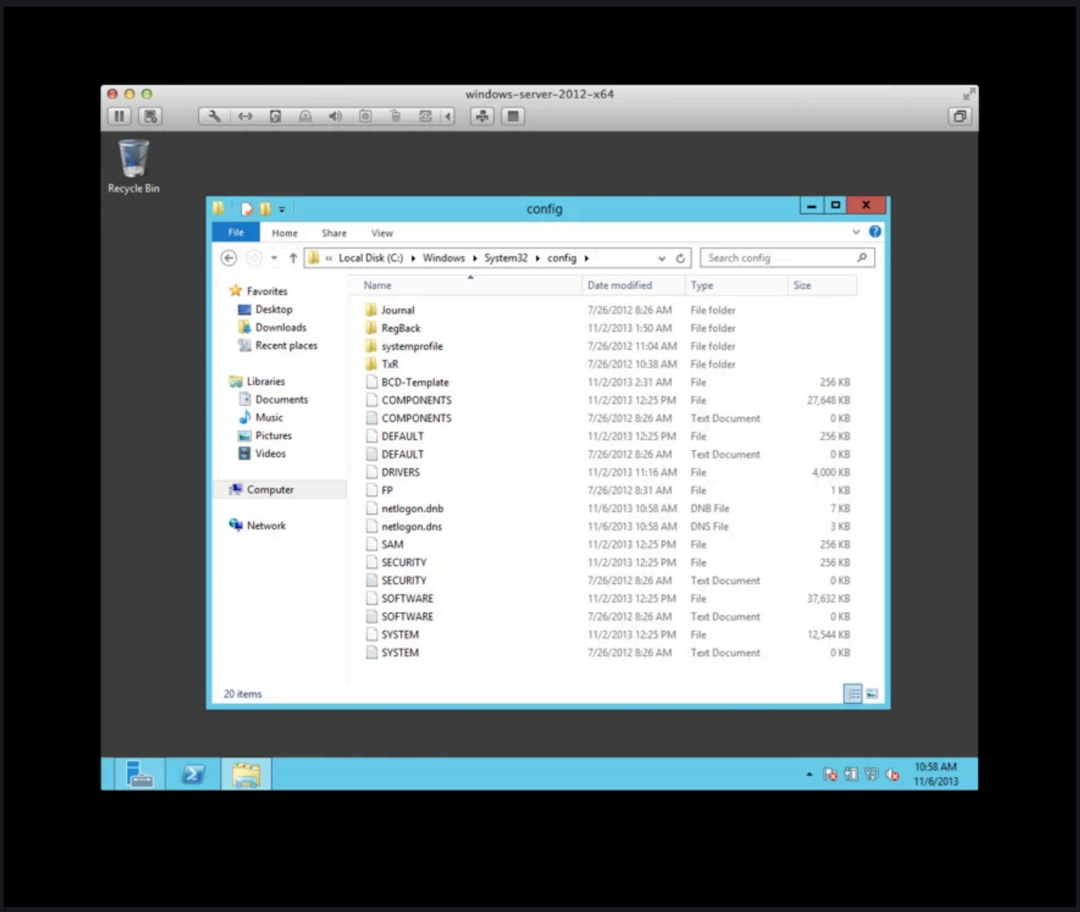
```
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\administrator>vssadmin list shadows
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2012 Microsoft Corp.

No items found that satisfy the query.

C:\Users\administrator>
```

The default path is c:\windows\ntds\ntds.dit. But it could be on any other drive, for example I found it on d:\NTDS\ntds.dit in my test.



Name	Date modified	Type	Size
edb.chk	11/2/2013 12:25 PM	Recovered File Fra...	8 KB
edb	11/2/2013 12:25 PM	Text Document	10,240 KB
edb00001	11/2/2013 12:12 PM	Text Document	10,240 KB
edbres00001.jrs	11/2/2013 12:12 PM	JRS File	10,240 KB
edbres00002.jrs	11/2/2013 12:12 PM	JRS File	10,240 KB
edbtmp	11/2/2013 12:12 PM	Text Document	10,240 KB
ntds.dit	11/6/2013 10:42 AM	DIT File	18,448 KB
temp.edb	11/6/2013 10:42 AM	EDB File	2,064 KB

I also created the SYSTEM file in path c:\windows\system32\.



Name	Date modified	Type	Size
Journal	7/26/2012 8:26 AM	File folder	
RegBack	11/2/2013 1:50 AM	File folder	
systemprofile	7/26/2012 11:04 AM	File folder	
TxR	7/26/2012 10:38 AM	File folder	
BCD-Template	11/2/2013 2:31 AM	File	256 KB
COMPONENTS	11/2/2013 12:25 PM	File	27,648 KB
COMPONENTS	7/26/2012 8:26 AM	Text Document	0 KB
DEFAULT	11/2/2013 12:25 PM	File	256 KB
DEFAULT	7/26/2012 8:26 AM	Text Document	0 KB
DRIVERS	11/2/2013 11:16 AM	File	4,000 KB
FP	7/26/2012 8:31 AM	File	1 KB
netlogon.dnb	11/6/2013 10:58 AM	DNB File	7 KB
netlogon.dns	11/6/2013 10:58 AM	DNS File	3 KB
SAM	11/2/2013 12:25 PM	File	256 KB
SECURITY	11/2/2013 12:25 PM	File	256 KB
SECURITY	7/26/2012 8:26 AM	Text Document	0 KB
SOFTWARE	11/2/2013 12:25 PM	File	37,632 KB
SOFTWARE	7/26/2012 8:26 AM	Text Document	0 KB
SYSTEM	11/2/2013 12:25 PM	File	12,544 KB
SYSTEM	7/26/2012 8:26 AM	Text Document	0 KB

A shadow copy of the c: drive had been created.

Next I copied the NTDS.dit file to a place where it could be retrieved on the main (non-shadowed) drive.

Then I did the same with the SYSTEM file.

The two files were then copied to the root of the c: drive.

I used Kali 1.0.5 as my attack platform.

To use the mount command to mount to the default Windows share, I needed cifs-utils on Kali.

Then I mounted the network share.

Next I copied the two files to the attack system.

This can be done remotely without interactively logging-on to the server by using the "wmic" command from any Windows computer. Kali's WMIS package allowed me to do the same.

Next, I ran the VSSADMIN command to list shadows remotely with WMIS.

Next I checked the output.txt file to see what happened.

Then I checked that the root was empty and deleted the previous NTDS.dit and SYSTEM files I copied.

I copied the NTDS.dit file, using WMIS.

Note that the shadow copy folder has three slashes ('\\\').

Next I copied the SYSTEM file using WMIS.

Then I checked whether the files were copied on the previously mounted drive.

My next step was to get the password hashes.

First I needed to download and unzip ntdsxtract_v1_0.zip from http://www.ntdsxtract.com/.

Second, I needed to download and unzip ntds_dump_hash.zip from http://www.ntdsxtract.com/.

Then I compiled and made libesedb.

Other information could also be exported using esedbexport, but I was only interested in Table 4 where the password hashes are.

This took some time and resulted in the creation of a folder called ntds.dit.export containing a file called datatable.

Then I went to the creddump folder to run the dsdump python script.

From there, I could output the hashes into a file and use my favorite password-cracking tool to recover the passwords.

Enjoy!

ABOUT TRUSTWAVE

Trustwave is a globally recognized cybersecurity leader that reduces cyber risk and fortifies organizations against disruptive and damaging cyber threats. Our comprehensive offensive and defensive cybersecurity portfolio detects what others cannot, responds with greater speed and effectiveness, optimizes client investment, and improves security resilience. Learn more about us.

Latest Intelligence

2024 Trustwave Risk Radar Report: Cyber Threats to the Retail Sector →

Hooked by the Call: A Deep Dive into The Tricks Used in Callback Phishing Emails →

How Threat Actors Conduct Election Interference Operations: An Overview →

ent Response

Hunting

Leadership Team

Our History

News Releases

Media Coverage

Careers

Global Locations

Awards & Accolades

Trials & Evaluations

Contact

Support

Security Advisories

Software Updates

Legal Terms of Use Privacy Policy