Trustwave®

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

Share:

Stay Informed:

Subscribe

RESEARCH REPORT

November 21, 2013

2 Minute Read

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.

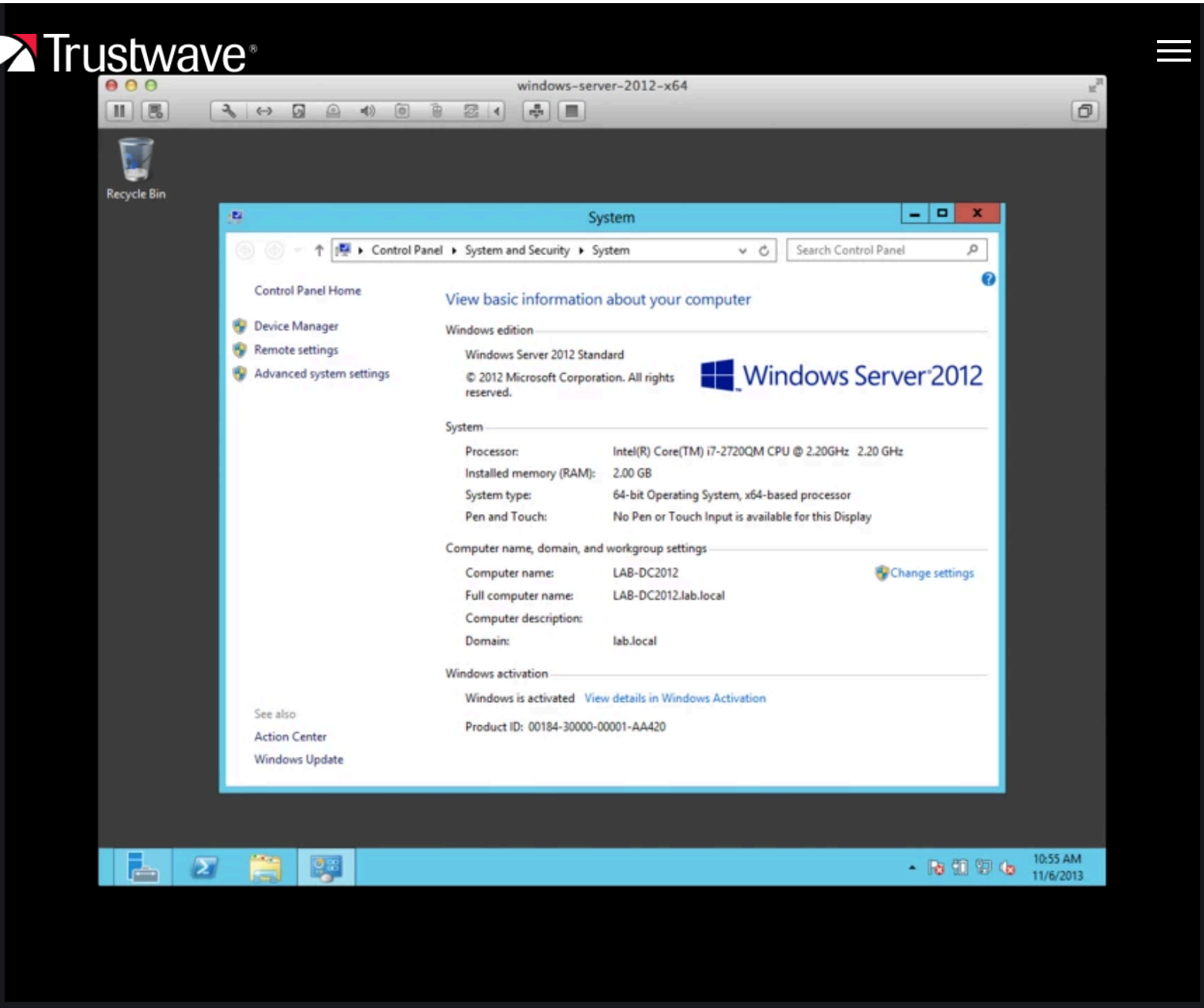
The client had two domain controllers, one Windows 2003 and one Windows 2008. One of the domain accounts obtained via other means (not described by this post) had rights to log-on locally on both domain controllers.

I attempted to dump the Active Directory database, but I couldn't get the SAM file through my usual methods. Eventually, and after much effort, I got the SAM file but found it only contained one hash.

The following actions allowed me to obtain the Active Directory password hashes. This method will work on Windows 2003, Windows 2008 and Windows 2012 servers.

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

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

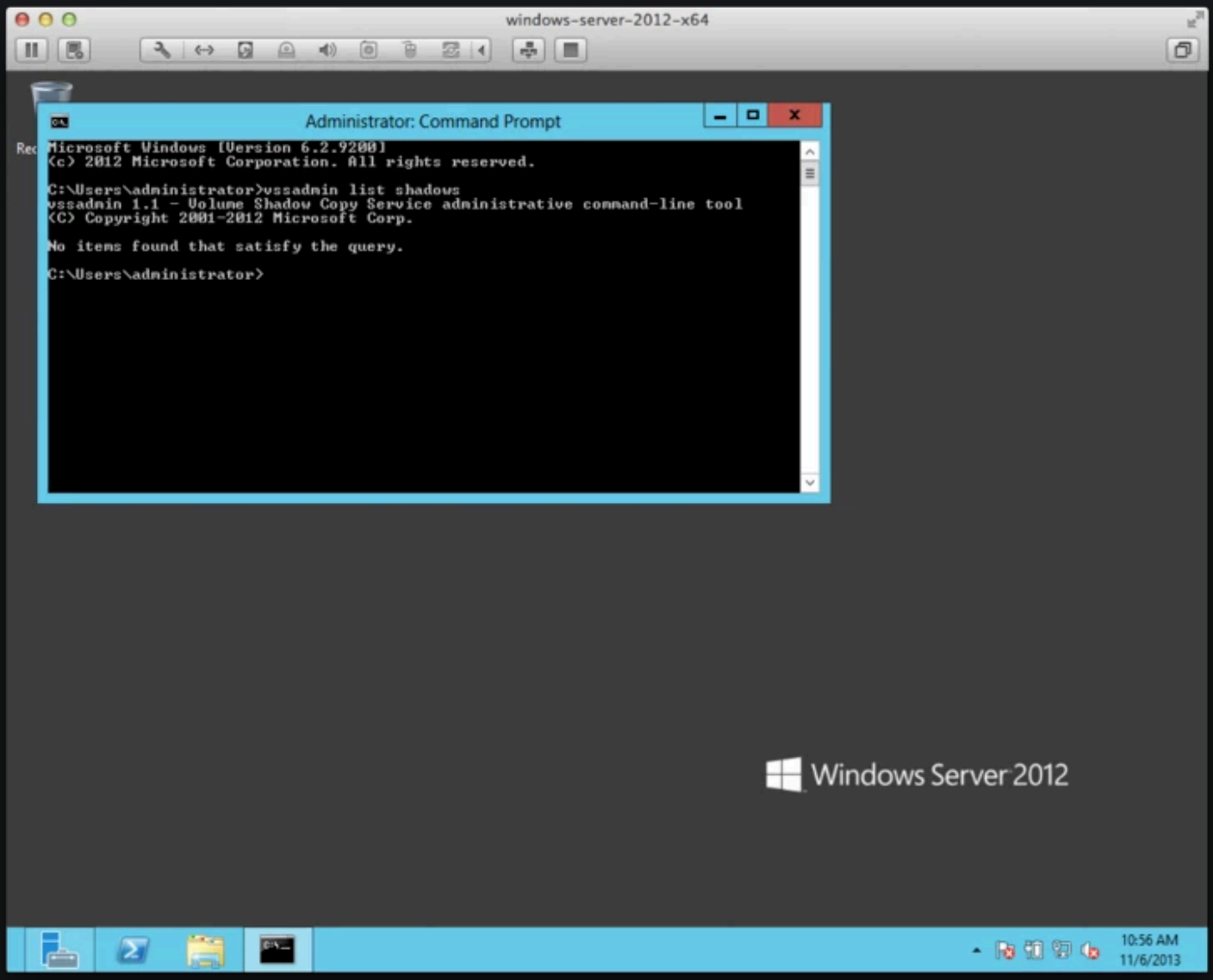


There are various ways of accessing the NTDS.dit file. It can't just be copied when it is in use (similar to a SAM file).

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.

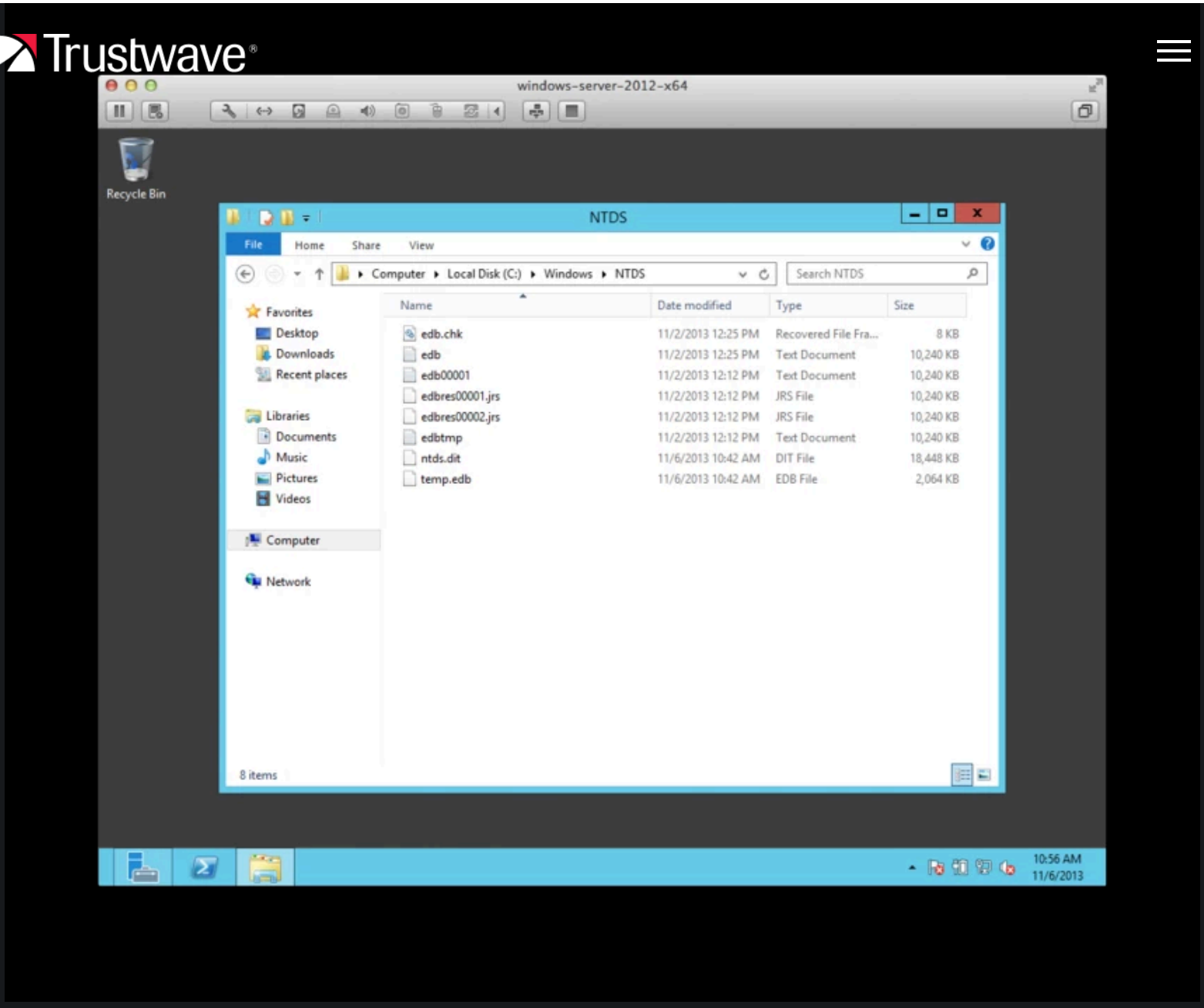
The command line utility I used was VSSADMIN.

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

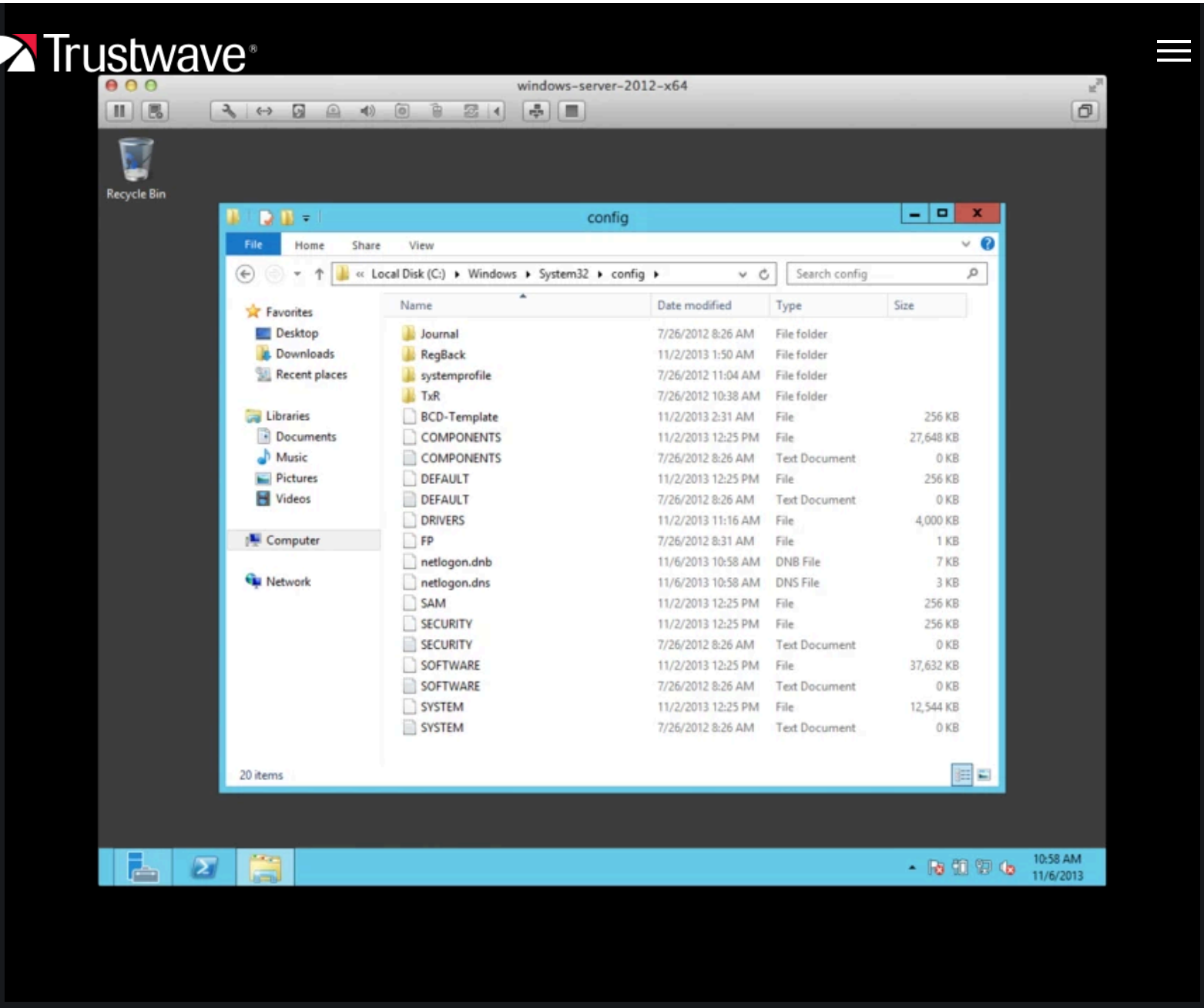


As you can see, no shadow copy existed yet. So I created one.

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.



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



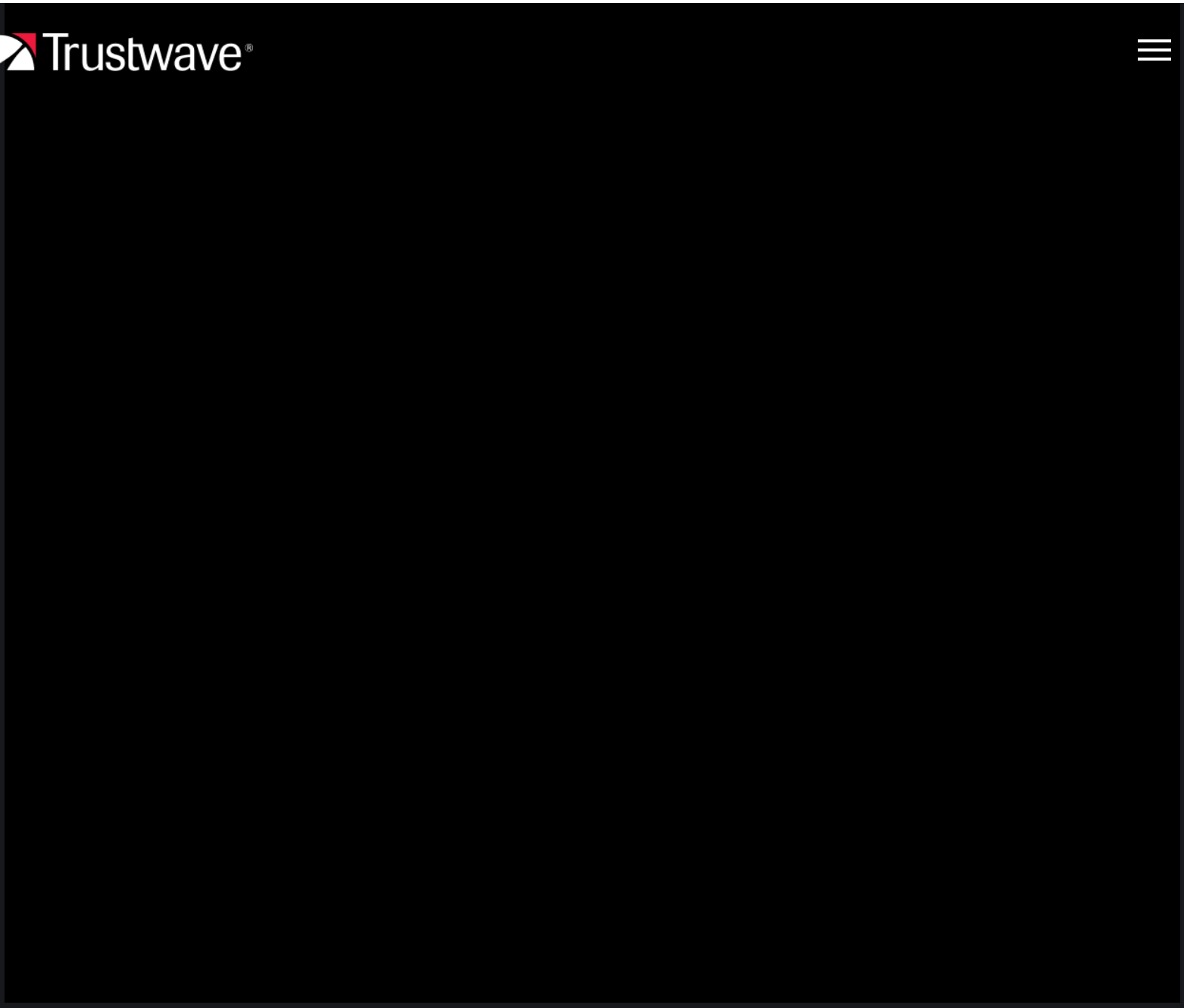
A shadow copy of the c: drive had been created.

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.

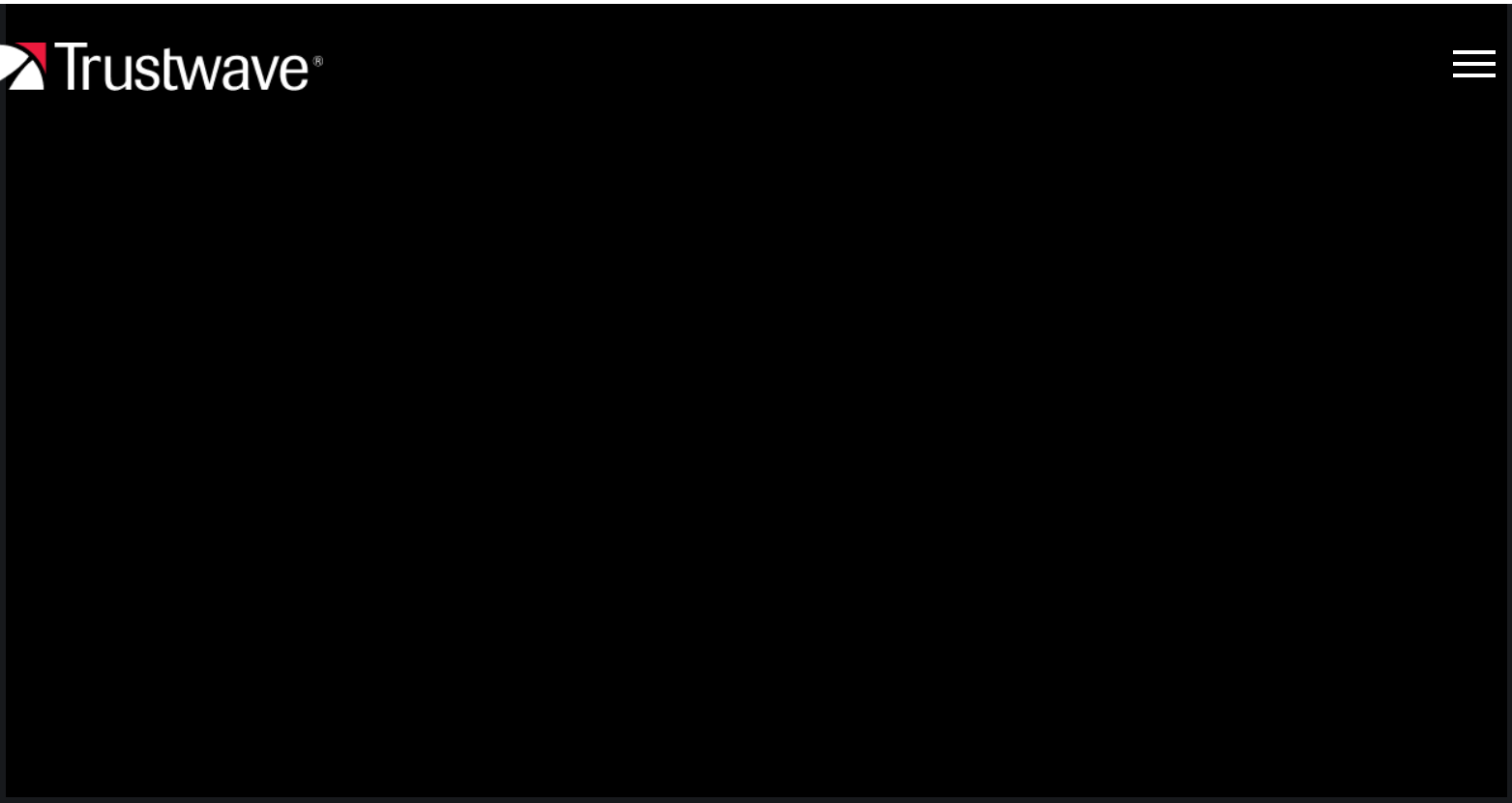
Next I copied the two files to the attack system.

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.

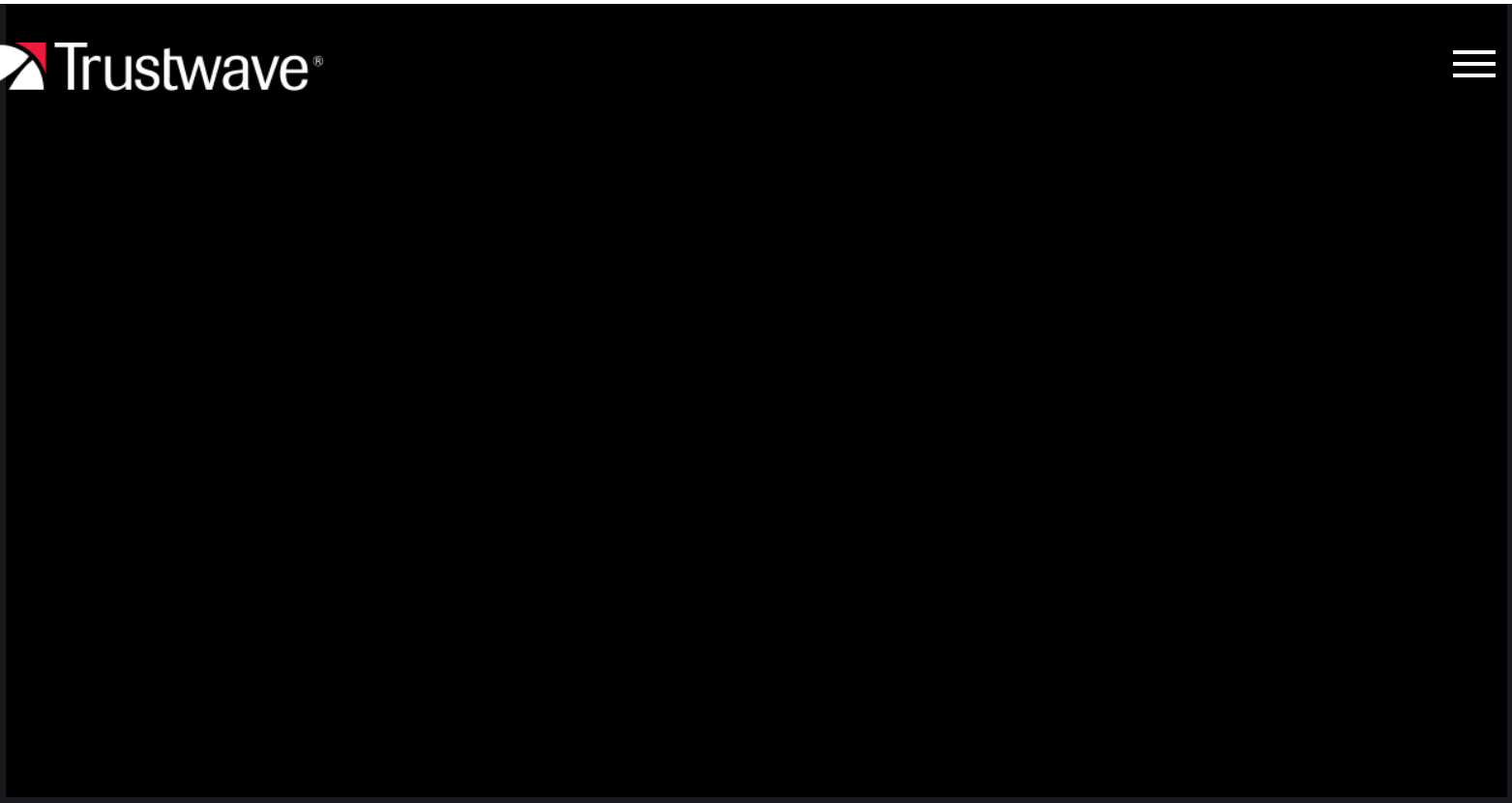


I copied the NTDS.dit file, using WMIS.

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.



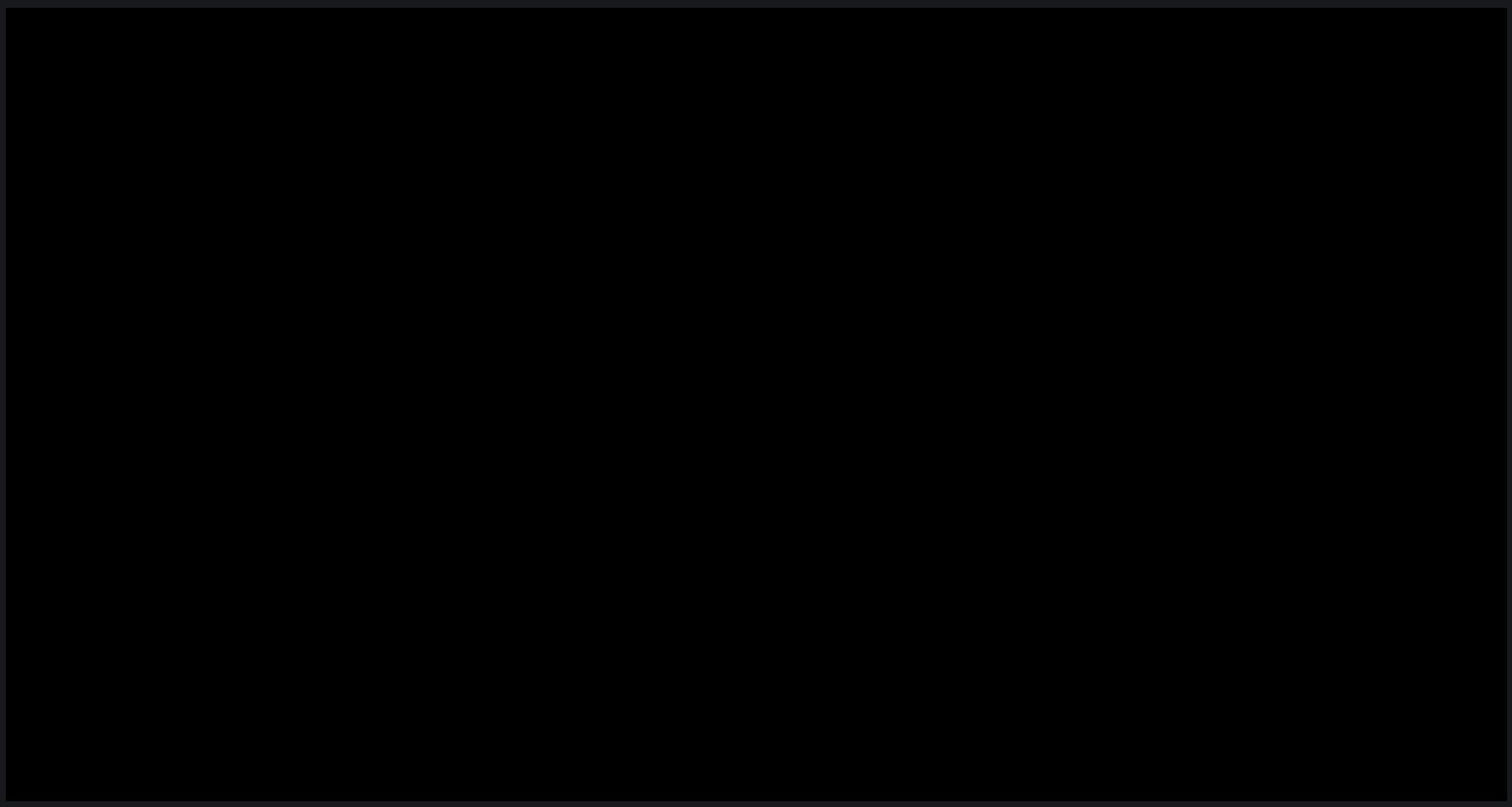
My next step was to get the password hashes.

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/.

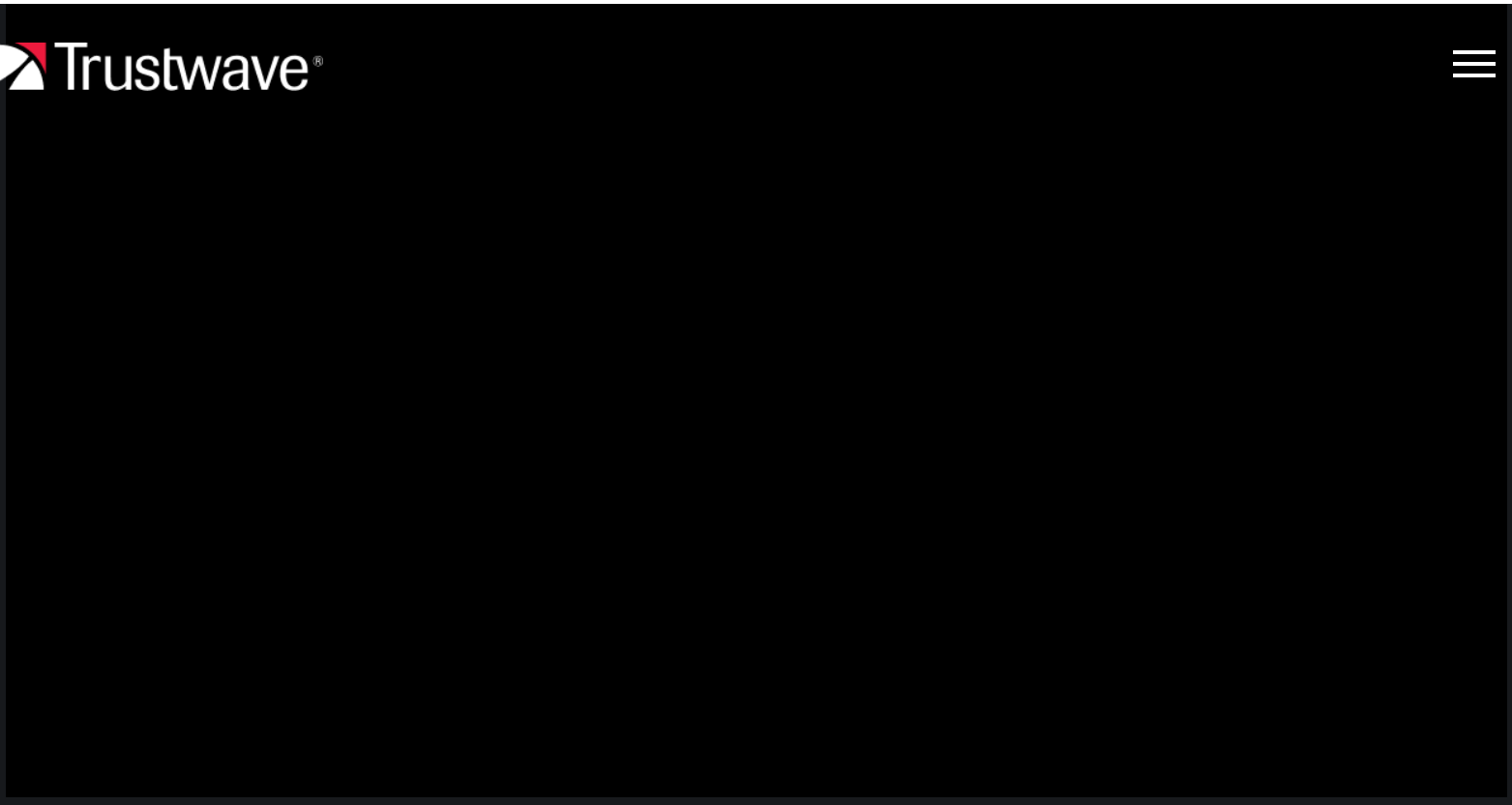
Then I compiled and made libesedb.

Here I exported tables from NTDS.dit, using the command esedbdumphash.

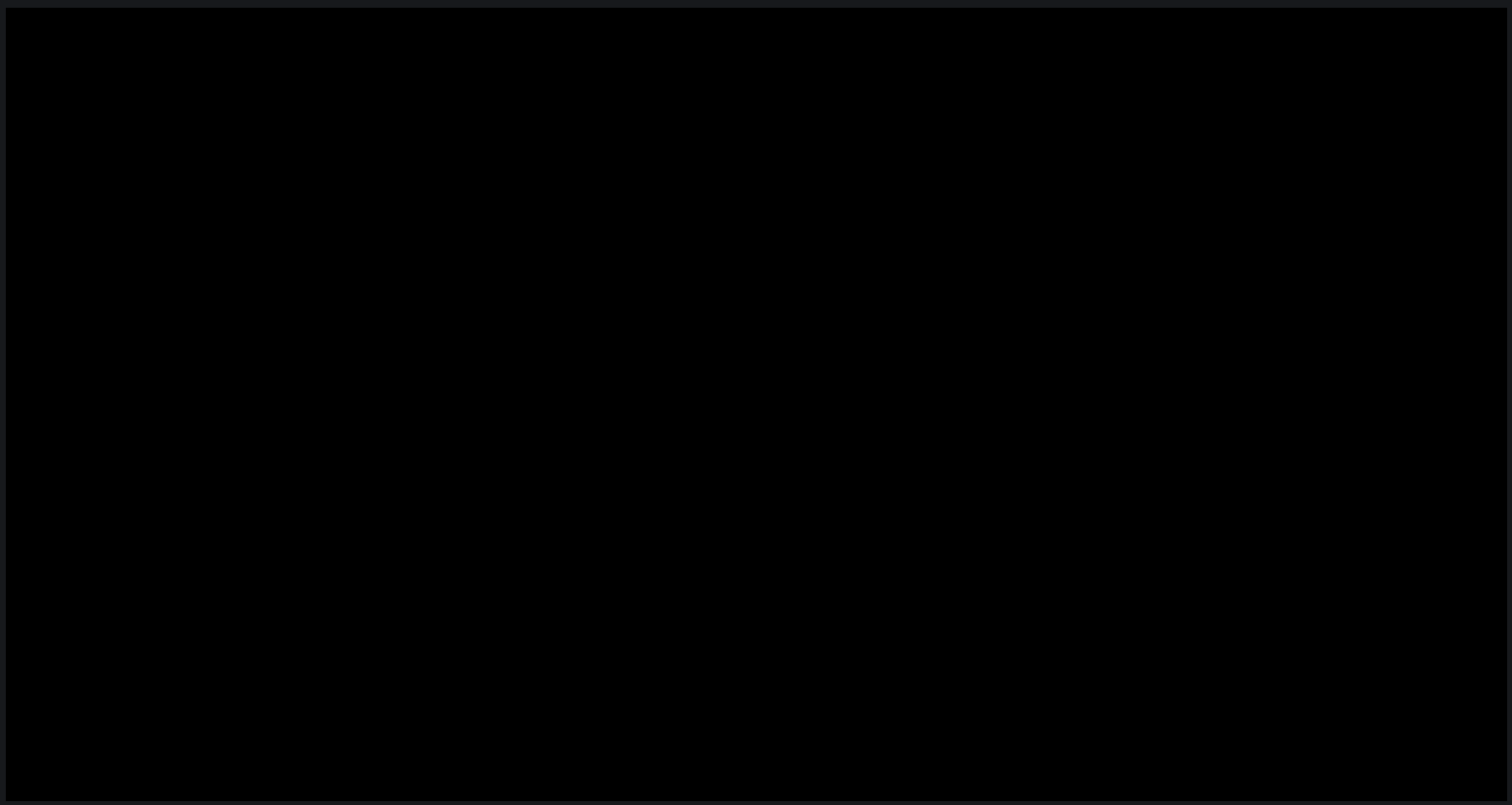


Other information could also be exported using esedbexport, but I was only interested in Table 4 where the password hashes are.

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

Trustwave

Stay Informed

Sign up to receive the latest security news and trends straight to your inbox from Trustwave.

Business Email*

Subscribe

Leadership Team
Careers
Our History
Global Locations
News Releases
Awards & Accolades
Media Coverage
Trials & Evaluations

Contact
Support
Security Advisories
Software Updates

Legal
Terms of Use
Privacy Policy