

NO PLACE TO HIDE


Hack the Box writeup

2/21/2021

Contents

Challenge.....	1
Process	1
Flag	4

Challenge

No Place To Hide [by feLamos] [38 solvers] 11 🍏 1 🗨️ Difficulty:  18/11/2020 ^

🔥 First Blood: HTB-Bot

We found evidence of a password spray attack against the Domain Controller, and identified a suspicious RDP session. We'll provide you with our RDP logs and other files. Can you see what they were up to?

[Download](#) Zip Password: `hackthebox sha256: db0866a21a3135e977d466163505667e57dd01fd1a1ffd281aba59a4abf16332`

Process

This PC > WDBLue (D:) > HTB > No Place To Hide >

Name	Date modified	Type	Size
bcache24.bmc	11/19/2020 6:57 AM	BMC File	0 KB
Cache0000.bin	11/19/2020 6:59 AM	BIN File	17,854 KB
no-place-to-hide.zip	2/21/2021 8:10 PM	zip Archive	2,715 KB

So, starting out I have two very important questions:

- 1: What is a bmc file?
- 2: How do I parse it?

I was able to find this blog post that conveniently explains both of those!

<https://www.allthingsdfir.com/do-you-even-bitmap-cache-bro/>

I went over to GitHub and grabbed bmc-tools

<https://github.com/ANSSI-FR/bmc-tools>

```
Windows PowerShell
PS D:\HTB\No Place To Hide> cd ..\_tools\
PS D:\HTB\_tools> git clone https://github.com/ANSSI-FR/bmc-tools.git
Cloning into 'bmc-tools'...
remote: Enumerating objects: 30, done.
remote: Counting objects: 100% (30/30), done.
remote: Compressing objects: 100% (24/24), done.
remote: Total 69 (delta 11), reused 24 (delta 6), pack-reused 39 receiving objects: 65% (45/69)
Receiving objects: 100% (69/69), 33.86 KiB | 1.69 MiB/s, done.
Resolving deltas: 100% (28/28), done.
```

I need to make a folder for these items to go so I made a directory called test so I could test out the tool.

I also realized the bmc file is empty so I used the cache0000.bin file instead.

```
PS D:\HTB\No Place To Hide> mkdir test

Directory: D:\HTB\No Place To Hide

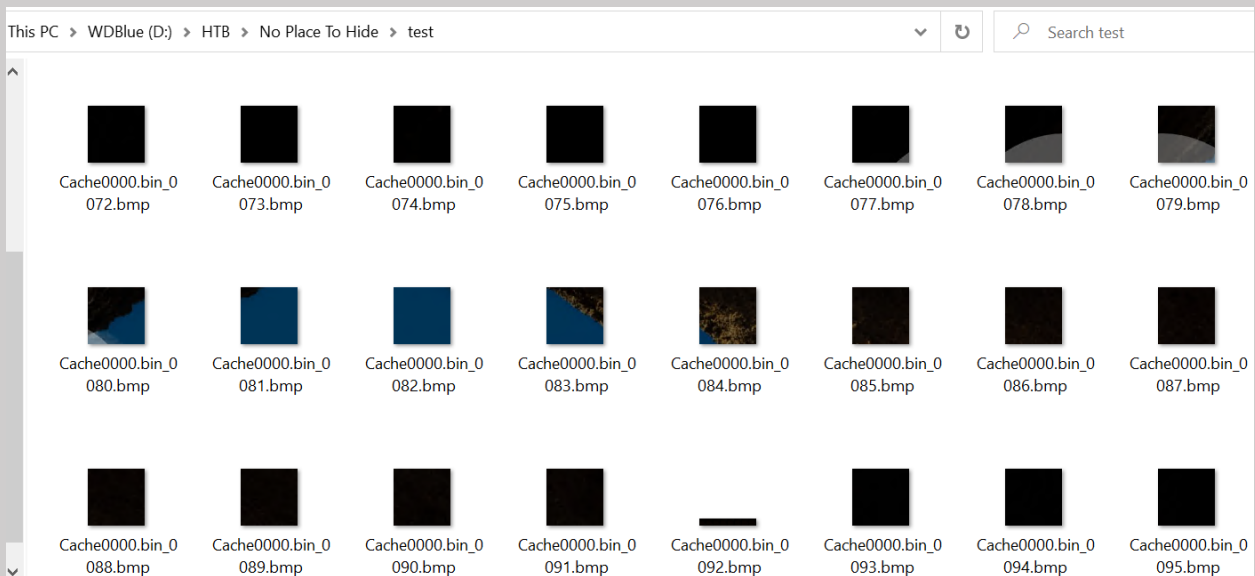
Mode                LastWriteTime         Length Name
----                -
d-----            2/21/2021   8:18 PM             test

PS D:\HTB\No Place To Hide> python.exe D:\HTB\tools\bmc-tools\bmc-tools.py -s .\cache0000.bin -d test
[++] Processing a single file: '.\cache0000.bin'.
[===] 1162 tiles successfully extracted in the end.
[===] Successfully exported 1162 files.
PS D:\HTB\No Place To Hide> ls .\test\

Directory: D:\HTB\No Place To Hide\test

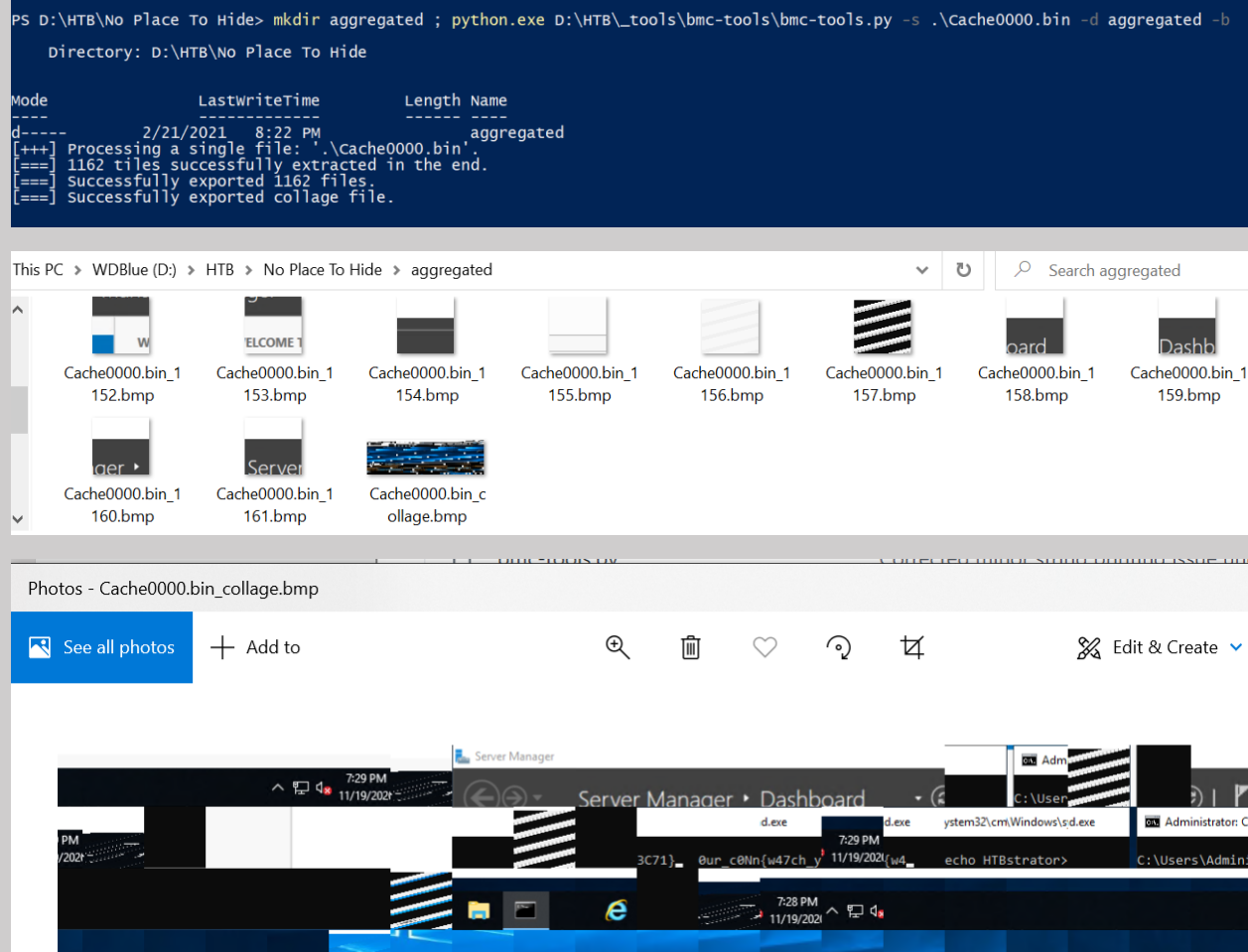
Mode                LastWriteTime         Length Name
----                -
-a-----            2/21/2021   8:19 PM        16506 Cache0000.bin_0000.bmp
-a-----            2/21/2021   8:19 PM         2170 Cache0000.bin_0001.bmp
-a-----            2/21/2021   8:19 PM        14458 Cache0000.bin_0002.bmp
-a-----            2/21/2021   8:19 PM        14458 Cache0000.bin_0003.bmp
-a-----            2/21/2021   8:19 PM         2170 Cache0000.bin_0004.bmp
-a-----            2/21/2021   8:19 PM        16506 Cache0000.bin_0005.bmp
-a-----            2/21/2021   8:19 PM        16506 Cache0000.bin_0006.bmp
-a-----            2/21/2021   8:19 PM         2170 Cache0000.bin_0007.bmp
-a-----            2/21/2021   8:19 PM        14458 Cache0000.bin_0008.bmp
-a-----            2/21/2021   8:19 PM         1914 Cache0000.bin_0009.bmp
-a-----            2/21/2021   8:19 PM        16506 Cache0000.bin_0010.bmp
-a-----            2/21/2021   8:19 PM        16506 Cache0000.bin_0011.bmp
-a-----            2/21/2021   8:19 PM        16506 Cache0000.bin_0012.bmp
-a-----            2/21/2021   8:19 PM        16506 Cache0000.bin_0013.bmp
-a-----            2/21/2021   8:19 PM        16506 Cache0000.bin_0014.bmp
-a-----            2/21/2021   8:19 PM        16506 Cache0000.bin_0015.bmp
-a-----            2/21/2021   8:19 PM        16506 Cache0000.bin_0016.bmp
```

I now have a bunch of fragments of what looks like a screenshot.



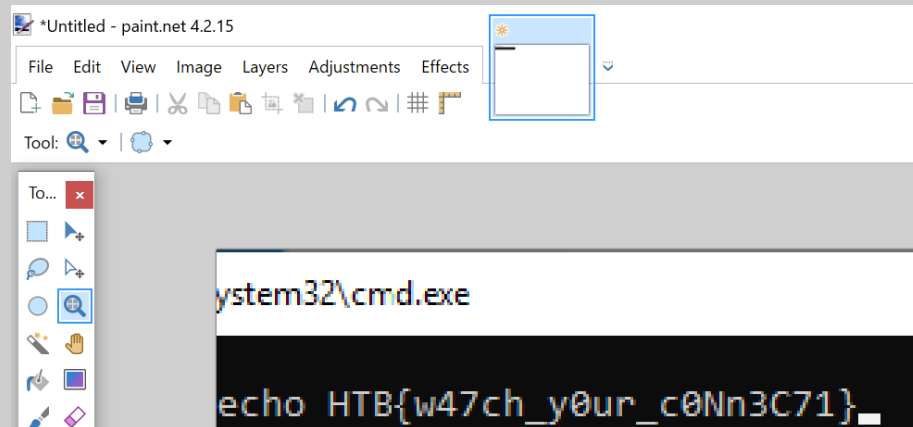
I looked through the documentation again to see if there was a way to combine all of these files together into a single picture, and it turns out there is.

I reran the command with the -b flag



So it isn't the best picture but I can make out a command prompt window.

I went back to the photos and grabbed the ones that contained the command prompt window and threw them into paint.net



Doing this I was able to pretty easily recreate the window and find the flag.

Flag

HTB{w47ch_y0ur_c0Nn3C71}