NO PLACE TO HIDE

Hack the Box writeup

Contents

Challenge	1
Process	1
Flag	4

Challenge

♣ First Blood: HTB-Bot	18/11/2020 ^
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?	ntified a suspicious RDP session. We'll provide you
Lownload Ztp Password: hackthebox sha256: db0866a21a3135e977d466163505667e57dd01fd1a1ffd281aba59a4abf16332	281aba59a4abf16332

Process

This	PC > WDBlue (D:) > HTB > No Place To F	lide »		~ ر
^	Name	Date modified	Туре	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 eceiving 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	e> mkdir tes	t	
	- \			
Direct	cory: D:\HTB\No F	Place To Hid	e	
мode	LastWr	riteTime	Length	Name
d	2/21/2021	8:18 PM		test
PS D:\HTB\	No Place Tọ Hìde	<pre>> python.ex</pre>	e D:\HTB_tc	ools\bmc-tools\bmc-tools.py -s .\Cache0000.bin -d test
[+++] Proc	essing a single	Tile: .\Ca	cheuuuu bin	
[===] 1162	2 tiles successfi	illy extract	ed in the en	la.
	essfully exporte		S.	
PS D:\HTB\	No Place To Hide	e> Is .\test	λ	
Direct	cory: D:\HTB\No F	Place To Hid	e∖test	
Mode	Lastwr	riteTime	Length	Namo
-a	2/21/2021 2/21/2021 2/21/2021	8:19 PM	16506	Cache0000.bin_0000.bmp
-a	2/21/2021	8:19 PM		Cache0000.bin_0001.bmp
-a	2/21/2021	8:19 PM		Cache0000.bin_0002.bmp
-a	2/21/2021	8:19 PM		Cache0000.bin_0003.bmp
-a	2/21/2021	8:19 PM		Cache0000.bin_0004.bmp
-a	2/21/2021 2/21/2021 2/21/2021 2/21/2021	8:19 PM		Cache0000.bin_0005.bmp
-a	2/21/2021	8:19 PM		Cache0000.bin_0006.bmp
-a	2/21/2021	8:19 PM		Cache0000.bin_0007.bmp
-a	2/21/2021	8:19 PM		Cache0000.bin_0008.bmp
-a	2/21/2021	8:19 PM		cache0000.bin_0009.bmp
-a		8:19 PM		Cache0000.bin_0010.bmp
-a	2/21/2021	8:19 PM		Cache0000.bin_0011.bmp
	2/21/2021	8:19 PM		Cache0000.bin_0012.bmp
		0120 110	T0200	
<u> </u>	2/21/2021	8:19 PM		Cache0000.bin_0013.bmp
-a	2/21/2021	8:19 PM	16506	
-a -a	2/21/2021 2/21/2021 2/21/2021	8:19 PM	16506 16506 16506	Cache0000.bin_0013.bmp

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

This F	PC > WDBlue (D:) >	HTB > No Place To	Hide > test			~ 1	ט 🔎 Search te	st
^	Cache0000.bin_0	Cache0000.bin_0	Cache0000.bin_0	Cache0000.bin_0	Cache0000.bin_0	Cache0000.bin_0	Cache0000.bin_0	Cache0000.bin_
	072.bmp	073.bmp	074.bmp	075.bmp	076.bmp	077.bmp	078.bmp	079.bmp
	Cache0000.bin_0	Cache0000.bin_0	Cache0000.bin_0	Cache0000.bin_0	Cache0000.bin_0	Cache0000.bin_0	Cache0000.bin_0	Cache0000.bin_0
	080.bmp	081.bmp	082.bmp	083.bmp	084.bmp	085.bmp	086.bmp	087.bmp
*	Cache0000.bin_0	Cache0000.bin_0	Cache0000.bin_0	Cache0000.bin_0	Cache0000.bin_0	Cache0000.bin_0	Cache0000.bin_0	Cache0000.bin_0
	088.bmp	089.bmp	090.bmp	091.bmp	092.bmp	093.bmp	094.bmp	095.bmp

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

ode		LastWriteTime	Length Name					
===1 1162	tiles suc	021 8:22 PM ingle file: '.\Cc cessfully extrac xported 1162 fil xported collage	aggr ache0000.bin'. ted in the end. es. file.	regated				
his PC 🔉 W	/DBlue (D:) »	HTB > No Place To	Hide 🔉 aggregated			~	ບ 🔎 Search a	ggregated
	w	ELCOME 1					oard	Dashb
	e0000.bin_1 52.bmp	Cache0000.bin_1 153.bmp	Cache0000.bin_1 154.bmp	Cache0000.bin_1 155.bmp	Cache0000.bin_1 156.bmp	Cache0000.bin_1 157.bmp	Cache0000.bin_1 158.bmp	Cache0000.bin 159.bmp
Cache	er ► 20000.bin_1 50.bmp	Server Cache0000.bin_1 161.bmp	Cache0000.bin_c ollage.bmp					
Photos - (Cache0000.b	in_collage.bmp		-			31 IIIIIIO SIIIIIIIII	
💌 See a	all photos	+ Add to		Ð	₫ ♡		X	Edit & Create
						_		_
			-29 PM /19/202t	Manager	Manager • Dasl		C:\User tem32\cm\Windows\s;d.exe)
PM	11111				71}_ 0ur_c0Nn{w47c	7:29 PM	cho HTBstrator>	C:\Users\Adm

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

🛃 *Untitled - paint.net 4.2.15 🛛 😹
File Edit View Image Layers Adjustments Effects 🔍
□ 📑 🖹 🖶 🗶 🐚 🗞 🖄 1 🖍 ∩ □ ♯ 🦵
Tool: 🔍 👻 💮 🕶
To ×
o a ystem32\cmd.exe
🔨 🧶
[™] ■
echo HTB{w47ch_y0ur_c0Nn3C71}_

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

Flag

HTB{w47ch_y0ur_c0Nn3C71}