How the Soldier's Saved Christmas

SANS Holiday Challenge 2012

by
Don Williams
Alex Dierkes

List of captured flags:

Heat Miser:

Zone 0:
flag: 1732bcff12e6550ff9ea44d594001418
Zone 1:
flag: d8c94233daef256c42bb95bd61382e02
Zone 2:
flag: ef963731de7e886226fe4a6a6c2971f1
Zone 3:
flag: 0d524fb8d8f9f88eb9da5b286661a824
Zone 4:
flag: e3ae414e6d428c3b0c7cff03783e305f
Zone 5:
flag: f478c549e37fa33467241d847f862e6f

Snow Miser:

Zone 0:
flag: 3b5a630fc67251aa5555f4979787c93f
Zone 1:
flag: 38bef0b61ba8edda377b626fe6708bfa
Zone 2:
flag: b8231c2bac801b54f732cfbdcd7e47b7
Zone 3:
flag: 08ba610172aade5d1c8ea738013a2e99
Zone 4:
flag: de32b158f102a60aba7de3ee8d5d265a
Zone 5:
flag: 3ab1c5fa327343721bc798f116be8dc6

Each question is answered throughout the story!

How the Soldier's Saved Christmas
by Don Williams and Alex Dierkes

Twas' the night before Christmas and all through the house, not a creature was stirring not even a mouse. I sat there and waited for the Jolly Old Man but he never showed up while reading the tech manual in my hand. I didn't know why but I started to worry. Why didn't St. Nicholas come here in a hurry?

I am deployed for the Army in a place that is scary, but he has always arrived with lots of merry. What will the solders think when they wake with no gifts; will they cry or be worried for the Jolly St. Nick? For it may be possible that his sleigh was shot down, by the terrorists Al Qaeda or Taliban. Next, my mind wondered if we were the first, for that meant no presents for my kids or the rest of Earth. I was not home to give my kids the bad news, that if St Nicholas was gone, that means Christmas was too.

Then all of a sudden I heard a loud "BANG", it was my friend Don writhing in pain. He knocked so hard to get my attention, for he had discovered there has been a dissension. He began to explain that Santa was sick, and didn't feel like Great St. Nick. He told me of Mrs. Claus and her attempt to bring cheer, that ended up with two elves crashing in Southtown along with Vixen the Reindeer. The angry old Mayor hatched an evil plan, that if the two elves wanted Vixen out of the can, they must bring a white Christmas to Southtown's land.

Therefore, Mrs. Claus went to find the leader of Frost, for if she was to free Vixen, Snow Miser was the cost. She begged and she pleaded this cold chilly man, and he agreed to provide the snow for the plan. He did make mention with a sly little smirk, unless his hotheaded brother agreed, this plan will not work. So off went Mrs. Claus to find the leader of Hot, for if she was to save Christmas, she must convince the Heat Miser to turn off his boiling pot. He agreed to the plan but with one condition; that he is allowed to turn off the North Pole's air condition. Mrs. Claus called up Frost, and offered the deal, but Frost would not have it, "Heat in the North Pole, for real?" Mrs. Claus was tired of the boy's games, and went to Mother Nature to put out the flames. Mother Nature told the boys make the deal, to the North some heat and the South some chill. The boys, always clever, hatched their own challenge of tag, for they would play capture the flag. My friend explained the rules of the game, and that both brothers agreed to keep it tame.

Unfortunately, neither brother was smart enough to win, so my friend and I decided to chip in. It was getting close to the end for St. Nick, if he wasn't in the air soon it wouldn't mean a lick. Don decided to decipher the code from Heat Miser while I went after the code from Snow Miser. To our excitement of the challenge at hand, we began to research and to save Christmas was our plan. We began to look at the Zone 0 site for any information that may give some insight.

For the rest of this story we will split it by site, first with Don's glory and then my might! For Heat Miser's page provided what Don needed next, on how to find Zone 1 through the robots.txt.

Heat Miser

Zone 0
http://heatmiser.counterhack.com/zone-0-0AD9934A-8081-462B-8364-9ADBFE963E91/
flag: 1732bcff12e6550ff9ea44d594001418

On Heat Miser's Zone 0 site you see, "We had a security concern where the Zone 1 URL ended up in search engine results. We added a file to prevent the search engines from caching these pages." This led Don to go to http://heatmiser.counterhack.com/robots.txt where we see:

How the Soldier's Saved Christmas
by Don Williams and Alex Dierkes

```
User-agent: *
Disallow: /zone-1-E919DBF1-E4FA-4141-97C4-3F38693D2161
Disallow: /zone-2-*
Disallow: /zone-3-*
Disallow: /zone-4-*
Disallow: /zone-5-*
```

Zone 1
http://heatmiser.counterhack.com/zone-1-E919DBF1-E4FA-4141-97C4-3F38693D2161/
flag: d8c94233daef256c42bb95bd61382e02

This provided Don with the Zone 1 link, and this made him begin to think. Could this be that easy, and finding the answers are just that cheesy? His next mission was for Zone 2 of course, and his first step was to view the page's source. To his amazement, the answer was there, right in the source for all to snare. When viewing the page source of Zone 1 Don found the following lines hidden or commented out:

<!-- redacted, too many people clicked on the link and took it offline
Zone 2
-->

Zone 2
http://heatmiser.counterhack.com/zone-2-761EBBCF-099F-4DB0-B63F-9ADC61825D49/
flag: ef963731de7e886226fe4a6a6c2971f1

Immediately, Don cheered for he knew, that the cold in the south slowly grew. Next, his task was simple and neat, for he had to find Zone 3's unique link. He searched and searched the typical ways like viewing the source or the pictures displayed. It took him awhile to realize there was nothing there, so "Off to the internet he declared!" He found the Twitter site and followed the tweets, which Heat Miser posted with all of his treats. Don's 24-inch monitor brightly glowed and through a picture, the link it showed. In a picture so dark, normal monitors failed to see, the link so light a little translucent you see. A tip helped him discover this neat little trick, from Snow Miser's tweets he learned very quick. A statement so tame it took a retake that Heat Miser failed to realize his mistake. Snow Miser states, "Another oops. Brilliant move @h34t_m1s3r. Your OS X term is semi-transparent, hot head! Oh, & u don't need Metasploit for any of these zones." This led Don to the discovery through his bright monitor that the Metasploit picture Heat Miser posted held the key to Zone 3.

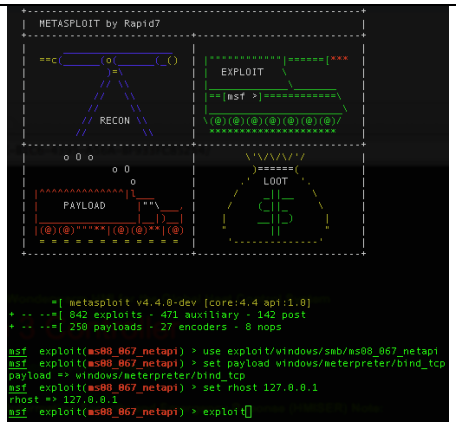


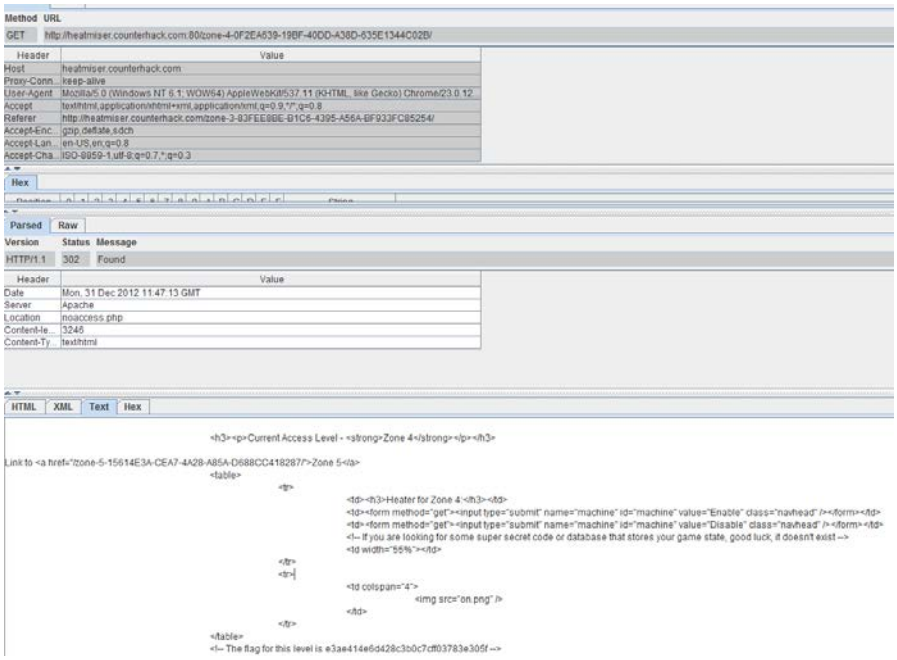
Figure 1 - **Heat Miser's Tweet Post**

Figure 2 - Zoomed in where the link is located

While the image is not easily seen, on Don's monitor it was very keen; the Zone 3 link was very clean. Using Windows Paint.exe and zoomed in close, Don extracted the code from the translucent ghost.

Zone 3
http://heatmiser.counterhack.com/zone-3-83FEE8BE-B1C6-4395-A56A-BF933FC85254/
flag: 0d524fb8d8f9f88eb9da5b286661a824

Don now knew that the last two zones would not be as easy, for Zone 3 had made him a little queasy. While visiting Zone 3, he found the link that he would need, but denied him access you see. This little challenge was an easy quest; all he needed to do was capture the response and request. He pulled out WebScarab by OWASP, the proxy tool of choice that helped him find his web voice. As he captured each request and response, a mistake was found, one that failed to exit and allowed him to capture the page source for Zone 4. This mistake showed the link to Zone 5, and allowed Don to continue and his hopes to survive.


Method URL
GET http://heatmiser.counterhack.com:80/zone-4-0F2EA639-19BF-40DD-A38D-635E1344C02B/
Header Value
Host heatmiser.counterhack.com
Proxy-Conn... keep-alive
User-Agent Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.11 (KHTML, like Gecko) Chrome/23.0.12...
Accept text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer http://heatmiser.counterhack.com/zone-3-83FEE8BE-B1C6-4395-A56A-BF933FC85254/
Accept-Enc... gzip,deflate,sdch
Accept-Lan... en-US,en;q=0.8
Accept-Cha... ISO-8859-1,utf-8;q=0.7,*;q=0.3
Hex
Parsed Raw
Version Status Message
HTTP/1.1 302 Found
Header Value
Date Mon, 31 Dec 2012 11:47:13 GMT
Server Apache
Location noaccess.php
Content-le... 3246
Content-Ty... text/html
HTML XML Text Hex
<h3> Current Access Level - Zone 4 </h3>
Link to Zone 5
<table>
<tr>
<td><h3>Heater for Zone 4:</h3></td>
<td><form method="get"><input type="submit" name="machine" id="machine" value="Enable" class="navhead" /></form></td>
<td><form method="get"><input type="submit" name="machine" id="machine" value="Disable" class="navhead" /></form></td>
<!-- If you are looking for some super secret code or database that stores your game state, good luck, it doesn't exist -->
<td width="55%"></td>
</tr>
<tr>
<td colspan="4">

</td>
</tr>
</table>
<!-- The flag for this level is e3ae414e6d428c3b0c7cf03783e305f -->

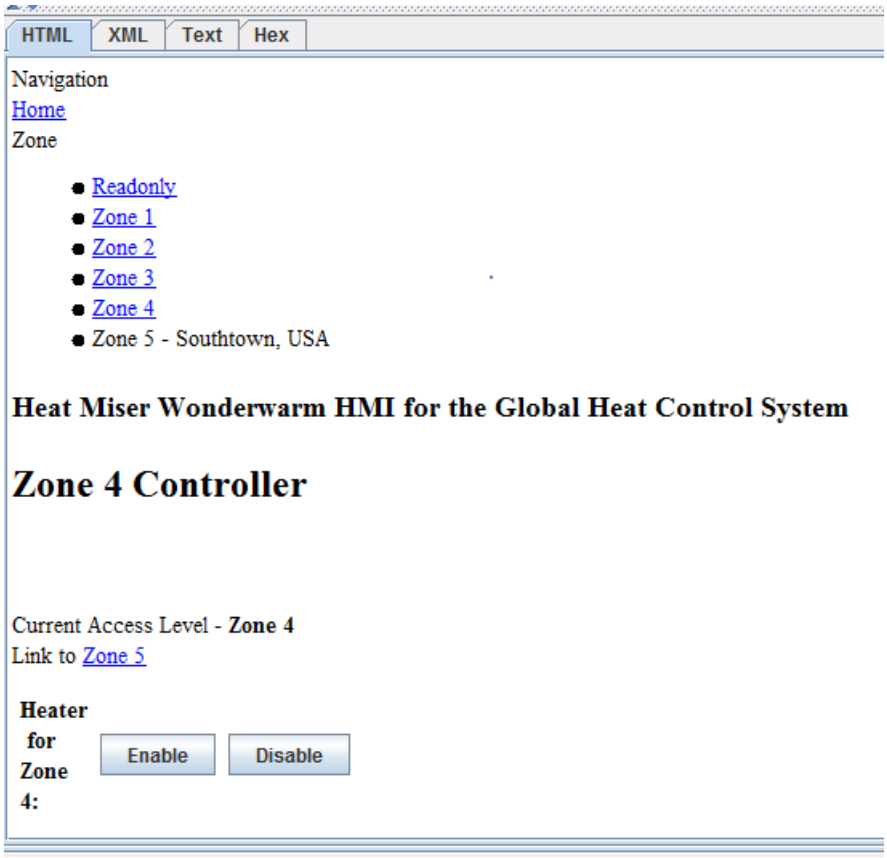


Figure 4 - HTML Capture of Zone 4 Response

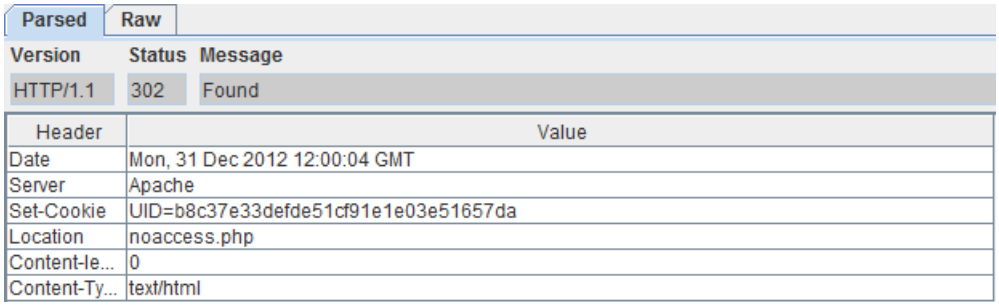
Zone 4
http://heatmiser.counterhack.com/zone-4-0F2EA639-19BF-40DD-A38D-635E1344C02B
flag: e3ae414e6d428c3b0c7cff03783e305f

At this moment of success, Don could barely contain, his emotions and excitement, but he knew to win the final Zone he must maintain. His composure changed, determined and willed he will beat Heat Miser so the south could be chilled. With his tools already on, and his will to survive, he continued to catch the request and responses to access Zone 5. After awhile of captures, Don realized there was one difference, Heat Miser had a method in place causing him hindrance. The use of a cookie to determine his access, made Don understand that he needed to hack less. To gain access to Zone 5 he didn't need to argue, all he needed to do was change the cookie's value. However, what UID was this cookie for, was it some new algorithm that closed this door? In that moment Don had an epiphany, this was a 32-bit hex value, and it had to be an MD5 hash if any. To verify his thought, he went online, an MD5 decrypter was divine. When he put in the hash it spit out 1001, which led him to a clue left by Snow Miser. Snow Miser left a clue in his tweets so nice, right there in the open but Don didn't think twice. This clue was only realized when he deciphered the hash, that it was there all along in Snow Miser's stash. "Mmmmm, @h34t_m1s3r left 1001 cookies for Santa, I see!" This tip left behind by Snow Miser, ensured that Don was all the wiser. He was right to assume that an MD5 hash was in use, giving him the ability to find a misuse.

He had found the way that was used and it was a disaster, but lacked the knowledge of which UID was the master. Don tested a few UIDs known to all, 0 for root but he hit a wall. All the UIDs he tried did not

work, he began to write a script in Python and go bizerk. During his script planning phase he tested a line with the number 1, when it attempted to connect he realized he had won. The value he needed to defeat Heat Miser was the MD5 hash of the first UID in his stash.

Don captured the request and responses for Zone 5 and replaced the Set-Cookie value of UID=b8c37e33defde51cf91e1e03e51657da with the MD5 hash value for the number 1. The new Set-Cookie value of UID=c4ca4238a0b923820dcc509a6f75849b allowed Don access to Heat Miser's Zone 5 and to turn off the Heat Miser Wonderwarm HMI for the Global Heat Control System. Don disabled Heat Miser's heater, and brought some chill to Southtown's theater.

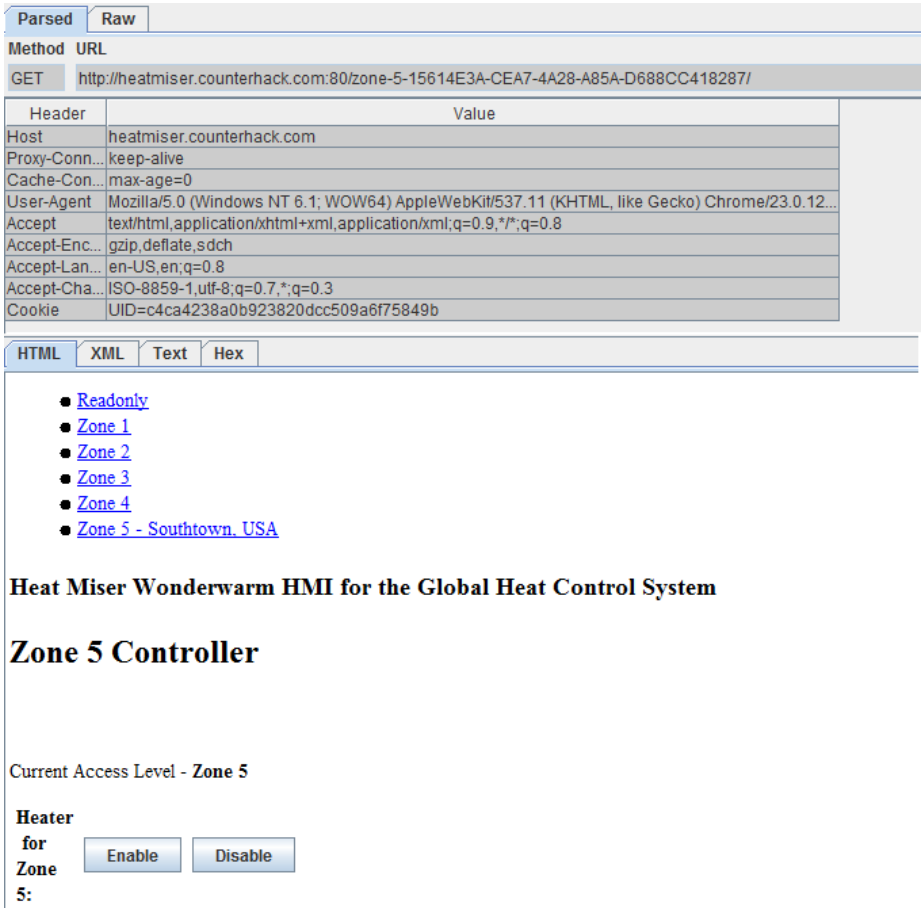


Parsed | Raw

Version	Status	Message
HTTP/1.1	302	Found

Header	Value
Date	Mon, 31 Dec 2012 12:00:04 GMT
Server	Apache
Set-Cookie	UID=b8c37e33defde51cf91e1e03e51657da
Location	noaccess.php
Content-le...	0
Content-Ty...	text/html

Figure 5 - Captured Response with Set-Cookie



Parsed | Raw

Method	URL
GET	http://heatmiser.counterhack.com:80/zone-5-15614E3A-CEA7-4A28-A85A-D688CC418287/

Header	Value
Host	heatmiser.counterhack.com
Proxy-Conn...	keep-alive
Cache-Con...	max-age=0
User-Agent	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.11 (KHTML, like Gecko) Chrome/23.0.12...
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Enc...	gzip,deflate,sdch
Accept-Lan...	en-US,en;q=0.8
Accept-Cha...	ISO-8859-1,utf-8;q=0.7,*;q=0.3
Cookie	UID=c4ca4238a0b923820dcc509a6f75849b

HTML | XML | Text | Hex

- Readonly
- Zone 1
- Zone 2
- Zone 3
- Zone 4
- Zone 5 - Southtown, USA

Heat Miser Wonderwarm HMI for the Global Heat Control System

Zone 5 Controller

Current Access Level - **Zone 5**

Heater for Zone 5: Enable Disable

Figure 6 - Captured with Cookie Set to MD5 Hash of UID 1

SNOW MISER

While Don pursued the fiery depths of Heat Miser's site, I began my analysis to determine Snow Miser's might. Immediately, Don bragged that he made it past Zone 1, and with a robots.txt, it was easily won. I tried to see if the same flaw was there, but all I got was a request that was unaware. So now, I knew the tasks would differ, so off on my own I would venture.

Zone 0
http://snowmiser.counterhack.com/zone-0-11698563-7582-4A51-B567-B4710BBE783F/
flag: 3b5a630fc67251aa5555f4979787c93f

To master Zone 1 took a little sass, since we found the link in the water glass. While researching Snow Miser's Twitter posts, I saw that he added a taunting toast. The image he posted, as I had suspected, in the water glass there it reflected; the Zone 1 link right there in the drink. It was not hard to get the code, all I had to use was zoom in mode. I opened the picture with Windows Paint, to get the link that looked so quant.

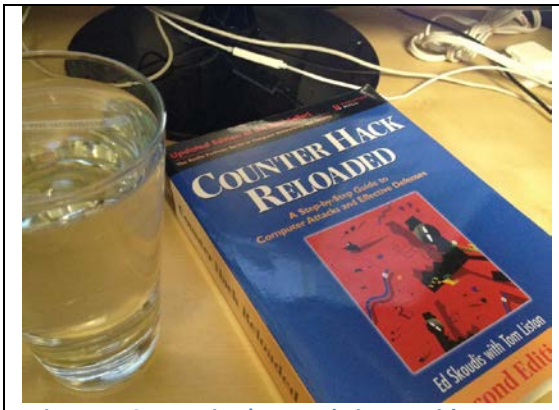


Figure 7 - Snow Miser's Posted Picture with Zone 1 Link

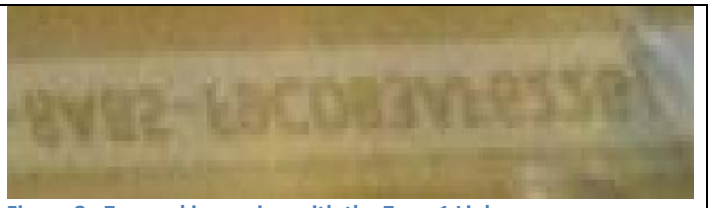


Figure 8 - Zoomed in version with the Zone 1 Link

Zone 1
http://snowmiser.counterhack.com/zone-1-D2E31380-50E6-4869-8A85-F9CDB3AF6226/
flag: 38bef0b61ba8edda377b626fe6708bfa

After my victory, I needed another win, so off I went for Zone 2 again. This Zone seemed different; it caught my attention for I realized that the off image had a different extension. What I found strange had me say maybe, since I found in the user comment "IceIceBaby!". By using Exiftool.exe I grabbed the metadata, which gave me the password to break out the data. Stegonagraphy was the game and with the user comment, the link I could claim.

I downloaded off.jpg from Zone 1 disabled website. I used Exiftool.exe version 8.79 to pull the metadata from off.jpg. I found in the User Comment "IceIceBaby!" as seen below:

User Comment : IceIceBaby!

How the Soldier's Saved Christmas
by Don Williams and Alex Dierkes

Since question 2 StegHide it did state, I took the easiest road first and attempted my fate. Using steghide version 0.5.1, I entered the following command to learn I had won:

steghide.exe extract -sf off.jpg -p "IceIceBaby!" -xf extracted.txt

When I viewed extracted.txt, the excitement set me off for I realized what was next; off to Zone 3 you see.

Zone 2
http://snowmiser.counterhack.com/zone-2-6D46A633-25D7-42C8-AF94-8E786142A3E3/
flag: b8231c2bac801b54f732cfbdcd7e47b7

My time was getting short and my nerves were shaken, since I couldn't seem to find what Snow Miser was makin. I searched up and down but the link I never found. I took a deep breath and researched some more, and that was when I found the door. Heat Miser extracted Snow Miser's phone, which gave me a chance to not go it alone. For in this Android pack the answer would sing, all I had to do was find the right search string.

I downloaded android.data.tgz from Heat Miser's Twitter post and extracted android.data.tar. By using Notepad++ version 6.1, I opened the android.data.tar file and searched for the following strings:

Zone 3, Zone 2, Zone 1.

The results from these three searches provided me not only Zone 3's link but also Zone 1 and Zone 2's. This meant that there was more than one way to find the earlier Zone answers. This is what I found through my searches:

*
Readonly
*
*
Zone 1
*
*
Zone 2
*
*
Zone 3
*
*
Zone 4
*
*
Zone 5 - North Pole
*

So I searched the phone to find the link, pretty nifty don't you think? All three Zones were found and I jumped off the ground. For I knew I was getting close and about to have a cow, cause I would soon be able to free Vixen from the hoosegow!

Zone 3
http://snowmiser.counterhack.com/zone-3-EAB6B031-4EFA-49F1-B542-30EBE9EB3962/
flag: 08ba610172aade5d1c8ea738013a2e99

The next Zone was the best, for it challenged me more than the rest. It took awhile to find I must say, but soon I did realize that xor was the way. Since I had a known and a cipher, I could pull the key and be the wiser. Using Python I wrote the code, but first I had to convert the known using hex mode.

Once I had the hex value for our known link I then had to xor the known hex into the known cipher. This will produce the key. Using the key, we will xor the key into the unknown cipher for the new Zone 4 link.

This will give us a Hex value that we would then decode into the valid link for Zone 4. The following commands were ran to get the link:

python

###** First, I have to encode the plaintext string into a hex value**###
>>> "zone-4-F7677DA8-3D77-11E2-BB65-E4BF6188709B".encode("hex")

###**This is the hex value of the above plain text link**###
'7a6f6e652d342d46373637374441382d334437372d313145322d424236352d4534424636311383837303942'

###** I take the known cipher text on the website and xor it with the above hex value for the known link. **###
###**This is a plaintext xor attack**###

>>> print hex(0x20d916c6c29ee53c30ea1effc63b1c72147eb86b998a25c0cf1bf66939e8621b3132d83abb1683df619238 ^
0x7a6f6e652d342d46373637374441382d334437372d313145322d424236352d4534424636311383837303942)

###**This is the key of the xor function above**###
'0x5ab678a3efaac87a07dc29c8827a245f273a8f5cb4bb1485fd36b42b0fdd4f5e05709e0c8a2ebbe851ab7a'

###** I then take the key and xor it into the cipher text of the unknown link**###
###**This gives me a plaintext hex string**###

>>> print hex(0x5ab678a3efaac87a07dc29c8827a245f273a8f5cb4bb1485fd36b42b0fdd4f5e05709e0c8a2ebbe851ab7a ^
0x20d916c6c29ee54343e81ff1b14c1372650cbf19998f51b5c51bf66f49ec62184034a94fc9198fa9179849)

###** This is the plain text hex of the unknown cipher after being xor by the key**###
'0x7a6f6e652d342d39443436393336372d423630452d344530382d424446312d4645443743433373441463333'

###** I then decode the hex string to get the plaintext link**###
>>>"7a6f6e652d342d39443436393336372d423630452d344530382d424446312d4645443743433373441463333".decode("hex")

###**Plaintext link**###
'zone-4-9D469367-B60E-4E08-BDF1-FED7CC74AF33'

Using the same key multiple times is a bad idea because if an attacker has a known plaintext version of the puzzle and a cipher text version of that plaintext version they can xor it to find the key that was used. This will allow the attacker to then break the unknown cipher key and any others that key was used to xor.

Zone 4
http://snowmiser.counterhack.com/zone-4-F7677DA8-3D77-11E2-BB65-E4BF6188709B
http://snowmiser.counterhack.com/zone-4-9D469367-B60E-4E08-BDF1-FED7CC74AF33
flag: de32b158f102a60aba7de3ee8d5d265a

Zone 4 gave me a run for my money, but my resolve was as sticky as honey. I will finish this and save Christmas, for the children I will not quit; for there is a fire that has been lit. I found Zone 5 link, so easily, for it was in Zone 4's page source just like previously. On to Zone 5 is the final game, before I warm the North Pole, the hidden folder I must name. To my surprise, there are some great directions to follow, for .svn is pretty hollow. It is amazing the flaws that exist, that allow hackers the ability to data twist. I followed the directions that Heat Miser so graciously provided me, his need to brag provided a way to pull the source code and find the key. The directory we found was easy enough, for once we were in we had the right stuff. I found it odd that the folder should have been named pristine however

to confuse it was changed. Spelling it prisinte was a trick not expected, however my skills were not neglected.

I found the link that I needed, once I ran these two commands:

wget http://snowmiser.counterhack.com/zone-5-89DE9B26-CF7D-4B07-88DE-7A2F0A7B16FE/.svn/wc.db
sqlite3 wc.db 'select local_relpath, ".svn/pristine/" || substr(checksum,7,2) || "/" || substr(checksum,7) || ".svn-base" as alpha from NODES;'

After running these two commands, I was given the following two folders:

noaccess.php|.svn/prisinte/41/4134e0e954d144ed932fd639b5a897f9ad47fff9.svn-base
index.php|.svn/prisinte/7d/7d63810b0da679648fc20b4f1c84680ac08ec872.svn-base

The next part of the task that was really bold, was following this link to the source code:
Had to change the prisinte to pristine:

http://snowmiser.counterhack.com/zone-5-89DE9B26-CF7D-4B07-88DE-7A2F0A7B16FE/.svn/pristine/7d/7d63810b0da679648fc20b4f1c84680ac08ec872.svn-base

When you evaluate the source code, you can see how the password is generated and is only valid for three minutes. First, you take the current time and the provided key and you SHA1 it. This gives you the current password and is valid for three minutes. The two pieces to the code is the key that we should not know and the current time of the server. Since the time could always be guessed, the secret to the puzzle was this key. To find the current time I viewed the page source of the Zone 5 noaccess.php site, and found this:

<!-- current server time is 2012-12-09 05:10 -->

This provided me with the second piece of the puzzle. With a simple command, the win was near, for what I needed to do was clear:

echo -n 2012-12-09 05:10 7998f77a7dc74f182a76219d7ee58db38be3841c | openssl sha1

This gave me the password that would last for three minutes:

810ce08ad46cfa2dbd1036f4019b173d8159592f

I then went to the Zone 4 site and entered the password to end the game, for I have put Snow Miser to shame. The total time spent in this exciting challenge was less than a few hours and Don and I left those two brothers to cower.

Zone 5
http://snowmiser.counterhack.com/zone-5-89DE9B26-CF7D-4B07-88DE-7A2F0A7B16FE/
flag: 3ab1c5fa327343721bc798f116be8dc6

Just like that, Don and I began to see, the snow was falling in Kuwait near the sea. It must mean we won and disabled the machines for snow was falling where heat should be. I started to cheer when a bright light began to sear, Mother Nature and Mrs. Claus suddenly appear. Their faces seemed happy for they

said you gave all your might, for your actions Santa Claus awakened tonight. You showed the spirit that Old St. Nick holds near, and off he went to spread holiday CHEER! To the victors a present was given, it was a free flight from the freed reindeer, Vixen. Mrs. Claus said we could go anywhere, but we said "Not tonight or tomorrow we would never dare, leaving our post would put our brethren in danger, and I can't imagine if was God we angered." Don asked Mrs. Claus for a favor instead, "Can you ask Santa for a more comfy bed?" I laughed aloud for I knew, that sleeping in combat is something you just do. She turned to me and asked what I needed, and my mind thought and pleaded. I started to speak and my voice cut through the air like scissors, "Mrs. Claus all we need are a few bags of Twizzlers!"