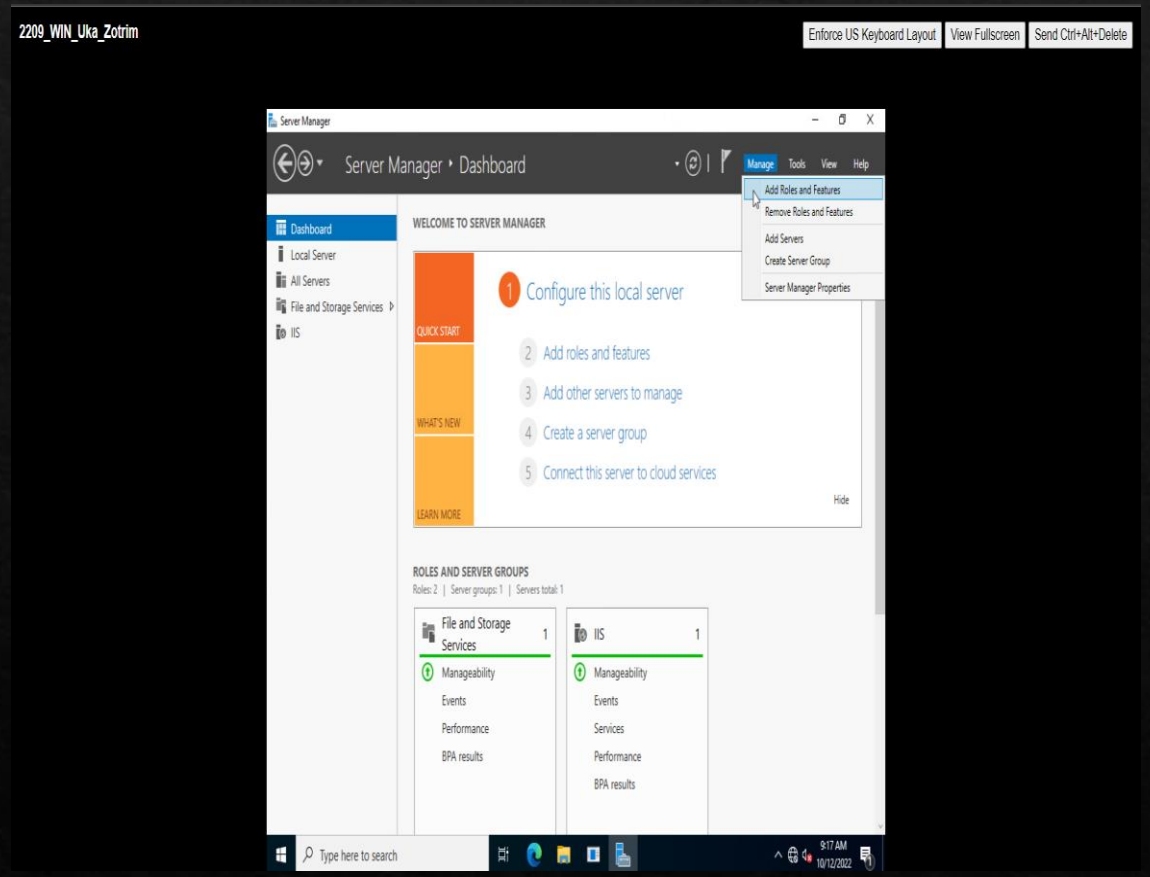
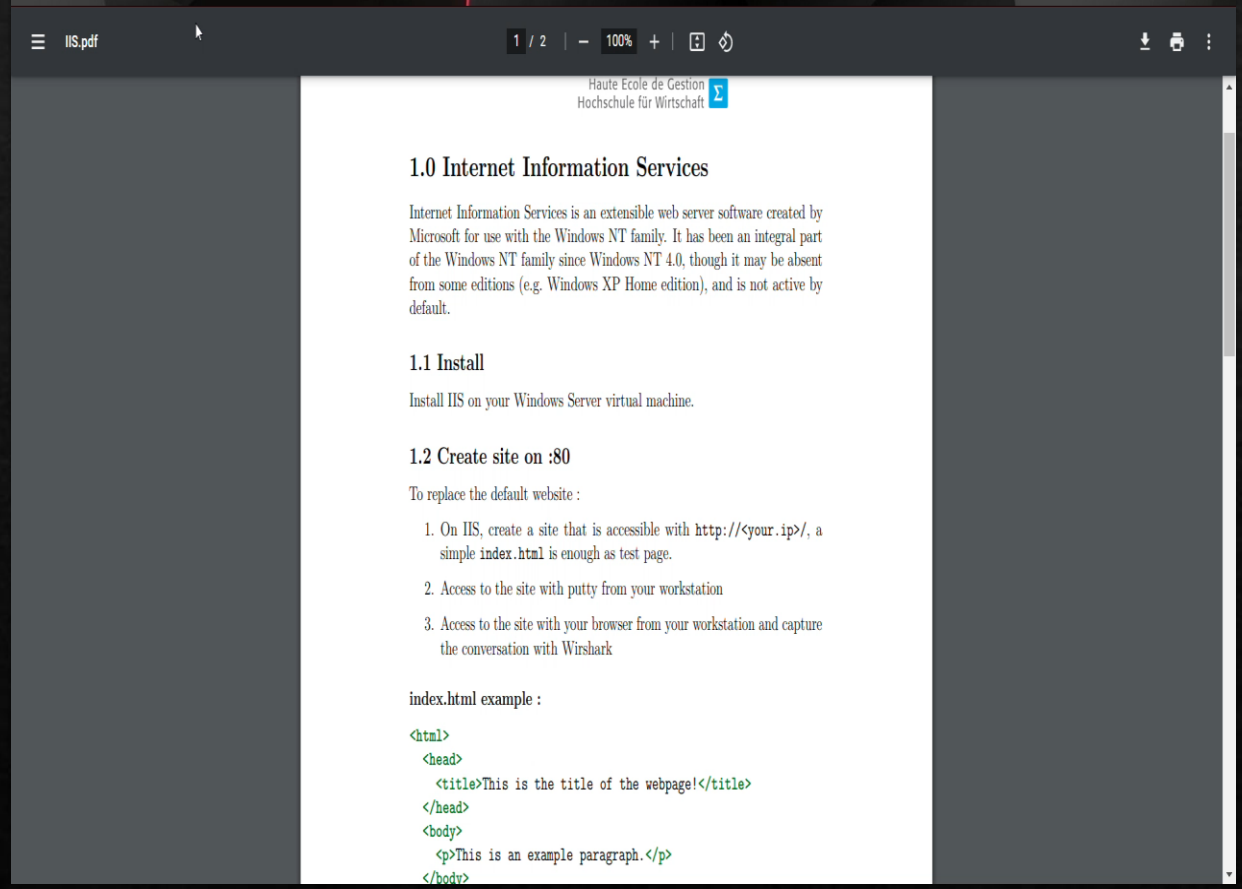
Infrastructure et réseaux

Zotrim UKA

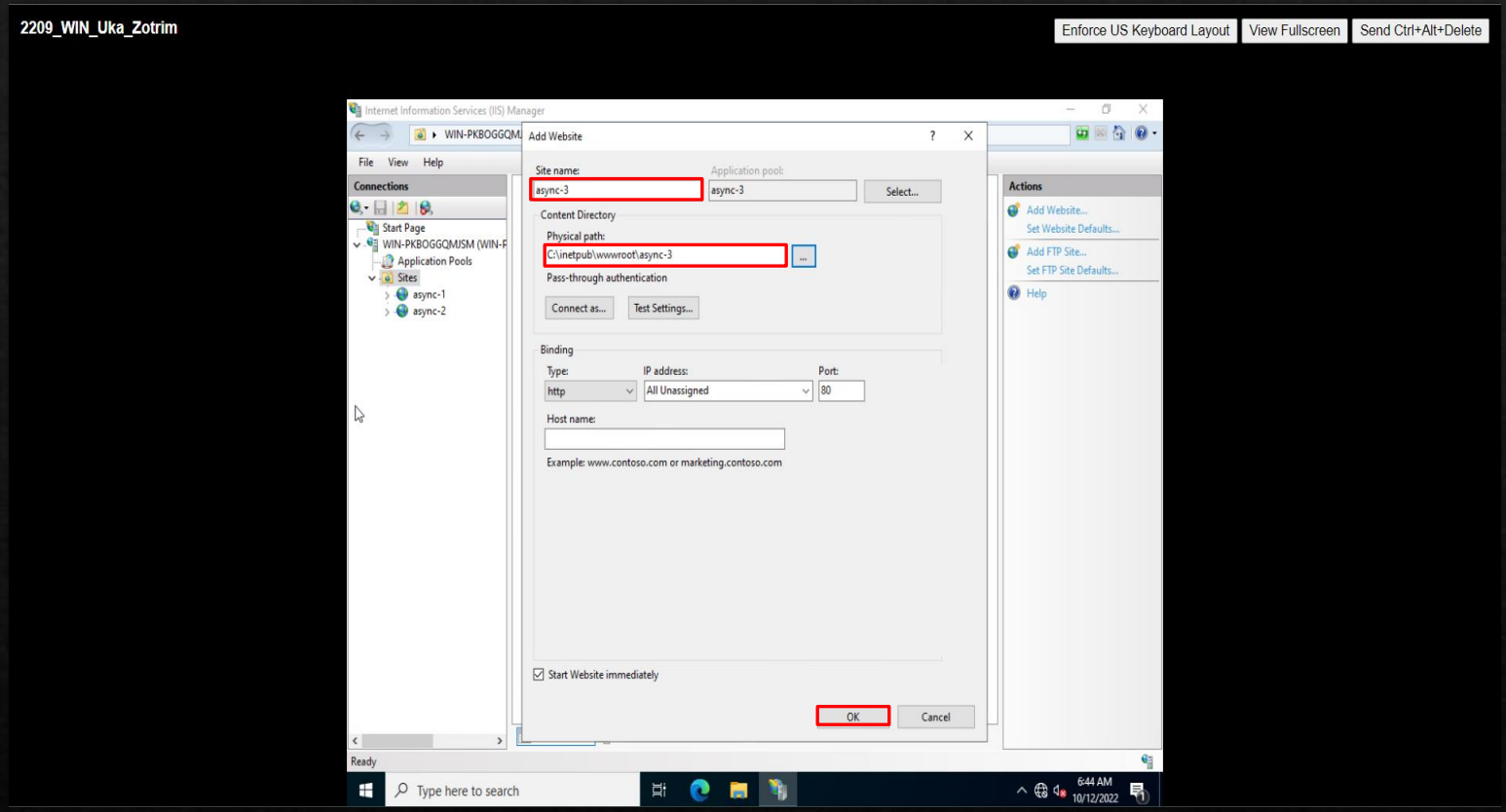
How to install IIS :
«Internet Information Services»





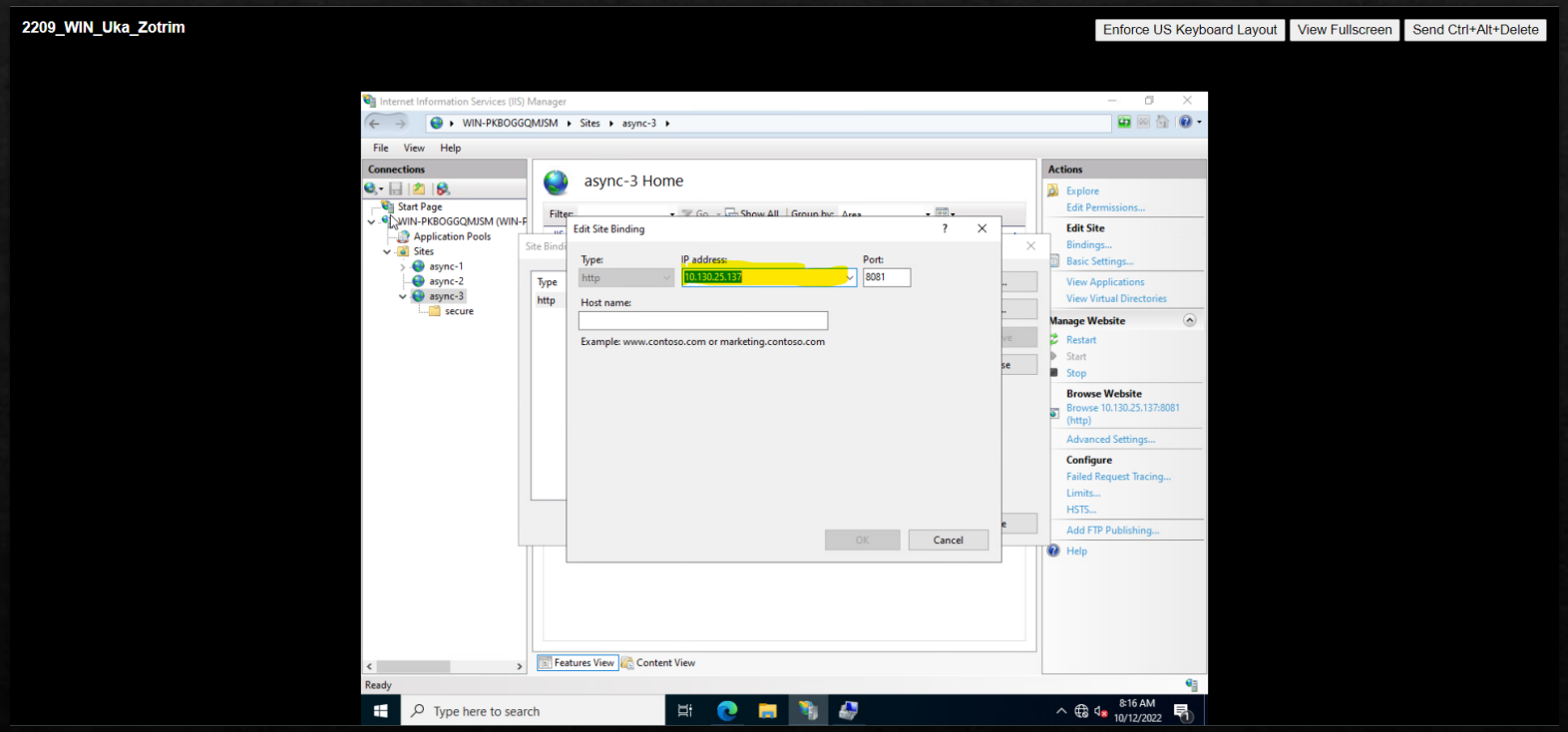
Settings configuration

1. I write the name of the site
2. I create a folder where i want on my PC Here i create my folder in : localDisk (C:)
3. I choose the path to the folder I created
4. I can click on OK



Settings configuration

- Remember to add the IP address and port number
- We can use the ports between 1 and 65536
- Usually, we use port 80 for http, but we are free to use the port we want
- Here I used port number “8081” because I created two other websites with the following ports: 80 and 8080

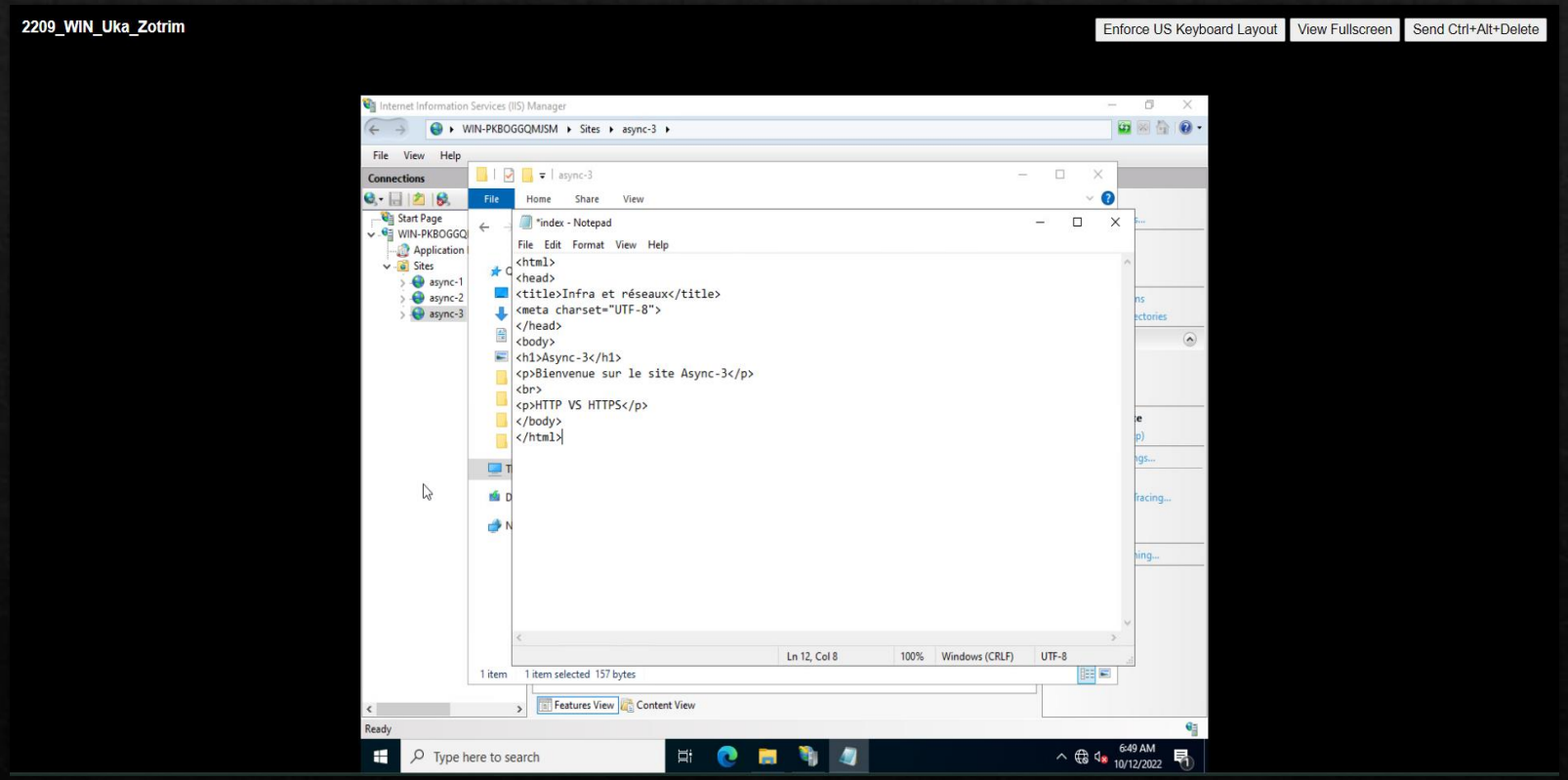


Create Index

I open my folder i created before, and I create a new file with «Notpad».

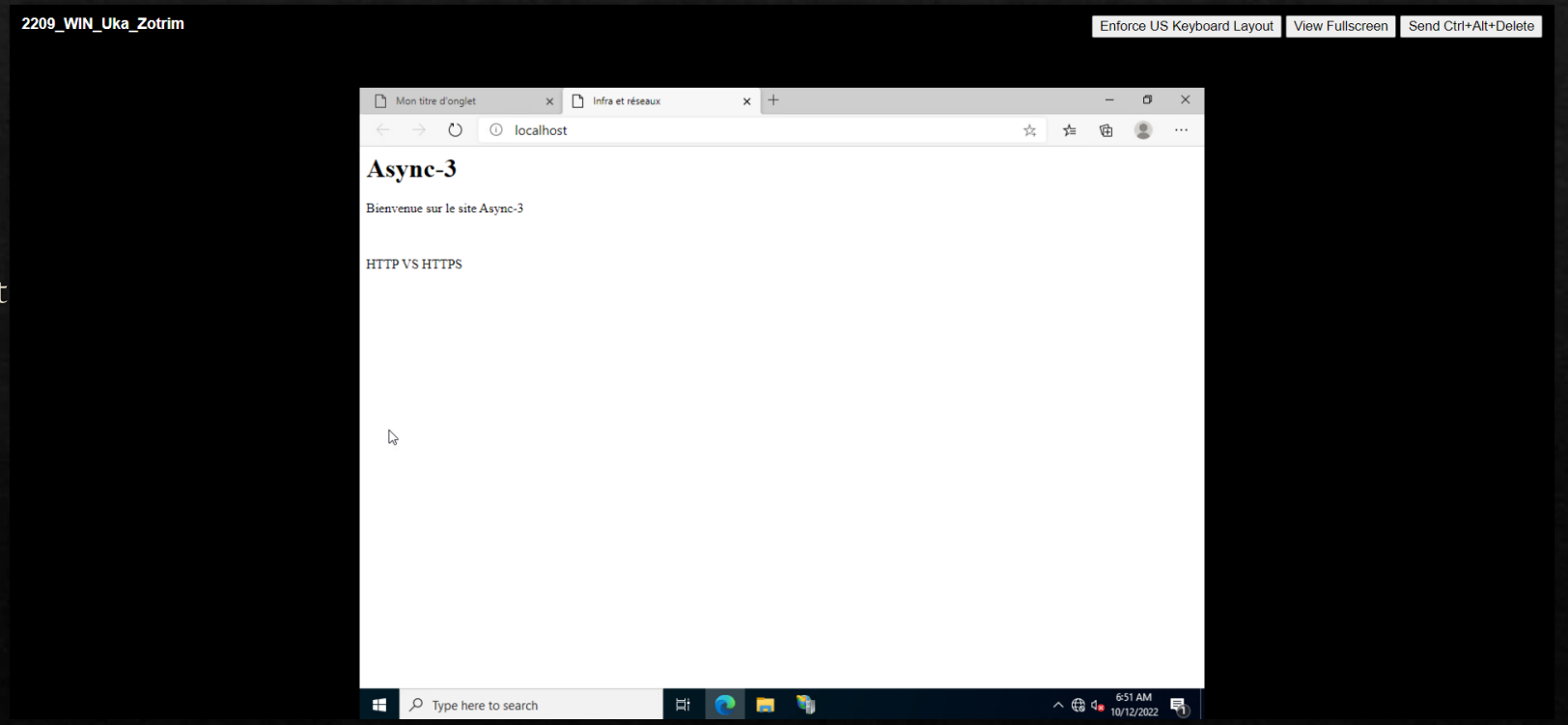
Inside this file, I wrote my HTML document.

I save (CTRL + S) and I can close notpad file.



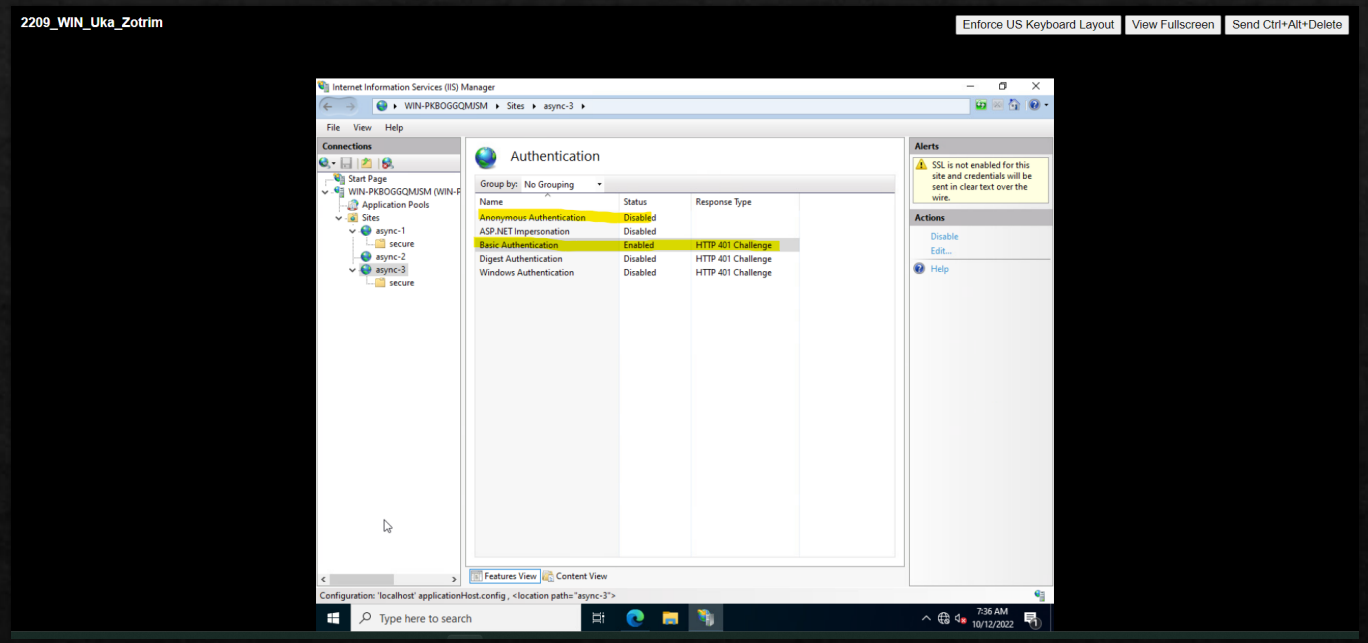
Overview

- With my HTML code I have words/ phrases on my website
- To access my website, I put my IP address in the search bar with the port number: 10.130.25.137:8081



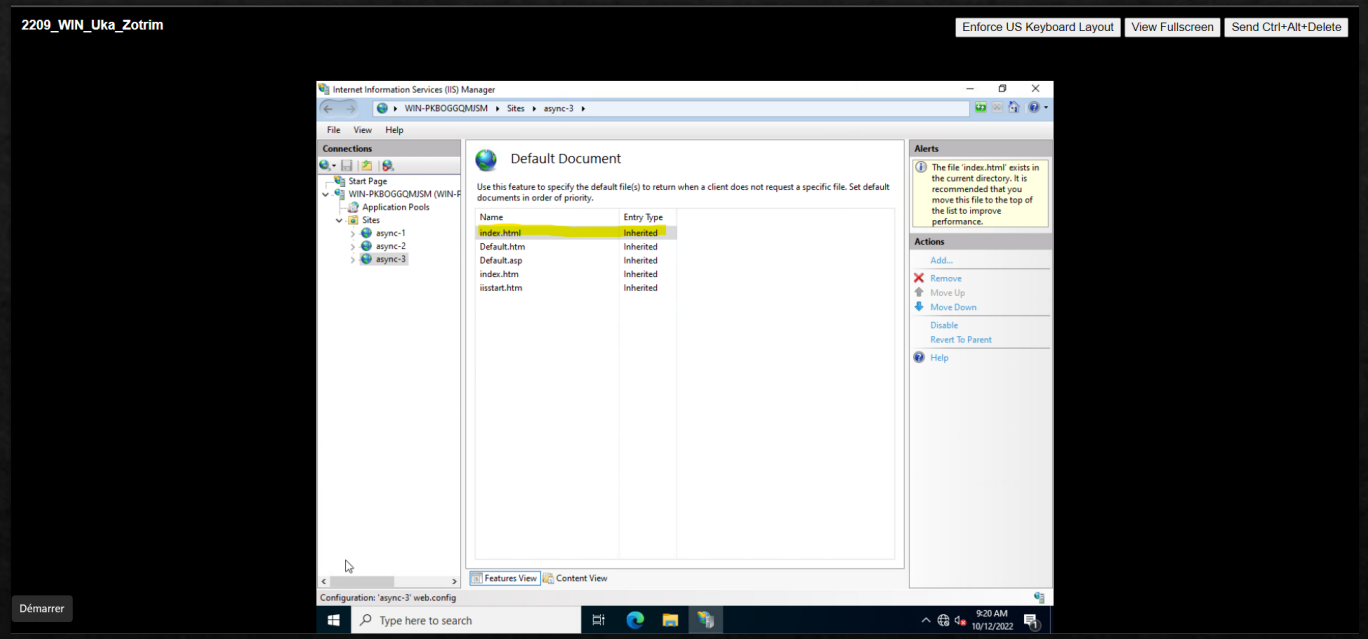
Authentication

Deactivate "anonymous authentication" and activate “basic authentication”.



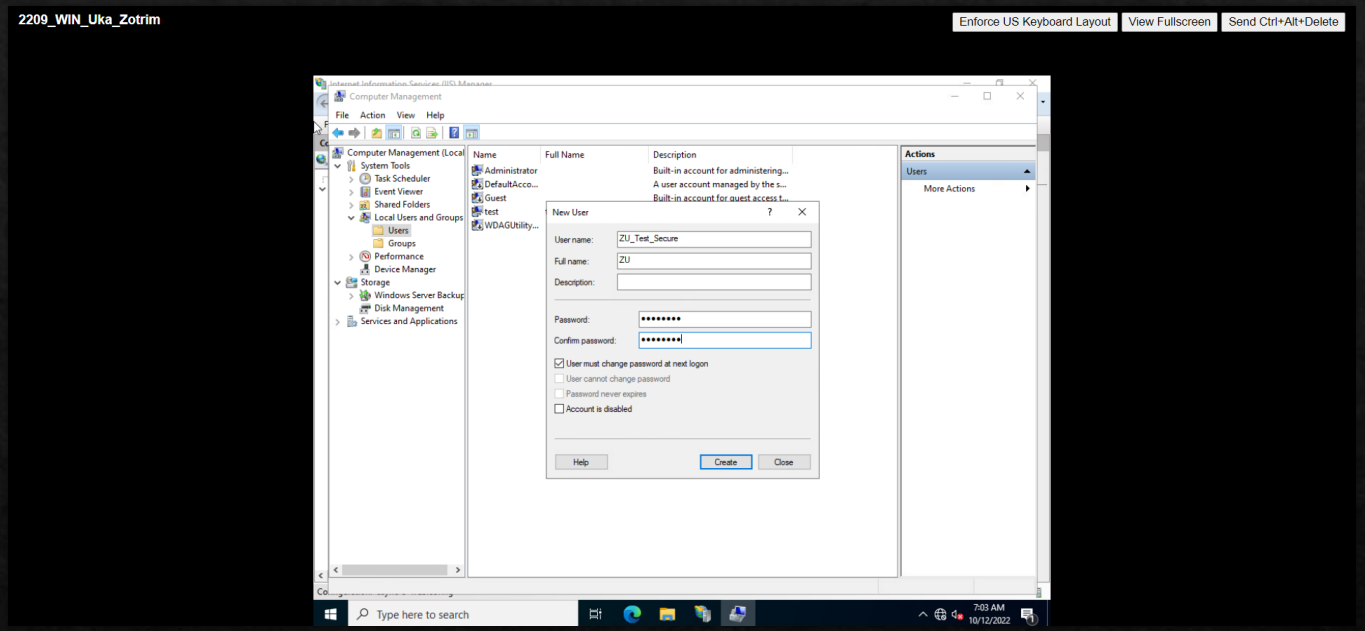
Default document

You have to put the index.html document at the top.



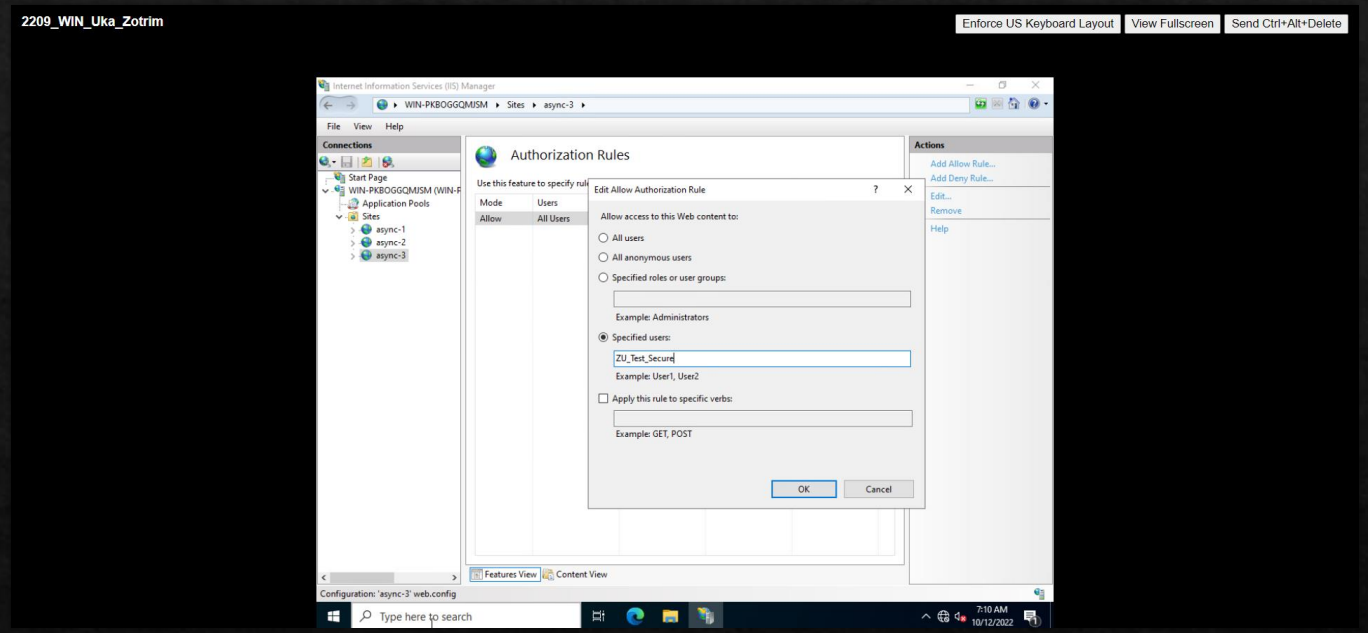
New user

Since we are local, in order to have a secure site and have to connect with a login and a password, we have to create a new windows user and a password.



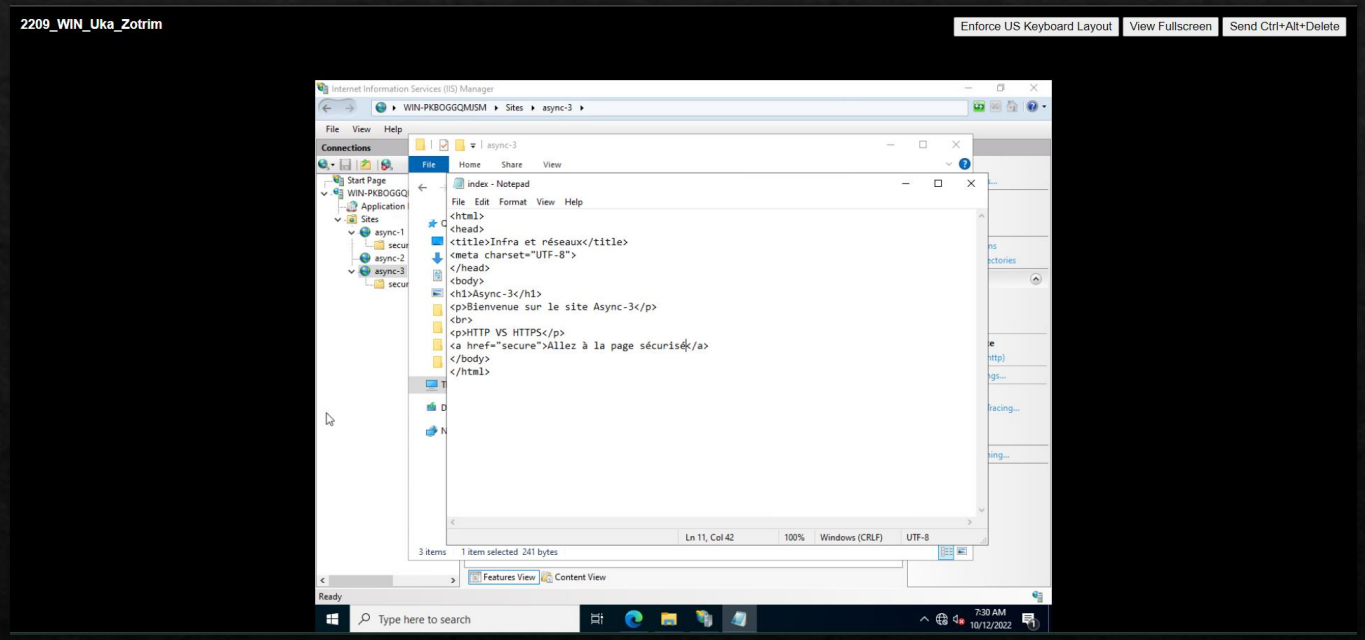
Authorization rules

to secure the site, we need to go to "authorization rules" and check the box "specified users" and enter the user name we created before



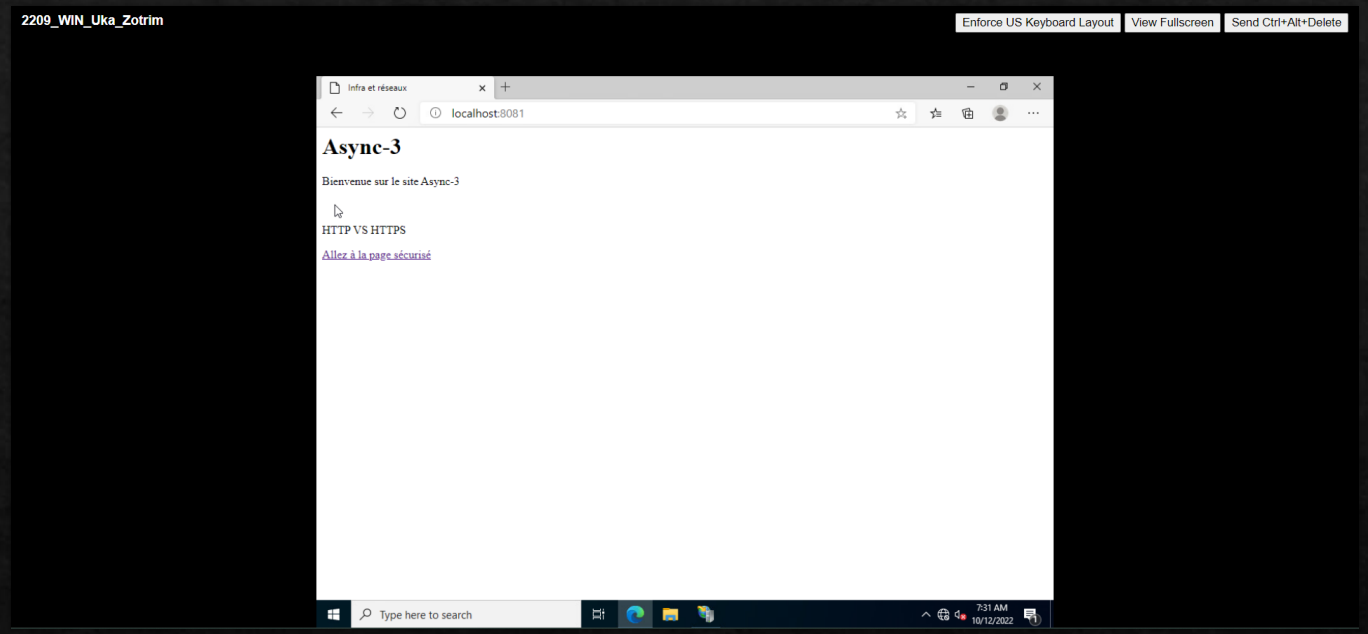
New page secure

- In my base folder I created a new folder "secure". In this folder I created a new file from notpad.
- Now I have a new tab on my page, which is secure.
- With this tab I can go back to the previous tab, which is not secured.



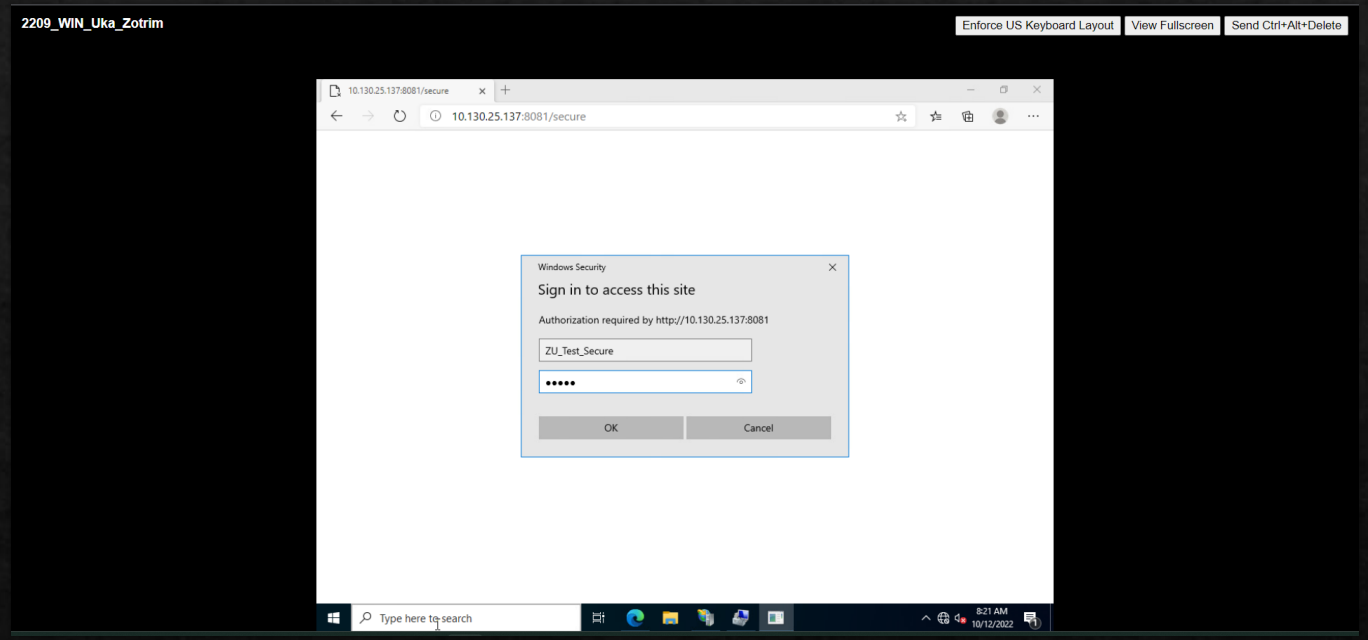
First page

Here we have the homepage of the site. There is the tab I created. This tab is a link that will direct me to another secure page.



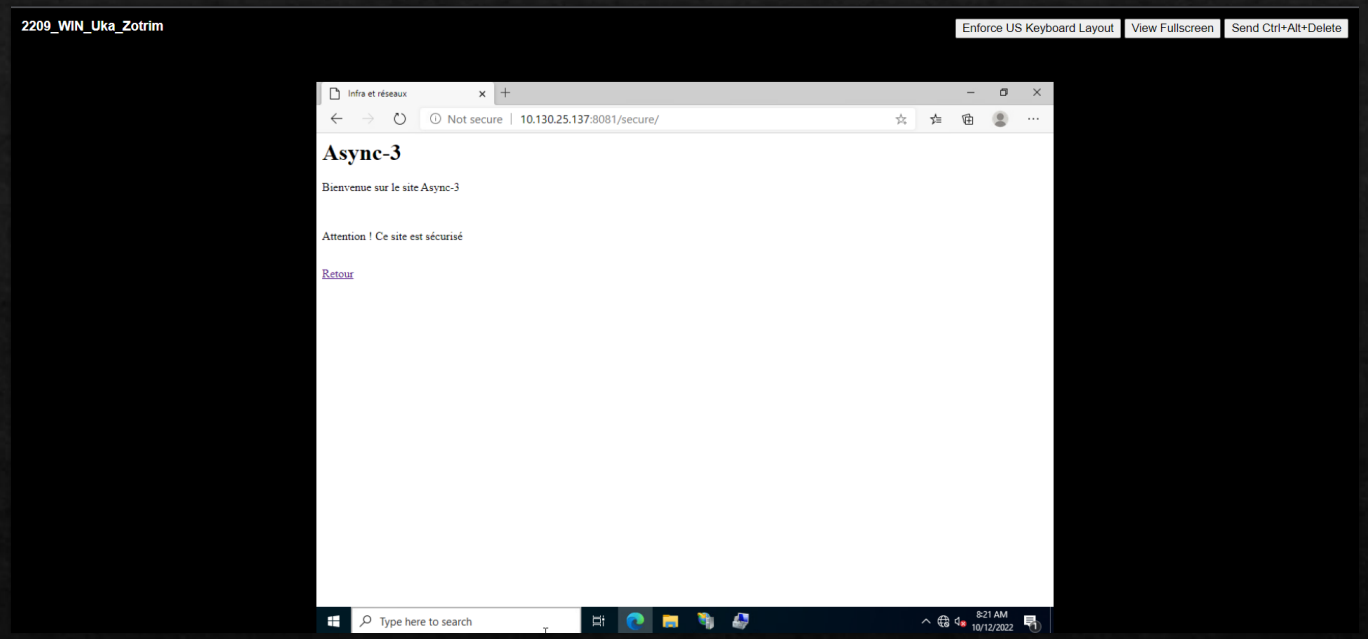
Pop-up

Once clicked on the link of the previous page, a pop-up appears. This pop-up asks us for a user name and a password. If we don't have the password, we won't be able to access this page.

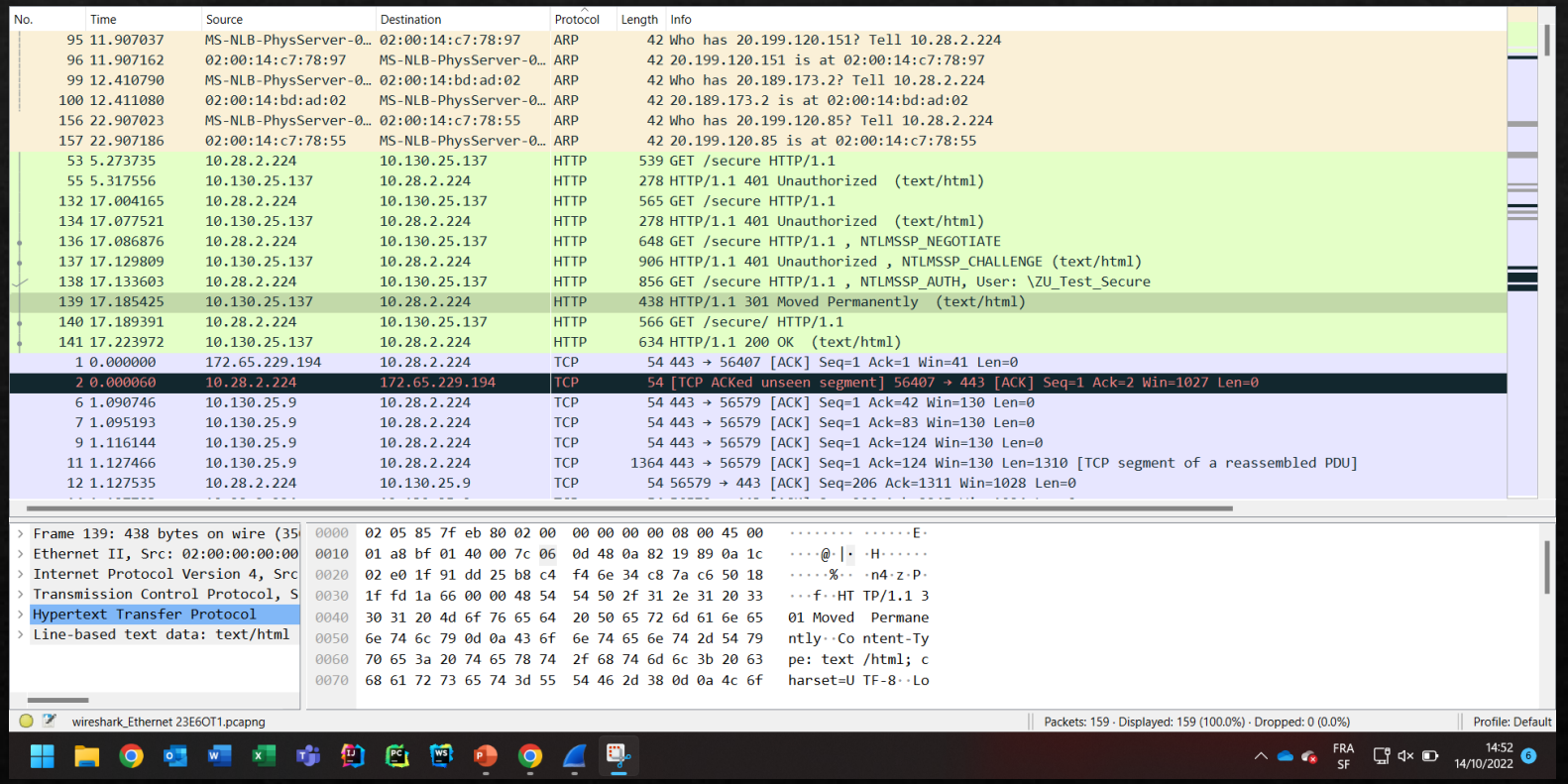


Second page

Once the password is entered, we have access to the second page.



Wireshark



No.	Time	Source	Destination	Protocol	Length	Info
95	11.907037	MS-NLB-PhysServer-0…	02:00:14:c7:78:97	ARP	42	Who has 20.199.120.151? Tell 10.28.2.224
96	11.907162	02:00:14:c7:78:97	MS-NLB-PhysServer-0…	ARP	42	20.199.120.151 is at 02:00:14:c7:78:97
99	12.410790	MS-NLB-PhysServer-0…	02:00:14:bd:ad:02	ARP	42	Who has 20.189.173.2? Tell 10.28.2.224
100	12.411080	02:00:14:bd:ad:02	MS-NLB-PhysServer-0…	ARP	42	20.189.173.2 is at 02:00:14:bd:ad:02
156	22.907023	MS-NLB-PhysServer-0…	02:00:14:c7:78:55	ARP	42	Who has 20.199.120.85? Tell 10.28.2.224
157	22.907186	02:00:14:c7:78:55	MS-NLB-PhysServer-0…	ARP	42	20.199.120.85 is at 02:00:14:c7:78:55
53	5.273735	10.28.2.224	10.130.25.137	HTTP	539	GET /secure HTTP/1.1
55	5.317556	10.130.25.137	10.28.2.224	HTTP	278	HTTP/1.1 401 Unauthorized (text/html)
132	17.004165	10.28.2.224	10.130.25.137	HTTP	565	GET /secure HTTP/1.1
134	17.077521	10.130.25.137	10.28.2.224	HTTP	278	HTTP/1.1 401 Unauthorized (text/html)
136	17.086876	10.28.2.224	10.130.25.137	HTTP	648	GET /secure HTTP/1.1 , NTLMSSP_NEGOTIATE
137	17.129809	10.130.25.137	10.28.2.224	HTTP	906	HTTP/1.1 401 Unauthorized , NTLMSSP_CHALLENGE (text/html)
138	17.133603	10.28.2.224	10.130.25.137	HTTP	856	GET /secure HTTP/1.1 , NTLMSSP_AUTH, User: \ZU_Test_Secure
139	17.185425	10.130.25.137	10.28.2.224	HTTP	438	HTTP/1.1 301 Moved Permanently (text/html)
140	17.189391	10.28.2.224	10.130.25.137	HTTP	566	GET /secure/ HTTP/1.1
141	17.223972	10.130.25.137	10.28.2.224	HTTP	634	HTTP/1.1 200 OK (text/html)
1	0.000000	172.65.229.194	10.28.2.224	TCP	54	443 → 56407 [ACK] Seq=1 Ack=1 Win=41 Len=0
2	0.000060	10.28.2.224	172.65.229.194	TCP	54	[TCP ACKed unseen segment] 56407 → 443 [ACK] Seq=1 Ack=2 Win=1027 Len=0
6	1.090746	10.130.25.9	10.28.2.224	TCP	54	443 → 56579 [ACK] Seq=1 Ack=42 Win=130 Len=0
7	1.095193	10.130.25.9	10.28.2.224	TCP	54	443 → 56579 [ACK] Seq=1 Ack=83 Win=130 Len=0
9	1.116144	10.130.25.9	10.28.2.224	TCP	54	443 → 56579 [ACK] Seq=1 Ack=124 Win=130 Len=0
11	1.127466	10.130.25.9	10.28.2.224	TCP	1364	443 → 56579 [ACK] Seq=1 Ack=124 Win=130 Len=1310 [TCP segment of a reassembled PDU]
12	1.127535	10.28.2.224	10.130.25.9	TCP	54	56579 → 443 [ACK] Seq=206 Ack=1311 Win=1028 Len=0

```
> Frame 139: 438 bytes on wire (35
> Ethernet II, Src: 02:00:00:00:00
> Internet Protocol Version 4, Src
> Transmission Control Protocol, S
> Hypertext Transfer Protocol
> Line-based text data: text/html
```

```
0000  02 05 85 7f eb 80 02 00  00 00 00 00 08 00 45 00   ........ ......E·
0010  01 a8 bf 01 40 00 7c 06  0d 48 0a 82 19 89 0a 1c   ····@·|· ·H·····
0020  02 e0 1f 91 dd 25 b8 c4  f4 6e 34 c8 7a c6 50 18   ·····%·· ·n4·z·P·
0030  1f fd 1a 66 00 00 48 54  54 50 2f 31 2e 31 20 33   ···f··HT TP/1.1 3
0040  30 31 20 4d 6f 76 65 64  20 50 65 72 6d 61 6e 65   01 Moved  Permane
0050  6e 74 6c 79 0d 0a 43 6f  6e 74 65 6e 74 2d 54 79   ntly··Co ntent-Ty
0060  70 65 3a 20 74 65 78 74  2f 68 74 6d 6c 3b 20 63   pe: text /html; c
0070  68 61 72 73 65 74 3d 55  54 46 2d 38 0d 0a 4c 6f   harset=U TF-8··Lo
```

wireshark_Ethernet 23E6OT1.pcapng — Packets: 159 · Displayed: 159 (100.0%) · Dropped: 0 (0.0%) — Profile: Default

FRA SF 14:52 14/10/2022