Université IBM i

7 novembre 2023

IBM Innovation Studio Paris

S10 – Synthèse d'une année de tentatives d'intrusion d'un IBM i exposé sur Internet

13:30 / 14:30

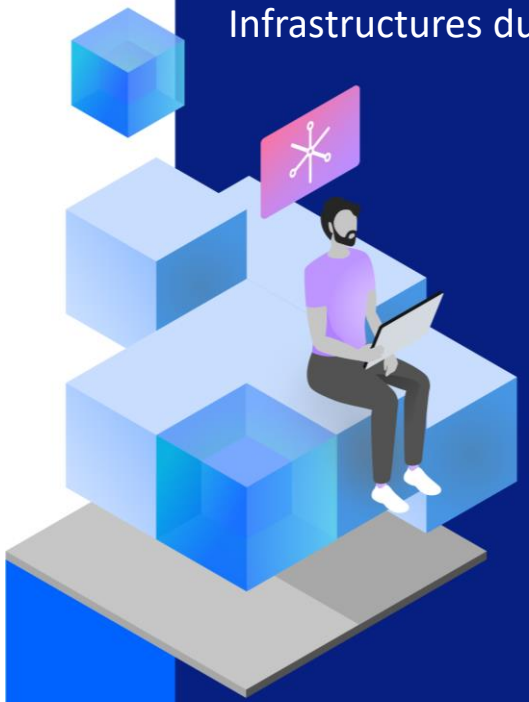
Dominique GAYTE
i.gayte.it
dominique@gayte.it

infrasdufutur

#ibmi
#uii2023
#infrastructuredufuturIBM23

IBM

Infrastructures du futur

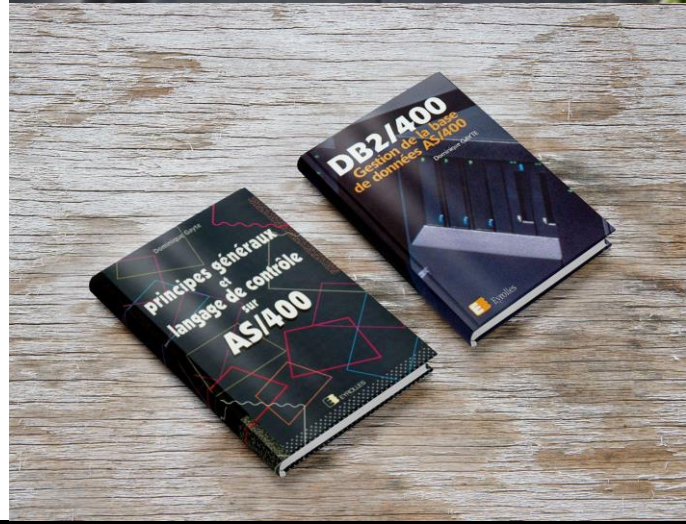


7 et 8 novembre 2023

Dominique GAYTE

I.GAYTE.IT
IBM i Security Softwares & Services

- Intervenant « AS/400 » depuis 1990
- Sécurité
  - Audit
  - Formation
  - Mise en œuvre : SSO, SSL, sécurisation de la BdD, RGPD…
- Développements complexes
  - Sécurité : Points d'exit (Power.exit), AD-iCT
  - API système
  - RPG IV : XML, Accès bases de données distantes
- Auteur des livres ci-contre



Dominique GAYTE - suite

- Evènement Sécurité IBM i
  - https://i.gayte.it/category/securiti/
  - https://www.youtube.com/@igayteit

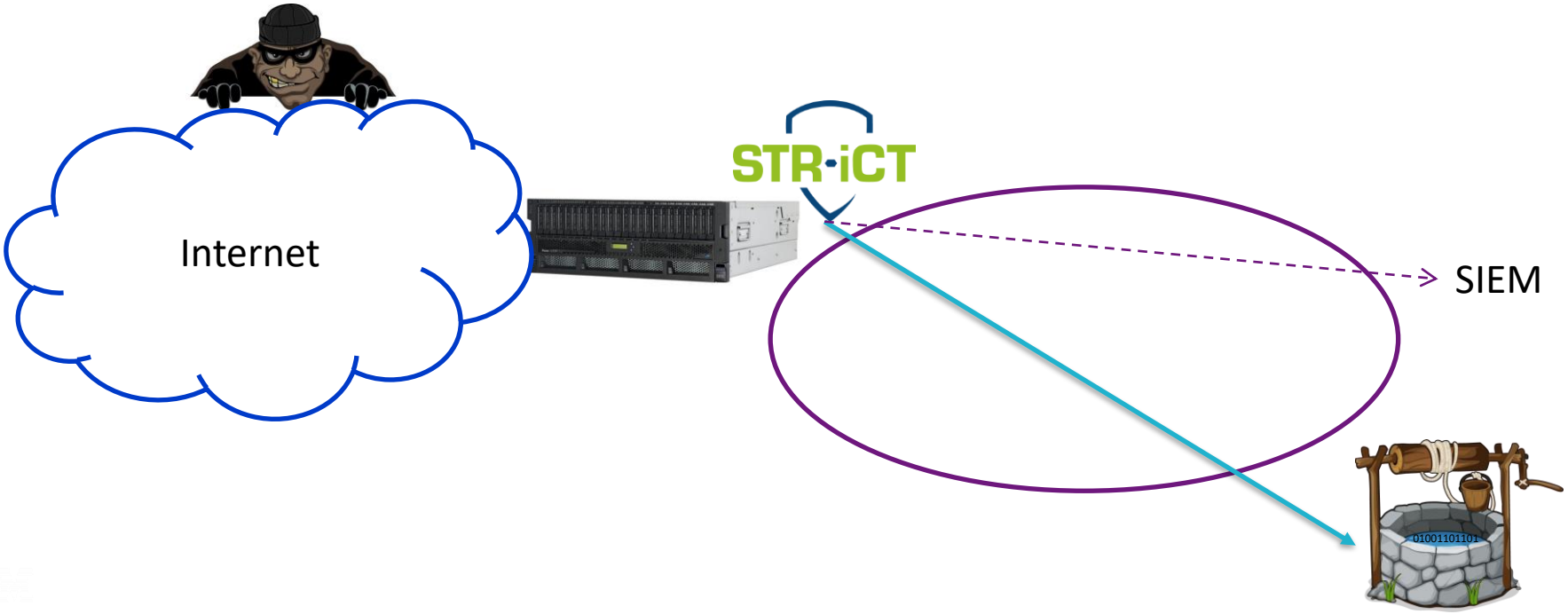
Securit.i
Événement Sécurité IBM i

- Distingué par IBM comme IBM Champion 2023
- Décerné aux experts reconnus par IBM

IBM i

Le pot de miel

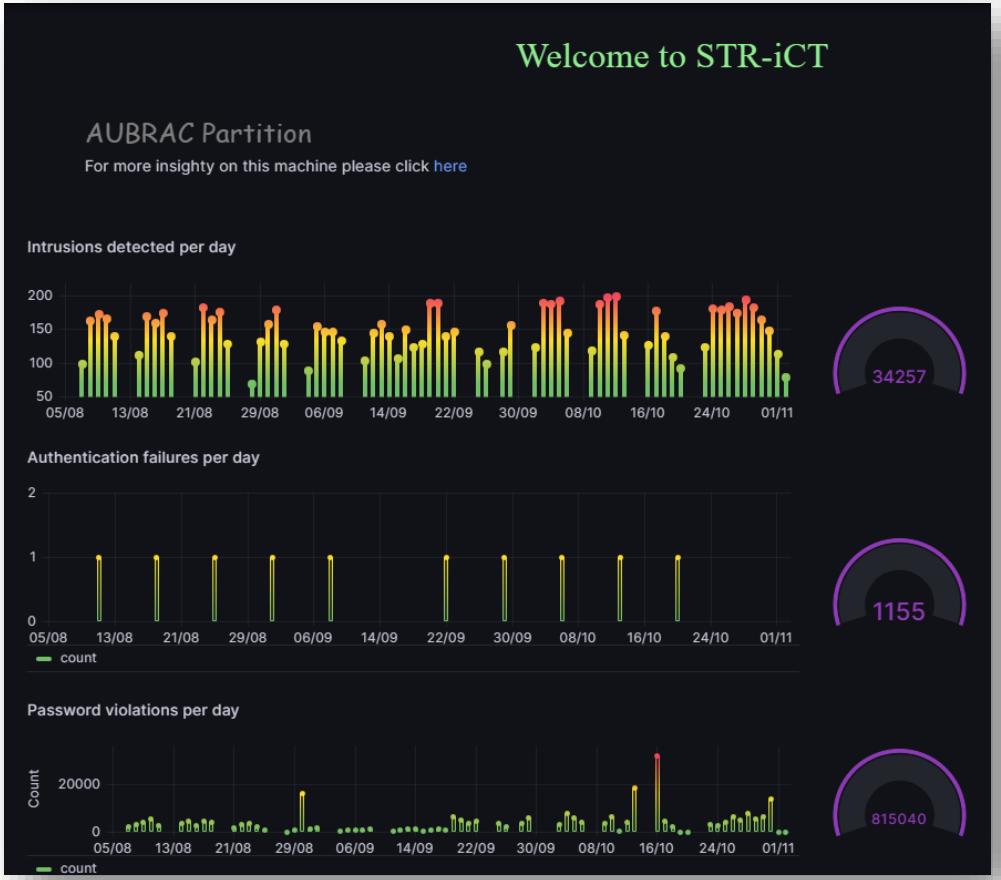
Architecture

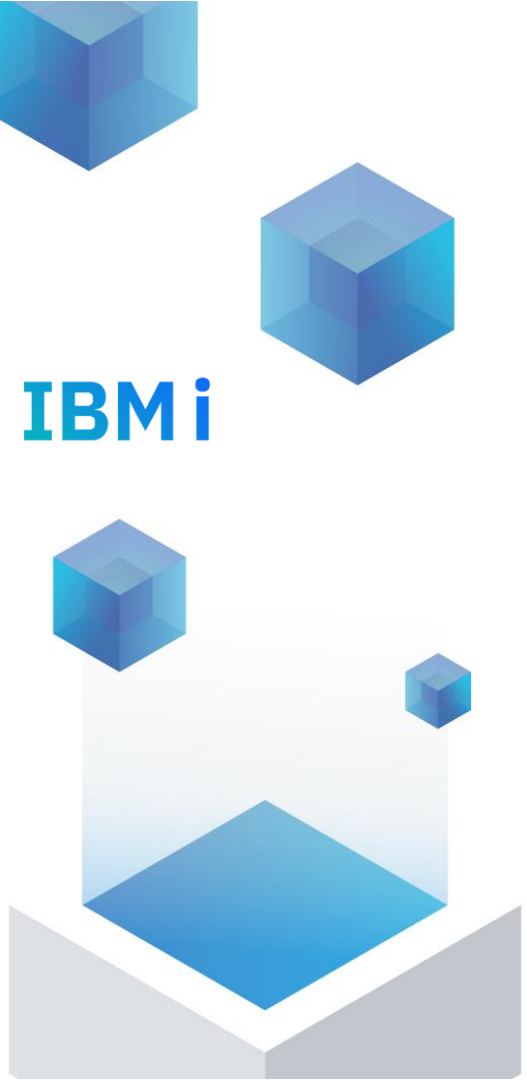


Et…

- Effet immédiat
  - Attaques très peu de temps après la mise en service
- Des milliers de tentatives de pénétrations par jour
- Protocoles standards
  - Telnet, FTP, SSH…
- Attaques
  - Paquets mal formés
  - Scans de ports
- Dénis de services
  - Conduisant à l'arrêt d'un service

STR-iCT : synthèse des incidents détectés sur 1 an





Traçabilité coté IBM i
Quelques rappels

La journalisation

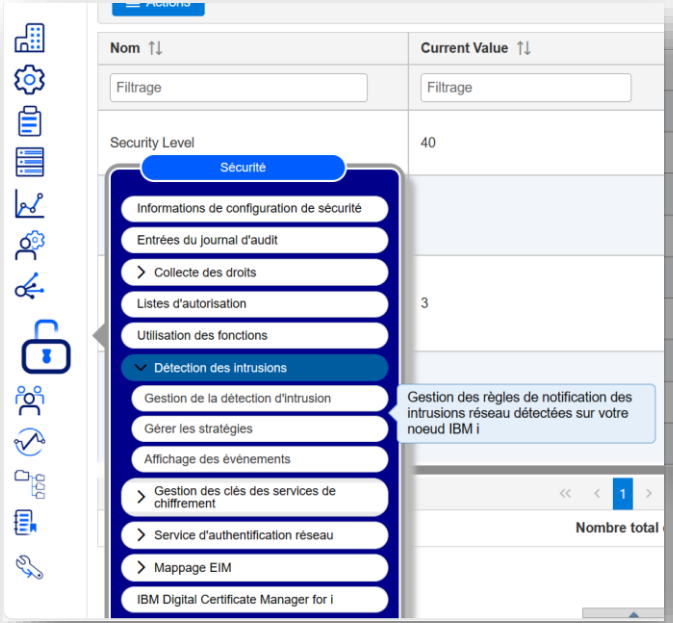
- Journal d’audit
  - La base de la traçabilité du système
  - Notamment conditionné par les valeurs systèmes
    - QAUDCTL, QAUDLVL, QAUDLVL2
- Journalisation
  - De la base de données
  - DTAARA, DTAQ
  - IFS

Les logs

- Historique du système
  - QHSTxxx
  - DSPLOG
- Spools
  - QPJOBLOG
  - Peu de QPJOBLOG (QRWTSRVR SQL coté serveur)
- Les logs des serveurs
  - Apache
  - Java
- QSYSOPR
  - Moindre mesure

IDS et IBM i

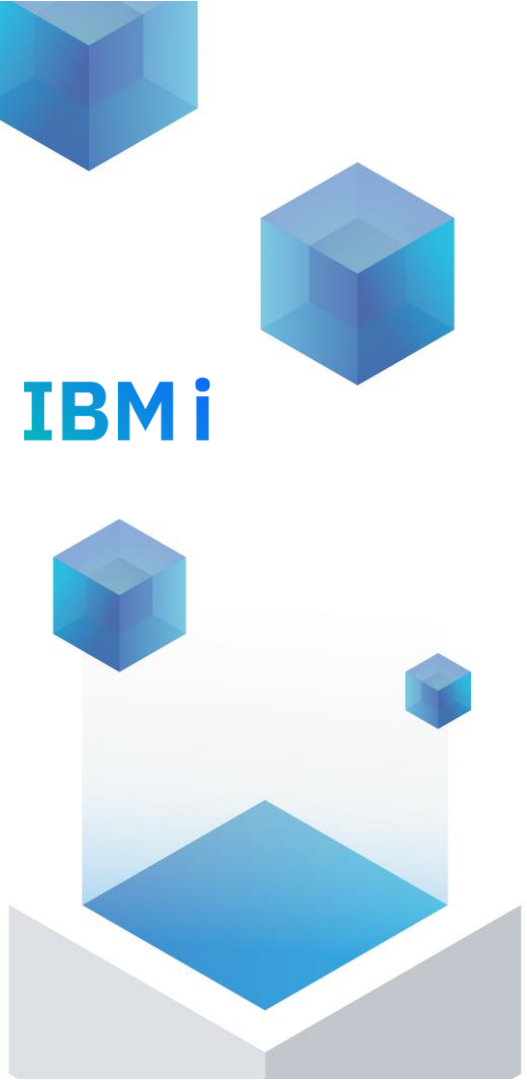
- *Intrusion Detection System*, système de détection d'intrusion
- Il en existe un en standard dans l'IBM i



Wed Nov 01 17:20:31 CET 2023	Attack (TCP ACK Storm)	Inbound	449	194.165.16.72
Wed Nov 01 17:50:46 CET 2023	Attack (TCP ACK Storm)	Inbound	449	167.248.133.125
Wed Nov 01 17:55:36 CET 2023	Attack (TCP ACK Storm)	Inbound	2002	167.248.133.182
Wed Nov 01 17:55:37 CET 2023	Attack (TCP ACK Storm)	Inbound	2002	167.248.133.182
Wed Nov 01 17:59:13 CET 2023	Attack (TCP ACK Storm)	Inbound	448	167.94.138.127
Wed Nov 01 18:04:16 CET 2023	Attack (Restricted IP Protocol)	Inbound	0	74.197.114.81
Wed Nov 01 18:11:24 CET 2023	Attack (TCP ACK Storm)	Inbound	5555	67.217.57.54
Wed Nov 01 18:37:01 CET 2023	Scan	Inbound	25216	77.90.185.180
Wed Nov 01 18:37:03 CET 2023	Scan	Inbound	55048	79.124.62.130
Wed Nov 01 18:39:14 CET 2023	Scan	Inbound	3311	213.109.202.212

IDS et IBM i (2)

- Simple en mettre en œuvre mais souvent de nombreux faux positifs
  - Souvent difficilement utilisable tel quel en production

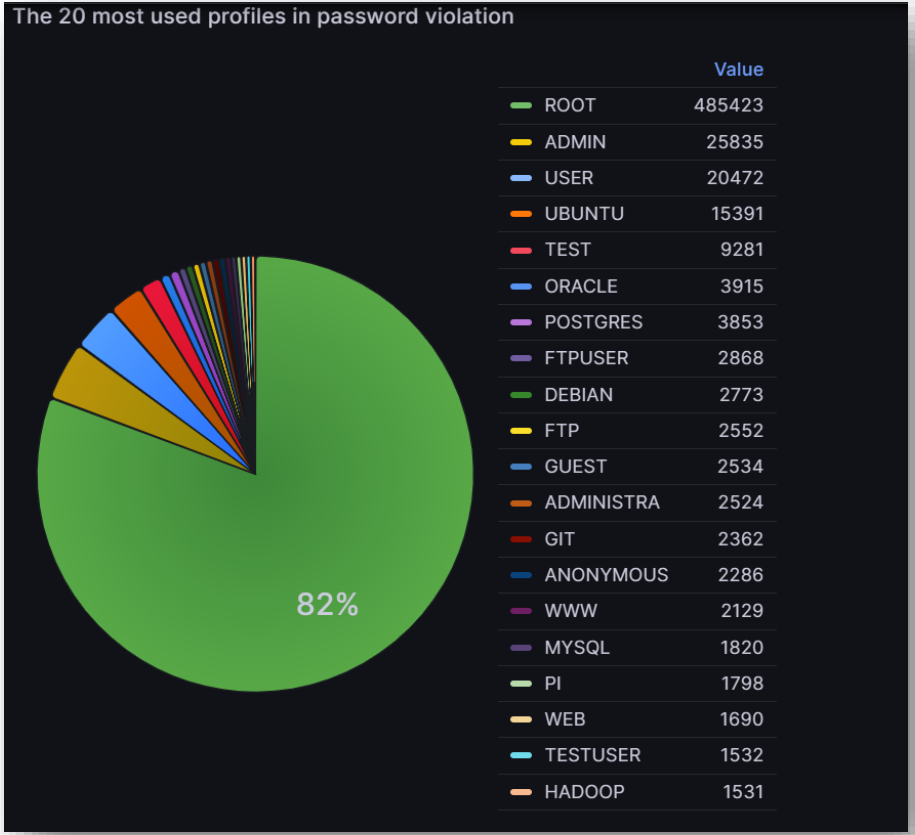


Les profils utilisateur

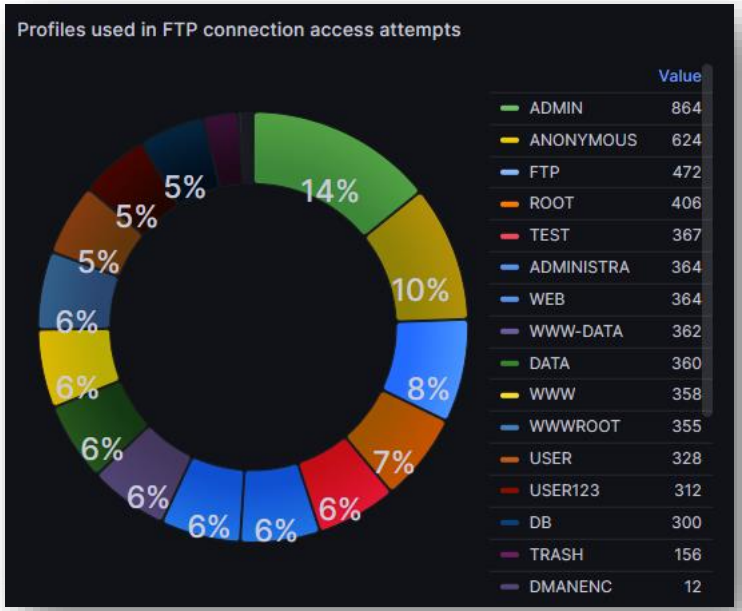
Utilisation des profils utilisateur

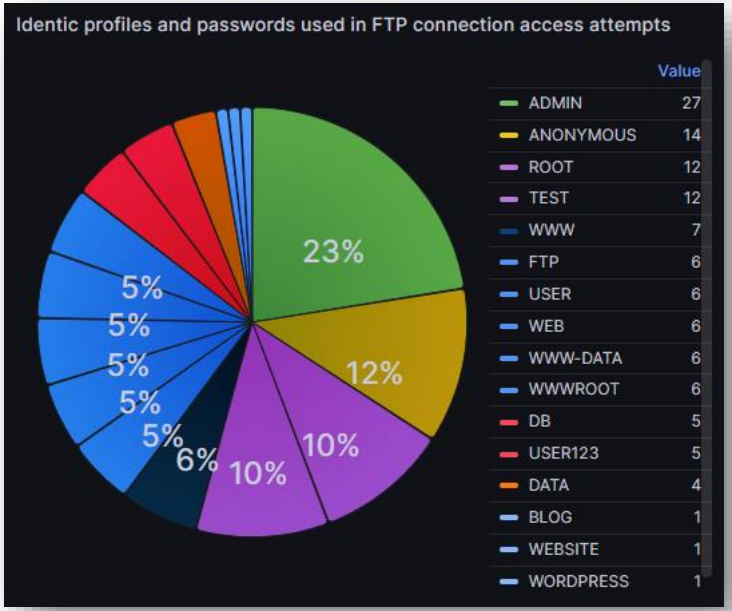
- Lors des connexions classiques tests d'authentifications
- La traçabilité permet de voir quels sont les profils (« comptes » !) utilisés
- Peuvent varier selon les services

STR-iCT : les profils liés aux problèmes de mot de passe



STR-iCT : les profils liés aux connexions FTP





Ne pas créer les profils des mondes Unix/Linux/Windows

- ROOT
- ADMIN
- UBUNTU
- DEBIAN

Ne pas créer les profils par défaut des applications

- FTP
- ORACLE
- UBUNTU
- DEBIAN
- WWW (WWW-DATA, WWWROOT, WEB)...

Ne pas utiliser les profils trop évidents

- TEST
- USER
- GUEST
- ANONYMOUS

Les mots de passe

Mots de passe

- Souvent mot de passe identique au profil
- Ou les mots de passe par défaut
- Souvent le mot de passe est court
- Peu ou pas de caractères accentués

STR-iCT : mots de passe FTP

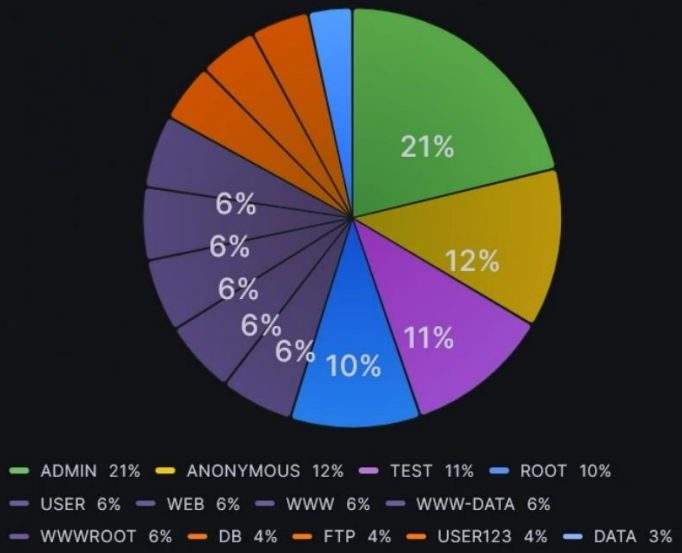
Home › Dashboards › Profiles used in connection attempts Add 2023-04-27 00:00:00 to 2023-09-13 00:00:00 UTC

DATA	298	6.52%
WWW	295	6.45%

7% 7%

USER123	250
DB	238
DMANENC	10
DGAYTE	1

Identic profiles and passwords used in FTP connection access atte...



Identic profiles and passwords used in FTP connection access atte...

profile	password
ADMIN	admin
ADMIN	Admin
ANONYMOUS	anonymous
DATA	data
DB	db
FTP	ftp
ROOT	root
TEST	test
USER	user
USER123	user123

STR-iCT

- Exemple de tests de connexions répétitifs

timedb	ibm_timestamp	mdp	ip
2023-08-31 10:19:01.1232777ba56378-24da-4109-b7bf-a05f7c54251d	2023-07-21 12:24:24	anonymous	123.234.131.230
2023-08-31 10:19:01.201409f644a729-182c-4811-aa59-04c6ab2ac4fd	2023-07-21 12:24:30	123456	123.234.131.230
2023-08-31 10:19:01.2795324b187491-c03f-442d-abae-0324cb4f9a34	2023-07-21 12:24:36	admin	123.234.131.230
2023-08-31 10:19:01.35770118145352-67d0-4cb9-b044-17cf9261d138	2023-07-21 12:24:42	root	123.234.131.230
2023-08-31 10:19:01.4358235c0325e9-05e8-4f38-a9cf-0a3b7c102d07	2023-07-21 12:24:48	password	123.234.131.230
2023-08-31 10:19:01.513949f3986886-602c-4abd-be54-d09ea52cc677	2023-07-21 12:24:54	123123	123.234.131.230
2023-08-31 10:19:01.607701106dc595-7a7e-4be6-bd6e-ef1a72b922f5	2023-07-21 12:25:00	123	123.234.131.230
2023-08-31 10:19:01.7014556d09bb6a-6944-4892-a655-fd9fd8e3354e	2023-07-21 12:25:07	pass1234	123.234.131.230
Count	372		

Définir un bon mot de passe : avant

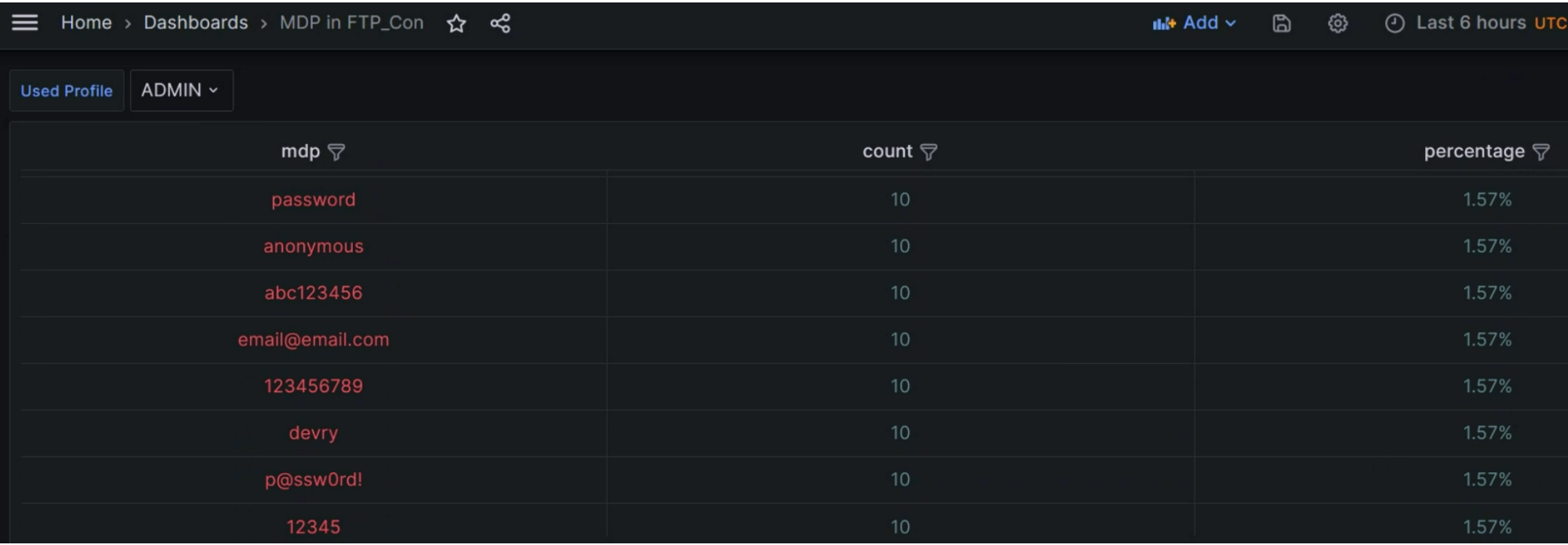
- 10 caractères
- Avant on prenait le nom de ses enfants, de son chien, de sa voiture…
- On pouvait remplacer des caractères
  - A => @
  - S => 5
  - O => 0
  - L => 1
- On répétait des mots pour avoir la bonne longueur
- Méthodes dépassées

Password => P@55w0rd

Admin => AdminAdmin

Attention à la facilité ou aux fausses bonnes idées

- Mettre des mots de passe complexes sur tous les profils



mdp	count	percentage
password	10	1.57%
anonymous	10	1.57%
abc123456	10	1.57%
email@email.com	10	1.57%
123456789	10	1.57%
devry	10	1.57%
p@ssw0rd!	10	1.57%
12345	10	1.57%

Le mot de passe préconisé par la CNIL

- La CNIL donne l'exemple de trois possibilités équivalentes en termes de Sécurité
  - 12 caractères au moins
    - Contenant des minuscules, des majuscules, des chiffres et des caractères spéciaux
  - 14 caractères sans caractères spéciaux obligatoires
  - Une phrase de passe doit être utilisée et elle doit être composée d'au minimum 7 mots
- Devinabilité
  - Ne dois pas contenir d'informations personnelles, ou de nom de société
  - Pas de mot du dictionnaire (ou alors 7 au minimum)
  - La littérature sur le sujet recommande une résistance aux attaques minimale de 10^{14} essais
- Un mot de passe différent pour chaque compte
  - Utiliser un gestionnaire de mot de passe (Keepass…)

https://www.cnil.fr/fr/mots-de-passe-une-nouvelle-recommandation-pour-maitriser-sa-securite

Le mot de passe (2)

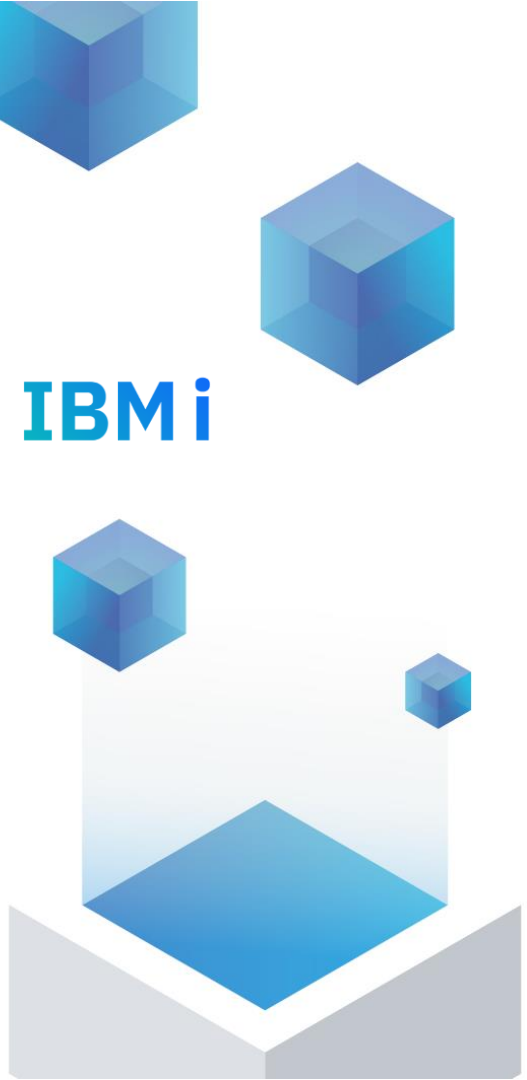
- Choisir une phrase, le couplet d'une chanson, une citation …

  « Ô rage ! ô désespoir ! ô vieillesse ennemie ! »

  « Moi je t'offrirai Des perles de pluie
  Venues de pays Où il ne pleut pas »

  « Pourtant que la montagne est belle
  Comment peut-on s'imaginer
  En voyant un vol d'hirondelles
  Que l'automne vient d'arriver? »

- L'adapter éventuellement
  - Ôr!ôd!ove!
  - Pqlmébcp-os'iev1vhqava?



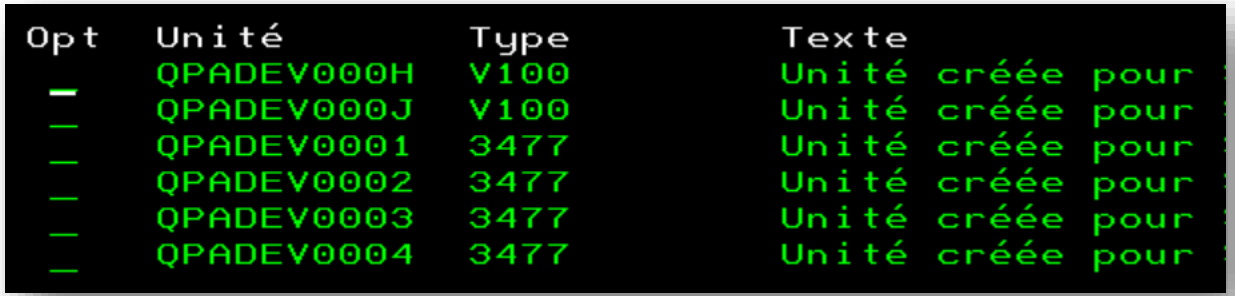
Les serveurs

Pot de miel : les services activés (ou pas !)

- Telnet
- NetServer
- FTP
- SSH
- ODBC/JDBC
- Sites Web arrêtés
  - Que 2001 ouvert

Telnet

- Création automatique des unités virtuelles si QAUTOVRT > 0
  - QPADEVxxxx
- Souvent sessions ouvertes en VT100
  - C'est-à-dire en mode Unix



Déni de services

- Lors de tentatives de connexions intensives les unités virtuelles sont toutes créées et hors fonction
  - Si QMAXSIGNACN = 1 ou 3
- Déni de service dans le sens ou le serveur Telnet ne peut plus créer des sessions virtuelles
- Solutions
  - Ne plus autoriser les unités virtuelles, mais contraignant
  - Ne plus désactiver les unités (QMAXSIGNACN), mais moins sécurisé car nombre de tentatives de connexions illimités
  - Disposer de sessions nommées pour les admins afin de toujours pouvoir se connecter (hors console). Gérer les QPADEVxxxx (remettre en fonction ou supprimer ceux qui sont hors fonction)

SSHD

- Le serveur pour SSH et SFTP
- Mode Unix, bien connu des hackeurs ou hackeuses
- Tentatives de connexions répétées

```
                          Historique du système

Travail 827934/QSECOFR/QPOZSPWT arrêté le 29/10/23 à 23:48:27; temps UC 0,040
Travail 827936/QSECOFR/QPOZSPWT arrêté le 29/10/23 à 23:48:37; temps UC 0,040
Travail 827938/QSECOFR/QPOZSPWT arrêté le 29/10/23 à 23:48:41; temps UC 0,040
Travail 827942/QSECOFR/QPOZSPWT arrêté le 29/10/23 à 23:48:47; temps UC 0,040
Travail 827945/QSECOFR/QPOZSPWT arrêté le 29/10/23 à 23:48:59; temps UC 0,039
Travail 827946/QSECOFR/QPOZSPWT arrêté le 29/10/23 à 23:48:59; temps UC 0,040
Travail 827948/QSECOFR/QPOZSPWT arrêté le 29/10/23 à 23:49:01; temps UC 0,040
Travail 827950/QSECOFR/QPOZSPWT arrêté le 29/10/23 à 23:49:09; temps UC 0,040
Travail 827952/QSECOFR/QPOZSPWT arrêté le 29/10/23 à 23:49:20; temps UC 0,040
Travail 827954/QSECOFR/QPOZSPWT arrêté le 29/10/23 à 23:49:27; temps UC 0,039
Travail 827956/QSECOFR/QPOZSPWT arrêté le 29/10/23 à 23:49:45; temps UC 0,013
Travail 827958/QSECOFR/QPOZSPWT arrêté le 29/10/23 à 23:49:46; temps UC 0,040
Travail 827940/QSECOFR/QPOZSPWT arrêté le 29/10/23 à 23:49:50; temps UC 0,010
Travail 827960/QSECOFR/QPOZSPWT arrêté le 29/10/23 à 23:50:05; temps UC 0,040
Travail 827962/QSECOFR/QPOZSPWT arrêté le 29/10/23 à 23:50:07; temps UC 0,040
Travail 827964/QSECOFR/QPOZSPWT arrêté le 29/10/23 à 23:50:10; temps UC 0,040
Travail 827966/QSECOFR/QPOZSPWT arrêté le 29/10/23 à 23:50:12; temps UC 0,040
```

Log4j

- Ne pas mettre en service le vieux Navigator for i
- Veiller à ne pas avoir d'applications qui seraient sensibles à Log4j

Conclusions

- L’IBM i est bien l’un des systèmes les plus sûrs du marché !
- A condition qu’il soit bien configuré !
- Pensez à mettre en place de la traçabilité

36