

Registres IA-32

EAX : Registre Accumulateur

Utilisé pour les opérations arithmétiques et le stockage de la valeur de retour des appels systèmes.

EBX : Registre de base : Pointeur de données

Utilisé comme pointeur de donnée (contient un offset de donnée).

ECX : Registre Compteur

Enregistre le nombre d'itérations des boucles du programme.

EDX : Registre de données

Utilisé pour les opérations arithmétiques et les opérations d'entrée / sortie.

ESI (Source) / EDI (Destination)

Pointeurs pour les opérations mémoires

EBP

Pointeur de la base de la pile de données

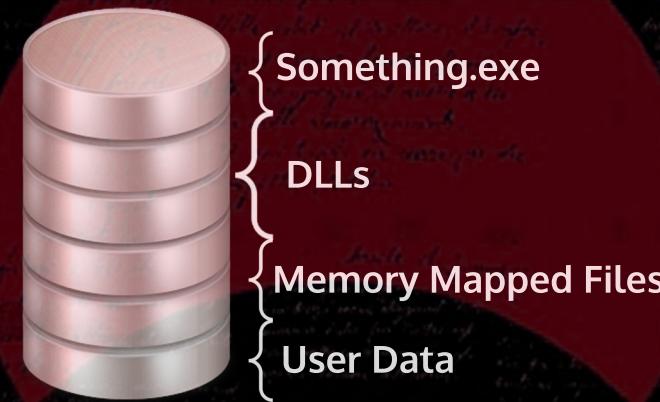
ESP

Pointeur de donnée de la pile (adresse mémoire du dessus de la pile = valeur la plus faible)

EIP

Pointeur vers la prochaine instruction à exécuter

Shéma processus



ESD academy

Site : esdacademy.eu

Twitter : @esd_academy

Instagram : esd_academy

Github : ESD-academy



Aide mémoire



Analyse de Malware



esdacademy.eu

Séquence de boot Windows

Power On



Bios



Démarrage du BIOS

Master Boot Record

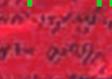


Initial Program Loader

BootMgr



Winload



Userland



Wininit.exe



lsm.exe



lsass.exe



Les commandes utiles GDB

[run] : lancement d'un programme dans l'environnement GDB

functions

[step] : pas à pas, descend dans les fonctions

[next] : pas à pas, sans descendre dans les fonctions

[fini] : exécute jusqu'à la fin de la fonction en cours

[continue] : reprend l'exécution dans la pile

[up] : permet de se déplacer dans le sens inverse

[info registers] : affiche l'état des registres

[volatile] : obtention d'informations relatives au dump :

[maginfo] : obtention d'informations sur les processus actifs.

[netscan] : infos sur les connexions TCP / UDP ;
[connections, sockets, connscan, desprocess] .

Les sections d'un PE Windows

[text] : le code (instructions) du programme

[bss] : les variables non initialisées

[relloc] : la table de localisations (de répertoire)

[data] : les variables initialisées

[rsrc] : les ressources du fichier (de répertoire : curseurs, sons)

[adata] : signe d'un package ADATA propre à ASPACK

[upx] : signe d'une compression UPX, propre au logiciel UPX

[idata] : la table d'import (2nd répertoire)

[rdata] : les données en lecture seule

[proper] à ADATA