Parseur de fichiers VMDK

ensisa

UNIVERSITÉ HAUTE-ALSACE

Tuteur d'entreprise : Julien RAEIS **Tuteur ENSISA : Frédéric FONDEMENT**

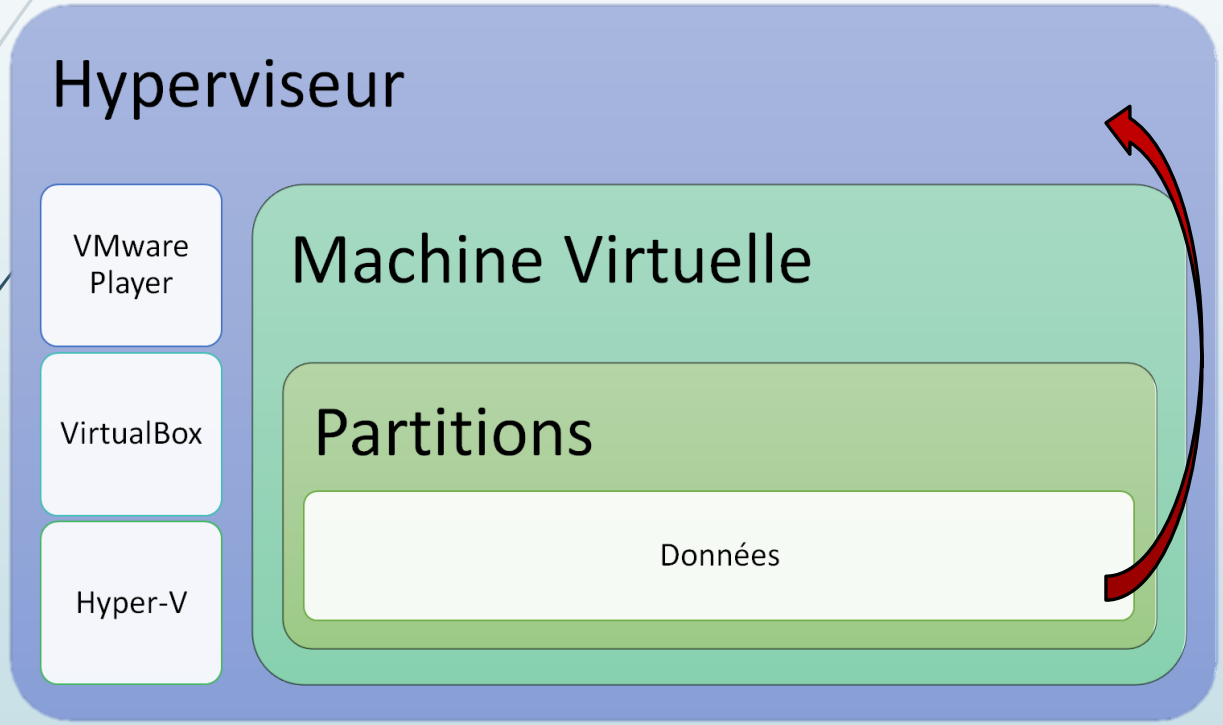
Etudiants : Jessy KERMANN & Raphaël LOB

Sommaire

I) Nature du projet

Agence Nationale de la sécurité des systèmes d'information – Bureau Audit et Inspection

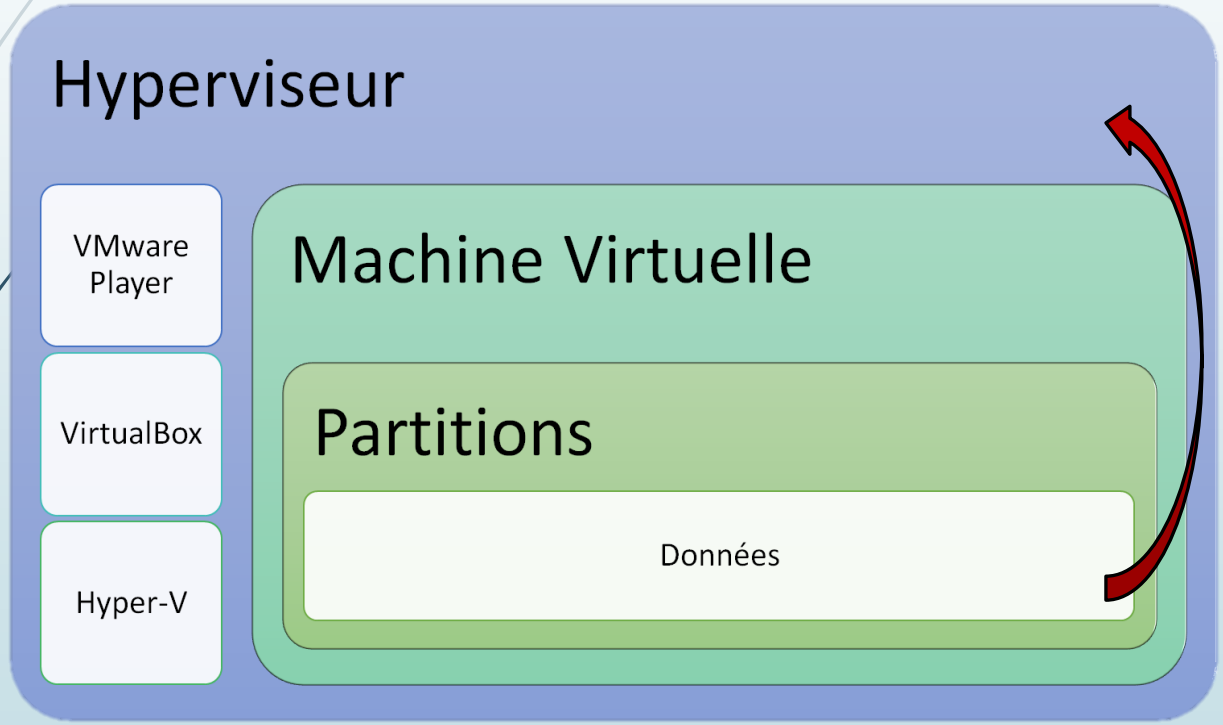
Extraction des données
d'une VM vers l'hyperviseur



I) Nature du projet

Agence Nationale de la sécurité des systèmes d'information – Bureau Audit et Inspection

Extraction des données
d'une VM vers l'hyperviseur



Exfiltration par le réseau

II - A) Classification des solutions

Bas niveau : Données brutes

- ✓ Lecture directe
- ✓ Rapide
- ✓ Consommation faible
- x Opérations simplistes

Haut niveau : Machine virtuelle

- ✓ API
- ✓ Stable
- ✓ Puissance des opérations
- x Lourd
- x Dépendant de l'hyperviseur

II - B) Solutions techniques

	API VMWare (VDDK / VIX API)	Solution Microsoft (Outdated)	7-Zip	The Sleuth Kit
Lisibilité du fichier VMDK	Oui	Partiel	Oui	Oui
Extraction des données	Oui mais Nécessite Login / Pass	?	Oui mais Nécessite l'utilisation de la GUI	Oui
Ecriture sur le fichier	Oui mais Nécessite Login / PASS	?	Non	Non
Interactivité avec la machine	Complète Nécessite Login/Pass · Shell · Ecrire · Extraire	?	Non	Non
Remarque	Dépendant d'un environnement VMWare Mécanique de Hook	Le logiciel n'est plus à jour depuis 2011	La console 7zip n'implémente pas les fonctionnalités recherchées. Open Source	Open Source

The Sleuth Kit

II - C) The Sleuth Kit (TSK)

Solution de forensique

Force :
- Popularité
- Open Source
- Documenté

Fonctionnalités :
- Gestion des images disques (VDMK, VHDI, …)
- Gestion des partitions systèmes (DOS, BSD, …)
- Gestion des systèmes de fichiers (NTFS, FAT, …)

```
PS D:\VMDK> .\mmls .\DebianGuest.vmdk
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Description
000:  Meta      0000000000   0000000000   0000000001   Primary Table (#0)
001:  -------   0000000000   0000002047   0000002048   Unallocated
002:  000:000   0000002048   0009951231   0009949184   Linux (0x83)
003:  -------   0009951232   0009953279   0000002048   Unallocated
004:  Meta      0009953278   0010483711   0000530434   DOS Extended (0x05)
005:  Meta      0009953278   0009953278   0000000001   Extended Table (#1)
006:  001:000   0009953280   0010483711   0000530432   Linux Swap / Solaris x86 (0x82)
007:  -------   0010483712   0010485759   0000002048   Unallocated
```

The Sleuth Kit

II - D) Procédé d'extraction (TSK)

Analyse image

- Analyse du Master Boot Record (.mbr)
- Facultative (VMDK)

Analyse partitions

- Détermine le type de partition (DOS, BSD, …)
- Renvoie l'adresse de début de la partition

Analyse du système de fichiers

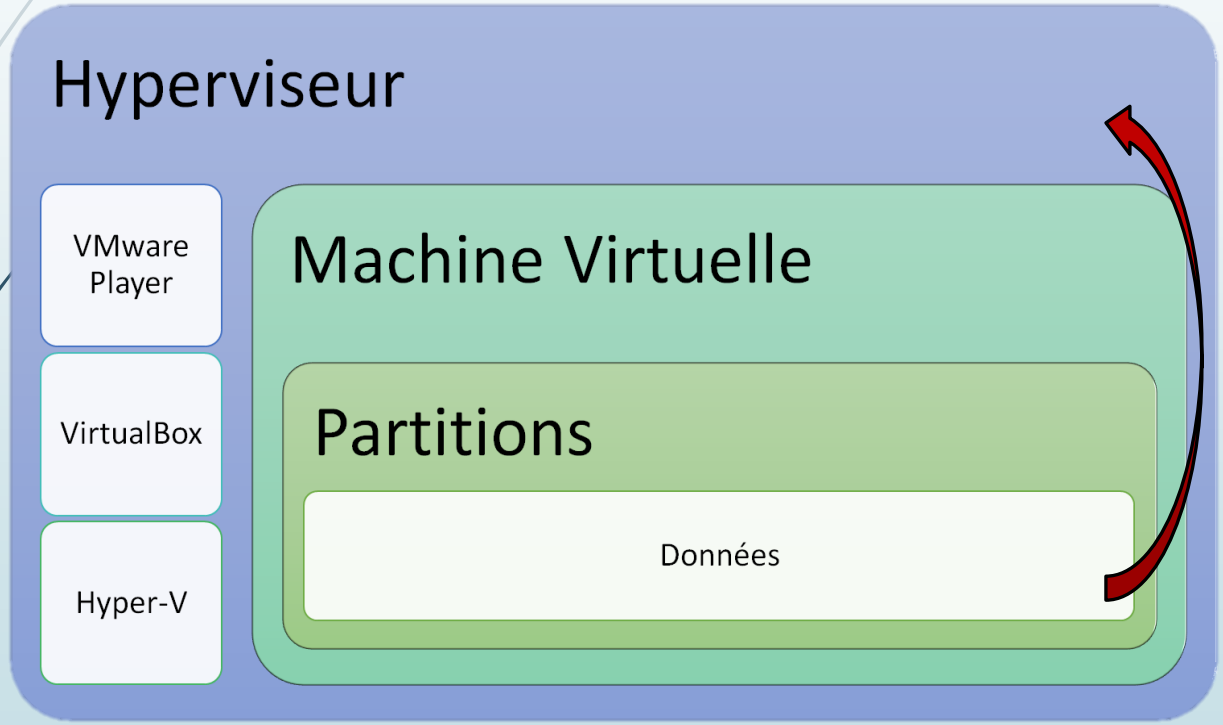
- Détermine le système de fichiers (NTFS, FAT32, …)
- Renvoie l'adresse des fichiers

Extraction

- Renvoie la donnée présente à une adresse

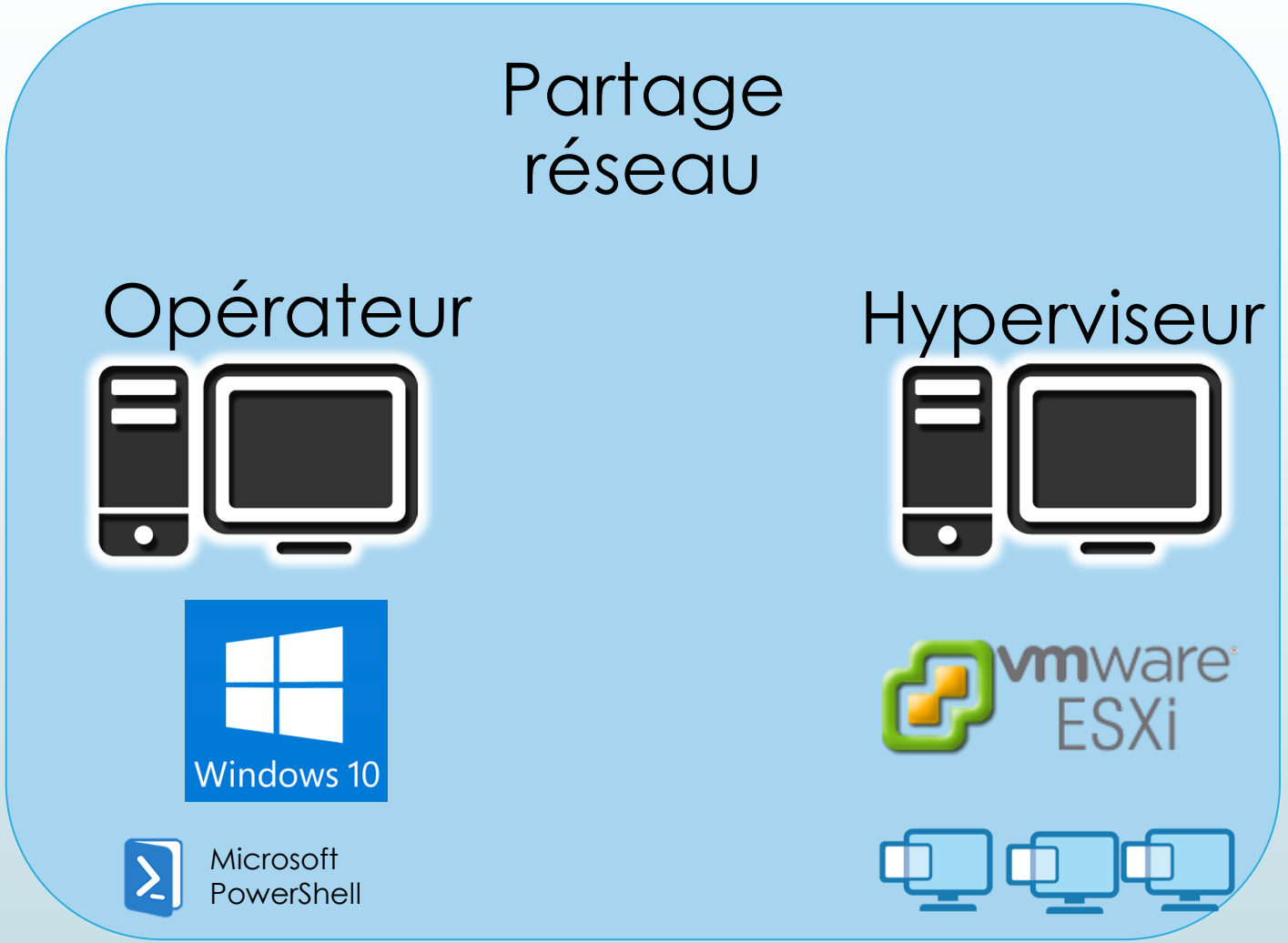
Récapitulatif

Extraction des données
d'une VM vers l'hyperviseur

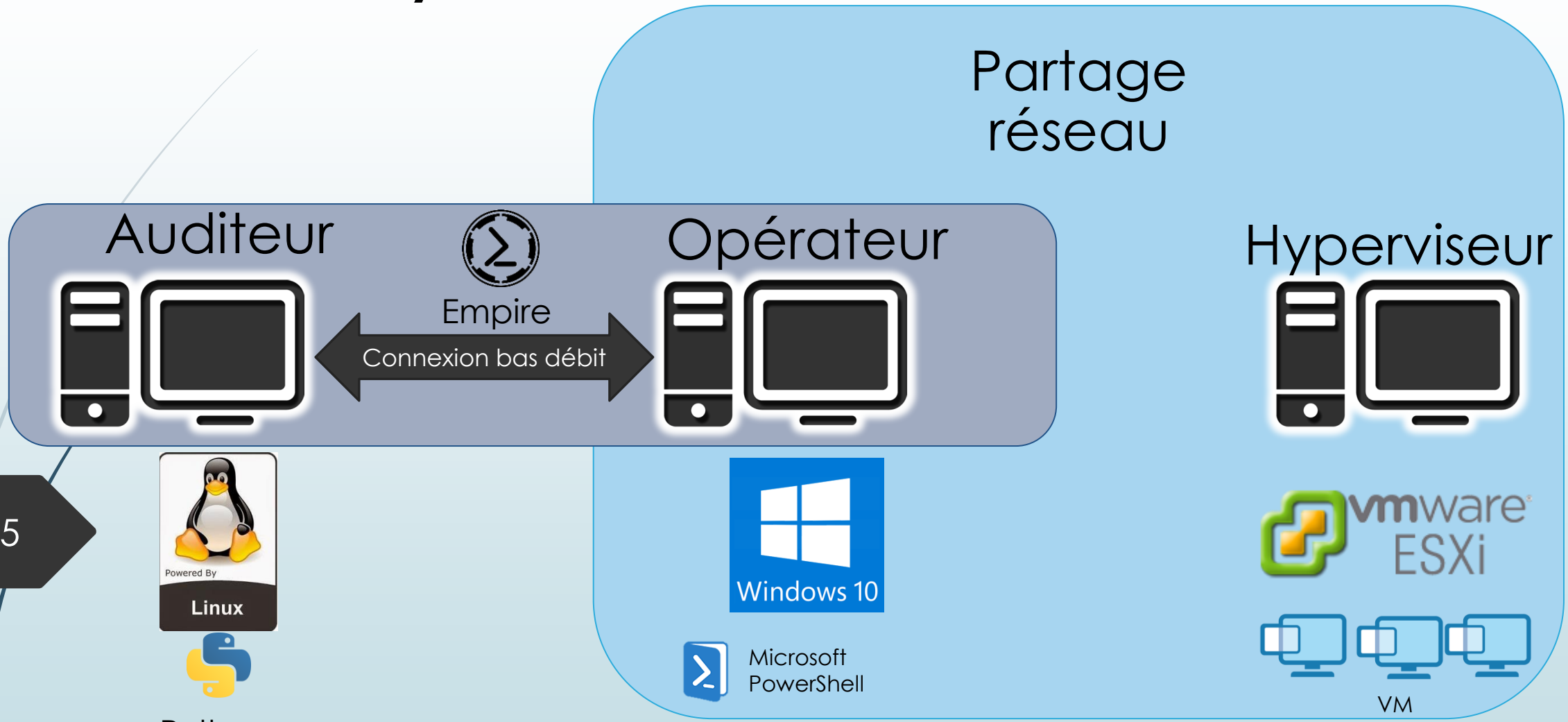


Exfiltration par le réseau

III - A) Architecture réseau



III - A) Architecture réseau

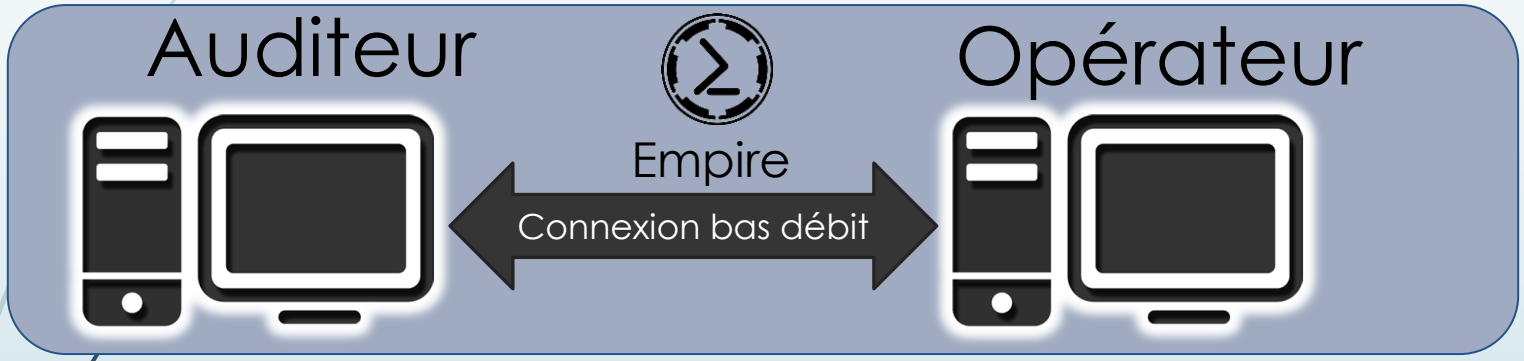


III - B) Empire

Outil Post exploitation

Assure l'exécution d'outils sur la machine cible et l'exfiltration des données

Fonctionne sous forme de compositions de modules



Python

Microsoft PowerShell

Spécification technique :

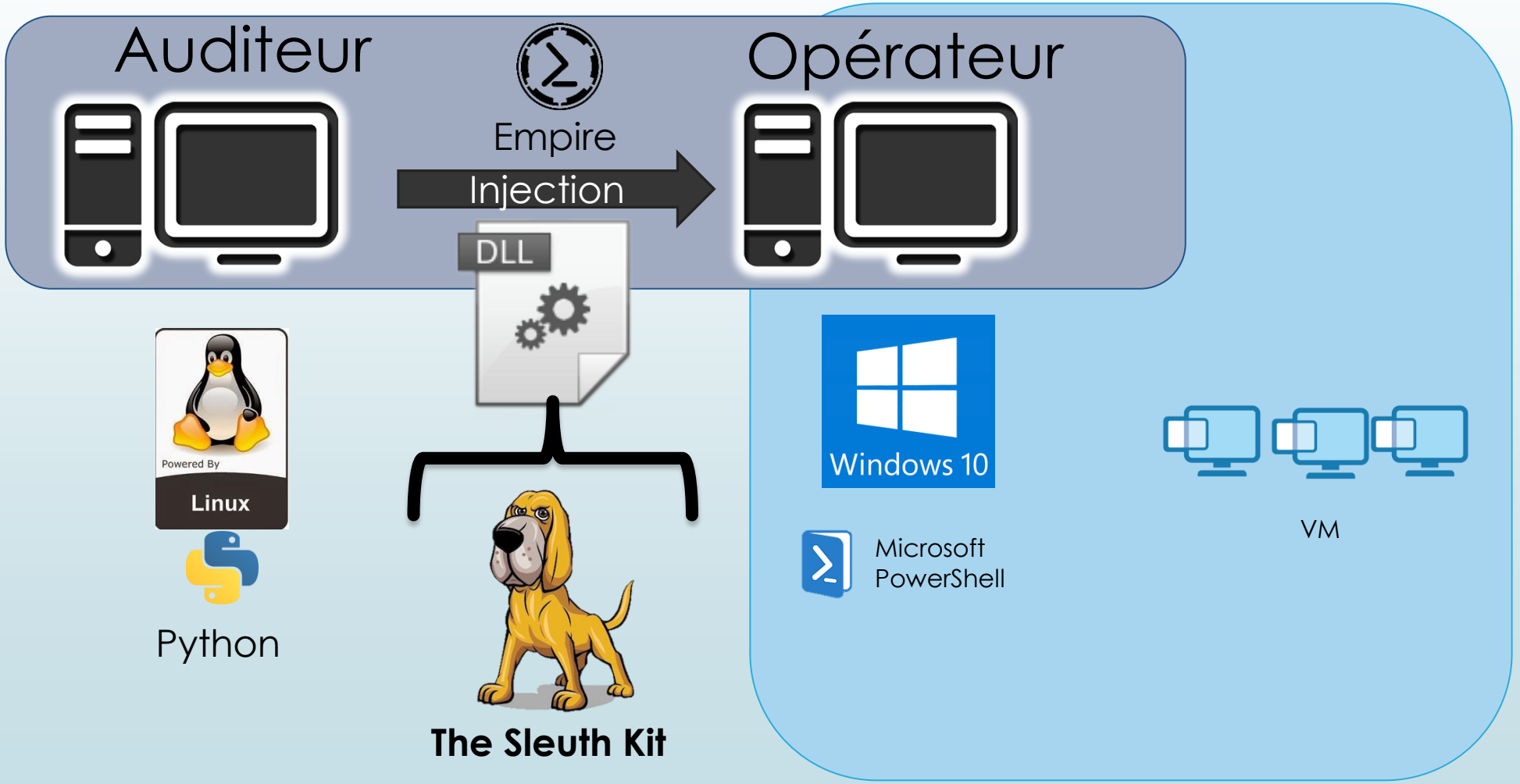
Framework en Python

Exécuté sur la machine de l'auditeur

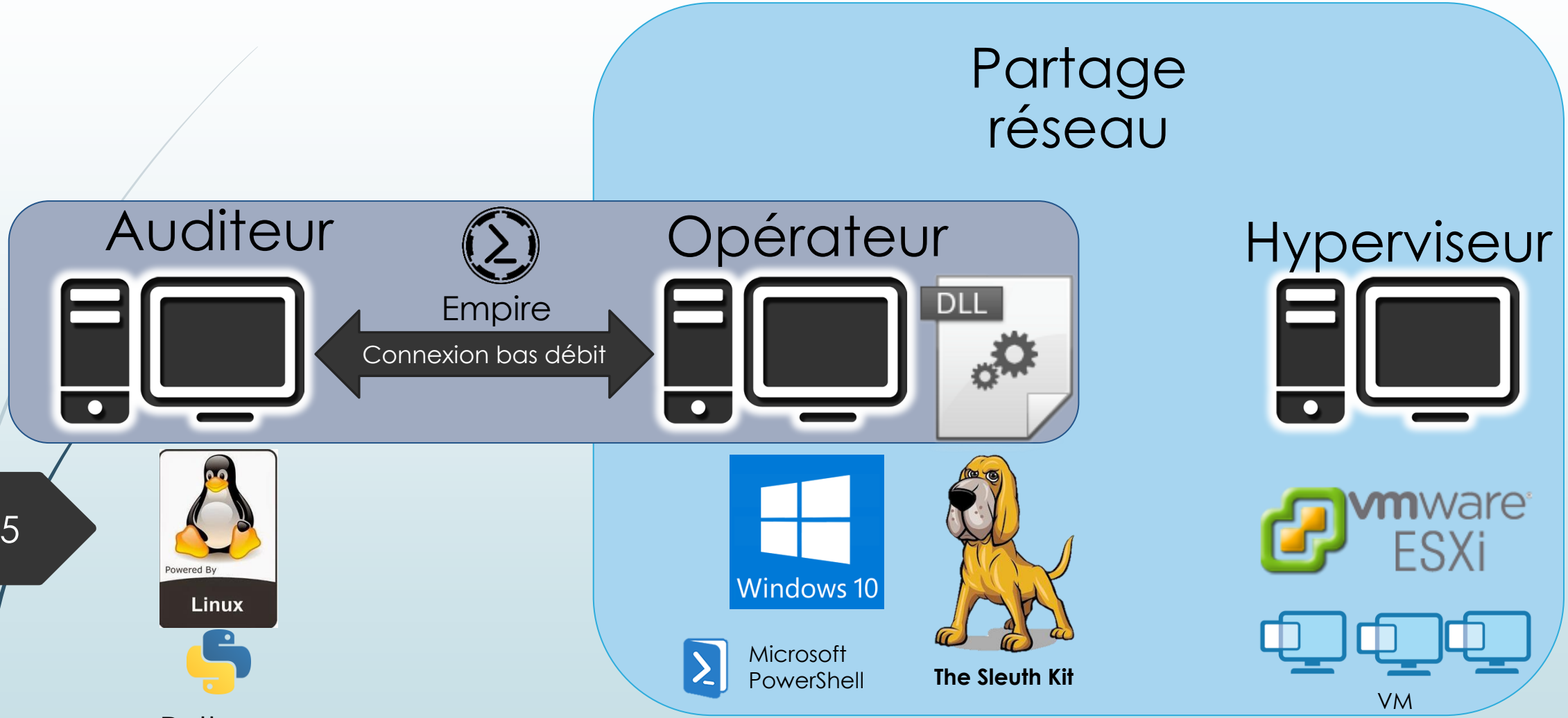
Génère et interagit avec des agents en Powershell sur la machine cible

III - C) Reflective Code Injection

2 Options : Recoder TSK en Powershell ou utiliser la *Reflective Code Injection*.



Récapitulatif



Remerciement

ensisa

UNIVERSITÉ HAUTE-ALSACE