MISSION Bash

Votre mission : Vidéo mission_bash2.mp4

Un espion d'un laboratoire de recherche étranger a installé une machine sous linux sur le réseau du laboratoire de SI avec des objectifs d'espionnage, voir de prise de contrôle du parc informatique.
Votre mission , et vous êtes obligé de l'accepter, est de retrouver la machine sur le réseau, vous y connecter en ssh puis retrouver les données sensibles stockés par l'espion. Vous devrez récupérer un maximum d'informations sur l'agent infiltré.
Afin de vous aider dans votre mission, le département R&D du labo SI à prévu une feuille de route que vous devrez suivre à la lettre.
Naturellement, en cas d'échec ou si votre activité de contre espionnage sur le réseau était découverte, le laboratoire niera vous connaitre et vous serez tenu pour entièrement responsable.

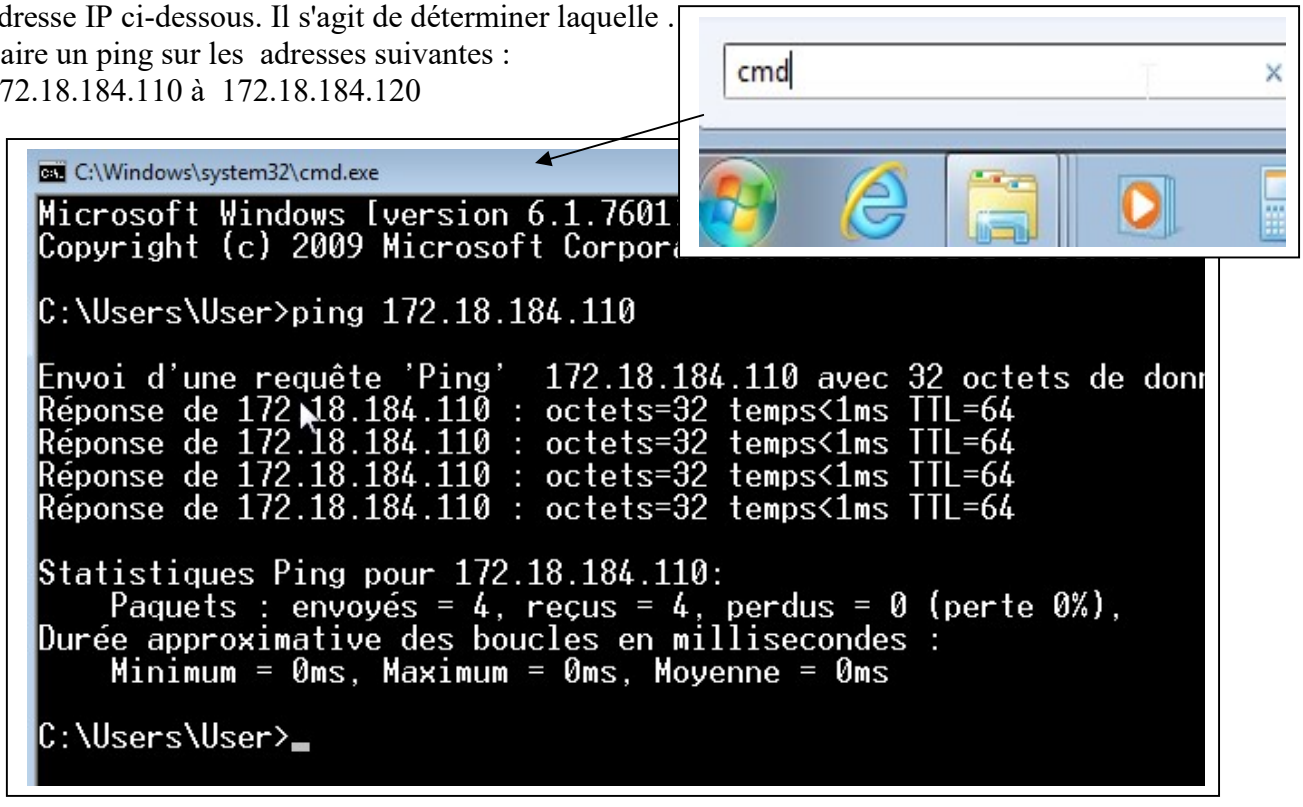
Votre feuille de route

Doc ressources dispo : memo_bash.pdf

Etape 1 :

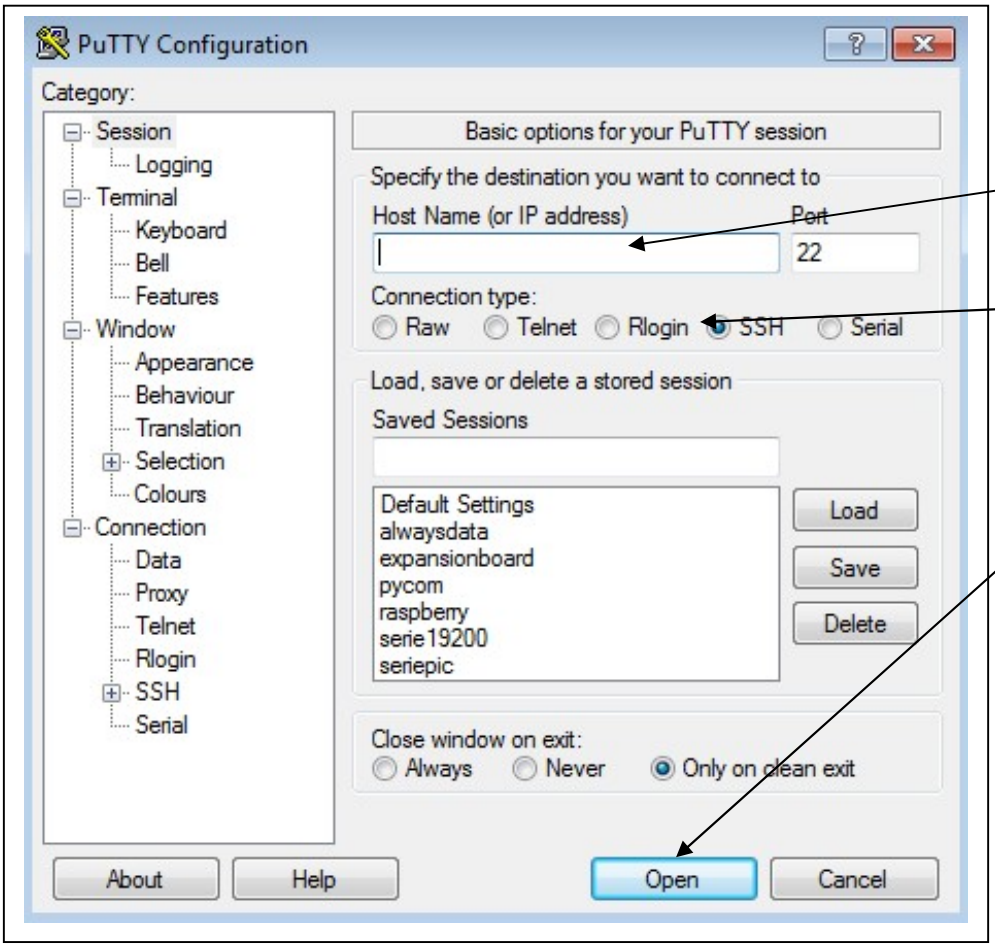
Commande DOS (cmd) : ping

Le département R&D a déterminé que la machine linux est connecté au réseau avec l'une des adresse IP ci-dessous. Il s'agit de déterminer laquelle .
Faire un ping sur les adresses suivantes :
172.18.184.110 à 172.18.184.120



Chaque fois que le ping renvoie une réponse valide, notez l'adresse IP

Lancer ensuite Putty qui est un logiciel qui va vous permettre de vous connecter en SSH au serveur distant sous linux. SSH est un Shell de commande en ligne avec un protocole de communication sécurisé.



Entrer l'adresse IP valide obtenu précédemment et

et sélectionner SSH .

Cliquer sur OPEN

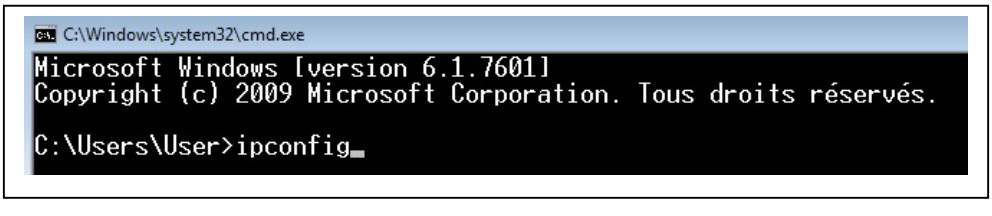
Si une erreur survient lors de la demande de connexion c'est que votre adresse IP ne convient pas. Passez à la suivante.
Si la connexion se fait, vous devrez entrer le login et le pass suivant:
login : agentx
pass : espion007

Etape 2 : who (linux) , ipconfig (windows), ifconfig (linux)

Une fois logué sous linux, taper la commande suivante :
ifconfig
--> Indiquer les données réseau du rasberry : adresse ip , broadcast et masque de eth0

Réponse :

who (permet de connaître tous les utilisateurs connectés et les IP associées)
--> Repérer l'adresse IPv4 de votre machine (pour la connaitre, sous Windows, taper **ipconfig** dans une fenêtre de commande cmd)



--> Donner les informations correspondant à votre connexion (exemple ci-dessous)

Réponse :

Etape 3: commandes cd , cd.. ls et pwd

Le dossier agentx se trouve dans le système de fichier de rasbian (linux) .
En utilisant les commandes cd , cd .. , ls et pwd , compléter la liste des dossiers situés à la racine :

Réponse : bin dev home lost+found mnt proc ....

Donner la liste des dossiers situés dans répertoire "home" :

Réponse :

Etape 4 : mkdir nom_repertoire et cp nom_fichier repertoire_destination

Dans le dossier agentx, créer un dossier votre_nom (sans accent ni espace)
copier dans ce dossier , copier les fichiers doc1.txt et doc2.txt

Etape 5 : **cat nom_fichier**

Dans le fichier doc2.txt , le nom de code de l'opération de l'agent infiltré a été enregistré.
Visualiser ce fichier en tapant cat doc2.txt et donner le nom de code enregistré.

Réponse :

Etape 6 : opération cachée ...
Vous devez maintenant suivre les instructions du fichier **info5.txt** qui se trouve dans **rep1** afin de retrouver la fiche de renseignement de l'agent infiltré :
nom :
prénom :
matricule :
spécialité :

Commande utilisée pour visualiser les fichiers cachés : .....

Votre mission est maintenant terminée, veuillez remettre le compte rendu au chef de centre du labo SI pour validation