TP : Attaque Défense

Parametre des machines :

UTHAYAKUMARAN3 / SRVATCK

Général Réseau Système Adapter 1 Adapter 1 Adapter 2 Adapter 3 Adapter 4 Affichage Activer l'Interface réseau Mode d'accès réseau : Réseau Interne Son Avancé 		1 1	🕑 si	rvatck - Paramètres				? ×			
	Général	Réseau				Général	Réseau				1
	Système	Adapter 1 Adapter 2	Adapter 3 Adapter 4			Système	Adapter 1 Adapter 2	Adapter 3 Adapter 4			
	Affichage	Activer l'interface réseau				Affichage	Activer l'interface réseau				
\mathbf{P}	Stockage	Mode d'accès réseau :	Réseau interne 🔹			Stockage	Mode d'accès réseau :	Réseau interne	•		
	Son	Nom :	carte 1			Son	Nom :	carte1		~	
	Péranu	 Avance 	1 100 0 (4000 T.G. (005 4000)			1	V Avancé				
er o	Neseau	Type d'interrace :	Intel PRO/1000 T Server (82543GC)		ē	Réseau	Type d'interface :	Intel PRO/1000 T Server (8254)	3GC)	Ψ	
	Ports séries	Mode Promiscuité :	Allow All	· · · · · · · · · · · · · · · · · · ·		Ports séries	Mode Promiscuité :	Allow All		•	
Ø	USB	Adresse MAC :	080027124FA3	S		USB	Adresse MAC :	0800273F0065		S	
	Dession and asís		Câble branché					🗹 Câble branché			
	Dossiers partages		Redirection de ports			Dossiers partagés		Redirection de ports			
	Interface utilisateur					Interface utilisateur					
			ſ	OK Annuler					OK	Annular	
			l	Armuler					OK	Annuer	



dans cmd : ipconfig/all Invite de commandes

 ■ Invite de commandes
 ■ □ ×

 Microsoft Windows XP [version 5.1.2600]
 ▲

 (C) Copyright 1985-2001 Microsoft Corp.
 ▲

 C:\Documents and Settings\admin>ipconfig/all
 ▲

 Configuration IP de Windows
 ■

 Nom de l'hôte
 ●

 Type de noud
 ●

 Noutage IP activé
 ●

 Proxy WINS activé
 ●

 Carte Ethernet Connexion au réseau local:
 Suffixe DNS propre à la connexion :

 Description
 ●

 Adresse physique
 ●

 Adresse IP
 ●

 OF
 ●

 C:\Documents and Settings\admin>

🔤 Invite de commandes

Carte Ethernet Connexion au réseau local 2 : Suffixe DNS propre à la connexion Description : Carte Intel(R) PRO/1000 T pour serv eur : 08-00-27-89-9E-08 : Oui : Oui : Oui : 169.254.213.230 : 255.255.0.0 Carte Ethernet Connexion au réseau local : Suffixe DNS propre à la connexion Description : Carte Intel(R) PRO/1000 T pour serv eur #2 08-00-27-3F-00-65 : Non : 192.168.1.50 : 255.255.255.0 : 192.168.1.254 C:\Documents and Settings\Administrateur>_

_ 🗆



ropriétés de Rou	utage et accès distant (Ordinateur loc ? 🔀	Pro	priétés de Pare	-feu Windows / Partage de connexi
Général Connexior	n Récupération Dépendances	G	énéral Connexion	Récupération Dépendances
Nom du service :	RemoteAccess		Nom du service : S	haredAccess
Nom complet :	Routage et accès distant	n, n	Nom complet :	Pare-feu Windows / Partage de connexion Internet
Description :	Offre aux entreprises des services de routage dans les environnements de réseau local ou 🗸		Description :	Assure la traduction d'adresses de réseau, l'adressage, les services de résolution de noms
Chemin d'accès de	es fichiers exécutables :		Chemin d'accès des	fichiers exécutables :
C:\WINDOWS\sys	stem32\svchost.exe -k netsvcs		C:\WINDOWS\syste	em32\svchost.exe -k netsvcs
Type de démarrage	e : Automatique 🗸		Type de démarrage :	Désactivé
Statut du service : Démarrer Vous pouvez spéc service. Paramètres de dén	Démarré Arrêter Suspendre Reprendre ifier les paramètres qui s'appliquent pour le démarrage du narrage :		Statut du service : A Démarrer Vous pouvez spécific service. Paramètres de déma	rrêté Arrêter Suspendre Reprendre er les paramètres qui s'appliquent pour le démarrage r rrage : DK Annuler Appli



dans le cmd, on a fait : ping 192.168.1.50 ou 192.168.1.52 sur les different machines pour tester la connectivité des 2 machines

Ctrl + Maj + echap : pour démarrer le gestionnaire des taches





Voici ce que donne la performances dans le gestionnaire de taches après avoir ouvert 50 fois le bloc-note Essai.bat et le bloc notenote pingdos.bat .

plications Processus	Performan	ces Mise en réseau Utilisateurs	
Util. de l'UC	Historique d	e l'utilisation de l'UC	
0 %			L A
Util, du fichier	Historique d	utilication du fichier d'échange	
our de nerlier	nisconque u	adisation da nenior a cellarige	
			\rightarrow
139 M0			
Totaux		Mémoire physique (Ko)	
Handles	37663	Total 196080	
Threads	268	Disponible 72428	
Processus	18	Cache systeme 6/668	
Charge dédiée (Ko)		Mémoire pour le noyau (Ko)	
Total	142972	Total 19472	
Limite	477432	Paginée 13668	
Pic	291216	Non paginée 5804	

	- Performan	CPS Mico op vácozu (Ukliczka wo
plications Process	IS renorman	Mise en reseau Oulisateurs
Util. de l'UC	Historique d	de l'utilisation de l'UC
0 %	A A A A A A A A A A A A A A A A A A A	
Util. du fichier 🚽	Historique d	l'utilisation du fichier d'échange
281 Mo	L	
2011/0		
Totaux		Mémoire physique (Ko)
Handles	40216	Total 196080
Threads	318	Disponible 38700
Processus	68	Cache système 70824
-Charge dédiée (Ko	·	Mémoire pour le novau (Ko)
Total	288324	Total 22364
Limite	477432	Paginée 16512
Pic	291216	Non paginée 5852

Après avoir fermé les 50 blocs- no

note.

En ouvrant plusieurs fois le même fichier, le processus, la mémoire utilisé, le total de la charges dédié, la disponible de la mémoire physique (Ko) ont tous augmenté en grandes quantité. En fermant simultanément tout les fichiers, tout cela à de nouveau baisser et est revenu à son point de départ.

4.

Les attaques par déni de service non distribuées peuvent être contrées en identifiant l'adresse IP de la machine émettant les attaques et en la bannissant au niveau du pare-feu ou du serveur. Les paquets IP provenant de la machine hostile sont dès lors rejetés sans être traités empêchant que le service du serveur ne soit saturé et ne se retrouve donc hors-ligne.

Jeux express

Propriétés de jeux express	Autorisations pour jeux express	<u> Y X</u>
Gén ^r yal Partage Sécurité Personnaliser	Autorisations du partage	
Vous pouvez partager ce dossier avec d'autres utilisateurs	Noms d'utilisateurs ou de groupes :	
du réseau. Pour activer le partage de ce dossier, cliquez sur Partager ce dossier.	Tout le monde	
C Ng pas partager ce dossier		\mathbf{k}
Partager ce dossier		
Nom du partage : ieux express		
Commentaire :	Ajouter	<u>Supprimer</u>
Nombre limite O Ma <u>xi</u> mum autorisé	Autorisations pour Tout le monde Autorise	r Refuser
Nombre d' <u>u</u> tilisateurs autorisés : 20	Contrôle total	
Pour définir les autorisations d'accès à ce	Modifier 🗹	
Pour configurer les paramètres d'accès hors		
connexion, cliquez sur Mise en cache.		
	Propriétés de jeux express	Appliquer
Sélectionnez Utilisateurs ou Groupes	Général Partage Sécurité Personnaliser	
<u>S</u> électionnez le type de cet objet :	Noms d'utilisateurs ou de groupes :	
Utilisateurs, Groupes ou Entités de sécurité intégrées Types d' <u>o</u> bjet	Administrateurs (ESM-0ZDM9T0XS2A\Administrateurs)	
À gartir de cet emplacement :	SYSTEM	
	Itilisateurs (ESM.0ZDM9T0XS24\Utilisateurs)	
Entrez les noms des objets à sélectionner (<u>exemples</u>) : Tout le monde Vérifier les noms	Utilisateurs avec pouvoir (ESM-0ZDM9T0XS2A/Utilisateurs avec p	ouvoir)
	Ajouter	Supprimer
Avancé UK Annuler	Autorisations pour Tout le monde Autoriser	Refuser
Modification	Contrôle total	
Affichage du contenu du dossier	Lecture et exécution	
	Affichage du contenu du dossier	
Autorisations spéciales	Écriture	
	Autorisations spéciales	<u> </u>
Pour definir des autorisations spèciales ou des paramètres <u>P</u> aramètres avancés, cliquez sur Paramètres avancés.	Pour définir des autorisations spéciales ou des paramètres	
	avancés, cliquez sur Paramètres avancés.	mètres avancés



Général Raccourci Options Police Disposition Couleurs Compatibilité Sécurité
JEUDECON T
Y
Type de cible : Application
Emplacement : system32
Cible : %windir%\system32\shutdown.exe -s
Démarrer dans : Xwindir%
Iouche de raccourci : Aucun
Exécuter : Fenêtre normale
Commentaire :
<u>R</u> echercher la cible Changer d'icône Ayancé

Ou retrouver le fichier attrape_nigault.bat :

Fichies Edition Affichage Fa	unia Outila 2						
	<u>zons Quais r</u>						
🔇 Précédente 👻 🕤 👻 🦻 🔎	Rechercher 🌔 Dossiers 🛛 🕼 🍞 🗙	∽					
Adresse 🗀 and Settings\All Users\UTHAYAKUMARAN\Documents\jeux express 🗾 🎅 OK							
Nom 🔺	Taille Type	Date de modif					
PJEUDECON	2 Ko Raccourci	25/11/2022 1					
attrape_nigault.bat	1 Ko Fichier de command	25/2/2022 1					
		ů					
•		E					

Dans propriétés de BEAUNIGAULT, faire :

Fichier	Machine	Ecran Entrée Périphériques Aide	
	2	Propriétés de BEAUNIGAULT	
Assig		Général Raccourci Options Police Disposition Couleurs Compatibilité Sécurité	L
Configur	Eichier E	BEAUNIGAULT	
-		Type de cible : Fichier de commande Windows	L
Ī	Nom 🔺	Emplacement : jeux express	
	P JEUDEC(<u>C</u> ible : HAYAKUMARAN\Documents\jeux express\attrape_nigault.bat"	
	P BEAUNIC	Démarrer dans : ettings\All Users\UTHAYAKUMARAN\Documents\jeux express"	
		Iouche de raccourci : Aucun	L
		Exécuter : Fenêtre normale	L
		Commentaire :	L
	•	Rechercher la cible Changer d'icône Avancé	
-			

Changer d'icone, puis cliquez ok, et

choisir l'icone du cadenas et ne pas oublier de cliquer sur «appliquer» et puis «ok» pour valider l'icone :

Général Raccourci Options Police Disposition Couleurs Compatibilité Sécurité	<u>.</u>	BEAUNIGAULT	
	CI	hanger d'icône	?
E BEAUNIGAULT	Type de	<u>R</u> echercher des icônes dans ce fichier :	
Type de cible : Fichier de commande Windows	Emplace	ystemRoot%\system32\5HELL32.dll	Parcourir
Emplacement : jeux express	<u>C</u> ible :	Sélectionner une icône dans la liste ci-d	essous :
Changer d'icône Changer d'icône Le fichier Ct/Documents and Settings\All	<u>D</u> émarre		2 💦
Users\UTHAYAKUMARAN\Documents\jeux x express express\attrape_nigault.bat ne contient aucune icône.	<u>I</u> ouche		
	E <u>x</u> écute		
Rechercher la cible Changer d'icône Avancé	Comm <u>e</u> r	N 🖉 🖉 🖳	3
	<u>R</u> echer	0 📝 🖬 🛃 太	6
			•
		ОК	Annuler

? ×

e

Į F attrape_n

nents\jeu

A<u>v</u>an

Pour faire la partage du fichier jeux express :

Fichier Machine Écran Entrée Périphériques Aide	incriter Internitie Letter	n endee renprienques mue	
Asse Sécurité Perspriétés de jeux express Configur Sécurité Partage Sécurité Orificat Précédet Adresse Porter de dossier avec d'autres utilisateurs du réaseu Pour activer le partage de ce dossier, cliquez au Partage ce dossier Nom ^ • • Partager ce dossier • • • Partager ce dossier • • • Partager ce dossier • • • • • • Partager ce dossier • • • • • • Partager ce dossier • • • • • • • • • • • • • • • • • • • • • • • • • • • • • • • • • • • • • • • • • •	? X Prot f Asset C <doc< td=""> Onligut C<doc< td=""> Prot f G Prot f <td< th=""><th>Autorisations pour jeux express Autorisations du partage Noms d'utilisateurs ou de groupes : Autorisations pour Tout le monde Autorisations pour Tout le monde Contrôle total Modifier Lecture</th><th>? ≍ Aiguter Supprimer Autoriser Refuser ☑ □ ☑ □</th></td<></doc<></doc<>	Autorisations pour jeux express Autorisations du partage Noms d'utilisateurs ou de groupes : Autorisations pour Tout le monde Autorisations pour Tout le monde Contrôle total Modifier Lecture	? ≍ Aiguter Supprimer Autoriser Refuser ☑ □ ☑ □
	rba ■ CTRL DRC Démarrer CTRL DRC	C:\Documents and Se	OK Annuler Appliquer
			🖸 💿 💷 🚽 🖄 🥅 💷 🔛 🌠 🚫 💽 CTRL DROITE 🔅

Connecter un lecteur réseau...

Connecter un lecteur	éseau	×			
	Windows vous permet de vous connecter à un dossier réseau partagé et d'assigner une lettre à la connexion afin d'accéder à ce dossier depuis le Poste de travail. Spécifiez la lettre désignant le lecteur et le dossier auxquels vous souhaitez vous connecter :				
	Lecteur : Z: Dossier : \\192.168.1.50\jeux express)			
a travail	Ouvrir une session de stockage en ligne ou se connecter a un serveur réseau.)			

Nom d'utilisateur : Administrateur

Mot de passe : Routeur0*



Jeux express est maintenant connecté sur les 2 machines virtuelles.

Tester un Trojan :



poste de travail.

En cliquant sur JEUDECON :



En cliquant sur BEAUNIGAULT :



Apres avoir lancer JEUDECON, un minuteur c'est lancé, affichant le temps restant avant que la machine ne s'eteigne.

Apres avoir lancer BEAUNIGAULT, le fichier JEUDECON a été effacer.

JEUDECON est un code attaque qui éteint la machine après l'avoir lancé, tandis que BEAUNIGAULT est un code défense qui supprime la menace d'attaque.

Ceci est un test trojan :

