Module Radio

Les commandes qui seront utiles dans ce module

- nc (netcat)
- base64
- echo
- La redirection > (chevron)
- La redirection | (pipe)
- cat
- vi (/ , .* , xG)

Le module se base sur la commande nc (netcat) qui permet de créer des sockets TCP. Il va falloir récupérer un message codé, le décoder puis trouver l'information recherchée parmi un grand texte. Enfin, il faudra recoder en base64 et le renvoyer via nc.

C'est parti !

Si vous voulez jouer au module radio seulement
./start —level 1234

Vous pouvez démarrer le module en lançant le script start.sh aprés avoir lancé la bombe

Vous devez ensuite déterminer le numéro de port à utiliser pour votre serveur TCP.
Pour cela, récupérer les lettre du serial de la bombe, transformez les en nombre via le tableau ci dessous et multiplier les entre eux. Ajouter 10 000 au résultat

Par exemple si le serial est ABC9999

num_port = (1*2*3)+10 000 =10 006

A	B	C	D	E	F	G	H	I
1	2	3	4	5	6	7	8	9
J	K	L	M	N	O	P	Q	R
10	11	12	13	14	15	16	17	18
S	T	U	V	W	X	Y	Z	
19	20	21	22	23	24	25	26	

Ouvrez un serveur TCP avec ncat au port choisi : nc -l -p num_port

Lancez dans un autre terminal start_transmission.sh afin de recevoir le message.

⚠ Le message est encodé en base64. Vous devez le décoder à l'aide de la commande base64 --decode (utilisez la redirection |).

Ce message étant très long, il serait judicieux de l'enregistrer dans un fichier texte (utilisez la redirection >).

Le message décodé est un script de film. Vous devez y trouver un code au format port:Motdepasse. Pour cela, suivez les instructions ci-dessous correspondant au film concerné. Utilisez vi pour naviguer dans le fichier (consultez « vi cheat sheet » sur Moodle).

Film	Instruction
Bee moovie	Le code se trouve après la 213ème ligne
Le seigneur des anneaux 1	Le code se trouve après la ligne de la célebre phrase de Gandalf : “You shall not pass”
Mission Impossible 2	Le code se trouve après la 7ème occurance du mot “gun”
Le parrain	Le code se trouve après une phrase qui commence par “What” et contient plus loin dans la phrase “strangers”

Une fois le code de la forme port:Motdepasse récupéré, lancez le script verif.sh.

Dans l'autre terminal, vous devrez envoyer une requête TCP avec nc, sur localhost au port trouvé dans le script du film et envoyer le Motdepasse codé en base64 (utilisez base64 et echo avec les redirections).

⚠ Si vous relancez start_transmission.sh, un nouveau texte sera généré et le mot de passe ainsi que le port vont changerr

Solution

Recevoir et décoder le message :

nc -l -p 10009 | base64 --decode > bob.txt

Envoyer le mot de passe

echo motdepasse | base64 | nc localhost port