RS2P

Contrôle final - 2024-2025

Durée : 1 heure

Aucun document autorisé sauf une calculatrice (non sur téléphone)

L'énoncé comprend trois parties : un énoncé sur la partie Réseau, un énoncé sur la partie Système et un énoncé sur la partie Sécurité et Cloud. Pour la partie Réseau, ainsi que pour la partie Sécurité et Cloud, vous répondrez directement sur l'énoncé qui sera rendu dans une copie d'examen. Le numéro d'anonymat de la copie d'examen sera reporté sur chaque énoncé/feuille rendu(e).

Numéro d'anonymat (à reporter de la copie d'examen) : **Il ne s'agit pas de votre numéro étudiant !**

Barême donné à titre indicatif :

Partie Réseau	Partie Système	Partie Sécurité
6,5 pts	6,5 pts	7 pts

Exercice - Partie Réseau

Questions :

1. Expliquez ce qu'est la technique de port mirroring qu'on peut configurer sur un commutateur.

2. Que va-t-il se passer si on applique les commandes suivantes sur un commutateur ?

   monitor session 1 source interface fa0/1 both
   monitor session 1 destination interface fa0/6

3. En supposant qu'aucune sécurité ne soit mise en place sur le commutateur, que peut faire un attaquant pour écouter le trafic transitant sur ce commutateur à l'aide des commandes précédentes ? Vous expliquerez toutes les étapes que vous devrez réaliser pour mettre en place cette attaque.

4. Pour réaliser cette attaque, quels sont les droits dont a besoin l'attaquant ? Vous en donnerez deux.

5. Expliquez le principe de l'attaque par inondation d'adresses MAC. Soyez précis dans votre description.

6. Est-ce que cette attaque nécessite les mêmes droits que l'attaque précédente ?

7. Est-ce que l'attaquant peut lancer une attaque par inondation d'adresses MAC à partir d'un commutateur connecté au commutateur attaqué (qui lui achemine le flux que l'on souhaite écouter) ? Pour vous aider dans la réponse, vous trouverez ci-dessous une partie du manuel pour la commande macof.

NAME

macof – flood a switched LAN with random MAC addresses

SYNOPSIS

macof [**-i** interface] [**-s** src] [**-d** dst] [**-e** tha] [**-x** sport] [**-y** dport] [**-n** times]

DESCRIPTION

macof floods the local network with random MAC addresses (causing some switches to fail open in repeating mode, facilitating sniffing). A straight C port of the original Perl Net::RawIP macof program by Ian Vitek <ian.vitek@infosec.se>.

OPTIONS

-i interface
Specify the interface to send on.

-s src Specify source IP address.

-d dst Specify destination IP address.

-e tha Specify target hardware address.

-x sport
Specify TCP source port.

-y dport
Specify TCP destination port.

-n times
Specify the number of packets to send.

Values for any options left unspecified will be generated randomly.

8. Donner une sécurisation possible sur les commutateurs pour éviter ces attaques.