Ancien-examen - Bon travail

Sécurité Informatique (École Polytechnique de Montréal)

Lequel de ces paradigmes ne fait pas partie des paradigmes de base de la cybersécurité :

- a. Cyber détection
- b. Cyber défense ✖
- c. Cyber résilience
- d. Cyber protection

Votre réponse est incorrecte.

La réponse correcte est :
Cyber détection

Lequel de ces principes n'est pas un principe de base de la cyber résilience :

- a. L'adaptabilité
- b. L'absorbabilité
- c. La recouvrabilité
- d. La disponibilité ✔

Je suis une technique de dissimulation de données dans des données, utilisée pour cacher des images, du texte et d'autres messages dans des images, des vidéos, de la musique ou des fichiers d'enregistrement. Je suis :

- a. La Stéganographie ✔
- b. La Tomographie
- c. La Cryptanalyse
- d. La Cryptographie

AES est l'acronyme de :

- a. Advanced Encryption Security
- b. Advanced Encryption Standard
- c. Active Encryption Standard
- d. Advanced Encrypted Standard ✖

Votre réponse est incorrecte.

La réponse correcte est :
Advanced Encryption Standard

Quel comportement malveillant consiste à remplir la boîte de courriel de la victime avec des courriers électroniques non sollicités ou indésirables ?

- a. Spamming ✔
- b. Phishing
- c. Denial of Service
- d. Hooking

Votre réponse est correcte.

La réponse correcte est :
Spamming

Nous sommes des petits fichiers téléchargés dans votre système lorsque vous visitez un site web. Nous sommes les :

- a. Crawlers
- b. Caches
- c. Bots
- d. Cookies ✔

Votre réponse est correcte.

La réponse correcte est :
Cookies

Dans un système de contrôle d'accès discrétionnaire :

- a. Seul l'administrateur peut changer le propriétaire d'un objet (« owner »), c'est-à-dire l'usager à qui « appartient » un objet dans le système informatique ✔
- b. Il est possible de définir des droits d'accès sur des groupes d'objets
- c. Les permissions d'accès données à un objet doivent rester cachées et à l'abri de regard « indiscrets » de potentiels attaquants
- d. Seul le propriétaire d'un objet peut déterminer quels droits d'accès un usager peut avoir sur cet objet

Votre réponse est correcte.

La réponse correcte est :
Seul l'administrateur peut changer le propriétaire d'un objet (« owner »), c'est-à-dire l'usager à qui « appartient » un objet dans le système informatique

L'utilisation d'une méthode d'authentification avec mot de passe à usage unique (« one-time password ») basée sur un secret partagé réduit le risque de compromission des comptes usagers dans le cas où la base de données d'usager est piratée.

Veuillez choisir une réponse.

- Vrai
- Faux ✖

La réponse correcte est « Vrai ».

Sous Linux, les applications s'exécutent généralement avec les droits d'accès de l'utilisateur qui a lancé l'application. Le fichier /etc/shadow peut seulement être modifié par l'utilisateur root. Comment est-ce que les utilisateurs peuvent changer leur propre mot de passe (contenu dans /etc/shadow) en utilisant le programme passwd ?

- a. Le mot de passe de l'utilisateur est vérifié plus tard par un administrateur, qui fait la mise à jour de /etc/shadow
- b. Le programme passwd s'exécute avec les droits de root parce qu'il utilise le bit setUID ✔
- c. Le mot de passe de l'utilisateur est originellement dans /etc/shadow, et il est copié dans /home/USER/shadow où l'utilisateur peut le modifier.
- d. Les utilisateurs peuvent seulement changer leur mot de passe s'ils ont le mot de passe de root

Votre réponse est correcte.

La réponse correcte est :
Le programme passwd s'exécute avec les droits de root parce qu'il utilise le bit setUID

L'entropie peut être une mesure décrivant la difficulté de mener les attaques suivantes, à l'exception de :

- a. Une attaque de crackage de mot de passe par force brute.
- b. Une attaque de cryptanalyse par analyse fréquentielle.
- c. Une attaque de « session hijacking » dans une application Web utilisant des jetons de session (session ID).
- d. Une attaque de déni de service par SYN flooding. ✔

Votre réponse est correcte.

La réponse correcte est :
Une attaque de déni de service par SYN flooding.

Une base de données de l'organisation X contenant des informations sensibles sur ses clients a fait l'objet d'une fuite et s'est retrouvée sur le marché noir, où elle a été vendue au crime organisé afin de leur permettre de commettre de la fraude. On soupçonne un employé de l'organisation d'avoir subtilisé ces informations, auxquelles il avait légitimement accès dans le cadre de ses fonctions, et de les avoir revendues. Quel facteur de l'analyse de risque est différent dans ce cas par rapport à un autre où un acteur externe aurait exploité une vulnérabilité des systèmes pour gagner accès à ces données, les copier et les revendre.

- a. Motivation
- b. Opportunité ✔
- c. Impact
- d. Capacité

Votre réponse est correcte.

La réponse correcte est :
Opportunité

On considère deux serveurs. Le premier combine un serveur web et un serveur FTP. Le second combine un serveur web et un serveur DNS. Chaque serveur est associé à une adresse privée dans le réseau local 192.168.0.1/24. On peut utiliser un unique pare-feu de type NetFilter pour filtrer les accès à ces deux serveurs.

Veuillez choisir une réponse.

- Vrai ✖
- Faux

La réponse correcte est « Faux ».

Laquelle de ces méthodes ne constitue pas une méthode de prévention des erreurs d'injection de code SQL

- a. L'utilisation d'un détecteur d'intrusion pouvant détecter les chaînes susceptibles d'être utilisées par une attaque d'injection de code SQL.
- b. La création d'un VPN SSL pour accéder à la base de données ✔
- c. L'utilisation de méthodes et fonctions directement implémentées sur le serveur de BD (« stored procedures »)
- d. L'utilisation de méthodes ou fonctions de filtrage des entrées venant des usagers

Votre réponse est correcte.

La réponse correcte est :
La création d'un VPN SSL pour accéder à la base de données

Le principe qui dit que la sécurité d'un algorithme de cryptographie ne devrait dépendre que du secret de la clé

- a. Ne s'applique qu'aux algorithmes de cryptographie à clé secrète
- b. S'appelle le principe de Kerchoff ✔
- c. N'est pas un principe de sécurité informatique
- d. A été énoncé par les inventeurs de l'algorithme RSA (Rivest, Shamir, Adleman)

Votre réponse est correcte.

La réponse correcte est :
S'appelle le principe de Kerchoff

Exploitation de vulnérabilité : Quelle est la différence entre une payload et un exploit ? (plusieurs réponses possibles)

- [x] a. L'exploit profite de la vulnérabilité pour faire exécuter la payload ✔
- [ ] b. La payload permet l'exécution de l'exploit
- [ ] c. C'est la même chose
- [x] d. L'exploit correspond au lanceur d'une fusée alors que la payload c'est le satellite, ou encore l'exploit correspond au missile et la payload à la charge explosive ✔

Votre réponse est correcte.

Les réponses correctes sont :
L'exploit correspond au lanceur d'une fusée alors que la payload c'est le satellite, ou encore l'exploit correspond au missile et la payload à la charge explosive,

L'exploit profite de la vulnérabilité pour faire exécuter la payload

Laquelle de ces affirmations est vraie. Un pare-feu en mode personnel :

- a. N'a pas besoin de faire du NAT même si la machine hôte possède une adresse IP privée ✔
- b. Ne peut pas être installé sur une machine hôte qui possède une seule carte réseau
- c. Ne peut pas appliquer des règles de filtrage à états (« stateful »)
- d. Ne peut filtrer que le trafic entrant sur la machine hôte

Votre réponse est correcte.

La réponse correcte est :
N'a pas besoin de faire du NAT même si la machine hôte possède une adresse IP privée

Le fichier examen.txt a été créé sur un système A en donnant les droits de lecture et écriture au propriétaire du fichier (rw-------). Le fichier est mis dans une clé USB et la clé est connectée dans un autre système B. Quel contrôleur de référence (système de contrôle d'accès) sera utilisé pour imposer les droits d'accès ?

- a. Le contrôleur de référence de la clé USB
- b. Le contrôleur de référence du système A
- c. Le contrôleur de référence du système B ✔
- d. Aucune de ces réponses

Votre réponse est correcte.

La réponse correcte est :
Le contrôleur de référence du système B

Donnez un exemple de défense dynamique et adaptative (Moving Target Defense)

- a. Canaries (StackGuard)
- b. Executable-space protection (ESP)
- c. StackShield
- d. Address space layout randomization (ASLR) ✔

Votre réponse est correcte.

La réponse correcte est :
Address space layout randomization (ASLR)

Les principes de segmentation d'un réseau et de défense en profondeur sont effectivement reliés dès lors que chaque segment du réseau est contrôlé par sa propre politique de filtrage. Sinon, cela ne sert à rien.

Si des pare-feu sont déployés pour filtrer l'accès à chaque segment, alors on atteint bien un objectif de défense en profondeur.

On peut notamment découper les segments en sous-segments pour renforcer la profondeur de la défense.

Suite à l'authentification d'un usager U, avec son identifiant et son mot de passe, un OTP est généré sur le dispositif local avec une fonction à sens unique connue de tous (y compris Ève) à partir d'une chaine codant l'intervalle de temps (timestamp) et un secret partagé S, associé à l'usager U. Cet OTP est alors copié par l'usager dans un troisième champ de saisie de donné fourni à cet effet dans l'application Web. L'OTP reçu est vérifié par le serveur en recalculant la fonction avec le secret partagé S, obtenu de la base de données d'usagers, et l'intervalle de temps actuel. Si le résultat est le même que l'OTP reçu, l'usager est authentifié.

Usurpation de certificat (3 sous-questions)

Bob.com est un serveur malveillant qui essaye de se faire passer pour le site légitime Charlie.com

Pour récupérer le certificat du serveur Charlie.com, il suffit que Bob.com fasse une demande de connexion HTTPS sur le site de Charlie.com

Veuillez choisir une réponse.

- (•) Vrai ✔
- ( ) Faux

La réponse correcte est « Vrai ».

Usurpation de certificat (3 sous-questions)

Bob.com est un serveur malveillant qui essaye de se faire passer pour le site légitime Charlie.com

Lorsque le browser de Alice se connecte en HTTPS sur le site Web Bob.com, Bob.com lui présente le certificat valide du site Charlie.com. Dans ce cas, le browser d'Alice va vérifier le certificat et détecter que Bob.com a usurpé le certificat de Charlie.com. Le browser va rejeter le certificat et indiquer un message d'erreur à l'usager.

Veuillez choisir une réponse.

- (•) Vrai ✔
- ( ) Faux

La réponse correcte est « Vrai ».

La réponse est non sauf si Bob.com a volé la clé privée du serveur Charlie.com.

Lorsque le browser de Alice va vérifier la certificat envoyé par Bob.com, le browser de Alice va vérifier si ce certificat est valide : (1) il a été signé par une autorité de certification reconnue par Alice, (2) le hash associé au certificat confirme que le certificat est intègre, (3) Alice va demander à l'autorité de certification de confirmer que le certificat n'a pas été révoqué.

Ensuite, Alice va forger une clé de session et la transmettre en la chiffrant avec la clé publique du certificat (donc celle de Charlie.com).

Code vulnérable (5 sous-questions)

On considère le code suivant :

```
#include <stdio.h>
#include <stdlib.h>

void vuln(char *arg)
 {  int i=1,
    char buffer[4];
    strcpy(buffer, arg);
    if (i=0) printf("Coooool !");
    if (i=1) printf(("Try again !");
 }
int main(int argc, char **argc)
 {
    if (argc < 2) exit(0);
    vuln(argv[1]);
    exit(1);
 }
```

Ce code est vulnérable à une attaque par débordement de pile (stack overflow)

Veuillez choisir une réponse.

- ○ Vrai
- ◉ Faux ✖

Code vulnérable (5 sous-questions)

On considère le même code que celui de la question précédente :

```
#include <stdio.h>
#include <stdlib.h>

void vuln(char *arg)
 {  int i=1,
    char buffer[4];
    strcpy(buffer, arg);
    if (i=0) printf("Coooool !");
    if (i=1) printf(("Try again !");
 }
int main(int argc, char **argc)
 {
    if (argc < 2) exit(0);
    vuln(argv[1]);
    exit(1);
 }
```

Le programme ci-dessus est appelé avec la chaîne de caractères « 123 ». La réponse du programme sera :

- a. Try again ! ✔
- b. Coooool !

Votre réponse est correcte.

La réponse correcte est :
Try again !

L'utilisateur va saisir la chaine de caractère "1234" (de longueur 4).

Une fois cette chaine saisie, celle-ci va être complétée par le symbole "00" pour indiquer la fin de la chaine.

La chaine "1234" va remplir le bufffer char.

Le "00" va créer un débordement de buffer qui va écraser la variable i.

La variable i vaut donc 0 et donc le message "Try again !" est affiché.

Si le programme est appelé avec la chaine de caractères « 12345 », alors c'est le caractère 5 qui va écraser la variable "i".

La valeur de "i" sera donc 5.

Dans ce cas, la chaine de caractères "123456789" risque d'écraser la variable d'environnement ainsi que de l'adresse de retour.

Cela risque donc de provoquer une erreur de type "segmentation fault".

La source des ennuis (8 sous questions)

On considère une source S1 markovienne qui génère des 0 et des 1. La probabilité d'apparition d'un 0 et de ¼ et celle d'un 1 est de ¾. Quelle est l'entropie d'un message de 10 chiffres généré par la source S1 ?

On applique la formule pour calculer l'entropie de la source :

$H(S1) = 1/4 * \log2(4) + 3/4 * \log2(4/3)$

$= 1/2 + 0,311 = 0,811$ bits

Comme la source est markovienne (source aléatoire sans mémoire), il suffit de multiplier par 10 pour avoir l'entropie du message :

La source des ennuis (8 sous questions)

En fait la source S1 contient un bug. Lorsque la source génère le premier chiffre, alors la probabilité d'apparition d'un 0 est bien de ¼ et celle d'un 1 est de ¾. En revanche, pour le second chiffre, le résultat est le suivant :

- Si le premier chiffre est un 0, alors la probabilité d'apparition d'un 0 est de ½ et celle d'un 1 est aussi de ½.
- Si le premier chiffre est un 1, alors la probabilité d'apparition d'un 0 est de 1/3 et celle d'un 1 est de 2/3.

Le processus se répète de façon identique pour le troisième et quatrième chiffre : les probabilités associées au troisième chiffre sont identiques à celles du premier chiffre et les probabilités associées au quatrième chiffre sont identiques à celles du second chiffre.

Et ainsi de suite.

On appelle S2 cette seconde source.

Proposer une méthode M1 pour calculer l'entropie fréquentielle caractère par caractère de la source S2. Justifier votre réponse.

Soient Pi(0) et Pi(1), la probabilité d'avoir respectivement un 0 ou 1 en position i.

On a donc P1(0) = 1/4 et P1(1) = 3/4

Soit P2(0) et P2(1), la probabilité d'avoir respectivement un 0 ou 1 en deuxième position.

On a P2(0) = P2(0 | 0) + P2(0 | 1) = 1/2 * 1/4 + 1/3 * 3/4 = 3/8

Et P2(1) = P2(1 | 0) + P2(1 | 1) = 1/2 * 1/4 + 2/3 * 3/4 = 5/8

La fréquence d'apparition de 0 est égale à la limite quand n tend vers l'infini de sigma(i) Pi(0) / n

Comme le processus se répète respectivement sur les positions paires et les positions impaires, on a :

P2n (0) = P2(0) et P(2n+1) (0) = P1(0)

Si on note Pf(0) la probabilité fréquentielle de 0, on a donc Pf(0) = 1/2 (P1(0) + P2(0)) = 1/2 (1/4 + 3/8)) = 5/16

On calcul de même Pf(1) = 1/2 (P1(1) + P2(1)) = 1/2 (3/4 + 5/8) = 11/16

L'entropie fréquentielle caractère par caractère de la source S2 sera donc égale à :

Hf(S2) = Pf(0) * Log2(1/Pf(0)) + Pf(1) Log2(1/Pf(1))

La source des ennuis (8 sous questions)

Appliquer la méthode M1 pour calculer l'entropie caractère par caractère de la source S2. Soit E1 la valeur obtenue.

E1 = 5/16 * Log2(16/5) + 11/16 + Log2(16/11) = 0,3125 * 1,678 + 0,6875 * 0,540 = 0,896

La source des ennuis (8 sous questions)

On considère un message de longueur N générée par la source S2. Expliquer pourquoi l'entropie réelle de ce message n'est pas égale à N * E1. Cette entropie réelle est-elle supérieure ou inférieure à N * E1 ?

Le source S2 n'est pas markovienne car la probabilité d'apparition d'un caractère en position paire dépend de la probabilité d'apparition d'un caractère en position impaire.

L'entropie réelle d'un message générée par la source S2 n'est donc pas égale à N * E1.

Elle est strictement inférieure à N * E1.

La source des ennuis (8 sous questions)

Proposer une méthode M2 pour calculer l'entropie réelle des messages générés par la source S2. Justifier votre réponse.

Pour calculer l'entropie réelle de la source S2, il faut calculer l'entropie par digramme (bloc de deux caractères).

On considère donc le langage S2^2 constitué de blocs de caractère en position impaire puis paire

Comme le processus de génération des caractères se répète tous les deux caractères, la source S2^2 est donc markovienne.

Pour calculer l'entropie réelle Hr de la source S2, il faut donc calculer l'entropie de la source S2^^2 et on aura : Hr(S2) = H(S2^2) / 2

La source des ennuis (8 sous questions)

Appliquer la méthode M2 pour calculer l'entropie d'un message de 10 chiffres généré par la source S2.

On calcule l'entropie du langage S2^2.

Il y a 4 digrammes possibles : 00, 01, 10, 11

On a P(00) = 1/4 * 1/2 = 1/8, P(01) = 1/4 * 1/2 = 1/8, P(10) = 3/4 * 1/3 = 1/4, P(11) = 3/4 * 2/3 = 1/2

Donc H(S^2/2) = 1/8 * Log2(8) + 1/8 * Log2(8) + 1/4 * Log2(4) + 1/2 * Log2(2) = 3/8 + 3/8 + 1/2 + 1/2 = 1,75

Une chaine de 10 caractères peux être divisée en 5 blocs de 2 caractères.

Donc H(S^2/2) = 1/8 * Log2(8) + 1/8 * Log2(8) + 1/4 * Log2(4) + 1/2 * Log2(2) = 3/8 + 3/8 + 1/2 + 1/2 = 1,75

Une chaine de 10 caractères peux être divisée en 5 blocs de 2 caractères.

L'entropie d'une chaine de 10 caractères générée par la source S2 sera donc égale à E2 = 5 * 1,75 = 8,75

On peut vérifier que 8,75 est bien inférieure à 10 * E1

La source des ennuis (8 sous questions)

Est-ce que la méthode M2 permet de calculer l'entropie du langage généré par la source S2 ? Justifier votre réponse

Comme le langage S2^2 est une source markovienne aléatoire, la méthode M2 permet bien de calculer l'entropie du langage S2.

La source des ennuis (8 sous questions)

On utilise les sources S1 et S2 pour générer des clés de longueur 128 bits. Est-ce que les clés générées par la source S1 sont plus faciles ou plus difficiles à casser que les clés générées par la source S2. Justifier votre réponse.

L'entropie d'une chaine de 128 bits générée respectivement par les sources S1 et S2 sera de :

128 * 0,811 pour S1

128 * 1,75 / 2 pour S2

Les clés générées par S2 devraient être plus difficiles à casser que celles générées par S1.

Configuration d'un pare-feu Netfilter (3 sous-questions)

On considère la configuration suivante d'un pare-feu Netfilter (il s'agit d'un extrait de la configuration vue en cours) :

```
# set default closed policy
iptables -P FORWARD DROP
# network interfaces
EXTIF=eth0
DMZIF=eth1
# addresses
EXTIP=195.55.55.1
WEB_SERVER=192.168.1.1
DNS_SERVER=192.168.1.2
# enable DNAT port translation from Internet to web server
iptables -t nat -A PREROUTING -i $EXTIF -p tcp --dport 80 -j DNAT --to-destination $WEB_SERVER:80
 # enable DNAT port translation from Internet to dns server
iptables -t nat -A PREROUTING -i $EXTIF -p udp --dport 53 -j DNAT --to-destination $DNS_SERVER:53
 # the web server must be accessible from Internet
iptables -A FORWARD -i $EXTIF -o $DMZIF -p tcp --dport 80 -m state --state NEW, ESTABLISHED -j ACCEPT
 # the dns server must be accessible from Internet
iptables -A FORWARD -i $EXTIF -o $DMZIF -p udp --dport 53 -m state --state NEW, RELATED -j ACCEPT
```

On considère que les paquets suivants arrivent, dans cet ordre, sur les interfaces du pare-feu NetFilter (on suppose que la pare-feu n'a pas reçu de paquet avant Packet#1) :

Packet	Protocole	Src-IP	Dest-IP	Src-Port	Dest-Port	TCP Flags		
						SYN	SYN-ACK	ACK
Packet#1	TCP	195.5.5.1	192.168.1.1	2240	80	1	0	0
Packet#2	TCP	195.5.5.1	195.55.55.1	2240	80	1	0	0
Packet#3	TCP	195.5.5.1	195.55.55.1	2240	80	0	0	1
Packet#4	TCP	192.168.1.1	195.5.5.1	80	2240	0	1	0
Packet#5	TCP	192.168.1.1	195.5.5.1	80	2045	0	1	0

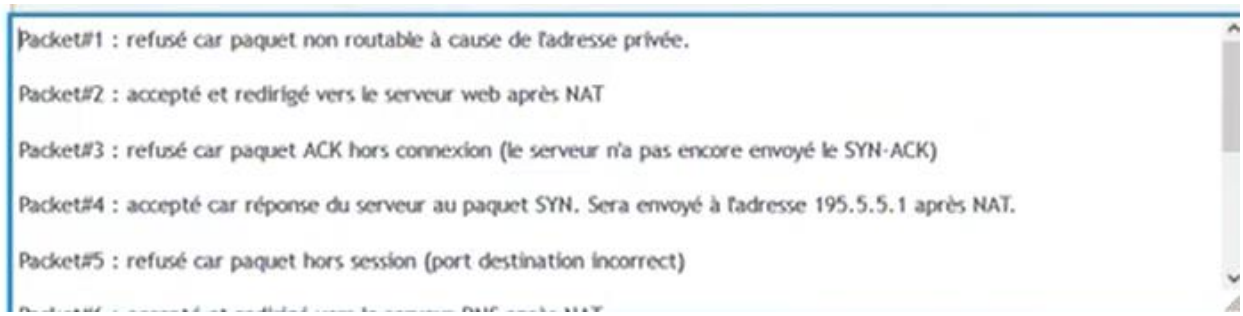
Packet	Protocole	Src-IP	Dest-IP	Src-Port	Dest-Port
Packet#6	UDP	195.5.5.1	195.55.55.1	3535	53
Packet#7	UDP	192.168.1.2	195.5.5.1	53	3535
Packet#8	UDP	192.168.1.2	195.4.4.1	53	3535

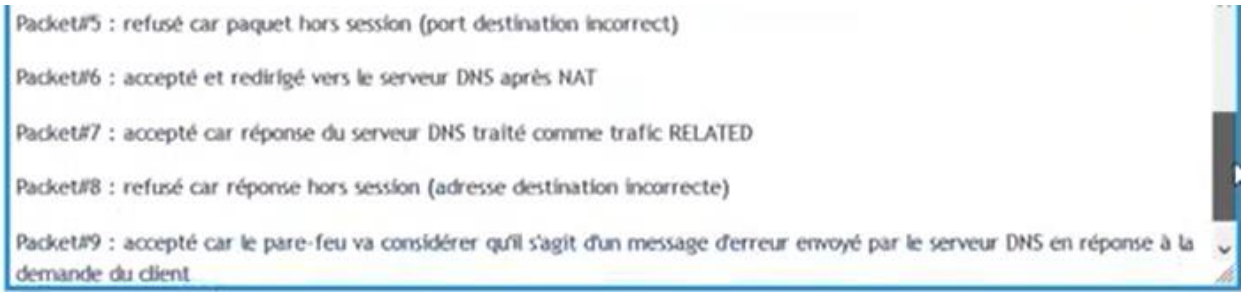
Packet	Protocole	Src-IP	Dest-IP	TYPE	CODE	Payload atttributes			
						Src-IP	Dest-IP	Src-Port	Dest-Port
Packet#9	ICMP	192.168.1.2	195.5.5.1	3	3	195.5.5.1	195.55.55.1	3535	53

Les paquets Packet#1, Packet#2, Packet#3 et Packet#6 arrivent sur l'interface EXTIF du pare-feu.

Les paquets Packet#4, Packet#5, Packet#7, Packet#8 et Packet#9 arrivent sur l'interface DMZIF du pare-feu.

Pour chaque paquet de Packet#1 à Packet#9, indiquer si le paquet sera accepté ou bloqué par le pare-feu Netfilter. Justifier la réponse.





Configuration d'un pare-feu Netfilter (3 sous-questions)

Pour le Packet#9, expliquer ce qu'il peut se passer au niveau du pare-feu et à quel type de comportement malveillant cela peut correspondre.

La pare-feu va accepter la paquet en considérant qu'il s'agit d'un message d'erreur envoyé par le serveur DNS.

Un attaquant peut utiliser cette possibilité pour générer du trafic ICMP en spoofant l'adresse du serveur DNS.

Cela peut mettre le pare-feu en déni de service (DOF - Denial of Firewall).

Ce comportement malveillant correspond à l'attaque Black-Nurse (voir dernier acétate du cours de Sécurité Réseau 1).