Yacine BOUZERARA

Échelle d'évaluation standard : **Notation en attente du traitement des éventuelles demandes de précision**	Échelle d'évaluation pondérée : **Notation en attente du traitement des éventuelles demandes de précision**

EN - A3 FISA info Sécurité filtrage

Échelle d'évaluation standard : **Notation en attente du traitement des éventuelles demandes de précision**

AAV:

- [2] Expliquer le principe de Zone DéMilitarisée
- [4] Sélectionner le filtrage réseau adapté
  - *[2] Explaining the principle of Demilitarized Zone*
  - *[4] Selecting the appropriate network filtering*

Question 1 **Question à réponse unique**

Quelle est la raison principale d’implémenter une DMZ dans une architecture réseau d’une entreprise ?
What is the main reason to implement a DMZ in an enterprise network architecture?

Réponses correctes

	Réponse attendue	Réponse saisie	Réponse discordante	
A	☐	☐	Non	Assurer un service Cloud pour accéder aux données de l’entreprise avec une couche de sécurité supplémentaire à partir d’internet. *To provide a cloud service to access company data with an additional layer of security from the Internet.*
B	☐	☐	Non	Protéger le flux de données de l’entreprise sortant via des serveurs calculateurs assurant la robustesse du chiffrement. *To protect the company's outgoing data flow via computer servers ensuring robust encryption.*
C	☑	☑	Non	Héberger les services accessibles depuis internet pour isoler et protéger le réseau interne de l’entreprise d’éventuelles attaques. *To host services accessible from the Internet in order to isolate and protect the company's internal network from possible attacks.*
D	☐	☐	Non	Authentifier les employés de l’entreprise via des serveurs RADIUS. *To authenticate company employees via RADIUS servers.*
E	☐	☐	Non	Assurer l’orchestration des différents conteneurs déployés au sein du cluster de l’entreprise. *To ensure the orchestration of the various containers deployed within the company's cluster.*

Question 2 — **Question à réponses multiples**

Parmi les propositions suivantes, quels sont les serveurs/services que nous trouvons souvent dans une DMZ ? (3 réponses)
Among the following propositions, which are the servers/services that we often find in a DMZ? (3 answers)

Réponses correctes | 0 discordance

	Réponse attendue	Réponse saisie	Réponse discordante	
A	☑	☑	Non	Serveur Nginx *Nginx server*
B	☑	☑	Non	Serveur Apache *Apache server*
C	☐	☐	Non	Serveur d'impression *Print server*
D	☑	☑	Non	Serveurs de Messagerie *Messaging Servers*
E	☐	☐	Non	Contrôleurs de domaine AD *AD domain controllers*

Question 3 — **Question à réponses multiples**

Lesquelles des ACL suivantes sont correctement écrites ? (2 réponses)
Which of the following ACLs are correctly written (2 answers)

Réponses correctes | 0 discordance

	Réponse attendue	Réponse saisie	Réponse discordante	
A	☐	☐	Non	Access-list 99 permit udp 192.168.20.0 0.0.0.255 host 8.8.8.8 eq 53
B	☑	☑	Non	Access-list 2500 permit udp 192.168.20.0 0.0.0.255 host 8.8.8.8 eq 53
C	☐	☐	Non	Access-list 1500 permit udp 192.168.20.0 0.0.0.255 host 8.8.8.8 eq 53
D	☐	☐	Non	Access-list 110 permit tcp 192.168.10.1 255.255.255.0 host 181.25.16.31 eq 443
E	☑	☑	Non	Access-list 2600 permit tcp 192.168.53.1 0.0.0.0 host 181.25.16.1 eq 443

? Question 4 **Question à réponse unique**

Quel protocole sera bloqué, si l'ACL suivante (access-list 110 deny udp 192.168.1.0 0.0.0.255 host 8.8.8.8 eq domain) est activée ?

Which protocol will be blocked, if the following ACL (access-list 110 deny udp 192.168.1.0 0.0.255 host 8.8.8.8 eq domain) is activated?

Réponses correctes

	Réponse attendue	Réponse saisie	Réponse discordante	
A	☐	☐	Non	HTTPS
B	☐	☐	Non	HTTP
C	☑	☑	Non	DNS
D	☐	☐	Non	SMTP
E	☐	☐	Non	SMB

? Question 5 **Question à réponse unique**

Un administrateur réseau souhaite bloquer le réseau 172.30.20.32/27 sauf sa première et dernière adresse machine utilisables, en autorisant tout autre trafic. Dans quel ordre doit-on appliquer les instructions suivantes via des ACL?

A network administrator wants to block the 172.30.20.32/27 network except for its first and last usable machine address, allowing all other traffic. In what order should the following instructions be applied via ACLs?

- a -permit any
- b - deny 172.30.20.32 0.0.0.31
- c - permit host 172.30.20.32
- d - permit host 172.30.20.33
- e - permit host 172.30.20.63
- f - permit host 172.30.20.62

Réponses incorrectes

	Réponse attendue	Réponse saisie	Réponse discordante	
A	☐	☐	Non	a > d > e > b
B	☐	☐	Non	b > d > f > b
C	☑	☐	Oui (+1)	d > f > b > a
D	☐	☑	Oui (+1)	e > c > b > a
E	☐	☐	Non	c > f > a > b

EN - A3 FISA info Sécurité configuration

Échelle d'évaluation standard : **Notation en attente du traitement des éventuelles demandes de précision**

AAV:

- [3] Administrer un proxy
- [3] Préparer et configurer un parefeu
- [3] Relier les outils de sécurité à l'annuaire du S.I.
  - *[3] Administering a proxy*
  - *[3] Preparing and configuring a firewall*
  - *[3] Linking the security tools to the I.S. directory.*

Question 1 — **Question d'association**

Associer chaque malware ou attaque avec la définition qui correspond :

Associate each malware or attack with the corresponding definition:

Réponses incorrectes	3 discordances

Élément à associer	Réponse attendue	Réponse saisie	Réponse discordante
Dialer	Programme qui peut établir des connexions au modem à notre insu pour établir des connexions ou composer un numéro sans qu'on le sache. A program that can establish connections to the modem stealthily in order to establish connections or dial a number without our knowledge	Une attaque dont l'objectif est de rendre inaccessibles des ressources assurant un service donné (exemple : hébergement web) en les inondant de requêtes comme TCP SYN ou ICMP echo. An attack whose objective is to render inaccessible the resources providing a given service (example web hosting) by flooding them with requests like TCP SYN or ICMP echo.	Oui (+1)
Worms	Programme qui se reproduit tout seul sans avoir besoin d'une aide extérieure en infectant plusieurs machines dans le réseau. A program that replicates itself without the need for outside help by infecting multiple machines in the network.	Programme qui se reproduit tout seul sans avoir besoin d'une aide extérieure en infectant plusieurs machines dans le réseau. A program that replicates itself without the need for outside help by infecting multiple machines in the network.	Non
Cross site scripting (XSS)	Une attaque basée sur la transmission d'un script malicieux aux victimes, et qui s'exécutera ensuite sur leur navigateur web pour accéder aux différents cookies ou aux tokens de session. An attack based on the transmission of a malicious script to the victims, which will then run on their web browser to access the various cookies or session tokens.	Une attaque basée sur la transmission d'un script malicieux aux victimes, et qui s'exécutera ensuite sur leur navigateur web pour accéder aux différents cookies ou aux tokens de session. An attack based on the transmission of a malicious script to the victims, which will then run on their web browser to access the various cookies or session tokens.	Non
Rootkit	Permet d'avoir un accès privilégié à une machine, souvent contrôlée à distance, tout en étant totalement discret. Allows to have a privileged access to a machine, often controlled remotely, while being totally discrete.	Programme qui peut établir des connexions au modem à notre insu pour établir des connexions ou composer un numéro sans qu'on le sache. A program that can establish connections to the modem stealthily in order to establish connections or dial a number without our knowledge	Oui (+1)
Distributed Denial-of-service	Une attaque dont l'objectif est de rendre inaccessibles des ressources assurant un service donné (exemple : hébergement web) en les inondant de requêtes comme TCP SYN ou ICMP echo. An attack whose objective is to render inaccessible the resources providing a given service (example web hosting) by flooding them with requests like TCP SYN or ICMP echo.	Permet d'avoir un accès privilégié à une machine, souvent contrôlée à distance, tout en étant totalement discret. Allows to have a privileged access to a machine, often controlled remotely, while being totally discrete.	Oui (+1)

? Question 2 **Question à réponse unique**

Laquelle des propositions suivantes représente une solution de sécurité qui consiste à isoler et exécuter un programme jugé suspect dans un environnement de test séparé (en quarantaine), pour étudier son comportement sans impacter l'infrastructure en production ?

Which of the following is a security solution that consists of isolating and executing a judged program suspect in a separate test environment (quarantine), to study its behavior without impacting the infrastructure in production?

Réponses correctes

	Réponse attendue	Réponse saisie	Réponse discordante	
A	☐	☐	Non	SIEM
B	☑	☑	Non	Sandbox
C	☐	☐	Non	IPS
D	☐	☐	Non	SOC
E	☐	☐	Non	IDS

? Question 3 **Question à réponses multiples**

Parmi les propositions suivantes, lesquelles ne sont pas considérées comme attaque en cybersécurité ? (2 réponses)

Which of the following is not considered a cybersecurity attack? (2 answers)

Réponses correctes | 0 discordance

	Réponse attendue	Réponse saisie	Réponse discordante	
A	☐	☐	Non	DHCP spoofing
B	☐	☐	Non	Cross site Scripting (XSS)
C	☑	☑	Non	OSPF Stub Area
D	☐	☐	Non	DNS Tunneling
E	☑	☑	Non	Split Horizon

Question 4 — **Question à réponse unique**

Parmi les propositions suivantes, laquelle différencie le mieux un IPS d'un firewall stateless ?

Which of the following best differentiates an IPS from a stateless firewall?

Réponses incorrectes

	Réponse attendue	Réponse saisie	Réponse discordante	
A	☐	☐	Non	L'IPS permet de détecter des intrusions en se basant sur une base de données de signatures, tandis que le firewall stateless bloque le trafic réseau selon l'état des protocoles (exemple : sessions TCP), basées sur des règles prédéfinies par l'administrateur de sécurité. *The IPS detects intrusions based on a database of signatures, while the stateless firewall blocks network traffic according to the state of the protocols (e.g. TCP sessions), based on rules predefined by the security administrator.*
B	☐	☐	Non	L'IPS permet de détecter et bloquer des intrusions en se basant sur une base de données de signatures, tandis que le firewall stateless bloque le trafic réseau selon l'état des protocoles (exemple : sessions TCP), basées sur des règles prédéfinies par l'administrateur de sécurité. *The IPS detects and blocks intrusions based on a signature database, while the stateless firewall blocks network traffic according to the state of the protocols (e.g. TCP sessions), based on rules predefined by the security administrator.*
C	☑	☐	Oui (+1)	L'IPS permet de détecter et bloquer des intrusions en se basant sur une base de données de signatures, tandis que le firewall stateless bloque le trafic réseau en se basant sur des règles prédéfinies par l'administrateur de sécurité. *The IPS detects and blocks intrusions based on a signature database, while the stateless firewall blocks network traffic based on rules predefined by the security administrator.*
D	☐	☑	Oui (+1)	L'IPS bloque le trafic réseau selon l'état des protocoles (exemple : sessions TCP), basées sur des règles prédéfinies par l'administrateur de sécurité, tandis que le firewall stateless permet de détecter et bloquer des intrusions en se basant sur une base de données de signatures. *The IPS blocks network traffic according to the state of the protocols (e.g. TCP sessions), based on rules predefined by the security administrator, while the stateless firewall detects and blocks intrusions based on a database of signatures.*
E	☐	☐	Non	L'IPS bloque le trafic réseau en se basant sur des règles prédéfinies par l'administrateur de sécurité, tandis que le firewall stateless permet de détecter et bloquer des intrusions en se basant sur une base de données de signatures. *The IPS blocks network traffic based on rules predefined by the security administrator, while the stateless firewall detects and blocks intrusions based on a database of signatures.*

Question 5 — **Question à réponses multiples**

Une sécurité en profondeur implique : (2 réponses)
In-depth security involves: (2 answers)

Réponses correctes | 0 discordance

	Réponse attendue	Réponse saisie	Réponse discordante	
A	☑	☑	Non	Un cumul de plusieurs lignes de défenses indépendantes *An accumulation of several independent lines of defense*
B	☐	☐	Non	Utilisation d'un serveur Proxy pour protéger les utilisateurs d'éventuelles attaques *Use of a proxy server to protect users from possible attacks*
C	☐	☐	Non	Utilisation de produits Opensource ou la communauté est plus active pour proposer des solutions au cas où le SI a été pénétré. *Use of Opensource products where the community is more active to propose solutions in case the IS has been penetrated.*
D	☑	☑	Non	Prévoir un plan de secours et reprise d'activité en cas de sinistre pour chaque équipement. *Providing a disaster recovery plan for each piece of equipment.*
E	☐	☐	Non	Implémenter une architecture réseau à 2 tiers pour assurer une défense immédiate contre d'éventuelles attaques. *Implementing a 2-tier network architecture to ensure immediate defense against possible attacks.*

Question 6 — **Question à réponse unique**

Dans quel fichier sont sauvegardés les logs d'accès web via le proxy squid ?
In which file are the web access logs saved via the squid proxy?

Réponses correctes

	Réponse attendue	Réponse saisie	Réponse discordante	
A	☑	☑	Non	cat /var/squid/logs/access.log
B	☐	☐	Non	cat /tmp/squid/cache/access.log
C	☐	☐	Non	cat /tmp/squid/logs/access.log
D	☐	☐	Non	cat /usr/squid/cache/access.log
E	☐	☐	Non	cat /etc/squid/cache/access.log

Question 7 — **Question à réponse unique**

Parmi les propositions suivantes, laquelle correspond à la solution de filtrage web à implémenter sur un serveur proxy squid installé sous pfsense ?

Among the following proposals, which one corresponds to the web filtering solution to implement on a squid proxy server installed under pfsense?

Réponses correctes

	Réponse attendue	Réponse saisie	Réponse discordante	
A	☐	☐	Non	SquidFilter
B	☐	☐	Non	PfSenseFilter
C	☐	☐	Non	GuardFilter
D	☑	☑	Non	SquidGuard
E	☐	☐	Non	PfsenseGuard

Question 8 — **Question à réponses multiples**

Parmi les propositions suivantes, lesquelles sont considérées comme avantages d'utilisation d'un serveur proxy au sein d'un système d'information ?

Which of the following are considered advantages of using a proxy server within an information system?

Réponses correctes — 0 discordance

	Réponse attendue	Réponse saisie	Réponse discordante	
A	☐	☐	Non	Un cryptage de bout en bout via un tunnel à travers un réseau non protégé comme le WAN, dans l'optique de sécuriser toute interception de données via une attaque MITM. *End-to-end encryption via a tunnel through an unprotected network such as the WAN, in order to secure any data interception via a MITM attack.*
B	☑	☑	Non	Préserver de la bande passante de la structure en mémorisant les sites favoris souvent consultés par les utilisateurs. *Preserving bandwidth by memorizing the favorite sites often consulted by users.*
C	☑	☑	Non	Cacher l'identité des utilisateurs en utilisant l'adresse IP du serveur proxy sur Internet. *Hiding the identity of users by using the IP address of the proxy server on the Internet.*
D	☐	☐	Non	Possibilité d'un échange sécurisé de clés asymétriques afin de chiffrer les données transitant le réseau WAN. *Possibility of a secure exchange of asymmetric keys to encrypt data passing through the WAN.*
E	☐	☐	Non	Téléchargement, Installation et déploiement automatique des mises à jour système sur toutes les machines de la structure. *Automatic download, installation, and deployment of system updates on all machines in the structure.*

Question 9 — **Question à réponse unique**

Parmi les propositions suivantes, laquelle est considérée aussi comme un service d’annuaire ?

Which of the following is also considered a directory service?

Réponses correctes

	Réponse attendue	Réponse saisie	Réponse discordante	
A	☐	☐	Non	AES
B	☐	☐	Non	DES
C	☑	☑	Non	X.500
D	☐	☐	Non	PKI
E	☐	☐	Non	Caesar

Question 10 — **Question à réponse unique**

Quel est le port utilisé par-default par pfsense pour authentifier des utilisateurs d’un annuaire LDAP ?

What port is used by default by pfsense to authenticate users in an LDAP directory?

Réponses correctes

	Réponse attendue	Réponse saisie	Réponse discordante	
A	☑	☑	Non	389
B	☐	☐	Non	390
C	☐	☐	Non	3128
D	☐	☐	Non	391
E	☐	☐	Non	443