



المدة : أربع ساعات
المعامل : 4

المادة الثانية : احصار في مجال التخصص المطلوب
لتخصص : الأنظمة والشبكات

Exercice 1 :

- Quelles sont les différentes mémoires d'un Routeur et quel est le rôle de chacune ?
- Citez les familles de protocoles du routage dynamique ?
- Donner une brève définition des normes suivantes : IEEE 802.1Q, IEEE 802.1X, IEEE 802.15, IEEE 802.1D, IEEE 802.1P
- Donner la première adresse IP valide, la dernière adresse IP valide et le l'adresse de broadcast des trois premiers sous réseaux de l'adresse IP suivante : 10.0.0.0/20
- A quoi sert le protocole ARP ?
- Que signifie convergence d'un protocole de routage ?
- A quoi sert la notion du « PORT » dans le modèle TCP/IP ?
- Quel est le numéro de port des protocoles suivants : FTP, SSH, Telnet, DNS.
- Définissez en détail l'architecture AAA
- Expliquer le rôle de la distance administrative ?
- Quelle est la distance administrative des protocoles suivants: RIP, EIGRP et OSPF

Exercice 2 :

- Donner une définition de la virtualisation et citez ses avantages.
- Citez trois solutions de virtualisation.
- Définissez les termes suivants : SaaS, PaaS et IaaS.
- Définissez c'est quoi un Cloud Privé, Cloud Public, Cloud Hybride.
- Quel est le nom de l'outil qui permet à une machine physique de faire fonctionner plusieurs machines virtuelles ?

Exercice 3 :

- Définissez 'NAS'.
- Définissez 'SAN'.
- Quelle est la différence entre les deux technologies citées ?
- Sauvegarde, archivage et backup. Quelles sont les principales différences ?
- Définissez et proposer des politiques de sauvegardes et la reprise des données pour une entreprise.
- Définissez les termes suivants : ISCSI, LUN, HBA
- Définissez RAID 0, 1 et 5

Exercice 4 :



المملكة المغربية
وزارة التثقيف
والعربية والعلوم
والتكنولوجيا

مباراة توظيف مهندسي الدولة من الدرجة الأولى
تخصص : مجال الأمن المعلوماتي
بتاريخ 10 فبراير 2019

المعامل: 2

المدة : ساعتان

موضوع عام يحرر وجوبا باللغة العربية.

المادة الأولى

يعتبر اختراق الأنظمة المعلوماتية ظاهرة تهدد أمن وسلامة جميع الدول، مما جعلها

تجند جميع الوسائل المادية والبشرية للحد من تداعياتها .

حلل وناقش.

appartient à un administrateur système (accès RDP aux serveurs d'application et de BD) avec un accès internet pour télécharger les patches nécessaires.

- a. Donner la table de routage du firewall F2 sous la forme suivante : (0.25 point)

Interface de sortie	Réseau destination	Passerelle
...	...	...

- b. Dresser la table de filtrage qui illustre les accès mentionnés précédemment. (0.5 point)

6. La politique de l'entreprise exige que les utilisateurs du site distant doivent se connecter à l'application (10.7.7.10) centralisée dans le réseau central de l'entreprise via une liaison VPN sur le port tcp/8080.

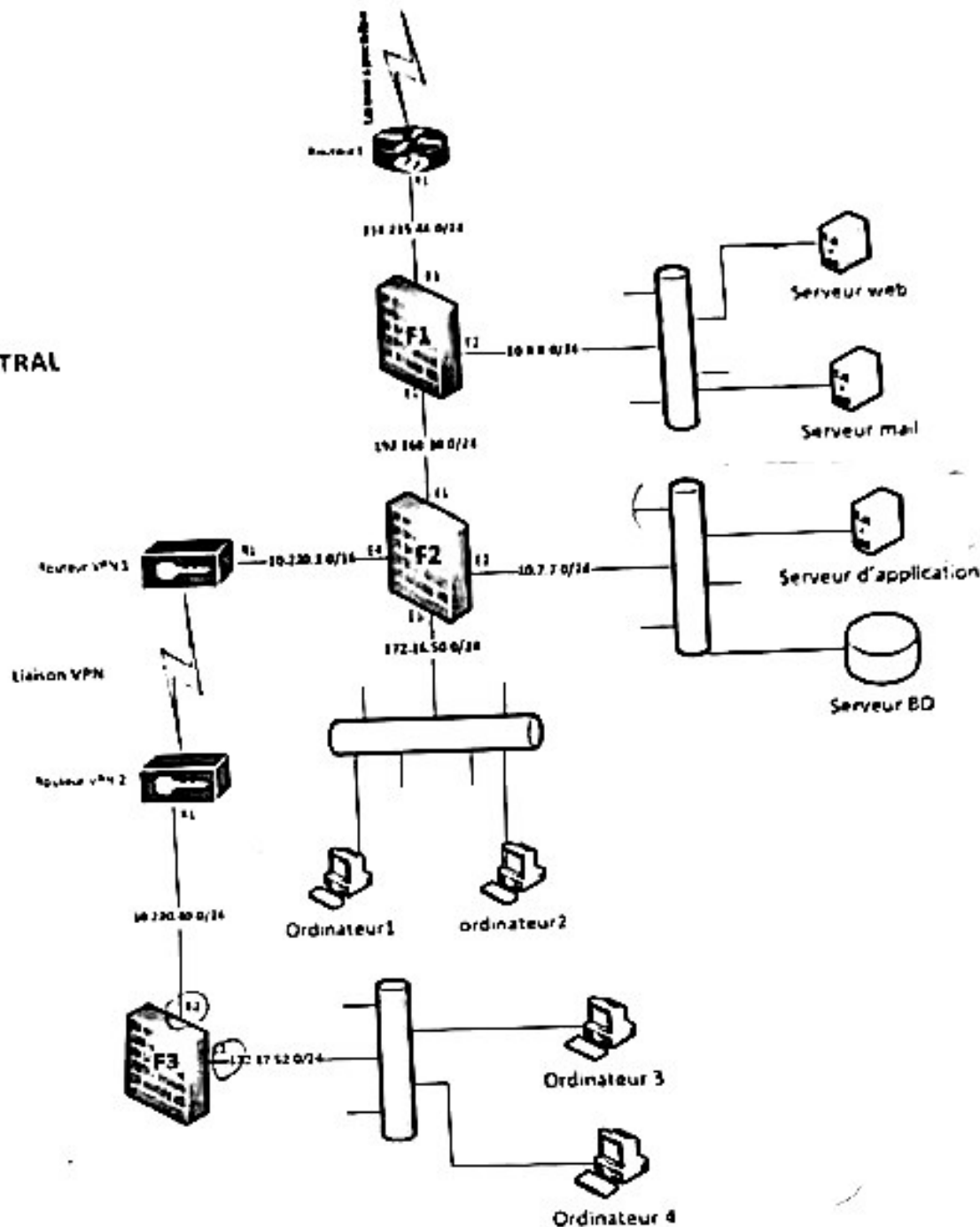
- a. Donner la table de routage du firewall F3. (0.25 point)

- b. Donner les règles qui vérifieront que la politique mentionnée soit applicable. (0.5 point)

7. Le firewall F3 est de type NGFW (Next Generation Firewall). Sur ce firewall l'application SSH est autorisée depuis l'ordinateur 3 vers l'ordinateur 1. Une application malveillante au niveau de l'ordinateur 3 utilise le port 22 pour accéder à l'ordinateur 1. Est-ce que ce trafic sera autorisé ? justifier. (0.75 point)

Annexe 1

SITE CENTRAL



SITE DISTANT

- Un Serveur passerelle SMTP (entrant et sortant).

Exercice N°7 : (5 points)

Une entreprise dispose des pare-feu pour limiter l'accès depuis et vers les machines de son réseau interne. L'architecture du réseau de l'entreprise comprend également un site distant. Le schéma de l'annexe 1 montre les composants de cette architecture. L'annexe 2 contient le plan d'adressage.

- Les règles de filtrage sont traitées en entrée.
- Les règles sont examinées dans l'ordre croissant à partir de la règle numéro 1.
- La première règle dont les paramètres correspondent exactement au paquet reçu est appliquée, sinon le firewall passe à la règle suivante.

Extrait table de filtrage du firewall frontal F2 :

N°	Interface entrée	@IP sce	@IP dest	protocole	Action
1	214.215.44.1	any	10.8.8.10	http	autorisé
2	214.215.44.1	any	10.8.8.100	Pop3, SMTP	autorisé
3	172.16.50.1	172.16.50.10	10.8.8.10	RDP	autorisé
4	172.16.50.1	172.16.50.10	10.8.8.100	RDP	autorisé
5	172.16.50.1	172.16.50.20	any	http,https,dns	autorisé
....					
10	172.16.50.1	any	any	ip	bloqué
11	214.215.44.1	any	any	ip	bloqué
12	10.8.8.1	any	any	ip	bloqué

1. Donner la politique correspondante à chaque règle (1,2 et 5). (0.75 point)
2. Préciser la règle qui vérifiera chacun des paquets suivants et dites si le paquet sera accepté ou refusé. (1 point)

Paquet 1 : 212.217.52.103 → 10.8.8.100 port tcp/995

Paquet 2 : 172.16.50.20 → www.entreprise.ma, port tcp/53

Paquet 3 : 172.16.50.20 → 10.8.8.10 port tcp/80

Paquet 4 : 212.217.52.103 → 10.8.8.100 port udp/53

3. Le firewall F1 applique le NAT sur les deux adresses privées 10.8.8.10 et 10.8.8.100. Définir l'utilité et les types du NAT. (0.5 point)
4. Proposer une solution pour renforcer la sécurité des applications web de l'entreprise. (0.5 point)
5. L'ordinateur 1 appartient à un administrateur de base de données (il dispose d'un accès SQL

Exercice N°4 : (3 points)

1- Compléter le tableau suivant par : AES, DES, RSA, ECC

Algorithme de Chiffrement symétrique	Algorithme de Chiffrement asymétrique

- 2- Dans la cryptographie asymétrique chaque entité possède une paire de clés (public et privé).
- Expliquez la différence entre ces deux clés ?
 - Quelle clé à utiliser pour chiffrer un message destiné à une entité X ? Qui peut lire ce message ?
 - Quelle clé à utiliser pour signer un message destiné à l'entité X ? Qui peut vérifier la signature du message ?

Exercice N°5 : (2,5 points)

- 1- Donner les noms des techniques d'attaque de déni de service (DoS : Denial of Service) dans : (0.75 points)
- un réseau local Ethernet.
 - un réseau sans fil.
 - un serveur web.
- 2- Les employés d'une entreprise, après avoir ouvert leur session et effectuer quelques tâches quotidiennes (lecture du courrier, navigation web, etc), de nombreux employés ont remonté au SOC un incident. Il s'agit d'un message apparaissant sur leurs écrans d'ordinateur indiquant que les fichiers de l'utilisateur sont cryptés. Une demande de rançon est exigée pour restauration. (0.5 points)
- Quel est le type du malware à priori ?
 - Quelle est la procédure à suivre suite à la déclaration de l'incident ?
- 3- Décrire l'attaque de web spoofing. (0.5 points)
- 4- Quels sont les étapes d'une cyberattaque ? (0.75 point)

Exercice N°6 : (2.5 points)

Vous devez établir l'architecture du réseau d'une petite entreprise. Proposer une architecture réseau sécurisée en justifiant l'emplacement des éléments ci-dessous. A cet effet, vous pourrez ajouter les éléments réseaux nécessaires (Firewall, DMZ, ...) et créer autant de réseau que cela vous semble nécessaire.

- Un serveur web public qui utilise une base de données, sachant que les employés de l'entreprise travaillent sur la base de données. Où doit-on placer la base de données et le serveur web dans notre réseau ?
- Un serveur DNS qui est utilisé par une grande proportion d'applications et de service
- Un serveur mandataire HTTP (proxyl).



سارة توفيق محمدي المولة من الدرجة الأولى
تخصص : مجال الأمن المعلوماتي
بتاريخ 10 فبراير 2019

المدة: 4 ساعات	المعامل: 4
المادة الثانية	اختبار يتعلق بالتخصص المطلوب أو بالمهام أو بالوظائف المطلوب شغلها.

Exercice N°1 : (2points)

Définir les concepts suivants :

- Analyse comportemental
- WAF ✓
- SOC ✓
- Cross-site Scripting
- Zero-day attaque
- Ping of Death
- OWASP ✓
- Non repudiation

Exercice N°2 : (3 points)

- 1- En quoi consiste le principe de cloisonnement dans la sécurité de réseaux informatiques ? (0.25 point)
- 2- Quelle est la différence entre VPN IPSEC et VPN SSL ? (0.5 point)
- 3- Citez 3 mécanismes pour assurer la haute disponibilité. (0.75 point)
- 4- Citez 3 avantages de l'utilisation des VLANs. (0.75 point)
- 5- Quel avantage et quel inconvénient pourrait-il avoir le fait de disposer de 2 types de technologies de firewall différentes au lieu de deux technologies similaires ? (0.5 point)
- 6- Quelle(s) technique(s) utilise un antivirus pour détecter les programmes malveillants ? (0.25 point)

Exercice N°3 : (2 points)

- 1- Que signifie un audit de sécurité du système d'information ? (0.25 point)
- 2- Comment assurer la sécurité physique d'un Datacenter ? (0.25 point)
- 3- Définir la norme ISO 27001. (0.75 point)

54) À quoi sert un snapshot dans un environnement de virtualisation ?

1. À restaurer rapidement une machine virtuelle à un état antérieur en cas de besoin
2. À capturer l'état actuel d'une machine virtuelle pour en faire une image figée
3. À augmenter les performances des machines virtuelles en réduisant la fragmentation du stockage
4. Toutes les réponses sont fausses

55) Dans la couche 2 du modèle OSI, comment s'appelle la sous couche de la moitié supérieure ?

1. Couche MAC
2. Couche LLC
3. Couche IP
4. Toutes les réponses sont fausses

56) Overclocking est une technique :

1. De synchronisation
2. D'accélération
3. De ralentissement
4. Toutes les réponses sont fausses

57) Quelle est la différence entre un IPS et un IDS ?

1. L'action prise lorsqu'un incident potentiel a été détecté
2. Les IPS ne sont pas conçus pour bloquer les attaques par contre les IDS oui
3. Les deux offrent une prévention proactive contre certaines des failles de sécurité réseau les plus connues
4. Toutes les réponses sont fausses

58) Quelle couche du modèle OSI est responsable de la transmission sans erreur des données sur le réseau ?

1. Couche physique
2. Couche liaison de données
3. Couche réseau
4. Toutes les réponses sont fausses

59) Quel type d'adresse est utilisé pour identifier un périphérique sur un réseau local ?

1. Adresse IP
2. Adresse MAC
3. Adresse DNS
4. Toutes les réponses sont fausses

60) Quelle est la fonction du protocole TCP/IP dans un réseau informatique ?

1. Assurer la transmission fiable des données
2. Déterminer le chemin optimal pour les paquets de données
3. Contrôler l'accès au réseau en utilisant des adresses MAC
4. Toutes les réponses sont fausses

Wadifa Info

www.wadifa-info.com

Le sujet suivant à préparer

النموذج التالي للتحضير

نموذج مباراة ولوج مهنة المفوضين القضائيين - قانون المسطرة المدنية 2023

Modèle : Concours d'accès à la profession d'huissier de justice
– Procédure civile 2023

www.wadifa-info.com/fr/modele-concours/959

Chaîne WhatsApp

قناة واتساب

المباريات الجديدة والنتائج كل يوم

Nouveaux concours et résultats chaque jour

www.wadifa-info.com/wa

Le site

الموقع

كل المباريات المفتوحة والنماذج مع التصحيح، مجاناً

Tous les concours ouverts et les sujets corrigés, gratuits

www.wadifa-info.com