NOM : PRENOM :

# DS – Réseaux 4

## IUT Département Informatique – Semestre 4

## Les documents et calculatrices sont interdits.

## Durée : 1h30

## 1ère partie : QCM

**Question 1 :** DNS. Donnez parmi les assertions suivantes, la bonne réponse. Un client demande la résolution DNS de tata.titi.domaine.com. Nous considérons une résolution itérative.

☐ Le client sollicite son DNS local qui lui renvoi l'adresse IP du DNS root. Le client sollicite le DNS root qui lui renvoi l'adresse du DNS responsable du domaine « .fr ». Le client sollicite le DNS « .fr » qui lui renvoi l'adresse du DNS responsable du domaine « domaine.fr ». Le client sollicite le DNS « domaine.fr » qui lui renvoi l'adresse du DNS responsable du domaine « titi.domaine.fr ». Le client sollicite le DNS « titi.domaine.fr » qui lui renvoi l'adresse de la machine « tata.titi.domaine.fr ».

☐ Le client sollicite son DNS local. Le DNS local sollicite le DNS root qui lui renvoi l'adresse du DNS responsable du domaine « .fr ». Le DNS local sollicite le DNS « .fr » qui lui renvoi l'adresse du DNS responsable du domaine « domaine.fr ». Le DNS local sollicite le DNS « domaine.fr » qui lui renvoi l'adresse du DNS responsable du domaine « titi.domaine.fr ». Le DNS local sollicite le DNS « titi.domaine.fr » qui lui renvoi l'adresse de la machine « tata.titi.domaine.fr ». Le DNS local renvoi cette adresse au client.

☐ Le client sollicite son DNS local. Le DNS local sollicite le DNS root. Le DNS root sollicite le DNS « .fr ». Le DNS « .fr » sollicite le DNS « domaine.fr ». Le DNS « domaine.fr » sollicite le DNS « titi.domaine.fr » Le DNS « titi.domaine.fr » renvoi l'adresse de la machine « tata.titi.domaine.fr » au DNS local qui la renvoi au client.

☐ Le client sollicite son DNS local. Le DNS local sollicite le DNS root. Le DNS root sollicite le DNS « .fr ». Le DNS « .fr » sollicite le DNS « domaine.fr ». Le DNS « domaine.fr » sollicite le DNS « titi.domaine.fr ». Le DNS « titi.domaine.fr » renvoi l'adresse de la machine « tata.titi.domaine.fr » au DNS local qui la renvoie au client.

☐ Le client sollicite le DNS root. Le DNS root sollicite le DNS « .fr ». Le DNS « .fr » sollicite le DNS « domaine.fr ». Le DNS « domaine.fr » sollicite le DNS « titi.domaine.fr ». Le DNS « titi.domaine.fr » renvoi l'adresse de la machine « tata.titi.domaine.fr » au client.

| NOM : | PRENOM : |
|---|---|

**Question 2 :** DNS. Quelles sont les informations **minimales** que doit avoir un DNS local responsable du domaine « moduleS4.fr »

☐ Il doit avoir : a) le fichier root qui contient les adresses IP de tous les serveurs DNS root b) les noms et adresses IP des machines de son domaine c) les adresses IP des DNS responsables des sous domaines d) l'adresse IP du serveur DNS responsable de « .fr ».

☐ Il doit avoir : a) les noms et adresses IP des machines de son domaine b) les adresses IP des DNS responsables des sous domaines c) l'adresse IP du serveur DNS responsable de « .fr ».

☐ Il doit avoir : a) le fichier root qui contient les adresses IP de tous les serveurs DNS root b) les noms et adresses IP des machines de son domaine c) l'adresse IP du serveur DNS responsable de « .fr ».

☐ Il doit avoir : a) le fichier root qui contient les adresses IP de tous les serveurs DNS root b) les noms et adresses IP des machines de son domaine c) les adresses IP des DNS responsables des sous domaines.

**Question 3 :** DNS - Une assertion ci-dessous est fausse. Retrouvez là.

☐ Un nom de machine ne peut pas avoir plusieurs adresses IP dans la base DNS (même domaine, même serveur DNS)

☐ Une même adresse IP peut correspondre à plusieurs noms (même domaine, même serveur DNS)

☐ Un même nom de machine peut avoir à la fois une adresse IPv4 et IPv6 (même domaine, même serveur DNS)

☐ Un même nom de machine (toto par exemple) peut appartenir à plusieurs domaine (univ-lyon1.fr et univ-lumiere.fr par exemples).

**Question 4 : SNMP - Trouvez la bonne réponse.**

☐ SNMP permet de récupérer des informations sur les matériels ou logiciel. Il permet la supervision de ces équipements mais pas leur configuration.

☐ SNMP est un protocole de supervision. Il permet de récupérer des informations sur les matériels et les logiciels. Il permet la supervision de ces équipements mais aussi leur configuration.

☐ SNMP est un protocole de supervision. Il permet de récupérer des informations sur les matériels et les logiciels. L'équipement ou le logiciel est sollicité par le client SNMP mais celui-ci ne peut pas envoyer d'information spontanément (sans que celle-ci ait été sollicité).

☐ SNMP permet de récupérer des informations sur les matériels et les logiciels. C'est un protocole de supervision. Il fonctionne exclusivement au travers d'un système de trappes où les équipements envoient des informations au serveur SNMP.

| NOM : | PRENOM : |
|---|---|

**Question 5 : SNMP.** Qu'est-ce que la MIB ?

☐ La MIB est un ensemble d'arbre décrivant les informations sur les équipements et systèmes. Chaque MIB est identifié par son OID. Elles sont récupérables et modifiables via le protocole SNMP.

☐ La MIB est un ensemble d'arbre où chaque nœud est identifié par son OID. L'OID est une suite de nombre séparé par des points. Le protocole SNMP se sert ensuite du nom qualifié de chaque nœud pour accéder au nœud en lecture ou parfois en écriture.

☐ La MIB est un arbre décrivant l'ensemble des équipements ou systèmes supervisés. Un équipement physique est alors l'un des nœuds dans l'arbre. Le protocole SNMP indique alors l'OID à un des nœuds pour récupérer une information de ce nœud.

☐ La MIB est un arbre unique décrivant l'ensemble des équipements ou systèmes supervisés. Un équipement est alors identifié par son OID qui est une suite de nombre séparée par des points ou son nom qualifié. Le protocole SNMP permet d'interroger ses équipements ou systèmes.

☐ La MIB est un arbre unique décrivant les informations disponibles sur les équipements et systèmes. Elles sont récupérables, et parfois modifiables via le protocole SNMP.

**Question 6 :** Authentification avec une clé symétrique. Indiquez laquelle de ces authentifications fonctionne (laquelle est la plus fiable). A souhaite s'authentifier auprès de B.

☐ B envoi un challenge à A. A hache le challenge et la clé symétrique séparément. A envoi ces deux résultats à B. B effectue ces deux hachages localement et compare avec ceux reçus. Si les deux résultats envoyés correspondent aux deux résultats locaux alors A est authentifié.

☐ A envoi sa clé symétrique à B. B compare celle reçue avec celle conservé en local. Si cela correspond A est authentifié.

☐ A envoi le hachage de sa clé symétrique à B. B hache la clé de A conservée en local. Si les deux correspondent A est authentifié.

☐ B envoi un challenge à A. A hache le challenge concaténé avec la clé symétrique. A envoi le résultat à B. B effectue le même hachage localement et compare avec celui reçu. Si les deux correspondent alors A est authentifié.

☐ A envoi un challenge à B. B hache le challenge concaténé avec la clé symétrique. B envoi le résultat à A. A effectue le même hachage localement et compare avec celui reçu. Si les deux correspondent alors A est authentifié.

☐ B envoi le hachage de sa clé symétrique à A. A hache la clé de B conservé en local. Si les deux correspondent A est authentifié.

| NOM : | PRENOM : |
|---|---|

**Question 7 :** Authentification avec des clés asymétriques. A doit s'authentifier auprès de B.

☐ B envoi un challenge à A. A le chiffre avec sa clé publique et l'envoi à B. B le déchiffre avec la clé privée de A. Si ce dernier correspond au challenge envoyé alors A est authentifié.

☐ A envoi un challenge à B. B le chiffre avec sa clé publique et l'envoi à A. A le déchiffre avec la clé privée de B. Si ce dernier correspond au challenge envoyé alors A est authentifié.

☐ B envoi un challenge à A. A le chiffre avec sa clé privée et l'envoi à B. B le déchiffre avec la clé publique de A. Si ce dernier correspond au challenge envoyé alors A est authentifié.

☐ A envoi un challenge à B. B le chiffre avec sa clé privée et l'envoi à A. A le déchiffre avec la clé publique de B. Si ce dernier correspond au challenge envoyé alors A est authentifié.

**Question 8 :** certificat. Dans les propositions ci-dessous, A est le client ou serveur correspondant au certificat. Autrement dit, nous parlons du certificat de A.

☐ Le certificat est composé (entre autres) du nom de A, d'une date d'expiration, d'un numéro de série, de la clé publique de A, d'une signature authentifiant le certificat.

☐ Le certificat est composé (entre autres) du nom de A, d'une date d'expiration, d'un numéro de série, de la clé privée de A, d'une signature authentifiant le certificat.

☐ Le certificat est composé (entre autres) d'une date d'expiration, d'un numéro de série, de la clé privée de A, d'une signature authentifiant le certificat.

☐ Le certificat est composé (entre autres) du nom de A, d'une date d'expiration, d'un numéro de série, de la clé publique et privée de A (mais cette dernière est chiffrée), d'une signature authentifiant le certificat.

**Question 9 :** certificat. Nous parlons ci-dessous de la signature se trouvant sur un certificat. Nous parlons du certificat de A. C est l'autorité de certification.

☐ La signature est le résultat du hachage du certificat chiffré avec la clé publique de A puis avec celle de C.

☐ La signature est le résultat du hachage du certificat chiffré avec la clé publique de C puis avec celle de A.

☐ La signature est le résultat du hachage du certificat chiffré avec la clé publique de C.

☐ La signature est le résultat du hachage du certificat chiffré avec la clé privée de C.

☐ La signature est le résultat du hachage du certificat chiffré avec la clé publique de A.

☐ La signature est le résultat du hachage du certificat chiffré avec la clé privée de A.

| NOM : | PRENOM : |
|---|---|

☐ La signature est le résultat du hachage du certificat chiffré avec la clé privée de C puis avec la clé publique de A.

☐ La signature est le résultat du hachage du certificat chiffré avec la clé privée de A puis avec la clé publique de C.

**Question 10 :**

☐ Le chiffrement symétrique est plus lourd que le chiffrement asymétrique. L'échange de clés est plus facile avec le système asymétrique qu'avec le système symétrique.

☐ Le chiffrement asymétrique est plus lourd que le chiffrement symétrique. L'échange de clés est plus facile avec le système asymétrique qu'avec le système symétrique.

☐ Le chiffrement asymétrique est plus lourd que le chiffrement symétrique. L'échange de clés est plus facile avec le système symétrique qu'avec le système asymétrique.

☐ Le chiffrement symétrique est plus lourd que le chiffrement asymétrique. L'échange de clés est plus facile avec le système symétrique qu'avec le système asymétrique.

**Question 11 :** https

Un client A se connecte sur un serveur web W. Donnez parmi les réponses ci-dessous la réponse décrivant les échanges https.

☐ A envoie son certificat à W en clair. W vérifie l'intégrité du certificat grâce à la signature de celui-ci. W envoie un challenge à A. A le chiffre avec sa clé privée et le renvoi à W. Si W peut le déchiffrer avec la clé publique de A alors le serveur est authentifié. W envoie une clé de session chiffrée avec la publique de A. A la déchiffre avec sa clé privée. Le reste des échanges est chiffré avec la clé de session (clé symétrique).

☐ W envoie un challenge à A. A le chiffre avec sa clé publique. W le déchiffre avec sa clé privée (celle de W provenant de son certificat). A renvoie le challenge en clair à A. Si le challenge est bon, A envoie une clé de session à W chiffrée avec sa clé publique. W le déchiffre avec la clé privée correspondante. Le reste des échanges est chiffré avec la clé de session (clé symétrique).

☐ W envoie son certificat à A. Le certificat est chiffré avec la clé publique de W. A le déchiffre avec sa propre clé privée. A envoie une clé de session chiffrée avec la publique de W se trouvant dans le certificat. W la déchiffre avec sa clé privée. Le reste des échanges est chiffré avec la clé de session (clé symétrique).

☐ W envoie son certificat à A en clair. A vérifie l'intégrité du certificat grâce à la signature de celui-ci. A envoie un challenge à W. W le chiffre avec sa clé privée et le renvoi à A. Si A peut le déchiffrer avec la clé publique de W alors le serveur est authentifié. A envoie une clé de session chiffrée avec la publique de W. W la déchiffre avec sa clé privée. Le reste des échanges est chiffré avec la clé de session (clé symétrique).

| NOM : | PRENOM : |
|---|---|

☐ A envoie son certificat contenant sa clé privée. W vérifie l'intégrité du certificat grâce à la signature de celui-ci. W chiffre un challenge avec la clé privée du certificat (celui de A) puis l'envoi à A. A le déchiffre avec sa clé publique et envoie le résultat à W. Si W constate que cela correspond bien au challenge qu'il a envoyé alors il envoie une clé de session chiffré avec la clé privée de A. A la déchiffrera avec sa clé publique. Le reste des échanges est chiffré avec la clé de session (clé symétrique).

**Question 12 :** chiffrement rsa

Nous considérons la clé publique de A =(e ,n)=(3,33). Nous considérons la clé privée de A=(d,n)=(7,33). B souhaite chiffrer le message « 2 » pour l'envoyer à A en toute sécurité. Quel sera le message chiffré ? La première question que vous devez vous poser est : dois-je chiffrer avec la clé privée ou publique ?

☐ 9 ☐ 27 ☐ 8 ☐ 7 ☐ 29 ☐ 6 ☐ 21 ☐ 11 ☐ 13

## Exercice firewall

Vous devez donner les commandes cisco pour la mise en œuvre des politiques A et B ci-dessous. Le routeur a deux interfaces FastE 0/0 donnant sur le réseau publique et FastE 0/1 donnant sur le réseau de l'entreprise. Vous êtes par défaut en mode conf-t.

Politique A :

Tout doit être accepté sauf :

- TCP sur le port 81 (source ou destination)
- Le trafic Ip sortant vers le réseau public avec l'adresse 10.1.0.1 comme adresse source

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

| NOM : | PRENOM : |
|---|---|

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Politique B :

Rien ne doit être accepté sauf :

- Le trafic web (port 80) avec des serveurs web extérieurs (il n'y a pas de serveur web sur le réseau d'entreprise). La plage d'adresse du réseau interne est 10.1.0.0/24.
- Le trafic DNS (port 53/UDP). Il n'y a pas de serveur DNS dans l'entreprise.

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

| NOM : | PRENOM : |
|---|---|

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

Router-conf>

# Annexe :

number prenant des valeurs dans [1-99]: *standard ACL*

**access-list** number **remark** name

**access-list** number **permit|deny** source source_wildcard dest dest_wildcard

**ip access-group** number **in|out** //en mode interface

number prenant des valeurs dans [100-199 | 2000-2699]: *Extended ACL*

**access-list** number **remark** name

**access-list** number **permit|deny** proto src src_wildcard dest dest_wildcard [**tos** tos]

**access-list** number **permit|deny** icmp src src_wildcard dest dest_wildcard

**[**icmp-type **[**icmp-code**] |**icmp-message**]** [**tos** tos]

**access-list** number **permit|deny tcp** src src-wildcard **[operator [**port**]]** dest dest-wildcard

**[operator [**port**]] [established | syn] [tos** tos**]**

**access-list** number **permit|deny udp** src src-wildcard **[operator [**port**]]** dest dest-wildcard

**[operator [**port**]] [tos** tos**]**

**operator =** eq ; lt ; gt ; neq ; range