Sécurité des réseaux Informatique

Questionnent des cours

1- Qu’est-ce que la sécurité ?

La sécurité sur un réseau consiste à s'assurer que celui qui modifie ou consulte des données du système en a l'autorisation et qu'il peut le faire correctement car le service est disponible.

2- Quels sont les principaux objectifs de la sécurité informatique ?

L'intégrité, La confidentialité, La disponibilité, La non répudiation, L'authentification

3- Quelle est la différence entre l’approche réactive et proactive dans la gestion des risques ?

•L’approche proactive efficace permette de diminuer considérablement les risques d'incidents de sécurité.
•L’approche réactive puisse s'avérer efficace pour résoudre des incidents de sécurité liés à l'exploitation de risques de sécurité**.**

4- Quels sont les types de pirates ?

•Les « white hat hackers »
•Les « black hat hackers »
•Les « script kiddies »
•Les « phreakers »
•Les « carders »
•Les « crackers **»**

5- Quels sont les types d’attaques ?

•Attaque direct
•Attaque par rebond
•Attaque indirecte par réponse

MED ZAKI

6- Donner quelques outils de détection des vulnérabilités réseaux ?

•MBSA
•GFA LANguard
•Nessus

7- Donnez quelques outils pour sécuriser notre système informatique ?

•Antivirus
•Pare Feu
•Proxy
•Anti-malwares
•DMZ

8- Pourquoi les systèmes sont-ils vulnérables ?

La sécurité est devenue un point crucial des systèmes d'informations. Cependant, les organisations sont peu ou pas protégées contre les attaques sur leur réseau ou les hôtes du réseau.

9- Qu'est-ce qu'un agent mobile ?

Un agent mobile est un programme autonome qui peut se déplacer de son propre chef, de machine en machine sur un réseau hétérogène dans le but de détecter et combattre les intrusions.

10- Quelle est la différence entre DES et RSA ?

•DES utilise des clés d'une taille de 56 bits ce qui la rend de nos jours faciles à casser avec les nouvelles technologies de cryptanalyse.
•RSA d'utiliser des clés de longueur variable de 40 à 2 048 bits.

11- Donnez l’équation qui caractérise le terme risque ?

Risque = (Menace * Vulnérabilité) /contre-mesure

12- Quel est le but du chiffrement ?

L’authenticité

MED ZAKI

13- Citer les principaux dispositifs permettant de sécuriser un réseau contre les intrusions ?

Agent Mobile, Proxy, Firewall.

14- Qu'est-ce que l’hameçonnage (phishing) ?

Le piratage de lignes téléphoniques Un procédé frauduleux permettant de collecter des informations personnelles**.**

15- En matière de sécurité informatique, Que désigne-t-on par cheval de Troie ?

Un logiciel malveillant ayant l'apparence d'un logiciel inoffensif mais qui comporte des instructions nuisibles qui s'exécutent une fois le logiciel installé

16- Comment appelle-t-on un programme qui s'installe discrètement sur l'ordinateur, collecte et envoie des informations personnelles à des organisations tierces ?

Espiogiciel

17- Quelles sont les méthodes d'authentification ?

•Authentification par mot de passe
•Authentification GSSAPI
•Authentification SSPI
•Authentification Kerberos
•Authentification DES
•Authentification RSA
•Authentification LDAP

18-Donner les trois catégories de sécurité réseaux :

La sécurité physique
La sécurité logique
La sécurité administrative

19- Les différents types d'attaques réseau

- Les attaques de reconnaissance (Un balayage de «Ping » ; Le balayage de port ; Un capture de paquets (Sniffing)
- Les attaques de mot de passe (L'attaque par une liste de mot ; L'attaque par force brute)
- Les attaques d'accès (Le Phishing - Le Pharming - L'attaque de « Man-in-the-middle » : spoofing et hijacking - Les attaques mélangées)
- Les attaques de réseau contre la disponibilité (les dénis de service par saturation-les dénis de service par exploitation de vulnérabilités-L 'attaque SYN flood-L 'attaque ICMP flood)
- Les attaques rapprochées
- Les attaques de relation d'approbation

20- Les types de trafic réseau

- Le plan de gestion
- Le plan de contrôle
- Le plan de données

21- le rôle de NTP

Le protocole NTP (Network Time Protocol ou NTP) permet de synchroniser l'horloge locale d'un élément réseau informatique avec celle d'un serveur de référence (un serveur de temps public sur Internet ou avec une source de temps interne)

22- le rôle de protocole SNMP :

Le protocole SNMP (Simple Network Management Protocol) permet de superviser,
Diagnostiquer et gérer, les équipements réseau à distance.

23- le rôle du protocole AAA :

Le Protocole AAA est une stratégie de sécurité implémenté dans certains routeurs Cisco qui réalise trois fonctions : l'authentification, l'autorisation, et la traçabilité

24- Les types de pare-feu :

- Pare-feu NAT
- Pare-feu de filtrage de paquets
- Pare-feu de filtrage de paquet avec état
- Pare-feu applicatif (pare-feu proxy)

25- Les types d'attaques sur la couche 2 :

- Les attaques d'inondation d'adresse MAC
- L'attaque par usurpation d'adresse MAC (ARPspoofing)

- L’attaque DHCP Starvation
- L’attaque par saut de VLAN
- Les attaques à base du protocole STP

26- Les algorithmes de chiffrements symétrique :

- DES
- 3DES
- AES
- IDEA
- RC2, RC4, RC5, RC6
- Blowfish

27- Les algorithmes de chiffrements symétrique :

- RSA
- Diffie-Hellman
- DSA

28- Les types de hachage les plus utilisés

- MD5 : permet de créer des empreintes numériques de taille 128-bit.
- SHA-1 : permet de créer des empreintes numériques de taille160-bit.
- SHA-2 : permet de créer des empreintes numériques de taille entre 224 bits et 512 bits.

Terminologie

- **Ressource** : tout objet ayant une valeur pour une organisation et qui doit être
  Protégée.
- **Une vulnérabilité :** C’est une faiblesse d'un système qui pourrait être exploitée par une Menace.
- **Une menace :** Un danger potentiel pour une ressource ou pour la fonctionnalité du

Réseau.

- **Une attaque** : C’est une action prise par un attaquant pour nuire à une ressource.
- **Un risque :** c’est la possibilité de la perte, l’altération, la destruction ou autres
  Conséquences négatives de la ressource d'une organisation. Le risque peut naître
  D’une seule ou plusieurs menaces ou de l'exploitation d’une vulnérabilité.
  Risque = Une Ressource + Menace + Vulnérabilité
- **Une contre-mesure :** Une protection qui atténue une menace potentielle ou un risque
- **Virus :** c’est un programme qui s'attache à un logiciel pour exécuter une fonction spécifique non souhaitée sur un ordinateur.
- **Worms :** ce sont des programmes autonomes qui exploitent des vulnérabilités connues Dans le but de ralentir un réseau. Ils ne nécessitent pas l'activation de l'utilisateur et ils se dupliquent et tente d'infecter d'autres hôtes dans le réseau
- **Spyware** : ce sont des logiciels espions qui sont généralement utilisés dans le but
  D’influencer l’utilisateur pour acheter certaine produits ou services. Les spywares, en Générale, ne se propagent pas automatiquement, mais ils s’installent sans autorisation.
- **Adware :** se réfère à tout logiciel qui affiche des publicités, sans l’autorisation de
  L’utilisateur parfois sous la forme de publicités pop-up.
- **Scaryware** se réfère à une classe de logiciels utilisés pour de convaincre les
  Utilisateurs que leurs systèmes sont infectés par des virus et leur proposer une solution Dans le but de vendre des logiciels.
- **Un système de détection d'intrusion IDS** (Intrusion Détection System) est un
  Capteur capable d’analyser les paquets circulant sur un ou plusieurs lien(s) réseau dans le but de détecter les activités suspectes.
- **Un système de prévention d’intrusion IPS** (Intrusion Prevention System) est un capteur capable de détecter et d’empêcher toutes les attaques potentielles sur un hôte Ou sur le réseau.
- **Cryptanalyse** : désigne l’ensemble des techniques et méthodes utilisées pour tenter de retrouver le texte en clair à partir du texte crypté.
- **La substitution poly-alphabétique** : consiste à remplacer un caractère par une autre choisie d’une façon dynamique, déterminé par la clé de cryptage, et non plus d’une manière fixe.

- **Chiffrement symétrique :** Dans le chiffrement symétrique, la même clé est utilisée pour le chiffrement et le déchiffrement d'où l'obligation que celle-ci reste confidentielle.
- **Le chiffrement asymétrique** (ou chiffrement à clés publiques), une clé différente est utilisée à la fois pour chiffrer et déchiffrer les données, et il est impossible de générer une clé à partir de l'autre.

Commandes

La sécurisation des mots de passe

Router(config)# **service password-encryption**	Cryptez tous les mots de passe
Router(config)# **security passwords min-length** *length*	Appliquer une longueur minimale pour tous les nouveaux mots de passe. La longueur peut être de 1 à 16.
Router(config)# ***enable algorithm-type {md5|scrypt|sha256|}secret*** *password*	Crypter le mot de passe du mode privilégié à l'aide de message de l'algorithme MD5

L'implémentation des restrictions de connexion

Login block-for X **attempts** Y **within** Z	Cette commande permet de bloquer l'accès Pendant « X » secondes après « Y » essaie d'accès dans 'z' secondes
Login delay second	Configurer un délai entre les tentatives successives de connexion.

La sécurisation de l'accès par les lignes console, VTY et auxiliaire

Router(config)# **username** *name* **privilege** *level* **secret** *password*	Créer une base de données d'utilisateurs locaux et crypter leurs mots de passe.
Router(config)#**line vty 0 4** Router(config-line) # **login local** Router(config-line) #**exec-timeout** *minutes seconds*	Réglez l'intervalle d'inactivité à une valeur. La valeur par défaut est 10 minutes.
Router(config-line)# **line aux 0**	Accéder au mode « line auxiliaire ».
Router(config-line)# **no exec**	Désactiver le port auxiliaire.
Router(config)# **ip ssh version [1|2]**	Il est recommandé d'utiliser la version 2
Router(config)# **ip ssh time-out** *seconds*	Définir le nombre de secondes à attendre pour que le client SSH réponde pendant la phase de négociation. La valeur par défaut est 120 secondes.
Router(config)# **ip ssh authentication-retries** *Integer*	Limitez le nombre de tentatives de connexion. La valeur par défaut est 3.

Router(config)# **login block-for** *seconds* **Attempts** *tries* **within** *Seconds*	Sécuriser la connexion vty.
Router(config-line) # **transport input ssh**	Autoriser uniquement les sessions SSH.
Router(config-line) # **access-class** *ACL-number*	Appliquez une ACL pour contrôler l'accès à la ligne vty.

Configurer un niveau de privilège

Router(config)# **privilege** *mode* {**level** *level command* **| reset** *command}*	Autoriser l'utilisation d'une commande à un Niveau de privilège personnalisé.
Router(config)# **enable secret level** *level password*	Permettre d'assignez un mot de passe au niveau de privilège personnalisé.
R1# **show privilege**	La Vérification du niveau de privilège
Router>**enable *level***	Accéder au niveau de privilège personnalisé.
R1(config)# **line console 0**	Accéder au port console (ou auxiliaire)
R1(config-line)#**privilege level 4**	Définir un niveau de privilège pour utiliser ce mode.

Sécuriser l'accès à l'aide de la gestion de « vues »

R1(config)# **parser view** SHOWVIEW	Créer une vue nommée« ShowView »
R1(config-view) # **secret** cisco123	Assignez une mot de passe à la vue.
R1(config-view)# **commands exec include show**	Cette vue peut utiliser tous les commandes du mode EXEC privilégié
.R1(config-view)# **commands exec include ping**	Cette vue peut utiliser la commande « ping » du mode EXEC privilégié.
R1# **enable view** SHOWVIEW	Se connecter à la vue ShowView pour la vérifier.
Router(config)# **parser view** *viewname* **Superview**	Créer une Super-vue en mode de configuration
Router(config-view) # **secret** *password*	Assigner un mot de passe à la Super-vue.
Router(config-view)# **view** *view-name*	Affecter une vue existante à la SuperView. Des vues multiples peuvent être assignées à une SuperView
Router# **enable view** *view-name*	Se connecter à la Super-vue pour la vérifier
R1#**show parser view all**	Afficher la liste des vues

Configuration du protocole NTP

Router(config)# **ntp master** *stratum*	Configurez le routeur pour qu'il soit le maitre NTP.
Router(config)# **ntp authenticate**	Activer l'authentification NTP
Router(config)# **ntp authentication-key** *key-number* **md5** *key-value*	Définissez la clé et le mot de passe NTP et cryptez-le à l'aide de MD5.

Router(config)# **ntp trusted-key** *key-number*	Identifiez la clé de confiance sur le maître.
Client(config)# **ntp server** *ntp-server-address*	Définir le routeur maitre NTP auquel le client va se synchroniser.

Configurer un client SysLog

Router(config)# **service timestamps** log datetimemsec	Activer les horodatages sur les messages de débogage et de journalisation.
Router(config)# **logging host** [ip-*address* | *hostname*]	Identifiez l'adresse du serveur SysLog ou son nom d'hôte.
Router(config)# **logging trap** *level*	Limiter les messages connectés aux serveurs syslog en fonction de la gravité. La valeur par défaut est 0 – 6.
Router(config)# **logging on**	Activer l'envoie des messages pour la Journalisation. La valeur est « on » par défaut
Router# **show logging**	Afficher l'état de journalisation et le contenu du tampon de journalisation système standard.

Configuration du SNMP

Router(config)#**snmp-server community**[tri] [ro]	Configurer l'identifiant de la « communauté » et son niveau d'accès (lecture seule ou lecture/écriture).
Router(config)#**snmp-server enable traps**[nom de traps]	Activer une «traps » SNMP.
Router(config)#**snmp-server host** [@ IP Gestionnaire SNMP][nom_community].	Superviser votre équipement
Router#**show snmp**.	Vérifier de la configuration SNMP

Sécurisation de l'accès de gestion avec AAA

Router(config)# **username** *username* **privilege** *level* **secret** *password*	Créer un utilisateur à la base de données locale et lui attribuer un mot de passe.
Router(config)# **aaa new-model**	Créer un nouveau modèle AAA.
Router(config)# **aaa authentication** login { **default** | *list-name}* { *method1*[*method2* ...]}	Définir la méthode d'authentification à utiliser lors de l'accès aux lignes console, vty ou aux. La méthode d'authentification incluelocal, localcase et Enable.
Router(config)# **aaa local Authentication attempts max-fail** *number*	Sécurisez les comptes AAA en verrouillant les comptes qui ont dépassé le nombre maximal de tentatives d'échec prédéfini
R1(config)# **tacacs-server host**{ *host-name* | *host-ip-address}*[**key** *string*] [**port** [*integer*]] [**single-connection**] [**timeout** [seconds*]*]	Configurer l'adresse IP (ou le nom) du serveur TACACS +. Les autres paramètres sont optionnels.
R1(config)# **radius-server host**{ *host-name* |	Configurer l'adresse IP (ou le nom) du serveur

host-ip-address }[**auth-port** *port-number*] [**acct-port** *port-number*] **[key** *password*]	RADIUS. Les autres paramètres sont optionnels.
Router(config)# **aaa group server radius** *groupname*	Grouper des hôtes de serveur RADIUS existants et les utiliser pour un service particulier
Router(config-sg-radius) # **server** *ip-address* [auth-**port** *port-number*] [acct-**port** *port-number*]	Configurez l'adresse IP du serveur RADIUS pour le serveur de groupe.
Router(config)# **aaa group server tacacs+** *group-name*	Regroupez les hôtes TACACS + Server existants et utilisez-les pour un service particulier.
Router(config-sg-tacacs+)# **server** *server-ip*	Configurez l'adresse IP du
Router(config)# **aaa authorization {exec | network | commands** *level}* {default | *List-name*} {method*1* [method*2* ...]}	Définit la stratégie d'autorisation à utiliser lors de l'accès aux modes exec,network,command

Les ACL IPv4

R1(config)#**access-list** *number* [**deny**|**permit**] **source** [*masque générique*]	Créer une ACL Standard numéroté
R1(config)#**ip access-list standard** *nom_ACL*	Créer une ACL Standard nommée
R1(Config-if) #**ip access-group** [number | *name* [**in** | **out**]]	Activer une ACL sur une interface
R1Config)#**access-list** *number* **{ deny | permit** } **protocol source**[*masque générique*]**destination**[*masque générique*]	Créer une ACL Etendue numérotée.
R1(config)# **ip access-list extended** nom_ACL	Créer une ACL Etendue nommée

Les ACL IPv6

R1(config)# **ipv6 access-list** *nom*_ACL	Création de l'ACL de IPv6
R1(config-ipv6-acl) # **{deny|permit} Protocole** *ipv6-source/CIDR* [{**eq**|**neq**|**gt**|**lt**|**range} port**] *ipv6-destination/CIDR* [{**eq**|**neq**|**gt**|**lt**|**range**} port]	Configuration d'une ACL IPv6
R1(config)#**interface*type*** *numéro* R1(config-if)#**ipv6 traffic-filte** *nom*_ACL **{in|out}**	Activation d'une ACL sur une interface

Configuration de l'IPS

Router(config)#**ip ips name** ips-name [list acl	Créer un nom pour la règle IPS.
Router(config)#**ip ips config location flash:**dirname	Spécifier l'emplacement du fichier de signature IPS.
Router(config)# **ip http server**	Activer le serveur http (requis lors de l'utilisation de SDEE).
Router(config)# **ip ips notify sdee**	Activer la notification d'événement SDEE.
Router(config)# **ip ips notify log**	Activer la journalisation.

MED ZAKI

Router(config)# **ip ips signature-category**	Entrez dans le mode de configuration des Catégories des signatures IPS.
Router(config-ips-category) # **category { all | ios_ips [basic | advanced]}**	Spécifiez la catégorie de signature à modifier
Router(config-if)# **ip ips** ips-name **{ in | out }**	Appliquez la règle IPS à une interface.

Les attaques d'inondation d'adresse MAC

Switch(config-if) # **switchport mode access** Switch(config-if) # **switchport port-security**	Activer la sécurité des ports et attribuez l'adresse MAC actuelle au port.
Switch(config-if) # **switchport port-security maximum** *value*	Définir le nombre maximal d'adresses MAC sécurisées pour l'interface.
Switch(config-if)# **switchport port-security mac-address** *mac-address*	Affecter manuellement les adresses MAC qui peuvent se connecter à ce port.
Switch(config-if) # **switchport port-security violation { protect | restrict | shutdown |shutdown vlan }**	Configurer l'action à prendre lorsque le nombre d'adresses MAC a dépassé le maximum prédéfini.
Switch(config)# **errdisable recoveryinterval** *seconds*	Configurer la période de désactivation d'un port.

L'attaque par usurpation d'adresse MAC (ARPspoofing)

switch(config)#**ip arp inspection vlan** vlan	Activer l'inspection ARP dynamique (DAI) sur un VLAN spécifique.
Switch(config)#**interface g0/0** switch(config-if)#**ip arp inspection trust**	configurer un port comme port fiable

L'attaque DHCP Starvation

S1(config)#**ip dhcp snooping**	activer la fonctionnalité « DHCP snooping » sur tous les VLAN.
S1(config)#**ip dhcp snooping vlan** *vlan*	Activer la fonctionnalité « DHCP snooping » sur un VLAN spécifique. .
S1(config)#**interface g0/0** S1(config-if)#**ip dhcp snooping trust**	configurer un port fiable
S1#**show ip dhcp snooping**	afficher la configuration « DHCP snooping »