DS

Sécurité et cryptographie

Classes: 2ing GTR

Documents autorisés

Exercice 1 [7pts]:

1) Expliquer pourquoi il est plus facile d'écouter (sniffer) un réseau local sans fil qu'un réseau local câblé ?
2) Expliquer comment la segmentation réseau (mise en place de sous réseau) assure une certaine sécurité pour le réseau de l'entreprise?
3) Vue le nombre limité des adresses publiques, on utilise souvent un adressage privée (adresse non routable) pour le réseau local d'une entreprise. Expliquer comment cet adressage permet de cacher le réseau local par rapport aux attaquants externes?
4) Est-ce que n'importe quelle attaque peut être lancée à partir de l'extérieur du LAN de l'entreprise? Expliquer ?
5) Expliquer pourquoi les attaques internes sont plus faciles à mener que les attaques externes ?
6) Expliquer pourquoi les attaques passives sont plus utiles (pour l'attaquant) dans un réseau partagé que dans réseau commuté ?
7) Expliquer comment un attaquant peut transformer un réseau Ethernet commuté en un réseau partagé ? Donner une solution permettant de contrer cette attaque ?
8) En se basant sur DHCP, expliquer comment un attaquant peut faire passer le trafic destiné à Internet par lui ? Donner une solution permettant de contrer cette attaque ?

Exercice 2 [3pts]:

1) Est-il nécessaire d'utiliser un canal authentifié pour échanger la clé de chiffrement dans un système à chiffrement symétrique? Expliquer ?
2) Citer deux problèmes principaux que le chiffrement hybride permet de résoudre. Expliquer ?
3) Expliquer l'utilité de changer la clé d'encryptage des données à chaque session dans un système à chiffrement hybride?
4) Quel problème peut surgir si la clé privée du PKI est compromise?

Exercice 3 [3pts]:

1) Soit le bout de code BC1 suivant implémenté au niveau d'un serveur. Expliquer comment un client peut exploiter ce code pour lancer une attaque ? Donner deux conséquences possibles.

BC1 :

```
Void mycopy (char * input) {
char buffer[20];
strcpy(buffer,input);
}
int main(int argc, char * argv[]) {
    mycopy(argv[1]) ;
}
```

2) Soit le bout de code BC2 suivant implémenté au niveau d'un serveur. Expliquer comment un client peut exploiter ce code pour lancer une attaque ? Comment peut-on alors améliorer ce code pour le rendre sécurisé?

BC2 :

```
$login = Request.Form("login")
$password = Request.Form("password")
SELECT * FROM users WHERE Login=$login AND Password=$password
```

Exercice 4 [7pts]:

Soit l'architecture du réseau indiqué dans la figure 1.

1) Soient les politiques de sécurité suivantes :
   P1 : Permettre aux utilisateurs externes d'accéder aux serveurs HTTP, Telnet et SMTP du LAN1.
   P2 : Permettre aux utilisateurs du LAN2 d'accéder aux serveurs du LAN3
   P3 : Permettre aux utilisateurs du LAN1 d'accéder à Internet
   a. Préciser le nombre de règles à implémenter pour chaque politique. Expliquer ?
   b. Dans quels routeurs doit-on implémenter chaque politique ?
2) Préciser les numéros de ports utilisés (port source et port destination) permettant à l'administrateur d'envoyer un trafic ICMP sur les machines internes ? Expliquer ?
3) Doit-on considérer l'état du bit ACK lors de l'implémentation de règles de filtrage du service TFTP (Trivial File Transfer Protocol) qui fonctionne au dessus d'UDP ?
4) Soient les deux politiques suivantes et les règles de filtrage correspondantes :
   - Politiques :
     - Permettre au LAN3 d'accéder aux serveurs du LAN1 fonctionnant au dessus de TCP
     - Interdire l'accès du LAN3 au serveur Telnet du LAN1
   - Règles de filtrages

Routeur	@IP source	@IP dest	Port source	port dest	protocole	ACK=1	Action
Routeur3	LAN3	LAN1	>1023	tous	TCP	*	Autoriser
Routeur3	LAN1	LAN3	tous	>1023	TCP	oui	Autoriser
Routeur3	LAN3	.33.6	>1023	23	TCP	*	Bloquer

   a. Expliquer comment les règles suivantes permettent à un utilisateur du LAN3 d'accéder au serveur Telnet du LAN1?
   b. En déduire les règles permettant de répondre aux deux politiques spécifiées ?

5) Traduire les règles de filtrage suivantes implémenté au niveau du routeur 3 en utilisant des ACL Cisco. Assigner les ACLs créées aux interfaces adéquates du routeur 3.

règle	@IP source	@IP dest	port src	Port dest	protocole	Action
1	LAN3	193.95.33.6	>1023	23	TCP	Accepter
2	193.95.33.6	LAN3	23	>1023	TCP	Accepter
3	LAN3	193.95.33.7	>1023	25	TCP	Accepter
4	193.95.33.7	LAN3	25	>1023	TCP	Accepter

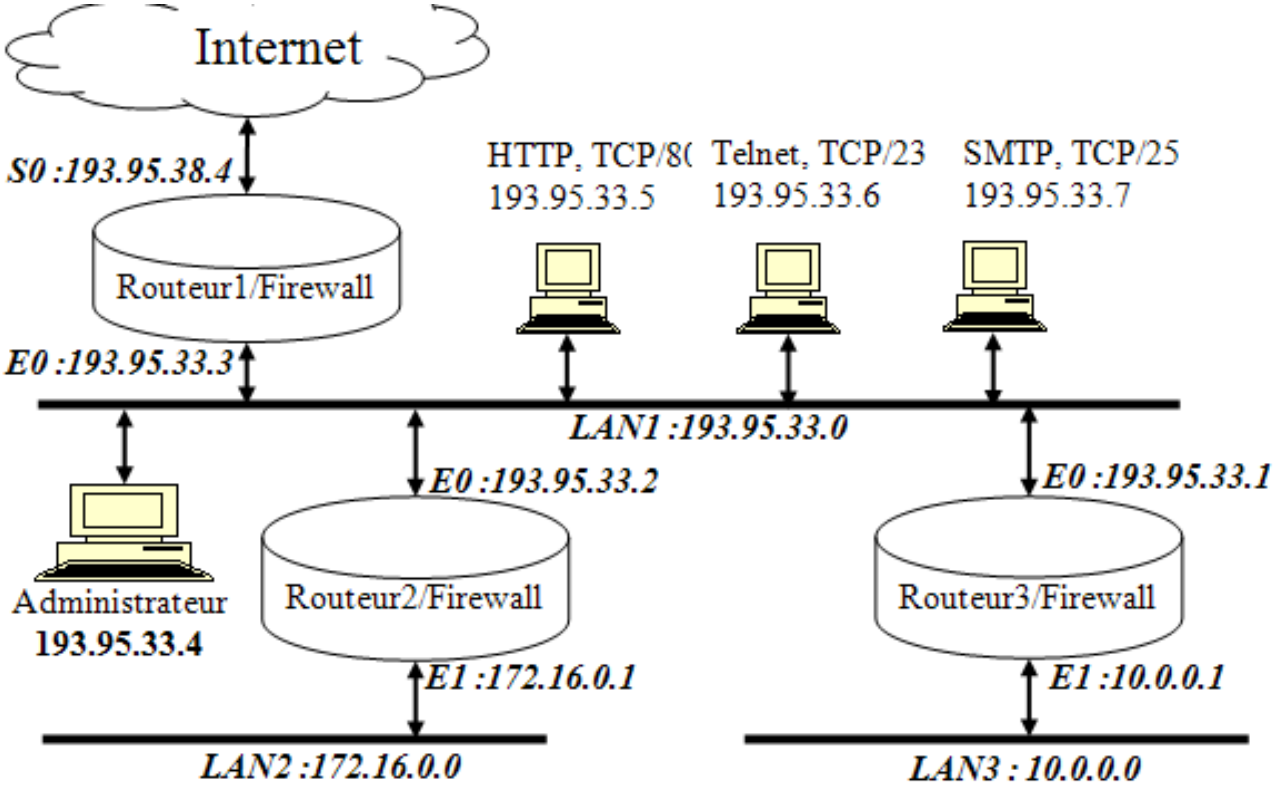

Figure 1 : architecture du réseau