Université de Tunis Elmanar
Institut Supérieur d'Informatique

Section :
Module : **Sécurité concepts et méthodes**
Classe : ….....**2ING-GTR**.....
Session : ….....**DS**.....

A.U. : 2014/2015

Signatures des Surveillants

Signature de l'étudiant

Nom : …… Prénom :……..
N° CIN : …….
N° d'inscription : ……

Date :..... Salle n° :……. Place n° :……..

Exercice 1 [4 pts]:

1) Expliquer pourquoi il est plus facile d'écouter (sniffer) un réseau local partagé qu'un réseau commuté.

….....

….....

….....

2) Expliquer pourquoi l'audit sécurité d'un système d'information d'une entreprise nécessite la connaissance de la politique de sécurité de cette dernière?

….....

….....

….....

3) Expliquer pourquoi l'utilisation de technologies robustes de sécurité n'assure pas toujours la sécurisation du système d'information de l'entreprise? Expliquer ?

….....

….....

….....

4) Expliquer pourquoi les attaques externes sont plus difficiles à mener que les attaques internes ?

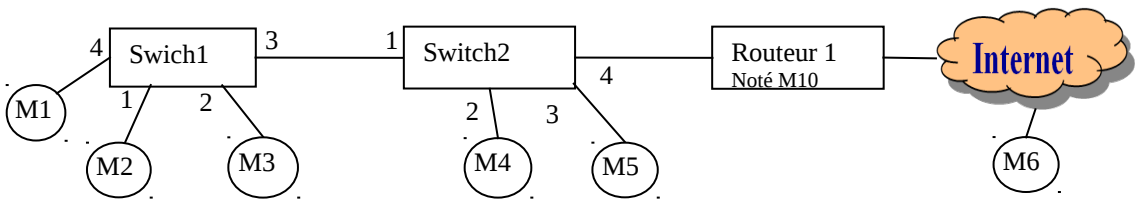
….....

….....

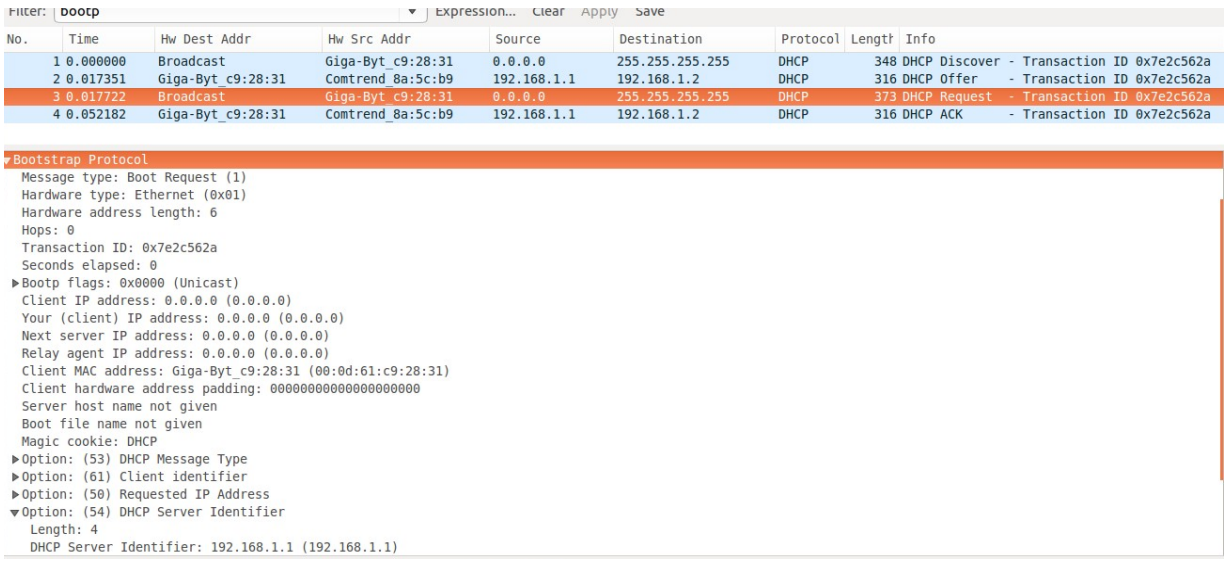
….....

Exercice 2 [16pts]:

Soit le réseau Ethernet câblé suivant où les cercles sont des stations de travail. **M5** implémente un serveur DHCP.



Soit les messages suivants décrivant le fonctionnement du protocole DHCP. "Hw Dest addr" et "Hw Src Address" représentent respectivement, l'adresse MAC destination et l'adresse MAC source. On donne seulement quelques détails du troisième message.



Filter: bootp Expression... Clear Apply Save

No.	Time	Hw Dest Addr	Hw Src Addr	Source	Destination	Protocol	Length	Info
1	0.000000	Broadcast	Giga-Byt_c9:28:31	0.0.0.0	255.255.255.255	DHCP	348	DHCP Discover - Transaction ID 0x7e2c562a
2	0.017351	Giga-Byt_c9:28:31	Comtrend_8a:5c:b9	192.168.1.1	192.168.1.2	DHCP	316	DHCP Offer - Transaction ID 0x7e2c562a
3	0.017722	Broadcast	Giga-Byt_c9:28:31	0.0.0.0	255.255.255.255	DHCP	373	DHCP Request - Transaction ID 0x7e2c562a
4	0.052182	Giga-Byt_c9:28:31	Comtrend_8a:5c:b9	192.168.1.1	192.168.1.2	DHCP	316	DHCP ACK - Transaction ID 0x7e2c562a

1) On suppose que M2 vient d'être configué par le serveur DHCP.

   a. Quels sont les noeuds qui ont reçu le DHCP discover? Expliquer.

…….

…….

   b. Quels sont les noeuds qui ont reçu le DHCP offer? Expliquer.

…….

…….

   c. Quels sont les noeud qui ont reçu le DHCP request? Expliquer.

…….

…….

   d. Quels sont les noeuds qui ont reçu le DHCP ack? Expliquer.

…….

…….

2) Dans cette partie, nous supposons que le serveur DHCP sauvegarde les adresses MAC des nœuds légitimes dans un fichier local. Un noeud ne peut être servi que si son adresse existe dans ce fichier.

   a. En se basant sur le **sniffing passif**, monter comment un attaquant lié à l'un des switch pourrait déterminer l'adresse IP du serveur DHCP et les adresses MAC des noeuds configurés par ce dernier.

…….

…….

…….

   b. En déduire que cet attaquant pourrait bloquer prochainement la configuration, par DHCP, des noeuds du réseau. Expliquer comment doit-il procéder ?

…….

…….

…….

3) Dans cette partie, nous ne considérons plus l'hypothèse de la partie précedente et nous considérons qu'un nœud malicieux d'adresse MAC « MAC_ATTAQUANT » a lancé l'attaque « DHCP starvation ». Les commutateurs fonctionnent correctement.

   a. Doit-il utiliser cette même adresse MAC au niveau liaison de donnée pour toutes les configurations IP à obtenir ? Expliquer ? ((N. B : les trames sont commutées selon l'adresse MAC)

….....

….....

   b. Doit-il utiliser cette même adresse MAC au niveau application (entête DHCP) pour toutes les configurations IP à obtenir ? Expliquer ?

….....

….....

   c. En déduire comment peut-on utiliser un sniffer passif installé au niveau du nœud hébergeant le serveur DHCP pour détecter qu'il y a des requêtes DHCP qui ont été lancées par un même nœud en spécifiant différentes adresses MAC.

….....

….....

….....

….....

4) Proposer une méthode permettant à l'attaquant d'utiliser différentes adresses MAC (niveau liaison) pour réussir son attaque « DHCP starvation » ? (N. B : les trames sont commutées selon l'adresse MAC et le switch diffuse les trames s'il ne connait pas le port de sortie de ces dernières).

….....

….....

….....

….....

5) Pour lutter contre l'attaque « dhcp starvation », l'administrateur a limité le nombre d'adresse MAC par port à 3 sur les deux switchs. Supposons que l'attaquant est le nœud M1. Montrer que M2 et M3 risquent de ne pas obtenir une configuration IP à partir du serveur DHCP ?

….....

….....

….....

….....

6) En se basant sur les attaques DHCP, proposer une méthode permettant à M1 de jouer le rôle de « man in the middle » entre le routeur et n'importe quel autre nœud du réseau .

….....

….....

….....

….....

7) Nous étudions maintenant comment le nœud M1 peut jouer le rôle de « man in the middle » entre le routeur et n'importe quel autre nœud du réseau en se basant sur l'attaque « ARP spoofing ». Nous utilisons les notations suivantes : @MAC_Mi (adresse MAC du nœud Mi), @IP_Mi (adresse IP de Mi).

a. Donner la table arp sauvegardé par M2 (@MAC_Mi, @IP_Mi) avant et après l'exécution de cette attaque

avant	après
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....

b. Quelles sont les conséquences de cette ataque si le routage est désactivé sur le nœud M1 ?

.....

.....

.....

.....

c. Sachant que les nœuds connaissent le routeur par défaut, proposer une solution permettant à un nœud de détecter qu'il est victime de cette attaque.

.....

.....

.....

8) Donner trois attaques possibles exploitant la rubrique suivante d'une page web. Préciser comment chaque attaque va être lancée et donner une contre mesure

.....

.....

.....

.....

.....

.....

.....