Base de CYBERSECURITE

TP1 :

Attaques passives : sniffing passif

Prérequis

1-VirtualBox

2-Deux machines clients :

- **Machine Windows 7 (lien de téléchargement),**
- **Machine linux (Ubuntu) : 'Lien téléchargement**

3-Machine centrale (KALI linux).

- **Lien de téléchargement ;**
- **Comment l'installer(**

4- Installation de Wire Shark dans KALI et ubuntu (Lien démonstration)

Config de base pour tous les TPs

- **Installer les machines virtuelles**
- **Elaborer un réseau local (adresses IP statiques)**
  - **Machine kali (adresse ip : 192.168.1.2)**
  - **Machine Ubuntu (adresse ip : 192.168.1.3)**
  - **Machine Windows 7 (adresse ip : 192.168.1.4)**
- **+ D'autres éléments seront communiqués plus tard dans les TPs**

Attaques passives : sniffing passif

Les sniffers (appelé aussi « analyseurs de protocoles » ou « analyseurs de réseau ») sont des outils logiciels qui peuvent capturer les trames circulant sur un réseau local et afficher leurs contenus (entêtes des protocoles, identités des utilisateurs, mot de passe non cryptés, etc). Ces outils sont utilisés par les administrateurs pour analyser leurs réseaux et localiser les problèmes dans ces derniers. Ils sont aussi utilisés par les attaquants pour espionner les données circulant dans un réseau local.

Le tableau 1 présente une comparaison de quelques sniffers (GUI : graphical User Interface, CLI : Command Line Interface)

sniffer	User interface	Software license	Microsoft Windows	OS X	Linux	BSDs	Solaris
Cain and Abel	GUI	Freeware	Yes	No	No	No	No
CommView	GUI	Proprietary	Yes	No	No	No	No
dSniff	CLI	BSD License	?	Yes	Yes	Yes	Yes
EtherApe	GUI	GNU General Public License	No	Yes	Yes	Yes	Yes
Ettercap	Both	GNU General Public License	Yes	Yes	Yes	Yes	Yes
netsniff-ng	CLI	BSD-style	No	No	Yes	No	No
tcpdump	CLI	BSD License	Yes WinDump	Yes	Yes	Yes	Yes
Wireshark (formerly Ethereal)	Both	GNU General Public License	Yes	Yes	Yes	Yes	Yes

Tableau 1 : comparaison de quelques sniffers

1- Objectifs de ce TP:

- Implémenter un sniffer passif simple
- Manipuler des logiciels de sniffing

2- Outils logiciels:

Linux, wireshark, compilateur cc ou gcc

3- Informations utiles :

- Les cartes réseau fonctionnent en deux modes
  - mode normal (mode par défaut) : permet à une carte de filtrer les trames reçus en fonction de l'adresse MAC destination
  - mode promiscuous : consiste à accepter toutes les trames circulant dans un réseau,

même ceux qui ne sont pas destinés à la carte.

- Sous Unix, la commande # ifconfig promisc permet d'activer le mode promiscuous.
- La plupart des logiciels sniffers permettent d'activer le mode promoscuous lors de leur lancement.
- Dans un réseau commuté, le sniffing **passif** de toutes les trames qui circulent dans le réseau est impossible à réaliser puisqu'un nœud ne peut recevoir que les trames qui lui sont destinées.
- Le sniffing **actif** (qui sera traité au niveau du TP2) permet de faire du sniffing sur un réseau même s'il est commuté.
- Le sniffer doit être sur le même réseau à sniffer. Sinon, il doit faire du « **remote sniffing** » en contrôlant à distance une machine qui se trouve sur le réseau à sniffer.

Partie 1 : Préparation d'environnement du TP

1. installer win7 32 et ubuntu64
2. dans Ubuntu, en utilisant le terminal, installer le package Gcc.
3. Configurez les deux machines dans un seul réseaux interne
   - Pour chaque machine, choisir réseau interne (dans les paramètres réseaux) dans la config de VirtualBox
   - Démarrer les machines et configurez l'adresse ip statique
   - Désactivez le firewall de Windows 7
4. tester la connexion entre les deux machines avec un ping

Partie 2 : Implémentation d'un sniffer passif

L'annexe 1 présente le code source d'un sniffer passif qui permet de récupérer les trames reçues par une interface réseau (exemple ETHERNET). Ce code source est écrit en langage C et peut être compilé et exécuté sur une machine Linux. Les fonctions les plus importantes de ce code sont (voir contenu de lafonction main):

- La fonction recvfrom qui permet de récupérer les trames reçues sur l'interface réseau.
- La fonction PrintPacketInHex qui permet d'afficher la trame sous format hexadécimal
- La fonction ParseEthernetHeader qui permet d'afficher quelques champs de l'entête ETHRNET
- La fonction ParseIpHeader qui permet d'afficher quelques champs de l'entête IP
- La fonction ParseTcpHeader qui permet d'afficher quelques champs de l'entête TCP
- La fonction ParseData qui permet d'afficher les données sous format hexadécimal

Manipulations à faire (sous linux):

1) Compiler (cc -c sniffer_eth_ip_tcp_data.c) le code source et générer l'exécutable (cc sniffer_eth_ip_tcp_data.c – o sniffer).
2) Exécuter (en mode root : « **sudo commande** » sous ubuntu) le sniffer (exemple : pour sniffer les 100 premières trames reçu sur l'interface eth0 tapez **./sniffer eth0 100**). Vous pouvez utiliser **wlan0** à la place de **eth0** si vous êtes connecté en sans-fil (les trames Wifi sont automatiquement traduites en ETHERNET) ou **lo** (loopback) si vous n'avez aucune connexion. Si rien ne s'affiche, cela veut dire que vous n'êtes pas en train de recevoir des paquets, exécuter alors (dans une nouvelle fenêtre) un ping vers une autre machine et consulter de nouveau le résultat du sniffer.
3) Dans la manipulation précédente, les trames sont affichées sous format hexadécimal. Pour afficher le contenu de l'entête ETHERNET, il faut enlever le commentaire de la fonction ParseEthernetHeader, recompiler, régénérer l'exécutable et refaire l'étape 2).
4) Pour Afficher le contenu des entêtes des protocoles des niveaux supérieurs, enlevez les commentaires des fonctions correspondantes (au niveau de la fonction main), recompiler, régénérer l'exécutable et exécuter de nouveau le sniffer. Pensez à faire un échange de trafic TCP (en utilisant par exemple le serveur vsftpd ou en se connectant à Internet).
5) Ecrire une fonction qui permet d'afficher l'entête UDP et l'intégrer dans le code source du sniffer (localiser udp.h dans /usr/include/netinet).

Partie3 : manipulation de sniffers

Dans cette partie, nous nous intéressons à la manipulation de quelques sniffers existants.
(Pour plus d'informations sur l'utilisation de wireshark (cliquez ici) et (ici)

1) Lancer le logiciel wireshark en arrière- plan (wireshark &) et commencez la capture sur l'interface ETHERNET ou sans fil.
2) Lancez des applications d'échange de trafic entre d'autres machines et la votre. Observez-les paquets capturés.
3) Est-ce que vous pouvez capturer les trafics échangés entre les machines du reste du réseau?
4) Configurer le filtre de wireshark pour (voir annexe 2).
    a. n'afficher que les trames concernant un protocole particulier : bootp, tcp, icmp,etc
    b. n'afficher que les trames dont l'adresse MAC destination est celle de votre machine
    c. n'afficher que les trames échangé entre deux machines d'adresse @IP1 et @IP2
    d. n'afficher que les trames dont la taille est supérieure à une taille donnée

Partie 4 : remote sniffing

Dans cette section, nous nous intéressons l'utilisation d'un sniffer à distance « remote sniffing » pour obtenir les données circulant sur un autre réseau que celui sur lequel nous sommes. Supposons que nous sommes sur le réseau RES1 et nous voulons sniffer le réseau voisin RES2 (nous sommes séparés par un routeur). Nous utilisons alors un **client sniffer** sur une machine du réseau RES2 qui va sniffer ce dernier et envoyer les données capturées à notre **serveur sniffer** sur le réseau RES1. Le réseau B qui, en principe, était impossible à sniffer est devenu donc très accessible.

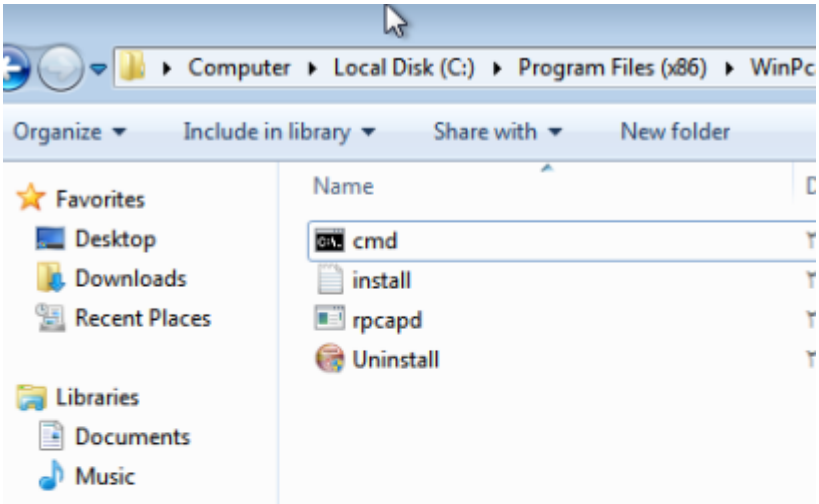
Nous utilisons le démon **Rpcapd** (plus de détails) qui capture le trafic sur une machine, et est capable d'envoyer les données récupérées à un sniffer comme wireshark qui facilite ainsi la lecture en différenciant les trames et les protocoles. Notons qu'il est utile d'exclure le trafic entre la machine locale et la machine distante en utilisant les filtres de wireshark.

Manipulations à faire (sous linux):

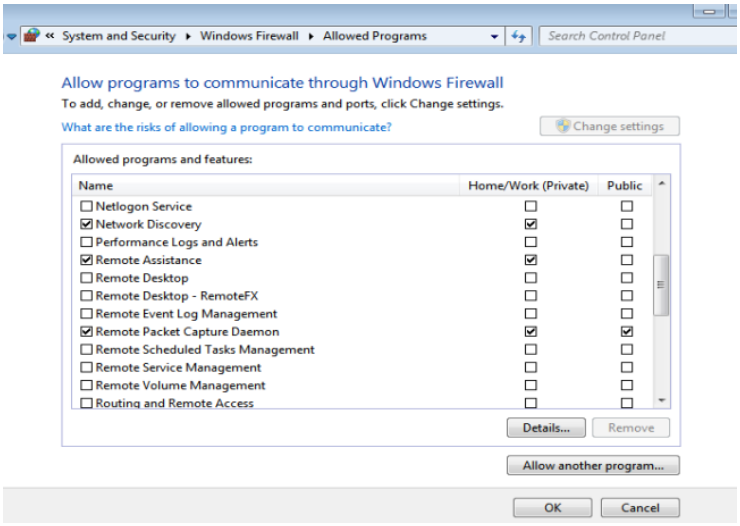
1) Sur votre machine, lancer wireshark et accéder aux options de capture puis taper dans interface « **rpcap://@ipmachine distante/eth0 » (par exemple machine windiws7)** et taper dans capture filter « **not host votre adresse IP »**
2) Etudier les paquets capturés.

Etapes à suivre :

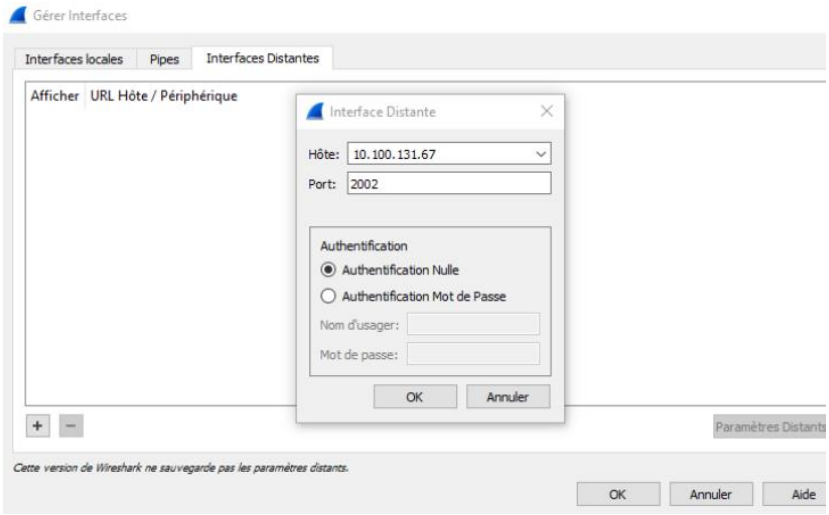
- Nous utilisons le démon Rpcapd qui capture le trafic sur une machine, et est capable d'envoyer les données récupérées à un sniffer comme wireshark qui facilite ainsi la lecture en différenciant les trames et les protocoles.
- Installez l'outil winPcap dans la machine windows7 (ordinateur distant) :
- Dans les fichiers winPcap on retrouve le service rpcapd
-



- Avant de commencer la manipulation, nous devons autoriser rpcapd à communiquer via le pare-feu Windows en l'ajoutant dans la liste des programmes et fonctionnalités autorisés :
-



- **Configurer les options des interfaces distantes dans wireshark:**
-



- **avant de cliquer sur OK pour ajouter l'interface distante nous devons activer le service rpcapd sur la machine distante**

- **Afin de connaître le port nous utilisons cette commande « netstat -a »**

- **Maintenant, après avoir activé le service rpcapd sur la machine distante, nous pouvons ajouter l'interface distante dans wireshark.**

- **Afin de confirmer que la connexion est établie entre la machine distante et la machine qui se trouve dans l'autre réseau nous utilisons cette commande « netstat -n »**
- **Enfin, après toutes ces étapes. Maintenant, nous pouvons commencer la capture du package (filtre bootp)**

Annexe 1: (site officiel de wireshark)

Display Filter comparison operators

English	C-like	Description and example
eq	==	Equal. ip.src==10.0.0.5
ne	!=	Not equal. ip.src!=10.0.0.5
gt	>	Greater than. frame.len > 10
lt	<	Less than. frame.len < 128
ge	>=	Greater than or equal to. frame.len ge 0x100
le	<=	Less than or equal to. frame.len <= 0x20

Display Filter Field Types

Type	Example
Unsigned integer (8-bit, 16-bit, 24-bit, 32-bit)	You can express integers in decimal, octal, or hexadecimal. The following display filters are equivalent: ip.len le 1500 ip.len le 02734 ip.len le 0x436
Signed integer (8-bit, 16-bit, 24-bit, 32-bit)	
Boolean	A boolean field is present in the protocol decode only if its value is true. For example, *tcp.flags.syn* is present, and thus true, only if the SYN flag is present in a TCP segment header. Thus the filter expression *tcp.flags.syn* will select only those packets for which this flag exists, that is, TCP segments where the segment header contains the SYN flag. Similarly,

	to find source-routed token ring packets, use a filter expression of *tr.sr*.
Ethernet address (6 bytes)	Separators can be a colon (:), dot (.) or dash (-) and can have one or two bytes between separators: eth.dst == ff:ff:ff:ff:ff:ff eth.dst == ff-ff-ff-ff-ff-ff eth.dst == ffff.ffff.ffff
IPv4 address	ip.addr == 192.168.0.1 Classless InterDomain Routing (CIDR) notation can be used to test if an IPv4 address is in a certain subnet. For example, this display filter will find all packets in the 129.111 Class-B network: ip.addr == 129.111.0.0/16
IPv6 address	ipv6.addr == ::1
String (text)	http.request.uri == "https://www.wireshark.org/"

Display Filter Logical Operations

English	C-like	Description and example
and	&&	Logical AND. `ip.src==10.0.0.5 and tcp.flags.fin`
or	||	Logical OR. `ip.scr==10.0.0.5 or ip.src==192.1.1.1`
xor	^^	Logical XOR. `tr.dst[0:3] == 0.6.29 xor tr.src[0:3] == 0.6.29`
not	!	Logical NOT. `not llc`
		Substring Operator. Wireshark allows you to select subsequences of a sequence in rather elaborate ways. After a label you can place a pair of brackets [] containing a comma separated list of range specifiers. eth.src[0:3] == 00:00:83 The example above uses the n:m format to specify a single range. In this case n is the beginning offset and m is the length of the range being specified. eth.src[1-2] == 00:83 The example above uses the n-m format to specify a single range. In this case n is the beginning offset and m is the ending offset. eth.src[:4] == 00:00:83:00 The example above uses the :m format, which takes everything from the beginning of a sequence to offset m. It is equivalent to 0:m eth.src[4:] == 20:20 The example above uses the n: format, which takes everything from offset n to the end of the sequence.

		eth.src[2] == 83 The example above uses the n format to specify a single range. In this case the element in the sequence at offset n is selected. This is equivalent to n:1. eth.src[0:3,1-2,:4,4:,2] == 00:00:83:00:83:00:00:83:00:20:20:83 Wireshark allows you to string together single ranges in a comma separated list to form compound ranges as shown above.