Université Ain Témouchent -Belhadj Bouchaïb-
Faculté des Sciences et de la Technologie
Département des Mathématiques et de l'Informatique
Année universitaire 2020-2021

TP1 / AR

Responsable du Module : Mr A. BENZERBADJ

1 Objectif

Installation et prise en main de Wireshark

2 Brève introduction à Wireshark

— *Wireshark* (anciennement *Ethereal*) est un analyseur de paquets (sniffer) open source, fonctionnant sur pratiquement tous les environnements et reconnaissant pratiquement tout les protocoles informatique existants. Son but est de réaliser des captures de trames dévoilant des failles de sécurité, voir de localiser des pertes de performances sur le réseau. *WireShark* est actuellement l'analyseur de paquets le plus utilisé au monde. Il est facilement téléchargeable sur le net (**https ://www.wireshark.org/**).

— Les sniffers servent à récupérer l'ensemble des données transitant à travers un réseau, des couches 2 à 7 du modèle OSI.

— L'installation de *Wireshark* sous Linux se fait par le biais de la commande : **apt-get install wireshark**. On notera tout de même qu'il peut arriver que lorsque l'on exécute Wireshark via l'utilisateur, les interfaces réseaux ne sont pas reconnues, car l'utilisateur n'a pas les droits d'accès. Il suffit de donner les droits à l'utilisateur ou de lancer directement Wireshark depuis root, ce qui est déconseillé.

— Une fois installé, exécutez Wireshark avec l'utilisateur Root (ce qui est déconseillé) ou exécutez les opérations suivante :

1. **sudo dpkg-reconfigure wireshark-common**
   Cette commande vous demandera si vous voulez autoriser un utilisateur non-root à renifler (à sniffer). C'est ce que nous vonlons, alors on répond par **"Yes"**. Ainsi, elle ajoute un groupe WireShark. N'importe qui dans ce groupe sera capable de renifler sans être root.
2. **sudo usermod -a -G wireshark $USER**
3. **Redémarrez ou déconnectez puis reconnectez-vous**

— Récap d'installation de wireshark :

1. apt-get install wireshark
2. sudo dpkg-reconfigure wireshark-common
3. sudo usermod -a -G wireshark $USER
4. sudo reboot

3 Les filtres

— L'intégralité des paquets capturés est listée dans la zone supérieure de l'analyseur. Il est souvent utile de filtrer les paquets à capturer, afin de pouvoir visualiser correctement un certain type de paquets seulement. Wireshark permet de filtrer les paquets à capturer en fonction des informations des différentes couches d'encapsulation.

— Un filtre est composé d'une ou plusieurs expressions reliées par les opérateurs logiques and, or et not : [not]Expresion[and|or[not]expresion...]. Dans expression on peut utiliser des opérateurs arithmétiques : eq, ne, gt, lt, ge, le, ou ==, !=, >, <, >=, <=.

3.1 Exemples de filtres

— **ip.src==192.168.10.0/24 and ip.ttl >= 100**, Paquets avec ip source égale à 192.168.10.0/24 avec un ttl >= 100.

— **ftp || tcp**, Paquets dont le type est : ftp ou tcp.

— **ip.addr == 10.20.144.150**, Paquets dont l'adresse IP source ou destination est 10.20.144.150

— **ip.src == 10.20.144.150**, Paquets dont l'adresse IP source 10.20.144.150

— **ip.dst == 10.20.144.15**1, Paquets dont l'adresse IP source 10.20.144.151

— **tcp.port == 35974**, Paquets dont le port source ou destination est 35974.

— **tcp.srcport == 21**, Paquets dont le port source est 21 (port FTP).

— **tcp.dstport == 21**, Paquets dont le port destination est 21.

— Segments TCP uniquement, **tcp**

— Paquets relatifs à TCP uniquement, **ip.proto == 0x06**

— Adresse ip 192.168.0.1 ou 192.168.1.5, **ip.addr == 192.168.0.1 || ip.addr == 192.168.1.5**

— Trafic HTTP uniquement, **http**

— Segment TCP sauf sur port 80, **tcp && !(tcp.port == 80)**

— Adresse Ethernet 00 :FF :12 :34 :AE :FF, **eth.addr == 00 :FF :12 :34 :AE :FF**

— Trafic 192.168.0.1 vers 197.168.10.5, **ip.src == 192.168.0.1 && ip.dst == 197.168.10.5**

— Trafic UDP entre ports 40 et 67, **udp && udp.port >= 40 && udp.port <=67**

4 Génération du trafic

Réaliser les actions suivantes dans l'ordre de leurs apparitions :

1. envoyer 10 paquets de taille 7000 octets à la machine 192.168.10.1

— $ ping -c 10 -s 7000 192.168.10.1

2. Lancer la commande :
   — $ ping -c 1 4.2.2.4
3. Lancer la commande :
   — $ traceroute www.google.fr
4. accéder au site :
   — www.google.fr
   — lancer la recherche avec le mot "Network".
5. accéder au site www.yahoo.fr
   — accéder au site ftp ://ftp.debian.org
   — accéder à quelques répertoires
6. accéder à votre messagerie personnelle.
7. arrêtez la capture (au niveau de l'interface).
8. sauvegardez cette capture dans un fichier.
9. relever l'adresse IP de votre réseau active.
   — sous Linux : $ ifconfig

5 Analyse du trafic

5.1 Cibler une machine particulière

1. Filtrer les paquets envoyés ou reçus par la station ayant l'adresse MAC suivante : xx :yy :zz :aa :bb :cc
   — **eth.src==xx :yy :zz :aa :bb :cc or eth.dst==xx :yy :zz :aa :bb :cc**
2. Sélectionner toutes les trames de diffusion (broadcast).
   — **eth.dst==ff :ff :ff :ff :ff :ff**
3. Donner le filtre pour observer le trafic sortant et à destination de votre machine.
   — **ip.addr==MyIPaddress**
4. Donner le filtre pour observer le trafic sortant de votre machine.
   — **ip.src==MyIPaddress**
5. Donner le filtre pour observer le trafic venant vers votre machine.
   — **ip.dst==MyIPaddress**
6. Visualiser seulement le trafic de paquets entre votre machine et le serveur 4.2.2.4 ?
   — **ip.addr==MyIPaddress and ip.addr==4.2.2.4**
7. Sélectionner les paquets dont la taille est inférieure à 100.
   — **ip.len>=100**

5.2 Protocole TCP

1. Qu'observer-vous (quels types de paquets) avec les filtres suivants :
   (a). **tcp.dstport==80 and ip.src==MyIPaddress** (c'est le trafic entre la machine 192.168.1.3 et tous les serveurs web)
   (b). **tcp.flags.syn==1 and tcp.flags.ack=1** (ce sont les paquets de confirmation d'ouverture de connexion de la part d'un(ou +ieurs)serveur(s))
2. Visualiser les paquets de fermeture de connexion TCP ?
   — **tcp.flags.fin=1**

5.3 Protocole ICMP

1. Quel est le pourcentage de paquets ICMP reçus par votre machine ? filtre **icmp ou ip.proto == 0x0001**, pourcentage : $100.\frac{Xmarked}{Ydisplayed}$, X et Y sont lus en bas de la fenêtre 2. Quel est le pourcentage de paquets ICMP envoyés par votre machine ? marked filtre **ip.proto == 0x0001 and ip.src == MyIPaddress**, pourcentage : $100.\frac{Xmarked}{Ydisplayed}$
2. Visualiser les paquets avec un TTL=1 et TTL=2 relatifs au protocole ICMP. D'après vous, quelle est l'application qui a généré ces paquets ? (c'est l'application tracert ou traceroute)
   — **ip.ttl==1**
   — **ip.ttl==2**

5.4 Protocole ARP

1. Identifier les paquets de type ARP ?
   — **arp ou eth.type==0x0806**
2. Identifier les paquets de type ARP-Request ?
   — **Arp.opcode==0x0001**
3. Identifier les paquets pour ARP-Reply ?
   — **Arp.opcode==0x0002**

5.5 IP et fragmentation

1. Quels sont les filtres succéssifs à utiliser pour retracer une fragmentation
   — ip.flags.mf == 1, pour trouver tous les fragments avec mf =1 et on repère un numéro d'iden- tifiant. Ensuite on applique le filtre ip.id== IDENTIFIANT, on aura tous les fragments constituant le paquet fragmenté d'identifiant IDENTIFIANT
2. Donner les fragments du premier paquet fragmenté dans votre capture sous forme : (identifiant,bit mf, offset, taille totale) l'offset relatif (non absolu. Une fois les paquets issus d'une fragmentation isolés, on peut exploiter les champs de l'entête. IP pour extraire les information demandés pour chaque fragment jusqu'au dernier dont le bit mf est à 0

5.6 Protocole DHCP

1. Relancer une nouvelle capture et lancer la commande suivante :
   — $ dhclient eth0
2. Lancer le filtre de visualisation suivant : bootp. Que représente cette visualisation ? Expliquer. Le trafic visualisé correspond à un renouvellement du bail attribué par un serveur DHCP. On remarque l'échange de quatre paquets : DHCP-DISCOVER, DHCP-OFFER, DHCP-REQUEST et enfin DHCP-ACK
3. Relancer une nouvelle capture. Débrancher le câble RJ45 de votre carte réseau, ensuite remettre le câble à sa place. Lancer le filtre de visualisation suivant : bootp . expliquer les échanges et les différentes adresses IP observées. L'action de débrancher le cable va avoir le même effet que de renouveler la demande explicite de renouvellement du bail attribué

par un serveur DHCP. Il y'aura également l'échange des quatre paquets : DHCP-DISCOVER, DHCP-OFFER, DHCP-REQUEST et enfin DHCP-ACK.Les adresses IP observées :

— 0.0.0.0 : adresse réservée qui signifie je suis une station dans ce réseau. (émise par la station demandant le bail)

— 255.255.255.255 : adresse de diffusion dans tout le réseau local pour atteindre le (ou les) serveurs DHCP dans ce réseau.

5.7 Protocoles applicatifs : HTTP, DNS, FTP

1. Quels sont les paquets contenant le mot clé « network » envoyés par votre machine ? http contains network
2. Donnez le filtre pour observer le trafic des commandes FTP.
   — ftp
   — ftp-data
3. Visualiser tous les paquets dont le protocole encapsulé porte le N o 17. De quel protocole il s'agit ?
   — ip.proto==17, il s'agit du DNS
4. Visualiser tous les paquets dont le protocole encapsulé porte le N o 0x006 . De quel protocole il s'agit ?
   — ip.proto==0x0006, il s'agit de TCP
5. Visualiser tous les paquets dont le protocole encapsulé porte le Numéro 0x001 . De quel protocole il s'agit ?
   — ip.proto==0x0001, il s'agit de ICMP