TP Protocoles d'Application

Dino Lopez Pacheco dino.lopez@univ-cotedazur.fr

1 Introduction

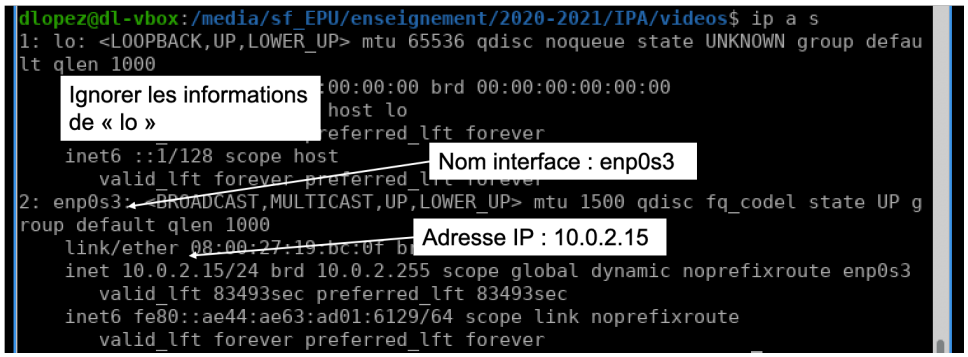
Ce TP a pour objectif de vous permettre d'observer et comprendre, le fonctionnement de certains protocoles que vous utilisez de manière courante. En tant qu'ingénieur en systèmes informatiques (de n'importe quel domaine), il est indispensable de comprendre et interagir avec notre environnement numérique immédiat de manière aisée.

2 Capture de trafic réseau

Pour debugger ou analyser un protocole, la première chose à faire est souvent capturer le trafic transitant par le réseau. Voici donc quelques exercices qui ont pour but de vous apprendre à maîtriser l'outil de capture tcpdump.

Pour les exercices de ce TP, la page web suivante peut s'avérer très utile https://docs.netgate.com/pfsense/en/latest/book/packetcapture/using-tcpdump-from-the-command-line.html

1. Dans votre machine virtuel Linux
    - Exécutez « ip a s ». Trouvez le nom de l'interface avec l'adresse IP « 10.0.X.X/24 » (ça devrait être 10.0.2.15/24, même si les chiffres peuvent toujours varier).



    - En mode super utilisateur (e.g. en exécutant « sudo su »), exécutez tcpdump de la manière suivante « tcpdump -i *yourIface* -w /tmp/test1.1.pcap », où *yourIface* est le nom de l'interface que vous avez trouvé dans le point précédent. Laissez le programme tourner, puis, visitez un site internet quelconque (e.g. twitter.com) à l'aide de votre navigateur.
    - tcpdump est un outil pour capturer le trafic réseau (un *sniffer*). A l'aide de la man page, expliquez à quoi sert chaque option passez en paramètre.

    On capture tout le trafique vue par l'interface *yourIface* est l'écrit dans le fichier /tmp/test1.1.pcap

    - Arrêtez tcpdump avec « Ctrl-C » dans le terminal, puis ouvrez le fichier pcap avec la commande « wireshark /tmp/test1.1.pcap ». Expliquez brièvement l'objectif de chaque division visible dans wireshark.

Interface graphique vu en cours. De manière simple, la partie supérieure montre tout le trafique capturé. La partie au milieu montre des détails sur les protocoles composant un paquet capturé. La partie base montre le contenu brut du paquet.

2. Comme vous l'avez sans doute compris, tcpdump a capturé tout le trafic réseau disponible sur votre interface, ce qui rend les choses très compliqués à la lecture et peut conduire à un fichier de trace trop volumineux. Il faut donc utiliser des filtres de capture afin de mieux cibler le trafic réseau à enregistrer.

   Quelques mots clés pour écrire des filtres de capture :

   « port X » permet de capturer le trafic en provenance ou à destination du port numéro X ; « tcp » capture le trafic TCP ; « udp » le trafic UDP ; « host adresse_IP_ou_nom_de_machine » capture le trafic en provenance ou à destination de l'adresse ou nom de machine donné ; « net » capture le trafic en provenance ou à destination de l'adresse réseau spécifiée.

   Il est possible de précéder les mots clés « port », « host », « net » par les mots clés « src » et « dst » pour capture uniquement le trafic en provenance et à destination respectivement de l'argument donné.

   Les opérateurs logiques « and » et « or » permettent de créer un filtre avec de multiples expressions, et « not » de trouver le complément d'une expression. L'utilisation de parenthèses permet également de définir l'ordre d'évaluation de filtres.

   - Expliquez à quoi sert donc la commande « tcpdump "tcp port 80" -i *yourIface* -w /tmp/test2.1.pcap », où « tcp port 80 » est en fait le filtre de capture.

   On capture tous les paquets TCP en provenance ou à destination du port 80. En d'autres termes, on capture le trafique HTTP.

   - Quel filtre de capture permet de capturer uniquement le trafic DHCP ? quel filtre utiliser pour capturer le trafic DNS ?

   DHCP = UDP and (port 68 or port 67)
   DNS = port 53

   - Comment capturer le trafic en provenance ou à destination de la machine www.unice.fr ?

   host www.unice.fr

   - Comment capturer le trafic à destination du réseau 134.59.1.0/24 ?

   dst net 134.59.1.0/24

   - Comment capturer tout le trafic qui n'est pas de type ICMP (ICMP est le protocole qui vous permet de faire un ping –entre autres–) ?

   not icmp

3 Le protocole DHCP

Comme on l'a vu en cours, le protocole DHCP permet d'obtenir de manière automatique des informations nécessaires pour devenir un membre actif du réseau.

3. Nous allons « jouer » avec le protocole DHCP. Exécutez :

- POX avec la commande « $ ./pox.py proto.arp_responder --192.168.0.254=00:00:00:00:00:FE proto.dhcpd forwarding.l2_learning ». Laissez POX s'exécuter
- Dans un autre terminal, exécutez Mininet : $ sudo mn --controller=remote »
- Ouvrez un terminal pour le client « h1 » (client deployez par mininet) : « xterm h1 », et dans ce terminal exécutez « # ip a del 10.0.0.1/8 dev h1-eth0 » pour effacer l'adresse IP automatiquement donné à h1 par mininet. Vérifiez qu'il n'y a plus d'adresse IP pour h1. Quelle commande utiliser ? Laissez la fenêtre xterm ouverte.

ip a s

- Ouvrez une 2ème fenêtre xterm pour h1. Puis, exécutez tcpdump avec un filtre permettant de capturer uniquement le trafic DHCP. Tcpdump doit garder les paquets *sniffés* dans le fichier « h1.pcap », dans l'espace personnel de votre utilisateur. Quelle commande utiliser ? **Laissez tcpdump tourner.**

tcpdump -i h1-eth0 "udp port 67" -w h1.pcap

4. Exécutez la commande « dhclient -v h1-eth0 » dans le premier xterm ouvert pour h1 (tcpdump sniffe toujours le réseau). A la fin de l'exécution de la commande dhclient, fermez tcpdump avec « Ctrl + c ». Vérifiez que le nombre de paquets capturés par tcpdump est > 0.
   - Dans la VM (en dehors de mininet, **mais surtout, ne pas arrêter mininet !**), ouvrez le fichier h1.pcap avec Wireshark. Le moyen le plus simple est d'utiliser l'explorateur de fichier est faire un double click sur ce fichier. Automatiquement wireshark ouvrira h1.pcap
   - Quels paquets ont été envoyés suite à votre commande dhclient ?

   DHCP Discover, DHCP Offer, DHCP Request, DHCP Ack

   - Quels paquets ont été envoyé en mode broadcast et quels paquets ont été envoyé en mode unicast (i.e. paquets dont l'adresse de destination es la 255.255.255.255) ? Expliquez brièvement, par paquet, pourquoi ils sont envoyés en broadcast ou unicast.

   DHCP Discover – Broadcast, afin de détecter tous les serveur DHCP du réseau
   DHCP Offer – unicast. Même si le client ne possède pas d'adresse IP, sa carte réseau possède une adresse matériel (l'adresse MAC), qui permet de l'idéntifier.
   DHCP Request – Broadcast. Si plusieurs serveur DHCP font une offre, ce paquet permet de faire comprendre à tous quel serveur a été choisi
   DHCP Ack – Unicast. Confirme l'assignation de l'adresse IP

   - Comment trouver, grâce à wireshark l'adresse IP proposée par le serveur dans le message DHCP Offer ? Combien de temps pouvons nous garder cette adresse IP (trouver l'option « IP Address Lease Time ») ?

   C'est dans le champ « your (client) IP address ». La période d'utilisation de cette offre est de 1 heure. « IP Address Lease Time » donne cette période en nombre de secondes.

   - Quel routeur, serveur DNS, nom de domaine sont fourni par le serveur DHCP ?

Pour trouver cette information, sur wireshark : « Routeur », c'est l'option 3 du protocole DHCP, « serveur DNS » option 6 et « nom de domaine » c'est l'option 15

5. Quels sont les ports d'écoute du client et du serveur ? Analyser les lignes « User Datagram Protocol » des paquets sur Wireshark (sous-fenêtre centrale).

   Client 68, Serveur 67

6. Expliquez comment les mécanismes du protocole DHCP peuvent être utilisés pour introduire de sérieux problèmes de sécurités dans un LAN.

   Vu qu'aucun mécanisme d'identification du serveur n'est pas implémenté côté client, c'est assez simple de mettre un serveur DHCP dans un réseau donnant des adresse IP des serveurs DNS et routeurs compromis. De plus, rarement les utilisatreurs·ices des ordinateurs vérifient ou peuvent vérifier que les informations données par le serveur DHCP sont celles attendues.

7. (Optionnel) en capturant à nouveau le trafic DHCP sur h1, exécutez sur h1 la commande « dhclient -r *yourIface* ». Quel paquet à été envoyé suite à votre commande ?

   DHCP Release. C'est le paquet qui indique au serveur que le client efface la configuration fournie

8. Quittez Mininet et POX.

4 Le protocole DNS

Nous avons vu en cours que le protocole DNS permet la traduction des noms canoniques de machines en adresse IP. Cependant, le service DNS permet d'autres opérations très courantes également, comme l'obtention du serveur SMTP d'un domaine. Nous allons illustrer maintenant avec quelques exercices les principaux services fournis par le protocole DNS.

Les prochains exercices se font dans la VM, sans exécuter Mininet.

9. Avec la commande « nslookup -querytype=A www.univ-cotedazur.fr » obtenez l'adresse IPv4 du serveur www.univ-cotedazur.fr.
   - Donnez l'adresse IPv4 du serveur

   134.59.204.162

   - Avez-vous trouvez que la réponse provient d'un serveur « Non-authoritative » ? expliquez pourquoi

   La réponse provient d'un serveur sans autorité dans le domaine. Nous voyons bien que l'adresse IP sur serveur DNS et la 127.0.0.53 (machine locale). Ceci veut dire que la requête exécutée par nslookup est répondu par l'information DNS en cache de notre machine locale.

10. Avec nslookup et le type de requête (-querytype) approprié, essayez d'obtenir l'adresse IPv6 du serveur www.univ-cotedazur.fr. Il y a-t-il une adresse IPv6 associé à ce serveur ?

    -querytype=AAAA. La réponse ne comportant pas d'adresse IPv6, et sans message d'erreur apparent de la commande nslookup, on peut déduire qu'il n'y a pas d'adresse IPv6 associé à ce serveur.

11. Pour obtenir le serveur DNS d'un domaine, on utilise une requête NS. Expliquez pourquoi les commandes « nslookup -querytype=NS www.google.com » et « nslookup -querytype=NS google.com » produisent des résultats distincts.

    www.google.com est un FQDN d'une machine. Une machine ne possède pas de serveur DNS. Ce sont les domaines qui possèdent (sont administrées avec) un DNS. « unice.fr » est un domaine qui possède donc un serveur DNS

12. Comment faire pour obtenir l'adresse IPv4 du serveur recevant les emails dans une organisation ? essayez avec un nom de domaine pris au hasard.

    On utilise -querytype=MX pour trouver le nom du serveur SMTP du domaine. Puis, -querytype=A pour trouver l'adresse IP de l'un des serveurs trouvés précédemment.

5 Le protocole HTTP

Pour étudier le protocole HTTP, nous aurons besoin d'un client web : c'est-à-dire, un navigateur web. Pour cette séance, nous utiliserons le navigateur wget, qui est un navigateur web en ligne de commandes qui peut être manipulé finement. L'utilisation d'un navigateur graphique est déconseillée car souvent ils téléchargent des ressources non demandées.

13. Utilisez tcpdump pour enregistrer uniquement le trafic TCP et UDP. Puis, exécutez la commande « wget http://www.i3s.unice.fr/~lopezpac --max-redirect=0 ». A la fin de l'exécution de wget, arrêtez la collecte de trafic et analysez la trace avec wireshark

    - Décrivez l'échange qui a lieu suite à votre commande, entre votre VM et les serveurs.

    On retrouve des requêtes DNS de type A et/ou AAAA pour retrouver l'adresse IPv4 ou IPv6 du serveur. Suite à l'obtention de l'adresse IPv4 de www.i3s.unice.fr, on établit une connexion TCP avec ce serveur pour télécharger une ressource.

14. Identifiez le paquet TCP contenant la requête HTTP.

    - Donnez cette requête en respectant les majuscules, minuscules, espaces et lignes vides.

```
GET /~lopezpac HTTP/1.1
... plusieurs lignes...
Host: www.i3s.unice.fr
Connection: Keep-Alive
<ligne vide = \r\n>
```

    - Donnez la liste d'en-têtes qui ont été ajoutés à ce paquet HTTP et la taille en octets de chaque en-tête, jusqu'à l'en-tête Ethernet (ou MAC).

    En-tête TCP 20 octets, en-tête IP 20 octets, en-tête Ethernet 14 octets visibles.

    - Donnez la réponse donnée par le serveur. Respectez les majuscules, minuscules, espaces et lignes vides.

    Procédure similaire au premier point de cet exercice. Question entièrement à la charge de l'étudiant.

15. Lors de l'exécution de la commande wget de l'exercice 13

    - Avez-vous effectivement obtenu le site de l'université ?

Par la trace wireshark, nous pouvons observer que la réponse HTTP possède un code d'erreur « 301 Moved Permanently ». Nous n'avons donc pas obtenu la ressource demandée. Uniquement un code de « 2XX » indique un code de retour de succès. Un code « 3XX » indique que la ressource se trouve à une autre adresse.

- si oui, expliquez brièvement le contenu de la page reçue. Sinon, comment faire pour obtenir via wget la page recherchée ?

On voit par la capture wireshark que la ressource est disponible a l'adresse http://www.i3s.unice.fr/~lopezpac/ (notez le « / » à la fin). Il ne reste qu'à exécuter « wget http://www.i3s.unice.fr/~lopezpac/ » pour enfin retrouver la ressource recherchée.