Création le : 24/03/2021
Quentin Giorgi.

TP – Observation et détermination des caractéristiques de l'implémentation du NAT dans Netfilter pour des flux UDP.

Préparation et recommandations

Pré-requis :

La bonne compréhension des TPs précédents est nécessaire.
Connaître les commandes UNIX suivantes : netcat, tcpdump, sysctl.

Travail à effectuer :

Lire la RFC 4787 concernant le comportement du NAT pour UDP.
Notamment lire attentivement les chapitres 1 à 4 (inclus)

Présentation du TP.

Introduction

La RFC4787 indique un certain nombre de comportements possibles et recommandés pour le comportement d'une « NAT BOX ». Vous allez à travers un projet Marionnet, vérifier le comportement de Netfilter par rapport à cette RFC.

Pour cela, lancez marionnet, chargez le projet TP-NAT-UDP.mar et lancez tous les éléments via le bouton « Start All ».

Le projet ressemble à l'architecture donnée à la page 8 de la RFC. (4.2.1)

L'objectif de cet exercice est d'indiquer les manipulations que vous avez réalisées pour déterminer les réponses aux questions suivantes, merci donc d'indiquer pour chaque question :
- la configuration du NAT ,
- les commandes exécutées sur les clients,
- les commandes exécutées sur les serveurs,
- et les observations permettant de répondre à la question.

Sous la forme de l'exemple suivant :

NAT	nft add 'chain ip nat sortie {type nat hook postrouting priority 100 ; } ;' nnft add rule ip nat sortie oifname "eth0" counter snat to 193.23.23.128-193.23.23.144
Clients :	X1 : nc -u -p 10000 193.22.22.1 8000 X2 : …

Serveurs	Y1 : tcpdump -i eth0 -n udp Y2 : …
Observations:	NAT : conntrack -L … …
Conclusions :	

Question 1 : (4.1 Address and Port Mapping)

A quel comportement (Endpoint-Independent Mapping, Addess-Dependent Mapping, Address and Port-Dependent Mapping) l'implémentation est-elle conforme ?

Question 2 : (4.1 Address and Port Mapping)

A quel comportement de « pooling » (paired ou Arbitratry) l'implémentation est-elle conforme ? Y a t-il des observations particulières ?

Question 3 : (4.2 Port Assignement)

L'implémentation fait-elle du « port preservation » ?

Question 4 : (4.2 Port Assignement)

Quel est le comportement en cas de « port collision », est-ce différent selon le cas où le NAT possède un pool d'adresses utilisables et non pas une seule ?

Question 5 : (4.2 Port Assignement)

Quel « range » de ports est utilisé en cas de « collision » (dynamic/well-known/registered) ?

Question 6 : (4.2.2 Port parity)

L'implémentation fait-elle du « port parity » ?

Question 7 : (4.2.3 Port contiguity)

L'implémentation fait-elle du « port contiguity » ?

Question 8 : (4.3 Mapping refresh)

Quelle est la valeur du délai d'expiration d'un mapping UDP ? Est-ce le même quelque soient les échanges effectués entre le client et le serveur ? Est-ce conforme à la recommandations ?

Question 9 : (4.3 Mapping refresh)

La valeur du délai d'expiration est-elle différente pour des ports destinations dans le « range well-known » ?

Question 10 :

Ces valeurs de délais d'expiration sont elles réglables ? Si oui comment ?

Question 11 :

Quelle est la valeur du « NAT Outbound refresh behavior »

Question 12 :

Quelle est la valeur du « NAT Inbound refresh behavior »