Rapport de projet IngProt – TFTP

Elbez Samuel 21200353
Stasyszyn Romain 21305734

Remarques générales **:**

Pour ce projet, nous avons choisi de traiter le protocole TFTP (Trivial File Transfert Protocol). Nous nous sommes documentés auprès des RFC 1350, 2347, 2348, 2349 traitant de ce protocole. Pour être plus précis, les deux RFC qui nous ont été indispensables sont :

- la RFC 1350 (https://tools.ietf.org/html/rfc1350) pour le traitement général.
- la RFC 2347 (https://tools.ietf.org/html/rfc2347) pour la gestion des options.

Au niveau du code, nous sommes partis d'une base que nous avons trouvée sur Github :
https://github.com/loic-hourdin/wireshark-in-C-with-TCPdump

Pour que le projet fonctionne il faut installer *libpcap* (libpcap0.8-dev).
A noter que nos ajouts à ce projet déjà existant sont principalement les fichiers tftp(.c/.h) ceci afin d'afficher les informations relatives au protocole TFTP.

Pour ce qui est des tests, ils ont été réalisés avec des fichiers pcap fournis sur le site indiqué dans le sujet, les fichiers *tftp-rrq.pcap* et *tftp-wrp.pcap* sont plus simples que *tftp-dup.pcap* car utilisant uniquement la RFC 1350. Il en résulte, que le troisième fichier qui utilise une extension de TFTP, contient des données cryptées, des erreurs, des OACK ainsi que des informations parasites que nous n'avons pas traitées (choix d'implémentation) rend le résultat un peu moins lisible mais tout aussi concluant.

Compilation **:**

Pour build le programme : **make**
Pour lancer le programme normalement : **sudo ./analyse example.pcap**
Pour lancer le programme en mode verbeux : **sudo ./analyse -v example.pcap**

Implémentation **:**

Nous traitons les types de paquets suivants : RRQ (Read Request), WRQ (Write Request), DATA (Data), ACK (Acknowledgement), ERROR (Error), OACK (Option Acknowledgement).
Pour les requêtes nous affichons : le mode, le format, le nom du fichier.
Pour les paquets, nous affichons : l'IP source, l'IP destination, le port utilisé par la source, le port utilisé par la destination, la taille du paquet, le type du paquet et le numéro du bloc.
Pour ce qui est des options dans les paquets de type OACK, nous affichons aussi la taille du bloc (*blksize*) ainsi que la taille de transfert (*tsize*).