Rapport capture trafic réseau.

Rapport rédigé par : Fabrice Bodson  
Date de rédaction : 13/10/2020  
Date et heure de début de la capture : 15/09/2020 à 00h 15m 57s,179957000

Date et heure de fin de la capture : 15/09/2020 à 00h 18m 12s,822894000

Nombre de trames capturées : 317

Protocoles capturés : icmp, arp, tcp, dns, telnet, ssdp, sshv2, dhcp

La commande ping a été envoyée et on constate un échange entre la source et le destinataire.

Une image contenant table

Description générée automatiquement

En date du 13/10/2020, à 12h10m25s, nous pouvons déduire que l’utilisateur a exécuté la commande « ping » à partir de la machine à l’adresse IP 192.168.169.128.

Avec le filtre « telnet » activé, on remarque un échange et on sait voir ce qui est envoyé au clavier car le serveur fait un echo de ce qu’il reçoit. On sait donc lire l’email administrateur et le mot de passe entré et le message « Hello HELMo ». La communication se fait donc en clair sur le réseau.

Il y a 94 trames correspondant au protocole telnet. La session débute à 00h 16min 26s,448912000 et se termine à 00h 17min 15s,028586000.

Le port TCP du protocole telnet est le 23.

On sait lire en clair le login ( **., .msfadmin**) et le mot de passe (**msfadmin**) d’un compte qui semble administrateur ainsi qu’un message affiché.

Il y a 72 trames correspondant au protocole ssh. La session débute à 00h 17min 44s,636043000 et se termine à 00h 18min 12s,822186000.

Le port TCP du protocole ssh est le 22.

On constate que les informations qui transitent sont cachées et sécurisées et donc illisibles. Il est évident que le protocole ssh est mieux que le telnet qui laisse les messages transiter en clair sur un réseau.