Semaine 7: Analyse de paquets
IPL I317B Sécurité : labo

Cedric Niyikiza
Questions

L'adresse ip 92.242.140.21 a eu une drôle d'activité, en regardant tous les paquets de cette ip, pouvez-vous en déduire son comportement ?

Tout d'abord le protocole ICMP (Network LAYER) est un protocole de bas niveau qui permet aux machines de communiquer entre-elles.

Ce qu'on peut constater c'est qu'une seule adresse IP tente de "tester", de voir, si des machines existent et répondent à ces appels PING. Et ci ces pings venaient à avoir une réponse il aurait une réponse sur quelles machines du réseaux il pourrait communiquer voir lancer une attaque.

L'adresse ip 192.168.11.62 a eu une drôle d'activité, en regardant tous les paquets de cette ip, pouvez-vous en déduire son comportement ?

Protocole : TCP

Tout d'abord dans ce problème ci on a deux adresses qui rentre en jeu.
```SOURCE : 192.168.11.62```

Source qui tente de communiquer avec une adresse par tous les moyens et sur différents de ces ports. ```DESTINATION : 192.168.11.46```

Qu'est ce que je peux déduire de ces évenements:

- La **_source_** tente par tous les moyens de communiquer avec la destination
- La **_destination_** à l'air d'être éteinte ou de refuser toute communication avec cette adresse IP (*source*) en particulier

On pourrait se demander ce que la *source* tente de trouver chez la destination
- Surment tenter de chercher une application qui tourne sur un des ports pour ensuite l'attaquer.

(La source fait un _scan_ sur l'adresse IP de la destiation)
Un paquet peut en cacher un autre ... </br>Pour cette exercice, nous allons nous intéresser aux paquets échangés entre 92.68.122.132 et 184.168.221.63.
1. Quel est l'unique type de paquet échangé ?
   - PING ICMP (0 et 8)
2. La taille de certains paquets ne vous semble-t-elle pas un peu grosse pour ce type de paquet ? Qu'y a-t-il dans les paquets plus gros ?

    Les tailles des paquets varient du à leurs contenues
    Dans les paquets les plus gros on a des data en ASCII
3. Pourquoi donc quelqu'un ferait-il ça ?
   a. **_Premier Scénario_** : la source et destination sont une est même personne
```

        et cette dernière utiliserait des PING ICMP pour encapsuler d'autres paquets.
        Pour contourner des limitations réseaux par exemple
   b. **_Second Scénario_** : Dans le but de cacher ces actions SSH au sein de son réseau pour que ce ne soit pas vu comme de l'SSH de l'extérieur

La plupart du temps, les protocoles ont leur contenu séparé dans plusieurs paquets et les lire un par un pour essayer de dégager le sens général de l'échange est fastidieux. Pour régler ce problème, intéressons nous maintenant à la fonctionnalité de Wireshark « follow : tcp-stream ». Celle-ci permet de rassembler le contenu de plusieurs paquets.En scrollant un peu dans ce pcap, vous devriez voir des paquets du protocole IMAP (mail), effectuer un clique-droit, « follow : tcp-stream ». Que constatez-vous ?

Que quelqu'un a tenter d'envoyer un mail de fishing

Un peu plus loin, vous pouvez trouver du trafic SMB avec un serveur SMB qui semble se trouver sur 192.168.1.8, procédez à l'inspection du tcp-stream comme nous l'avons vu à l'exercice précédent.

Apparement le contenu malvaillant à été téléchargé par la victime, elle a cliquer sur le lien.

Avec quelques autres suivis de tcp-stream, vous pouvons continuez à analyser cette histoire, que ce passe-t-il ensuite ...