TP

Sécurité des réseaux

10 janvier 2023

1 Modèle OSI ↔ Modèle TPC/IP

I. (8 points) **Modèle OSI**

(1) Modèle OSI :

- Quelles sont les couches les plus importantes du modèle OSI? Quel est leur rôle?
- Quels sont les équipements caractéristiques de ces couches?
- À quoi servent-ils?

(2) Décrivez une connexion TCP ainsi qu'une connexion UDP, éventuellement en vous appuyant de schémas.

- Que se passe-t-il en cas de port TCP inaccessible (envoi d'un paquet SYN vers un port où n'écoute aucun service?)
- Idem pour un port UDP? Dans ce dernier cas, la séparation en couches préconnisée par le modèle OSI est-il respecté?

2 Man-in-the-middle!

I. (5 points) **Fonctionnement du protocole ARP**

(1) Videz la table ARP de votre système et affichez-là. Écoutez le trafic réseau à partir de *wireshark*. Après avoir contacté quelques adresses (à partir par exemple de votre navigateur), affichez de nouveau la table ARP de votre système.

- Comment la table ARP s'est-elle remplie? Quels sont les paquets réseau mis en jeu? Avez-vous pus capturer les paquets ARP en question? Quels sont les différents champs?
- À quoi sert cette table? Quel est son fonctionnement?
- Proposez un schéma permettant de comprendre les échanges niveaux 2 ayant lieu à partir du protocole ARP.

(2) Au niveau sécurité :

- Une authentification est-elle mise en place?
- Un état est-il maintenu?
- En s'appuyant sur le fonctionnement de ce protocole, proposez un mécanisme permettant d'usurper le trafic de votre binôme depuis et vers une adresse IP légitime ciblée. Un schéma est le bienvenu!

II. (7 points) **Exploitation des faiblesses du protocole ARP**

(1) Écrivez un script python utilisant scapy pour réaliser le *man-in-the-middle* Pour cela, vous pouvez découper votre code en fonctions :

- `def get_mac(IP, interface):`
  Pour obtenir l'adresse MAC à partir de l'adresse IP
- `def trick(interface, victim_IP, router_IP):`
  Pour spoofer les adresses du routeur et de la victime
- `def reARP(interface, victim_IP, router_IP):`
  Pour rétablir la vérité une fois l'attaquer terminée!

Si le cache ARP de la victime associe l'adresse IP de la passerelle à l'adresse MAC de l'attaquant, c'est bien joué! Cependant, le noyau Linux ne fonctionne pas comme un routeur par défaut. Il est encore nécessaire d'activer les fonctions de routage sur le système de l'attaquant :

```
echo 1 > /proc/sys/net/ipv4/ip_formward
```

(2) Pouvez-vous observer le trafic réseau de la victime à partir de Wireshark?

(3) **Question chasseurs de points : Observez les échanges réseau lors du *man-in-the-middle* avec votre outil. Régulièrement, un paquet de signalisation ICMP est émis. À partir de quelle machine? À quoi sert ce paquet? En quoi risque-t-il de faire échouer l'attaque?**

(4) Quelles recommandations pouvez-vous formuler pour améliorer la sécurité d'un SI et vous protéger de ce type d'attaque?