École Polytechnique de Montréal

Département de génie informatique et génie logiciel

INF4420a - Sécurité Informatique

Travail Pratique 3

Automne 2022

Table des matières

1 Directives **2**

2 Scénario **2**

3 Analyse de traces réseau [/5] **2**

4 Reconnaissance [/5] **3**

5 Mise en œuvre de l'attaque [/10] **3**
5.1 Empoisonnement ARP [/4] 3
5.2 Usurpation d'adresse IP [/2] 3
5.3 Machine in the Middle [/4] 3

6 Investigation numérique [/5] **4**

7 Attaque de l'infrastructure docker [3 points bonus] **4**

1 Directives

Tous les travaux devront être remis avant 23h55 le jour de la remise sur le site Moodle du cours. À moins que cela ne soit explicitement demandé dans le sujet, vous ne devez remettre qu'un fichier PDF nommé selon le format TPX-matricule1-matricule2.pdf. Vous pouvez inclure des annexes dans votre rapport si vous jugez que cela améliore la lisibilité (code source, ...)

- Voir la date de remise du rapport de ce laboratoire dans le plan du cours.
- Le travail devra être fait par équipe de deux. Toute exception (travail individuel, équipe de trois) devra être approuvée au préalable par le professeur.
- L'orthographe et la forme seront prises en compte pour chaque question.
- Indiquez toutes vos sources d'information, qu'elles soient humaines ou documentaires.

NOTE : POUR TOUTES LES QUESTIONS, VOUS DEVEZ MONTRER COMMENT VOUS AVEZ OBTENU LES RÉPONSES, INCLUANT DANS VOTRE RAPPORT LES CAPTURES D'ÉCRAN MONTRANT LES COMMANDES UTILISÉES ET LEUR SORTIE.

2 Scénario

Votre équipe à été mandatée pour réaliser un audit de sécurité de Rainbowtech, une entreprise spécialiste dans la conception d'instruments de mesure médicale connectés de haute précision. La compagnie à récemment subit une vague de cyberattaques suite à l'annonce de leur lecteur de glycémie non invasif basé sur des analyses optique et de l'intelligence artificielle. Les fonctionnalités de leur infrastructure informatique ont été restaurées, mais l'équipe d'administration système craint que les pirates aient laissé des portes dérobées dans certaines des machines.
Votre mission est de retracer leurs pas et de déterminer les failles qui ont été utilisées afin de les corriger pour se prémunir contre de prochaines attaques.

3 Analyse de traces réseau [/5]

Pendant l'attaque, des communications réseau suspectes vers l'extérieur sont été enregistrées en provenance d'un des serveurs de l'entreprise. Le serveur est placé derrière un pare-feu restrictif qui interdit l'accès aux sites web qui ne sont pas pré approuvés par l'équipe d'administration système pour éviter les fuites de données sensibles.
Les traces réseau sont disponibles sur Moodle dans le fichier `capture.pcap`.

1. [/1] Ouvrez le fichier de capture avec Wireshark[1]. Quelle est l'adresse ip machine source des paquets envoyés ? Quelle est l'adresse IP de destination ? De quel protocole s'agit-t-il ?
2. [/2] Des données sensibles ont-elles été exfiltrées ? Si oui, retrouvez le contenu du fichier exfiltré.
3. [/2] À votre avis, pourquoi le protocole DNS n'est-il pas bloqué par le pare-feu de l'entreprise ? Expliquez la méthode utilisée par les pirates pour exfilter des informations.

4 Reconnaissance [/5]

Vous soupçonnez les pirates d'avoir d'abord infecté le poste d'un·e employé·e de Rainbowtech via des techniques de hameçonnage avant de s'être propagé·e·s dans le reste du réseau. L'équipe informatique vous a fourni des identifiants de connexion SSH pour une machine Kali Linux[2] située sur le réseau des employé·e·s.

Lancez la machine virtuelle `TP3` disponible dans `/home/INF4420a/A2022/TP3/` et connectez vous en SSH à la machine Kali Linux en utilisant la commande `ssh root@localhost -p 2222` et le mot de passe `password`.

En utilisant des outils de découverte réseau comme nmap[3], construisez un schéma du réseau de Rainbowtech. Indiquez les noms des machines, leurs adresses IP ainsi que les services exposés et leurs versions. Vous serez amené·e à compléter votre schéma au fur et à mesure que vous avancez dans le TP et que vous découvrez des machines et des ports ouverts.

Note : vous pouvez ignorer les adresses `10.22.*.1` qui représentent les connexions au réseau de docker utilisé pour héberger l'infrastructure du TP ainsi que le port `2222` qui est utilisé pour la connection ssh à la machine Kali Linux.

5 Mise en œuvre de l'attaque [/10]

5.1 Empoisonnement ARP [/4]

1. [/2] En utilisant arpspoof[4], effectuez une attaque d'empoisonnement ARP sur la machine de Alice. Avec vos mots, expliquez comment fonctionne cette attaque.[5]
2. [/0.5] Utilisez tcpdump[6] pour capturer pendant quelques minutes les communications réseaux de la machine de Alice au format `pcap`.
3. [/0.5] Analysez votre capture avec Wireshark[1] (Vous pouvez utiliser la commande `scp` pour récupérer votre fichier de capture). Quels protocoles observez-vous ? Avec quelles machines Alice communique-t-elle ?
4. [/1] Récupérez l'identifiant et le mot de passe du serveur FTP auquel se connecte Alice. Essayez de vous connecter à ce serveur. Est-ce possible ? Pourquoi ?

5.2 Usurpation d'adresse IP [/2]

1. [/0.5] Quelle est l'adresse IP de la machine de Alice ?
2. [/1] Usurpez l'adresse IP de Alice. Connectez vous ensuite au serveur FTP et récupérez le fichier `password.txt`.
3. [/0.5] Quel est le mécanisme qui empêchait de se connecter au serveur dans la partie 5.1.4 ? Est-ce un mécanisme de sécurité efficace ?

5.3 Machine in the Middle [/4]

1. [/0.5] Il semble qu'Alice grade des copies de ses fichiers de configuration sur le serveur FTP. Récupérez la configuration de son client SSH.

2. [/1.5] Identifiez les vulnérabilités présentes dans cette configuration. Que pourriez-vous faire comme attaque ? Expliquez précisément.
3. [/2] Utilisez SSH-MITM[7] pour réaliser une attaque Machine in the Middle sur la connexion SSH de Alice et prendre le contrôle du serveur.

Note : pour rediriger les connexions qui arrivent sur le port 22 de votre machine Kali Linux sur le port 10022 utilisé par SSH-MITM, vous pouvez utiliser la commande iptables suivante :

```
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 22 -j REDIRECT --to-port 10022
```

6 Investigation numérique [/5]

1. [/1] Connectez vous au serveur FTP en utilisant la méthode vue en 5.2.2. En remarquant qu'il est possible d'écrire des fichiers arbitraires sur le serveur, ajoutez la clé publique SSH de votre machine Kali Linux à la liste des clés autorisées pour se connecter au compte d'Alice et connectez vous en SSH au serveur.[8]
2. [/1] Retrouvez la porte dérobée laissée par les pirates.[9]
3. [/2] Transférez le programme de porte dérobée sur la machine Kali Linux et analysez le à l'aide de radare2[10]. Que fait ce programme ? Que se passe-t-il lorsqu'il est exécuté sur la machine du serveur ?[11]
4. [/1] En utilisant la porte dérobée, devenez root et récupérez le fichier `steal_secret`. Que fait ce programme ?[12]

7 Attaque de l'infrastructure docker [3 points bonus]

L'infrastructure du TP tourne sur docker. Une vulnérabilité importante est présente dans la configuration de docker qui permet de briser la conteneurisation et prendre le contrôle de l'hôte. À vous de trouver cette vulnérabilité et de l'exploiter pour prendre le contrôle de la machine virtuelle et lire le fichier `/congratulations.txt`. Cette question rapporte 3 points bonus sur le TP.

Indice : des informations qui pourraient vous êtes utiles ont été cachées dans la photo de Jalapeño, le chaton d'Alice.[13]

Références

[1] **wireshark** => https://www.wireshark.org/

[2] **Kali Linux** => https://www.kali.org/

[3] **nmap** => https://nmap.org/

[4] **arpspoof** => https://www.monkey.org/~dugsong/dsniff/

[5] **ARP Spoofing Tutorial** => https://www.javatpoint.com/arp-spoofing-using-arpspoof

[6] **tcpdump** => https://www.tcpdump.org/

[7] **SSH-MITM** => https://docs.ssh-mitm.at/

[8] **ssh-keygen** => https://www.tutorialspoint.com/unix_commands/ssh-keygen.htm

[9] **Privilege Escalation Tutorial** => https://medium.com/go-cyber/linux-privilege-escalation-with-suid-files

[10] **radare2** => https://rada.re/n/radare2.html

[11] **Radare2 Tutorial** => https://stackrip.github.io/blog/radare-1/

[12] **dnsteal** => https://github.com/m57/dnsteal

[13] **steghide** => https://steghide.sourceforge.net/