TD

Sécurisation d'un système Linux

28 janvier 2023

1 Découverte des cibles - Rappel TP OSINT

I. (2 points) **Scan réseau**

(1) À partir du tunnel VPN, rechercher les services installés sur le serveur d'adresse IP `172.31.7.83`!

- De manière à contacter de manière sûre les serveurs vulnérables, nous allons nous connecter en VPN. Pour cela, récupérez le fichier de configuration VPN [1] et lancez openvpn à partir de la commande `sudo openvpn cours.ovpn`.
- Quelles routes sont désormais accessibles ? Quels hôtes sont joignables ? Quels services sont accessibles ?
- Quelle technique utilise `nmap` pour détecter un hôte ?
- Quelle stratégie utilisez-vous pour découvrir efficacement les hôtes présents sur le réseau ?

2 Serveur WriteHat

II. (4 points) **À partir d'Internet**

- En utilisant `patator`, ou un autre outil permettant de bruteforcer l'accès SSH, expliquer comment vous parvenez à obtenir les authentifiants nécessaires pour vous connecter sur le serveur !

III. (4 points) **À partir d'un compte sans privilège**

Vous disposez désormais d'un compte sur le serveur d'adresse IP 172.31.7.83 :

- `student` : mot de passe ???
- `chibollo` : mot de passe ???

(1) Élevez vos privilèges vers le compte `root` en exploitant localement les vulnérabilités relatives à la configuration de l'utilitaire `sudo`

- Quelle vulnérabilité avez-vous exploitée ?
- Quel principe général pouvez-vous énoncer pour déterminer si une commande présente dans la configuration de `sudo` peut présenter des risques d'élévations non maîtrisées ?
- Quelles recommandations proposer à l'administrateur système pour améliorer la sécurité de cet utilitaire ?

1. `https://cours.pelicanux.net/static/conf/cours.ovpn`

(2) **Question bonus chasseurs de points (+8pts) : Concernant le serveur WRITEHAT, une autre vulnérabilité permet à l'utilisateur `chibollo` d'obtenir les privilèges `root`. Pour cela, vous devrez vous appuyer sur une action que réalisera l'administrateur légitime de la machine tôt ou tard, en vous aidant de la configuration vulnérable d'un service non présent de manière standard sur un système Linux.**
- Les services sont définis dans le répertoire `/etc/systemd`,
- Pouvez-vous trouver la vulnérabilité en question et l'exploiter ?

3 Serveur backup

IV. (3 points) **Découverte d'un second backup et connexion !**

(1) Une fois l'accès privilégié obtenu sur le serveur WRITEHAT :
- Quelles actions entreprenez-vous pour découvrir et atteindre un second serveur ?
- Quelles recommandations proposeriez-vous au défenseur, pour utiliser le script `rsync.sh` de manière sécurisée ?

V. (3 points) **Différentes techniques d'élévation de privilèges à partir d'une configuration vulnérable de sudo**

(1) Quelles sont les différentes vulnérabilités constatées concernant la configuration de l'utilitaire `sudo` ?
- *backup1* → *backup2* : `/usr/bin/find`
- *backup2* → *backup3* : `/usr/bin/man`
- *backup3* → *backup4* : `/bin/cat`
- *backup4* → *backup5* : `/bin/date`

(2) Les mots de passe des différents utilisateurs sont identiques à leur identifiant :) ce qui vous permet de basculer d'un utilisateur à l'autre si vous êtes bloqués sur une élévation en particulier à partir de la commande `su - backup3` par exemple pour changer d'utilisateur pour `backup3`.

4 Root sur le serveur backup !

VI. (4 points) **Confinement dans le script de supervision !**

(1) Le compte `backup5` permet de se connecter en SSH en tant qu'utilisateur `root` sur le serveur lui-même. Cependant, vous vous retrouvez confinés (le mot est à la mode...) sur l'exécution d'un script qui ne nous présente pas un immense intérêt dans notre quête.
- Quelle méthodologie vous permet de contourner la sécurité mise en place ?
- Une fois les privilèges `root` obtenus, pouvez-vous expliquer quel mécanisme a permis de vous contraindre à l'exécution de ce script ?
- Quelles recommandations pouvez-vous formuler au défenseur ?