Mise en place d'un serveur web sécurisé

INITIATION A LA SECURITE WEB (ATTAQUE ET DEFENSE)

CEDRIC BERTRAND

1 Identification

Nom étudiant : xxxxxxxxxxxxxxx

Note : /23

2 Sommaire

3 Sécurité

3.1 Exploitation de vulnérabilités (13 pts)

Cette version de Joomla souffre de plusieurs vulnérabilités dont une injection sql et la possibilité de créer un compte utilisateur privilégié.

3.1.1 Joomla (6 pts)

3.1.1.1 Création d'un utilisateur avec les droits privilégiés

Exploiter la vulnérabilité cve-2016-8869 pour créer un utilisateur avec des droits privilégiés (Url pour enregistrer un utilisateur : http://<ip>/joomla/index.php/log-out?view=registration)

CVE : https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8869

Exploiter la vulnérabilité avec Burp/Zap : 2 pts

3.1.1.2 L'injection SQL

Exploiter l'injection sql avec le logiciel sqlmap et récupérer l'ensemble des utilisateurs Joomla (1 pt)

Trouver le mot de passe de l'utilisateur « joomla_root» (1 pt) (utiliser le fichier weaksauce.txt avec des règles john)

Indication : le mot de passe est de la forme : <mot_en_minuscule>[0-9][0-9][0-9] (ex : cybersec785)

3.1.1.3 Prise de contrôle du serveur web

Exploiter l'une des vulnérabilités pour installer un webshell (utiliser « wso2.5.1.php ») sur joomla et prendre le contrôle du serveur. Afficher le contenu du fichier configuration.php situé dans joomla. (2 pts)

3.1.2 Dokuwiki (7 pts)

3.1.2.1 Partie offensive

Il existe un wiki installé sur le serveur. Pourquoi celui-ci n'a-t-il pas été détecté par Nessus ? (0,5 pt)

Cherchez ce répertoire et accédez-y au wiki (Utiliser comme wordlist le fichier « fuzz_common.txt ») (0,5 pt)

Une fois le répertoire découvert, réalisez une attaque de brute-force sur le compte « admin». (2 pts)

Indication : le mot de passe du l'administrateur wiki est de la forme : <mot_en_minuscule>[0-9].

Une fois le mot de passe découvert, générer un backdoor avec metasploit et utiliser celle-ci pour contrôler le serveur avec un meterpreter (2 pts)

Indication :

- https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics/
- https://nitesculucian.github.io/2018/07/24/msfvenom-cheat-sheet/

3.1.2.2 Escalade de privilège

A partir du webshell installé lors de la prise de contrôle du serveur, découvrir un moyen de devenir root. (2 pts)

Indication n°1 : à partir du webshell, uploader et exécuter le script « linuxprivchecker.py ». Analyser les résultats découvrir la backdoor présente sur le serveur. Celle-ci peut être utilisée pour devenir root. Lien :

- *https://nnc3.com/mags/LM10/Magazine/Archive/2007/77/022-028_backdoors/article.html*
- *http://www.hackingarticles.in/linux-privilege-escalation-using-suid-binaries/*

3.2 SSH (2 pts)

Détecter un compte d'utilisateur valide (le compte élève ne compte pas) (1pt)

Indication : Utiliser l'exploit CVE-2018-15473. Utiliser comme liste de noms utilisateurs le fichier simple_users2.txt

Une fois le (ou les) compte(s) utilisateur(s) détecté(s), tenter de découvrir un mot de passe valide associé au compte (1 pt)

Indication : Utilisez comme fichier de mot de passe weaksauce.txt.

3.3 Gestions des backups (2 pts)

Il y a un répertoire backups sur la racine du serveur web. Ce répertoire est protégé par une authentification de type htaccess (url : http://<ip>/backups)

Réaliser une attaque par brute-force de l'authentification htaccess et découvrir le compte utilisateur associé (nom de l'utilisateur : joomhtaccess)

Indication n°1 : chercher sur google comment configurer Burp pour tester une authentification htaccess…

Télécharger et découvrir le mot de passe de l'archive joomla.zip (1 pt)

Indication : Utiliser les règles jumbo (http://www.openwall.com/john/j/john-1.8.0-jumbo-1.tar.xz)

Indication : le mot de passe est de la forme : <mot_en_minuscule>[0-9][& ?!:,] (ex : cybersec7?)

3.4 Web (6 pts)

3.4.1 WAF

Installer et configurer mod-security (lien : https://www.lecoindesdocs.fr/2016/12/05/installation-et-configuration-dun-waf-debian-8-6/) (1pt)

Ré-exploiter vulnérabilités liées à Joomla (utiliser sqlmap pour l'injection sql et Burp pour la création du compte privilégié). Regarder les journaux d'événements de mod-security et analyser si l'exploitation de ces 2 vulnérabilités a été détectée. Les 2 vulnérabilités ont-elles été détectées ? Pourquoi ? (2 pts)

3.4.2 Détection de backdoor

Trouver 2 moyens / outils de détecter les webshells utilisés pour ce tp (fichiers « wso.php » et meterpreter) (2 pts)

3.4.3 Défense

Configurer fail2ban pour bloquer les attaques de force-brute sur l'application phpmyadmin. Tester la configuration (2 pts).