Fiche pratique n°3 : Exploitation d’une faille applicative via Metasploit(Framework)

**1.3 Outils**

Serveur FTP vulnérable : VSFTPd 2.3.4 via Metasploitable.

Outil d’exploitation de la vulnérabilité : Metasploit via Kali.

**2 Recherches**

Q1. Metasploit est un outil d’instrustion capable d’analyser, tester et exploiter des systemes et une grande variétés d’application

Q2.

Payload :

Le payload est un virus dissimulé et il peut être déclenché à tout moment notamment il peut agir en conséquence via des attaques informatiques.

Exploit :

Un exploit est un outil capable d’exploiter une vulnérabilité (une faille de sécurité) laissé par un hacker, la forme peut être soit un code ou soit un programme malveillant pour atteindre des données.

Backdoor : Prevoir un accès tenu secret vis-à-vis de l’utilisateur.

**3 Manipulations**

**Travail à faire 2**

**Q4. RHOST Hote distant : Contient l’adresse IP de notre système cible**

**RPORT : Cette variable contient le numéro du port**

**A quoi sert la commande nmap ?**

Q5.Nmap est un scanner de ports libre.
Il est conçu pour détecter les ports ouverts, identifier les services hébergés et obtenir des informations sur le système d'exploitation d'un ordinateur distant.

Q6.

nmap –A

****

**Permet de connaitre l’état, le service et le port**

**3.2 Exploitation du Framework Metasploit**

**Depuis un terminal, il faut saisir la commande :**

**« Msfconsole**

**Puis, il faut selectionner l’exploit associé au service VsFTPD :**

**Use exploit**

****

 **Les options disponibles pour l’exploitation d’une vulnérabilité sont visibiles à l’aide de la commande suivante :**

**Show options**

**A ce niveau, la commande info donne des détails sur la vulnérabilité exploitable**

****

**La vulnérabilité concerné est une brèche ouverte sur le serveur VFPTD download, elle à été introduite dans le fichier compréssé : vsftpd-2.3.4.tar.gz archive**

**Le seul paramètre à indiquer est donc l’adresse distante : set RHOSTS 172.17.1.7**

**Une fois l’exploit chargé sur Metasploit, il ne reste plus qu’à lancer avec la commande : run**

****

**On peut voir tout les fichiers du serveur et que l’ip à été changé**

**Travail à faire**

**Q8. L'acronyme CVE, pour Common Vulnerabilities and Exposures en anglais, désigne une liste publique de failles de sécurité informatique.**

**Q9. Les developpeurs sont aussi concernés**

**Q10. C’est important que le système soit à jour car il ne faut pas negliger que cela ouvre une porte pour les hackers**

**Q11. On peut remarquer les fichiers de la machine cible, consulter les fichiers, on peut récupérer ces fichiers pour former une base de donnée confidentiels à la base pour la machine cible.**