Q1 – Qu’est-ce qu’une attaque par déni de service (DoS) :

Q2 – Indiquez les deux types d’attaques de DoS et leur conséquences :

* Type d’attaque 1 :
* Conséquence du type d’attaque 1 :
* Type d’attaque 2 :
* Conséquence du type d’attaque 2 :

Q3– Qu’est-ce qu’une attaque par déni de service distribuée (attaque DDoS) :

Q4– Qu’est-ce qu’un ordinateur zombi ?

Q5 – De quelle manière le hacker déclenche-t-il l’attaque DDOS?

Q6– Citez un outil logiciel qui permet de faire du repérage dans un réseau.

Q7 – Indiquez quatre types d’attaque par usurpation :

Q8 – Quel est le principe de l’attaque Man-in-the-Middle ?

Q9 – Que permet de faire ZeuS, un exploit avec des fonctionnalités MitMo (une variante de l’attaque Man-in-the-Middle) ?

Q10 – Qu’est-ce qu’une attaque zero-day ?

Q11 – Qu’est-ce qu’un enregistreur de frappe et quel intérêt représente-t-il ?

Q12 – Qu’est-ce que le SMiShing ?

Q13 – Quel risque peut-on avoir dans un réseau si un hacker installe un point d’accès non autorisé ?

Q14 – Qu’est-ce qu’une attaque Evil Twin ?

Q15 – Qu’est-ce qu’une attaque bluesnarfing ?

Q16 – Pourquoi ne faut-il pas utiliser le protocole de sécurité WEP pour configurer un accès Wifi  ?

Q17 – Quel est l’intérêt du logiciel NetStumbler pour l‘administrateur d’un réseau ?

Q18 – Qu’est-ce que le Cross-site scripting ?

Q19 – Qu’est-ce qu’une attaque par injection de code ?

Q20 – Qu’est-ce que l’attaque par buffer overflow ?

Q21 – Que permet l’outil Metasploit ?

Q22 – Quelle vulnérabilité peut présenter un programme Java dans un navigateur ?