1.**Origine du terme "hacker"** : Le terme "hacker" trouve son origine dans les laboratoires du MIT dans les années 1960. Il désignait à l'origine des programmeurs innovants et passionnés par la résolution de problèmes informatiques complexes.

- **Black Hat Hacker** : Un hacker malveillant qui exploite les systèmes à des fins personnelles.
- **White Hat Hacker** : Un hacker éthique (ethical hacker) qui utilise ses compétences pour sécuriser les systèmes.
- **Grey Hat Hacker** : Un hacker qui opère entre les domaines du black hat et du white hat, généralement en exploitant des vulnérabilités pour en informer les propriétaires.
- **Red Team** : Une équipe de professionnels de la sécurité chargée de simuler des attaques réalistes sur un système afin de tester sa résistance.
- **Blue Team** : Une équipe chargée de défendre un système ou un réseau contre les attaques.
- **Script Kiddies** : Des individus peu qualifiés qui utilisent des outils développés par d'autres pour mener des attaques sans comprendre pleinement leur fonctionnement.
- **Carders** : Des individus qui volent et utilisent frauduleusement des informations de cartes de crédit.
- **Phreakers** : Des individus qui explorent et exploitent les systèmes de télécommunications, notamment les réseaux téléphoniques.
- **Crackers** : Des individus qui s'engagent dans le contournement des mesures de sécurité pour accéder à des systèmes ou des données de manière non autorisée.
- **Hacktivists** : Des hackers qui utilisent leurs compétences pour promouvoir des causes politiques ou sociales.

2.**Métiers de la cybersécurité** : Analyste en sécurité informatique, Ingénieur en sécurité des systèmes, Expert en réponse aux incidents, Consultant en sécurité, Administrateur de la sécurité des réseaux.

3.**États-nations et attaques de malware** : Les États-Unis, la Russie et la Chine sont en pointe dans le domaine du malware. Quelques exemples d'attaques récentes sont Stuxnet, NotPetya et WannaCry.

4.Mécanismes de sécurité et leurs objectifs :

- **Antivirus** : Détection, Isolation, Correction, Prévention.
- **Cryptographie** : Confidentialité, Intégrité, Authentification, Non-répudiation.
- **Pare-feu** : Protection contre les intrusions, Contrôle d'accès.
- **Droit d'accès logique** : Sécurisation de l'accès aux ressources, Authentification des utilisateurs.
- **Sécurité physique des locaux** : Protection des équipements et des données physiques.
- **Audit de sécurité** : Vérification de la conformité, Détection des vulnérabilités.
- **Clauses contractuelles avec les partenaires** : Garantir la sécurité des échanges de données.
- **Formation et sensibilisation** : Sensibilisation des utilisateurs, Réduction des risques humains.

5.**Forme de malware la plus répandue** : Ransomware. Un exemple récent est l'attaque WannaCry en 2017, qui a affecté plus de 200 000 ordinateurs dans plus de 150 pays.

6.**Attaques récentes sur des systèmes d'information et leurs impacts** : Attaque SolarWinds, Attaque Colonial Pipeline, Attaque Kaseya. Les impacts comprennent la perturbation des opérations, la perte de données sensibles et des dommages à la réputation et à la confiance des clients.

7.**Types de vulnérabilités et exemples concrets** :

- **Vulnérabilité au niveau de la conception** : Un exemple serait une application Web qui stocke les mots de passe des utilisateurs dans une base de données sans les hasher ou les saler correctement, ce qui rend les mots de passe vulnérables aux attaques par force brute ou par dictionnaire.
- **Vulnérabilité au niveau de la réalisation** : Un exemple serait une application qui utilise des bibliothèques logicielles obsolètes ou non sécurisées, ce qui expose l'application à des failles de sécurité connues et exploitées.
- **Vulnérabilité au niveau de l'installation** : Un exemple serait l'installation d'un logiciel sur un système sans appliquer les correctifs de sécurité ou les mises à jour nécessaires, laissant ainsi le système exposé à des vulnérabilités connues.
- **Vulnérabilité au niveau de la configuration** : Un exemple serait la configuration incorrecte d'un pare-feu qui autorise un accès non autorisé à certains services ou ports, ce qui compromet la sécurité du réseau.
- **Vulnérabilité au niveau de l'utilisation d'un bien** : Un exemple serait l'utilisation de mots de passe faibles ou partagés par plusieurs utilisateurs, ce qui facilite les attaques par force brute ou par devinettes.

8.Vulnérabilités les plus exploitées par des attaquants : Une des vulnérabilités les plus exploitées par des attaquants est la faille CVE-2017-11882 dans Microsoft Office, qui permet l'exécution de code à distance. Cette vulnérabilité a été largement exploitée par des acteurs malveillants pour diffuser des logiciels malveillants et des attaques ciblées.

9.Vulnérabilité sur BASH avec un score CVSS élevé : Une vulnérabilité sur BASH avec un score CVSS le plus élevé est CVE-2014-6271, également connue sous le nom de Shellshock. Cette vulnérabilité permettait l'exécution de code arbitraire via une manipulation des variables d'environnement Bash. Son score CVSS élevé reflète le potentiel de dommages importants qu'elle pouvait causer en permettant à un attaquant d'exécuter du code malveillant sur un système affecté.

10.Faille de sécurité sur OpenSSL et logiciels open-source : La faille de sécurité sur OpenSSL qui est restée plus de 2 ans avant d'être découverte souligne l'importance de la transparence et de la collaboration dans le développement de logiciels open-source. Cela montre que même avec un modèle de développement ouvert et une licence GPL, les logiciels open-source peuvent présenter des vulnérabilités importantes qui peuvent rester non découvertes pendant une période prolongée. En entreprise, cela souligne la nécessité d'avoir des processus robustes de gestion des correctifs et des mises à jour pour atténuer les risques associés aux vulnérabilités non découvertes dans les logiciels open-source utilisés dans leurs environnements.

11.APT (Advanced Persistent Threat) : Une APT (Advanced Persistent Threat) est une attaque sophistiquée et ciblée menée par des acteurs malveillants, généralement soutenus par des ressources importantes et motivés par des objectifs spécifiques à long terme. Un exemple réel est l'attaque contre Sony Pictures Entertainment en 2014, attribuée à la Corée du Nord.

12.Exemples de phishing, d'ingénierie sociale et de ransomware :

- **Phishing** : Un exemple de phishing serait de recevoir un e-mail prétendument de la part d'une banque vous demandant de mettre à jour vos informations de compte en cliquant sur un lien, qui mène à un faux site Web conçu pour voler vos identifiants de connexion.
- **Ingénierie Sociale** : L'ingénierie sociale peut impliquer des tactiques telles que le pretexting, où un attaquant se fait passer pour quelqu'un en autorité pour manipuler des individus afin de divulguer des informations sensibles ou d'effectuer des actions qu'ils ne devraient pas.
- **Ransomware** : Un exemple de ransomware est l'attaque WannaCry, où un logiciel malveillant a chiffré des fichiers sur des ordinateurs infectés et a demandé une rançon pour le décryptage.

13.Fonctionnement des vulnérabilités :

- **Débordement de Tampon (Buffer Overflow)** : Le débordement de tampon se produit lorsqu'un programme écrit plus de données dans une zone de mémoire tampon qu'elle peut en contenir, entraînant le dépassement dans des zones mémoire adjacentes. Pour se protéger, il est important d'utiliser des pratiques de programmation sécurisées telles que la vérification des limites et la validation des entrées pour éviter les débordements de tampon, ainsi que des langages de programmation et des bibliothèques sécurisées qui gèrent automatiquement la gestion de la mémoire.
- **Injection SQL** : L'injection SQL est une technique d'attaque où un attaquant insère du code SQL malveillant dans les champs d'entrée d'une application Web. Pour se protéger, il est important d'utiliser des requêtes paramètres ou des instructions préparées pour traiter les données utilisateur et empêcher l'exécution de commandes SQL non autorisées, ainsi que de mettre en œuvre une validation stricte des entrées utilisateur pour filtrer les caractères spéciaux et les commandes SQL.

14.Bonnes pratiques en cybersécurité :

- **Minimisation** : La minimisation consiste à réduire la surface d'attaque en éliminant les fonctionnalités, services ou privilèges d'accès inutiles. Par exemple, désactiver les ports ou services réseau inutilisés sur les serveurs réduit les voies potentielles d'attaque.
- **Moindre Privilège** : Le principe du moindre privilège consiste à accorder aux utilisateurs uniquement les autorisations nécessaires pour effectuer leurs fonctions, limitant ainsi les dommages potentiels en cas de violation. Par exemple, restreindre les utilisateurs réguliers d'accéder aux fichiers système critiques ou aux fonctions administratives.
- **Défense en Profondeur** : La défense en profondeur implique l'utilisation de plusieurs couches de contrôles de sécurité pour protéger les systèmes contre différents types de menaces. Par exemple, utiliser des pare-feu, des systèmes de détection d'intrusion et des logiciels

antivirus en combinaison pour défendre contre les attaques réseau, les logiciels malveillants et autres menaces.

- **Veille et Journalisation** : La veille et la journalisation impliquent de surveiller activement les systèmes pour détecter les activités suspectes et de conserver des journaux détaillés des événements pour une analyse ultérieure. Par exemple, mettre en place des systèmes de journalisation centralisée pour enregistrer les activités système et réseau, permettant une analyse approfondie en cas d'incident.

15.Outils pour mesurer l'exposition à Internet :

- **Shodan** : Shodan est un moteur de recherche spécialisé dans la recherche d'appareils connectés à Internet. Il indexe les informations sur les appareils connectés, y compris les serveurs, les routeurs, les caméras IP, les objets connectés, etc. Les entreprises peuvent utiliser Shodan pour identifier les appareils exposés à Internet et évaluer leur vulnérabilité potentielle.
- **Censys** : Censys est une autre plateforme de recherche qui fournit des informations sur les appareils connectés à Internet. Il scanne et indexe les protocoles Internet pour découvrir les appareils connectés, les certificats SSL/TLS, les sites Web, etc. Les entreprises peuvent utiliser Censys pour évaluer leur empreinte numérique et identifier les éventuelles vulnérabilités.
- **Nmap (Network Mapper)** : Nmap est un scanner de réseau open-source qui permet aux entreprises d'analyser les réseaux informatiques pour découvrir les appareils connectés, les services actifs et les ports ouverts. Il peut aider les entreprises à identifier les points d'entrée potentiels pour les attaquants et à évaluer la sécurité de leur réseau.
- **Qualys Vulnerability Management** : Qualys propose une suite de solutions de gestion des vulnérabilités qui permet aux entreprises de découvrir, évaluer et prioriser les vulnérabilités dans leur infrastructure informatique. Cela inclut la découverte des actifs, l'évaluation des vulnérabilités et la gestion des correctifs pour réduire les risques liés à l'exposition à Internet.

- **Rapid7 InsightVM** : InsightVM est une plateforme de gestion des vulnérabilités de Rapid7 qui aide les entreprises à découvrir, évaluer et remédier aux vulnérabilités dans leur environnement informatique. Il offre une visibilité complète sur les actifs et les vulnérabilités, ainsi que des fonctionnalités de gestion des correctifs pour réduire les risques liés à l'exposition à Internet.