1) **Un utilisateur peut être authentifié pour accéder à un service à l'aide de l'une des trois caractéristiques suivantes :**
   - ce que l'utilisateur connait
   - ce que l'utilisateur possède
   - ce que l'utilisateur est

Pour ce que l'utilisateur connait, on peut utiliser le code PIN.
Pour ce que l'utilisateur possède on peut utiliser la carte à puce.
Pour ce que l'utilisateur est on peut utiliser l'empreinte digital.

2) **Quelles différences voyez-vous entre un "Script Kiddie" et une "APT (Advanced Persistant Threat)" ?**

- "script kiddie" : Néophyte dépourvu de compétence et sans stratégie utilisant des scripts, des outils tout faits récupérés sur internet. À la recherche d'entrées faciles sur les systèmes.
- "APT" : Cyberattaque qui met en œuvre des moyens humains et techniques importants pour infiltrer durablement les systèmes d'information vitaux d'une organisation. Une cyberattaque persistante recourt à des techniques furtives qui s'adaptent graduellement aux actions de cyberprotection qu'elle suscite.

3) **L'installation d'une mise à jour de sécurité sur un équipement (par exemple un serveur) nécessite l'arrêt et le redémarrage de l'équipement afin que cette mise à jour soit active.**
   Pour le besoin du service que propose cet équipement (par exemple un serveur gérant le fonctionnement d'une chaîne de production industrielle) celui-ci ne peut être arrêté fréquemment car son arrêt engendre la non-disponibilité de ce service indispensable.
   S'il s'avère impossible de dupliquer cet équipement (et donc le service indispensable qu'il rend) alors comment procéder pour s'affranchir du risque que cette mise à jour devait couvrir tant qu'on ne peut pas redémarrer l'équipement ?

Entre l'équipement qui ne peut être arrêté et la source du risque (internet par exemple) on applique, sur un mécanisme intermédiaire de contrôle du flux, une règle qui va permettre d'identifier et d'arrêter ce risque afin qu'il n'affecte pas l'équipement en question.
Le correctif sera installé sur l'équipement lorsqu'il sera possible de le redémarrer à un moment propice fonction du service à rendre. Maintenant ainsi protégé, la règle sur le mécanisme de contrôle intermédiaire n'est plus nécessaire et elle peut y être enlevée.

4) **Un réseau d'ordinateurs compromis et pilotés à distance par un malveillant (Botnet) :**

Offre la résilience (résistance aux pannes) au malveillant le pilotant.

5) **Qu'entend-t-on par « décapiter » un botnet ?**

Identifier les serveurs de commandes et de contrôles du botnet (C&C servers) qui envoient des ordres malveillants aux équipements infectés (zombies).
Puis couper les liens réseaux entre ces serveurs C&C et les équipements zombies afin qu'ils ne soient plus en mesure de les contrôler.

6) Comment combattre les risques liés aux keyloggers ?

Les keyloggers logiciels peuvent être combattus comme des virus
- Les keyloggers commerciaux ne sont pas traités par les anti-virus
- Les bases de signatures de ces anti-virus doivent être maintenues à jour

Les firewalls peuvent être un moyen de détecter l'activité réseau générée par un keylogger.
- En alertant lors de l'utilisation d'un port non conforme à la politique de sécurité

La protection physique des systèmes permet de combattre les keylogger matériels
- En examinant notamment leur présence éventuelle

7) La direction informatique vous charge de lui présenter les différents éléments techniques et organisationnels qui permettront à l'entreprise de prévenir l'intrusion d'un virus ou d'un ver dans ses réseaux internes et qui lui permettront de réagir en cas d'infections dues à un virus ou un ver.

- Sécurisation des équipements (durcissement, réduction de la surface d'attaque)
- Sensibilisation des acteurs
- Anti-virus de deux types (base de signature et analyse du comportement)
- Veille concernant l'apparition des nouveaux malwares et des nouvelles parades
- Organisation des mises à jour
- Préparation à la réaction en cas d'attaques virales (isolation des équipements infectés, cellule de crise en cas de propagation de vers dans le réseau de l'entreprise)

8) Expliquez comment fonctionne un anti-virus basé sur des signatures.

Lorsque le virus est découvert il est remonté auprès de l'éditeur de solutions d'anti-virus où des experts l'analyse et en détermine une signature laquelle vous est envoyée afin d'être intégrée dans la base de signature de votre anti-virus.
Si le virus vous atteint votre anti-virus le repérera en comparant sa signature à celles pré-enregistrées dans votre base de données de signatures associée à votre anti-virus et régulièrement mise à jour par l'éditeur d'anti-virus.

9) Donnez une limite liée au mécanisme d'un anti-virus basé sur des signatures

La base de données de l'anti-virus peut ne pas contenir la signature d'un nouveau virus ou d'un virus ancien.

10) Selon vous en quoi consiste le phishing (ou hameçonnage) ?

Le phishing est une technique de fraude où des cybercriminels se font passer pour des entreprises afin de tromper les victimes et leur soutirer des informations importante, comme des mots de passe, des numéros de carte bancaire ou des données personnelles. Cela se fait généralement via des e-mails, des messages ou des sites web qui sont recopié de manière identique. L'objectif étant d'inciter la victime à cliquer sur un lien frauduleux ou à fournir volontairement ses informations.

11) Quels moyens peuvent utiliser les phishers (escrocs menant des campagnes de phishing) pour usurper ou altérer des liens DNS afin de leurrer les utilisateurs ?

- DNS spoofing : attaquer un serveur de noms DNS pour altérer le lien entre un nom en le faisant pointer sur l'adresse IP du phisher
- DNS cache poisoning : même technique mais en altérant un cache DNS plus facilement accessible
- Similarité de nom de domaine en jouant sur le code pays ou l'orthographe du nom
- Altération de lien : exemple proposer dans le lien une page sur un site portant le nom à leurrer
- Mettre à profit une faille dans un navigateur, masquer une partie de l'URL affichée

12) Selon vous, quelles actions préventives peuvent être menées P A R U N E E N T R E P R I S E pour participer à la lutte contre les tentatives de phishing dont ses clients pourraient être victimes ?
Comment l'entreprise peut-elle réagir à une campagne de phishing en cours imitant ses services ?

- Rappel de prudence aux clients (attention aux emails frauduleux circulant ...)
- Pas de campagnes de mailing demandant des informations confidentielles à ses clients
- Indiquer dernières dates et heures de connexion
- Surveiller ou faire surveiller l'apparition de noms approchants
- Surveiller l'appariement ente noms DNS et adresses IP (DNS spoofing et cache poisoning)
- Préparer la réaction (qui contacter : registrant, registrar, hébergeur DNS, hébergeur site ...) ,
- Constituer un dossier de preuves pour éventuelles poursuites juridiques avant de faire fermer le faux-site)

13) Un des principes de Kerchoffs stipule "Il faut qu'un système cryptographique n'exige pas le secret". Expliquez en quoi, selon vous, le respect de ce principe lors du développement d'un système de chiffrement apporte de la confiance à celui-ci.

On ne fait JAMAIS de sécurité par l'obscurité surtout en matière de cryptographie. Ce qui est obscure , incompréhensible ne peut être de confiance. En cryptographie, la sécurité ne se décrète pas elle se prouve.

C'est parce que les outils cryptographiques que nous utilisons ont été challengés par de multiples experts en la matière que nous savons qu'ils sont sûrs. Ceux qui sont secrets dont on ne connaît pas le fonctionnement car il n'a pas été rendu public ne peuvent être de confiance.

Ce qui doit rester secret c'est la clé injectée dans le mécanisme de chiffrement pas le mécanisme lui-même qui doit pouvoir être challengé.

14) Comparez les avantages et les inconvénients des systèmes cryptographiques basés sur le chiffrement symétrique (dit aussi "à clé secrète") à ceux qui sont basés sur le chiffrement asymétrique (dits aussi "à clés publiques").

CHIFFREMENT ASYMÉTRIQUE

-Avantages :

--- on peut distribuer la clé de chiffrement (clé publique)

---utilisation d'annuaires publics pour la distribution des clés publiques

--- nombre de clés d'ordre N (si N acteurs)

-Inconvénients :

--- calculs fort demandeur en ressources

--- niveau de sécurité "challengé" par l'arrivée des machines quantiques

--- lent pour une utilisation intensive

CHIFFREMENT SYMÉTRIQUE

-Avantages :

--- besoin en ressources moindre

--- état de l'art en termes de niveau de sécurité (avec AES)

-Inconvénients :

--- il faut convenir de la clé entre partenaires

--- la clé doit être échangée de manière sécurisée.

--- la clé secrète doit rester secrète. Seuls les partenaires doivent la connaître

--- taille du réseau (n acteurs ---> n (n-1)/ 2 clés)

15) Pour assurer la confidentialité d'un document à l'aide d'un système de cryptographie asymétrique on peut chiffrer le document avec:

La clé publique de l'expéditeur

La clé publique du destinataire

16) Pour prendre connaissance du contenu d'un fichier dont la confidentialité est assurée à l'aide d'un chiffrement asymétrique il faut posséder :

La clé privée du destinataire du document

17) Pour signer un message à l'aide d'un système utilisant un algorithme de chiffrement asymétrique, l'émetteur...

... utilise sa propre clé privée

18) Dans un système de cryptographie à clés publiques, un utilisateur ayant perdu sa clé privée peut encore ...

... envoyer des messages chiffrés

... vérifier la signature d'un émetteur dont il a la clé publique

19)Un hash (on dit aussi une empreinte) généré par une fonction de hashage permet de vérifier que le contenu d'un document n'a pas été modifié, altéré, que le document est resté "intègre".

1/ Vous rappelez le principe sur lequel s'appuie le hashage pour permettre cette vérification d'intégrité.

2/ Vous décrivez les différentes étapes suivies par l'émetteur d'un document et son destinataire afin que celui-ci soit en mesure, à l'aide d'une fonction de hashage, de vérifier qu'un document n'a pas été altéré en cours de transmission à travers le réseau.

1/ Principe :

Les fonctions de hashage s'appuient (entre autres) sur le principe de non-collision : Pour un document donné en entrée d'une fonction de hashage il n'existe qu'un seul hash possible en sortie pour une même fonction de hash. Si deux hashes différent alors forcément ils proviennent de deux documents dont les contenus ne sont pas identiques.

2/ Les étapes :

- L'émetteur du document en calcule le hash
- L'émetteur du document transmet le document et le hash ainsi calculé au destinataire à travers le réseau
- Le destinataire recalcule le hash du document reçu avec la même fonction de hash
- Le destinataire compare le hash qu'il a recalculé au hash qu'il a reçu
- SI ces deux hashes sont identiques cela signifie forcément que le contenu du document n'a pas été altéré (qu'il est intégre) en cours de transmission