Résumé sécurité des terminaux

Module 1:Menaces,vulnérabilités et attaques en matiere de cybersecurite:

Domaines de menace:
Un domaine de menace est une zone de contrôle, d'autorité ou de protection que les hackers peuvent exploiter pour accéder à un système. Les cybermenaces comprennent les attaques et les erreurs logicielles, le sabotage, l'erreur humaine, le vol, les pannes matérielles, l'interruption des services publics et les catastrophes naturelles. Les menaces internes sont généralement le fait d'employés actuels ou anciens et d'autres partenaires contractuels. La source d'une menace externe provient généralement d'attaquants amateurs ou qualifiés qui peuvent exploiter les vulnérabilités des dispositifs en réseau ou utiliser des techniques d'ingénierie sociale. Un domaine d'utilisateurs comprend toute personne ayant accès au système d'information d'une organisation. Les menaces courantes pour les utilisateurs incluent les politiques de sécurité mal appliquées, le vol de données, les téléchargements et les supports non autorisés, les VPN et les sites web non autorisés, et la destruction des systèmes, des applications ou des données. Les équipements individuels, les réseaux locaux et les clouds privés et publics sont également vulnérables aux attaques. Il existe des menaces complexes telles que les attaques APT et les attaques par algorithme. Les cybercriminels utilisent des programmes de porte dérobée pour obtenir un accès non autorisé à un système en contournant les procédures d'authentification normales. Les portes dérobées permettent aux cybercriminels de continuer à accéder à un système, même si l'organisation a corrigé la vulnérabilité initiale utilisée pour attaquer le système. La plupart des rootkits exploitent les vulnérabilités logicielles pour accéder aux ressources et modifier les fichiers système. Il est également fréquent que les rootkits modifient les investigations du système et les outils de surveillance, ce qui rend très difficile leur détection.

Le dark web est un contenu web chiffré qui n'est pas indexé par les moteurs de recherche classiques et dont l'accès nécessite des logiciels, des autorisations ou des configurations spécifiques. Les IOC, tels que les signatures de malwares ou les noms de domaine, fournissent des preuves des failles de sécurité. Le système AIS permet d'échanger en temps réel des indicateurs de menaces pour la cybersécurité à l'aide de langages standardisés et structurés appelés STIX et TAXII.

Déception:
L'ingénierie sociale est une stratégie non technique qui vise à manipuler les individus pour les amener à effectuer certaines actions ou à divulguer des informations confidentielles. On parle de prétextage lorsqu'une personne ment pour avoir accès à des données privilégiées. Les attaques quid pro quo sont une demande d'informations personnelles en échange de quelque chose. L'usurpation d'identité

consiste à utiliser l'identité volée d'une personne pour obtenir des biens ou des services par la tromperie.

Les tactiques d'ingénierie sociale incluent l'usurpation d'identité d'une figure d'autorité, l'intimidation, le consensus ("tout le monde le fait"), prétendre que quelque chose est rare ou qu'une situation est urgente, établir la familiarité et la confiance avec un employé pour en tirer parti pour l'accès. Surfer par-dessus l'épaule d'une cible pour obtenir des informations précieuses telles que des codes PIN, des codes d'accès ou des informations de carte bancaire. Les criminels n'ont pas besoin d'être toujours près de leur victime pour surfer sur l'épaule, ils peuvent utiliser des jumelles ou des caméras de sécurité pour obtenir ces informations. La recherche dans les poubelles consiste à fouiller dans la corbeille d'une cible pour voir quelles informations ont été rejetées. On parle de se greffer ou de talonnage lorsqu'un criminel suit une personne autorisée pour pénétrer physiquement dans un lieu sécurisé ou une zone d'accès restreint. D'autres méthodes de tromperie incluent les arnaques aux factures, les attaques de points d'eau, le typosquatting, l'ajout de préfixes et les campagnes d'influence.

Les organisations doivent promouvoir la sensibilisation aux tactiques d'ingénierie sociale et former correctement les employés aux mesures de prévention.

Cyber-Attaques:
Un logiciel malveillant est un code qui peut être utilisé pour voler des données, contourner les contrôles d'accès, endommager ou compromettre un système. Un virus est un type de programme informatique qui, lorsqu'il est exécuté, se réplique et s'attache à d'autres fichiers en y insérant son propre code. Un ver est un logiciel malveillant qui se reproduit en exploitant de manière indépendante les vulnérabilités des réseaux. Un cheval de Troie est un logiciel malveillant qui effectue des opérations malveillantes en masquant sa véritable intention. Une bombe logique est un programme malveillant qui attend un déclencheur pour déclencher le code malveillant. Les rançongiciels sont conçus pour retenir captif un système informatique ou les données qu'il contient jusqu'à ce qu'un paiement soit effectué. Les attaques DoS créent une quantité considérable de trafic ou envoient des paquets formatés de manière malveillante qui ne peuvent pas être identifiés par une application, ce qui ralentit ou bloque l'appareil récepteur. Les attaques DDoS sont similaires mais proviennent de plusieurs sources coordonnées. Les attaques DNS incluent l'usurpation d'identité et le piratage.

Les attaques de couche 2 incluent l'adresse MAC, l'usurpation ARP et IP, l'inondation MAC, l'homme du milieu et l'homme du mobile. Les attaques Jour zéro exploitent les vulnérabilités logicielles avant qu'elles soient connues. La journalisation du clavier (keylogging) enregistre les frappes au clavier et configure le logiciel enregistreur de frappe pour envoyer le fichier journal au criminel. Ce fichier journal peut révéler des noms d'utilisateur, des mots de passe, des sites web visités, etc.

Pour vous défendre contre ces attaques, utilisez des pare-feu, restez à jour sur les mises à niveau et les correctifs, répartissez la charge de travail sur les systèmes de serveurs et bloquez les paquets ICMP externes avec des pare-feu.

Attaques visant les terminaux sans fil et mobiles:
Un Grayware est une application indésirable qui se comporte de manière gênante ou indésirable. Les SMiShing sont de faux messages texte qui vous invitent à visiter un site web malveillant ou à appeler un numéro de téléphone frauduleux, ce qui peut entraîner le téléchargement de malwares sur votre appareil. Un point d'accès malveillant est un point d'accès sans fil installé sur un réseau sécurisé sans autorisation. Une attaque jumelle malveillante consiste à configurer le point d'accès du hacker pour ressembler à une meilleure option de connexion. Le brouillage des fréquences radio brouille délibérément la transmission d'une station radio ou satellite pour empêcher un signal sans fil d'atteindre la station réceptrice.

Le Bluejacking envoie des messages non autorisés ou des images choquantes à un autre appareil Bluetooth. Bluesnarfing, c'est lorsqu'un hacker copie des informations à partir du périphérique d'une cible à l'aide de Bluetooth. WEP et WPA sont des protocoles de sécurité conçus pour sécuriser les réseaux sans fil. WPA2 est un protocole de sécurité amélioré. Contrairement au protocole WEP, un hacker ne peut pas récupérer la clé de chiffrement WPA2 en observant le trafic réseau.

Pour vous défendre contre les attaques sur les terminaux mobiles et sans fil: modifiez les configurations par défaut. Limitez le placement des points d'accès en plaçant ces périphériques à l'extérieur du pare-feu ou dans une DMZ. Utilisez les outils WLAN pour détecter les points d'accès non autorisés ou les postes de travail non autorisés. Mettez en place une politique d'accès invité à un réseau Wi-Fi. Les collaborateurs doivent utiliser un VPN d'accès à distance pour l'accès WLAN.

Application et autres attaques:
XSS est une vulnérabilité présente dans de nombreuses applications web. Les types d'attaques par injection de code incluent XML, SQL, DLL, et LDAP. Un dépassement de tampon se produit lorsque des données sont écrites au-delà des limites d'un tampon. L'exécution de code à distance exploite les vulnérabilités des applications pour exécuter des commandes avec les privilèges de l'utilisateur autorisé. D'autres attaques d'applications incluent CSRF, les conditions de concurrence, la gestion incorrecte des entrées, la gestion des erreurs, l'API, la relecture, la traversée de répertoires et l'épuisement des ressources.

Écrivez du code solide pour vous défendre contre les attaques contre les applications. Traitez et validez toutes les entrées externes à une fonction comme si elle était hostile. Maintenez tous les logiciels à jour. Les spams sont des e-mails non sollicités qui sont généralement utilisés à des fins publicitaires. Certains spams sont envoyés en masse par des ordinateurs infectés par des virus ou des vers. Le phishing consiste à contacter un utilisateur par e-mail ou par message instantané

par un hacker se faisant passer pour une personne légitime. Le spear phishing envoie des e-mails personnalisés à une personne spécifique en fonction des informations que le hacker connaît à son sujet. Les autres escroqueries courantes incluent le vishing, le Pharmacie et le Pêche à la baleine. Les autres types d'attaques incluent les attaques physiques contre les équipements, les attaques malveillantes basées sur l'intelligence artificielle, les attaques de la chaîne d'approvisionnement et les attaques dans le cloud.

Utilisez un logiciel antivirus pour vous défendre contre les attaques par e-mail et par navigateur. Ne partez jamais du principe que les pièces jointes sont sécurisées. Analysez toujours les pièces jointes avant de les ouvrir. Devenez membre de l'Anti-Phishing Working Group (APWG). Tous les logiciels doivent être mis à jour.

Question 1 :
Quel type d'attaque se produit lorsque les données dépassent les zones de mémoire allouées à une application ?
Réponse : Dépassement de tampon (Débordement de tampon)

Question 2 :
Laquelle des affirmations suivantes décrit une attaque par déni de service distribué (DDoS) ?
Réponse : Un botnet de zombies, coordonné par un hacker, submerge un serveur d'attaques DoS

Question 3 :
Les employés d'une entreprise signalent que l'accès au réseau est lent. Une enquête plus approfondie révèle qu'un employé a téléchargé un programme de numérisation tiers pour l'imprimante. Quel type de malware a pu être introduit ?
Réponse : Cheval de Troie

Question 4 :
Les employés d'une entreprise signalent qu'ils ne peuvent pas accéder à la base de données des clients sur le serveur principal. Une enquête plus approfondie révèle que le fichier de base de données est désormais chiffré. Peu après, l'organisation reçoit un courriel menaçant exigeant un paiement pour le décryptage du fichier de la base de données.
Réponse : Rançongiciel

Question 5 :
Un test de pénétration effectué par une entreprise a identifié une porte dérobée sur le réseau. Quelles mesures l'organisation doit-elle prendre pour savoir si ses systèmes ont été compromis ?
Réponse : Recherchez les comptes non autorisés

Question 6 :
Quelle méthode non technique un cybercriminel pourrait-il utiliser pour recueillir des informations sensibles auprès d'une organisation ?
Réponse : Ingénierie sociale

Question 7 :
Une secrétaire reçoit un appel téléphonique d'une personne prétendant que son directeur est sur le point de faire une présentation importante mais que les fichiers de la présentation sont corrompus. L'appelant demande sévèrement à la secrétaire d'envoyer immédiatement la présentation par courriel à une adresse personnelle. L'appelant précise également que le secrétaire est tenu personnellement responsable du succès de cette présentation. Quel type de tactique d'ingénierie sociale l'appelant utilise-t-il ?
Réponse : L'intimidation

Question 8 :
Tous les employés d'une organisation reçoivent un courriel indiquant que le mot de passe de leur compte expire immédiatement et qu'ils doivent le réinitialiser dans les cinq minutes. Laquelle des affirmations suivantes décrit le mieux cet e-mail ?
Réponse : C'est un canular

Question 9 :
Quelles meilleures pratiques peuvent aider à se défendre contre les attaques d'ingénierie sociale ? Sélectionnez trois bonnes réponses.
Réponses :

- Mettre en place une politique qui stipule que le service informatique ne doit fournir des informations par téléphone qu'aux responsables
- Résistez à l'envie de cliquer sur des liens Internet attrayants
- Former les employés aux politiques de sécurité

Question 10 :
Comment appelle-t-on une attaque par usurpation d'identité qui tire parti d'une relation de confiance entre deux systèmes ?
Réponse : L'homme au milieu

Question 11 :
Un cybercriminel envoie une série de paquets au format malveillant à un serveur de base de données, ce qui provoque l'arrêt du serveur. Comment appelez-vous ce type d'attaque ?
Réponse : DoS

Question 12 :
La sensibilisation et l'identification des vulnérabilités sont des fonctions essentielles d'un spécialiste de la cybersécurité. Laquelle des ressources suivantes peut-il utiliser

pour identifier les détails spécifiques des vulnérabilités ?
Réponse : Base de données nationale CVE

Module 2:Sécurisation des réseaux :

Etat actuel des choses:
La sécurité du réseau est directement liée à la continuité de l'activité de l'entreprise. Les failles de sécurité du réseau peuvent perturber le commerce électronique, entraîner la perte de données commerciales, menacer la confidentialité des personnes et compromettre l'intégrité des informations. Ces violations peuvent entraîner des pertes de revenus pour les entreprises, le vol de propriété intellectuelle, des poursuites et peuvent même menacer la sécurité publique. De nombreux outils sont disponibles pour aider les administrateurs réseau à s'adapter, à développer et à mettre en œuvre des techniques de réduction des menaces, notamment Cisco Talos Intelligence Group. Un vecteur d'attaque est un chemin par lequel un acteur de menace peut accéder à un serveur, un hôte ou un réseau. Les vecteurs d'attaque proviennent de l'intérieur ou de l'extérieur du réseau d'entreprise. Les données sont probablement l'atout le plus précieux d'une organisation. Divers contrôles DLP doivent être mis en œuvre, qui combinent des mesures stratégiques, opérationnelles et tactiques. Les vecteurs de perte de données courants sont les e-mails et les réseaux sociaux, les périphériques de données non chiffrés, les périphériques de stockage dans le cloud, les supports amovibles, les copies papier et les contrôles d'accès inappropriés.

Qui s'attaque à notre réseau?:

Pour comprendre la sécurité du réseau, vous devez comprendre les termes suivants: menace, vulnérabilité, surface d'attaque, exploitation et risque. La gestion des risques consiste à trouver un juste équilibre entre les coûts générés par les mesures de protection et les gains résultants de la protection des ressources. Quatre façons communes de gérer les risques sont l'acceptation des risques, l'évitement des risques, la réduction des risques et le transfert des risques. Pirate est un terme commun utilisé pour décrire un acteur de menace. Les hackers en chapeau blanc sont des hackers éthiques qui utilisent leurs capacités dont les activités sont bénéfiques, éthiques et légales. Les hackers chapeau gris sont des personnes qui commettent des délits ou effectuent des actions non éthiques, mais pas à des fins de profit financier ni pour infliger des dommages. Les hackers chapeau noir sont des criminels qui compromettent la sécurité des systèmes informatiques et des réseaux à des fins de profit personnel ou avec des intentions malveillantes. Parmi les acteurs de menace, on trouve des script kiddies, des testeurs de vulnérabilités, des hacktivistes, des cybercriminels et des hackers

sponsorisés par un État. De nombreuses attaques de réseau peuvent être évitées en partageant des informations sur les CIO. la cybersécurité est une priorité pour de nombreux gouvernements dans le monde. La CISA et la NCSA sont des exemples de telles organisations.

Question 1 :
Quelle est la ressource la plus précieuse d'une entreprise en matière de sécurité du réseau ?
Réponse : les données

Question 2 :
Quelle ressource est affectée par des paramètres de sécurité faibles pour un périphérique appartenant à l'entreprise, mais hébergé dans un autre emplacement ?
Réponse : dispositifs de stockage en nuage

Question 3 :
Quelle équipe Cisco est chargée d'analyser et de corriger les vulnérabilités potentielles des produits Cisco ?
Réponse : Groupe de recherche Cisco Talos

Question 4 :
Qu'est-ce qu'un vecteur d'attaque ?
Réponse : Il s'agit d'un chemin par lequel un acteur de la menace peut accéder à un serveur, un hôte ou un réseau.

Question 5 :
Associez les vecteurs de perte de données les plus courants à la description qui en est faite.
Réponses :

- **Supports amovibles (A)** : Un employé pourrait transférer sans autorisation des données sur une clé USB. En outre, une clé USB contenant des données d'entreprise précieuses pourrait être perdue.
- **E-mail/Réseaux sociaux (B)** : Les e-mails ou les messages instantanés interceptés peuvent être capturés et révéler des informations confidentielles.
- **Périphériques non chiffrés (C)** : Si les données ne sont pas stockées à l'aide d'un algorithme de chiffrement, le voleur peut récupérer des données confidentielles précieuses.
- **Contrôle d'accès incorrect (D)** : Les mots de passe volés ou les mots de passe faibles qui ont été compromis peuvent permettre à un attaquant d'accéder facilement aux données de l'entreprise.

Question 6 :
Quel terme de sécurité des réseaux est utilisé pour décrire un danger potentiel pour

un actif tel que des données ou le réseau lui-même ?
Réponse : menace

Question 7 :
Quelle affirmation décrit le terme « surface d'exposition aux attaques » ?
Réponse : Il s'agit de la somme totale des vulnérabilités d'un système qu'un hacker peut exploiter.

Question 8 :
Le département IT procède à une évaluation approfondie de l'état de sécurité du data center de l'entreprise. Le risque de perte ou de compromission des données critiques est identifié. Après discussion avec l'équipe de direction, il est décidé que les données critiques doivent être répliquées vers un fournisseur de services cloud et assurées auprès d'une compagnie d'assurance. Quelle stratégie de gestion des risques est utilisée ?
Réponse : Transfert des risques

Question 9 :
Associez le type de pirates à la description.
Réponses :

- **Hackers chapeaux blancs (A)** : Il s'agit de pirates éthiques qui utilisent leurs compétences en matière de programmation à des fins bénéfiques, éthiques et légales. Ils peuvent effectuer des tests de pénétration en utilisant leurs connaissances des dispositifs de sécurité informatique pour simuler des attaques ciblant les réseaux et les systèmes afin d'en révéler les vulnérabilités.
- **Hackers chapeaux noirs (B)** : Il s'agit de criminels sans éthique qui violent la sécurité des ordinateurs et des réseaux à des fins d'enrichissement personnel ou pour des raisons malveillantes, comme l'attaque de réseaux.
- **Hackers chapeau gris (C)** : Il s'agit de personnes qui commettent des délits et dont l'éthique est discutable, mais qui ne le font pas pour leur gain personnel ou pour causer des dommages. Ce peut être par exemple une personne qui compromet un réseau sans autorisation, puis dévoile publiquement la vulnérabilité.

Question 10 :
Quel terme désigne les hackers qui sont indépendants ou qui travaillent pour de grandes entreprises spécialisées dans la cybercriminalité ?
Réponse : Cybercriminels

Question 11 :
Quel énoncé décrit les caractéristiques des indicateurs d'attaque ?
Réponse : Ils peuvent être des fonctionnalités qui identifient les fichiers malveillants,

les adresses IP des serveurs utilisés dans les attaques, les noms de fichiers et les modifications caractéristiques apportées aux logiciels du système final, entre autres.

Question 12 :
Quelles sont les deux raisons pour lesquelles les menaces internes à une organisation peuvent causer plus de dégâts que les menaces externes ? (Choisissez deux propositions.)
Réponses :

- Les utilisateurs internes peuvent avoir connaissance du réseau de l'entreprise, de ses ressources et de ses données confidentielles.
- Les utilisateurs internes ont un accès direct à l'équipement de l'infrastructure.

Module 3:Attaques ciblant les fondements du réseau :

Détails d'IP PDU:
L'IP a été conçu comme un protocole sans connexion de couche 3. L'en-tête IPv4 se compose de plusieurs champs tandis que l'en-tête IPv6 contient moins de champs. Il est important que les analystes en sécurité connaissent les différents champs des en-têtes IPv4 et IPv6.

Vulnérabilités IP:
Il existe différents types d'attaques ciblant les composantes IP. Les attaques courantes liées à l'IP sont les suivantes:

- Attaques ICMP
- Attaque par déni de service (DoS)
- Attaque par déni de service distribué (DDoS)
- Attaques par usurpation d'adresse
- Attaques de l'homme-au-milieu (MiTM)
- Piratage de session

Le protocole ICMP a été conçu pour transporter des messages de diagnostic et pour signaler des conditions d'erreur lorsque les routes, les hôtes et les ports ne sont pas disponibles. Les acteurs de menace utilisent le protocole ICMP pour leurs attaques de reconnaissance et d'analyse. Les acteurs de menace utilisent également ICMP pour les attaques DoS. Les acteurs de menace utilisent souvent des techniques d'amplification et de réflexion pour créer des attaques DoS. Les acteurs de menace utilisent également les attaques par saturation des ressources pour consommer les ressources d'un hôte cible afin de le faire planter ou de consommer les ressources d'un réseau. Les attaques d'usurpation d'adresse IP se produisent lorsqu'un acteur de menace crée des paquets contenant de fausses informations d'adresse IP source pour masquer l'identité de l'expéditeur ou pour se faire passer pour un autre utilisateur légitime. Les attaques d'usurpation d'adresse peuvent être une usurpation non aveugle pour détourner une session, ou une usurpation aveugle pour créer une

attaque DoS. Les attaques par usurpation d'adresse MAC sont utilisées lorsque les cyberpirates ont accès au réseau interne.

Vulnérabilités liées aux protocoles TCP et UDP:
Les informations de segment TCP et de datagrammes UDP apparaissent immédiatement après l'en-tête IP. Il est important de comprendre les en-têtes de couche 4 et leurs fonctions dans la communication de données. TCP fournit une livraison fiable, un contrôle de flux et une communication dynamique. La communication avec état TCP entre deux parties se produit pendant la prise de contact à trois voies TCP. Les acteurs de menace peuvent mener une variété d'attaques liées au protocole TCP:

- Analyse de port TCP
- TCP SYN Attaque par inondation
- Attaque de réinitialisation du TCP
- Attaque par détournement de session TCP

Le segment UDP (c'est-à-dire datagramme) est beaucoup plus petit que le segment TCP, ce qui le rend très souhaitable pour les protocoles qui effectuent des transactions de requête et de réponse simples tels que DNS, DHCP, SNMP, etc. Les acteurs de menaces peuvent mener des attaques UDP inondation qui balayent tous les ports UDP connus sur un serveur en essayant de trouver des ports fermés. Cela peut créer une situation de déni de service.

Question 1 :
Quel champ dans un paquet IPv6 est utilisé par le routeur pour déterminer si un paquet a expiré et doit être supprimé ?
Réponse : **Limite de nombre de tronçons**

Question 2 :
Un hacker utilise un ordinateur portable comme point d'accès non autorisé pour capturer tout le trafic réseau provenant d'un utilisateur ciblé. De quel type d'attaque s'agit-il ?
Réponse : **l'homme au milieu**

Question 3 :
Quel champ de l'en-tête IPv4 permet d'empêcher un paquet de traverser un réseau indéfiniment ?
Réponse : **Time To Live (durée de vie)**

Question 4 :
Que signifie une attaque par usurpation d’adresse IP ?
Réponse : **Une adresse réseau IP légitime a été détournée par un nœud indésirable.**

Question 5 :
Quel type d'attaque implique la découverte et la cartographie non autorisées de systèmes et de services réseau ?
Réponse : **Reconnaissance**

Question 6 :
Lors de quelle attaque TCP le cybercriminel tente-t-il de submerger un hôte cible au moyen de connexions TCP semi-ouvertes ?
Réponse : **Attaque par inondation SYN**

Question 7 :
Comment les informations de couche réseau facultatives sont-elles transportées par les paquets IPv6 ?
Réponse : **À l'intérieur d'un en-tête d'extension associé à l'en-tête de paquet IPv6 principal**

Question 8 :
Un acteur de menace veut interrompre une communication TCP normale entre deux hôtes en envoyant un paquet usurpé aux deux points de terminaison. Quel bit d'option TCP l'acteur de menace mettrait dans le paquet usurpé ?
Réponse : **RST**

Question 9 :
Un acteur de menace utilise un programme pour lancer une attaque en envoyant un flot de paquets UDP à un serveur sur le réseau. Le programme balaye tous les ports connus afin de trouver les ports fermés. Il provoque la réponse du serveur avec un message de port ICMP inaccessible et est similaire à une attaque DoS. Quels deux programmes pourraient être utilisés par l'acteur de la menace pour lancer l'attaque ? (Choisissez deux réponses.)
Réponses :

- **ping**
- **Low Orbit Ion Cannon**

Question 10 :
Quel terme décrit un champ dans l'en-tête de paquet IPv4 utilisé pour détecter la corruption dans l'en-tête IPv4 ?
Réponse : **Somme de contrôle d'en-tête**

Question 11 :
Quel type de message ICMP peut être utilisé par les acteurs de menace pour mapper un réseau IP interne ?
Réponse : **Requête d'écho ICMP**

Question 12 :
Les utilisateurs d'une entreprise se sont plaints des performances du réseau. Après

enquête, le personnel informatique a déterminé que le hacker utilisait une technique spécifique pour entraver la connexion TCP en trois étapes. Quel est le nom de ce type d'attaque de réseau ?
Réponse : **Inondation SYN**

Module 4:Attaques ciblant les activités :

Services IP:
Les hôtes diffusent une requête ARP vers d'autres hôtes sur le segment afin de déterminer l'adresse MAC d'un hôte doté d'une adresse IP spécifique. Tout client peut envoyer une réponse ARP non sollicitée (appelé «réponse ARP gratuite»). Cette fonctionnalité du protocole ARP implique également que chaque hôte peut prétendre être propriétaire de l'adresse IP/MAC de son choix. Un acteur de menace peut empoisonner le cache ARP des appareils sur le réseau local, créant une attaque MITM pour rediriger le trafic.

Le protocole DNS (Service de nom de domaine) définit un service automatisé qui associe les noms de ressource à l'adresse IP d'hôte numérique requise. Il comprend le format des demandes, des réponses et des données. Il utilise des enregistrements de ressources (RR) pour identifier le type de réponse DNS. DNS est indispensable à l'exploitation d'un réseau et doit être sécurisé en conséquence. De nombreuses entreprises utilisent les services de serveurs DNS publiquement ouverts pour répondre aux requêtes. Les résolveurs ouverts DNS sont vulnérables à plusieurs activités malveillantes, y compris l'empoisonnement du cache DNS, dans lequel des enregistrements falsifiés sont fournis au solveur ouvert. Les attaques d'amplification et de réflexion DNS sont un autre type d'attaque dans lequel la nature bénigne du protocole DNS est exploitée pour provoquer des attaques DOS/DDoS. Dans les attaques d'utilisation des ressources DNS, une attaque DoS est lancée contre le serveur DNS lui-même. Les acteurs de menace se cachent souvent à l'aide de techniques furtives DNS telles que Fast Flux, dans lesquelles les serveurs malveillants modifient rapidement leur adresse IP. Les acteurs de la menace utilisent le double flux IP, qui consiste à changer rapidement à la fois leur nom de domaine et leur mappage IP, ainsi que leur serveur de noms faisant autorité. Les acteurs de menace peuvent également utiliser la domaines miroirs pour cacher la source de leurs attaques en recueillant les informations d'identification des comptes de domaine afin de créer silencieusement de multiples sous-domaines à utiliser lors des attaques. On oublie parfois en entreprise que le protocole DNS peut être utilisé par les réseaux de zombies. Les cyberpirates qui utilisent une attaque DNS par tunnellisation introduisent un trafic non DNS dans le trafic DNS. Cette méthode

permet généralement de contourner les solutions de sécurité. Pour arrêter les attaques DNS par tunnellisation, il faut utiliser un filtre inspectant le trafic DNS. Les serveurs DNS dynamiques sont populaires auprès des acteurs de menace et le trafic qui utilise le DNS dynamique devrait être une préoccupation particulière pour l'analyste de la cybersécurité.

DHCP utilise un simple échange de messages de diffusion et de monodiffusion pour fournir aux hôtes des informations d'adressage. Une attaque par usurpation DHCP se produit lorsqu'un serveur DHCP non autorisé (rogue) se connecte au réseau et fournit des paramètres de configuration IP incorrects aux clients légitimes. Le serveur non autorisé peut fournir des informations de passerelle par défaut, des informations de serveur DNS ou des informations d'adressage IP incorrectes.

Services professionnels:
Les navigateurs World Wide Web sont utilisés par presque tout le monde. Impossible d'envisager de bloquer complètement la navigation sur Internet, car les entreprises ont besoin d'accéder au web. Les analystes de cybersécurité doivent bien connaître le déroulement d'une attaque sur le web standard. Les étapes courantes d'une attaque web typique comprennent la visite, sans le savoir, par la victime d'une page web qui a été compromise par un logiciel malveillant. La page Web compromise redirige l'utilisateur vers un site qui héberge du code malveillant. Le navigateur est fait pour visiter ce site et le code malveillant infecte leur ordinateur. Ceci est connu sous le nom de téléchargement de type drive-by. Indépendamment du type d'attaque utilisé, l'acteur de menace souhaite avant tout s'assurer que le navigateur web de la victime accède à sa page web, sur laquelle repose l'attaque, qui sert ensuite à l'exploitation malveillante de la victime. Certains sites malveillants tirent parti de plug-ins vulnérables ou des vulnérabilités du navigateur pour compromettre le système du client. Les réseaux d'envergure s'appuient sur les systèmes IDS pour analyser les fichiers téléchargés à des fins d'exploitation malveillante. En cas de détection, le système IDS émet des alertes et enregistre l'événement dans les fichiers journaux à des fins d'analyse ultérieure. Les journaux de connexion au serveur révèlent souvent des informations sur le type d'analyse ou d'attaque. Les différents groupes de codes d'état de connexion sont les suivants: Informationnel 1xx, Couronné de succès 2xx, Redirection 3xx, Erreur client 4xx et erreur du serveur 5xx. Pour se défendre contre les attaques basées sur le Web, les contre-mesures qui doivent être utilisées incluent toujours la mise à jour du système d'exploitation et des navigateurs avec les correctifs et les mises à jour actuels, l'utilisation d'un proxy Web pour bloquer les sites malveillants, l'utilisation des meilleures pratiques de sécurité du Projet de sécurité des applications Web ouvertes (OWASP) lors du développement Web et éduquer les utilisateurs finaux en leur montrant comment éviter les attaques basées sur le Web.

Il existe un certain nombre d'attaques qui utilisent le courrier électronique pour transporter des charges utiles de logiciels malveillants ou pour hameçonner des

informations personnelles. Les serveurs SMTP peuvent également présenter des vulnérabilités et doivent être tenus à jour avec les correctifs. Les appliances de sécurité de la messagerie peuvent détecter et bloquer de nombreux types de menaces connues, y compris le phishing, le spam et les logiciels malveillants.

Les applications web se connectent généralement à une base de données. Étant donné que ces bases de données peuvent contenir des informations sensibles, elles sont souvent la cible d'attaques. Les attaques par injection de code et par injection SQL exploitent des champs d'entrée insuffisamment validés pour envoyer des commandes à des bases de données ou à d'autres applications afin d'accéder à des informations privées. Les attaques XSS (script intersite) se produisent lorsque les navigateurs exécutent des scripts malveillants sur le client et fournissent aux acteurs de menaces un accès aux informations sensibles sur l'hôte local.

Les 10 principaux risques de sécurité des applications Web OWASP sont conçus pour aider les organisations à créer des applications Web sécurisées. Il s'agit d'une liste utile de vulnérabilités potentielles qui sont couramment exploitées par les acteurs de menace.

Atténuation des attaques de réseau courantes:
Les bonnes pratiques suivantes sont appliquées pour sécuriser un réseau: développer une politique de sécurité écrite, former les collaborateurs, contrôler l'accès physique aux systèmes, utiliser des mots de passe forts, chiffrer et protéger par mot de passe les données sensibles, mettre en œuvre du matériel et des logiciels de sécurité, effectuer des sauvegardes et tester le retour d'informations. des fichiers, de l'arrêt des services et des ports inutiles, de la mise à jour des correctifs et de la réalisation d'audits et de tests de sécurité.

Le principal moyen d'atténuer les attaques de virus et de chevaux de Troie est le logiciel antivirus. Un professionnel de la sécurité du réseau doit connaître les principaux virus et suivre les mises à jour de sécurité concernant les virus émergents.

Les vers sont davantage basés sur le réseau que les virus. La réponse à une attaque de ver peut être divisée en quatre phases: confinement, inoculation, quarantaine et traitement.

Les attaques par reconnaissance peuvent être atténuées de plusieurs manières: mettez en œuvre l'authentification pour garantir un accès approprié, utilisez le chiffrement pour rendre inutiles les attaques par détection de paquets, utilisez des outils anti-reniflés pour détecter les attaques par détection de paquets, mettez en œuvre une infrastructure commutée et utilisez un pare-feu et un système de prévention des intrusions. Le chiffrement est également efficace pour limiter les attaques par détection de paquets. Plusieurs techniques sont disponibles pour limiter les attaques d'accès: une sécurité renforcée par mot de passe, le principe de

confiance minimale, la cryptographie et l'application de correctifs pour le système d'exploitation et les applications.

Pour réduire le nombre d'attaques DoS, un logiciel d'utilisation du réseau doit être exécuté en permanence. Les attaques DoS peuvent faire partie d'une offensive plus vaste. Les attaques DoS peuvent entraîner des problèmes dans les segments de réseau des ordinateurs attaqués. Par le passé, de nombreuses attaques DoS provenaient d'adresses usurpées.

Question 1 :
Quelle action décrit le mieux une attaque d'usurpation d'adresse MAC ?
Réponse : **modification de l'adresse MAC d'un hôte attaquant pour qu'elle corresponde à celle d'un hôte légitime**

Question 2 :
Quel est l'objectif d'une attaque d'usurpation DHCP ?
Réponse : **pour fournir de fausses adresses de serveur DNS aux clients DHCP afin que les visites d'un serveur Web légitime soient dirigées vers un serveur faux**

Question 3 :
Quel est le principal moyen pour atténuer les attaques par virus et par cheval de Troie ?
Réponse : **Logiciel antivirus**

Question 4 :
Quelle méthode peut être utilisée pour limiter les balayages ping ?
Réponse : **bloquer les échos et les réponses ICMP à la périphérie du réseau.**

Question 5 :
Quelle phase de réduction des vers implique la désinfection active des systèmes infectés ?
Réponse : **traitement**

Question 6 :
Quel est le résultat d'une attaque par insuffisance des ressources DHCP ?
Réponse : **Les clients légitimes ne peuvent pas louer d'adresses IP.**

Question 7 :
Quel terme est utilisé pour les e-mails publicitaires envoyés en masse à autant d'utilisateurs que possible ?
Réponse : **Courrier indésirable**

Question 8 :
Quel type d'attaque DNS implique que le cybercriminel compromet un domaine

parent et crée plusieurs sous-domaines à utiliser pendant les attaques ?
Réponse : **l'observation (ombrage)**

Question 9 :
Quel protocole est ciblé par une attaque par amortissement ?
Réponse : **DNS**

Question 10 :
Quel langage est utilisé pour interroger une base de données relationnelle ?
Réponse : **SQL**

Question 11 :
Quelles attaques ciblent des serveurs web en exploitant les éventuelles vulnérabilités des fonctions d'entrée utilisées par une application ? (Choisissez deux réponses.)
Réponses :

- **injection SQL**
- **scripting intersites**

Question 12 :
Dans quel type d'attaque des informations falsifiées sont-elles utilisées pour rediriger les utilisateurs vers des sites Internet malveillants ?
Réponse : **Empoisonnement du cache DNS**

Question 13 :
Quelle est la caractéristique d'une attaque d'amplification et de réflexion DNS ?
Réponse : **Les acteurs de menace utilisent des attaques DoS ou DDoS sur les résolveurs ouverts DNS pour augmenter le volume des attaques et masquer la véritable source d'une attaque.**

Module 5:Communication en réseau sans fil :

Communications sans fil:
Les périphériques de mise en réseau sans fil se connectent à un point d'accès (AP) ou à un contrôleur de réseau local sans fil (WLC) conformément à la norme 802.11. Le format de trame 802.11 est similaire au format de trame Ethernet, sauf qu'il contient de champs additionnels. Les appareils WLAN utilisent un accès multiple à détection de porteuse avec prévention des collisions (CSMA/CA) comme méthode pour déterminer comment et quand envoyer des données sur le réseau. Pour se connecter au WLAN, les périphériques sans fil réalisent un processus en trois étapes pour découvrir un point d'accès sans fil, s'authentifier auprès du point d'accès et s'associer au point d'accès. Les points d'accès peuvent être configurés de manière autonome (individuellement) ou à l'aide d'un WLC pour simplifier la configuration et la surveillance de nombreux points d'accès.

Menaces visant le réseau WLAN:
Les réseaux sans fil sont sensibles aux menaces, notamment l'interception de données, les intrus sans fil, les attaques DoS et les points d'accès malveillants. Les attaques DoS sans fil peuvent être le résultat: d'appareils mal configurés, d'un utilisateur malveillant interférant intentionnellement avec la communication sans fil et d'interférences accidentelles. Un point d'accès non autorisé est un point d'accès ou un routeur sans fil qui a été connecté à un réseau d'entreprise sans autorisation explicite. Une fois connecté, un acteur de menace peut utiliser le point d'accès non autorisé pour capturer des adresses MAC, capturer des paquets de données, accéder à des ressources réseau ou lancer une attaque MITM. Dans une attaque MITM, l'acteur de menace est positionné entre deux entités légitimes pour lire ou modifier les données qui passent entre les deux parties. Une attaque MITM sans fil populaire est appelée l'attaque «evil twin AP», où un acteur de menace introduit un AP escroc et le configure avec le même SSID qu'un AP légitime. Pour empêcher l'installation d'AP escrocs, les organisations doivent configurer les WLC avec des politiques d'AP escrocs.

WLAN sécurisés:
Pour éloigner les intrus sans fil et protéger les données, deux premières fonctions de sécurité sont toujours disponibles sur la plupart des routeurs et des points d'accès: le masquage SSID et le filtrage des adresses MAC. Il existe quatre techniques d'authentification par clé partagée: WEP, WPA, WPA2 et WPA3 (les appareils avec WPA3 ne sont pas encore disponibles). Les routeurs domestiques ont généralement deux choix pour l'authentification: WPA et WPA2. WPA2 est le plus fort des deux. Le cryptage est utilisé pour protéger les données. Les normes WPA et WPA2 utilisent les protocoles de cryptage suivants: TKIP et AES. Dans les réseaux qui ont des exigences de sécurité plus strictes, une authentification ou une connexion supplémentaire est requise pour accorder l'accès aux clients sans fil. Le choix du mode de sécurité d'entreprise nécessite un serveur RADIUS d'authentification, d'autorisation et de comptabilité (AAA).

Question 1 :
L'hôpital du centre-ville offre une connectivité WLAN à ses collaborateurs. La politique de sécurité exige que les communications entre les terminaux mobiles des collaborateurs et les points d'accès soient chiffrées. Quel est l'objectif de cette exigence ?
Réponse : **pour empêcher la lecture du contenu des messages interceptés**

Question 2 :
Quelle fonctionnalité peut être utilisée par un administrateur pour empêcher les utilisateurs non autorisés de se connecter à un point d'accès sans fil ?
Réponse : **Filtrage des adresses MAC**

Question 3 :
Quel est l'avantage du masquage SSID ?
Réponse : **Les clients doivent identifier manuellement le SSID pour se connecter au réseau.**

Question 4 :
Pour quel mode de découverte un point d'accès générera-t-il le plus de trafic sur un WLAN ?
Réponse : **mode actif**

Question 5 :
Dans une université locale, les étudiants sont autorisés à se connecter au réseau sans fil sans mot de passe. Quel mode le point d'accès utilise-t-il ?
Réponse : **ouvert**

Question 6 :
Un collaborateur se connecte sans fil au réseau de l'entreprise à l'aide d'un téléphone portable. Le collaborateur configure ensuite son téléphone portable pour qu'il agisse comme un point d'accès sans fil et permette aux nouveaux collaborateurs de se connecter au réseau de l'entreprise. Quel type de menace pour la sécurité décrit le mieux cette situation ?
Réponse : **point d'accès non autorisé**

Question 7 :
Le manuel de l'entreprise indique que les employés ne peuvent pas avoir de fours à micro-ondes dans leurs bureaux. Au lieu de cela, tous les employés doivent utiliser les fours à micro-ondes situés dans la cafétéria des employés. Quel risque pour la sécurité sans fil l'entreprise essaie-t-elle d'éviter ?
Réponse : **interférence accidentelle**

Question 8 :
Quels sont les deux rôles généralement remplis par un routeur sans fil utilisé dans une maison ou une petite entreprise ? (Choisissez deux réponses.)
Réponses :

- **Commutateur Ethernet**
- **Point d'accès**

Question 9 :
Quelle méthode d'authentification sans fil dépend d'un serveur d'authentification RADIUS ?
Réponse : **WPA2 Enterprise**

Question 10 :
Quelle méthode de cryptage sans fil est la plus sûre ?
Réponse : **WPA2 avec AES**

Question 11 :
Quel paramètre est généralement utilisé pour identifier un nom de réseau sans fil lorsqu'un point d'accès sans fil domestique est configuré ?
Réponse : **SSID**

Question 12 :
Quel paramètre sans fil fait référence aux bandes de fréquences utilisées pour transmettre des données à un point d'accès sans fil ?
Réponse : **paramètres de canal**

Question 13 :
Quel périphérique peut commander et gérer un grand nombre de points d'accès d'entreprise ?
Réponse : **WLC**

Question 14 :
Un ingénieur sans fil compare le déploiement d'un réseau utilisant l'authentification WPA2 à l'authentification WPA3. Comment l'authentification WPA3 est-elle plus sécurisée lorsqu'elle est déployée dans un réseau WLAN ouvert dan

Module 6:Infrastructure de sécurité du réseau :

Dispositifs de sécurité:
Il existe plusieurs types de pare-feu. Pare-feu (apatride) de filtrage des paquets assure le filtrage de couche 3 et parfois de couche 4. La conception des pare-feu repose principalement sur des interfaces d'appareils qui autorisent ou refusent le trafic en fonction de la source, de la destination et du type de trafic. Un pare-feu d'inspection (avec état) autorise ou bloque le trafic selon l'état, le port et le protocole. Pare-feu de la passerelle d'applications (pare-feu proxy) filtre les informations au niveau des couches 3, 4, 5 et 7. Les pare-feu de nouvelle génération fournissent des services supplémentaires au-delà des passerelles d'application, tels que la prévention intégrée des intrusions, la sensibilisation et le contrôle des applications pour voir et bloquer les applications à risque, l'accès aux futurs flux d'informations et les techniques permettant de faire face aux menaces de sécurité en constante évolution. Les systèmes de prévention des intrusions (IPS) et les systèmes de détection des intrusions (IDS) sont utilisés pour détecter les risques potentiels de sécurité et alerter/arrêter le trafic dangereux. IDS/IPS peut être implémenté en tant qu'hôte ou réseau avec des avantages et des inconvénients spécifiques à chaque implémentation. Des appliances de sécurité spécialisées sont disponibles, notamment Protection avancée contre les logiciels malveillants de Cisco (AMP), Cisco Web Security Appliance (WSA) et Cisco Email Security Appliance (WSA). Ces appliances de sécurité utilisent les services de Cisco Talos Security Intelligence and Research Group. L'équipe Talos identifie et met en corrélation les attaques en temps réel grâce au réseau de détection le plus étendu au monde.

Services de sécurité:
Les services de sécurité réseau incluent les technologies suivantes. Les listes de contrôle d'accès sont une série de commandes qui déterminent si un routeur achemine ou abandonne les paquets en fonction des informations contenues dans l'en-tête de paquet. NTP synchronise l'heure sur tous les appareils du réseau afin d'assurer un horodatage précis et cohérent des messages système. Les serveurs Syslog permet d'accéder aux messages système générés par les périphériques réseau. SNMP permet aux administrateurs réseau de contrôler et de gérer les performances du réseau, d'identifier et de résoudre les problèmes et d'anticiper la croissance du réseau. NetFlow est une technologie Cisco qui fournit des statistiques sur les paquets transitant par un routeur ou un commutateur multicouche Cisco. Mise en miroir du port est une fonctionnalité qui permet à un commutateur de dupliquer des copies du trafic qui le traverse, puis d'envoyer les données depuis un port équipé d'un système de surveillance du réseau. AAA est un cadre pour configurer les services d'authentification, d'autorisation et de comptabilité des utilisateurs. AAA utilise généralement un serveur TACACS+ ou RAYON à cette fin. Les VPN sont des réseaux privé créés entre deux terminaux sur un réseau public.
Question 1 :
Quel est le but d'un pare-feu personnel sur un ordinateur ?
Réponse : **pour filtrer le trafic qui se déplace à l'intérieur et à la sortie du PC**

Question 2 :
Quelle est la principale différence entre la mise en œuvre des dispositifs IDS et IPS ?
Réponse : **Un IDS permettrait au trafic malveillant de passer avant qu'il ne soit adressé, alors qu'un IPS l'arrête immédiatement.**

Question 3 :
Quel protocole offrant des services d'authentification, d'intégrité et de confidentialité est également un type de réseau privé virtuel ?
Réponse : **IPsec**

Question 4 :
Parmi les affirmations suivantes, laquelle est une caractéristique du protocole TACACS+ ?
Réponse : **Il chiffre tout le corps du paquet pour des communications plus sécurisées.**

Question 5 :
Quelle fonctionnalité du pare-feu permet de s'assurer que les paquets entrants sur un réseau sont des réponses légitimes à des requêtes provenant d'hôtes internes ?
Réponse : **Filtrage dynamique de paquets (SPI)**

Question 6 :
Reportez-vous à l'illustration. Le réseau « A » contient plusieurs serveurs

d'entreprise auxquels des hôtes accèdent via Internet pour obtenir des informations sur la société. Quel terme est utilisé pour décrire le réseau « A » ?
Réponse : **DMZ**

Question 7 :
Quelle déclaration décrit la sécurité Web Cisco Cloud ?
Réponse : **Il s'agit d'un service de sécurité basé sur le cloud permettant d'analyser le trafic à la recherche de logiciels malveillants et d'appliquer.**

Question 8 :
Quels énoncés à propos des serveurs NTP dans un réseau d'entreprise sont corrects ? (Choisissez deux réponses.)
Réponses :

- **Les serveurs NTP assurent un horodatage précis des informations de journalisation et de débogage.**
- **Les serveurs NTP de strate 1 sont connectés directement à une source temporelle faisant autorité.**

Question 9 :
Comment une adresse IP source est-elle utilisée dans une liste de contrôle d'accès standard ?
Réponse : **Il s'agit du critère utilisé pour filtrer le trafic.**

Question 10 :
Quel service réseau permet aux administrateurs de surveiller et de gérer les périphériques réseau ?
Réponse : **SNMP**

Question 11 :
Pouvez-vous citer une fonction d'un pare-feu proxy ?
Réponse : **Il se connecte à des serveurs distants pour le compte de clients**

Question 12 :
Quelle technologie de surveillance du réseau permet à un commutateur de copier et de transférer le trafic envoyé et reçu sur plusieurs interfaces, via une autre interface, vers un dispositif d'analyse du réseau ?
Réponse : **Mise en miroir des ports**

Module 7:Le système d'exploitation windows :

Histoire de windows:
Les premiers ordinateurs nécessitaient un système d'exploitation de disque (DOS) pour créer et gérer des fichiers. Microsoft a développé MS-DOS comme interface de ligne de commande (CLI) pour accéder au lecteur de disque et charger les fichiers du système d'exploitation. Les premières versions de Windows se composaient

d'une interface utilisateur graphique (GUI) exécutée sur MS-DOS. Cependant, les versions modernes de Windows sont en contrôle direct de l'ordinateur et de son matériel et prennent en charge plusieurs processus utilisateur. contrairement à MS-DOS qui fonctionne en mode monotâche et mono-utilisateur. Depuis 1993, plus de 20 versions de Windows basées sur le système d'exploitation NT ont vu le jour. Les utilisateurs utilisent une interface graphique Windows pour travailler avec des fichiers de données et des logiciels. L'interface graphique comporte une zone principale appelée Bureau et une barre des tâches située sous le Bureau. La barre des tâches comprend le menu Démarrer , les éléments de lancement rapide et la zone de notification. Windows présente de nombreuses vulnérabilités. Les recommandations pour sécuriser le système d'exploitation Windows incluent l'utilisation de la protection contre les virus ou les logiciels malveillants, l'utilisation de mots de passe forts, l'utilisation d'un pare-feu et l'utilisation limitée du compte administrateur, entre autres.

Architecture et fonctionnement de windows:
Windows comporte une couche d'abstraction du matériel est un code qui gère l'ensemble des communications entre le matériel et le noyau. Le noyau gère toutes les demandes d'entrée et de sortie, la mémoire ainsi que tous les appareils connectés à l'ordinateur. Windows fonctionne dans deux modes différents. Le premier est le mode utilisateur. La plupart des programmes dans Windows s'exécutent en mode utilisateur. Le second est le mode noyau. Il permet un accès direct au code du système d'exploitation au matériel informatique. Windows prend en charge plusieurs systèmes de fichiers différents, mais NTFS est le plus utilisé. Les volumes NTFS incluent le secteur de démarrage de la partition, la table de fichiers maître, les fichiers système et la zone de fichiers. Lorsqu'un ordinateur démarre, il accède d'abord aux informations système et au code stockés dans le matériel du BIOS. Le code de démarrage du BIOS effectue un auto-test système appelé POST, localise et charge le système d'exploitation Windows et charge d'autres programmes associés pour démarrer le système d'exploitation. Windows doit toujours être arrêté correctement.

Pour fonctionner, un ordinateur stocke des instructions dans la mémoire RAM en vue de leur traitement par le processeur. Chaque processus d'un ordinateur Windows 32 bits prend en charge un espace d'adressage virtuel de 4 gigaoctets maximum. Chaque processus d'un ordinateur Windows 64 bits prend en charge un espace d'adressage virtuel jusqu'à 8 téraoctets. Windows stocke toutes les informations relatives aux paramètres du matériel, des applications, des utilisateurs et du système dans une grande base de données appelée le Registre. Le registre est une base de données hiérarchique dont le niveau le plus élevé est appelé ruche , et dont les niveaux inférieurs sont appelés clés ou sous-clés, respectivement. Il existe cinq ruches de Registre qui contiennent des données concernant la configuration et le fonctionnement de Windows. Il y a des centaines de clés et de sous-clés.

Configuration et contrôle de windows :
Pour des raisons de sécurité, il est déconseillé de se connecter à Windows avec le compte d'administrateur ou un compte disposant de privilèges d'administrateur. Ne donnez pas de privilèges d'administration aux utilisateurs standard. N'activez pas le compte Invités à moins que l'ordinateur ne soit utilisé par de nombreuses personnes différentes qui n'ont pas de compte. Pour faciliter l'administration des utilisateurs, Windows utilise des groupes. Les utilisateurs et les groupes locaux sont gérés à l'aide de l'applet lusrmgr.msc du panneau de configuration.

Vous pouvez utiliser l'interface de ligne de commande ou Windows PowerShell pour exécuter des commandes. PowerShell, permet de créer des scripts d'automatisation des tâches que l'interface de ligne de commande standard ne peut pas créer. Windows Management Instrumentation (WMI) est utilisé pour gérer les ordinateurs distants. La commande net peut être combinée avec des commutateurs pour se concentrer sur une sortie spécifique. Le gestionnaire des tâches fournit de nombreuses informations sur tout ce qui est en cours d'exécution et sur les performances générales de l'ordinateur. Le moniteur de ressources fournit des informations plus détaillées sur l'utilisation des ressources. Le centre Réseau et partage permet de configurer et de tester les propriétés du réseau Windows. Le protocole SMB (Bloc de messages du serveur) est utilisé pour partager des ressources réseau. Le format UNC (Convention de dénomination universelle) vous permet de vous connecter aux ressources. Windows Server, une autre édition de Windows, est principalement utilisé dans les data centers. Il fournit des services de réseau, de fichiers, de Web et de gestion à un réseau ou à un domaine Windows.

Sécurité windows:
Les logiciels malveillants peuvent ouvrir des ports de communication pour communiquer et diffuser. La commande Windows netstat affiche tous les ports de communication ouverts sur un ordinateur et peut également afficher les processus logiciels qui sont associés aux ports. Cela permet d'identifier et d'arrêter les logiciels potentiellement malveillants inconnus. L'observateur d'événements Windows permet d'accéder à de nombreux événements consignés concernant le fonctionnement d'un ordinateur. Windows enregistre les événements Windows et les événements d'applications et de services. Les niveaux de gravité des événements consignés varient entre les niveaux d'information, d'avertissement, d'erreur ou critique. Il est très important de garder Windows à jour pour se prémunir contre les nouvelles menaces de sécurité. Les correctifs logiciels, les mises à jour et les Service Packs corrigent les vulnérabilités de sécurité à mesure qu'elles sont découvertes Windows doit être configuré pour télécharger et installer automatiquement les mises à jour à mesure qu'elles deviennent disponibles. Windows peut être configuré pour installer et redémarrer un ordinateur uniquement à des heures spécifiées de la journée.

Question 1 :
Lorsqu'un utilisateur apporte des modifications aux paramètres d'un système

Windows, où ces modifications sont-elles stockées ?
Réponse : **Registre**

Question 2 :
En matière de sécurité, un administrateur de réseau doit s'assurer que les ordinateurs locaux ne peuvent pas se lancer de requêtes ping. Quels paramètres peuvent accomplir cette tâche ?
Réponse : **Paramètres du pare-feu**

Question 3 :
Quel compte utilisateur doit être utilisé uniquement pour effectuer la gestion du système et non comme compte pour une utilisation régulière ?
Réponse : **Administrateur**

Question 4 :
Quelle technologie a été développée pour remplacer le programme BIOS sur les cartes mères des ordinateurs personnels modernes ?
Réponse : **UEFI**

Question 5 :
Quel terme désigne un lecteur logique pouvant être formaté pour le stockage de données ?
Réponse : **volume**

Question 6 :
Quel utilitaire permet de visualiser les ressources système utilisées par chaque utilisateur ?
Réponse : **Gestionnaire des tâches**

Question 7 :
Quelle commande permet d'interroger manuellement un serveur DNS pour résoudre un nom d'hôte spécifique ?
Réponse : **nslookup**

Question 8 :
Quelle commande net n'ayant pas d'espace de coupure est utilisée sur un PC Windows pour établir une connexion avec un répertoire partagé sur un serveur distant ?
Réponse : **net use**

Question 9 :
Qu'est-ce qui s'afficherait si la commande netstat -abno était saisie sur un PC Windows ?
Réponse : **toutes les connexions TCP et UDP actives, leur état actuel et l'ID de processus (PID) associé**

Question 10 :
Quel est le but de la commande cd\ ?
Réponse : **Définir le répertoire sur le répertoire racine**

Question 11 :
Quelle fut la première version de Windows à être disponible avec une architecture 64 bits ?
Réponse : **Windows XP**

Question 12 :
Quelle est la quantité de mémoire vive adressable par une version 32 bits de Windows ?
Réponse : **4 Go**

Question 13 :
Un incident a été consigné et un employé pense que quelqu'un a utilisé son ordinateur depuis qu'il a quitté son poste la veille au soir. L'employé affirme qu'il a éteint son ordinateur avant de partir. L'ordinateur est très lent et les applications présentent un comportement étrange. Quel outil de Microsoft Windows l'analyste en sécurité peut-il utiliser pour déterminer si quelqu'un s'est connecté à l'ordinateur après les heures de bureau et le moment auquel cette intrusion a eu lieu ?
Réponse : **Observateur d'événements**

Module 8:Présentation de linux :

Les bases de linux:
Linux est un système d'exploitation open-source rapide, fiable et de petite taille. Il nécessite peu de ressources matérielles pour fonctionner et est hautement personnalisable. Il est conçu pour être utilisé sur des réseaux. Le noyau Linux est distribué par différentes organisations avec différents outils et paquets logiciels. Une version personnalisée de Linux, appelée Security Onion, contient des logiciels et des outils conçus pour être utilisés dans le cadre de la surveillance de la sécurité des réseaux par les analystes en cybersécurité. Kali Linux est une autre distribution personnalisée de Linux qui possède de nombreux outils conçus pour les tests de pénétration de la sécurité des réseaux.

Travailler dans le shell linux:
Sous Linux, l'utilisateur communique avec le système d'exploitation par le biais d'une interface graphique ou d'une interface de ligne de commande (CLI), ou shell. Si une interface graphique est en cours d'exécution, l'interpréteur de commandes est accessible via une application de terminal telle que xterm ou gnome terminal. Les commandes Linux sont des programmes qui exécutent une tâche spécifique. La commande man, suivie d'une commande spécifique, fournit de la documentation pour cette commande. Il est important de connaître au moins les commandes Linux de base, les commandes de fichiers et de répertoires, et les commandes permettant

de travailler avec des fichiers texte. Dans Linux, tout est traité comme s'il s'agissait d'un fichier, y compris la mémoire, les disques, le moniteur et les répertoires.

Serveurs et clients linux:
Les serveurs sont des ordinateurs sur lesquels sont installés des logiciels qui leur permettent de fournir des services aux ordinateurs clients sur le réseau. Certains services permettent aux clients qui en font la demande d'accéder à des ressources externes telles que des fichiers, des courriers électroniques et des pages Web. D'autres services fonctionnent en interne et effectuent des tâches telles que la gestion des journaux, la gestion de la mémoire ou l'analyse des disques. Pour permettre à un ordinateur de fournir plusieurs services, on utilise des ports. Un port est une ressource réseau réservée qui "écoute" les demandes des clients. Bien que le numéro du port utilisé par un service puisse être configuré, la plupart des services écoutent sur des ports par défaut "bien connus". Les applications logicielles clientes sont conçues pour communiquer avec des types de serveurs spécifiques. Les navigateurs Web sont conçus pour communiquer avec les serveurs Web en utilisant le protocole HTTP sur le port 80. Les clients FTP communiquent avec les serveurs FTP pour transférer des fichiers.

Administration de base du serveur:
Sous Linux, les serveurs sont gérés à l'aide de fichiers de configuration. Divers paramètres peuvent être modifiés et enregistrés dans les fichiers de configuration. Lorsqu'un service est lancé, il consulte son ou ses fichiers de configuration pour savoir comment il doit fonctionner. Il n'y a pas de règle concernant la façon dont les fichiers de configuration sont écrits. Le formatage des fichiers de configuration dépend du créateur du logiciel serveur. Les périphériques Linux doivent être sécurisés en utilisant des méthodes éprouvées pour protéger le périphérique et l'accès administratif. C'est ce qu'on appelle le durcissement des périphériques. Une façon de renforcer un périphérique est de conserver les mots de passe, de configurer des fonctions de connexion améliorées et d'implémenter une connexion à distance sécurisée avec SSH. Il est également très important de maintenir le système d'exploitation à jour. D'autres moyens de renforcer un dispositif sont de forcer des changements de mot de passe périodiques, d'imposer des mots de passe forts et d'empêcher la réutilisation des mots de passe. Enfin, les clients et serveurs Linux utilisent des fichiers journaux pour enregistrer le fonctionnement du système et les événements importants. Un certain nombre de fichiers journaux différents sont maintenus, notamment les journaux d'applications, les journaux d'événements, les journaux de services et les journaux système. Les journaux du serveur enregistrent les activités menées par les utilisateurs distants qui accèdent aux services du système. Il est important de connaître l'emplacement des différents journaux dans le système de fichiers Linux afin de pouvoir y accéder et de surveiller les problèmes.

Le système de fichiers linux:

Linux prend en charge un certain nombre de systèmes de fichiers différents qui varient en termes de vitesse, de flexibilité, de sécurité, de taille, de structure, de logique, etc. Certains des systèmes de fichiers pris en charge par Linux sont ext2, ext3, ext4, NFS et CDFS. Les systèmes de fichiers sont montés sur des partitions et accessibles via des points de montage, ou des répertoires. Les lettres de lecteur de Windows sont des exemples de points de montage. La commande mount peut être utilisée pour afficher les détails des systèmes de fichiers qui sont actuellement montés sur un ordinateur Linux. Le système de fichiers racine est représenté par le symbole '/'. Il contient par défaut tous les fichiers de l'ordinateur. Linux utilise les autorisations de fichiers pour contrôler qui est autorisé à avoir différents types d'accès aux fichiers et aux répertoires. Les autorisations comprennent la lecture (r), l'écriture (w) et l'exécution (x). Les fichiers et les répertoires ont des autorisations qui sont attribuées pour les utilisateurs, les groupes et autres. Les autorisations des fichiers et des dossiers sont affichées à l'aide de la commande ls -l. Cette commande affiche également les liens d'un fichier. Les liens matériels créent un autre fichier avec un nom différent qui est lié au même endroit dans le système de fichiers. Le propriétaire du fichier et le groupe du fichier sont également affichés, ainsi que la date et l'heure de la dernière modification du fichier. Les autorisations de fichiers sont des fonctionnalités puissantes du système de fichiers Linux et ne peuvent pas être violées. Seul l'utilisateur root peut outrepasser les autorisations de fichiers. En raison du pouvoir de l'utilisateur root, l'accès root doit être soigneusement contrôlé. Les liens durs sont créés avec la commande ln. Les modifications apportées à l'un des fichiers liés en dur sont également apportées au fichier d'origine. Les liens symboliques, ou symlinks, sont similaires aux liens physiques en ce sens qu'une modification du fichier lié est répercutée sur le fichier d'origine. Les liens symboliques présentent plusieurs avantages par rapport aux liens physiques.

Travailler avec l’interface graphique de linux:

Le système X Windows, ou X11, est un environnement logiciel de base qui comprend des fonctions permettant de créer, de contrôler et de configurer une interface graphique de fenêtres dans une interface de type pointer-cliquer. Différents fournisseurs utilisent le système X Windows pour créer différents gestionnaires de fenêtres pour Linux. Des exemples de gestionnaires de fenêtres sont Gnome et KDE. La distribution Ubuntu Linux utilise Gnome 3 par défaut. Le bureau Gnome 3 se compose du menu des applications, du dock Ubuntu, de la barre supérieure, du calendrier et de la zone des messages système, de la zone des activités et du menu d'état.

Travailler avec un ordinateur linux:

Afin d'installer des applications sur des ordinateurs Linux, des programmes appelés gestionnaires de paquets sont utilisés. Les paquets sont des applications logicielles et tous les fichiers qui les accompagnent. Les gestionnaires de paquets sont extrêmement utiles pour installer des applications logicielles complexes à partir de

dépôts de paquets centralisés accessibles sur Internet. Différentes distributions Linux utilisent différents gestionnaires de paquets. Par exemple, Arch Linux utilise pacman, Debian utilise dpkg comme gestionnaire de paquets de base et apt pour communiquer avec dpkg. Ubuntu utilise également apt. Les commandes CLI du gestionnaire de paquets sont utilisées pour installer, supprimer et mettre à jour les paquets logiciels. Les commandes de mise à jour mettent à niveau tous les paquets actuellement installés. La gestion des paquets peut également être effectuée dans une interface graphique. Les processus logiciels sont des instances de programmes informatiques en cours d'exécution. Les systèmes d'exploitation multitâches peuvent exécuter plusieurs processus en même temps. La duplication est une méthode utilisée par le noyau pour permettre à un processus en cours d'exécution de se copier lui-même. La commande ps répertorie les processus en cours d'exécution, top affiche des informations sur les processus en cours d'exécution de manière dynamique, et kill est utilisé pour supprimer, redémarrer ou mettre en pause les processus en cours d'exécution. Bien que Linux soit considéré comme mieux protégé contre les logiciels malveillants (malware) que d'autres systèmes d'exploitation, il reste sensible aux chevaux de Troie, aux vers et à d'autres types de malware. Linux est généralement attaqué par ses services et ses processus. Les logiciels obsolètes sont souvent vulnérables aux attaques. Les acteurs de la menace peuvent sonder un appareil à la recherche de ports ouverts liés à des processus de serveur obsolètes. Avec cette connaissance, des attaques peuvent être lancées. Il est important de maintenir le système d'exploitation, ses composants et ses applications à jour. Le programme chkrootkit est conçu pour détecter les logiciels malveillants de type rootkit. Les rootkits sont des programmes malveillants de niveau inférieur qui sont très difficiles à détecter et à supprimer. Ils peuvent modifier le fonctionnement fondamental du système d'exploitation lui-même et peuvent être utilisés pour créer un accès non autorisé aux systèmes. Les commandes de pipeline utilisent le symbole '|' pour enchaîner différentes commandes en utilisant la sortie d'une commande comme entrée pour une autre.

Question 1 :
Un auteur télécharge un document de chapitre de son ordinateur personnel vers un serveur de fichiers d'une maison d'édition. Quel rôle joue le PC dans ce modèle de réseau ?
Réponse : **Client**

Question 2 :
Dans le cas d'un système d'exploitation Linux, quelle commande permet d'afficher la syntaxe et les paramètres d'une commande spécifique ?
Réponse : **man**

Question 3 :
Un administrateur système lance la commande ps sur un serveur qui exécute le

système d'exploitation Linux. Quel est l'objectif de cette commande ?
Réponse : **répertorier les processus en cours d'exécution dans le système**

Question 4 :
Un administrateur système lance la commande apt-get upgrade sur un système d'exploitation Linux. Quel est l'objectif de cette commande ?
Réponse : **Chaque application installée sera mise à jour vers la dernière version.**

Question 5 :
Pourquoi un attaquant utiliserait-il un rootkit ?
Réponse : **Pour accéder à un périphérique sans être détecté**

Question 6 :
Considérez le résultat de la commande ls -l dans la sortie Linux ci-dessous. Quelles sont les autorisations de groupe de fichiers attribuées au fichier analyst.txt ?
Réponse : **lecture, écriture**

Question 7 :
Quel type d'outil est utilisé par un administrateur Linux pour attaquer un ordinateur ou un réseau dans le but de trouver des vulnérabilités ?
Réponse : **Test d'intrusion**

Question 8 :
En quoi le fait d'être un système d'exploitation Open Source constitue-t-il un avantage de Linux ?
Réponse : **Le code source de la distribution Linux peut être modifié, puis recompilé.**

Question 9 :
Quelle méthode peut-on utiliser pour sécuriser un appareil ?
Réponse : **Modifier régulièrement les mots de passe.**

Question 10 :
Quelle commande Linux peut être utilisée pour afficher le nom du répertoire de travail en cours ?
Réponse : **pwd**

Question 11 :
Quel est le système de fichiers primaire utilisé par Apple dans les ordinateurs Macintosh actuels ?
Réponse : **APFS**

Question 12 :
Un technicien a capturé des paquets sur un réseau particulièrement lent à accéder à Internet. Quel numéro de port le technicien doit-il rechercher dans les trames

capturées pour localiser les paquets HTTP ?
Réponse : **80**

Question 13 :
Quel code source du système d'exploitation peut être téléchargé et modifié par une personne ou une entreprise ?
Réponse : **Linux**

Question 14 :
Qu'est-ce qu'un démon ?
Réponse : **Un processus d'arrière-plan qui s'exécute automatiquement**

Module 9:Protection des systèmes et des terminaux :

Protéger les systèmes et les appareils:
Pour sécuriser un système d'exploitation, les administrateurs doivent supprimer tous les programmes et services inutiles, et s'assurer que les correctifs de sécurité et les mises à jour sont installés. Une entreprise doit établir des procédures pour surveiller les informations liées à la sécurité, évaluer les mises à jour et installer les mises à jour à l'aide d'un plan documenté. En outre, ils doivent identifier les vulnérabilités potentielles en établissant une référence pour comparer les performances d'un système.

Les logiciels malveillants comprennent les virus, les vers, les chevaux de Troie, les enregistreurs de frappe, les logiciels espions et les logiciels publicitaires. Ils portent atteinte à la vie privée, volent des informations, endommagent le système ou suppriment et corrompent des données. Utilisez un logiciel antimalware fiable. Les virus sans fichier utilisent des langages de script tels que Windows PowerShell et sont difficiles à détecter. Les langages de script tels que Python, Bash ou VBA peuvent être utilisés pour créer des malwares. Supprimez immédiatement les logiciels non conformes.

Les correctifs sont des mises à jour de code qui empêchent un nouveau virus, ver ou autre logiciel malveillant de réussir une attaque. Les correctifs et les mises à niveau sont souvent combinés dans un service pack. Un outil de gestion des correctifs peut être utilisé pour gérer les correctifs localement. Il est également important de mettre à jour les applications tierces telles qu'Adobe Acrobat, Java et Chrome pour corriger les vulnérabilités. Un pare-feu basé sur l'hôte s'exécute sur un périphérique pour limiter l'activité réseau entrante et sortante pour ce périphérique. Le logiciel HIDS

surveille les appels système et l'accès au système de fichiers pour détecter les requêtes malveillantes. HIPS surveille un périphérique pour les attaques et les anomalies connues. EDR surveille et collecte en permanence les données d'un terminal, puis analyse les données et répond à toutes les menaces. Les outils DLP garantissent que les données sensibles ne sont pas perdues ou accessibles par des utilisateurs non autorisés. Le pare-feu NGFW combine un pare-feu classique avec d'autres fonctions de filtrage des périphériques réseau. Le chiffrement est un outil utilisé pour protéger les données en utilisant un algorithme pour les transformer et les rendre illisibles.

La fonctionnalité EFS (Système de fichiers de cryptage Windows) permet aux utilisateurs de chiffrer des fichiers, des dossiers ou un disque dur entier. L'intégrité du démarrage garantit que le système est fiable et qu'il n'a pas été altéré pendant le chargement du système d'exploitation. Le démarrage sécurisé est un standard de sécurité qui garantit qu'un périphérique démarre à l'aide d'un logiciel fiable. Le démarrage mesuré permet d'identifier les applications non fiables qui tentent de se charger et permet également aux antimalwares de se charger plus tôt.

Les administrateurs doivent mettre en place des politiques et des contre-mesures pour les logiciels non corrigés, les téléchargements d'utilisateurs non autorisés, les malwares, les périphériques sans surveillance, les violations des politiques d'utilisation acceptable et les supports non autorisés. Protégez les équipements physiques avec des câbles de verrouillage, des verrous de porte chiffrés, des cages de Faraday pour bloquer les champs électromagnétiques et des balises RFID pour identifier et suivre les éléments. Protection contre les programmes malveillants.

Les points d'extrémité sont des hôtes sur le réseau qui peuvent accéder à (ou être accédés par) d'autres hôtes sur le réseau. Avec l'IoT, d'autres types d'équipements sont désormais des terminaux. Chaque point d'extrémité est une ouverture potentielle permettant à un logiciel malveillant d'accéder au réseau. Tous les points d'extrémité ne se trouvent pas dans le réseau. De nombreux points de terminaison se connectent aux réseaux à distance via VPN. Le périmètre du réseau est en constante expansion. Divers appareils de sécurité du réseau sont nécessaires pour protéger le périmètre du réseau contre tout accès extérieur. De nombreuses attaques proviennent de l'intérieur du réseau. par conséquent, la sécurisation d'un LAN interne est également importante. Une fois qu'un hôte interne est infecté, il peut devenir un point d'entrée pour un hacker qui souhaite accéder à des éléments critiques du système. Il y a deux éléments internes au LAN à sécuriser: les points de terminaison et l'infrastructure du réseau.

Un logiciel antivirus/antimalware est installé sur un hôte pour détecter et atténuer les virus et les logiciels malveillants. Pour ce faire, il utilise des méthodes basées sur les signatures (en utilisant diverses caractéristiques des fichiers de logiciels malveillants connus), sur l'heuristique (en utilisant des caractéristiques générales partagées par divers types de logiciels malveillants) et sur le comportement (en utilisant une

analyse du comportement suspect). De nombreux programmes antivirus sont capables de fournir une protection en temps réel en analysant les données au fur et à mesure qu'elles sont utilisées par le terminal. Un pare-feu basé sur l'hôte limite les connexions entrantes et sortantes aux seules connexions initiées par cet hôte. Certains logiciels de pare-feu peuvent également empêcher l'infection d'un hôte et les hôtes infectés de propager des malwares à d'autres hôtes. La plupart des logiciels de sécurité d'hôte incluent une fonctionnalité de journalisation efficace, essentielle aux opérations de cybersécurité. Pour protéger les points d'extrémité dans un réseau sans frontières, utilisez des techniques basées sur le réseau et sur l'hôte.

Prévention des intrusions basée sur l'hôte:
Les pare-feu d'hôte utilisent un ensemble de politiques ou de profils prédéfinis pour contrôler les paquets entrant et sortant sur un ordinateur. Ils peuvent aussi avoir des règles qui peuvent être directement modifiées ou créées pour contrôler l'accès en fonction des adresses, des protocoles et des ports. Ils peuvent aussi être configurés pour émettre des alertes aux utilisateurs si un comportement suspect est détecté. La journalisation d'événements varie en fonction de l'application de pare-feu. Elle inclut généralement la date et l'heure de l'événement, si la connexion a été autorisée ou refusée, des informations sur les adresses IP source ou de destination des paquets, et les ports source et de destination des segments encapsulés. (Les pare-feu distribués combinent les caractéristiques des pare-feu basés sur l'hôte avec une gestion centralisée).

Quelques exemples de pare-feu basés sur l'hôte incluent le pare-feu Windows Defender, iptables, nftables et TCP Wrappers. Un HIDS protège les hôtes contre les logiciels malveillants connus et inconnus. Il peut effectuer une surveillance et des rapports détaillés sur la configuration du système et l'activité des applications, l'analyse des journaux, la corrélation des événements, la vérification de l'intégrité, l'application des politiques, la détection des rootkits et les alertes. Un HIDS comprend souvent un serveur de gestion. Le logiciel HIDS devant s'exécuter directement sur l'hôte, il est considéré comme un système basé sur un agent. Un HIDS utilise à la fois des stratégies proactives et réactives. Un HIDS peut protéger des intrusions, car il utilise des signatures pour détecter les malwares connus et les empêcher d'infecter un système.

Les signatures ne sont pas efficaces contre les nouvelles menaces ou celles de tapez zéro jour. En outre, certaines catégories de malwares utilisent le polymorphisme. D'autres stratégies visant à détecter la possibilité d'attaques réussies comprennent la détection basée sur les anomalies et la détection basée sur les politiques.

Sécurité des applications:
La surface d'exposition aux attaques est la somme totale des vulnérabilités d'un système donné qu'un hacker peut exploiter. Il peut s'agir de ports ouverts sur des

serveurs ou des hôtes, de logiciels fonctionnant sur des serveurs orientés Internet, de protocoles de réseau sans fil, de dispositifs à distance et même d'utilisateurs. La surface d'exposition aux attaques continue de s'élargir. De plus en plus d'appareils se connectent aux réseaux grâce à l'IdO et au BYOD.

L'Institut SANS décrit trois composantes de la surface d'attaque: la surface d'attaque réseau, la surface d'attaque logicielle et la surface d'attaque humaine. Une façon de réduire la surface d'exposition aux attaques consiste à limiter l'accès aux menaces potentielles en créant des listes d'applications interdites. De même, une organisation peut créer des listes de programmes autorisés en fonction d'une base de sécurité qu'elle a établie. Le sandboxing est une technique qui consiste à analyser les fichiers suspects et à les exécuter dans un environnement sécurisé. Les sandboxes d'analyse automatisée des malwares offrent des outils qui analysent le comportement des malwares. Ces outils observent les actions de malwares inconnus lors de leur exécution afin que les caractéristiques de leur comportement puissent être déterminées puis utilisées pour créer des défenses contre eux. Les malwares polymorphes évoluent fréquemment et de nouveaux malwares apparaissent régulièrement. Même les périmètres et les systèmes de sécurité d'hôte les plus résistants peuvent laisser passer des malwares. Les HIDS et autres systèmes de détection créent des alertes lorsque des malwares présumés entrent dans le réseau et sont exécutés sur un hôte.

Question 1 :
Quelle technologie relative aux logiciels anti-programme malveillant peut reconnaître diverses caractéristiques de fichiers malveillants connus pour détecter une menace ?
Réponse : **basée sur la signature**

Question 2 :
Faites correspondre la fonction de sécurité du système Apple à son objectif.

1. autorisé uniquement l'exécution de logiciels signés authentiques - **Portier**
2. stockage chiffré - **FileVault**
3. permet d'effacer le disque dur à distance - **Localiser mon Mac**
4. technologie anti-programme malveillant - **XProtect**

Question 3 :
Quel périphérique au sein d'une infrastructure LAN est susceptible de subir des attaques par mystification et par débordement de la table d'adresses MAC ?
Réponse : **commutateur**

Question 4 :
Dans la plupart des suites de sécurité basées sur l'hôte, quelle fonction permet de consigner les événements liés à la sécurité et d'envoyer les journaux vers un emplacement centralisé ?
Réponse : **télémétrie**

Question 5 :
Quelle technologie risque d'accroître les problèmes de sécurité liés à la mise en œuvre de la

technologie IoT au sein d'un environnement d'entreprise ?
Réponse : **le cloud computing**

Question 6 :
Quel énoncé décrit une protection antivirus sans agent ?
Réponse : **Des analyses antivirus sont effectuées sur les hôtes à partir d'un système centralisé.**

Question 7 :
Quel système de détection des intrusions basé sur l'hôte (HIDS) est un produit Open Source ?
Réponse : **OSSEC**

Question 8 :
Dans le pare-feu Windows, quand le profil Domaine est-il appliqué ?
Réponse : **lorsque l'hôte est connecté à un réseau approuvé, tel qu'un réseau d'entreprise interne**

Question 9 :
Qu'est-ce qu'un système de détection d'intrusion basé sur l'hôte (HIDS) ?
Réponse : **Un système qui identifie les attaques potentielles et envoie des alertes, mais ne bloque pas le trafic.**

Question 10 :
Selon la description du SANS Institute, quelle surface d'exposition aux attaques comprend l'exploitation de vulnérabilités dans les protocoles filaire et sans fil utilisés par les appareils connectés à l'IoT ?
Réponse : **surface d'exposition aux attaques réseau**

Question 11 :
Quelle affirmation décrit le terme « surface d'exposition aux attaques » ?
Réponse : **Il s'agit de la somme totale des vulnérabilités d'un système qu'un hacker peut exploiter.**

Question 12 :
Selon la description du SANS Institute, quelle surface d'exposition aux attaques comprend l'utilisation du piratage psychologique ?
Réponse : **surface d'exposition aux attaques humaines**

Question 13 :
Quel paramètre de sécurité des terminaux un analyste en charge de la sécurité utilisera-t-il pour déterminer si un ordinateur a été configuré pour empêcher l'exécution d'une application donnée ?
Réponse : **création de listes blanches**

Question 14 :
Que pouvez-vous faire pour vous assurer que les logiciels d'exploitation du réseau restent sécurisés ?
Réponses :

- **Installez régulièrement les correctifs et les mises à jour.**
- **Élaborer une politique concernant les mises à jour des logiciels d'application et des systèmes d'exploitation.**
- **Tests du logiciel avant son lancement.**

Question 15 :
Quel type de technologie peut empêcher les logiciels malveillants d'afficher des publicités contextuelles indésirables sur un appareil ?
Réponse : **La protection contre les logiciels publicitaires**

Question 16 :
Quel type de serrure est recommandé pour sécuriser une porte de bureau ?
Réponse : **Serrure d'entrée à clé**

Module 10:Principes,pratiques et processus de cybersécurité :

Les trois dimensions:
La première dimension du cube de la cybersécurité identifie les objectifs de protection du cyberespace. La confidentialité des données empêche la divulgation d'informations à des personnes, des ressources ou des processus non autorisés. L'intégrité des données désigne l'exactitude, la cohérence et la fiabilité des données. La disponibilité des données garantit que les informations sont accessibles aux utilisateurs autorisés en cas de besoin. Vous pouvez utiliser l'acronyme CIA pour vous souvenir de ces trois principes. La deuxième dimension du cube de cybersécurité représente les trois états possibles des données: les données en transit, les données au repos ou en stockage et les données en cours.

La troisième dimension du cube de la cybersécurité définit les piliers sur lesquels baser vos défenses en matière de cybersécurité. Il s'agit de: 1. la technologie, 2. les politiques et les pratiques, et 3. l'amélioration de l'éducation, de la formation et de la sensibilisation du public.

Pour assurer la confidentialité sans utiliser de chiffrement, la segmentation est une technique de substitution qui permet d'isoler les éléments de données de l'exposition à d'autres systèmes de données. La gestion des droits couvre à la fois la gestion des droits numériques (DRM) et la gestion des droits relatifs à l'information (IRM). Tous deux protègent les données contre les accès non autorisés en utilisant le cryptage. Il existe trois types d'informations sensibles: les informations personnelles , les informations professionnelles et les informations classifiées . Certaines entreprises déploient des technologies d'amélioration de la confidentialité, notamment l'anonymisation, la minimisation et la segmentation des données pour résoudre les problèmes de confidentialité des données.

L'intégrité est l'exactitude, la cohérence et la fiabilité des données tout au long de leur cycle de vie. Les méthodes utilisées pour garantir l'intégrité des données comprennent le hachage, les contrôles de validation des données, les contrôles de cohérence des données et les contrôles d'accès. La disponibilité garantit que les informations sont accessibles à tout moment. Les actions qui contribuent à garantir la disponibilité incluent la maintenance des équipements, les mises à jour et les correctifs du système d'exploitation et des logiciels, les tests de sauvegarde, la planification en cas de sinistre, la mise en œuvre de nouvelles technologies, la surveillance des activités et les tests de disponibilité.

Etats des données:

La sécurité des informations exige que les données soient protégées dans les trois états: au repos, en transit et en cours. Les données sont au repos lorsqu'aucun utilisateur ou processus n'y accède, ne les demande ou ne les modifie. Les données peuvent être stockées dans un système DAS, RAID, NAS, SAN ou dans le cloud. Il est, en effet, vulnérable aux attaques malveillantes sur l'hôte local. Les données au repos incluent également les données de sauvegarde (quand elles ne sont pas en cours d'écriture ou en transit). Les sauvegardes peuvent être manuelles ou automatiques. Ce type de stockage garantit de meilleures performances et une redondance accrue. Ils manipulent beaucoup de données, ce qui représente un risque accru pour l'organisation en cas de défaillance du dispositif. Les défis uniques des systèmes de stockage en réseau comprennent la configuration, les tests et la surveillance du système.

Les données en transit sont des données en cours de transmission - elles ne sont pas au repos ni en cours d'utilisation. Un sneaker net utilise des supports amovibles pour déplacer physiquement des données d'un ordinateur à un autre. Les réseaux filaires incluent des supports en cuivre et en fibre optique et peuvent desservir un réseau local (LAN) ou couvrir de grandes distances dans des réseaux étendus (WAN). Les réseaux filaires et sans fil utilisent tous deux des paquets ou unités de données. Les protocoles standard tels que le protocole Internet (IP) et le protocole de transfert hypertexte (HTTP) définissent la structure et la formation des paquets de données. Les cybercriminels peuvent capturer, enregistrer et voler des données en transit. Les professionnels de la cybersécurité peuvent mettre en œuvre des VPN à l'aide de protocoles SSL, IPsec et de diverses autres méthodes de chiffrement. Les cybercriminels peuvent intercepter et modifier les données en transit. Les professionnels de la cybersécurité déploient des systèmes d'intégrité des données qui testent l'intégrité et l'authenticité des données transmises afin de contrer ces actions. Ces systèmes incluent le hachage et la redondance des données. Les cybercriminels peuvent utiliser des dispositifs malveillants ou non autorisés pour interrompre la disponibilité des données, en les capturant pendant leur transit. Les systèmes d'authentification mutuelle exigent que l'utilisateur s'authentifie auprès du serveur et demandent au serveur de s'authentifier auprès de l'utilisateur.

Les données en cours de traitement font référence aux données en cours d'entrée initiale, de modification, de calcul ou de sortie.

La protection de l'intégrité des données commence lors de la saisie initiale des données. Les organisations utilisent plusieurs méthodes pour collecter des données, chacune présentant une menace potentielle pour l'intégrité des données: saisie de données, numérisation de formulaires, téléchargement de fichiers et données collectées par des capteurs.

Les perturbations au cours du processus d'entrée peuvent inclure un mauvais étiquetage et des formats de données incorrects ou mal assortis, des erreurs de saisie de données ou des capteurs du système déconnectés et/ou fonctionnant mal ou inopérants. Lorsque les données sont modifiées d'une manière qui les empêche d'être lisibles ou utilisables, on parle souvent de corruption des données. Parmi les exemples de corruption des données de sortie, citons l'utilisation incorrecte des délimiteurs de données, les configurations de communication incorrectes et les imprimantes mal configurées. La modification de données non valides pendant le traitement peut avoir un impact négatif, et il est important de se prémunir contre de tels cas.

Contre-mesures de cybersécurité:

Les administrateurs peuvent installer les contre-mesures logicielles ou les protections suivantes sur des hôtes ou des serveurs individuels: pare-feu logiciels, analyseurs de réseau et de ports, analyseurs de protocoles, analyseurs de vulnérabilités et IDS basés sur les hôtes. Un programme de sensibilisation à la sécurité et des politiques de sécurité complètes et solides sont extrêmement importants. Intégrez la formation à la sécurité dans le processus d'intégration de l'organisation. Liez la sensibilisation à la sécurité aux exigences du poste ou aux évaluations des performances. Organisez des sessions de formation en personne à l'aide de jeux et d'activités. Compléter les modules et les cours en ligne.

Un programme actif de sensibilisation à la sécurité dépend de l'environnement et du réseau de l'entreprise, du niveau de menace, ainsi que de la nature et des exigences des données détenues par l'entreprise. Le développement de la sensibilisation à la sécurité doit être un processus continu car de nouvelles menaces et techniques apparaissent en permanence.

Une politique de sécurité complète démontre l'engagement d'une organisation en matière de sécurité. Il fixe les règles du comportement attendu et assure la cohérence des opérations du système et de l'acquisition, de l'utilisation et de la maintenance des logiciels et du matériel. Elle définit les conséquences juridiques des violations et offre au personnel de sécurité le soutien de la direction. Les types de politiques de sécurité incluent l'identification et l'authentification, les mots de

passe, l'utilisation acceptable, l'accès à distance, la maintenance du réseau et la gestion des incidents.

Les documents de normes fournissent les technologies dont des utilisateurs ou des programmes spécifiques ont besoin. En outre, elles spécifient les exigences du programme ou les critères qu'une entreprise doit suivre. Cela permet au personnel informatique de simplifier les opérations de conception, de maintenance et de dépannage, et d'en améliorer l'efficacité. En plus des bonnes pratiques définies par une entreprise, des directives sont également disponibles auprès des organismes suivants: le centre de ressources sur la sécurité informatique du Institut national des normes et de la technologie (NIST), les guides de configuration de la sécurité de la Agence de Sécurité Nationale (NSA) et le Critères communs standards.

Les documents de procédure sont plus longs et plus détaillés que les standards et les directives. Ils comprennent des détails de mise en œuvre qui contiennent généralement des instructions étape par étape et des graphiques.

Question 1 :
Qu'est-ce qui est identifié par la première dimension du cube magique de la cybersécurité ?
Réponse : **objectifs**

Question 2 :
Quels types de lois sur la cybersécurité vous protègent contre une entreprise susceptible de vouloir partager vos données sensibles ?
Réponse : **respect de la vie privée**

Question 3 :
Quelles sont les deux méthodes qui garantissent l'intégrité des données ? (Choisissez deux réponses.)
Réponses :

- **contrôles de la cohérence des données**
- **hash**

Question 4 :
Comment appelle-t-on un appareil de stockage connecté à un réseau ?
Réponse : **NAS**

Question 5 :
Quelle méthode permet d'envoyer des informations d'un appareil vers un autre à l'aide de supports amovibles ?
Réponse : **Sneaker net**

Question 6 :
Quel état de données est géré dans les services NAS et SAN ?
Réponse : **données stockées**

Question 7 :
Quel type de réseau pose des défis toujours plus nombreux aux spécialistes de la cybersécurité en raison de la croissance du BYOD sur le campus ?
Réponse : **réseaux sans fil**

Question 8 :
Une entreprise autorise ses collaborateurs à travailler depuis leur domicile deux fois par semaine. Quelle technologie doit être mise en place pour garantir la confidentialité des données lors de leur transmission ?
Réponse : **VPN**

Question 9 :
Lesquels des éléments suivants sont des types d'informations sensibles ? (Sélectionnez trois réponses.)
Réponses :

- **Personnel**
- **Top secret**
- **Entreprise**

Question 10 :
Parmi les principes suivants, lesquels sont à la base de la cybersécurité ? (Sélectionnez trois réponses.)
Réponses :

- **Confidentialité**
- **Intégrité**
- **Disponibilité**

Question 11 :
Quelles sont les tâches accomplies par une politique de sécurité globale ? (Sélectionnez trois réponses.)
Réponses :

- **Il donne au personnel de sécurité le soutien de la direction**
- **Il fixe les règles du comportement attendu**
- **Il définit les conséquences juridiques des violations**