1. **Quelle déclaration décrit la cybersécurité?**
   - C'est un cadre pour l'élaboration de politiques de sécurité.
   - Il s'agit d'un modèle standard pour développer des technologies de pare-feu pour lutter contre les cybercriminels.
   - C'est le nom d'une application de sécurité complète pour les utilisateurs finaux pour protéger les postes de travail contre les attaques.
   - **Il s'agit d'un effort continu pour protéger les systèmes connectés à Internet et les données associées à ces systèmes contre toute utilisation non autorisée ou tout dommage.**

La cybersécurité est l'effort continu pour protéger les systèmes de réseau connectés à Internet et toutes les données associées aux systèmes contre une utilisation non autorisée ou des dommages.

2. **Quels sont les deux objectifs pour garantir l'intégrité des données? (Choisissez deux.)**
   - Les données sont disponibles à tout moment.
   - **Les données ne sont pas modifiées pendant le transit.**
   - L'accès aux données est authentifié.
   - **Les données ne sont pas modifiées par des entités non autorisées.**
   - Les données sont chiffrées pendant leur transit et lorsqu'elles sont stockées sur des disques.

Les objectifs d'intégrité des données incluent les données qui ne sont pas modifiées pendant le transit et ne sont pas modifiées par des entités non autorisées. L'authentification et le cryptage sont des méthodes garantissant la confidentialité. La disponibilité permanente des données est l'objectif de la disponibilité.

3. **Un administrateur de serveur Web configure les paramètres d'accès pour obliger les utilisateurs à s'authentifier avant d'accéder à certaines pages Web. Quelle exigence de sécurité de l'information est abordée par la configuration?**
   - intégrité
   - évolutivité
   - disponibilité
   - **confidentialité**

La confidentialité garantit que les données ne sont accessibles qu'aux personnes autorisées. L'authentification aidera à vérifier l'identité des individus.

4. **Une entreprise connaît des visites écrasantes sur un serveur Web principal. Le service informatique élabore un plan pour ajouter quelques serveurs Web supplémentaires pour l'équilibrage de charge et la redondance. Quelle exigence de sécurité de l'information est abordée par la mise en œuvre du plan?**

- intégrité
- évolutivité
- **disponibilité**
- confidentialité

La disponibilité garantit que les services réseau sont accessibles et fonctionnent correctement dans toutes les conditions. En équilibrant la charge du trafic destiné aux principaux serveurs Web, en période de grand volume de visites, les systèmes seront bien gérés et entretenus.

5. **Un employé fait quelque chose en tant que représentant de l'entreprise avec la connaissance de cette entreprise et cette action est considérée comme illégale. L'entreprise serait légalement responsable de cette action.**
Vrai ou faux?

- **Vrai**
- Faux

C'est un peu une zone grise et dépendrait également des lois locales. Dans de nombreux cas, si l'employé a fait quelque chose avec la connaissance ou l'approbation de l'entreprise, la responsabilité légale incomberait probablement à l'entreprise et non à l'employé. Dans certains domaines ou situations, l'entreprise et l'employé peuvent être tenus pour responsables légalement.

6. **Quel est le principal objectif de la cyberguerre?**

- pour protéger les data centers basés sur le cloud
- **pour prendre l'avantage sur les adversaires**
- pour développer des périphériques réseau avancés
- pour simuler des scénarios de guerre possibles entre les nations

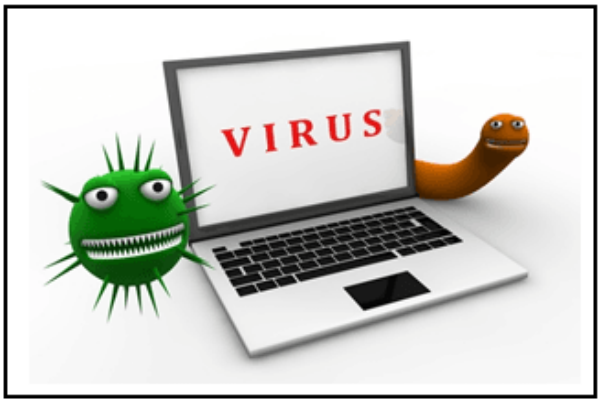
Commentaires récents

Administrateur sur CyberOps Associate (Version 1.0) - Examen FINAL (Réponses)

reetesh sur CCIE / CCNP 350-401 ENCOR dépose des questions complètes avec VCE et PDF

La cyberguerre est un conflit basé sur Internet qui implique la pénétration des réseaux et des systèmes informatiques d'autres pays. Le but principal de la cyberguerre est de prendre l'avantage sur les adversaires, qu'ils soient des nations ou des concurrents.

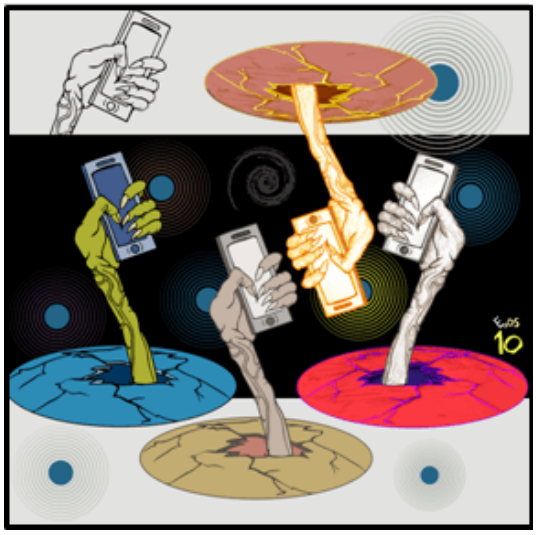
7. **Lors de la description d'un malware, quelle est la différence entre un virus et un ver?**



- Un virus se concentre sur l'obtention d'un accès privilégié à un périphérique, contrairement à un ver.
- Un virus peut être utilisé pour diffuser des publicités sans le consentement de l'utilisateur, contrairement à un ver.
- **Un virus se réplique en s'attachant à un autre fichier, tandis qu'un ver peut se répliquer indépendamment.**
- Un virus peut être utilisé pour lancer une attaque DoS (mais pas une attaque DDoS), mais un ver peut être utilisé pour lancer à la fois des attaques DoS et DDoS.

Les logiciels malveillants peuvent être classés comme suit:
- Virus (se réplique automatiquement en se rattachant à un autre programme ou fichier)
- Worm (se réplique indépendamment d'un autre programme)
- Cheval de Troie (se fait passer pour un fichier ou programme légitime)
- Rootkit (obtient un accès privilégié à une machine tout en se dissimulant)
- Spyware (recueille des informations à partir d'un système cible)
- Adware (fournit des publicités avec ou sans consentement)
- Bot (attend les commandes du pirate informatique)
- Ransomware (retient un système informatique ou des données captives jusqu'à ce que le paiement soit reçu)

8. **Quel type d'attaque utilise des zombies?**



- cheval de Troie
- **DDoS**
- Intoxication SEO
- hameçonnage

Le hacker infecte plusieurs machines (zombies), créant un botnet. Les zombies lancent l'attaque par déni de service distribué (DDoS).

9. **Le service informatique signale qu'un serveur Web d'entreprise reçoit simultanément un nombre anormalement élevé de demandes de pages Web provenant de différents emplacements. Quel type d'attaque de sécurité se produit?**

- adware
- **DDoS**
- Hameçonnage
- ingénierie sociale
- Spyware

Le phishing, les logiciels espions et l'ingénierie sociale sont des attaques de sécurité qui collectent des informations sur le réseau et les utilisateurs. Les logiciels publicitaires consistent généralement en des fenêtres contextuelles gênantes. Contrairement à une attaque DDoS, aucune de ces attaques ne génère de gros volumes de trafic de données pouvant restreindre l'accès aux services réseau.

10. **Quelle est la meilleure approche pour empêcher un appareil IoT compromis d'accéder de manière malveillante**

aux données et appareils sur un réseau local?

- Installez un pare-feu logiciel sur chaque périphérique réseau.
- **Placez tous les appareils IoT ayant accès à Internet sur un réseau isolé.**
- Déconnectez tous les appareils IoT d'Internet.
- Définissez les paramètres de sécurité des navigateurs Web des postes de travail à un niveau supérieur.

La meilleure approche pour protéger un réseau de données contre un appareil IoT potentiellement compromis consiste à placer tous les appareils IoT sur un réseau isolé qui n'a accès qu'à Internet.

11. **Quelle est la meilleure méthode pour éviter de recevoir des logiciels espions sur une machine?**

- Installez les dernières mises à jour du système d'exploitation.
- Installez les dernières mises à jour du navigateur Web.
- Installez les dernières mises à jour antivirus.
- **Installez le logiciel uniquement à partir de sites Web de confiance.**

La meilleure méthode pour éviter d'obtenir des logiciels espions sur la machine d'un utilisateur consiste à télécharger des logiciels uniquement à partir de sites Web de confiance.

12. **Quelles sont les deux implémentations de sécurité qui utilisent la biométrie? (Choisissez deux.)**

- **reconnaissance vocale**
- gousset
- téléphone
- **empreinte digitale**
- carte de crédit

L'authentification biométrique peut être utilisée grâce à l'utilisation d'une empreinte digitale, d'une empreinte de paume et d'une reconnaissance faciale ou vocale.

13. **Quelle technologie crée un jeton de sécurité qui permet à un utilisateur de se connecter à une application Web souhaitée à l'aide des informations d'identification d'un site Web de médias sociaux?**

- gestionnaire de mots de passe
- **Autorisation ouverte**
- mode de navigation en privé
- Service VPN

L'autorisation ouverte est un protocole standard ouvert qui permet aux utilisateurs finaux d'accéder à des applications tierces sans exposer leurs mots de passe utilisateur.

14. **Un employé du cabinet médical envoie des courriels aux patients sur les récentes visites de patients à l'établissement. Quelles informations mettraient en danger la vie privée des patients si elles étaient incluses dans l'e-mail?**

- **dossiers patients**

- prénom et nom
- Informations de contact
- prochain rendez-vous

Un e-mail est transmis en texte brut et peut être lu par toute personne ayant accès aux données alors qu'elles sont en route vers une destination. Les dossiers des patients contiennent des informations confidentielles ou sensibles qui doivent être transmises de manière sécurisée.

15. **Quels sont les deux outils utilisés pour la détection des incidents peuvent être utilisés pour détecter les comportements anormaux, pour détecter le trafic de commande et de contrôle et pour détecter les hôtes infectés? (Choisissez deux.)**

- **système de détection d'intrusion**
- Pot de miel
- **NetFlow**
- Nmap
- un serveur proxy inverse

Bien que chacun de ces outils soit utile pour sécuriser les réseaux et détecter les vulnérabilités, seule une journalisation IDS et NetFlow peut être utilisée pour détecter les comportements anormaux, commander et contrôler le trafic et les hôtes infectés.

16. **Dans quel but un administrateur réseau utiliserait-il l'outil Nmap?**

- **détection et identification des ports ouverts**
- protection des adresses IP privées des hôtes internes
- identification d'anomalies réseau spécifiques
- collecte et analyse des alertes de sécurité et des journaux

Nmap permet à un administrateur d'effectuer une analyse des ports pour sonder les ordinateurs et le réseau pour les ports ouverts. Cela aide l'administrateur à vérifier que les politiques de sécurité réseau sont en place.

17. **Quelle étape de la chaîne de destruction utilisée par les attaquants se concentre sur l'identification et la sélection des cibles?**

- livraison
- exploitation

- militarisation
- **reconnaissance**

C'est la première étape, la reconnaissance, de la chaîne de mise à mort qui se concentre sur l'identification et la sélection des cibles.

18. **Qu'est-ce qu'un exemple de Cyber Kill Chain?**
- un groupe de botnets
- **un processus planifié de cyberattaque**
- une série de vers basés sur le même code de base
- une combinaison de virus, de ver et de cheval de Troie

La Cyber Kill Chain décrit les phases d'une opération de cyberattaque progressive. Les phases comprennent les suivantes:
- Reconnaissance
- Armement
- Livraison
- Exploitation
- Installation
- Commander et contrôler
- Actions sur les objectifs

En général, ces phases sont réalisées en séquence. Cependant, lors d'une attaque, plusieurs phases peuvent être menées simultanément, surtout si plusieurs attaquants ou groupes sont impliqués.

19. **Quel outil est utilisé pour attirer un attaquant afin qu'un administrateur puisse capturer, enregistrer et analyser le comportement de l'attaque?**
- Netflow
- IDS
- Nmap
- **pot de miel**

Un pot de miel est un outil mis en place par un administrateur pour attirer un attaquant afin que le comportement de l'attaquant puisse être analysé. Ces informations peuvent aider l'administrateur à identifier les faiblesses et à renforcer sa défense.

20. **Quelle est l'une des fonctions principales de l'équipe de réponse aux incidents de sécurité Cisco?**

- pour concevoir des malwares polymorphes
- pour concevoir des routeurs et des commutateurs de nouvelle génération moins sujets aux cyberattaques
- fournir des normes pour les nouvelles techniques de chiffrement
- **pour assurer la préservation de l'entreprise, du système et des données**

Le temps entre une cyberattaque et le temps qu'il faut pour découvrir l'attaque est le moment où les pirates peuvent pénétrer dans un réseau et voler des données. Un objectif important du CSIRT est d'assurer la préservation de l'entreprise, du système et des données grâce à des enquêtes opportunes sur les incidents de sécurité.

21. **Quelle action un IDS entreprendra-t-il lors de la détection d'un trafic malveillant?**

- bloquer ou refuser tout trafic
- supprimer uniquement les paquets identifiés comme malveillants
- **créer une alerte réseau et enregistrer la détection**
- rediriger le trafic malveillant vers un pot de miel

Un IDS, ou système de détection d'intrusion, est un appareil capable d'analyser les paquets et de les comparer à un ensemble de règles ou d'attaques de signatures. Si les paquets correspondent aux signatures d'attaque, l'IDS peut créer une alerte et enregistrer la détection.