Corrigé Travaux Dirigés [Série n°2]

R1 : Un malware (logiciel malveillant) est un programme informatique conçu pour infiltrer, endommager ou prendre le contrôle d'un système informatique sans le consentement de l'utilisateur.

R2 : Les types de malwares les plus courants sont les virus, les chevaux de Troie, les vers, les ransomwares, les spywares, les adwares et les bots.

R3 : Les malwares peuvent se propager via des sites Web infectés, des pièces jointes de courrier électronique malveillantes, des téléchargements de logiciels malveillants et des périphériques de stockage infectés, entre autres méthodes.

R4 : Vous pouvez éviter de télécharger un malware en utilisant un logiciel antivirus et anti-malware, en évitant de télécharger des fichiers à partir de sites Web non sécurisés et en étant vigilant avec les pièces jointes de courrier électronique et les liens.

R5 : Si vous pensez que votre ordinateur est infecté par un malware, vous devriez immédiatement exécuter une analyse antivirus et anti-malware, puis supprimer tous les fichiers infectés. Il est également recommandé de changer tous vos mots de passe.

R6 : Les malwares peuvent endommager votre système informatique en supprimant des fichiers, en prenant le contrôle de votre ordinateur, en volant des informations personnelles ou sensibles, en utilisant votre ordinateur pour des activités illégales ou en bloquant l'accès à vos fichiers et dossiers.

R7 : Vous pouvez éviter de propager un malware à d'autres ordinateurs en ne partageant pas de périphériques de stockage infectés, en ne transférant pas de fichiers vers d'autres ordinateurs sans les avoir analysés au préalable et en désinfectant tous les ordinateurs qui ont été infectés.

R8 : Les différents types de malwares présentent des différences dans leur mode de fonctionnement et leur objectif. Voici une brève description de chaque type :

- **Virus** : Un virus est un logiciel malveillant qui s'attache à des fichiers exécutables et se propage en infectant d'autres fichiers et programmes.
- **Cheval de Troie** : Un cheval de Troie est un logiciel malveillant qui se cache à l'intérieur d'un programme apparemment légitime pour accéder à un système informatique et prendre le contrôle de celui-ci.
- **Vers** : Un ver est un logiciel malveillant qui se réplique et se propage automatiquement à travers les réseaux informatiques en exploitant les vulnérabilités du système.
- **Ransomware** : Un ransomware est un type de malware qui crypte les fichiers d'un utilisateur et exige une rançon en échange d'une clé de déchiffrement.
- **Spyware** : Un spyware est un type de malware conçu pour espionner l'utilisateur et recueillir des informations sur ses activités en ligne.
- **Adware** : Un adware est un logiciel malveillant qui affiche des publicités non sollicitées sur l'ordinateur de l'utilisateur.

- **Bots** : Un bot est un logiciel malveillant qui infecte un ordinateur et utilise sa connexion Internet pour effectuer des tâches automatiques et souvent malveillantes, telles que l'envoi de courrier indésirable ou la propagation de malwares.

R9 : Les antivirus utilisent généralement plusieurs techniques pour détecter les programmes malveillants. Voici les principales techniques utilisées :

1. **La correspondance de signatures** : Cette technique consiste à rechercher des correspondances entre les fichiers suspectés et les signatures de programmes malveillants connus. Les signatures sont des codes ou des empreintes numériques spécifiques aux malwares.
2. **L'analyse heuristique** : Cette technique consiste à identifier les comportements suspects des programmes. Les antivirus utilisent des règles et des algorithmes pour détecter les comportements qui sont typiques des programmes malveillants, comme la modification des fichiers système, la création de nouveaux fichiers ou l'exécution de commandes système.
3. **L'analyse comportementale** : Cette technique consiste à observer le comportement des programmes en temps réel. Les antivirus analysent l'activité des programmes pour détecter les comportements malveillants, tels que l'accès non autorisé à des fichiers, l'ouverture de ports réseau ou la communication avec des serveurs de commande et de contrôle.
4. **L'analyse de code** : Cette technique consiste à analyser le code source des programmes pour détecter les vulnérabilités et les failles de sécurité. Les antivirus utilisent cette technique pour détecter les programmes malveillants qui exploitent des vulnérabilités connues pour infecter les ordinateurs.

R10 : Même si certains vers qui se propagent sur Internet ne provoquent pas de dommages directs sur les machines atteintes, ils peuvent toujours être nuisibles pour plusieurs raisons :

1. **Encombrement du réseau** : Les vers qui se propagent sur Internet peuvent consommer une grande quantité de bande passante, ce qui peut ralentir les réseaux et causer des temps d'attente supplémentaires pour les utilisateurs.
2. **Vulnérabilité accrue** : Les machines infectées par des vers peuvent devenir plus vulnérables à d'autres types d'attaques, car les portes dérobées et les autres failles de sécurité peuvent rester ouvertes, permettant à d'autres malwares d'entrer et de causer des dommages.
3. **Perte de temps et d'argent** : Les organisations qui doivent traiter les infections par des vers peuvent perdre du temps et de l'argent en nettoyant les machines infectées, en rétablissant les services et en réparant les dommages causés.
4. **Impact sur la réputation** : Les organisations touchées par des infections par des vers peuvent subir une baisse de leur réputation en raison de leur incapacité à empêcher ces infections, ou en raison des perturbations et des temps d'arrêt qui en résultent.

R11 : - **Les attaques passives** ont trait à l'écoute ou à la surveillance des transmissions. Le courrier électronique, les transferts de fichiers et les échanges client / serveur sont des exemples de transmissions qui peuvent être surveillées (publication du contenu du message et analyse du trafic).

- **Les attaques actives** incluent la modification des données transmises et les tentatives d'accès non autorisé aux systèmes informatiques (mascarade, relecture, modification des messages et déni de service).

R12 : - **Les attaques de porte d'entrée** exigent les actions d'un utilisateur légitime - par exemple, un logiciel malveillant qui est exécuté lorsqu'un utilisateur légitime ouvre une pièce jointe infectée ou exécute un programme malveillant que l'utilisateur a téléchargé sur Internet.

- **Les attaques de porte arrière** ne nécessitent pas les actions d'un utilisateur légitime. Au lieu de cela, ils ciblent les vulnérabilités du logiciel serveur qui exécute un ordinateur. Les défauts dans le logiciel serveur peuvent provoquer un programme serveur pour répondre à une demande inattendue de telle manière qu'il donne accès à l'ordinateur. Une attaque de débordement de tampon (buffer overflow attack) est un exemple d'attaque de porte arrière.

R13 : Les pirates informatiques utilisent généralement une variété de techniques pour pénétrer dans les systèmes informatiques et voler des données, compromettre la sécurité ou perturber les activités des utilisateurs. Voici quelques-unes :

1. **Ingénierie sociale** : les pirates informatiques utilisent des tactiques de manipulation pour inciter les utilisateurs à leur fournir des informations sensibles, telles que des noms d'utilisateur, des mots de passe ou des numéros de carte de crédit. Ils peuvent également tromper les utilisateurs pour qu'ils téléchargent des logiciels malveillants ou cliquent sur des liens qui conduisent à des sites infectés.
2. **Exploitation de vulnérabilités** : les pirates informatiques utilisent des logiciels malveillants qui exploitent les failles de sécurité dans les systèmes informatiques pour accéder aux données et aux ressources. Les logiciels malveillants peuvent être téléchargés sur un système via un e-mail piégé, un site Web compromis, ou un autre vecteur d'attaque.
3. **Attaques par force brute** : les pirates informatiques utilisent des outils automatisés pour essayer de deviner les noms d'utilisateur et les mots de passe en utilisant des combinaisons de caractères aléatoires jusqu'à ce qu'ils trouvent une correspondance valide.
4. **Attaques de déni de service (DoS)** : les pirates informatiques lancent des attaques de déni de service pour perturber les activités des utilisateurs en inondant les serveurs ou les sites Web avec une quantité excessive de trafic, rendant ainsi ces services indisponibles pour les utilisateurs légitimes.
5. **Attaques de phishing** : les pirates informatiques utilisent des techniques de phishing pour piéger les utilisateurs en leur faisant croire qu'ils communiquent avec une entité de confiance, telle qu'une banque ou une entreprise. Les utilisateurs sont ensuite invités à fournir des informations sensibles, telles que des noms d'utilisateur, des mots de passe ou des numéros de carte de crédit.
6. **Attaques de logiciels malveillants** : les pirates informatiques créent et diffusent des logiciels malveillants, tels que des virus, des chevaux de Troie, des ransomwares et des spywares pour infecter les ordinateurs des utilisateurs. Les logiciels malveillants peuvent être utilisés pour voler des informations, contrôler à distance les systèmes informatiques, ou extorquer de l'argent aux utilisateurs.

R14: Les pirates blancs (white-hat hackers) tentent de rendre les systèmes informatiques plus sécurisés en recherchant et signalant des vulnérabilités afin de pouvoir les réparer. Ils peuvent également aider à caractériser de nouveaux virus et à développer des patchs pour eux.

R15: Backdoor – Une porte dérobée (backdoor) est une méthode utilisée par les pirates informatiques pour obtenir un accès non autorisé à un système informatique. Il s'agit d'une technique qui permet de contourner les mécanismes de sécurité normaux d'un système pour accéder à des données ou des ressources sensibles.

Les portes dérobées sont souvent installées sur des systèmes à l'insu des utilisateurs, ce qui permet aux pirates de maintenir un accès non autorisé et de contrôler à distance le système infecté. Les portes dérobées sont souvent introduites dans les systèmes informatiques par des chevaux de Troie, des vers ou d'autres malwares qui exploitent des failles de sécurité pour installer la porte dérobée.

Les pirates peuvent également utiliser des techniques d'ingénierie sociale pour convaincre les utilisateurs de télécharger et d'installer des logiciels malveillants contenant des portes dérobées. Les portes dérobées peuvent être utilisées pour de nombreuses activités malveillantes, telles que la collecte d'informations, la modification de données, la suppression de fichiers, l'installation d'autres malwares, la prise de contrôle à distance du système infecté, ou même la création d'un réseau de machines zombies (botnet) pour lancer des attaques coordonnées.

R16 : Une attaque informatique peut prendre de nombreuses formes, mais il y a généralement des étapes communes dans la plupart des attaques. Voici les étapes générales d'une attaque informatique :

1. **Reconnaissance** : L'attaquant recueille des informations sur la cible, tels que des noms d'utilisateur, des adresses IP, des numéros de téléphone, des adresses email, ou d'autres informations sensibles. Cette étape peut impliquer des techniques d'ingénierie sociale, des analyses de vulnérabilités, ou des scans de port.
2. **Exploitation (établissement d'un point d'entrée)** : L'attaquant utilise des outils ou des techniques pour exploiter les vulnérabilités qu'il a identifiées pour accéder au système de la cible. Cette étape peut inclure l'utilisation de logiciels malveillants, des attaques de force brute, ou l'exploitation de failles de sécurité connues.
3. **Accès** : Une fois que l'attaquant a exploité les vulnérabilités, il obtient un accès à la cible. L'attaquant peut utiliser ce point d'accès pour collecter des informations sensibles, installer des logiciels malveillants, ou pour établir un accès persistant au système.
4. **Mouvement latéral** : L'attaquant peut tenter de se déplacer à travers le réseau de la cible pour atteindre d'autres systèmes ou appareils connectés. Cette étape peut impliquer l'utilisation d'outils ou de techniques pour se déplacer de manière furtive à travers le réseau de la cible.
5. **Collecte de données** : L'attaquant peut collecter des données sensibles de la cible, telles que des informations personnelles, des données financières, des propriétés intellectuelles, ou des informations stratégiques.
6. **Exfiltration de données** : L'attaquant peut utiliser des techniques pour extraire les données collectées de la cible vers des serveurs ou des appareils contrôlés par l'attaquant.

7. **Nettoyage** : Pour effacer les traces de son attaque, l'attaquant peut effacer les journaux d'événements, les fichiers, ou autres données qui pourraient donner une indication de son activité.

R17 : - Une première stratégie utilisée par les codes malveillants consiste à empêcher les antivirus de fonctionner correctement. Ceci peut se faire en arrêtant ces programmes ou en bloquant les connexions vers les sites de mise à jour de l'antivirus. Un utilisateur attentif peut remarquer que l'antivirus ne fonctionne plus ou ne se met pas à jour.

- Les codes malveillants plus avancés contiennent un rootkit, c'est-à-dire un module qui modifie le comportement du système d'exploitation afin que celui-ci ne divulgue pas la présence du code malveillant. Par exemple, ils vont modifier les appels système utilisés pour lister le contenu d'un répertoire ou les processus actifs afin qu'ils omettent de signaler la présence du code malveillant.

Rootkit : un type de malware conçu pour infecter un PC et qui permet au pirate d'installer une série d'outils qui lui permettent d'accéder à distance à un ordinateur.

R18 : L'installation d'un antivirus permet de protéger le système informatique des virus actuellement connus. Il est donc primordial de mettre à jour son antivirus dès que l'éditeur en offre la possibilité. Cependant, même en effectuant ces mises à jour, le système n'est pas à l'abri des nouveaux virus, qui ne sont pas encore reconnus par les antivirus.

R19 : Si les produits antivirus des grandes marques sont tous capables de reconnaître l'ensemble des virus connus, ils ne sont pas tous aussi réactifs lors de la découverte d'un nouveau virus. Certains produits proposeront des mises à jour plus rapidement que d'autres.

R20 : Quels sont les différents types d'IDS

Il existe plusieurs types d'IDS, voici quelques exemples :

1. **IDS réseau** : surveille le trafic réseau à la recherche de modèles d'activité suspecte. Il peut être placé à différents points d'accès du réseau tels que les pare-feu, les routeurs ou les commutateurs.
2. **IDS hôte** : surveille l'activité sur un système informatique spécifique pour détecter les tentatives d'intrusion. Il peut surveiller les fichiers système, les journaux d'événements et les connexions réseau.
3. **IDS hybride** : combine les fonctionnalités des IDS réseau et hôte pour offrir une protection plus complète.
4. **IDS basé sur les signatures** : utilise des signatures connues de menaces pour détecter les activités malveillantes.
5. **IDS basé sur l'anomalie** : surveille les modèles de trafic réseau ou de comportement d'un système pour détecter les activités qui ne sont pas conformes à la normale.
6. **IDS basé sur le comportement** : surveille les comportements suspects des utilisateurs, tels que la tentative de se connecter à des ressources auxquelles ils n'ont pas accès.