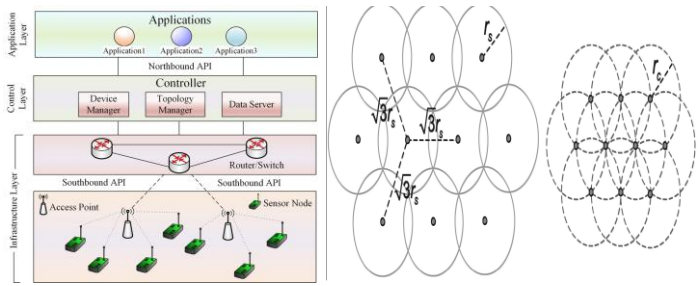
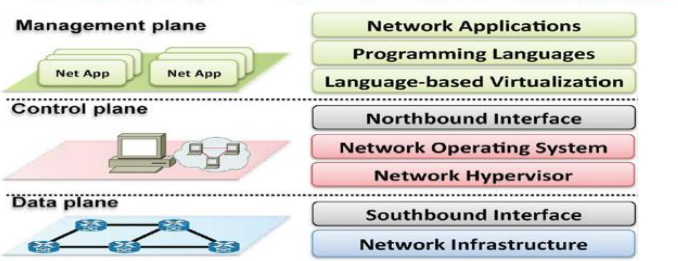
Introduction à l'Informatique Mobile et réseaux sans fil Mobilité et informatique mobile - La mobilité dans le domaine des réseaux de communications peut être définie comme la capacité d'accéder, à partir de n'importe où, à l'ensemble des services disponibles normalement dans un environnement fixe et câblé tels une maison ou un bureau.Informatique mobileLe- concept d'informatique mobile réfère à la possibilité pour des usagers munis de périphériques portables ou d'ordinateurs mobiles d'accéder à des services et à des applications évolués, à travers une infrastructure partagée de réseau, indépendamment de leur localisation physique ou du comportement de mouvement de ces usagers. Il se distingue de l'informatique classique fixe par les deux aspects suivants : la mobilité des utilisateurs et de leurs ordinateurs faisant ainsi référence aux concepts d'ubiquité et de nomadisme ; les contraintes de ressources mobiles telles la largeur de bande sans fil limitée et l'autonomie limitée des batteries. Il existe plusieurs forme de mobilité: Nomadisme Le nomadisme des utilisateurs implique que ceux-ci peuvent se connecter à des points d'accès différents en ayant recours éventuellement à des liaisons sans fil. Ubiquité L'ubiquité des utilisateurs fait référence au fait que ces derniers peuvent vouloir rester connectés lorsqu'ils sont en mouvement, en subissant éventuellement des déconnexions intermittentes.Typologie de la mobilité 1-Mobilité terminale La mobilité des unités, aussi appelée mobilité terminale, réfère à la capacité de localiser et d'identifier un terminal mobile, en permettant à ce terminal d'accéder aux services de réseau à partir de n'importe quelle position où se trouverait ce terminal. Elle est intimement liée à l'accès radio. 2-Mobilité personnelle La mobilité personnelle concerne l'abonné qui est muni d'un numéro d'identification personnel et qui peut être ainsi joint à partir de n'importe quel terminal. Ce type de mobilité implique l'identification des usagers auxquels il permet non seulement de recevoir et d'initier des appels, mais aussi d'accéder aux services de communications en utilisant n'importe quel périphérique ou unité mobile. 3- Mobilité des services La portabilité des services réfère à la capacité du réseau d'identifier les usagers en mouvement, de permettre à ces usagers d'initier et de recevoir des appels, de fournir les services souscrits à ces usagers mobiles ou à la localisation que ces derniers ont désignée. La portabilité des services est intimement liée au concept de réseau intelligent selon lequel le profil de service de l'usager peut être maintenu dans une base de données convenable, à laquelle l'usager peut accéder, qu'il peut interroger et mettre à jour, pour gérer et contrôler les services auxquels il a souscrit. La mobilité qu'est-ce que ça implique? Portabilité L'accessibilité des services et des applications CouvertureLe territoire où le service est utilisé soit couvert par une technologie et qu'il soit possible d'y accéder InteropérabilitéLes architectures et les protocoles doivent être compatibles pour pouvoir coopérer, traduire et réaliser le service tel que l'utilisateur l'attend SÉCURITÉ : comment on peut donner sécurité aux utilisateurs mobiles ? Les réseaux sans fil Classification selon l'étendu du réseaux (sans fil) **•Réseaux au niveau du corps (WBAN: *Wireless Body Area network*) : Bluetooth, HomeRF •Réseaux maison (WPAN: *Wireless Personal Area Network*) : Bluetooth, HomeRF •Réseaux locaux (WLAN: *Wireless Local Area Network*) : IEEE 802.11 •Réseaux métropolitains (WMAN) : IEEE 802.16 – WiMax •Réseaux étendus (WWAN: *Wireless Wide Area Network*) : GSM, GPRS, UMTS** 5G : Architecture orientée servicesUtilisation de 'software-defined networking' (SDN) et 'Network Functions Virtualization' (NFV) NFV et SDN utilisent tous deux des composants logiciels, mais les deux sont fondamentalement différents. NFV convertit les processus réseau eux-mêmes en applications logicielles, tandis que SDN virtualise la gestion des réseaux afin que vous puissiez bénéficier de fonctionnalités telles que la priorisation du trafic basée sur les applications. Évolution des réseaux de communication Troisième Génération (3G) ***Caractéristiques*** •présence de la commutation de circuits et de paquets; •débits de données plus élevés, meilleure qualité de voix; •nouveaux services : Internet, vidéo, GPS, itinérance mondiale; •technologie UMTS comme principale technologie de 3G; •adoption de nouvelles technologies : UTRAN, WCDMA; •améliorations technologiques de la spécification UMTS : HSPA (3.5G); ***Limites*** •liées aux technologies sous-jacentes adoptées des générations précédentes.Quatrième Génération (4G)***Caractéristiques***•descendante des générations précédentes;•normalisation des technologies LTE et WiMax comme celles de la 4G;•améliorations significatives, ubiquité dans l'offre de service (voix, données multimédia);•adoption de l'infrastructure Tout-IP, support des mécanismes de QoS;•adoption d'une nouvelle infrastructure du réseau: EPC;•débits de données élevés.***Limites*** •difficulté à supporter la croissance soutenue et rapide de la demande de connectivité mobile.Transition vers la cinquième génération (5G) ***Statistiques*** •croissance du trafic de données mobiles à un taux annuel de 46 % (2017-2022); •à l'horizon : 1- 99 % du trafic de données mobiles généré proviendra essentiellement de périphériques intelligents; 2- 79 % du trafic de données mobiles proviendra de la vidéo mobile avec une croissance annuelle anticipée estimée à 35 % jusqu'en 2024. ***Constat global*** •croissance soutenue et rapide de l'utilisation de la connectivité mobile; •nécessité de passer à une nouvelle génération de technologies; •besoin de connectivité omniprésente, accès ubiquitaire à l'infrastructure du réseau. ***Résultat à long terme*** Avènement de la prochaine génération: le réseau 5G.Différences entre 4G-LTE et 5G ***La 5G est plus rapide que la 4G*** et offre plus de bits par seconde pour parcourir le réseau. ***La 5G est plus réactive que la 4G*** et présente un temps de latence plus faible, ce qui correspond au temps nécessaire pour établir des communications entre appareils et réseaux. ***La 5G utilise moins de puissance que la 4G,*** car elle peut rapidement passer à une utilisation à faible consommation d'énergie lorsque les fréquences radios cellulaires ne sont pas utilisées. ***La 5G offre un service solide et rapide plus fiable que la 4G grâce*** à une meilleure utilisation de la bande passante et à un plus grand nombre de points de connexion. ***La 5G peut accueillir plus d'appareils que la 4G,*** car elle élargit les ondes radio disponibles. Sécurité 5GLa sécurité décentralisée. Les réseaux antérieurs à la 5G avaient moins de points de contact pour communiquer avec le matériel, ce qui facilitait les contrôles de sécurité ainsi que l'entretien. Les systèmes logiciels dynamiques de la 5G présentent beaucoup plus de points de routage du trafic. **L'augmentation de la bande passante mettra à rude épreuve les contrôles de sécurité actuels.** L'augmentation de la vitesse et du volume mettra les équipes de sécurité devant le défi de mettre au point de nouvelles méthodes pour arrêter les menaces.**De nombreux appareils connectés ne sont pas suffisamment sécurisés**. Tous les fabricants ne font pas de la cybersécurité une priorité, comme c'est le cas pour de nombreux appareils intelligents bas de gamme. La 5G implique plus d'utilité et de potentiel pour l'IdO. **L'absence de chiffrement au début du processus de connexion** entraîne la divulgation d'informations sur l'appareil qui peuvent être utilisées pour mener des attaques ciblées sur des appareils connectés en particulier.Bluetooth• Apparition de la norme Bluetooth Low Energy avec la norme 4.0 en 2010.• Développé par le Bluetooth Special Interest Group • Pour l'échange périodique de petites quantités de données. (Ex. Internet des objets)• Les réseaux Bluetooth sont des réseaux ad hoc fonctionnant dans la bande radio sans licence de 2,4 GHz (bande ISM, Industrial, Scientific and Medical) avec un multiplexage TDM (Time Division Multiplexing) avec des tranches de temps de 625 µs

Bluetooth : Les outils de sécurité La norme définit trois composantes de sécurité principales:**• Encryptions** : - Les deux appareils doivent être 'pairés'. - Le 'pairage' utilise un mot de passe. - Les appareils changent une clé à long terme. **• Addresses MAC aléatoires :** - Le périphérique peut modifier son adresse MAC de façons périodique. Cette méthode prévient le tracking. **• Whitelisting :** On peut créer une liste des adresses MAC acceptées. **L'architecture de sécurité de Bluetooth comporte cinq fonctionnalités distinctes** : le couplage, la liaison, l'authentification des appareils, le cryptage et l'intégrité des messages. • Le **couplage** est le processus de création d'une ou plusieurs clés secrètes partagées • La **liaison** est l'acte de stocker les clés créées lors du couplage pour les utiliser dans des connexions ultérieures afin de former une paire de périphériques de confiance. • **L'authentification** de l'appareil est la vérification que les deux appareils ont les mêmes clés • Le **cryptage** est le processus qui assure la confidentialité des messages • **L'intégrité** des messages protège contre les falsifications de messages. **Il existe deux modes de sécurité LE, le mode de sécurité LE 1 et le mode de sécurité LE 2.** • Le mode de sécurité LE 1 présente les niveaux de sécurité suivants : 1-Aucune sécurité (Pas d'authentification et pas de cryptage) 2-Couplage non authentifié avec cryptage 3- Appairage authentifié avec cryptage 4-Couplage LE Secure Connections authentifié avec cryptage à l'aide d'une clé de cryptage de 128 bits. • LE Mode de sécurité 2 n'est utilisé que pour la signature de données basée sur la connexion (plus d'informations seront expliquées plus tard) et il comporte deux niveaux de sécurité : **1**- Couplage non authentifié avec signature de données **2**-Appairage authentifié avec signature de données Wi-Fi**Association Balayage passif (« Passive scanning ») 1**-Trames de balise (« beacon frames ») envoyées par les points d'accès **2**-Trame de demande d'association (« Association Request ») envoyée par la station H1 au point d'accès sélectionné AP 2 **3**-Trame de réponse d'association (« Association Response ») envoyée par le point d'accès AP 2 à la station H1 **Balayage actif (« Active scanning ») 1**-Trame de demande de détection (« Probe Request ») envoyée par la station H1 aux points d'accès **2**-Trames de réponse de détection (« Probe Response ») envoyées par les points d'accès Trame de demande d'association (« Association Request ») envoyée par la station H1 au point d'accès sélectionné AP 2 **3**-Trame de réponse d'association (« Association Response ») envoyée par le point d'accès AP 2 à la station H1 **Trames Trames de gestion** •Balise (beacon) •Probe Request / Response •Authentification •Association **Trame de contrôle** •contribuent au bon acheminement des trames de données •exemple : ACK, RTS/CTS **Trame de données** Wireless Sensor Networks (WSN) •Un réseau de nœuds sans fils dédiés à une application. •Acquérir des données et les transmettre à une station de traitement. •Dispositifs de consommation d'énergie basse •Capables de traiter de l'information •Capables de se communiquer par radio **Caractéristiques des réseaux de senseurs**• La topologie change fréquemment • Le paradigme de communication est la diffusion • Capacités réduites en mémoire, calcul et puissance• Capteurs peu fiables • Pas d'identificateur global • Déployés en grand nombre (103, 106)**WSN – Architecture Déploiement**

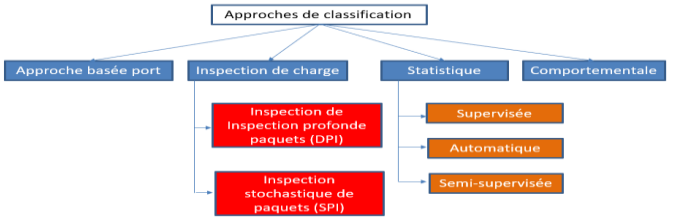


(**a**) Schéma de 'couverture garantie' et (**b**) Schéma de 'connectivité garantie'

Estimation de la distance• Angles d'arrivé: Méthode pour évaluer les angles entre les signaux reçues • **Temps d'arrivé:** méthode pour estimer la distance entre deux nœuds en utilisant le temps • **Temps d'arrivé avec synchronisation:** méthode pour déterminer la distance entre une station mobile et une station synchronisée • **Puissance de la signal:** méthode pour calculer la distance à partir de la puissance la signal reçue **Calcule de la position • Latération**: Téchnique basée sur des mésures précises avec trois recepteurs non colinéaires • **Angulation ou triangulation:** téchnique basée sur les angls à la place de distance **Attaques DoS • Attaque DoS sur la couche 1: brouillage** du signal radio en direction d'un nœud ou d'un ensemble de nœuds du réseau. Ce brouillage radio peut être de 2 formes : **constant ou intermittent**. **• Attaque DoS sur la couche 2:** violer intentionnellement le protocole de la couche Mac en **envoyant continuellement des paquets** sur le support de transmission. Telle manœuvre **provoque des collisions** de paquets, forçant ainsi leur réémission jusqu'à l'épuisement total des ressources des nœuds émetteurs. **• Attaque DoS sur la couche 3 : un nœud malicieux pourrait refuser de router les paquets** .Cette manœuvre peut être exercée de façon constante ou intermittente. Une autre variante de cette attaque consiste au routage vers des destinations erronées. **• Attaque DoS sur la couche 4:** un nœud malicieux **envoie des requêtes de connexion de façon intensive** jusqu'à épuisement des ressources du nœud victime. Équivalente à l'attaque TCP Syn Flooding RFID Une méthode d'identification automatique permettant de stocker et de récupérer des informations sur une étiquette **RFID Étiquette RFID L'étiquette contient** • Identificateur unique(Statique/ Permet de différencier les objets) • Communication sans fil • Logique (en quantité limité) **Peut aussi contenir** • Mémoire en écriture • Capteurs environnementaux (température, pression, accélération, etc.) **Type d'étiquette •Étiquette passive** : Sans batterie, alimentée par le lecteur. **•Étiquette active** : Avec batterie, pas besoin de l'énergie du lecteur pour fonctionner. **•Étiquette semi-active** : Avec batterie, mais utilisée pour les calculs plus complexes **Caractéristiques RFID** • Communication de données bidirectionnelle sans fil. • Transfert de puissance unidirectionnel sur l'air. • Transfert d'horloge à travers l'air. •Appareils passifs et pas d'interrupteur marche/arrêt (switch ON/OFF). **Attaques RFID • Écoute de la communication (Eavesdropping on the communication) • Skimming • Relay and man-in-the-middle attack** - Intercepter la transmission tag-lecteur - Manipulation de l'informations - Se faire passer comme le composant original - Dévier l'ancien signal **• Eavesdropping and Replay** Attaque sur le lecteur - Semblable à MITM -Intercepter et écouter le signal - Conserve le signal pour le rejouer **• Cloning :**- Attaque sur le tag - Dupliquer l'information - Utiliser le clone **• Déni de service (DoS) -** Interférences pour le protocole d'anti – collision - 'Reader- and card jamming'- 'Faraday cage' **Mesure contre Les attaques RFID Authentification** • Lecteur et tag possède une clé • Lecteur déchiffre le code • Tag déchiffre le code • Approbation mutuelle • Empêche une composante non autorisée d'initier une transmission**Chiffrement** • Lecteur chiffre les données • Tag contient et reçoit uniquement des données chiffrées • Lecteur non autorisé ne pourra jamais déchiffrer l'information **Étapes: Clonage de carte RFID** **1**-Identifier la fréquence des cartes RFID et l'ISO utilisé **2**-Se procurer le matériel nécessaire pour lire et cloner une carte **3**-Capturer le UID d'une carte RFID avec un lecteur dissimulé **4**-Cloner la carte sur une nouvelle carte **5**-Tester la carte La technologie NFC • **N**ear **F**ield **C**ommunication • Échange d'informations sur une courte distance Exemples d'application: • Paiement mobile • Contrôle d'accès sécurisé • Connexion WiFi • Accès direct à un site web • Partage de contact **Caractéristiques NFC** • Communication sans fil basé sur l'induction magnétique • Portée maximale de 10cm, en pratique 2-4cm • Historiquement c'est la « sécurité » de la technologie: Assure une démarche volontaire de l'utilisateur • Fréquence de 13.56MHz • Débit allant de 106kbps à 424 kbps • NFC tags: stockage passive de donnée **Modes de fonctionnement Émulation de carte (*Card Emulation mode*)** • L'appareil mobile se comporte comme une carte sans contact • Permet de payer, valider dans le bus … **Mode lecteur (Reader/Writer mode)** • L'appareil mobile va lire une carte ou une étiquette (*tag*) • Permet de lire des informations sur des abris de bus, des monuments … **Mode pair-à-pair (Peer-to-Peer mode)**• Permet à deux mobiles d'échanger des informations**Tag NFC**• Possède une antenne et une mémoire• Peut-être adhésif• Rarement plus de 1KB de mémoire **Utilisation pratique** •Portefeuille électronique•Échanges d'information de contacts•Passeports électroniques •Horaire de transport •Information commerciale •Capteurs de santé •Authentification •Programmation de tags pratiques **Avantages**• Échange rapide• Simple à utiliser• Sans fil• Protocol léger• Répandu• Implémentation open-source• Tags NFC à bas prix **Désavantages**•Taille d'échange de donnée limitée •Protocol non sécurisé •Portée très limitée •Plus lent que Bluetooth **Problèmes de sécurité** • Émission permanente d'informations • Authentification non requise **Utilisation malveillante**• Ouverture d'un site web malicieux • Transmission de malware • Activation de la communication Bluetooth et Wifi • Autorisation des échanges de données • Activation de la caméra • Vol de l'information des cartes NFC • Retransmission d'une transaction bancaire (replay) **Proposition de solutions** •Désactiver toutes fonctions NFC •Dispositifs bloquant l'émission des ondes •Customiser sa carte VANET : Vehicular ad hoc networks IoT – Internet of vehicles La communication de voiture-à-voiture (V2V), souvent mentionnée comme des **réseaux ad hoc véhiculaires** (VANETs ou Vehicular Ad hoc Networks), permet de nouveaux services pour des véhicules et crée de nombreuses opportunités pour améliorer la sécurité routière. • Des changements de topologie du réseau arrivent fréquemment en raison de la haute mobilité des nœuds. • Tous les nœuds partagent le même canal menant à la congestion dans des réseaux très denses. • La nature décentralisée de ces réseaux mène au besoin de nouveaux systèmes et protocoles de diffusion de l'information. • De plus, de nouvelles approches pour la sécurité de communication doivent être conçues pour adapter les besoins spécifiques du réseau et garantir des services fiables et dignes de confiance. • Normes 802.11p : Wireless access in the vehicular environment (WAVE) - (5,85 GHz) The Tor Project • Réseau informatique mondial décentralisé • Projet open-source • Maintenu par l'organisation sans but lucratif "The Tor Project" • Vise l'anonymat sur Internet • Transmission des paquets réseaux chiffrés à travers des relais • Accessible via différentes applications dont le Tor Browser, basé sur FirefoxFonctionnement TOR • Le client « connait » d'avance tous les nœuds du circuit. Il chiffre le message N fois, où N correspond au nombre de nœuds du circuit. • Chaque nœud ne « connait » que le nœud précédent et le nœud suivant. Il déchiffre une couche du message, puis l'envoie au prochain nœud. • Le serveur ne « connait » que le dernier nœud traversé. Inconvénients techniques du réseau Tor • Lenteur inhérente au service • Vulnérabilités du reseau "ingénierie sociale, fingerprinting, JavaScripts, terminaux corrompus ,remonté du circuit par méthodes avancées, analyse des signaux entrants et sortants du réseau par relais de sortie corrompus (niveau physique) " **Vulnérabilités ne proviennent principalement pas des services onion du réseau Tor** Vulnérabilité - Exit node eavesdropping (HTTP) Le nœud final, est celui qui va "dialoguer" avec le serveur que le client souhaite contacter. A l'intérieur du routage Onion, les données sont chiffrées, mais du nœud final au serveur, si la connexion est HTTP, alors les données transmises sont en clair.Introduction to Software Defined Network (SDN)



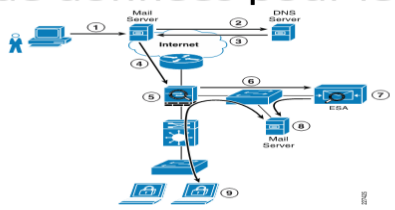
Définition Cloud Computing La principale raison de l'existence de différentes perceptions du cloud computing est que le cloud computing, contrairement à d'autres termes techniques, n'est pas une nouvelle technologie, mais plutôt un nouveau modèle de fonctionnement qui regroupe un ensemble de technologies existantes pour traiter des affaires d'une manière différente Définition de virtualisation La virtualisation est une technologie qui fait abstraction des détails de matériel physique et fournit des ressources virtualisées pour les applications de haut niveau. Un serveur virtualisé est communément appelé une machine virtuelle (VM).Content Delivery Network (CDN) C'est un ensemble de serveurs distribués qui sont reliés en réseau à travers Internet et qui coopèrent afin de mettre à disposition du contenu ou des données à des utilisateurs **Caractéristiques** • Résilience (Attaque DDOS, etc.) • Tolérance aux fautes (bris matériels, etc.) • Haute disponibilité (SLA élevé) • Répartition équitable de la charge (optimisation des ressources) • QoS élevée (SLA, etc.) Fog Computing: A Platform for IoT and Analytics Le Fog Computing utilise des serveurs décentralisés entre le cœur du réseau et la périphérie du réseau pour le traitement des données et pour répondre aux besoins immédiats des systèmes finaux.Est-ce que cela remplace le cloud ? Non,Le Fog Computing est une extension non triviale du paradigme du Cloud Computing jusqu'à la périphérie du réseau. Bordure du réseau : applications et hôtes, routeurs proches des systèmes finaux sur Internet ; Cœur de réseau : routeurs interconnectés sur Internet, réseau de réseaux les nœuds de brouillard peuvent être déployés n'importe où avec une connexion réseau : dans une usine, au sommet d'un poteau électrique, le long d'une voie ferrée, dans un véhicule ou sur une plate-forme pétrolière. Tout appareil doté d'un système informatique, de stockage et d'un réseau la connectivité peut être un nœud de brouillard. Les exemples incluent les contrôleurs industriels, les commutateurs, les routeurs, les serveurs intégrés et caméras de vidéo surveillance. Sécurité réseau et Web Flux réseau (Flot) Les flux de trafic : C'est une série de communications entre deux points d'extrémité; qui sont délimités par l'ouverture et la fermeture de la session. • Une séquence de paquets.• Échangées entre les sources discrètes + destinations.• Les données de flux ne sont pas nécessairement une correspondance 1:1. • Peut aussi être un groupe de paquets dans le réseau. Les données collectés sont: • Adresses IP source et de destination échangeant des informations • Ports source et de destination (ICMP, par exemple, n'utilise pas de ports) • Le protocole • Continue ('streaming') ou rafale • Taille des paquets • Répétitif ou unique • La taille des flux • Le temps inter-arrivé des paquets • Date, heure • La durée des flux, etc. Trois étapes dans l'analyse des flux: • Recueillir les flux. • Exporter les flux. • Analyser les flux. **Dans certains cas:** • Débit d'exportation n'est pas vraiment nécessaire. • Collection + analyse peut se faire localement. • Non extensible, mais peut être un "quick & dirty" fix. **Exporter les flux:** • Ressources du périphérique sont limitées. • Appareils construits pour commutation / routage, pas l'analyse des flux. • Ainsi, les flux peuvent être exportés vers un analyseur dédié. **Analyser les flux:** • Données sur les flux exportés est cru. • Doit être analysé pour plus de commentaires. • Analyseurs peut générer beaucoup d'informations provenant de l'écoulement. Analyse du trafic réseau **Objectif de l'analyse de trafic réseau** • Identifier « qui », « quand » et «quoi » du trafic réseau • Identifier les trafics réseau qui sont suspects. • Découvrir le réseau qui génère du trafic douteux. • Découvrir la destination du trafic douteux. • Découvrir les sources des attaques de sécurité contre le réseau. • Identifier les problèmes du réseau. • Identifier le type des applications. **Pour quoi le faire:** améliorer la performance et gestion réseau, analyser la sécurité **Difficile à faire ?** Simple en théorie mais relativement complexe en pratique. **Préalable** Capture et enregistrement des paquets (fichiers de trafic). Utilisation analyse trafic •**QoS** : Les flots appartenant à une classe sont traités différemment par rapport aux autres selon les niveaux de qualité de services prédéfinis • **La classification et de l'identification** des tendances de trafic sont nécessaires pour concevoir et dimensionner les réseaux •**Système de sécurité**, en particulier dans les mécanismes de détection d'intrusion, d'utilisation injustifiée des ressources réseau ou de trafic malicieux ainsi que les fonctions de sécurité conventionnelles telles que les pare-feu



Classification du trafic reseau **Classification de trafic se basent sur les numéros de ports** • Cette approche est particulièrement simple et rapide en comparaison avec d'autres approches ; elle classifie efficacement les applications standards vu qu'elles utilisent des ports assignés par l'IANA qui sont bien connues. • La classification basée sur les ports est devenue inefficace avec la présence des applications non standards telle que le trafic P2P (Peer to Peer). **Classification par inspection de charge Cette** approche consiste à examiner la charge utile de chaque paquet dans sa recherche d'un indice ou la signature de l'application **Inspection profonde de paquets (DPI pour Deep Packet Inspection) :** inspection mécanique de la charge utile de chaque paquet lors de la recherche d'une expression ou d'un mot clé caractérisant une application donnée. **Inspection stochastique de paquets (SPI pour Stocastic Packet Inspection)** : inspection de la charge, mais d'une manière statistique de façon à chercher les propriétés distinctives de chaque application **Classification par approche comportementale** L'approche comportementale se focalise sur l'analyse du comportement des hôtes et de la distribution des connexions pour déduire le type de trafic avec le but d'identifier les applications actives sur un hôte donné. Les classifieurs de cette catégorie examinent les patrons générés par le trafic en observant un certain nombre de paramètres, tel que le nombre d'hôtes qui y sont connectés, le nombre de ports et les protocoles utilisés. L'idée derrière une telle approche est que différentes applications génèrent des patrons différents **Classification par approche statistique -** La classification du trafic par l'approche statistique s'appuie d'un côté sur les techniques d'apprentissage machine et d'un autre côté sur le fait que les différents types de traffic possèdent différentes caractéristiques ou métadonnées telles que la taille des paquets (petite ou grande), la taille des flux, le temps interarrivé des paquets, la durée des flux. - L'idée derrière une telle approche est que différentes applications génèrent des patrons différents Apprentissage modèles de comportement• Utilisateurs • Communications intérieur et extérieur (serveurs, clients) • Détecter anomalies (augmentation de l'utilisation de la bande passante, attaque Dos, …) Acquérir information sur • Connexions entrant et sortant, adresses IP actives. • Quels DNS sont actives et associes aux adresses IP. •Liste adresses IP (locale ou externe) •Type de trafic •Distribution taille de paquets •Processus d'arrivée des paquets Type de trafic • Contrôle • Données • Malicieux Analyse en temps réel •Recueille données en temps réel •Analyse et décisions en temps réel Analyse pas en temps réel •Recueille données en temps réel. •Analyse et décisions pas en temps réel. Analyse spatiale ou temporelle Choix de l'analyse de trafic **Single-point vs. Multi-point** Number of probing or test packet generation point **In-service vs. Out-of-service** Whether monitoring should be executed during service or not **Continuous vs. On-demand** Monitoring executes continuously or by on-demand. **Packet vs. Flow-based** Collect packets or flows from network devices.

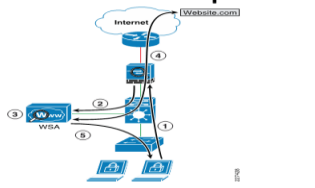
One-way vs. Bi-directional Monitor forward path only / forward and return path Informations révélées par l'analyse de trafic • Comment l'intrus a accédé au réseau. • Le parcours de l'intrusion. • Les techniques d'intrusion utilisées. • Les traces laissées par l'intrus et les preuves Ce que l'analyste réseau ne peut faire • Résoudre seul le cas d'attaque • Lier un suspect à une attaque.Analyse des preuves• Sur le poste d'attaque et les postes intermédiaires (Journaux (*logs*), fichiers, données courantes et outils). • Sur les pare-feux et les équipements de réseaux (ayant un accès internet) Journaux *(logs), buffers* (selon le cas).• Sur le poste victime «Journaux (*logs*), fichiers, données courantes, fichiers de configuration modifiés, outils, chevaux de Troie, virus, fichiers dont les extensions sont inconnues, fichier de données stockées illégalement, etc. » Remarque sur l'analyse des journaux : Ces fichiers sont facilement modifiables. Un intrus peut donc facilement y insérer de fausses informations.Intrusion dans un réseau Processus d'intrusion Énumération ou découverte du réseau •Topologie du réseau. •Liste des nœuds actifs. •Architecture du réseau et type de trafic (TCP, UDP, RTP, etc.) •Ports ouverts, systèmes d'exploitation, nom d'utilisateurs, privilèges des utilisateurs, etc. L'attaquant peut utiliser l'outil nMap pour scanner le réseau afin de connaître les ports ouverts. •Vulnérabilités potentielles de chaque nœud Étude des vulnérabilités potentielles • Faiblesses du système, du réseau, des éléments du réseau.• Comment tirer profit des vulnérabilités. **Réalisation de l'intrusion proprement dite (attaque) et effacement des traces si possible** • Virus, cheval de Troie, infection d'email , attaque de routeur, bris de mot de passe (cracking), élévation de privilèges, etc.Exemples d'outils **Kiwi Syslog Daemon** • Analyse de journaux Syslog pour windows • Freeware **Firewall Analyzer** • Interface web de surveillance de pare-feu et d'analyse de journaux provenant des pare-feux, proxy, serveurs RADIUS, etc. **Tcpdump** • Extraction de trafic réseau, analyse statistique, diagnostic. • WinDump (version Windows) **HTTP Sniffer** • Renifleur de paquets HTTP, analyseur de protocole, ré-assembleur de fichier • Plate-forme Windows uniquement. **OmniPeek** • Outil d'analyse de trafic réseau, analyseur de protocole. Attaques contre le réseau Principaux types d'attaques contre le réseau •IP spoofing.•Attaque contre le routeur.•Ecoute (eavesdropping, sniffing).•Déni de service. •Attaque de l'homme du milieu (man-in-the-middle). •Altération de données Sécurité du routeur **Vulnérabilités du routeur** • **Vulnérabilité relative à l'authentification HTTP** : Avec l'aide de http//router.address/level/$NUMBER/exec/... où $NUMBER est un entier entre 16 et 99, il est possible pour un utilisateur distant d'avoir un complet accès administrateur à un routeur• **Vulnérabilité NTP** : En envoyant un paquet de contrôle NTP (network time protocol) fabriqué, il est possible de déclencher un buffer overflow dans le démon NTP • **Vulnérabilité relative au parsing SNMP** : La réception de messages SNMP malformés par un système affecté peut causer l'échec du parsing et du traitement de ces messages, d'où un crash du système ou des tentatives répétées de chargement **Types d'attaques contre le routeur** • Attaque de déni de service • Empoisonnement de la table de routage • Attaques persistantes **Analyse du routeur** •**Préalable** : Acquisition des preuves volatiles (configuration courante du routeur, liste d'accès (access list), temps, fichier journaux (logs)) • **Éléments analysés** • Configuration du routeur : comparée la configuration au démarrage avec la configuration courante. Commandes : **Show startup-config/ Show running-config** • Table de routage • Liste de contrôle d'accès • Journaux du routeur (logs) **Exemple d'outil** Router Audit Tool (RAT) Attaques DoS / DDoS **Types d'attaques DoS**• Ping de la mort (ping of death) (année 2002) • ICMP flooding ('ping','Nping') • SYN flooding ('Nping') • Buffer Overflow attack • SIP INVITE Flood Attacks • Encrypted SSL DDoS Attacks **Attaques avec NPING** NPING peut être utilisé pour : •Pour détecter les serveurs actives •Générateur de paquets pour test de 'stress' sur les réseaux •ARP poisoning•Attaques DoS •Route tracing **NPING peut être utilisé pour :** nping --tcp –c 2 1.1.1.1 –p 100-102→similaire à NMAP nping --tcp –c 2 1.1.1.1 –p 80 --rate 10000→ inondation **Mode d'action des attaques DoS**• Connectivité réseau • Manque de ressources internes • Consommation de la bande passante •Consommation des ressources •Destruction ou altération des informations de configuration **Techniques de détection des attaques DoS** • Profilage d'activité • Surveillance de l'utilisation du CPU • Utilisation de Cisco NetFlow •Utilisation des systèmes de détection d'intrusion réseau (NIDS) **Analyse des attaques DoS** •Identification de l'adresse IP de l'attaquant dans le journal (log) du DNS •Traçage des paquets (suivre la trace des paquets). •Exemple de méthodes de traçage ICMP traceback **Attaque de négation de service (DoS) DDos :** attaque répartie contre la disponibilité de services. **ICMP attack ou Smurf attack**: attaque utilisant le protocole ICMP. Exemple, le ping. **TCP SYN FLOOD attack :** attaque utilisant le protocole de ouverture de connexion de TCP en conjonction avec usurpation d'adresse **DNS Amplification Attacks** **1**-The attacker triggers and directs the compromised machines to begin the attack **2**-The compromised machines send a DNS query for the domain *example.com* and set the source IP address to the victim's IP address **3**-The open resolver servers ask the upstream name server(s) the location of *example.com* **4**-The name server sends a reply back to the open recursive servers **5**-The open recursive servers send DNS responses to the victim Attaques Web Identification des attaques Web • Incapacité de l'utilisateur à accéder aux services en ligne. • Redirection des URLs bien saisis vers des sites indésirables.• Diminution inhabituelle des performances du réseau. • Redémarrage fréquent du serveur.• Anomalies dans les fichiers journaux (log). Types d'attaques Web • Cross-site scripting (XSS). • Cross-site request forgery (CSRF). • Injection SQL. • Injection de code.• Injection de commande. • Falsification de paramètre (parameter tampering). • Empoisonnement de cookie (cookie poisoning). • Buffer overflow. • Espionnage de cookie (cookie snooping). • Attaque de protocoles dans la DMZ.• Détournement d'authentification (authentication hijacking).• Falsification de journal (log tampering). • Interception cryptographique. • Interprétation d'URL. • Usurpation d'identité Injection SQL • Une injection SQL est un type d'exploitation d'une faille de sécurité d'une application web, en injectant une requête SQL non prévue par le système et pouvant compromettre sa sécurité. • Cette faille apparaît quand il est possible d'injecter du code SQL dans les requêtes SQL qui sont faites à partir d'une page web Empoisonnement de cookie• L'attaquant modifie le contenu du cookie pour voler les informations personnels de l'utilisateur ou frauder sur un site web pour lequel l'utilisateur s'authentifie avec confiance. Attaque de protocoles dans la DMZ• **DMZ** : zone réseau de demie-confiance qui sépare la zone de confiance du réseau d'une compagnie, de l'internet (non confiant). • Pour sécuriser davantage la DMZ et réduire les risques seuls quelques protocoles sont autorisés dans cette zone- FTP + TCP (ports 20, 21) - SMTP + TCP (port 25) - DNS + TCP ou UDP (port 53) - HTTP + TCP (port 80) - HTTPS + TCP (port 443) Cross-site Request Forgery (CSRF) • L'attaquant force la victime à soumettre au serveur Web victime un formulaire préparé par l'attaquant. • Le formulaire soumis par l'attaquant permet de forger une requête. • Le serveur Web accepte les données du formulaire car provenant d'un utilisateur de confiance. • Utilisation d'expressions régulières pour détecter l'attaque. Analyse d'empoisonnement DNS (DNS Poisoning) • Cache DNS corrompu. • **Préalable** : Décharger le contenu du cache et l'analyse afin d'identifier les entrées inappropriées. • **Méthodologie d'analyse** : - Démarrer un outil d'analyse de paquets comme Wireshark. - Capturer les paquets DNS. - Identifier l'adresse IP utilisée pour la résolution des noms de domaines. - Si l'adresse IP n'appartient pas au réseau alors il y a attaque d'empoisonnnement DNS. - Démarrer une recherche sur l'adresse IP : Détenteur et localisation. - Faire une recherche WHOIS Lookup à partir de l'adresse IP. Outils de localisation d'adresse IP **Nslookup** • Interrogation des informations de DNS. • Systèmes UNIX et Windows. **Traceroute** • Identification du chemin suivi par les paquets. • Sous Windows utiliser la commande : tracert **WHOIS** • Disponible sur certains systèmes d'exploitation. • Exemple d'utilisation: whois –h <host name> <identifier> **CountryWhois** • Application WHOIS pour la localisation géographique d'adresses IP. • Autres fonctionnalités : Analyse de journal, analyse d'en-tête de mail, identification de fraude par carte de crédit, etc.. **Whois.net** • Outil web pour la localisation géographique d'adresses IP ou de domaines.• **WHOIS Lookup**• Outil web pour la localisation géographique d'adresses IP ou de domaines.• http://whois.domaintools.com **Hide Real IP** • Localise automatiquement les serveurs proxy anonymes et achemine le trafic Internet par eux, ce qui permet de cacher l'adresse IP de l'utilisateur. Ainsi le traçage de l'utilisateur (IP) devient impossible. **www.whatismyip.com** • Site web permettant de connaître l'adresse IP externe d'un poste (adresse vue par les autres à l'extérieur du réseau) même si le poste est derrière un routeur ou un pare-feu. Cybercriminalité Types de cybercrimes• Phishing • Vol d'identité • Fraude de cartes de crédit • Téléchargement illégal • Espionnage d'entreprise • Pornographie infantile • Abus sur les enfants par clavardage • Cyber-terrorisme • Création et distribution de virus et courriels indésirables Crimes liés au e-Mail Crimes commis par envoi d'e-Mail • Envoi de spam • Fabrication de faux e-Mails • Mail bombing • Mail storms Crimes ayant pour support un e-Mail • Vente de narcotique • Harcèlement • Fraude • Pornographie infantile • Enlèvement d'enfant Pare-Feu Définition Un pare-feu est un composant ou un ensemble de composants restreignant l'accès entre un réseau externe (Internet) et un réseau interne. Propriétés d'un pare-feu • Résistant aux attaques • Le trafic entre les réseaux doit passer a travers du pare-feu • Le pare-feu suive les politiques de sécurité Rôle principale: séparation et protection du réseau privé et INTERNET • **Contrôle**: gérer les connexions sortantes à partir du réseau local • **Sécurité**: protéger les réseaux internes des intrusions venant de l'extérieur • **Vigilance**: surveiller et tracer le trafic entre le réseau local et internet De quoi protège un pare-feu? • Protège l'exposition des systèmes sensitives : cache les fonctionnalités de diapositives, du réseau, des systèmes informatiques, … • Evite l'exploitation de failles des protocoles réseau • Evite l'accès des utilisateurs non autorisés : méthodes d'authentification, use authentification, autorisation, comptabilité 'accounting' (AAA) •Protège des données malicieuse • Les attaques qui ne passent pas par lui (i.e. réseaux sans fil, modem, …) • Mauvaise configuration du réseau ou pare-feu • Application qui ne fonctionnent pas avec le pare-feu • Attaques internes • Les virus importées par Laptot, PDA, etc. Approche défense en profondeur • Le routeur de frontière peut vérifier l'adresse IP source, peut avoir quelques règles de sécurité (ACL) • Le pare-feu peut vérifier plusieurs règles. Peut simuler le serveur et accepter la connexion TCP ('three-way handshake') pour éviter un attaque d'inondation SYN, etc. • Le commutateur peut avoir quelques règles de sécurité, VLAN, etc. Rôles d'un pare-feu• déterminer le type de trafic qui sera acheminé ou bloqué • limiter le trafic réseau et accroître les performances • contrôler le flux de trafic • fournir un niveau de sécurité d'accès réseau de base • autoriser un administrateur à contrôler les zones auxquelles un client peut accéder sur un réseau • filtrer certains hôtes afin de leur accorder ou de leur refuser l'accès à une section de réseau • translation d'adresses ou de ports (connexion et protection des réseaux à adressage privé).Périmètre Routeur de frontière • Première ligne de défense contre accès non autorisé, DDoS, etc. • Utilise ACL pour anti-spoofing et bloquer les paquets invalides Protection du routeur de frontière • Contrôler l'accès • Protéger le plan de gestion • Protéger le plan de contrôle • Sécuriser l'inter-change d'information entre les routeurs Politiques Firewall • Bloquer toute connexion de l'extérieur (Internet – trafic 'inbound') vers les ressources intérieurs et les sous-réseaux. •Permettre trafic HTTP vers l'extérieur ('outbound') à partir de l'intérieur •Permettre trafic 'outbound' SSL •Permettre accès à DMZ de l'intérieur du réseau •Permettre seulement le trafic 'inbound' des protocoles HHTP vers web server, SMTP vers les agents de courriel, DNS vers le serveur DNS, etc. •Restreindre les connexions initiées depuis la DMZ sur les protocoles et sources nécessaires: DNS depuis le serveur DNS, SMTP depuis le serveur de courriel, etc. •Implémenter NAT et PAT (port address translation) pour protéger les adresses de l'intérieur.

Flux de données pour le courriel



Step 1	Sender sends an E-mail to xyz@domain X.
Step 2	What's the IP address of domain X?
Step 3	It's a.b.c.d (public IP address of ESA).
Step 4	E-mail server sends message to a.b.c.d using SMTP.
Step 5	Firewall permits incoming SMTP connection to the ESA, and translates its public IP address.
Step 6	ESA performs a DNS query on sender domain and checks the received IP address in its reputation database, and drops, quarantines E-mail based on policy.
Step 7	ESA forwards E-mail to preconfigured inbound E-mail server.
Step 8	E-mail server stores E-mail for retrieval by receiver.
Step 9	Receiver retrieves E-mail from server using POP or IMAP.

Flux de données pour le WEB



Step 1	Client's browser requests connection to http://website.com.
Step 2	Cisco ASA intercepts and redirects HTTP requests over GRE.
Step 3	If content not present in local cache, WSA performs a DNS query on destination domain and checks the received IP address against URL and reputation rules, and allows/denies request accordantly.
Step 4	WSA fetches content from destination web site.
Step 5	Content is inspected and then delivered directly to the requesting client.

Architecture pare-feux Architecture du réseau avec des pare-feux **Un réseau privé :** des clients et des serveurs inaccessible de l'extérieur. • normalement, aucune connexion TCP, aucun échange UDP ne peuvent être initiés depuis l'Internet vers cette zone. **Une « DMZ » (DeMilitarized Zone)** : contient des serveurs accessibles depuis l'Internet et depuis le réseau privé. **Les réseaux** sont séparés par des pare-feux Communications possibles avec un pare-feu Entre le réseau privé et l'extérieur • les utilisateurs internes initialisent des communications avec l'extérieur • seules les réponses à ces requêtes doivent entrer dans cette zone • cette zone est construite sur une classe d'adresses privées et nécessite donc une translation d'adresse (NAT) ou de port (PAT) pour accéder à l'extérieur Entre la DMZ et l'extérieur • serveurs qui doivent être accessibles depuis l'extérieur • il faudra permettre de laisser passer des connexions initiées depuis l'extérieur vers ces serveurs uniquement (*à surveiller)* Entre le réseau privé et la DMZ • les accès devraient être à peu près du même type qu'entre zone privée et l'extérieur •avec un peu plus de souplesse pour mettre à jour les serveurs web, d'envoyer et recevoir les messages (i.e. le SMTP est dans le réseau privé).Types de pare-feu • Filtrage de paquets 'stateless' • Pare-feu – filtrage de paquets 'stateful' • Pare-feu mandataire. • Inspection Niveau Application 'layer Gateway or Proxy' • Pare-feu transparent • Prochaine génération • NAT Pare-feu – filtrage de paquets • Le filtrage s'appuie en priorité sur les en-têtes IP, UDP et TCP. • L'analyse de la couche application applicative est réservée à une catégorie particulière de pare-feu • **Principe :** le filtrage statique compare le contenu des en-têtes IP, TCP et UDP avec les règles définies par l'administrateur pour autoriser ou non un paquet entrant ou sortant.• Normalement, le filtrage accepte toutes les connexions qui viennent de l'extérieur pour les ports > 1024 Filtrage statique des paquets • Adresse IP source • Adresse IP destination • Protocole (TCP, UDP, ou ICMP) • Numéro de port source TCP ou UDP • Numéro de port destination TCP ou UDP • Type de message ICMP • Taille du paquet **Filtrage dynamique des paquets (ou « stateful »)** • Un pare-feu 'stateful' fait la même vérification qu'un pare-feu de filtrage de paquets, mais il maintient aussi une table avec toutes les connexions TCP (crées de l'intérieur) pour accepter seulement les paquets de ces connexions (vérification du numéro de port) et rejet les paquets avec ports > 1024 qui n'appartiennent pas à ces connexions. • Tous les paquets ne sont pas analysés, la surveillance étant centrée sur la phase d'établissement de session TCP.• « Stateful inspection » inclut également une analyse de charge utile, de façon à identifier les attaques de type « déni de service ». • Ils examinent chaque paquet IP dans un contexte. • Assurer le suivi des sessions client-serveur • Vérifier si chaque paquet appartient à une session valide Pare-feu – avantages et désavantages Avantages : • Très simple • Impact minimal sur la performance du réseau • Peut être configuré dans les routeurs • Peut réaliser le filtrage de base Désavantages • Problèmes avec le 'spoofing'. Si un ACL permet trafic d'une adresse IP, une attaque 'spoofing' avec cette adresse est possible. • Ne fait pas le filtrage de paquets fragmentes • 'Stateless' : pas d'information sur les connexions actuelles • Problème avec applications qui utilisent différents port (création dynamique du port), donc ACL doit avoir une liste de ports accessibles très grande • attaques de petit paquets ('tiny fragment attacks') Pare-feu mandataire Application Level Gateway or Proxy Un serveur mandataire est une machine sur laquelle on a installé tous les services que l'on souhaite fournir aux utilisateurs Les pare-feu mandataire : • ont une passerelle ou délégué ('proxy') pour chaque application spécifique • ont un accès complet au protocole • ont besoin de passerelle distinctes pour chaque service ou application Politique global de Sécurité **1**- Tout autoriser **2**- Tout interdire **3**- Tout autoriser et interdire ce qui est dangereux • Déconseillé **4**- Tout interdire et autoriser ce qui est utile • Bonne stratégie • Ce qui n'est pas explicitement permis est interdit Principes basiques de fonctionnement • Les règles de filtrage déterminent le devenir des paquets grâce à une politique • Un paquet entrant dans le pare-feu teste toutes les règles définies jusqu'à en trouver une qui lui corresponde. Et il obéit à la politique spécifiée par la règle trouvée. • Si aucune règle s'appliquant au paquet n'a été trouvée, alors c'est la politique par défaut qui est utilisée pour savoir que faire de ce paquet. • Il est donc important, avant de créer les règles, de définir la politique par défaut d'une chaîne. Les politiques Les politiques de base : • ACCEPT : le paquet est accepté • REJECT : le paquet est rejeté avec envoi d'un message d'explication ICMP • DENY : le paquet est rejeté en mode silencieux • MASQ : le paquet est redirigé par 'masquerading' (translation d'adresses IP NAT) Les critères de sélection pour les règles Les règles reposent sur des critères de sélection très variés : • Machine source • Port source • Machine destination • Port destination • Interface • TOS (Type of service) • Protocole • Codes spéciaux du paquet TCP • Types et codes spéciaux du paquet ICMP Actions sur les paquets Les règles peuvent définir différentes actions sur un paquet : • Mise en fichier de log • Application d'une politique • Redirection vers une autre chaîne • Marquage du paquet Politique de sécurité • IP masquerading (NAT) • Interdire le Ping • Éviter l'IP Spoofing • Restreindre Telnet • Gérer l'accès aux sites web • Limiter les autres services • Garder trace du trafic sensible Fonctionnalités de haute disponibilité: Active-Standby Failover: le pare-feu principal est toujours actif et le secondaire est en mode veille. Lorsque le pare-feu principal échoue, le pare-feu secondaire prend le relais. Active-active Failover: les deux pare-feu sont actifs. Si l'un échoue, l'autre continuera à transmettre le trafic dans le réseau Clustering: regroupement de pare-feu pour augmenter le débit des paquets et pour protéger dans des environnements étendus et hautement évolutifs. Pare-feu bastion Un **bastion** (ou *bastion host* en anglais) est un élément du réseau qui fournit un point d'entrée et/ou de sortie unique vers Internet . • Les bastions : hôte servant de plate-forme aux pare-feu de type applicatif ou circuit.• système hôte hautement sécurisé • peut être circuit / passerelles niveau de l'application • fournit des services accessibles de l'extérieur • potentiellement exposés aux attaques donc doit être très sécuritaire • peut supporter 2 ou plusieurs connexions réseaux Pare-feu virtuel • Déployé dans le centre de données pour founir une segmentation et une protection réseau aux environnements virtuels • Utilisation de pare-feu virtuels, car le traffic entre les machines virtuelles ne quitte pas le serveur physique et ne peut pas être inspecté ou appliqué avec des pare-feu physiques Pare-feu personnels • Logiciels populaires pour installer sur des machines ou des serveurs d'utilisateurs finaux (end-user) pour protéger contre les menaces de sécurité externes et les intrusion. • Logiciel de base qui contrôle l'accès des couches 3 et 4 aux machines clients. DMZ Zones intermédiaires dans lesquelles des serveurs réalisent des traitements sur des flux de données **Crées pour** : • faciliter la gestion des flux de données au niveau du point de cloisonnement • empêcher les flux de données de passer d'une zone sûre à une zone non sûre directement et inversement •séparer les grandes fonctionnalités **Publique, privée, semi-privée** NAT • NAT – Network Address Translation • Fonction dans routeur d'accès (entre site et Internet) • Traduit les adresses IP • Une station du site • Le système est transparent pour les stations• Le routeur entre le site et l'Internet fait la traduction •La fonction NAT utilise les ports définis dans TCP et UDP pour associer les paquets entrants dans le réseau local (ayant la même adresse IP publique dans l'entête) vers le bon ordinateur dans le réseau local. NAT : avantages et inconvénients Avantages • On dispose d'un espace d'adresses énorme en interne • Pas de limitation dans l'architecture des sous réseaux • Pas de problème quand nouvelles stations à numéroter • Les stations clientes ont des @ IP dynamiques • Plus difficiles à attaquer : meilleure sécurité **Désavantages** • Sécurité : les stations clientes sont « anonymes » Difficile de savoir quelle station interne a attaqué un site externe • Coupe le principe IP de connectivité de bout en bout • Retarde l'arrivée de IPv6 Pare-feu dans un centre de données Circulation Est-Ouest (east-west traffic): Le trafic allant d'un segment de réseau ou d'une application du centre de données vers un autre segment de réseau ou une application dans le centre de données est souvent appelé trafic est-ouest. Circulation Nord-Sud (North-South traffic): Le trafic entrant et sortant du centre de données et le reste du réseau d'entreprise est souvent appelé trafic nord-sud. IDS Intrusion Detection System **Détection d'attaques** : afin de détecter les attaques que peut avoir un système, il est nécessaire de disposer d'un logiciel spécialisé dont le rôle sera de surveiller les données qui transitent sur ce système et qui serait capable de réagir si ces données semblent suspectes. **Un système de détection d'intrusion (ou IDS : Intrusion Detection System) est** un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte). Il permet ainsi d'avoir une action de prévention sur les risques d'intrusion. **Système logiciel ou matériel** : Détection en temps réel de tentatives d'intrusion **La détection d'intrusion est :** • le processus de suivi des événements survenus dans un système informatique ou réseau, • analyser les événements pour les signes d'incidents possibles, qui constituent des violations ou de menace **Des incidents ont de nombreuses causes**, telles que • les logiciels malveillants (par exemple, vers, logiciels espions), • les attaques à partir à partir d'Internet • les utilisateurs autorisés de systèmes qui abusent de leurs privilèges ou qui tentent d'obtenir des privilèges supplémentaires pour lesquelles ils ne sont pas autorisés. Les méthodes de détections Techniques principales sont mises en place dans la détection d'attaques : **Détection des signatures d'attaques connues dans les paquets circulant sur le réseau.** • Signature: Numéro de port particulier, mots clés dans les données utiles, etc. • Base de données de signatures d'attaques doit être à jour • Ne peut pas détecter les nouvelles attaques ou les variantes d'anciennes attaques dont les caractéristiques sont modifiées **Détection d'une activité suspecte dans le comportement de l'utilisateur. Détection d'anomalies** • Caractérisation du comportement « normal » • Tout trafic déviant des caractéristiques normales est supposé malveillant (l'inverse n'est pas vraie) • Peut détecter les nouvelles attaques dont les caractéristiques ne correspondent pas aux caractéristiques normales Types d'IDS À cause de la diversité des attaques que mettent en œuvre les attaquants, la détection d'instrusion doit se faire à plusieurs niveaux. Il existe donc différents types d'IDS : Les systèmes de détection d'intrusions (IDS) : Un système de détection d'intrusion (IDS) est un logiciel qui automatise le processus de détection d'intrusion. Les systèmes de détection d'intrusions "réseaux" (NIDS) : • Détection des activités malveillantes en analysant les flots d'information échangés sur un réseau Les systèmes de détection d'intrusions de type hôte (HIDS) • Détection des activités malveillantes en analysant les évènements observés par un ordinateur hôte • Seulement couvre une machine • IDS doit être placé sur le système où il y a des information critiques/sensibles pour l'entreprise. Il existe donc différents types d'IDS :Les systèmes de détection d'intrusions hybrides Les systèmes de prévention d'intrusions (IPS) Un système de prévention d'intrusion (IPS) est un logiciel qui a toutes les fonctionnalités d'un système de détection d'intrusion et peut aussi tenter d'éviter d'éventuels incidents Ensemble de composants logiciels et matériels dont la fonction principale est de détecter et d'analyser toute tentative d'effraction (volontaire ou non). Fonctions de détection :• des techniques de sondage (balayage de ports, fingerprinting), • d'activités suspectes internes, • des activités virales, • ou encore des audits de fichiers journaux (logs). Deux notions fondamentales : • **Faux positifs** : une alerte provenant d'un IDS qui ne correspond pas à une attaque réelle.• **Faux négatifs** : une intrusion réelle qui n'a pas été détectée. NIDS Objectif : analyser de manière passive les flux en transit sur le réseau et détecter les intrusions en temps réel. Un NIDS écoute donc tout le trafic réseau, puis l'analyse et génère des alertes si des paquets semblent dangereux. Network behavior analysis (NBA) system examine le trafic réseau ou les statistiques sur le trafic réseau afin d'identifier les flux de trafic inhabituels, tels que le déni de service distribué (DDoS), certaines formes de logiciels malveillants (par exemple, vers, backdoors), et les violations des politiques de sécurité HIDS • Un HIDS se base sur une unique machine, n'analysant cette fois plus le trafic réseau mais l'activité se passant sur cette machine. • Il analyse en temps réel les flux relatifs à une machine ainsi que les journaux.• Un HIDS a besoin d'un système correct pour vérifier l'intégrité des données. Si le système a été compromis par un attaquant, le HIDS ne sera plus efficace. Comment évader l'IDS **Technique fréquente: Fragmentation** • Pour détecter une activité malveillante, l'IDS doit capturer, stocker et analyser tous les fragments. • Beaucoup de fragments s'étalent sur une longue période du temps => IDS doit avoir de grandes zones tampons et une puissance de traitement pour rassembler ces fragments **L'attaquant crée deux fragments de chaque datagramme de l'attaque :** • Premier fragment avec un entête TCP avec un numéro de port inoffensif et pas fortement surveillé par la configuration de l'IDS (Ex:80) • Deuxième fragment à un chevauchement avec le premier et comporte un numéro de port différent qui écrase le port originale **IDS laisse passer les deux fragments**• Premier fragment pour un serveur WEB • Deuxième fragment de la même session **Une fois les deux datagrammes arrivent au serveur** • Réassemblage de deux fragments avec la valeur du port dans le fragment numéro 2 • Segment dirigé vers un service vulnérable IPS Ensemble de composants logiciels et matériels dont la fonction principale est d'empêcher toute activité suspecte détectée au sein d'un système. Les IPS sont des outils aux fonctions « actives », qui en plus de détecter une intrusion, tentent de la bloquer. Les IPS ne sont pas la solution parfaite. Plusieurs stratégies de prévention d'intrusions existent : **host-based memory and process protection** : surveille l'exécution des processus et les tue s'ils ont l'air dangereux (buffer overflow). **session interception / session sniping** : termine une session TCP avec la commande TCP Reset : « RST ». Ceci est utilisé dans les NIPS. **gateway intrusion detection** : si un système NIPS est placé en tant que routeur, il bloque le trafic ; sinon il envoie des messages à d'autres routeurs pour modifier leur liste d'accès Un IPS possède de nombreux inconvénients : • Le premier est qu'il bloque toute activité qui lui semble suspecte. i.e. un IPS peut détecter une tentative de déni de service alors qu'il s'agit d'une période chargée en trafic. • Le deuxième inconvénient est qu'un attaquant peut utiliser la fonctionnalité de blocage de l'IPS pour mettre hors service un système.

IPS	IDS
Intercepte et traite le trafic réel (mode inline)	Fonctionne sur une copie du paquet (mode promiscuous)
Ajoute une latence due au traitement des paquets	Pas de latence ajoutée

Peut arrêter les paquets malveillants	Impossible d'arrêter les paquets malveillants directement. Peut travailler avec d'autres appareils.
Paquets malveillants peuvent toujours être rejetés	Certains paquets malveillants peuvent passer (par exemple, le premier paquet)

NIDS/NIPS (Network-Based)	HIDS/HIPS (Host-Based)
Le logiciel est déployé sur une machine dédiée	Le logiciel est installé sur le système d'exploitation hôte. Cela peut nécessiter le support de plusieurs systèmes d'exploitation.
Facile à entretenir et à mettre à jour	Peut nécessiter une mise à jour de plusieurs points de terminaison
A une visibilité sur tout le trafic réseau; par conséquent, peut offrir une meilleure corrélation d'événements	A une visibilité uniquement sur le trafic frappant l'hôte
Peut introduire un retard dû au traitement de paquet	Peut ralentir le système d'exploitation de l'hôte
N'a pas de visibilité sur le succès d'une attaque	Peut vérifier si une attaque a réussi à attaquer un hôte
N'a pas de visibilité sur les paquets cryptés	A une visibilité après cryptage et peut bloquer une attaque transmise via des paquets cryptés
Peut bloquer une attaque au point d'entrée	l'attaquant est capable d'atteindre la cible avant d'être bloqué

Divers méthodes de détection utilisées par NIDS et NIPS: **Pattern matching and stateful pattern-matching recognition** • détection des signatures d'attaques connues dans les paquets circulant sur le réseau • base de données de signatures d'attaques doit être à jour • ne peut pas détecter les nouvelles attaques ou les variantes d'anciennes attaques dont les caractéristiques sont modifiées • Signature: numéro de port particulier, mots clés dans les données utiles,etc **Protocol analysis** • décode tous les protocoles ou les conversations de client-serveur, identifie les éléments du protocole et les analyse en recherchant une infraction• Certains systèmes de détection d'intrusion examinent les champs de protocole explicites dans les paquets inspectés •Dépend si les protocoles sont bien définis **Heuristic-based analysis** • le balayage heuristique utilise une logique algorithmique à partir de l'analyse statistique du trafic qui traverse le réseau • beaucoup de réglage et de modification pour une meilleure réponse **Anomaly-based analysis** • caractérisation du comportement "normal", tout trafic déviant des caractéristiques normales est supposé malveillant • peut détecter les nouvelles attaques dont les caractéristiques ne correspondent pas aux caractéristiques normale **Global threat correlation capabilities** • permet au capteur IP de filtrer le trafic réseau en utilisant la "réputation" de l'adresse IP source d'un paquet • la "réputation" est calculée à l'aide des actions passées de l'adresse IP Conception services de sécurité et protection de l'infrastructure Conception Réseau"Top-Down" Conception •Compréhension de flux de données, les types de services, le type de trafic, le type de données, traitement et stockage des données, etc. •Besoins des utilisateurs •Analyser les système informatique existant, le réseau actuel (s'il existe), les exigences « requeriments ». •Concevoir une architecture logique (système représenté par ses composantes, les relations existants entre elles) avant d'un réseau physique (dispositifs, technologies, etc.) Étapes de conception**Étape 1 – Analyser les exigences "requirements** • Analyser l'entreprise et "la concurrence" : objectives et contraintes • Analyser les objectives techniques • Analyser les applications ou services • Analyser le "réseau existant" • Analyser le trafic réseau **Étape 2 – Conception architecture logique du réseau** • Concevoir une topologie logique • Concevoir les modèles pour l'adressage et les "noms" • Sélectionner les dispositifs réseau ("switchs", routeurs, etc.) • Incorporer les éléments des politiques de sécurité • Incorporer les éléments de gestion du réseau **Étape 3 – Conception physique du réseau**• Sélectionner les technologies et les dispositifs pour le réseau local • Sélectionner les technologies et les dispositifs pour l'interconnexion des réseaux (WAN) **Étape 4 – Test, évaluation, performance et documentation de la conception** • Test et évaluation du réseau • Optimisation du réseau • Documentation du réseau the network design Principes de conception• Hiérarchie• Modularité • Flexibilité • Résilience ('resiliency')

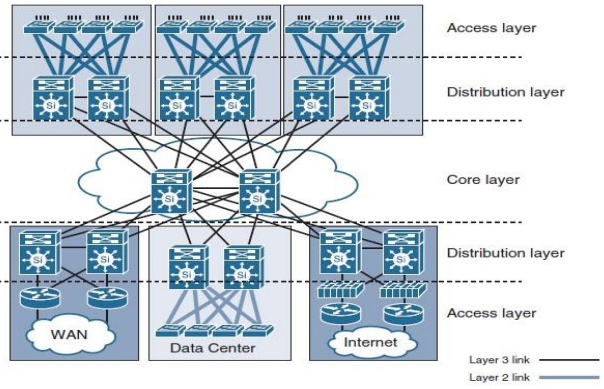
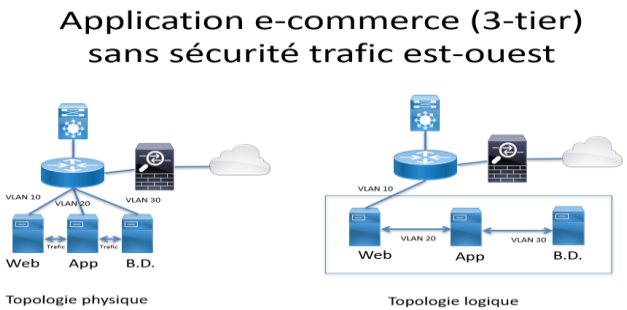
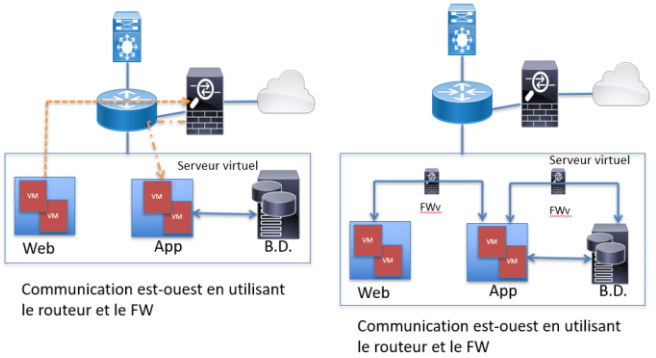


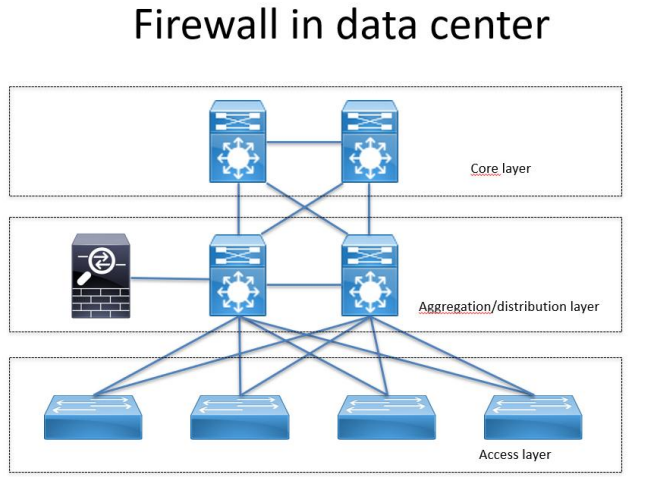
Figure 3-3 *Typical Modular Enterprise Campus Architecture*

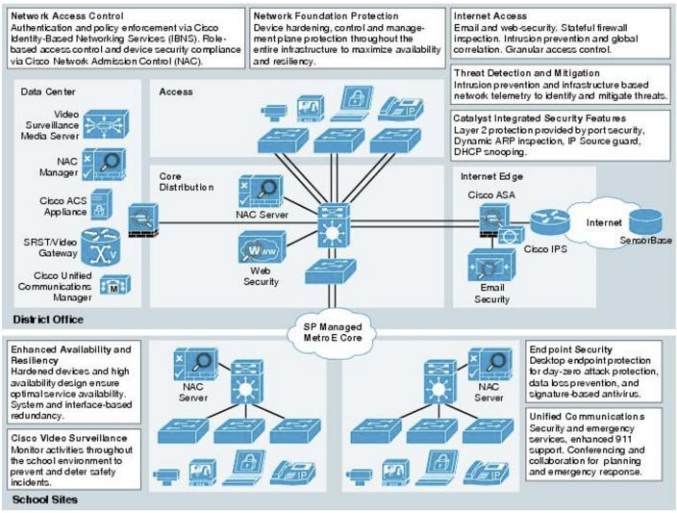
Couches • **Couche d'accès:** services pour la connectivité des dispositifs finaux ('end-device') • **Couche de distribution**: frontière entre la couche d'accès et la couche cœur • **Coche cœur ('core'):** garantir connectivité sans-arrêt au niveau du réseau ('non-stop communication') **Couche accès – services** • Sécurité • QoS • Différents services : voix, vidéo, accès données • Autres services: Découverte et configuration de services (802.1AF, CDP, LLDP)**,** Services de sécurité, identification et accès (802.1X, DHCP snooping, IPSG, …)**,** Services intelligents de contrôle **Couche de distribution But**: Services et contrôle entre la couche d'accès et la couche cœur 'core'. • Point d'agrégation pour tous les points d'accès: au niveau physique et trafic) • Connectivité pour trafic est-ouest (east-west) •Services d'agrégation, contrôle nord-sud (north-south) **Résilience** • Être capable de maintenir la stabilité comportementale d'un système même pendant les perturbations est une caractéristique essentielle de la résilience. • L'objectif d'un système résilient est d'être capable de fournir un service auquel on peut légitimement faire confiance même face à des changements, puis il doit fournir des mécanismes pour assurer la stabilité comportementale, c'est-à-dire absorber les perturbations, dégrader temporairement son état mais récupérer par la suite à son état désigné plus tard. Zone de sécurité réseau générale Zone publique (Outside) Une zone externe qui n'est pas sous le contrôle de l'organisation. Les services publics sont situés dans cette zone. Zone d'accès public (DMZ) Une zone qui héberge les services publics de l'organisation et est souvent appelée la zone démilitarisée (DMZ). Ces services sont accessibles depuis la zone publique. Les services typiques incluent le proxy de courrier électronique, le proxy Web, le proxy inverse et les services d'accès distant. Zone restreinte (Inside) Une zone interne hébergeant les services de données les plus critiques pour l'organisation. Habituellement, cette zone est la zone la plus sécurisée, et l'accès à cette zone devrait être limité. Zones de sécurité d'une architecture modulaire à des emplacements spécifiques Permet d'offrir une conception de sécurité plus sécurisée, gérable et évolutive Zone publique: En dehors de l'organisation et se trouve dans le bord d'Internet de l'entreprise (Enterprise Internet edge) Zone d'accès public: La zone d'accès public est utilisée pour héberger les services publics d'une organisation et sécuriser l'accès des utilisateurs de l'entreprise à la zone publique. Il est situé dans le bord Internet d'entreprise. Zone d'opérations: La zone d'opérations héberge des services de support pour les utilisateurs internes et les services. Cette zone est généralement située dans le module fonctionnel du centre de données intranet. Zone restreinte: La zone restreinte héberge les services de données les plus critiques et l'accès doit être limité au trafic nécessaire uniquement. Cette zone est située dans le centre de données intranet. Zone de gestion restreinte: La zone restreinte héberge les services de données les plus critiques et l'accès doit être limité au trafic nécessaire uniquement. Cette zone est située dans le centre de données intranet. Principes pour une architecture de réseau modulaire • Défense en profondeur • Modularité et flexibilité • Disponibilité du service et résilience • Conformité réglementaire • Viser l'efficacité opérationnelle • Implémentations vérifiables • Partage d'informations et collaboration globales Modules fonctionnels communs d'une architecture d'entreprise modulaire Noyau de l'entreprise (Enterprise core): partie principale du réseau et connecte tous les autres modules Centre de données intranet (Intranet data center): héberge de nombreux systèmes pour servir à des applications et à stocker des volumes importants de données. Le centre de données gère également l'infrastructure réseau qui prend en charge les applications, notamment les routeurs, les commutateurs, les équilibreurs de charge et l'accélération des applications. Campus d'entreprise (Enterprise campus): Fournit un accès réseau aux utilisateurs et aux périphériques Bord d'Internet d'entreprise (Enterprise Internet edge): Fournit la connectivité à Internet Bord WAN d'entreprise (Enterprise WAN edge): Regroupe les liens WAN qui relient les succursales distantes à un site central Succursale de l'entreprise (Enterprise branch): Les succursales fournissent une connectivité aux utilisateurs et aux périphériques à un emplacement distant. Télétravailleur (Teleworker): Réfère à tout utilisateur distant tel qu'un utilisateur disposant d'un bureau à domicile se connectant via l'Internet public au réseau d'entreprise. Commerce électronique (E-commerce): Réfère au bloc ou au module d'entreprise qui héberge des périphériques réseau et de sécurité pour fournir une connectivité sécurisée aux applications de commerce électronique. Partenaire et extranet (Partner and extranet): Ces modules fournissent une connectivité à des réseaux ou à des utilisateurs externes, tels que des partenaires commerciaux, via des liens ou des réseaux dédiés. La gestion (Management): gestion du réseau Produits et technologies pour fournir une conception de réseau sécurisée Accès sécurisé au réseau (Secure network access): utiliser un ensemble complexe et divers de points de terminaison, à la fois câblés et sans fil Technologies VPN (VPN technologies): fournit un accès sécurisé au site central Pare-feux / IPS (Firewalls/IPS): fournit un contrôle d'accès entre différents points du réseau Protection de l'infrastructure (Infrastructure protection): l'accès aux appareils doit être limité aux appareils et employés autorisés Sécurité du contenu et des applications (Content and application security): déployer des produits tels que des dispositifs de sécurité Web ou e-mail pour éviter les attaques sur les données et le contenu. Gestion de réseau et de sécurité (Network and security management): Les outils de gestion de réseau et de sécurité aident les entreprises à automatiser et à simplifier la gestion de réseau pour réduire les coûts opérationnels 3 plans de fonctionnement d'une fonctionnalité d'un périphérique réseau Plan de données (Data plane) • La grande majorité des paquets traités par un routeur le traversent au moyen du plan de données (plan d'acheminement). •Sécurité: Devrait appliquer la politique de réseau et sécuriser l'infrastructure de commutation Plan de contrôle (Control plane) •Le protocole spanning-tree, les protocoles de contrôle de routage, les keepalives, ICMP avec les options IP, MPLS LDP et les paquets destinés aux adresses IP locales du routeur traversent le plan de contrôle. •Sécurité: Devrait sécuriser l'infrastructure de routage et de commutation Plan de gestion (Management plane) •Le trafic provenant des protocoles de gestion et d'autres protocoles d'accès interactifs, tels que Telnet, Secure Shell (SSH) et SNMP, traverse le plan de gestion. •Sécurité: Devrait se concentrer sur la sécurisation de l'accès aux périphériques d'infrastructure Base pour protéger les différents plans Protection du plan de contrôle: Protège le trafic du plan de contrôle responsable du transfert de trafic en "verrouillant" les services et les protocoles de routage Protection du plan de gestion: Protège le plan de gestion contre les accès de gestion et les interrogations de gestion non autorisés, et fournit un accès sécurisé pour la gestion et le contrôle Protection du plan de données: Protège le plan de données contre le trafic malveillant et protège le transfert de données via le périphérique Éléments de sécurité de base d'une infrastructure de réseau • Sécuriser l'accès au périphérique d'infrastructure • Sécuriser l'infrastructure de routage • Résilience et survivabilité du dispositif • Mise en application des politiques du réseau • Sécuriser l'infrastructure de commutation • Considérations de sécurité SDN (Software-Defined Network) Conception de la protection de l'infrastructure • Sécuriser l'accès aux périphériques de l'infrastructure (device access) • Sécuriser l'infrastructure de routage • Dispositifs pour la résilience • Politiques réseaux • Sécuriser l'infrastructure de commutation (switchs) • Sécuriser SDN • La fonctionnalité des dispositifs réseaux est divisée en: **Plan de contrôle**: verrouiller services et protocoles de routage **Plan de gestion**: sécuriser la plan de gestion et le protéger des accès non-autorisés **Plan de données:** Sécuriser le plan de données, le protéger de trafic malicieux et éviter de renvoyer ce trafic Infrastructure de commutation • Interdire domaines de 'broadcast' • Utiliser spanning-tree sécurité • Utiliser mécanismes de filtrage • Désactiver VLAN dynamique • Désactiver port pas utilisés et les mettre dans une VLAN pas utilisée • Ne pas utliser VLAN 1

Étapes • Network Foundation Protection (NFP)— Assurer la disponibilité et l'intégrité de l'infrastructure réseau, en protégeant les plans de contrôle et de gestion.• Internet Perimeter Protection— Assurer une connectivité Internet sécurisée et protéger les ressources internes et les utilisateurs contre les logiciels malveillants, les virus et autres logiciels malveillants. Protéger les utilisateurs des contenus nuisibles et inappropriés. Application des règles de messagerie et de navigation Web. • Network Access Security and Control— Sécuriser les accès. Renforcer l'authentification et l'accès basé sur les rôles pour les utilisateurs. S'assurer que les systèmes sont à jour et conformes aux politiques de sécurité du réseau.• Network Endpoint Protection— Protéger les utilisateurs, contre les contenus nuisibles et inappropriés. Application des règles de messagerie et de navigation Web

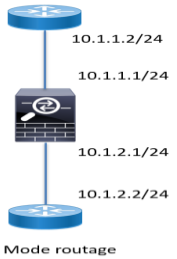








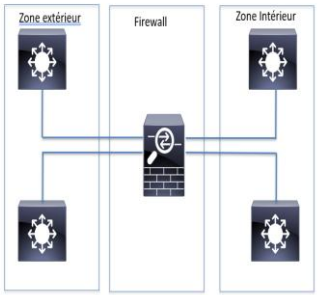
Firewall mode



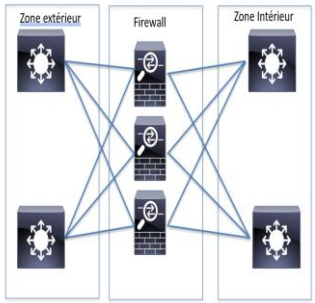
Mode routage

Mode transparente: les plus utilisé

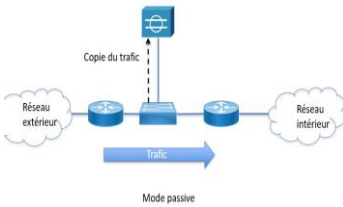
Non redondant



Haute disponibilité



IPS mode de déploiement

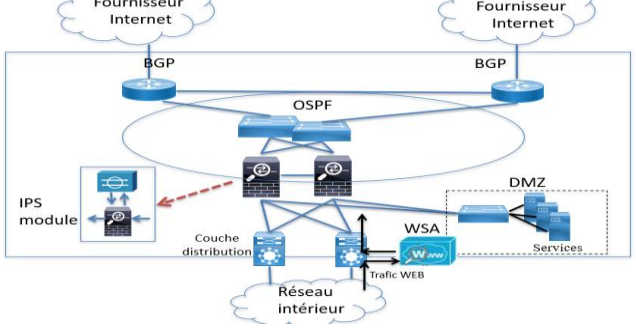


Mode passive

IPS mode de déploiement

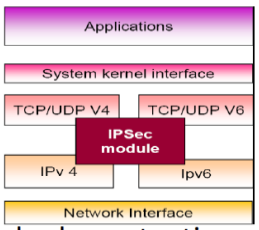
Mode en ligne

Connectivité + Sécurité + IPS + WSA (web security appliance)

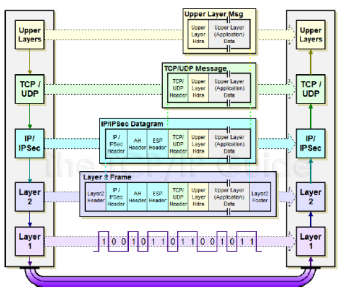


Protection de base pour le réseau Dispositifs d'accès • Restreindre: personnes, port et protocoles• Renforcer AAA (authentication, authorization, accounting) •Utiliser SH et HHTPS •Désactiver connexions pas utilisées Infrastructure de routage •Utiliser MD5 pour authentification de voisins •Renforcer le filtrage de routes •Utiliser logs Résilience Synchronisation du réseau • Utiliser NTP • Utiliser SNMP, Radius • Surveiller utilisation de CPU et mémoire des systèmes critiques Renforcer politiques du réseau • Utiliser filtres à la frontière du réseau • Renforcer protection contre IP spoofing: utiliser ACL, unicast reverse path forwarding (uRPF) Protection des commutateurs • Concevoir une architecture hiérarchique, segmentation du LAN en multiples sous-réseaux IP ou VLAN pour réduire les domaines de 'broadcast'.• Désactiver port pas utilisés et les associer à une VLAN pas utilisée Gestion réseau • ACL, NAT, SH, HHTPS Protection périmètre Internet Campus et succursales • Une connexion Internet centralisée. • Définir services communes (courriel, web, serveur web entreprise, ...) • Fonctions de sécurité pour le périmètre -Internet border router (routeur de frontière) -Firewall -Services publiques (DMZ) -Sécurité courriel -Sécurité web Sécurité Protection de l'infrastructure 1IPsec •Afin de réduire le risque des écoutes et des usurpations d'identité, le groupe IPsec de l'IETF a intégré des mécanismes de sécurité dans les protocoles IPv 4 et IPv 6 afin de : –chiffrer les paquets IP (leur contenu seul ou le paquet entier), –introduire un authentificateur permettant de certifier l'équipement émetteur et de contrôler l'intégrité de tout ou parties du dupaquet IP. •La version protégée du protocole IP fait appel à la suite de protocoles IPsec qui comprend les protocoles **AH (Authentication Header), ESP Encapsulating Security Payload et le protocole de gestion dynamique de la sécurité IKE Internet Key Exchange).** • Ces trois protocoles reposent sur la définition d'une politique de sécurité liée aux besoins de sécurité du réseau. •La suite de protocole IPsec comprend **trois sous protocoles, •Les deux premiers** servent directement à la protection des paquets IP et consistent en deux nouveaux en têtes (encore appelés «extensions» pour la nouvelle génération IPv 6 du protocole IP), • Le **troisième** intervient au niveau applicatif afin de gérer dynamiquement la sécurité. •**L'en-tête d'authentification (Authentication Headerou AH)** contient, entre autre,

IPSec

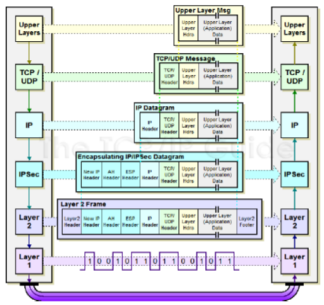


Mode de protection



Le mode transport

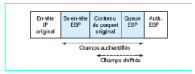
Mode de protection



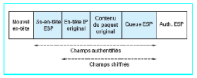
Le mode tunnel

un authentificateur Il permet donc de vérifier l'identité de l'équipement de sécurité émetteur et de contrôler l'intégrité des données, **•L'en-tête ESP (Encapsulating Security Payload)** permet de transporter un paquet IP, tout ou en partie chiffré, ainsi qu'un authentificateur offrant la même gamme de services que l'en-tête d'authentification. •**Le protocole IKE (Internet Key Exchange)** assure une gestion dynamique de la sécurité en permettant aux équipements de sécurité de s'authentifier et de convenir de la manière de protéger leurs échanges IP. •Les protocoles IPsec peuvent servir à protéger des échanges IP: **–de bout en bout**, **–sur des segments de réseau**. •Deux modes de protection par IPsec: **–Le mode tunnel, –Le mode transport. 1.1En tête d'authentification AH** •AH assure le contrôle d'intégrité et la protection contre le rejoué des messages (anti replay) mais pas le secret (pas de chiffrement). •AH est utilisé lorsqu'on souhaite vérifier l'intégrité des données sans se soucier du

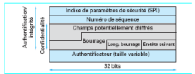
ESP



En-tête ESP en mode transport



En-tête ESP en mode tunnel

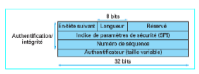


Format de l'en-tête ESP

En-tête AH

En-tête d'authentification AH en mode transport

En-tête d'authentification AH en mode tunnel



Format de l'en-tête AH

secret. •L'une des caractéristiques importantes d'AH est que le test d'intégrité ne porte que sur les champs fixes de l'en-tête IP (ceux qui restent identiques au cours du transit de message de routeur en routeur. Adresse IP-source ne change pas (pour éviter falsification de l'origine d'un paquet), TTL change à chaque routeur. 1.**AH-Mode transport** : L'authentificateur ne protège que le contenu du paquet IP L'en-tête AH est placé entre l'entête IP original du paquet IP original et le contenu du paquet. 2.**AH-Mode tunnel :** Le paquet IP original, arrivant sur un équipement tunnelier, est encapsulé dans un nouveau paquet IP La protection offerte par l'en-tête AH porte alors sur tout le paquet IP original et sur les champs en-tête et options du nouveau

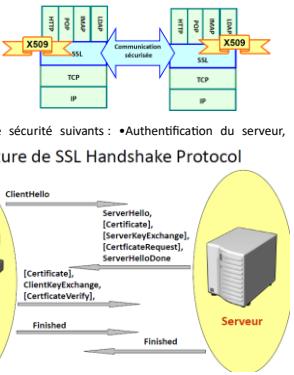
Tableau 2 – Mécanismes de sécurité en fonction des couches TCP/IP

Service	Mécanisme	Couche physique	Réseau IP	Transport TCP	Application
Confidentialité	Chiffrement de données	x	x	x	x
	Masquage d'identité		x	x	
	Saturation de ligne	x			
	Anonymat des flux	x	x (1)		
Intégrité spatiale	Motif explicite		x	x	x
Intégrité temporelle	Antisuppression			x	x
	Anti-interversion			x	x
	Anti-insertion (2)		x	x	x
	Antirejeu		x	x	x
	Antirépudiation				x
Authentification	Preuve personnelle				x
	Preuve de l'origine		x	x	x

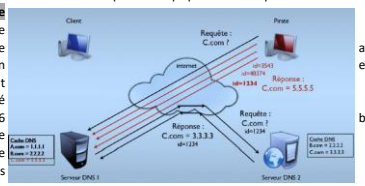
(1) L'anonymat des flux est un mécanisme de confidentialité permettant de dissimuler la nature des sessions (occurrence des sessions, type d'application et profil des séquences de messages). La saturation de flux permet de l'obtenir au niveau physique. Il existe aussi des possibilités pour mettre en œuvre ce mécanisme de façon plus ou moins limitée au niveau IP, mais avec des conséquences rédhibitoires sur l'efficacité du réseau.
(2) Mécanisme très rarement considéré, car il vient en corollaire du contrôle d'intégrité spatiale et de l'antirejeu.

paquet qui ne sont pas modifiables par le réseau de transit. **1.2 L'en-tête ESP (Encapsulating Security Payload)** permet d'assurer la confidentialité des paquets IP, mais aussi celle des flux, cette dernière permettant de garantir que même une analyse statistique sur les flux échangés (Volume, fréquence), ne conduira à aucune déduction quant à la teneur des échanges, •Tout comme l'en-tête d'authentification le fait, l'en-tête ESP peut prouver l'intégrité des paquets et l'identité de son émetteur L'authentificateur permet optionnellement de détecter les rejeux de paquets, •Contrairement à AH, ESP encapsule véritablement l'ensemble des champs à protéger, ce qui justifie le Encapsulating de ESP. **1.ESP-Mode transport:** seul le contenu du paquet IP est protégé Plus précisément le contenu du paquet et la queue ESP sont chiffrés Ainsi, le contenu du paquet IP est protégé L'en-tête ESP est placé après l'en-tête IP original en dernière position, **2.ESP-Mode tunnel** tout le paquet IP est protégé C'est à dire, le paquet IP, arrivant sur un équipement tunnelier, est entièrement chiffré, ainsi que la queue ESP. **1.3AH et ESP** •Les possibilité d'ESP recouvrent celles d'AH et vont plus loin. •AH existe pour des raisons historiques. l'origine, AH ne gérait que l'intégrité et ESP ne gérait que le secret. •Après, la gestion de l'intégrité a été ajouté à ESP. **1.4IKE Internet Key Exchange** •L'IETF a défini un protocole de gestion dynamique des clés d'associations de sécurité appelé IKE pour Internet Key Exchange Les équipements mettant en oeuvre IKE sont en écoute sur le port 500. **1.5 SSL : Secure Socket Layer** •Protocole de sécurité d'Internet pour les connexions point-à-point, •Développé par Netscape pour garantir la sécurité de la transmission de données sur Internet, •Fournit une connexion sécurisée entre le client et le serveur, •Protocole entre TCP et les protocoles applicatifs, •2001 l'IETF : rachète le brevet de SSL à Netscape et le rebaptise TLS (Transport Level Security, RFC 2246) (version 1 0). 2.Présentation de SSL SSL **2.1Secure Socket Layer** •SSL permet de sécuriser la transmission de données sur, internet en utilisant la cryptographie par clé publique. •Son principe consiste à établir un canal de communication sécurisé (chiffré) entre deux machines (un client et un serveur) après une étape d'authentification. •SSL est un complément à TCP/IP et permet (potentiellement) de sécuriser n'importe quel protocole ou programme utilisant TCP/IP. **2.2 Fonctionnement de SSL** SSL fonctionne selon un mode client-serveur Il fournit les objectifs de sécurité suivants : •Authentification du serveur, •Confidentialité des données qui s'échangent, •Intégrité des données, •Authentification du client, optionnellement. **SSL consiste en deux protocoles:** •SSL handshake protocol, •SSL Record Protocol. **1.Authentification** : –Serveur (obligatoire) : pour confirmer son identité, **–Client (optionnel)** : nécessaire quand par exemple le serveur est une banque, –Utilisation de certificat X509 v3, –Utilisation d'algorithme de chiffrement à clé publique pour vérifier le certificat, –Se fait à l'établissement de la session. **2.Confidentialité :** –Algorithme de chiffrement symétrique, –Clé générée à l'établissement de la session. **3.Intégrité, 4.**Fonction de hachage avec une clé secrète qui génère une empreinte appelée MAC (Message Authentication Code). **2.3Pile protocolaire de SSL** •Consiste en deux niveaux de protocoles, –Le protocole Record, –3 protocoles de niveau supérieur : •Handshake Protocol, •Change Cipher Spec Protocol, •Alert Protocol. **2.4 SSL : Session / Connexion** **•Session :** –Association entre un serveur et un client, –Créée par le protocole Handshake, –Définit un ensemble de paramètres cryptographiques, de sécurité qui peuvent être utilisés pour plusieurs connexions (évite une négociation de paramètres de sécurité à chaque connexion). **•Connexion:** –Relation de type point à point, –Chaque connexion est associée à une session. **2.5 SSL Handshake Protocol** Négociation SSL Deux parties: un Client et un Serveur Elles s'échangent, au début de la communication: •la liste des méthodes de chiffrement et de signature que chacun connaît, avec longueur des clés, •les méthodes de compression, •les nombres aléatoires, •les certificats. **2.6 SSL Record Protocol** **•Le protocole Record fournit 2 services à une connexion SSL**: –**Confidentialité**: définit une clé secrète pour le chiffrement, **–Intégrité du message**: définit une clé secrète pour le calcul de l'empreinte. **•SSL Record Protocol: opérations** –Fragmentation: Le message est fragmenté en blocs de taille maximum 214 octets –Compression: Cette opération est prévue dans les spécifications mais non implémentée, –Calcul du MAC (message authentication code): Utilise la clé secrète. •Utilise l'algorithme SHA-1 ou MD5. –Chiffrement : Le message + MAC sont chiffrés avec un chiffrement symétrique. –Ajout de l'en-tête: 5 octets, composée de longueur du message, version, etc. **2.6.1Avec SSL, l'expéditeur des données :** •découpe les données en paquet (de 16384 octets ou moins), •compresse les données (optionnellement), •signe cryptographiquement les données, •chiffre les données, •envoie les données. **2.6.2 Avec SSL, celui qui réceptionne les données** •déchiffre les données, •vérifie la signature des données, •décompresse les données, •réassemble les paquets de données, **2.6.3 Alert Protocol** •Peut être invoqué par: –l'application (pour signaler la fin d'une connexion), –le protocole Handshake (suite à un problème survenu au cours de la négociation). **2.7 Analyse de SSL** SSL et Sécurité : risque dans les négociations À la négociation, les parties vont s'authentifier, 3 modes d'authentification possible: •les deux parties s'authentifient, •le serveur s'authentifie seulement, •aucune des parties ne s'authentifie pas (total anonymat). En mode «total anonymat » la communication est seulement protégée contre l'écoute passive. Une attaque du type "man in the middle" est toujours possible. **2.7.1 HTTPS** HTTPs (HTTP + SSL) Avec HTTPs. On ouvre d'abord une connexion sur le port 443 du serveur (port par défaut pour HTTPs). Lorsque la connexion TCP est établie, le client et le serveur initialisent la couche SSL en négociant les paramètres cryptographiques et en échangeant les clés. Les requêtes et réponses HTTP échangées entre le client et le serveur sont alors encryptées avant d'être transportées par TCP. 3. SMTP •Standard permettant de transférer le courrier d'un client SMTP a un serveur SMTP, •Protocole à des commandes textuelles, •Décrit dans le RFC 821 (protocole de transmission) et le RFC 822 (format des messages), •Port utilisé par défaut sur le port 25). **3.1Principe du SMTP** **•L'envoie de Email est base sur le principe suivant:** –Un client SMTP fait une requête d'expédition de Email vers le serveur SMTP. –Ce serveur peut être la destination finale ou ne peut être qu'un intermédiaire. –Les commandes SMTP ne sont générées que par le client SMTP et sont destiné au serveur SMTP. –Chacune des commandes envoyées par le client est suivi d'une réponse du serveur SMTP composée d'un numéro et d'un message descriptif. **•Format du message messageSMTP** –To : liste des destinataires principaux, –Cc : liste des destinataires secondaires, –Bcc : liste des destinataires de copie cachée, – From : auteur du message, –Sender: adresse de messagerie de l'émetteur, –Subject : pour le sujet du message. –Date : date a laquelle le message a été envoyé, parfait pour antidater un message, –Return-Path : donne une adresse pour la réponse qui soit différente de l'adresse utilisée pour l'envoi (celle qui figure dans le champ 'To'). Quand le destinataire utilisera la fonction 'Répondre' de son outil de messagerie, c'est cette adresse qui sera utilisée. **•Limitation du protocole SMTP** •la longueur du message qui ne doit pas excéder 64Ko, •Problème de temporisation, •SMTP ne convient plus au type d'échange multimédia, •Un serveur SMTP peut servir de relais de mailing anonyme, •Les commandes EXPN et VRFY posent un problème de sécurité, •Pas d'accuse de réception, •La communication se fait en clair. **3.2.Sécurité** •Une des limitations de SMTP vient de l'impossibilité d'authentifier l'expéditeur, •Extension SMTP AUTH été définie, mais pas beaucoup utilisé, •ISP bloquent le port 25 pour éviter au client résidentiel d'envoyer messages SMPT. 4. DNS (Domain Name Server) •DNS (Domain Name Server) permet d'effectuer une correspondance entre un nom de système et son adresse IP. •C'est un protocole qui possède deux parties : •client: «Resolver» ; •serveur: «Name server». **4.1 Principe de Empoisonnement du cache** Toute la difficulté de repose sur la possibilité d'envoyer une réponse bon identifiant, avant le serveur DNS original. En serveur DNS ne modifiera pas son cache s'il reçoit réponse avec un identifiant qu'il n'a pas utilisé relayer une requête. Cet identifiant est codé sur 16 donc 65536 possibilités. A première vue, il semble d'envoyer assez de message pour tomber sur le identifiant. Pourtant, d'après le paradoxe des

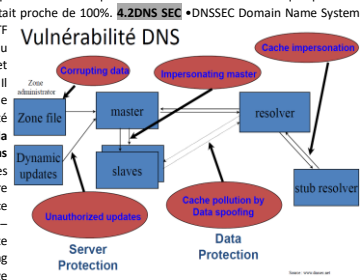
Structure de SSL Handshake Protocol



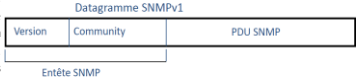
l'attaque l'attaque avec le effet, le une pour bits, il y a difficile bon



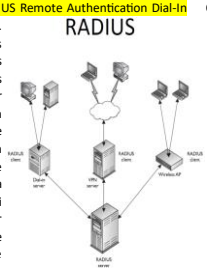
anniversaires*, la probabilité de collision est assez élevée pour rendre l'attaque faisable. Une étude a montré qu'à partir de 800 réponses envoyées, le taux de réussite de l'attaque était proche de 100%. **4.2DNS SEC** •DNSSEC Domain Name System Security Extensions est un protocole standardisé par l'IETF permettant de résoudre certains problèmes de sécurité du protocole DNS. •DNSSEC a été conçu pour protéger l'Internet contre certains attaques, tels que 'DNS cache poisoning Il s'agit d'un ensemble d'extensions au DNS, qui prévoient une authentification de l'origine de données DNS et l'intégrité des données. **•Notez que DNSSEC ne prévoit pas la confidentialité des données et DNSSEC ne protège pas contre les attaques DDoS.** •Ces mécanismes nécessitent des modifications du protocole DNS DNSSEC ajoute quatre nouveaux types d'enregistrement de ressource : –Resource Record Signature (RRSIG), –DNS Public Key(DNSKEY), –Delegation Signer(DS), –Next Secure(NSEC). •DNSSEC ajoute aussi deux nouveaux champs DNS tête : –Checking Disabled(CD), –Authenticated Data(AD). •DNSSEC protège contre l'usurpation et corruption de données, •DNSSEC prévoit également des mécanismes pour authentifier les serveurs et les demandes. •DNSSEC prévoit des mécanismes pour établir l'authenticité et l'intégrité. 5.SNMP •Le protocole SNMP (Simple Network Management Protocol): protocole pour la gestion des équipements réseaux. •Les principaux acteurs: –**Les superviseurs**: machines centrales permettant aux administrateurs de contrôler en temps réel toute l'infrastructure réseau et de diagnostiquer les problèmes. –**Les équipements**: éléments du réseau (routeur, serveur, switch…). –**Les agents**: entités qui se trouvent sur chaque noeud administrables connectant l'équipement managé au réseau et qui permettent de récupérer des informations réseaux. –**MIB**: base de données maintenue par les agents et contenant des informations matérielles, des paramètres de configuration qui sont liés au comportement des équipements réseaux. L'administrateur va interroger chacune des machines du réseau et va pouvoir ainsi obtenir les informations souhaitées et en modifier certaines. •Modèle client/serveur, •Fonctionne avec des requêtes, des réponses et des alertes. **5.1 Fonctions du protocole SNMP** Permet l'échange d'information entre les gestionnaires et les agents : •De manière sollicitée ou non, •Par l'utilisation d'un nombre très réduit de messages, •Contenant des unités d'information simples.



•Aspect authentification de la transmission, •Le gestionnaire et l'agent traitent le PDU SNMP seulement si la version et le "community string" du message sont valides.

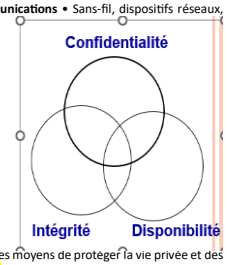


5.2 Les différentes versions Le protocole SNMP V1 : Ses avantages : •Conception simple, •Largement répandu aujourd'hui, •Evolutif. **Ses inconvénients :** •le transfert des données à travers le réseau entraine une surcharge, •Non efficace pour le transport d'une grande quantité de données, •Aucune vérification n'est mise en place, •L'authentification n'est pas sécurisée. **Malgré un système de sécurité quasi inexistant, SNMP v1 est largement implémenté aujourd'hui dans les différents réseaux!. Le protocole SNMP V3** résout principalement les problèmes de sécurité et de modularité. **5.3Les principaux changements: 1.L'authentifications** : L'authentification permet d'assurer que le paquet reste inchangé pendant la transmission et que le mot de passe est valide l'usager qui fait la requête. **2.Le cryptage**: permet d'empêcher qu'un pirate potentiel obtienne des informations de gestion en écoutant sur le réseau les requetes et les réponses des utilisateurs. Il se fait par le biais d'un mot de passe <partagé> entre le superviseur et l'agent. SNMP v3 utilise deux mots de passe: un pour l'authentification, l'autre pour le cryptage, les systèmes d'authentification et de cryptage sont indépendants. **3.L'estampillage du temps:** empêche la réutilisation d'un paquet SNMP v3 déjà transmis antérieurement. **Un pirate potentiel peut** : •Saisir un paquet lorsqu'un administrateur effectue une mise à jour sur un équipement. •Le retransmettre à l'équipement lorsqu'il souhaite faire une mise à jour illicite sur l'équipement. **On appelle ce type d'attaque: Replay Attack, Solutions :** •Le temps est estampillé sur chaque paquet, •On compare le temps actuel avec le temps du paquet, •Si la différence est supérieure à 150 secondes : le paquet est ignoré. **5.4Vulnérabilités 5.4.1Principales vulnérabilités dans SNMP v1** le protocole SNMP v1 n'est pas sécurisé. **Problème**: c'est la seule version admise et supportée par tous les équipements. **Vulnérabilités dans la gestion des notifications:** découvertes de multiples vulnérabilités sur de nombreux superviseurs SNMP qui décodent et traitent les messages d'alarmes SNMP, **Vulnérabilités dans la gestion des requêtes:** découvertes de multiples vulnérabilités dans la manière dont les nombreux agents SNMP décodent et traitent les messages SNM. **Impacts**: •Déni de service, •Vulnérabilités dans le format des chaines de caractères, •Débordement de buffer. **5.4.2 Attaque de la chaine communauté sur SNMP v1.** Principe de général : La communauté est une chaine de caractères qui est utilisée dans les requêtes SNMP pour établir de sécurité. **But :** Utilisée comme moyen d'authentification dans SNMP v1. **Les communautés:** Public: permet d'accéder aux informations basiques et accessibles à tous, Privé: permet d'accéder aux informations plus sensibles. Chaque communauté possède des droits différents en lecture et en écriture. Problème : passe en clair sur le réseau, Impact : entraine des attaques de reniflement de paquets (sniffing). **Principe de l'attaque**, 1.Utilisation d'un scanner de ports comme **nmap** pour repérer quels sont les **agents** et quels sont les **superviseurs**. Les ports habituels sont : •161 pour l'écoute des requetes par les agents. •162 pour l'écoute des traps par le superviseur. 2.Trouver le nom de la communauté accessible : il existe des outils qui : •testent une grande quantité de noms automatiquement en essayant toutes les combinaisons possibles. •regardent quand une communauté est trouvée, si elle est accessible en écriture ou non. **Solution:** •Si SNMP est non indispensable: désactivation, •Modifier le nom de communauté en un nom de notre propre choix, •Valider et vérifier les noms <communauté> en utilisant snmpwalk, •Si possible, mettre la MIB en lecture seule. **Attention! Même si les noms de communautés sont modifiés, ils passeront toujours en texte clair et seront donc sujets à des attaques. SNMP v3 offre des possibilités additionnelles pour assurer l'authentification et l'intégrité.** 6.RADIUS Remote Authentication Dial-In User Service •Protocole standard d'authentification. •Défini RFC 2865 et 2866. •Fonctionnement basé sur un système client/serveur chargé de définir les accès d'utilisateurs distants à un réseau. •Le protocole RADIUS permet de faire la liaison entre des besoins d'identification et une base d'utilisateurs en assurant le transport des données d'authentification de façon normalisée. •Architecture RADIUS : –sur un serveur (le serveur RADIUS),relié à une base d'identification (base de données,annuaire LDAP, etc). –sur un client RADIUS, appelé NAS (Network Access Server), faisant office d'intermédiaire entre l'utilisateur final et le serveur. •En général seulement le mot de passe est chiffré. •Utilisation d'UDP (UDP ports: 1812 pour RADIUS Authentication ,1813 for RADIUS Accounting'). •Le serveur RADIUS peut faire office de proxy, c'est à dire transmettre les requêtes du client à d'autres serveurs RADIUS. •Le serveur traite les demandes d'authentification en accédant si nécessaire à une base externe base de données SQL, annuaire LDAP, comptes d'utilisateur de machine ou de domaine. –un serveur RADIUS dispose pour cela d'un certain nombre d'interfaces ou de méthodes. •Protocole d'authentification PAP,CHAP,orEAP. •Utilisation de PPP



Introduction Sécurité 1-Pourquoi c'est difficile de sécuriser un système? • Développement de nouveaux usages • Ouverture du système d'information • Multiplication de projets complexes • Refonte du système d'information • Essor de la mobilité intra et inter entreprise • Accès distants • Technologies sans fil • Architectures multi-tiers • Infonuagique (Cloud computing), fog computing • Internet des objects (IoT) • Télémaintenance • Diversité et multiplicité des acteurs • Complexité technologique, organisationnelle, juridique • Dépendance et vulnérabilité

2-Les points clés de la sécurité : **2.1 Authentification :** • Garantie de l'identité du correspondant ; • Contrôle basé sur des critères prédéfinis (savoir, avoir, être). **2.2 Contrôle d'accès :** • Contrôle de l'accès à une ressource. **2.3 Non-répudiation :** • L'expéditeur d'une information ne peut rejeter, renoncer, démentir, récuser, contester, nier en être l'auteur. **2.4 Protection de la vie privée ('privacy') 2.5 Simplicité :** • Simplification des mécanismes de contrôle d'accès, d'authentification, etc. • Adaptation aux environnements et situations propres à l'activité. **2.6'Anti-replay' :** • S'assurer que les données ne peuvent être émises / traitées, un nombre de fois, à l'insu des correspondants. **2.7 Communications** • Sans-fil, dispositifs réseaux, protocoles réseaux 3-Confidentialité • qui peut "voir" quoi? • Intérêts publics/privées vs. vie privée



4- Intégrité • exactitude • précision • modifications autorisées seulement • cohérent 5- Disponibilité • présence sous forme utilisable • capacité à rencontrer • les besoins et spécifications • les contraintes de « temps ,performance ,qualité « 6- Définitions de termes de sécurité 6.1 Accessibilité 'Accessibility': capacité de limiter, contrôler, et de déterminer le niveau d'accès que les entités ou utilisateurs ont sur un système et la quantité d'informations qu'ils peuvent recevoir; 6.2 Responsabilité 'Accountability': La capacité de suivre ou de vérification des activités d'un individu ou une entité sur un système. 6.3 Authenticité 'Authenticity': La propriété d'être en mesure de vérifier l'identité d'un utilisateur, processus, ou un dispositif, souvent comme une condition préalable à permettre l'accès aux ressources dans un système d'information. 6.4 Confidentialité 'Confidentiality': Préserver les restrictions sur l'accès à l'information et de communication, y compris les moyens de protéger la vie privée et des renseignements exclusifs. 6.5 Prévention des fautes 'Fault Avoidance (Prevention)': Une technique utilisée dans une tentative pour empêcher l'apparition de défauts.

6.6 Isolation des fautes 'Fault Containment': Le processus consistant à isoler une faute et la prévention de l'effet de multiplication 6.7 Détection d'une faute 'Fault Detection': Le processus de détection qu'une faute s'est produite 6.8 Prévision des fautes Fault Forecasting (Prediction)': Les moyens utilisés pour estimer le nombre actuel, l'incidence future, et la conséquence probable de fautes 6.9 Localisation de fautes 'Fault Location': Le processus de détermination où la faute s'est produit alors une reprise peut être utilisé 6.10 Intégrité 'Integrity': Protection contre la modification ou la destruction de l'information, et consiste à veiller pour la non-répudiation et l'authenticité de l'information 6.11 Maintenabilité 'Maintainability': La facilité avec laquelle un système ou un composant peut être modifié pour corriger les fautes, améliorer les performances, ou de s'adapter à un environnement modifié 6.12 Non-répudiation 'Non-Repudiation': l'assurance que l'expéditeur de l'information est fourni avec une preuve de livraison et le destinataire est fourni avec une preuve d'identité de l'expéditeur, de sorte que ni peut ensuite nié avoir traité l'information 6.13 Performabilité 'Performability': La mesure dans laquelle un système ou un composant accomplit ses fonctions désignés au sein de contraintes, comme la vitesse, l'exactitude ou l'utilisation de mémoire. Il est également défini comme une mesure de la probabilité que certain sous-ensemble des fonctions est effectuée correctement 6.14 Sécurité 'Safety': La propriété d'un système qui tombe en panne de façon de ne pas des dommages catastrophiques pendant une période de temps spécifiée 6.15 La fiabilité (reliability) désigne ici la capacité d'un réseau d'exécuter, dans certaines conditions, un ensemble de fonctions pendant des durées d'opérations spécifiées. On peut la mesurer de deux façons: **6.15.1 la disponibilité (availability),** soit la capacité d'un réseau d'exécuter ses fonctions, à n'importe quel instant donné, sous certaines conditions incluant la dégradation du service (Probabilité pour qu'un système soit en fonctionnement à un instant t donné) **6.15.2 La fiabilité** : Probabilité pour qu'un système soit continûment en fonctionnement sur une période donnée (entre 0 et t).

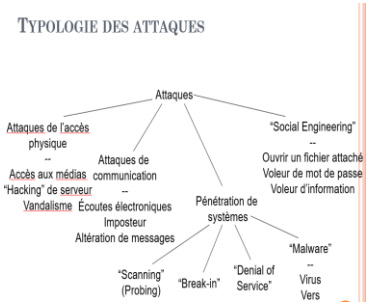
7- CYBER KILL CHAIN 7.1 Reconnaissance C'est la phase de collecte de renseignements. Dans la phase de reconnaissance, les cyber-attaquants sont concernés par la recherche, l'identification et la sélection des cibles. Ceci est souvent réalisé en parcourant Internet à la recherche de participants des conférences, d'adresses e-mail, de relations sur les réseaux sociaux ou d'informations sur les systèmes cibles. L'étape de reconnaissance est celle où les comportements sécurisés peuvent avoir un impact important. Une organisation soucieuse de la sécurité saura qu'elle est une cible potentielle et limitera les informations qu'elle partage, réduisant ainsi le risque d'attaques de 'spear phishing' et 'whaling attacks' (les deux attaques sont du type 'phishing' pour des personnes spécifiques: CEO, …)

Cela ne veut pas dire que détecter les efforts de **reconnaissance** en temps réel n'est pas difficile. C'est le cas et ces contrôles n'arrêteront pas tout. Cependant, découvrir une reconnaissance après coup peut toujours fournir un contexte sur l'intention d'un attaquant. Mécanismes de détection suivants : • Collecte des journaux (logs) des visiteurs du site Web pour la modification et la recherche historique • Collaborer avec les administrateurs Web pour utiliser leurs analyses de navigateur existantes • Création de détections pour les comportements de navigation propres à la reconnaissance • Donner la priorité aux défenses autour de technologies ou de personnes particulières en fonction de l'activité de reconnaissance 7.2 L'étape de militarisation ('weaponization') est la phase de préparation et de mise en scène d'une cyberattaque. L'agresseur n'a toujours pas interagi avec sa victime. Au lieu de cela, ils créent leur attaque. Cela signifie généralement associer un logiciel malveillant, comme un cheval de Troie d'accès à distance, à un exploit au moyen d'un outil automatisé appelé 'weaponizer'. Par exemple, un attaquant peut créer un document Microsoft Office infecté destiné à être livré via des e-mails pour 'phishing'. La détection contre les artefacts de militarisation est l'une des défenses les plus durables et les plus résistantes. Contrôles de sécurité qui peuvent réduire la probabilité et l'impact de l'étape de militarisation : • Formations de sensibilisation à la sécurité • Effectuer une analyse des logiciels malveillants non seulement sur la charge utile, mais aussi sur la façon dont elle a été créée • Détections de construction pour les 'weaponizer' 7.3 Livraison • La livraison est la troisième phase de la chaîne de destruction cybernétique et fait référence aux vecteurs d'attaque utilisés pour livrer des charges utiles malveillantes(les pièces jointes aux courriels, les sites Web et les supports USB étaient les trois vecteurs de livraison les plus répandus). • Parmi les trois vecteurs d'attaque les plus courants ci-dessus, deux d'entre eux reposent sur une forme d'interaction humaine. • En apprenant aux gens à s'arrêter lorsqu'ils ont l'impression que quelque chose ne va pas, on peut empêcher la livraison d'une multitude de logiciels malveillants différents. • On ne peut pas arrêter tous les exploits 'wormable'. Par exemple, l'attaque EternalBlue qui ciblait les protocoles SMB obsolètes et a conduit à l'attaque du rançongiciel WannaCry. • Les contre-mesures pour l'étape de livraison comprennent : • Analyse du support de diffusion pour comprendre l'impact des systèmes cibles • Comprendre les serveurs et les personnes ciblés, leurs rôles et responsabilités, et les données sensibles auxquelles ils ont accès • Déduire l'intention des adversaires sur la base du ciblage • Tirer parti des outils de militarisation pour détecter de nouvelles charges utiles malveillantes au point de livraison • Analyser l'heure de la journée à laquelle l'attaque a commencé • Collecte des courriels et des journaux Web pour la reconstruction, même si une intrusion est détectée tardivement, vous devez être en mesure de déterminer quand et comment la livraison a commencé • Processus de gestion et d'évaluation des vulnérabilités 7.4 Exploitation Une fois à l'intérieur du système, l'intrus tentera de se déplacer latéralement vers d'autres systèmes/comptes sur le réseau. Le but est d'augmenter le niveau d'autorisation afin d'accéder à plus de données • Une fois que la charge utile a été livrée à la victime, l'exploitation déclenche le code des intrus. • Le plus souvent, cela ciblera une vulnérabilité d'application ou de système d'exploitation, mais cela pourrait aussi simplement exploiter la victime ou tirer parti d'une fonctionnalité du système d'exploitation qui exécute automatiquement le code. • Pour améliorer la sécurité : - Formation à la sensibilisation des utilisateurs et tests de messagerie pour les employés Formation au codage sécurisé pour les développeurs Web - Analyse régulière des vulnérabilités et tests de pénétration

- Mesures de renforcement des points de terminaison telles que la restriction des privilèges d'administrateur et des règles de point de terminaison personnalisées pour bloquer l'exécution du shellcode - Audit des processus des terminaux pour déterminer de manière médico-légale l'origine de l'exploit

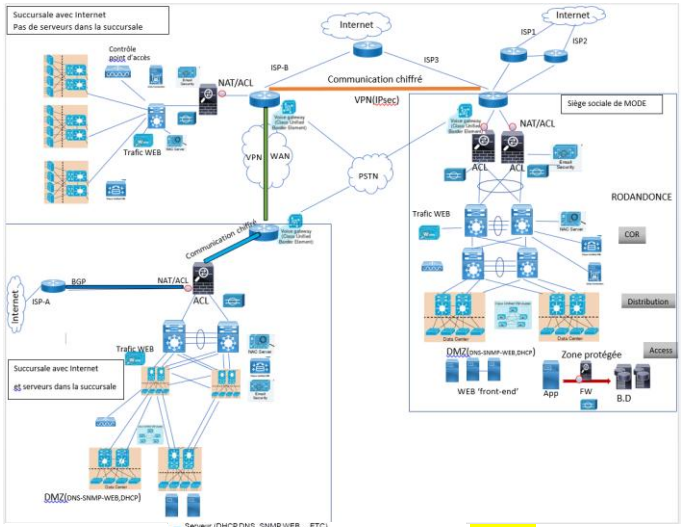
7.5 Installation La phase d'installation décrit les actions entreprises par un acteur malveillant pour établir une porte dérobée ('backdoor') dans le système ciblé. Cela donne à l'acteur malveillant un accès soutenu et persistant à la cible, lui fournissant ainsi un moyen d'accéder au système quand il le souhaite • La phase d'installation implique que l'attaquant a un exploit actif en cours d'exécution sur le système cible. • Dans cette situation, ils peuvent rechercher des vulnérabilités supplémentaires ou utiliser l'élévation de privilèges pour obtenir un accès supplémentaire au système afin d'installer une porte dérobée ('backdoor') ou un cheval de Troie d'accès à distance qui permet la persistance dans l'environnement. • Ils peuvent également utiliser une certaine forme d'obscurcissement pour dissimuler leur présence et masquer leur activité afin d'éviter d'être détectés et de contrecarrer une enquête. Cela peut inclure l'effacement de fichiers et de métadonnées, l'écrasement de données avec de faux 'timestamps' et des informations trompeuses, ou la modification d'informations critiques pour donner l'impression que l'accès n'a jamais été accordé. • Défendre cette étape signifie que vous devez disposer des outils pour détecter et consigner l'activité d'installation : - Comprendre si les logiciels malveillants nécessitaient ou non des privilèges d'administrateur - Alerter ou bloquer les chemins d'installation courants - Audit du traitement des terminaux pour découvrir les créations de fichiers anormales - Extraire les certificats de tous les exécutables signés - Comprendre le temps de compilation des logiciels malveillants pour déterminer s'il est ancien ou nouveau 7.6 Commandement et contrôle (C2) (command and control) • Généralement, les hôtes compromis communiquent avec un serveur externe pour établir un canal de commande et de contrôle. Une fois la connexion établie, les intrus ont les mains sur le clavier pour accéder à l'environnement cible. • Cette étape est probablement votre dernière meilleure chance de bloquer l'opération si les adversaires ne peuvent pas émettre de commandes, vous pouvez empêcher l'impact. - Découvrez l'infrastructure C2 grâce à l'analyse des logiciels malveillants - Renforcez votre réseau en consolidant le nombre de points de présence internet et exigez des proxys pour tous les types de trafic (HTTP, DNS) 7.7 Actions sur les objectifs• Après avoir parcouru les six phases précédentes de la chaîne d'intrusion, les intrus peuvent prendre des mesures pour atteindre leurs objectifs initiaux. • Il s'agit généralement d'une violation de la confidentialité, de l'intégrité ou de la disponibilité ou d'une combinaison des trois.• Alternativement, les attaquants peuvent uniquement souhaiter accéder à la victime initiale afin de compromettre des systèmes supplémentaires et utiliser un mouvement latéral pour accéder à de nouveaux systèmes plus profonds dans le réseau.

• **Contremesures** - Établir un manuel de réponse aux incidents, y compris un plan d'engagement et de communication de la direction -Détecter l'exfiltration de données, les mouvements latéraux, l'utilisation non autorisée des informations d'identification - Réponse immédiate des analystes à toutes les alertes - Capture de package pour recréer l'activité Effectuer une évaluation des dommages avec des experts en la matière 8- EDR (Endpoint Detection and Response) Solutions sont des solutions de sécurité des 'endpoints' qui surveille en permanence les appareils des utilisateurs finaux pour détecter et répondre aux cybermenaces telles que les ransomwares et les logiciels malveillants une solution EDR est conçue pour surveiller et protéger le point final 9- SIEM (Security information and event management) La gestion des informations et des événements de sécurité est un domaine de la sécurité informatique, où les produits et services logiciels combinent la gestion des informations de sécurité et la gestion des événements de sécurité. Ils fournissent une analyse en temps réel des alertes de sécurité générées par les applications et le matériel réseau. SIEM offre une visibilité de la sécurité sur l'ensemble du réseau d'entreprise 10- Le Risque • **Le fait qu'un événement puisse empêcher de:** - maintenir une situation donnée **et** - de maintenir un objectif dans des conditions fixées **et** - de satisfaire une finalité - pour qu'un tel événement adverse se produise, • se traduit par la notion de potentialité de survenance du risque • L'importance de ses conséquences se traduit par la notion d'impact 10.1 Gestion du risque **10.1.1 Items :** • Dommage physique • Interaction humaine • Problème fonctionnement équipement • Attaques internes/externes • Perte de données • Erreur application **10.1.2 Point de vues :** • Risque pour organisationnelle • Risque pour l'entreprise et les clients • Risque pour les données 10.2- Évaluation et choix - deux principes fondamentaux Principe **du point le plus faible** • Une personne cherchant à pénétrer un système utilisera tous les moyens possibles de pénétration, mais pas nécessairement le plus évident ou celui bénéficiant de la défense la plus solide. **Principe de la protection adéquate (Gestion du risque)** • La durée de la protection doit correspondre à la période pendant laquelle l'importance et la valeur sont présentes, et pas plus . • Le niveau et le coût de la protection doivent correspondre à l'importance et à la valeur de ce qu'on veut protéger: *Choisir la contre-mesure avec le meilleur rapport "qualité" (réduction de risque) vs. "prix" (coût total)* 10.3 Analyse « qualitative » des risques • Méthode principalement utilisée • On utilise le coût potentiel de perte - Voir classification des ressources • On utilise des relations entre les ressources et/ou - Vulnérabilités - Menaces * Contrôles « Prévention ,Correction,Détection »10.4 Énumération des ressources• Ressources : éléments à protéger (hôtes, données, etc.)• En premier lieu, créer la liste des ressources et la mettre à jour (tâche éventuellement difficile) • Responsabilité des ressources : chaque ressource est sous la responsabilité d'une personne identifiée. 10.5 Classification des ressources (vs les objectifs) • **Classification des ressources en fonction de la continuité des** activités - Étendue et pourcentage de perturbation : combien d'éléments, quelle gravité des dommages ? - Impact financier d'un ralentissement ou d'un arrêt • **Classification des ressources en fonction du coût des** réparations 10.6 Analyse « quantitative » des risques • **Analyse de la gravité de la menace (pertes escomptées)** • Le coût de l'attaque en cas de réussite multiplié par la probabilité de réussite de l'attaque • Exprimé par rapport à un intervalle de temps, comme une année • **Valeur de la protection** • La réduction de la gravité de la menace (bénéfice) moins le coût de la contre-mesure • N'investir dans la contre-mesure que si la valeur de la protection est positive. • **Priorité** • Investir en premier dans les dispositifs affichant les plus grandes valeurs de protection 10..7Analyse des risques **Quantitative** • Valeur du item ('asset') • Facteur de perte: représente le pourcentage de perte sur un item si un menace est réalisée • Valeur-total = valeur-item x facteur d'exposition • Perte-par-année = Fréquence de menace par année x valeur-total • Ex. Valeur de la base de données = 1000000$ • Facteur de perte = 30% • Fréquence de menace par année = 0,5 • Perte-par-année = (1000000) x 0,3 x 0,5 = 150000$ • Assurance minimum par 150000$



11.Menaces et formes d'attaques • Menaces non défaites par des canaux sécurisés ou autres techniques de cryptographie ; • **Attaques déni de service :** - Utilisation excessive de ressources afin de les rendre indisponibles aux autres utilisateurs • **Chevaux de Troie (Trojan horses) et autres virus :** - Virus peut entrer dans un ordinateur seulement si un programme est importé ; - Les usagers ont besoin de nouveaux programmes (Nouvelle installation de logiciels, code mobile téléchargé dynamiquement par des logiciels existant, exécution accidentelle de programmes transmis clandestinement) ; - **Défenses** : authentification de code (code signé), validation de code (vérification de type, démonstration), confinement (sandboxing). • **Espionnage (*Eavesdropping*) :** - Obtenir une information secrète ou privée • **Personnification (*Masquerading*) :** - réception ou envoi de messages en utilisant l'identité d'un autr • **Falsification (*Tampering*) :** - Modification non autorisée d'information en transite. • **Retransmission (*Replaying*) :** - Stockage et retransmission à une date ultérieure d'un message. • **Déni de service (*Denial of service*) :** -innonder un canal ou toute autre ressource, niant l'accès à d'autres

Exam Final Automne 2022 Question 1: D'après les informations communiquées dans cette architecture, chaque succursale possède son propre serveur, cependant la base de données est centralisée et elle est localisée au centre de données du siège social. D'après les informations communiquées dans l'énoncé, on comprend que l'architecture proposée est une architecture **(Réseau en étoile),** où le hub qui est le siège social est connecté aux différentes villes à travers des liaisons câblées ou sans fil. Chaque ville possède de plus de cette liaison avec le hub, une connexion vers Internet et d'autres connexions vers les différentes succursales. Ci-dessous l'architecture du siège social et ses liaisons avec les différentes villes avec les spécifications suivantes: - Le siège qui est le point central de l'architecture doit avoir une connexion redondante vers Internet à travers deux ISP différents et en utilisant deux technologies d'accès différentes, par exemple ils peuvent utiliser la fibre optique pour la connexion principale et une connexion backup avec la technologie faisceaux hertzien ou LTE/ 5G. -Comme mentionné dans l'énoncé, le siège a une architecture trois tiers, on peut distinguer sur le diagramme les trois couches (Accès, Distribution et Coeur), - L'utilisation d'un pare-feu combiné avec un IPS est nécessaire pour la protection des services qui sont dans la DMZ. -La zone DMZ comprend les éléments suivants : le serveur Web, le serveur mail, Email Security pour la protection contre les attaques liées au serveur mail, le serveur DNS et DHCP et un serveur d'authentification lié à l'application Web (transaction bancaire). - La zone Protégé comprend les éléments suivants: le serveur de base de données,pour la protection contre les attaques liées au serveur de donnés, -L'application Web a une architecture 3 tiers, il est nécessaire pour assurer un niveau de sécurité élevé, d'ajouter un autre pare-feu entre le serveur web et le serveur d'application. On a ajouté également un Web Security Appliance pour bloquer les connexions malicieuses. -Il est nécessaire d'ajouter une autre couche de protection (pare-feu et IPS) pour protéger le réseau interne de la banque au cas où le serveur d'application sera compromis. ◆ **- On a divisé le réseau interne du siège en trois blocs:** ➢ WAN : Une liaison VPN site to site sera déployé pour connecter chaque ville au siège. Un pare-feu est obligatoire à l'entrée du siège et à chaque sortie d'une ville. Le VPN est limité à l'extérieur du pare-feu pour rendre l'inspection de ce dernier plus facile (trafic non crypté) ➢ Data Center : C'est la partie de l'architecture la plus sensible, c'est pour cette raison qu'on a ajouté un autre pare feu et IPS pour une protection même contre les attaques internes. Cette partie comprend plusieurs serveurs : le serveur d'authentification de la banque combiné avec l'Active Directory, le serveur de base de données, le serveur des fichiers, surveillance … •Campus du siège :C'est le réseau d'accès du sucursal , il regroupe les différentes installations réseaux dans les différents sites du siège (commutateurs, points d'accès …) ainsi qu'un NAC pour l'application de la politique de sécurité, un contrôleur WIFI et un Web Security pour filtrer les sites web malveillants. Afin de répondre au besoin de l'entreprise en termes de BYOD, on a décidé d'implémenter la solution Cisco ISE qui va nous permettre de contrôler les appareils des utilisateurs, vérifier leurs conformités aux politiques de sécurité appliquées et prendre les décision adéquates pour protéger le réseau. Par exemple, pour un client qui utilise son propre laptop qui n'a pas été mise à jour et qui n'a aucun antivirus installé, Cisco ISE peut mettre cet utilisateur dans un VLAN isolé et lui donner un accès restreint aux ressources de l'entreprise (accès internet seulement par exemple). -Pour assurer une haute disponibilité et une tolérance au faute, tous les éléments de l'architecture réseau doivent être redondants. Sur le diagramme ci-dessous, j'ai essayé de montrer cette redondance au niveau des liens et des commutateurs modulaires mais il reste quelques SPOF (Single Point Of Failure) que j'ai gardé pour simplifier l'architecture. -Dans un réseau redondant il est nécessaire d'utiliser des technologies comme l'agrégation de lien (Etherchannel), le protocole de redondance HSRP et le protocole Spanning Tree (STP) pour bénéficier de toutes les ressources disponibles. -Dans les succursale , il est nécessaire d'appliquer la solution NAT avec un adressage privé adéquat et des protocoles réseaux sécurisés par exemple: OSPF pour le routage, des VLANs par secteur et par technologie (VLAN WIFI, VLAN MANAGEMENT, …) pour limiter les domaines de broadcast, NTP pour la synchronisation du temps, SNMP pour la supervision… -Il est obligatoire d'utiliser HTTPS/TLS au niveau du serveur Web. Et le protocole SSH pour le management des équipements réseau à distance. **Architecture ville et succursale:** D'après l'énoncé, chaque ville regroupe plusieurs succursales et possède un accès à Internet et un serveur avec BD centralisé sur le siège social . C'est ce que nous avons essayé de montrer dans le diagramme ci-dessous avec une seule succursale. **But de architecture 3 tiers :** ●Un réseau doit être évolutif, résilient et facile à gérer, ● Pour mettre en oeuvre ces trois caractéristiques, vous devez avoir clairement défini le rôle de chaque appareil dans le réseau. Cisco recommande de définir trois rôles (couches, niveaux) : accès, distribution et noyau, ●Les commutateurs de couche d'accès connectent physiquement les utilisateurs et appliquent les politiques d'accès au réseau, ●Les commutateurs de distribution connectent plusieurs commutateurs d'accès au coeur et appliquent des politiques telles que le pare-feu ou le routage des politiques, ●Les commutateurs de la couche centrale acheminent simplement le trafic entre les commutateurs de distribution, le plus rapidement possible. Vous ne devriez appliquer aucune politique là-bas, ●Lorsque vous avez des contraintes de conception, vous pouvez réduire ensemble la couche de distribution et la couche principale, ●Cisco recommande de préférer les liaisons de couche 3 aux liaisons de couche 2 lors de la connexion des couches ensemble dans la mesure du possible **une architecture réseau détaillée de LA MODE**

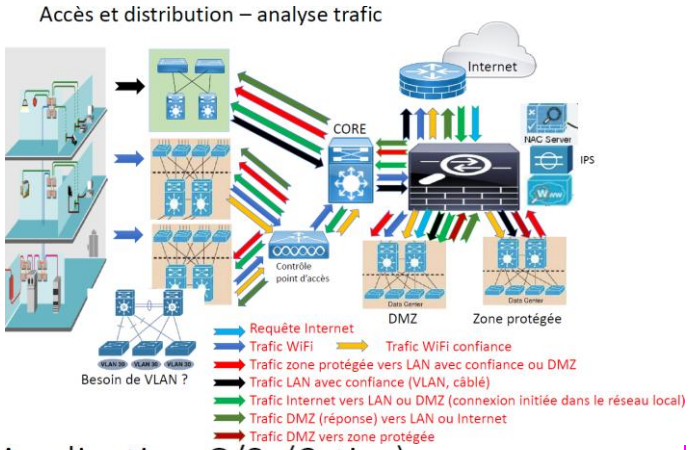


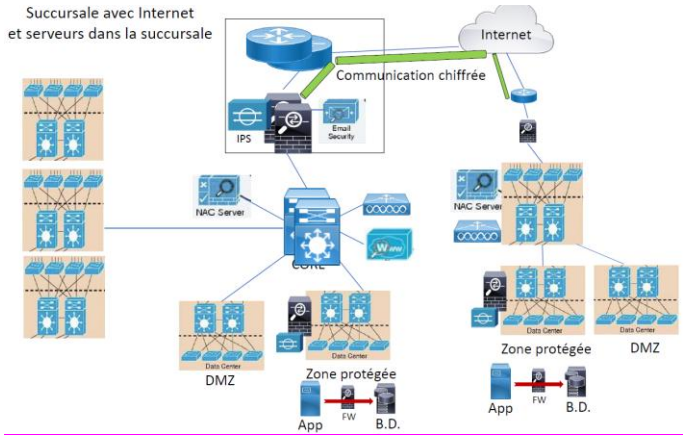
Question 2: Par ailleurs, un réseau VPN est beaucoup plus rapide qu'un réseau Tor parce que vous passez directement par un seul serveur. De plus, les VPN sont disponibles gratuitement et sont généralement financés grâce aux publicités. **les avantages VPN Une protection contre les attaques de hackers:** Lorsqu'il surfe sur Internet, chaque utilisateur laisse des « traces » derrière lui. La trace la plus évidente est son adresse IP. Cette dernière permet aux hackers d'attaquer directement votre ordinateur avec pour éventuelle conséquence un vol de données ou une usurpation d'identité ! Dans le pire des cas, cette attaque peut porter sur des données bancaires particulièrement sensibles et entraîner des dommages financiers considérables. Au contraire, toute personne qui surfe sur Internet par l'intermédiaire d'un VPN dissimule son adresse IP et se rend ainsi inattaquable ! **.Un anonymat complet sur Internet** L'adresse IP permet de déterminer l'identité d'un utilisateur. Si vous souhaitez rester anonyme, il est conseillé de surfer sur Internet en passant par un serveur VPN afin d'effacer vos traces. De cette manière, vous dissimulez également votre identité. **Les inconvénients du VPN** Le VPN étant relié à une entreprise, cette dernière peut être interdite dans certains pays. La Russie par exemple a interdit des entreprises de VPN sur son territoire. De façon générale, il n'existe pas beaucoup d'informations sur les éditeurs de VPN. De ce fait, il faudra avoir une totale confiance à la société éditrice du VPN, car tout votre trafic passe par ses serveurs. Vos données pourraient être utilisées sans votre accord. De même, vous devrez débourser une somme un peu élevée par mois pour accéder à plus de fonctionnalités et éliminer les publicités. Le réseau Tor pour accéder au darknet La dénomination « The Onion Routeur » fait référence à sa capacité d'acheminement de vos données à partir de couches de sécurité différentes, jusqu'à leur destination finale. En général, le réseau Tor protège votre ordinateur contre l'analyse de trafic. Cela permet de ne pas révéler votre identité personnelle et le lieu où vous vous trouvez au moment de votre connexion sur internet. L'objectif que vise ce réseau est de pouvoir éviter les censures internet établies dans certains pays. Dans le même temps, il se charge de surveiller vos données à différents points entre votre ordinateur et les sites web que vous consultez. C'est aussi le moyen le plus connu d'accéder au darknet (dit aussi deepweb). Le fonctionnement du réseau Tor est pratiquement le même que celui du serveur VPN. La différence réside principalement dans le fait que votre trafic ne passera pas par un seul serveur, mais vous ferez trois sauts minimum avant d'atteindre la page web que vous souhaitez consulter. Concrètement, vous passerez par trois relais : le garde à l'entrée, le relai du milieu et le noeud de sortie. Ces relais permettent de protéger votre identité, car chaque noeud ne montrera que l'adresse IP du noeud précédent et celle du noeud suivant. Au cours de leur transmission, vos données seront également chiffrées. Il sera donc impossible pour un serveur de connaître la provenance et la destination finale de vos données. Toutefois, à la sortie du dernier noeud de protection, vos données seront complètement déchiffrées. Il vous faudra alors une connexion HTTPS pour que vos informations ne soient pas totalement exposées à la personne qui procède à l'exécution du noeud de sortie. **Les avantages du réseau Thor** Le principal avantage de ce réseau est que votre adresse personnelle ne sera pas révélée aux sites et pages web que vous consulterez. De même, l'utilisation du réseau et du logiciel est totalement gratuite. Grâce au Tor, vous pourrez accéder à des contenus bloqués par géo-restriction. De plus, ce réseau est distribué et exécuté par des volontaires, ce qui empêche un gouvernement ou une quelconque organisation de réussir à le fermer. C'est le meilleur choix pour bénéficier de l'anonymat le plus complet possible sur internet. En comparaison avec le VPN, le Tor est totalement gratuit et ne requiert aucun abonnement. De plus, il est plus sécurisé, car ne disposant pas d'une seule entité de protection. L'application ne permet aucun log d'activité. Seul un administrateur a le pouvoir de voir les connexions sur son serveur ThOR. **Les inconvénients du réseau Thor** Par rapport au VPN, Tor s'avère être très lent. En effet, le fait que les données passent par trois serveurs avant d'atteindre leur destination finale ralentit considérablement la connexion. C'est alors un mauvais choix si vous désirez regarder des films, séries ou autres contenus HD en streaming. De plus, le réseau Tor est uniquement accessible via un navigateur internet défini dont l'accès TOR est intégré. Si vous utilisez un navigateur incompatible, vous ne serez pas protégé par le réseau. En outre, le noeud de sortie peut être installé par n'importe qui, ce qui induit que celui qui l'exécute pourra visualiser votre trafic internet et même le pirater. En effet, la maintenance des noeuds de Tor ne nécessite aucune responsabilité ni aucun financement direct. Question 3: Il est possible de collecter toute cette information ('Open Source Intelligence –OSINT' ou renseignements de sources ouvertes) grâce aux différents outils disponibles sur Internet qui cherchent des informations non classifiées qui ont été délibérément découvertes, discriminées, distillées et diffusées à un public choisi afin de répondre à une question spécifique, ou d'utiliser des outillages pour récolter le maximum possible d'information Collecte d'information 'Google hacking, Collecte d'information d'utilisation de Shodan collecte d'information à travers les réseaux sociaux ..etc**. L'usurpation d'identité est en hausse. Les réseaux sociaux ne sont pas étrangers au phénomène pour diminuer ou réduire la collecte de données personnelles sur les réseaux sociaux afin d'éviter le vol d'identité on peut commencer par:** ●Avant de nous connecter, faut d'abord protéger notre ordinateur, notre téléphone intelligent et tablette avec un logiciel antivirus, un programme antiespion et un pare-feu obtenu chez un fournisseur sérieux. Il est important que nos logiciels soient actifs et à jour, particulièrement nos logiciels de sécurité. ●Durant la navigation, il faut toujours aux aguets avant d'ouvrir un fichier joint ou de cliquer sur un hyperlien; vous pourriez être victime d'hameçonnage, d'un logiciel espion ou d'un virus informatique. Toute transaction ou communication demande aussi de la prudence. Même la messagerie instantanée et les réseaux sociaux représentent un risque. ●Si on est obligé de divulguer des informations personnelles, n'interagissez qu'avec des fournisseurs fiables. Lisez les politiques de confidentialité afin de comprendre pourquoi nos données personnelles sont recueillies, mais également savoir l'utilisation qui en sera faite et la façon dont elles sont protégées. ●Éviter de faire des transactions comme des achats en ligne ou la consultation de notre compte bancaire à partir d'un point d'accès Internet sans fil public. ●Lors de transactions financières en ligne, l'environnement doit être sécurisé. Notre navigateur devrait afficher l'icône d'un cadenas fermé ou d'une clé dès qu'on vous demande d'indiquer notre numéro de carte de crédit. Si ce n'est pas le cas, ne faut pas fournir de données sensibles; il pourrait s'agir d'un site frauduleux. ●Favoriser les technologies qui protègent notre sécurité et vie privée. La signature numérique et le chiffrement permettent de mieux vous protéger. Toutefois. ●Il faut également que la consultation ou la modification d'informations sur nos différents comptes en ligne exige un mot de passe différent, de préférence d'utiliser la double authentification. ●Chaque mot de passe devrait être unique, surtout si les combinaisons de chiffres et de lettres servent à accéder à nos données financières. ●Changez nos mots de passe fréquemment et évitez de les inscrire sur un papier glissé dans votre portefeuille. ●Après la navigation sur des sites sécurisés, il faut vider la mémoire du cache de votre appareil. Ainsi, les adresses Internet seront supprimées de votre ordinateur. Il est également conseillé de fermer son ordinateur après l'utilisation. ●Pensez à verrouiller nos appareils mobiles après quelques minutes d'inactivité. ●Intégrez un mot de passe ou un processus d'accès. Si on perd notre appareil, il faut directement communiquer avec notre fournisseur pour le localiser et supprimer les données à distance. **●Pseudonymiser** : l'identification réelle de l'utilisateur est remplacée par un autre identifiant protégeant son identité (Anonymiser : retirer tout élément d'identification de l'utilisateur). ●Ne jamais faire confiance au fournisseur de Cloud pour la sécurité des données, **Il faudrait chiffrer les informations avant même leur envoi sur le Cloud. 2eme réponse pour la Question 3 : 1.Sensibilisation et Éducation**: Informez les utilisateurs, en particulier les jeunes, sur les risques liés à la divulgation d'informations personnelles en ligne. Mettez en place des programmes éducatifs pour sensibiliser les gens aux techniques de collecte d'informations et aux conséquences du vol d'identité. **2.Paramètres de Confidentialité:** Utilisez les paramètres de confidentialité des réseaux sociaux pour restreindre l'accès à vos informations personnelles. Limitez la visibilité de votre profil et de vos publications uniquement à vos amis ou à des personnes de confiance. **3.Réduisez les Informations Sensibles:** Limitez la quantité d'informations sensibles que vous partagez en ligne. Évitez de publier des détails tels que votre adresse, numéro de téléphone, et informations financières. **4.Vérification des Paramètres par Défaut:** Assurez-vous de vérifier et de personnaliser les paramètres de confidentialité dès la création de votre compte sur un réseau social. Les paramètres par défaut peuvent souvent être trop permissifs. **5.Gestion des Amis et des Contacts:** Soyez sélectif dans le choix de vos amis ou contacts en ligne. Évitez d'accepter des demandes d'amis de personnes que vous ne connaissez pas personnellement. **6.Utilisation Minimale d'Informations Réelles:** Si possible, utilisez des informations minimales ou fictives dans les sections de profil qui ne nécessitent pas de données réelles, comme la date de naissance.**7.Surveillance de l'Activité en Ligne:** Surveillez régulièrement votre activité en ligne. Supprimez ou limitez la visibilité des informations que vous ne souhaitez plus partager. **8.Utilisation d'un Alias:** Utilisez un pseudonyme ou un alias plutôt que votre nom réel, en particulier si cela est possible sans violer les conditions d'utilisation du réseau social. **9.Réflexion Avant de Partager:** Avant de partager une information, réfléchissez aux implications potentielles. Posez-vous la question de savoir si cette information peut être utilisée contre vous. **10.Mises à Jour Régulières:** Assurez-vous que vos informations de profil sont à jour et que les paramètres de confidentialité sont adaptés aux changements dans votre vie. **La mise en œuvre de ces mesures permet de créer une stratégie globale visant à réduire la quantité d'informations personnelles accessibles en ligne, contribuant ainsi à la protection contre le vol d'identité. La sensibilisation et l'éducation restent des éléments clés pour encourager les utilisateurs à adopter ces bonnes pratiques.** Question 4: Les attaquants ont tendance à créer de faux sites Web qui sont pratiquement identiques aux sites légitimes. Une fois que vous avez entré vos informations d'identification sur eux, ils les collectent et en tirent parti. » Dans la même présentation, les étudiants ont indiqué certaines mesures préventives 1:Supprimez les courriels suspects. 2:Utilisez des filtres anti-spam. 3:Changez régulièrement les mots de passe des comptes et n'utilisez jamais le même mot de passe pour chaque compte. 4:Évitez d'utiliser les réseaux publics lorsque vous accédez à des informations sensibles telles que des documents d'identification et des plateformes bancaires. 5: S'il y a des liens hypertexte, passez la souris sur l'URL, le lien peut se diriger vers un site complètement différent. Faites attention à l'orthographe de l'URL, de petits changements dans un lien valide peuvent passer inaperçus. Exemple : facebook.com » vs « fasebook.com ».6: Configurez les paramètres de navigation pour éviter l'ouverture de sites Web trompeurs. **On va analyser chacune de ces mesures pour les utilisateurs qui connaissent pas vraiment informatique et dire quels sont les avantages et les inconvénients de ces mesures vu précédemment chacun avec son numéro indiqué en haut:**

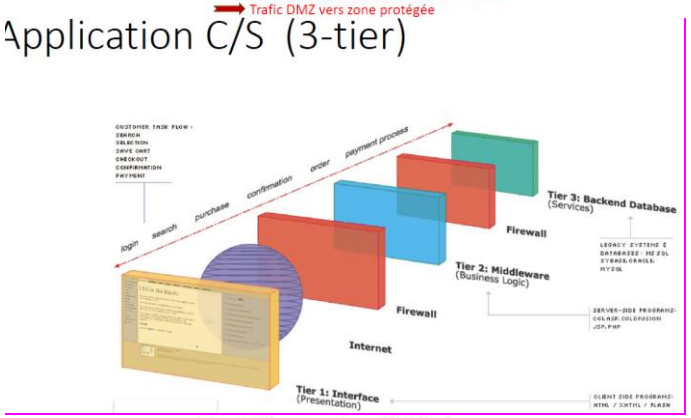
Avantages	Inconvénients
1: éviter les courriels frauduleux et minimiser leurs accès	1: ça se peut qu'il ne soit pas un courriel frauduleux et donc on va bloquer ce courriel pour rien et donc ignorance de ce qu'il contient pour information
2: filtrage des courriels connue comme spam et avoir une analyse sur nos courriels afin de faciliter l'accès	2: bloqué dès courriels légitimes par erreur ou en pensant que c'est une menace
3: Chaque mot de passe devrait être unique, surtout si les combinaisons de chiffres et de lettres servent à accéder à nos données personnels qui vont être difficiles à craquer	3: risque de perdre ou d'oublier le mot de passe surtout si on utilise différents mots de passe difficiles à les retenirs.
4: Évitez d'utiliser les réseaux publics va nous permettre de naviguer sur des sites sécurisées et éviter des attaques de Phishing comme MITM ou autre qui permets d'intercepter facilement le trafic qui transit sur le web	4:besoin de se connecter surtout si on pas pas autre accès internet, et surtout que souvent les endroits qu'on fréquent on toujours des réseau public et pas forcément ses liens sont des menaces par exemple les réseau public de notre institution financières
5: utilisation du https nous permettre d'accéder en tout sécurité car les flux de données qui transit sur ce site sont chiffré par SSL , aussi la vigilance nous permettre d'éviter les sites frauduleuses qui sont utilisés pour usurpé le site de confiance	5:Des algorithmes de chiffrement lourd peuvent être utilisés pour protéger les communications et données donc vont alourdir la connexion et ugmenté la latence sur le réseau
6: Exemple supprimer les caches et les cookies qui contiennent des informations -utiliser un moteur de recherche de confiance -supprimer l'agent utilisateur du navigateur qui contient l'information sur le web et la version et l'appareil utilisé -ajouter dans les navigateurs juste les sites de confiance qu'on fréquente souvent	6: peut rendre le surf sur internet un peu difficile car -changer la manière d'accéder sur notre navigateur peut être désagréable surtout pour des gens qui ne connaissent pas ses préventif de sécurité

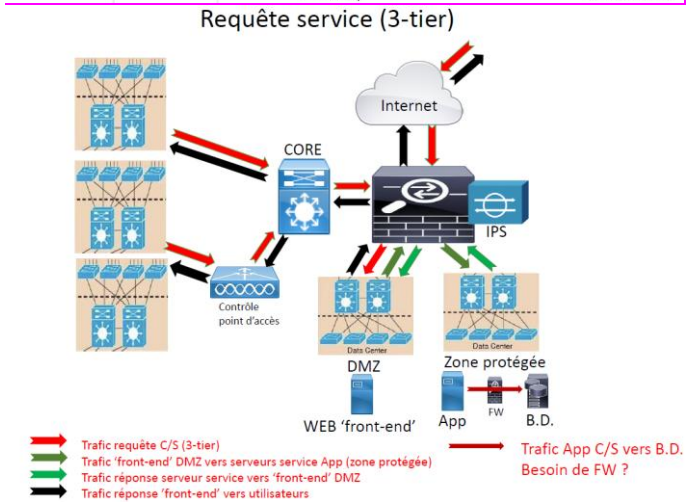
Le nombre de cas des utilisateurs qui sont victimes pour de l'hameçonnage continue à augmenter. puisque La protection de la vie privée : -N'est pas un concept absolu !, -Dépend de la tolérance de l'utilisateur concerné, -Dépend souvent de la législation du pays, -Peut être en balance avec la sécurité de la société (caméras par exemple), -Souvent en opposition avec les business models d'Internet, -la sécurité S'impose dans de nombreux domaines :Domicile, Voiture, Santé, Transports collectifs, Bâtiments, Tourisme, -Les protocoles de communication et de sécurité doivent être adaptés aux capacités -ignorance sur les mesures préventif de sécurité surtout pour les personnes âgés génération X, --Objectif d'IoT : permettre la réutilisation et le partage des données entre systèmes, -L'anonymisation peut être une possibilité pour protéger la vie privée tout en permettant l'échange, -Compromis à trouver entre vie privée et authentification d'un capteur/utilisateur, -Compromis entre la sécurité de la société et le respect de la vie privée, -Importance du contrôle d'accès à la fois des utilisateurs et des applications, -manque de prévoyance pour les utilisateurs avec peu d'expérience dans TI Conclusion Recoupement des données peut être un véritable Danger pour la vie privée car des informations non sensibles par elle-même peuvent le devenir une fois regroupées, Il faudrait chiffrer les informations avant même leur envoi sur le Cloud, ou utiliser Anonymiser nos donnés personnels surtout dans les réseau sociaux Attention au réseautage social. Notre profil devrait être exempt de numéro de téléphone, d'adresse et même d'une date de naissance, car tous ces renseignements peuvent servir à voler Notre identité. N'acceptez pas n'importe quel ami, car derrière une identité virtuelle pourrait se cacher un fraudeur. **Les présentations:** craquage et sécurité de mots passe La présentation a couvert divers aspects de la sécurité des mots de passe, débutant par une exploration du Dark Web, une partie cachée de l'internet souvent associée à des activités illicites. Les mécanismes de protection de l'anonymat sur le réseau Tor ont été expliqués, mettant en lumière l'acheminement du trafic via des relais et l'utilisation de .onion pour les sites du Dark Web. La partie consacrée à l'obtention des mots de passe a mis en avant des méthodes d'exploitation, telles que l'injection NoSQL, avec des démonstrations pratiques à l'appui. L'outil John The Ripper a été présenté comme une solution puissante pour évaluer la robustesse des mots de passe, incluant des modes comme le "Single crack mode" et le "Wordlist mode". La démonstration a illustré le processus de recherche et de craquage de mots de passe par force brute. En matière de protection, des recommandations ont été fournies, mettant en avant l'utilisation de gestionnaires de mots de passe, l'authentification à deux facteurs (MFA), et l'exploration de protocoles comme OAuth. La conclusion a souligné l'importance de ces mesures de protection, offrant aux participants la possibilité de poser des questions pour une compréhension approfondie. vulnérabilité sudoedit La présentation a abordé une vulnérabilité majeure de sécurité, identifiée sous le code CVE-2023-22809, concernant le commandeur "sudoedit" sous Linux. Les intervenants ont commencé par une introduction générale sur Linux, soulignant sa popularité, sa gratuité, et sa grande communauté. Ils ont également fourni des statistiques sur les vulnérabilités par système d'exploitation entre 2015 et 2021. Ensuite, la présentation s'est concentrée sur l'explication de "sudo" et "sudoedit", mettant en lumière leur utilité dans la gestion des accès privilégiés sur les systèmes Linux. La vulnérabilité CVE-2023-22809 a été détaillée avec une chronologie de sa découverte, de la publication du correctif, jusqu'à sa divulgation publique. Les versions affectées ont été spécifiées, et les préalables pour exploiter la vulnérabilité ont été discutés, avec un score CVSSv3 de 7,8. La partie exploitation a illustré comment un attaquant pourrait abuser de la vulnérabilité pour élever ses privilèges, en utilisant des extraits de code pertinents. Une démonstration pratique a également été présentée. La réaction à la vulnérabilité a été rapide, avec un correctif publié 13 jours après sa découverte. Les intervenants ont souligné l'importance de la divulgation responsable des vulnérabilités. Des mesures correctives, telles que la mise à jour de la version de "sudo" et l'ajout de configurations spécifiques au fichier "sudoers", ont été recommandées. En conclusion, la présentation a mis en évidence la nécessité d'une surveillance continue des systèmes, la découverte proactive des vulnérabilités par les entreprises, et a souligné que bien que l'exploitation soit potentiellement dangereuse, aucune attaque pratique n'a été répertoriée. Vulnérabilité wordpress La présentation a traité de la vulnérabilité CVE-2023-2636 affectant le plugin WordPress AN_GradeBook version 5.0.1, une faille de type SQL injection découverte par Lukas Kinneberg en juillet 2023. La vulnérabilité a été rendue publique, entraînant la non-disponibilité du plugin. Le score CVSS 3.x de 8.8 a souligné son impact significatif sur l'intégrité, la confidentialité et la disponibilité, avec une faible complexité d'attaque et peu de privilèges requis. La présentation a expliqué le contexte de l'attaque SQL injection, démontrant la possibilité de manipuler les requêtes en utilisant des mots de passe spécifiques, comme ' OR 1=1', ou en exploitant le caractère #. Les détails techniques ont mis en évidence la vulnérabilité dans l'URL spécifique du plugin, illustrant comment un attaquant pourrait exfiltrer des données de la base de données WordPress. Une démonstration en direct a été effectuée avec l'utilisation de SQLMAP, un programme automatisant les tests d'injection SQL, montrant comment il peut déterminer le schéma de base de données, extraire des données des tables et même lancer un shell à distance sur le serveur de base de données. Les impacts potentiels de cette vulnérabilité ont été énumérés, notamment l'accès non autorisé aux données, la modification des données, la divulgation d'informations sensibles, l'exécution de commandes système, les attaques par déni de service, l'escalade de privilèges, les injections de code malveillant et la perte de confiance des utilisateurs. En ce qui concerne les solutions et les remédiations, la présentation a recommandé l'utilisation de requêtes paramétrées, la validation et la sanitisation des entrées, ainsi que des audits de sécurité et des revues de code. Les mises à jour régulières des cadriciels ont été soulignées, tout comme le principe de moindres privilèges, l'évitement d'ajouter des plugins développés par des inconnus, et l'utilisation d'outils d'analyse automatique de code et comportementale (SAST, DAST). Vulnérabilité STP La présentation se concentrait sur la sécurité des réseaux locaux, en mettant en lumière le

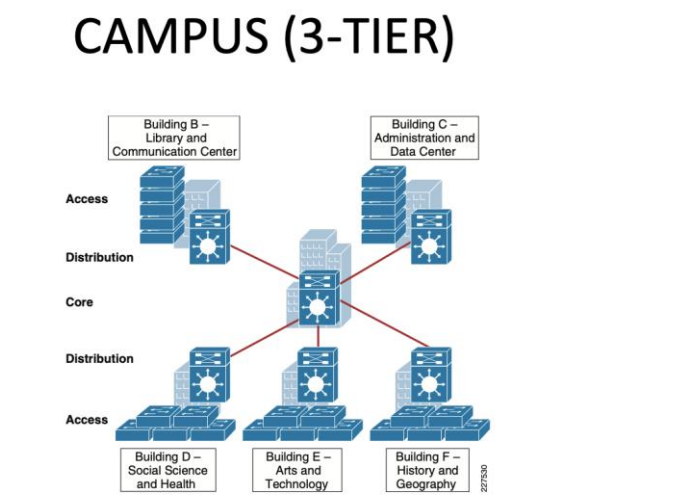
protocole Spanning-Tree (STP) et ses enjeux. Elle a souligné l'importance cruciale de la disponibilité dans la sécurité de l'information, avec une attention particulière portée à la redondance des liens physiques entre les commutateurs. Le protocole STP, présenté conformément à la norme IEEE 802.1D, a été exposé comme une solution pour éviter les boucles dans les réseaux locaux. Cependant, la présentation a également mis en avant les inconvénients opérationnels de STP, tels que l'utilisation non optimale de la bande passante. Les vulnérabilités de STP ont été discutées, notamment l'absence de chiffrement et d'authentification des Bridge Protocol Data Units (BPDU), exposant les réseaux à des risques de Man-In-The-Middle et de déni de service. Pour atténuer ces vulnérabilités, des mesures de protection ont été proposées, allant de la désactivation de certaines fonctionnalités à l'utilisation de gardiens de ports pour prévenir les attaques. La présentation s'est conclue par une démonstration pratique d'exploitation d'une vulnérabilité de STP, soulignant ainsi l'importance de comprendre et de sécuriser ce protocole pour garantir la disponibilité des réseaux locaux. WEBUI-Aria Vulnérabilité La présentation portait sur la vulnérabilité CVE-2023-39141 découverte en juillet-août 2023 dans le projet WebUI-Aria2, une interface utilisateur graphique web pour Aria2, un utilitaire de téléchargement en ligne. Identifiée comme une vulnérabilité de type "Path Traversal", elle permet une attaque de traversée de chemin, offrant un accès non autorisé au répertoire www, incluant des fichiers sensibles tels que /etc/passwd et /etc/host. L'exploitation de cette faille était démontrée à travers l'utilisation de l'outil nuclei. La présentation mettait en avant les avantages de WebUI-Aria2, notamment les téléchargements en parallèle et la gestion à distance, soulignant l'importance de la sécurité dans de telles interfaces. Pour se protéger contre cette vulnérabilité, la présentation suggérait des mesures telles que des mises à jour régulières du logiciel, le changement vers une alternative plus sécurisée, et la mise en place de protections d'accès à la page. En conclusion, la présentation mettait en lumière l'importance de la vigilance en matière de sécurité, soulignant la nécessité de prendre des mesures proactives pour protéger les systèmes contre de telles vulnérabilités et assurer la sécurité des données. http rapid reset La présentation portait sur la vulnérabilité "HTTP/2 Rapid Reset", exposée par Léonard Galibois, Matis Grégoire et Olivier Duguay. Cette vulnérabilité concerne une attaque DDoS exploitant les fonctionnalités de HTTP/2, atteignant jusqu'à 398 millions de requêtes par seconde. En exploitant le stream multiplexing de HTTP/2, l'attaque génère une asymétrie de charge entre le client et le serveur en envoyant un grand nombre de requêtes RST_STREAM, perturbant ainsi le traitement des requêtes légitimes. La démonstration mettait en lumière l'efficacité de l'attaque et son impact sur le service, entraînant une interruption du traitement des requêtes et pouvant provoquer des plantages du serveur. Pour se protéger, la présentation suggérait des améliorations du traitement des requêtes, la surveillance du taux d'annulation des streams, l'utilisation de l'IP Jailing comme mesure temporaire, et la distribution de la logique de détection pour contrer l'attaque. En conclusion, l'attaque HTTP/2 Rapid Reset se révèle très efficace, nécessitant des contre-mesures proactives telles que l'amélioration de la capacité de traitement et la surveillance constante pour maintenir la disponibilité du service. Apache http La présentation portait sur la vulnérabilité CVE-2021-41773 du serveur Apache HTTP 2.4.49, exposée par Oida Kon Fataki, Benoit Dambrine, et Ndeye Penda Ndiongue. La vulnérabilité, découverte le 4 octobre 2021, impliquait une traversée de chemin et une divulgation de fichiers dans les versions 2.4.49 et 2.4.50, pouvant conduire à une exécution de code à distance. La configuration non par défaut du serveur était nécessaire pour exploiter ces vulnérabilités. La présentation a expliqué que la traversée de chemin permettait un accès non autorisé à des fichiers en dehors du répertoire racine du site web, tandis que l'exécution de code à distance permettait l'exécution de code arbitraire sur le serveur. Une démonstration a été réalisée, illustrant la création d'un shell inversé pour établir un contrôle sur le serveur compromis. Les solutions pour remédier à la vulnérabilité impliquaient la mise à jour vers la version corrigée 2.4.51 publiée le 7 octobre 2021. Le CISA (cert américain) avait émis une alerte sur les risques d'exploitation rapide de cette vulnérabilité. La présentation a également mentionné d'autres vulnérabilités modérées, telles que le déréférencement de pointeur nul dans le fuzzing h2 (CVE-2021-41524). En résumé, la vulnérabilité CVE-2021-41773 dans Apache HTTP Server 2.4.49 présentait des risques sérieux de traversée de chemin et d'exécution de code à distance, nécessitant une mise à jour immédiate vers la version corrigée 2.4.51 pour assurer la sécurité du serveur. DDoS La présentation sur les attaques par Déni de Service Distribué (DDoS), menée par Ikram Kohil, Johnatan Gao, et Bintou Seni, a fourni une vue exhaustive des différents types d'attaques, à savoir sur la couche Application, Protocole, et Volumétrique. Les démonstrations pratiques ont mis en lumière les risques concrets associés à ces attaques, utilisant des outils tels que MHDDoS. Les stratégies de mitigation ont été élaborées en quatre étapes clés, de la détection à l'adaptation, mettant l'accent sur l'importance d'une réponse intelligente pour gérer le trafic malveillant. La conclusion a souligné l'importance de la mise à l'échelle, de la flexibilité et de la fiabilité des services pour une protection efficace contre les attaques DDoS. L'interaction avec le public au cours de la session de questions a permis d'approfondir la compréhension des participants sur les aspects techniques et stratégiques de la défense contre ces attaques potentiellement dévastatrices. Attaques par phishing La présentation sur l'attaque par phishing, dirigée par Bilal Mersali et François Mourier, a abordé de manière approfondie les mécanismes de cette menace, mettant en lumière une démonstration pratique de l'attaque, combinant l'Open Source Intelligence (OSINT) et le phishing. La vulnérabilité WordPress CVE-2023-5561 a été expliquée en détail, illustrant comment les attaquants peuvent exploiter cette faille pour obtenir des informations sensibles. La démonstration avec l'outil Gophish a montré comment créer une campagne d'hameçonnage, soulignant l'importance de la sensibilisation et de la vigilance face aux techniques sophistiquées de spear phishing. Les contre-mesures proposées comprennent la mise à jour régulière des sites WordPress, la sécurisation de l'API REST, l'utilisation de filtres anti-phishing, et la reconfiguration des serveurs SMTP pour prévenir l'usurpation d'adresses électroniques. En conclusion, la présentation a souligné la redoutable efficacité du spear phishing, rappelant l'importance de la sensibilisation et de la vigilance individuelle, en complément des mesures technologiques. Protocole SSH La présentation portant sur la vulnérabilité CVE-2023-38408 dans le protocole SSH met en lumière une récente découverte concernant une exécution de code à distance dans OpenSSH's forwarded ssh-agent. Cette vulnérabilité a été divulguée anonymement via le forum Full Disclosure sur SecLists.org, après une communication préalable avec OpenSSH. L'objectif de l'attaque était d'obtenir un accès à un compte utilisateur à partir d'un serveur malveillant distant. La vulnérabilité touche l'outil OpenSSH, exploitant une faille dans le protocole SSH et impliquant l'utilisation de librairies partagées. Bien que récente, aucune preuve d'exploitation passée n'a été identifiée. OpenSSH, utilisé par environ 46 000 systèmes, est une suite logicielle open-source pour des communications sécurisées. La démonstration de l'attaque a illustré les étapes d'un attaquant exploitant le forwarding ssh-agent pour exécuter un code distant sur la machine de la victime. Les contre-mesures recommandées comprennent la mise à jour vers la dernière version d'OpenSSH, la désactivation du forwarding, et la restriction de l'accès physique au serveur. En conclusion, bien que la vulnérabilité ait été résolue dans la dernière version, elle reste exploitable chez de nombreux utilisateurs qui n'ont pas effectué la mise à jour. Certains cas spécifiques doivent être réunis pour une exploitation réussie, mais la vigilance demeure essentielle. Comment faire pour diminuer ou réduire la collecte de données personnelles sur les réseaux sociaux afin d'éviter le vol d'identité ? Justifiez clairement votre réponse.1) Configurer les paramètres de confidentialité 2) Soyez prudent avec les informations partagées 3) Utiliser des pseudonymes ou des noms d'utilisateur non identifiants 4) Activer l'authentification à deux facteurs











- Assurer la connectivité de et vers l'Internet
- Renfoncer les politiques de sécurité pour le trafic entre le DMZ, le réseau intérieur et l'extérieur
- Cacher les adresses de l'intérieur en utilisant NAT
- Assurer l'accès de l'intérieur vers Internet
- Assurer l'accès de l'intérieur vers DMZ
- Assurer l'accès de l'Internet vers DMZ
- Bloquer tout les reste du trafic
- Assurer la résilience
- Détecter et bloquer les attaques contre les services en DMZ
- Détecter le trafic malicieux