1

PLAN

- Introduction à la sécurité
- Objectifs de la sécurité informatique
- Firewall et IDS
- Environement Hadoop
- Solution de sécurité appliqué aux big data

2

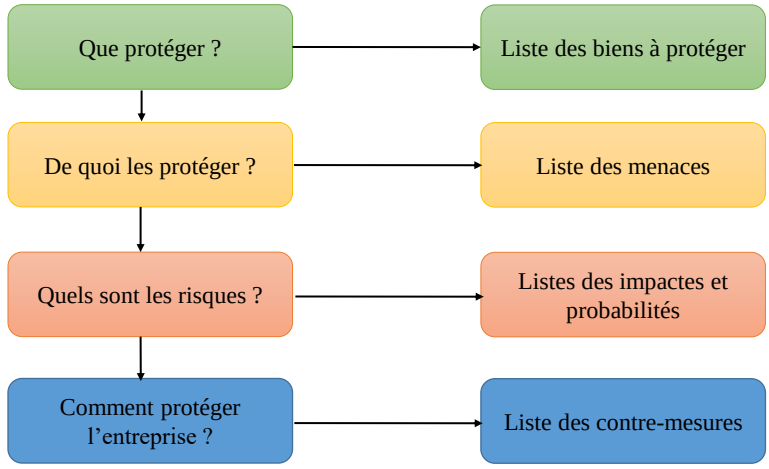
INTRODUCTION À LA SÉCURITÉ

Malek Rekik

3

Introduction

- Démarche de la Norme ISO 17799



4

Menaces

- un objet, une personne ou un événement nuisible qui peut être la source d'une attaque ou destruction
- Il existe plusieurs types de menaces tel que :
  - les accidents : perte de service, panne, événements naturels , choc, rayonnement, explosion, etc.
  - Erreur : erreur de conception, erreur d'utilisation, Erreur de saisie, de transmission de données
  - Malveillance : fraude informatique, intrusion, divulgation des informations privées, accès non autorisé par un dispositif sans fil, blocage de compte, refus de service, piratage, usurpation d'identité, etc.

5

Vulnérabilités et risques

- **Vulnérabilités :** Failles ou faiblesse qui exposent un système d'être exploiter par les menaces
- **Risque :** Une probabilité exprimant le pourcentage qu'une attaque soit réalisée contre une ressource en exploitant ses vulnérabilité
- **Analyse de risque :** Identifier les risques et les évalués en se basant sur :
  - les valeurs des différents ressources
  - Les menaces de chaque ressource
  - les vulnérabilités de chaque ressource
- **Gestion de risque :** sélectionner et implémenter les mesures de sécurité selon :
  - Les risques spécifiés
  - Le niveau de risque acceptable pour chaque ressource

6

Attaques de sécurité

Une attaque est l'exploitation d'une faiblesse découverte dans un système informatique

Il existe 2 types d'attaques :

- **attaque passive**
  - Pas de modification d'information
  - Aucun effet indésirables sur le service ou le système
  - Divulgation de la vie privée
- **attaque active**
  - modifier l'information
  - Non disponibilité du service, etc.

Les attaques peuvent être encore classifiées comme :

- **attaque interne**
- **attaque externe**

7

Programmes malveillants

- un logiciel malveillant (*malware*) est un logiciel développé dans le but de nuire un système informatique
  - Virus
  - Cheval de troie
  - Vers
  - Logiciel espion (spyware), logiciel publicitaire et scareware
  - Hameçonnage (phishing)
  - Mascarade (spoofing)
  - Renifflage (sniffing)
  - Craquage (cracking)

8

virus

- Un virus est un code exécutable malveillant attaché à un autre fichier exécutable, tel qu'un programme légitime. L'exécution de ce programme active le virus.
- Les virus peuvent s'activer à une heure ou une date spécifique.
- Les trois modes de diffusion des virus informatiques sont les suivants :
  - supports amovibles,
  - téléchargements effectués sur Internet
  - pièces jointes dans un e-mail.
- Les virus peuvent être destructeurs, comme ceux qui modifient ou suppriment des données.
- Un virus de secteur d'amorçage, ou de système de fichiers, infecte les clés USB et peut affecter le disque dur du système.

9

Cheval de troie

- Un cheval de Troie est un type de malware qui effectue des opérations malveillantes sous le couvert d'une opération souhaitée ;
- Ce code malveillant exploite les privilèges de l'utilisateur qui l'exécute.
- Un cheval de Troie est différent d'un virus parce qu'il se lie à des fichiers non exécutables, comme des fichiers images, audio ou des jeux.

10

comme : ILOVEYOU (2000)
Description : Le ver ILOVEYOU a été distribué par e-mail sous la forme d'une pièce jointe intitulée " LOVE-LETTER-FOR-YOU.txt.vbs". Lorsque la pièce jointe était ouverte, le ver se dupliquait et envoyait des copies à tous les contacts de l'utilisateur dans sa liste d'adresses e-mail.
Propagation : Il s'est propagé via des e-mails en exploitant la curiosité des utilisateurs.
Impact : Environ 10 % des ordinateurs connectés à Internet à l'époque ont été infectés, causant des dommages estimés à plus de 10 milliards de dollars. Il a également endommagé des fichiers sur les systèmes infectés, rendant certaines données irrécupérables.

vers

- Les vers sont des codes malveillants qui se répliquent en exploitant de façon indépendante les vulnérabilités au sein des réseaux.
- Les vers ralentissent généralement les réseaux.
- Alors que le virus nécessite un programme hôte pour s'exécuter, les vers peuvent fonctionner par eux-mêmes.
- À l'exception de l'infection initiale, les vers n'ont plus besoin d'intervention extérieure.
- Dès qu'un ver a infecté un hôte, il peut se répandre très rapidement sur le réseau.

11

Qu'est-ce qu'une signature de malware ?

Une signature de malware est une séquence spécifique de code, un modèle de comportement ou un ensemble d'attributs qui permet de reconnaître un logiciel malveillant. Chaque malware possède une signature distincte, qui peut être basée sur ses caractéristiques internes, telles que des instructions spécifiques, des fichiers qu'il génère, ou des comportements observés lorsqu'il s'exécute sur un système.

Protection contre les attaques virales

- **Programme antivirus** :
  - détectent les formes de malware les plus répandues.
  - les nouveaux virus ne sont pas détectés
  - il faut mettre à jour les signatures périodiquement.
  - Une signature est similaire à une empreinte digitale. Elle identifie les caractéristiques d'un programme malveillant.
- **Logiciels à jour** :
  - Les programmes malveillants exploitent les vulnérabilités logicielles
  - Il faut mettre à jour les applications avec leurs nouvelles versions dont les failles sont traitées

12

Spyware

exemple :.
Keylogger :
Description : Un keylogger est un type de spyware qui enregistre toutes les frappes du clavier effectuées par l'utilisateur, y compris les mots de passe, les identifiants de connexion, les messages et autres informations sensibles.

- est un logiciel qui permet à son propriétaire d'obtenir des informations sur les activités informatiques d'un utilisateur.
- inclut souvent le suivi des activités, la collecte de frappes sur clavier et la capture des données.
- Le logiciel espion se regroupe souvent avec des logiciels légitimes ou avec des chevaux de Troie.

shar3i

13

adware

Adware : Un programme qui affiche des publicités indésirables, souvent en analysant les habitudes de navigation de l'utilisateur. Exemple : Gator, qui suivait l'historique des navigateurs et affichait des publicités en fonction des sites visités.

- affiche des fenêtres publicitaires pour induire des revenus à son développeur.
- analyse les centres d'intérêt des utilisateurs par l'analyse des sites web visités.
- envoie des publicités relatives à ces sites

14

scareware

Scareware : Logiciel qui tente de faire peur à l'utilisateur pour qu'il télécharge ou achète des logiciels inutiles ou malveillants. Exemple : WinFixer, qui prétendait détecter des virus et poussait les utilisateurs à acheter une version "complète" pour résoudre de faux problèmes.

- convaincre l'utilisateur d'effectuer une action donnée en jouant sur la peur.
- créer des fenêtres contextuelles similaires que les boîtes de dialogue du système d'exploitation contenant de faux messages indiquant que le système a besoin de l'exécution d'un programme spécifique pour fonctionner correctement.
- Quand l'utilisateur cède à la pression et exécute le programme spécifié, il infecte son système.

15

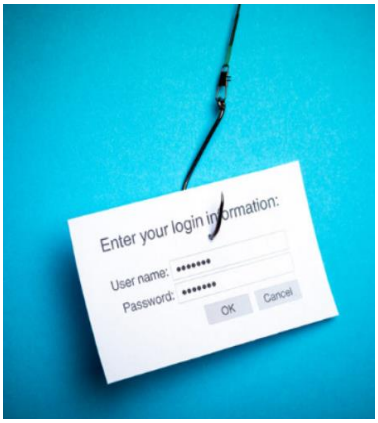
Courrier indésirable

- Appelé aussi « spam » est un e-mail non sollicité.
- Il peut comporter des liens malveillants, un malware ou un contenu trompeur.
- Peut fournir des informations sensibles, comme un numéro de sécurité sociale ou de compte bancaire à son développeur.
- Peut se propager par les ordinateurs infectés par un virus ou un ver.
- Il faut se méfier des éléments suspects suivants :
  - E-mail demandant des informations sur un compte
  - E-mail contenant des caractères ou une ponctuation inhabituelle
  - E-mail contenant des liens très longs ou difficiles à lire
  - E-mail inconnu portant une pièce jointe

16

Phishing

- Les attaquants se font passer pour une personne fiable
- Les attaquants se servent des e-mails, de la messagerie instantanée ou d'autres réseaux sociaux pour essayer de collecter des informations comme celles de connexion ou des compte utilisateurs
- Le phishing consiste à envoyer un e-mail frauduleux comme s'il provenait d'une source de confiance légitime. (banque, magasin, …..)
- L'objectif du message est de piéger le destinataire pour qu'il installe un malware sur son appareil ou partage des informations personnelles et critiques.
- **Exemple** : un e-mail factice ayant l'apparence d'un site de magasin, demandant à l'utilisateur de cliquer sur un lien pour demander un prix. Le lien peut le diriger vers un faux site demandant des informations personnelles, ou installer un virus.



17

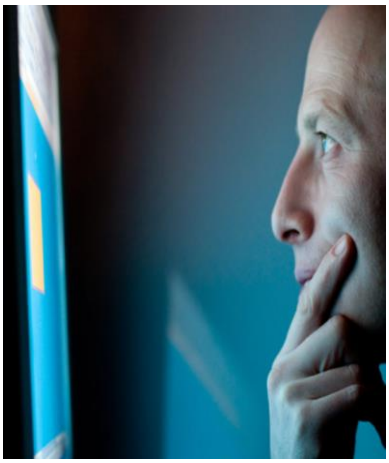
Phishing ciblé

- le phishing ciblé personnalise les e-mails visant ainsi une personne spécifique. Le malfaiteur recherche les intérêts de la cible avant d'envoyer l'e-mail.
- **Exemple** :
- un attaquant apprend que la victime s'intéresse à un modèle spécifique de voiture par ses recherches.
- il crée une fausse publication de vente de voiture demandée par la victime et envoie une notification à la cible.
- La notification inclut un lien vers les photos de la voiture.
- Lorsque la victime clique sur le lien, un malware sera installé à son insu sur son ordinateur.

18

Protection contre les attaques par e-mail et via le navigateur

- S'il est difficile de supprimer le spam, certaines méthodes permettent toutefois d'en limiter les effets:
  - filtrer les e-mails
  - apprendre aux utilisateurs à se méfier des e-mails envoyés par des inconnus
  - De nombreux logiciels antivirus de messagerie procèdent à un filtrage automatique des e-mails pour détecter et supprimer le courrier indésirable de la boîte de réception.
  - Se méfier des pièces jointes des e-mails et Analyser les toujours avec un programme antivirus avant de les ouvrir.
  - mettre à jour des logiciels pour disposer tous les correctifs de sécurité nécessaires éliminant les vulnérabilités connues.



19

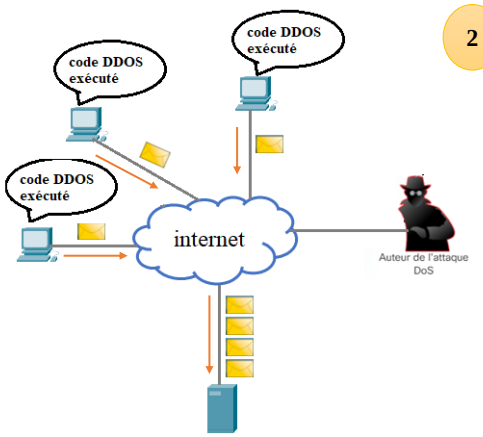
Déni de service (DOS)

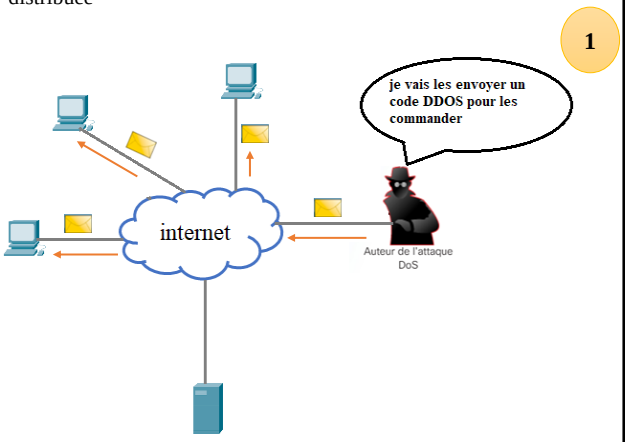
- DOS cause une interruption des services de réseau pour les utilisateurs, les appareils ou les applications entraînant une perte importante de temps et d'argent.
- DOS est effectuée suite à l’épuisement des ressources de la victime.
- Il existe deux types majeurs d'attaques par déni de service :
  - L’épuisement s’effectue par l’envoie d'énormes quantités de données à la victime jusqu’à elle devient incapable de poursuivre son travail.
  - L’épuisement s’effectue par l’envoie d’un paquet formaté de manière malveillante contenant des erreurs pour causer un ralentissement de l'appareil victime ou une panne.

20

DDOS

- une attaque par déni de service distribuée peut procéder comme suit :
  - Un intrus établit un réseau d'hôtes infectés, appelé réseau de zombies.
  - Les hôtes infectées esclaves sont commandées par l'attaquant
  - L'intrus leurs demande d'effectuer une attaque par déni de service distribuée

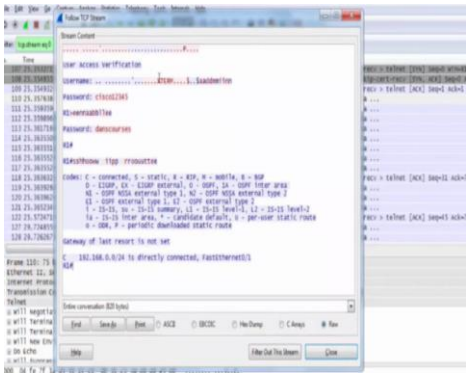




21

Écoute ou sniffer

- L'attaquant examine tout le trafic réseau et collecte des informations privées.
- Les attaquants interceptent le trafic réseau à l'aide d'une application logicielle (wireshark,..)
- Le logiciel d'écoute peut cibler :
  - un protocole,
  - un service,
  - un nom de connexion
  - un mot de passe
  - Numéro de carte de crédit
- Les administrateurs réseau peuvent utiliser des sniffers pour analyser le trafic réseau, identifier les problèmes de bande passante et résoudre d'autres problèmes affectant le réseau.



22

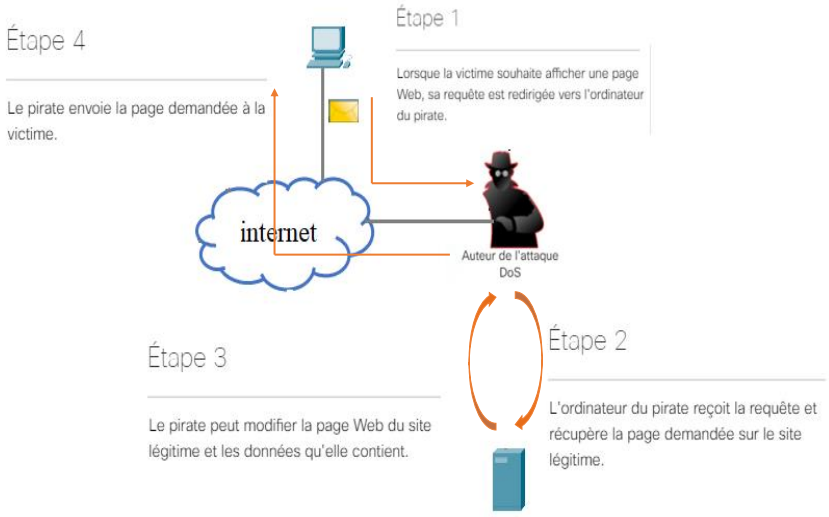
Usurpation

- Technique consistant à prendre l'identité d'une machine . elle est utilisée pour récupérer les informations sensibles.
- Il existe plusieurs types d'attaque d'usurpation :
  - Usurpation de mot de passe
  - Usurpation de compte
  - Usurpation d'adresse MAC
  - Usurpation d'adresse IP
  - Usurpation (DNS): réacheminer un nom de domaine spécifique vers une autre adresse IP contrôlée par le criminel.

23

Man in the middle

- L'intrus peut communiquer de fausses informations entre l' hôte qui ne remarque pas que les messages ont été modifiés et les serveurs destinés par la victime.



24

Falsification

- l'attaquant modifie les données
- l'attaquant externe utilise un accès non autorisé
- l'attaquant interne utilise de mauvais privilèges
- Cette attaque peut créer des menaces comme :
  - Falsification des salaires, inscription, score, etc.
  - Suppression des logins et mots de passe
  - Installation des chevaux de Troie pour intercepter les informations sensibles

25

Enregistreur de frappe

- un logiciel qui enregistre les saisies effectuées au clavier par l'utilisateur du système.
- Les attaquants peuvent mettre en place des enregistreurs de frappe via un logiciel installé sur un système informatique ou via du matériel connecté physiquement à un ordinateur.
- L'enregistreur de frappe est configuré pour les frappes consignées dans un fichier journal divulguant les **noms d'utilisateur, les mots de passe**, les **sites web visités** et d'autres informations sensibles.
- De nombreux logiciels anti-espions sont en mesure de détecter et de supprimer les enregistreurs de frappe non autorisés.

26

ARP spoofing

ARP (Address Resolution Protocol) est un protocole qui traduit les adresses IP en adresses MAC pour transmettre des données dans une trame.

L'usurpation ARP envoie des messages ARP réponse falsifiés sur un réseau local afin de lier l'adresse MAC de l'intrus à l'adresse IP d'un membre autorisé du réseau.

Cette attaque cause la pollution des caches ARP avec de fausses associations adresse mac/adresse IP.

elle permet des attaques Man in the middle , dos , Transgression des règles d'un firewall par spoofing

27

Password guessing

- C'est le crackage du mot de passe , elle peut être réalisé par une recherche exhaustive (force brute) ou une recherche intelligente :
- une recherche exhaustive:
  - Essai toutes les combinaisons possibles
  - il est facile si le mot de passe est de longueur faible
- une recherche intelligente :
  - le mot de passe est trouvé à partir des informations de la victime comme son nom, son numéro de téléphone, sa date de naissance
  - attaque par dictionnaire

28