2021

Sécurité Informatique

Dr. Cheikh Mohamed

Université 20 Aout 1955 de SKIKDA

01/01/2021

Objectifs de l'enseignement *:* L'objectif du ce cours focalise sur deux points principaux : apprendre les notions de bases de l'intégration des nouveaux réseaux dans les systèmes informatiques et aussi à permettre au candidat de faire le point sur les problèmes de sécurité qui se posent actuellement et les moyens, les approches et les techniques de lutte et de prévention disponibles comme La sécurité des systèmes informatiques constitue de nos jours une préoccupation permanente pour tout développeur d'application

Connaissances préalables recommandées *:* Réseaux, architecture des réseaux de communication

Contenu de la matière

- Problématique de la sécurité : Confidentialité, intégrité, disponibilité, authentification, non-répudiation, contrôle d'accès, -Vulnérabilités, menaces à la sécurité et attaques

-SPAM ; virus, spyware, Détection d'intrusion, Filtrage, para-feux, Mécanismes de recouvrement,

-Principes et politiques de sécurité

- Techniques de base en sécurité : Techniques de chiffrage, Caractérisation des systèmes de chiffrage, Cryptanalyse et attaques Mécanismes sécuritaires modernes :

- Applications sécurisés : Identification et authentification, Protocole (signature, authentification mutuelle), …….

CHAPITRE 1

Sécurité informatique

1 Introduction

Les réseaux et applications informatiques sont utilisés de façon croissante et touchent des domaines aussi variés que les applications d'entreprise, le domaine médical ou le commerce électronique. Dans ce contexte, la sécurisation des systèmes d'information est une problématique de premier plan. La sécurité informatique a pour but d'assurer la confidentialité et l'intégrité des données ainsi que la disponibilité des services. Pour assurer la sécurité des systèmes d'information, il existe toute une gamme de solutions telles que la cryptographie, l'application de politiques de sécurité utilisant des pares-feux ou de serveurs mandataires. Cependant, ces mécanismes ne peuvent assurer une sécurité totale des systèmes d'information. En effet, ils peuvent présenter des failles de conception, être mal configurés ou mettre en œuvre une politique de sécurité mal adaptée, ce qui permet à un attaquant de contourner les mesures de sécurité. Il est donc nécessaire d'utiliser, en plus, des outils permettant de détecter les attaques visant les systèmes d'information. Ces outils sont les systèmes de détection d'intrusion.

A l'origine, les premiers systèmes de détection d'intrusion ont été initiés par l'armée américaine, puis par des entreprises. Plus tard, des projets open-source ont été lancés et certains furent couronnés de succès, comme par exemple Snort. Parmi les solutions commerciales, on retrouve les produits des entreprises spécialisées en sécurité informatique telles qu'Internet Security Systems, Symantec, Cisco Systems, … Mais avant cela, il est important, pour comprendre le rôle précis de ces systèmes, de faire un rappel sur la sécurité informatique et les principales attaques existant à l'heure actuelle [5].

- ## Sécurité informatique

La sécurité recouvre l'ensemble des moyens informatiques mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles, permettant ainsi aux systèmes informatiques de fonctionner normalement. Elle consiste aussi à s'assurer que celui qui modifie ou consulte les données du système en a l'autorisation et qu'il peut le faire car le service est disponible [6].

Le **risque** en termes de sécurité est généralement caractérisé par l'équation suivante [7] :

$$\text{Risque}=\frac{\text{Menace}*\text{vulnerabilité}}{\text{Contre mesure}} \qquad (1)$$

- **La menace** représente une action ou événement dont le déclenchement pourrait porter atteinte à l'une, voire à plusieurs des caractéristiques critiques de l'information et des systèmes qui la traitent et la maintiennent, à savoir : la confidentialité, l'intégrité, et la disponibilité [7].
- **Vulnérabilité :** toutes les failles, les brèches dans le système, tout ce qui expose le système à la menace : manque de sauvegarde, de robustesse, une architecture défaillante [8].
- **Contre mesure** : Les actions mises en œuvre pour prévenir la menace, une fois qu'elle est mesurée. Ceci passe d'abord par une prise de conscience [8].

Les contre-mesures à mettre en œuvre ne sont pas uniquement des solutions techniques mais également des mesures de formation et de sensibilisation à l'intention des utilisateurs, ainsi qu'un ensemble de règles clairement définies.

Afin de pouvoir sécuriser un système, il est nécessaire d'identifier les menaces potentielles, et donc de connaître et de prévoir la façon de procéder de l'ennemi. Le but de la prochaine section est ainsi de donner un aperçu des motivations éventuelles des pirates, de catégoriser ces derniers, et enfin de donner une idée de leur façon de procéder afin de mieux comprendre comment il est possible de limiter les risques d'intrusion.

- ## Les critères de sécurité

La sécurité informatique repose sur cinq principes clés : disponibilité, intégrité, confidentialité, non répudiation et authentification.

2.1 La Disponibilité (Availability) :

consiste à s'assurer du bon fonctionnement du système, de l'accès à un service et aux ressources à n'importe quel moment. La disponibilité d'un équipement se mesure en divisant la durée durant laquelle cet équipement est opérationnel par la durée durant laquelle il aurait dû être opérationnel [8].

2.2 La Confidentialité (confidentiality):

concerne la prévention de la divulgation non autorisée de information. La divulgation pourrait être intentionnelle, comme la rupture d'un chiffre de données pour lire l'information, ou cela pourrait être involontaire, en raison de la négligence ou de l'incompétence des personnes qui traitent les informations [9].

2.3 L'Intégrité (integrity):

elle garantit trois buts principaux [9]:

- ✓ Préserver la modification des informations par les utilisateurs non autorisés.
- ✓ Préserver la modification non autorisée ou involontaire de l'information par les utilisateurs autorisés.
- ✓ Préserver la cohérence interne et la cohérence externe :
  - La cohérence interne consiste à garantir la cohérence des données internes. Par exemple, dans une organisation on assure que le nombre total des articles maintenus par cette organisation est égal à la somme des mêmes articles dans la base de données.
  - La cohérence externe consiste à assurer que la cohérence entre les données dans la base de données et le monde réel est maintenue. Par exemple, dans une entreprise on assure que le nombre des articles vendus est le même nombre dans la base de données.

2.4 Non-répudiation :

elle garantit qu'aucun des correspondants ne pourra nier la transaction. Ainsi, lorsqu'un message est envoyé, le receveur peut prouver que le message a bien été envoyé par l'expéditeur prétendu. De même, lorsqu'un message est reçu, l'expéditeur peut prouver que le message a bien été reçu par le prétendu récepteur [10].

2.5 Authentification :

elle permet d'assurer l'authenticité d'une communication. Dans le cas d'un message élémentaire, tel un signal d'avertissement, d'alarme, ou un ordre de tir, la fonction du service d'authentification est d'assurer le destinataire que le message a bien pour origine la source dont il prétend être issu. Dans le cas d'une interaction

suivie, telle une connexion d'un terminal à un serveur, deux aspects sont concernés. En premier lieu, lors de l'initialisation de la connexion, il assure que les deux entités sont authentiques (c'est-à-dire, que chaque entité est celle qu'elle prétend être). Ensuite, le service doit assurer que la connexion ne peut pas être perturbée par une tierce partie qui pourrait se faire passer pour une des deux entités légitimes à des fins de transmissions ou de réceptions non autorisées [11].

- **Attaques de sécurité**

Une attaque peut être définie comme toute action ou ensemble d'actions qui peuvent porter atteinte à la sécurité des informations d'un système ou réseau informatique [12]. Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque. Sur internent, des attaques ont lieu en permanence, à raison de plusieurs attaques par minute sur chaque machine connectée. Ces attaques sont pour la plupart lancées automatiquement à partir de machines infectées (par des virus, chevaux de Troie, vers, etc.), à l'insu de leur propriétaire. Plus rarement il s'agit de l'action de pirates informatiques.

Afin de contrer ces attaques, il est indispensable de connaître les principaux types d'attaques afin de mettre en œuvre des dispositions préventives. Les motivations des attaques peuvent être de différentes sortes :

- Obtenir un accès au système ;
- Voler des informations, tels que des secrets industriels ou des propriétés intellectuelles ;
- Glaner des informations personnelles sur un utilisateur ;
- Récupérer des données bancaires ;
- S'informer sur l'organisation (entreprise de l'utilisateur, etc.) ;
- Troubler le bon fonctionnement d'un service ;
- Utiliser le système de l'utilisateur comme « rebond » pour une attaque ;
- Utiliser les ressources du système de l'utilisateur, notamment lorsque le réseau sur lequel il est situé possède une bande passante élevée
- …

- **Anatomie d'une attaque**

Fréquemment appelés « les 5 P » [12] dans la littérature, ces cinq verbes anglophones constituent le squelette de toute attaque informatique : Probe, Penetrate, Persist, Propagate et Paralyze.
Observons le détail de chacune de ces étapes :

- **Probe** : consiste en la collecte d'informations par le biais d'outils comme whois, Arin, DNS lookup. La collecte d'informations sur le système cible peut s'effectuer de plusieurs manières, comme par exemple un scan de ports grâce au programme Nmap pour déterminer la version des logiciels utilisés, ou encore un scan de vulnérabilités à l'aide du programme Nessus. Pour les serveurs web, il existe un outil nommé Nikto qui permet de rechercher les failles connues ou les problèmes de sécurité. Des outils comme firewalk, hping ou SNMP Walk permettent quant à eux de découvrir la nature d'un réseau.
- **Penetrate**: utilisation des informations récoltées pour pénétrer un réseau. Des techniques comme la brute force ou les attaques par dictionnaires peuvent être utilisées pour outrepasser les protections par mot de passe. Une autre alternative pour s'infiltrer dans un système est d'utiliser des failles applicatives.
- **Persist :** création d'un compte avec des droits de super utilisateur pour pouvoir se réinfiltrer ultérieurement. Une autre technique consiste à installer une application de contrôle à distance capable de résister à un reboot (ex : un cheval de Troie).
- **Propagate :** cette étape consiste à observer ce qui est accessible et disponible sur le réseau local.
- **Paralyze :** cette étape peut consister en plusieurs actions. Le pirate peut utiliser le serveur pour mener une attaque sur une autre machine, détruire des données ou encore endommager le système d'exploitation dans le but de planter le serveur.

Après ces cinq étapes, le pirate peut éventuellement tenter d'effacer ses traces, bien que cela soit rarement utile. En effet, les administrateurs réseaux sont souvent surchargés de logs à analyser. De plus, il est très difficile de supprimer entièrement des traces.

- **Les différents types d'attaques**

L'informatique étant un domaine très vaste, le nombre de vulnérabilités présentes sur un système peut donc être important. Ainsi, les attaques visant ces failles peuvent être à la fois très variées et très dangereuses, et peuvent engendrer des graves conséquences.

- **Les attaques réseaux**

Ce type d'attaque se base principalement sur des failles liées aux protocoles ou à leur implémentation (*cf.* Tableau 1). Les RFC1 ne sont parfois pas assez spécifiques, et un choix particulier d'implémentation dans les différents services ou clients peut entraîner un problème de sécurité. Observons dans le tableau 1 [12] quelques attaques bien connues.

Attaque	But	Description
Les techniques de scan	Le but des scans est de déterminer quels sont les ports ouverts	Les scans de ports ne sont pas des attaques à proprement parler. Le but des scans est de déterminer quels sont les ports ouverts, et donc en déduire les services qui sont exécutés sur la machine cible (ex : port 80/TCP pour un service HTTP). Par conséquent, la plupart des attaques sont précédées par un scan de ports lors de la phase Probe qui est, la première phase des 5P's dans le déroulement d'une attaque.

IP Spoofing	usurper l'adresse IP d'une autre machine.	se faire passer pour une autre machine en truquant les paquets IP. Cette technique peut être utile dans le cas d'authentifications basées sur une adresse IP (services tels que rlogin ou ssh par exemple).
ARP Spoofing (ou ARP Redirect)	rediriger le trafic d'une machine vers une autre.	grâce à cette redirection, une personne mal intentionnée peut se faire passer pour une autre. De plus, le pirate peut rediriger les paquets qu'il reçoit vers le véritable destinataire, ainsi l'utilisateur usurpé ne se rendra compte de rien. La finalité est la même que l'IP spoofing mais on travaille ici au niveau de la couche liaison de données.
DNS Spoofing	fournir de fausses réponses aux requêtes DNS, c'est-à-dire indiquer une fausse adresse IP pour un nom de domaine.	rediriger, à leur insu, des Internautes vers des sites pirates. Grâce à cette fausse redirection, l'utilisateur peut envoyer ses identifiants en toute confiance.
Fragments attacks	le but de cette attaque est de passer outre les protections des équipements de filtrage IP.	en passant outre les protections, un pirate peut par exemple s'infiltrer dans un réseau pour effectuer des attaques ou récupérer des informations confidentielles.

TCP Session Hijacking	le but de cette attaque est de rediriger un flux TCP afin de pouvoir outrepasser une protection par mot de passe.	Le contrôle d'authentification s'effectuant uniquement à l'ouverture de la session, un pirate réussissant cette attaque parvient à prendre possession de la connexion pendant toute la durée de la session.

Tableau 1: Les attaques réseaux [13]

- **Les attaques applicatives**

Les attaques applicatives se basent sur des failles dans les programmes utilisés, ou encore des erreurs de configuration. Toutefois, comme précédemment, il est possible de classifier ces attaques selon leur provenance (*cf.* Tableau 2).

Attaque	**Description**
Les problèmes de configuration	Il est très rare que les administrateurs réseaux configurent correctement un programme. En général, ils se contentent d'utiliser les configurations par défaut. Celles-ci sont souvent non sécurisées afin de faciliter l'exploitation du logiciel (ex : login/mdp par défaut d'un serveur de base de données).
Les bugs	Liés à un problème dans le code source, ils peuvent amener à l'exploitation de failles. Il n'est pas rare de voir l'exploitation d'une machine suite à une simple erreur de programmation. On ne peut toutefois rien faire contre ce type de problèmes, si ce n'est attendre un correctif de la part du développeur.

Les buffer overflows	Les buffers overflows, ou dépassement de la pile, sont une catégorie de bug particulière. Issus d'une erreur de programmation, ils permettent l'exploitation d'un shellcode à distance. Ce shellcode permettra à une personne mal intentionnée d'exécuter des commandes sur le système distant, pouvant aller jusqu'à sa destruction.
Les scripts	Principalement web (ex : Perl, PHP, ASP), ils s'exécutent sur un serveur et renvoient un résultat au client. Cependant, lorsqu'ils sont dynamiques (i.e. qu'ils utilisent des entrées saisies par un utilisateur), des failles peuvent apparaître si les entrées ne sont pas correctement contrôlées.
Les injections SQL	Tout comme les attaques de scripts, les injections SQL profitent de paramètres d'entrée non vérifiés. Comme leur nom l'indique, le but des injections SQL est d'injecter du code SQL dans une requête de base de données. Ainsi, il est possible de récupérer des informations se trouvant dans la base (exemple : des mots de passe) ou encore de détruire des données.
Man in the middle	Moins connue, mais tout aussi efficace, cette attaque permet de détourner le trafic entre deux stations. Imaginons un client C communiquant avec un serveur S. Un pirate peut détourner le trafic du client en faisant passer les requêtes de C vers S par sa machine P, puis transmettre les requêtes de P vers S. Et inversement pour les réponses de S vers C.

Tableau 2: Les attaques applicatives [12]

- **Le Déni de service**

Evoqué précédemment, le déni de service est une attaque visant à rendre indisponible un service. Ceci peut s'effectuer de plusieurs manières : par le biais d'une surcharge réseau, rendant ainsi la

machine totalement injoignable ; ou bien de manière applicative en crashant l'application à distance.

L'utilisation d'un buffer overflow peut permettre de planter l'application à distance. Grâce à quelques instructions malicieuses et suite à une erreur de programmation, une personne mal intentionnée peut rendre indisponible un service (serveur web, serveur de messagerie, … etc) voire un système complet.

Nous citons quelques attaques réseaux connues permettant de rendre indisponible un service :

- **SYN Flooding** : exploite la connexion en 3 phases de TCP (Three Way Handshake SYN / SYN-ACK / ACK). Le principe est de laisser un grand nombre de connexions TCP en attente. Le pirate envoie de nombreuses demandes de connexion (SYN), reçoit les SYN-ACK mais ne répond jamais avec ACK. Les connexions en cours occupent des ressources mémoire, ce qui va entraîner une saturation et l'effondrement du système. Parmi les attaques de type SYN Flood l'attaque Neptune.
- **Neptune :** est une attaque SYN floods. Il attaque l'hôte victime en envoyant de manière continue des paquets TCP SYN à un taux de 248 paquets SYN par seconde.
- **UDP Flooding**: le trafic UDP est prioritaire sur TCP. Le but est donc d'envoyer un grand nombre de paquets UDP, ce qui va occuper toute la bande passante et ainsi rendre indisponible toutes les connexions TCP.

  Exemple : l'envoi d'une requête (port 19 / service de génération de caractères) à une machine en spoofant l'adresse et le port source, pour rediriger vers echo (port 7 / service qui répète la chaîne de caractères reçue) d'une autre machine.
- **Packet Fragment (fragmentation de paquet)**: utilise une mauvaise gestion de la défragmentation au niveau ICMP.
- **Smurfling** : le pirate envoie des requêtes ICMP ECHO à des adresses de broadcast en « Spoofant » l'adresse source (en indiquant l'adresse de la machine cible). Cette machine cible va recevoir un nombre énorme de réponses, car toutes les machines vont lui répondre, et ainsi utiliser toute sa bande passante.
- **Déni de service distribué** : le but ici est de reproduire une attaque normale à grande échelle. Pour ce faire, le pirate va tenter de se rendre maître d'un nombre important de machines. Grâce à des failles (buffer overflows, failles RPC4, … etc) il va pouvoir prendre le contrôle de machines à distance et ainsi pouvoir les commander à sa guise. Une fois ceci

effectué, il ne reste plus qu'à donner l'ordre d'attaquer à toutes les machines en même temps, de manière à ce que l'attaque soit reproduite à des milliers d'exemplaires. Ainsi, une simple attaque comme un SYN Flooding peut rendre une machine ou un réseau totalement inaccessible.

4. Conclusion

Le concept de sécurité est très important pour garder les systèmes et réseaux informatiques dans les meilleurs états et garantir la protection la plus optimale de leurs données et services, c'est une notion que chaque entreprise doit prendre en compte en mettant en œuvre tous les moyens et outils qui la réalisent et la maintiennent.

Avec certitude il n'y pas un système sécurisé à 100% pour cette raison le plus important ce n'est pas de savoir qu'une menace va l'attaquer mais c'est de savoir quand cela va arriver et d'avoir des mécanismes qui protègent les systèmes et réseaux informatiques.

Références

[5] M.Cheikh «un mécanisme de détection d'intrusion adaptatif à base d'agents,» Mémoire de magistère, Ecole doctorale de l'est , 2009.

[6] S. Gunadiz, «Algorithme d'intelligence artificielle pour la classification d'attaques réseaux à partir de données TCP,» (These de magistere). Université M'hamed Bougara., Boumerdes, 2011.

[7] D. Godart, « Sécurité informatique Risques,stategies et solutions: échec au cyber-roi », (2e édition)., CCI de wallonie., 2005.

[8] J. Musset, « Securité informatique ,Ethical Hacking:Apprendre l'attaque pour mieux se défendre », ENI editions, 2009.

[9] E. Cole, R. Krutz and J. Conley, « Network security bible», Wiley Publishing, Inc, 2005.

[10] Y. Farhaoui, «Evaluation des systèmes de détection et de prévention des intrusions et la conception d'un BiIDS,» (These de doctorat). Université IBN ZOHR, Agadir, 2012.

[11] L. Poinsot, «Introduction à la sécurité informatique,» Université Paris 13 - Institut Galilée., Paris, 2009.

[12] D. Burgermeister and J. Krier, «Les systèmes de détection d'intrusions,» 2006. [En ligne]. Available: http://dbprog.developpez.com .