

Partie I:

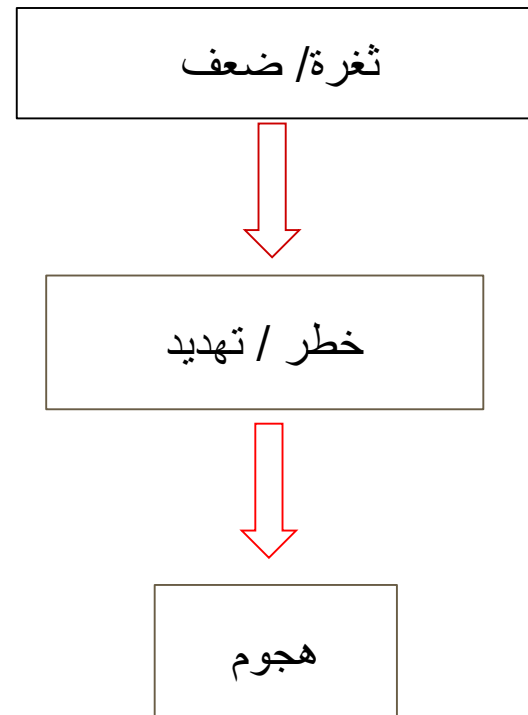
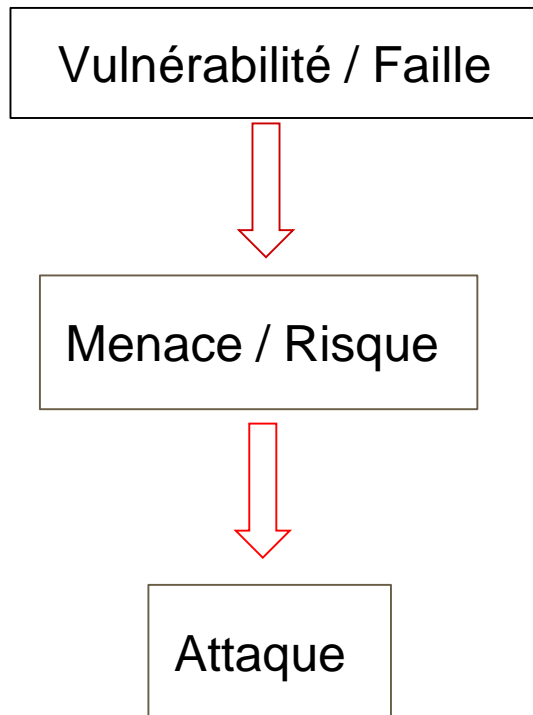
- I.1 Introduction à la sécurité Informatique
- I.2 Enjeux de la sécurité Informatique
- I.3 Propriétés/Services de la sécurité
- **I.4 Vulnérabilités, Failles, Menaces, Attaques**

Rappel

- ***Objectif Sécurité Informatique:***
 - réduire -voir éliminer- les **risques** pesant sur le système d'information, pour limiter leurs impacts sur le fonctionnement et les activités métiers des organisations...
 - La sécurité informatique à pour objectif de fournir et garantir les services de DCIP
 - Protection contre les **actions malveillantes volontaires** → **Attaques**

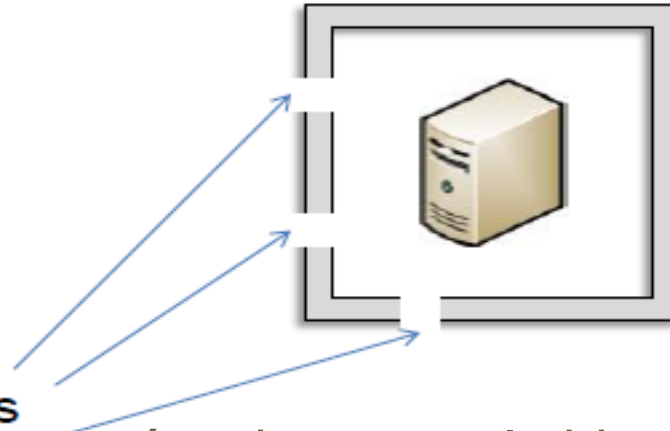
A chaque histoire un début: A l'origine d'une attaque

- Comment une attaque peut avoir lieu?



Vulnérabilité / Faille

- Faute accidentelle ou intentionnelle introduite dans la spécification, conception, configuration ou utilisation d'un bien ou d'un système



- Un point clé pour lancer une attaque réussie contre le bien, si bien **exploité**
- Analogie: un bon entraîneur de foot cherche à trouver une **faille** dans la défense adverse → c'est cette faille qui permettra probablement à son équipe de marquer

Vulnérabilité / Faille

- Intervient à tous les niveaux
 - Humain → Utilisation de Mdp banales, divulgation d'informations précieuses, etc.
 - Physique → Récupération image mémoire RAM, accès au secteur boot...
 - Système → Stockage Mdp, Élévation de privilèges, dépassement de tampons, ...
 - Réseau → Écoute passive/active, flooding, ...
 - Web → Injection SQL, ...
 - Applicative → Injection code, dépassement de tampon, ...

Vulnérabilité/Faibles logiciels

* Parmi les logiciels les plus ciblés

- Navigateurs Internet: Internet Explorer, Firefox, Chrome, etc.
- Microsoft Office: Word, Excel
- Logiciels Adobe: Adobe Reader, Adobe Acrobat, Adobe Flash
- Java

- Toutefois, pratiquement tous les logiciels, applications, OS peuvent contenir des vulnérabilités, avec des degrés différents (nombre, et gravité)
- La découverte des failles peut se faire par l'éditeur du logiciel, des sociétés spécialisés en sécurité, des individus passionnés, des attaquants, etc.

Vulnérabilité/Faile: exemple Windows 7

Plusieurs sites listent les vulnérabilités des OS/Logiciels -www.cvedetails.com/

CVE Details

The ultimate security vulnerability datasource

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

[Log In](#) [Register](#) [Reset Password](#) [Activate Account](#)

Vulnerability Feeds & Widgets^{New}

www.itsecdb.com



[Switch to https://](#)

[Home](#)

Browse :

[Vendors](#)

[Products](#)

[Vulnerabilities By Date](#)

[Vulnerabilities By Type](#)

Reports :

[CVSS Score Report](#)

[CVSS Score Distribution](#)

Search :

[Vendor Search](#)

[Product Search](#)

[Version Search](#)

[Vulnerability Search](#)

[By Microsoft References](#)

Top 50 :

[Vendors](#)

[Vendor Cvss Scores](#)

[Products](#)

[Product Cvss Scores](#)

[Versions](#)

Microsoft » Windows 7 : Vulnerability Statistics

[Vulnerabilities \(517\)](#)

[CVSS Scores Report](#)

[Browse all versions](#)

[Possible matches for this product](#)

[Related Metasploit Modules](#)

[Related OVAL Definitions :](#)

[Vulnerabilities \(436\)](#)

[Patches \(92\)](#)

[Inventory Definitions \(6\)](#)

[Compliance Definitions \(0\)](#)

[Vulnerability Feeds & Widgets](#)

CVSS score distribution report

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2009	15	3	10	2	6										1
2010	64	16	29	15	9		1			2	1	22			4
2011	102	14	18	9	8		2			4	2	65			3
2012	44	4	14	6						2	3	22			
2013	100	16	19	24	6			1		3	2	67			4
2014	36	6	12	5	3					6	5	12			4
2015	147	11	52	12	9			1		24	24	60			1
2016	9		4	1						1	1	6			
Total	517	70	150	71	44		3	2		40	20	254			17

Classement des logiciels/OS par nombre de vulnérabilités connues (2015*)

1	<u>Mac Os X</u>	<u>Apple</u>	OS	<u>444</u>
2	<u>Iphone Os</u>	<u>Apple</u>	OS	<u>387</u>
3	<u>Flash Player</u>	<u>Adobe</u>	Application	<u>329</u>
4	<u>Ubuntu Linux</u>	<u>Canonical</u>	OS	<u>261</u>
5	<u>Air Sdk</u>	<u>Adobe</u>	Application	<u>259</u>
6	<u>AIR</u>	<u>Adobe</u>	Application	<u>259</u>
7	<u>Air Sdk & Compiler</u>	<u>Adobe</u>	Application	<u>259</u>
8	<u>Opensuse</u>	<u>Novell</u>	OS	<u>242</u>
9	<u>Debian Linux</u>	<u>Debian</u>	OS	<u>234</u>
10	<u>Internet Explorer</u>	<u>Microsoft</u>	Application	<u>231</u>

*source: www.cvedetails.com/

Classement des logiciels/OS par nombre de vulnérabilités connues (2016*)

1	<u>Android</u>	<u>Google</u>	OS	<u>523</u>
2	<u>Debian Linux</u>	<u>Debian</u>	OS	<u>327</u>
3	<u>Ubuntu Linux</u>	<u>Canonical</u>	OS	<u>279</u>
4	<u>Flash Player</u>	<u>Adobe</u>	Application	<u>266</u>
5	<u>Leap</u>	<u>Novell</u>	OS	<u>260</u>
6	<u>Opensuse</u>	<u>Novell</u>	OS	<u>228</u>
7	<u>Acrobat Reader Dc</u>	<u>Adobe</u>	Application	<u>227</u>
8	<u>Acrobat Dc</u>	<u>Adobe</u>	Application	<u>227</u>
9	<u>Acrobat</u>	<u>Adobe</u>	Application	<u>224</u>
10	<u>Linux Kernel</u>	<u>Linux</u>	OS	<u>217</u>

*source: www.cvedetails.com/

Classement des logiciels/OS par nombre de vulnérabilités connues (2017*)

1	<u>Android</u>	<u>Google</u>	OS	<u>842</u>
2	<u>Linux Kernel</u>	<u>Linux</u>	OS	<u>453</u>
3	<u>Iphone Os</u>	<u>Apple</u>	OS	<u>387</u>
4	<u>Imagemagick</u>	<u>Imagemagick</u>	Application	<u>357</u>
5	<u>Mac Os X</u>	<u>Apple</u>	OS	<u>299</u>
6	<u>Windows 10</u>	<u>Microsoft</u>	OS	<u>268</u>
7	<u>Windows Server 2016</u>	<u>Microsoft</u>	OS	<u>252</u>
8	<u>Windows Server 2008</u>	<u>Microsoft</u>	OS	<u>243</u>
9	<u>Windows Server 2012</u>	<u>Microsoft</u>	OS	<u>235</u>
10	<u>Debian Linux</u>	<u>Debian</u>	OS	<u>230</u>

* source: www.cvedetails.com/

Classement des logiciels/OS par nombre de vulnérabilités connues (2018*)

1	<u>Android</u>	<u>Google</u>	OS	<u>74</u>
2	<u>Debian Linux</u>	<u>Debian</u>	OS	<u>36</u>
3	<u>R4299g Firmware</u>	<u>Tp-link</u>	OS	<u>25</u>
4	<u>Wvr1300l Firmware</u>	<u>Tp-link</u>	OS	<u>25</u>
5	<u>R488 Firmware</u>	<u>Tp-link</u>	OS	<u>25</u>
6	<u>Wvr900l Firmware</u>	<u>Tp-link</u>	OS	<u>25</u>
7	<u>R4239g Firmware</u>	<u>Tp-link</u>	OS	<u>25</u>
8	<u>Wvr1300g Firmware</u>	<u>Tp-link</u>	OS	<u>25</u>
9	<u>R483 Firmware</u>	<u>Tp-link</u>	OS	<u>25</u>
10	<u>Wvr900g Firmware</u>	<u>Tp-link</u>	OS	<u>25</u>

* source: www.cvedetails.com/

Classement des logiciels/OS par nombre de vulnérabilités connues (tous les temps)

1	Linux Kernel	Linux	OS	2035
2	Mac Os X	Apple	OS	1978
3	Android	Google	OS	1607
4	Chrome	Google	Application	1525
5	Firefox	Mozilla	Application	1438
6	Iphone Os	Apple	OS	1371
7	Debian Linux	Debian	OS	1210
8	Flash Player	Adobe	Application	1045
9	Windows Server 2008	Microsoft	OS	1022
10	Safari	Apple	Application	934
11	Acrobat	Adobe	Application	909
12	Internet Explorer	Microsoft	Application	905
13	Ubuntu Linux	Canonical	OS	888
14	Windows 7	Microsoft	OS	877
15	Windows Vista	Microsoft	OS	816

* source: www.cvedetails.com/

Vulnérabilité/Exploit

Une fois une vulnérabilité trouvée, il reste à l'exploiter en trouvant un **exploit** → un bout de code (écrit dans n'importe quel langage) qui permet de tirer un quelconque profit de la vulnérabilité au sein de la machine cible:

- Exécuter un code arbitraire
- Réaliser un déni de service
- élévation de privilèges
- Accès non autorisé à des données

Plusieurs sites internet référencent les exploits comme www.exploits-db.com, en donnant le code source de l'exploit

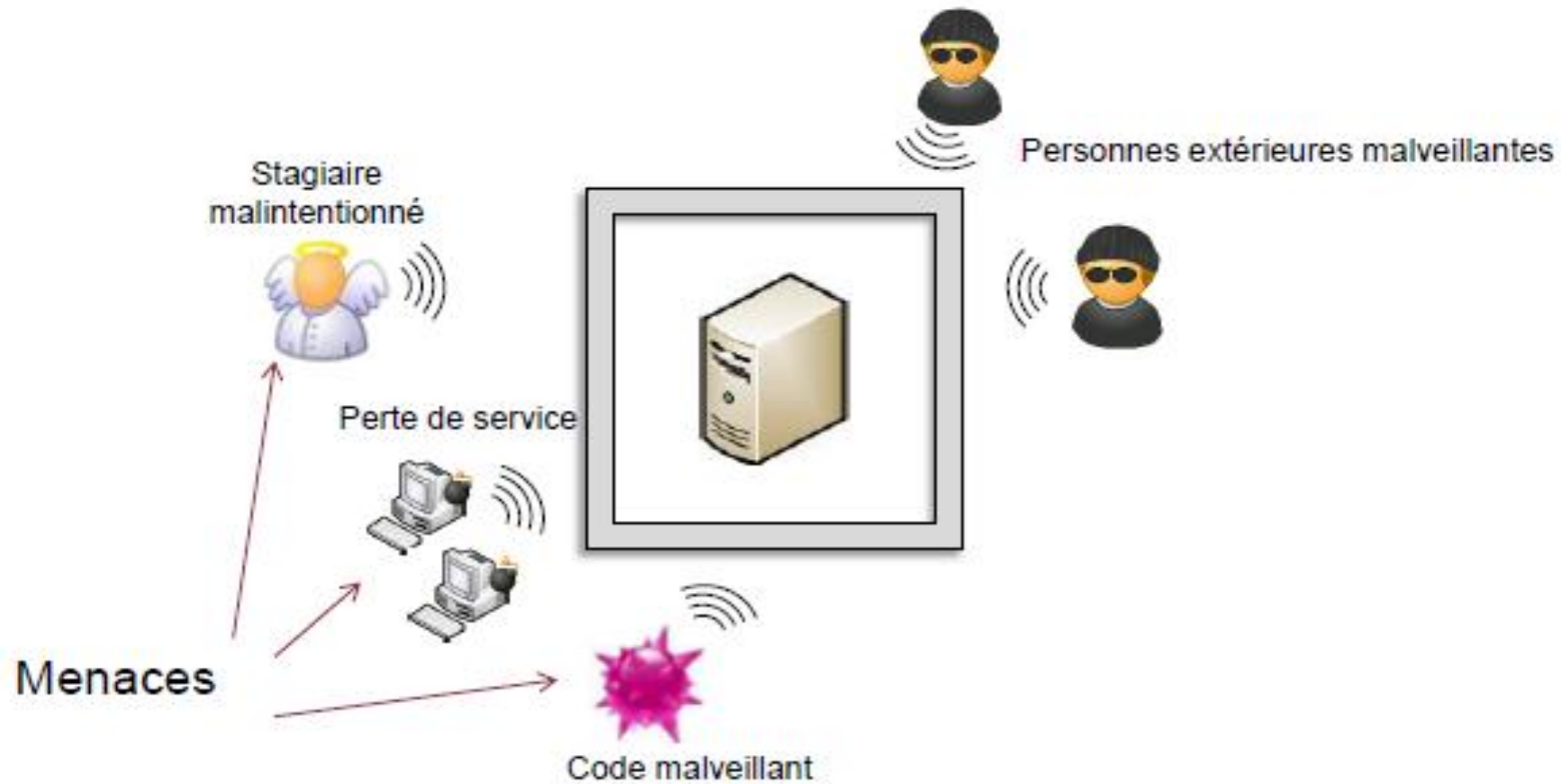
14

Failles/Vulnérabilité

- Au-fil du temps, les vulnérabilités sont découvertes (rendues publiques), puis corrigées par les éditeurs logiciels correspondant (ex: mise à jour de sécurité Windows) → **Patches** de sécurité, dans ce cas les exploits correspondants aux vulnérabilités ne sont plus efficaces sur les produits corrigés
- Néanmoins, il y a toujours de nouvelles vulnérabilités qui apparaissent non-connues auparavant, pour lesquelles de nouveaux exploits sont trouvés (vulnérabilité/exploit **0-day**). → ces vulnérabilités/exploits sont vendues à des dizaines de milliers de \$

Menace

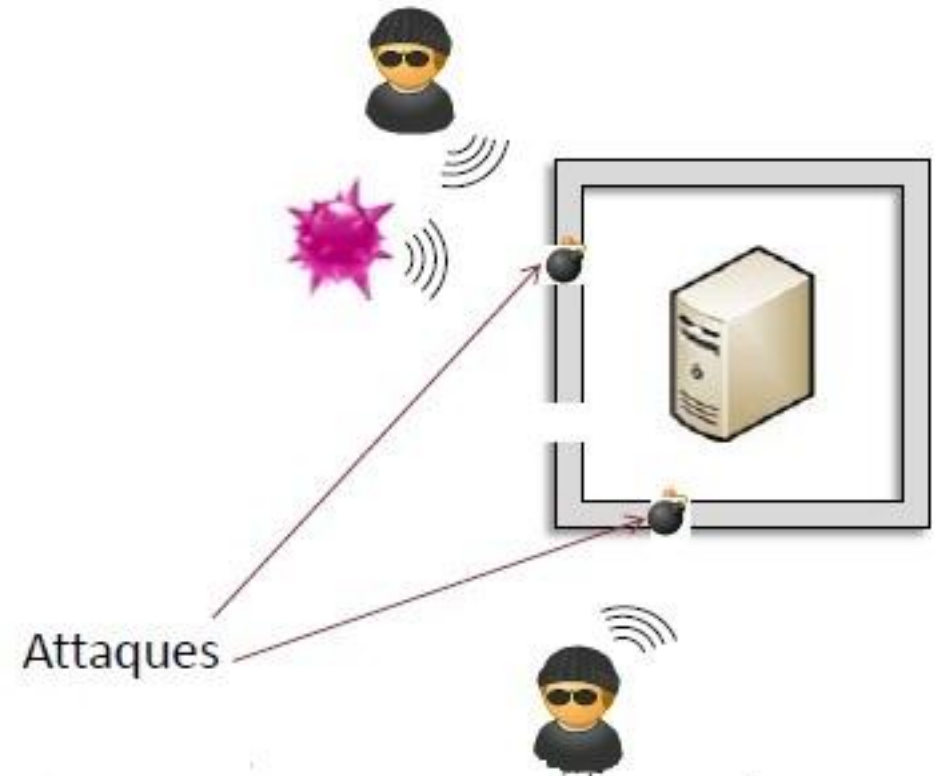
- Une cause potentielle d'incident, qui peut résulter en un dommage au système ou à l'organisation



Attaque

* Action **malveillante** qui tente **d'exploiter** une **faiblesse** dans le système et de violer un ou plusieurs besoins de sécurité (DICP)

* Une attaque n'a lieu que si le bien est affecté d'une vulnérabilité quelconque (**connue** ou **pas**) exploitable.



Exemple: vulnérabilité de type injection SQL

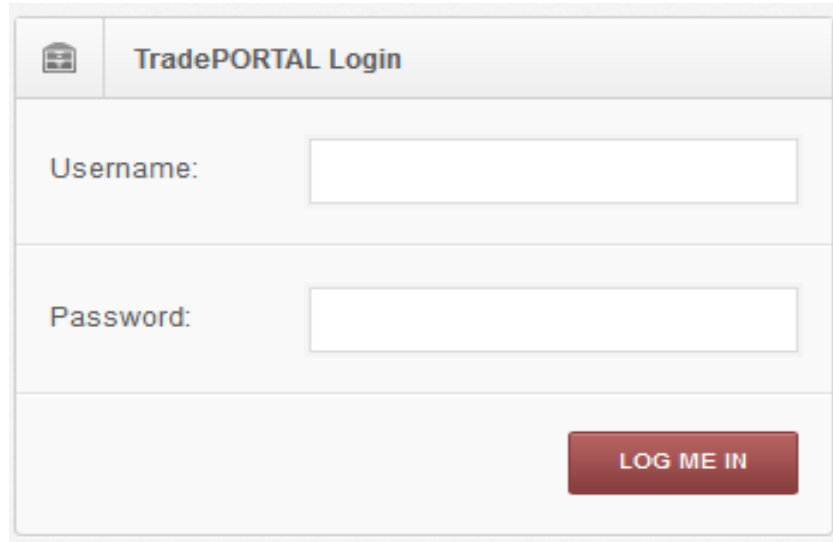
- Principe:

- Injecter une requête SQL mal formée et ceci en indiquant dans les paramètres (souvent les champs d'un formulaire) des données dont les valeurs n'ont pas été prévus par l'application
- Ceci est le plus souvent dû, du fait qu'il n'y a pas un contrôle au préalable du formatge correct des champs et l'interprétation des caractères spéciaux (', ", --)

- Risques encourus

- Bypasser une authentification
- Lire des données sensibles depuis les tables SQL
- Injecter le nom et le schéma de la base de données

Exemple: vulnérabilité de type injection SQL* (basique!)



```
01. // page processlogin.php
02. $username = $_POST['username'];
03. $password = $_POST['password'];
04. $sql = mysql_query("SELECT * FROM users WHERE username =
    '$_POST['username']' AND password = '$_POST['password']'") or die(mysql_error());
05. if(mysql_num_rows($sql) == 1)
06. {
07.     echo "Bienvenue $username dans votre espace membre!";
08. }
09. else
10. {
11.     echo "Nom d'utilisateur et/ou mot de passe incorrecte";
```

saisie login/mdp pour se connecter à un compte distant

Le client saisie **admin'--** dans Username et n'importe quoi dans Password

Script Php (côté serveur) récupérant les données du formulaire et interagissant avec le BDD via des requêtes SQL. Ainsi, la requête qui sera interprété (exécuté) est la suivante (on constate bien une injection au niveau de la requête SQL initiale)

```
SELECT * FROM users WHERE username = 'admin'--' AND password = '$password'
```

les caractères **'--** saisis (injectés) par l'utilisateur ont été interprétés comme faisant partie de la requête et non pas une partie de la chaîne \$username

* source: <http://www.mcherifi.org/hacking/tutoriel-sql-injection-les-classiques.html>
<https://codebashing.com/>