



Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Centre Universitaire de Mila
Institut des Sciences et de la Technologie



Administration des Réseaux

– Chapitre 4 – Sécurité des Réseaux – Partie 2

Département MI

s.meghzili@centre-univ-mila.dz



Plan du cours

1. Services cryptographiques

1. Chiffrement Asymétrique.
2. Protocole SSL/TLS
3. Signature Numérique
4. Certificat Numérique

2. Politique de sécurité

1. Pare-feu
2. Proxy
3. Traduction D'adresses : NAT
4. Zone Démilitarisée : DMZ
5. VPN & Protocole IPsec

3. Analyse et de Détection d'intrusion

1. Démarche
2. NMAP
3. Burp Suite
4. SQLmap
5. TCPdump
6. Wireshark
7. Snort
8. AcunetixWeb

Chiffrement Asymétrique

Les **problèmes de distribution des clés** sont résolus par la **cryptographie de clé publique** d'où Cryptographie **Asymétrique**

EXEMPLE

- Un ami doit vous faire parvenir un **message** très important par la poste, mais vous n'avez pas confiance en votre facteur que vous soupçonnez d'ouvrir vos lettres.
- **Alors!:**
 - Vous envoyez à votre ami un **cadenas** sans sa clé, mais en position **ouverte**.
 - Celui-ci glisse alors le message dans une boîte qu'il ferme à l'aide du cadenas, puis il vous envoie cette boîte.
 - Le facteur ne peut pas ouvrir cette boîte et surtout, la **clé n'a pas voyagé !**
 - La meilleure clé et la plus utilisée à ce jour, la cryptographie **RSA**.

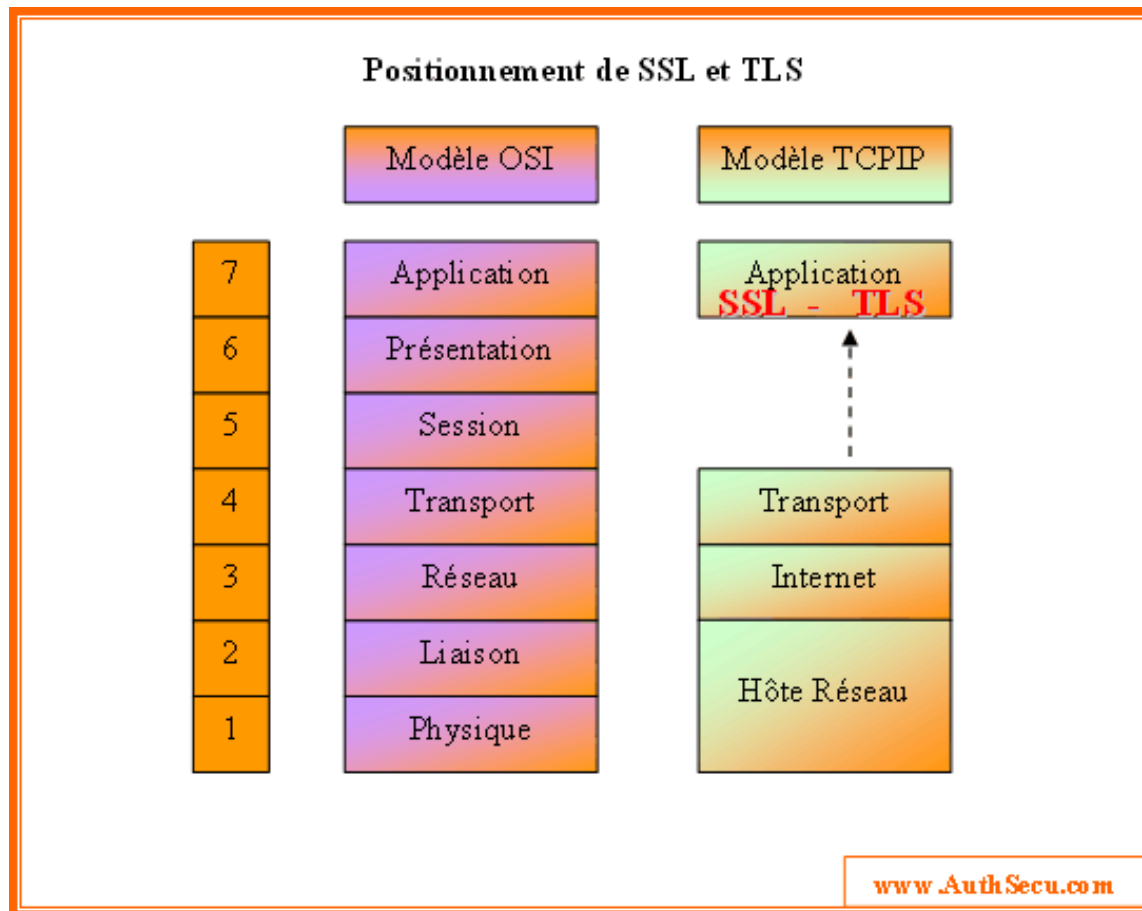
Protocole SSL/TLS (1)

- ❖ Le standard **SSL** (Secure Sockets Layers), ou couche de sockets sécurisée est un procédé de sécurisation des **transactions** effectuées via Internet.
- ❖ **SSL** a été mis au point par Netscape en **1994**, avec Mastercard, Bank of America, MCI et Silicon Graphics.
- ❖ **Principe**: consiste à établir un **canal** de communication **chiffré** entre deux machines (un client et un serveur) après une étape d'**authentification**.
- ❖ **TLS** (Transport Layer Security): est une **version récente** de SSL.

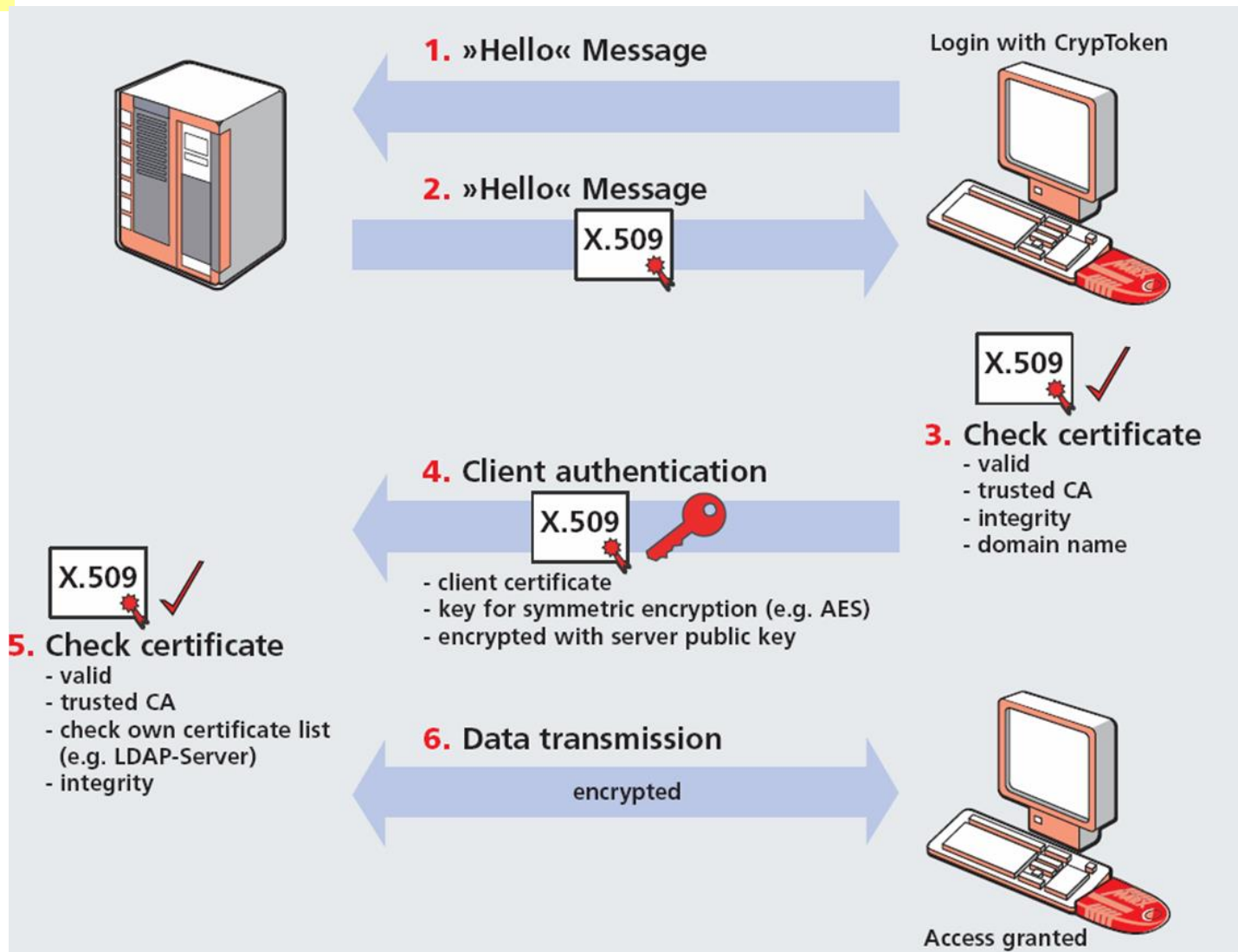
Protocole SSL/TLS (2)

- ❖ Le système **SSL** est indépendant du protocole utilisé,
- ❖ **SSL** peut aussi bien sécuriser des **transactions** faites sur le **Web** par le protocole **HTTP** que des connexions via le protocole **FTP**, **POP**...etc.
- ❖ Un serveur **web** sécurisé par **SSL** possède une URL commençant par **https://**, ou le "s" signifie **secured** (sécurisé).
- ❖ **SSL** utilise la cryptographie à clé publique, la cryptographie à clé **secrète**, et les **certificats électroniques**.

Protocole SSL/TLS (3)



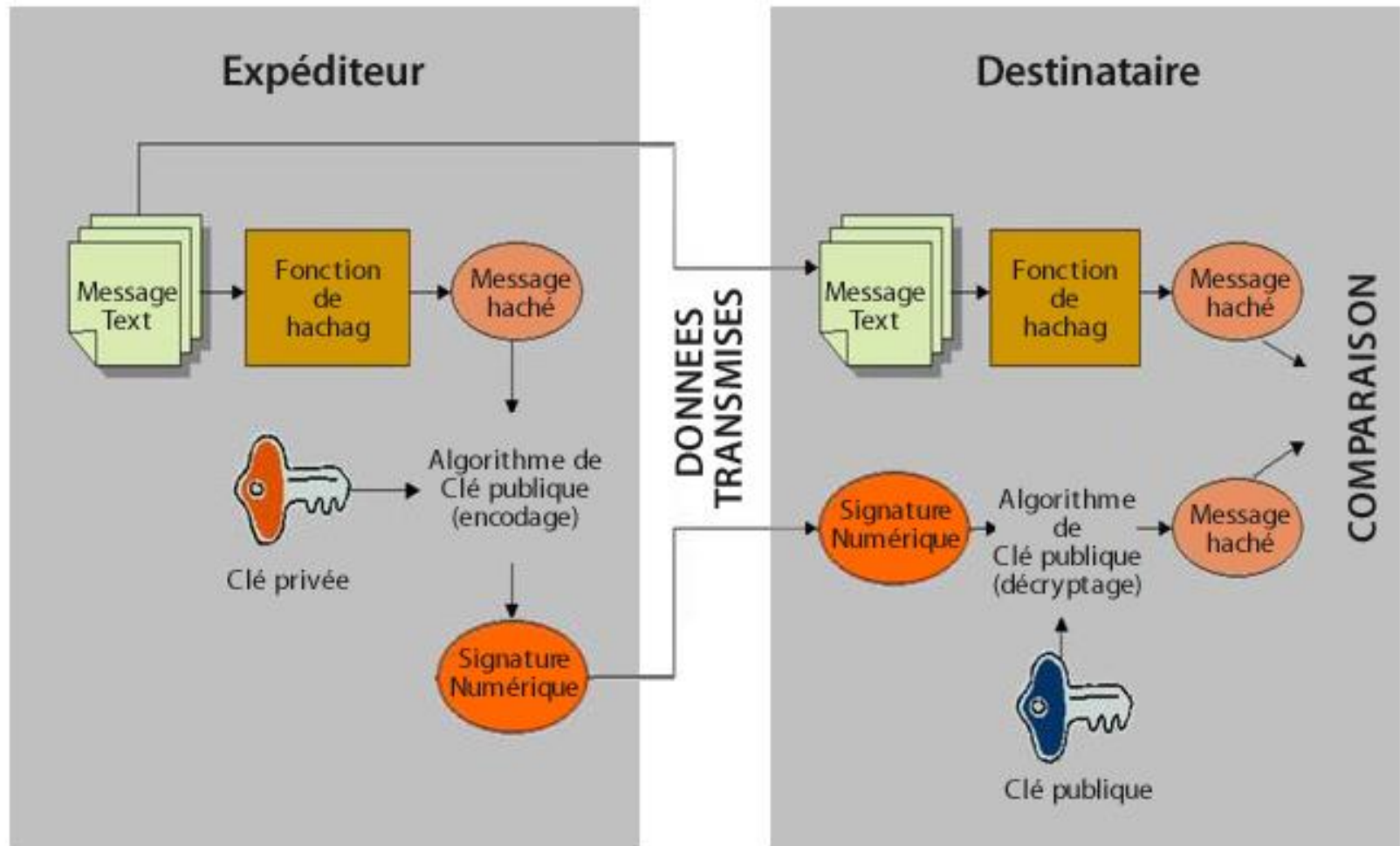
Mécanisme SSL : (4)



Signature Numérique (1)

- ❖ **Intégrité**: Il faut vérifier si le **message** n'a pas subi de **modification** durant la communication.
- ❖ Une **signature numérique** ou électronique a la même utilité qu'une signature **manuscrite**.
- ❖ Cependant, une signature manuscrite peut être facilement **imitée**, alors qu'une signature numérique est pratiquement **infalsifiable**.
- ❖ De plus, elle atteste du contenu des informations, ainsi que de l'identification du **signataire**. C'est ici qu'interviennent également les **fonctions de hachage**.

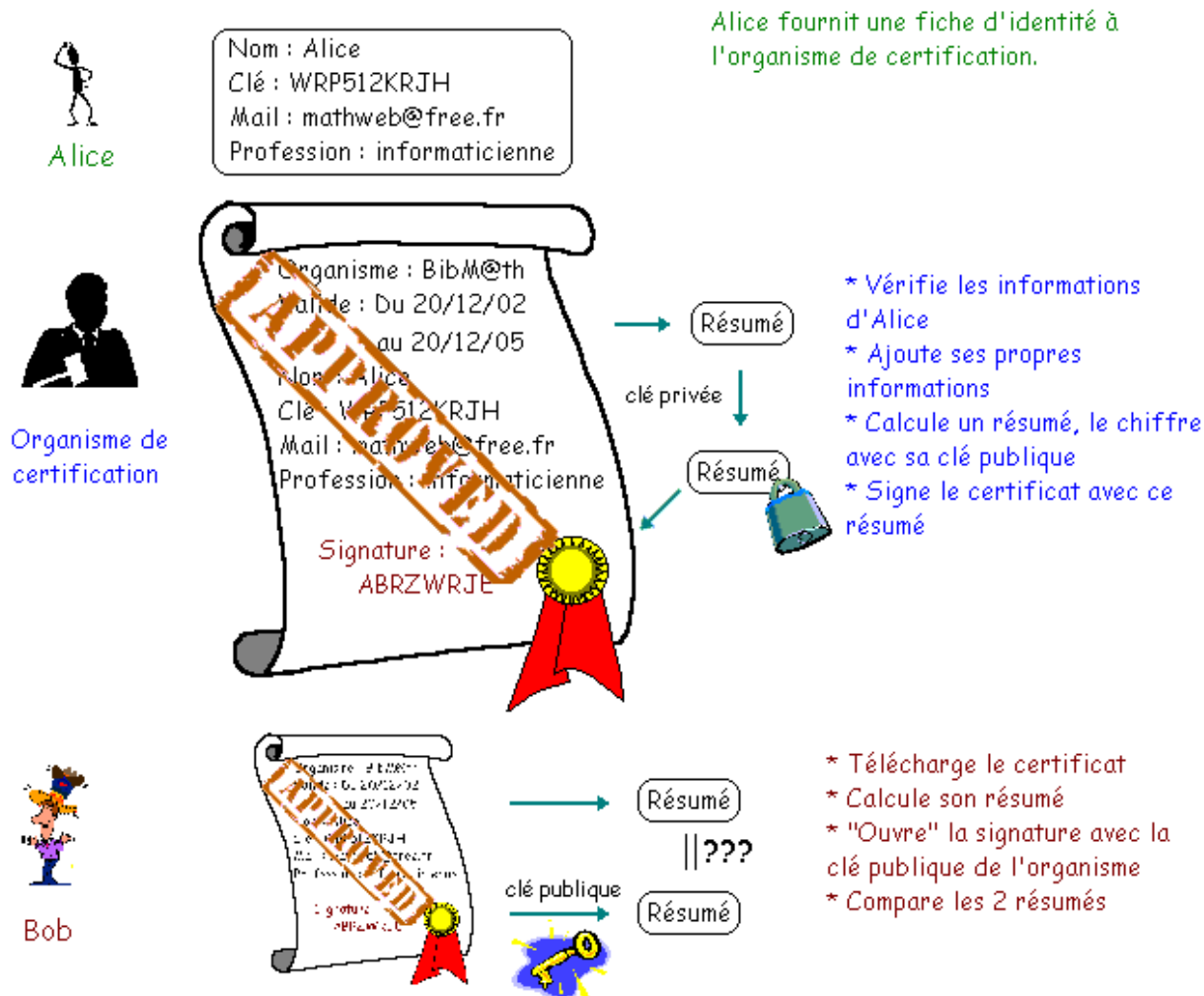
Signature Numérique (2)



Certificat Numérique (1)

- Un **certificat numérique** contient des données similaires à celles d'un certificat **physique**.
- Il contient des informations associées à la **clé publique** d'une personne, aidant d'autres personnes à vérifier qu'une clé est **authentique** ou **valide**.
- Il permet d'éviter les **tentatives** de **substitution** de la **clé** d'une personne par une autre.
- Un certificat **numérique** se compose de trois éléments :
 - Une **clé** publique.
 - Des **informations** sur le certificat. (Informations sur l'identité de l'utilisateur, telles que son **nom**, son **ID** utilisateur, etc.)
 - Une ou plusieurs **signatures** numériques.
 - Les deux formats les plus utilisés sont :
X.509 (RFC 5280) et **OpenPGP** (RFC 4880).

Certificat Numérique (2)



Certification numérique d'une clé publique

Certificat Numérique (3)

Autorité de certification des **sites web** open source:

- **ZeroSSL**
- **Let's Encrypt**
- **SSL For Free**
- **Cloudflare**

En Algérie.



الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
ⵜⴰⴷⵓⴷⴰ ⵜⴰⵎⴳⴷⴰⵢⵜ ⵜⴰⵖⴻⵔⴼⴰⵏⵜ ⵜⴰⵣⵣⴰⵢⵔⵉⵜ
السلطة الحكومية للتصديق الإلكتروني
Autorité Gouvernementale de Certification Électronique
ⵏⴰⵎⴰⵔⵉ ⵏⴰⵎⴰⵔⵉⵏ ⵏⴰⵎⴰⵔⵉⵏ ⵏⴰⵎⴰⵔⵉⵏ



Plan



1. Sécurisation des Données ou cryptographie
- 2. Politique de sécurité**
 1. Définition
 2. Pare-feu
 3. Proxy
 4. Traduction D'adresses : NAT
 5. Zone Démilitarisée : DMZ
 6. VPN & Protocole IPsec
3. Moyens d'Analyse et de Détection des Attaques

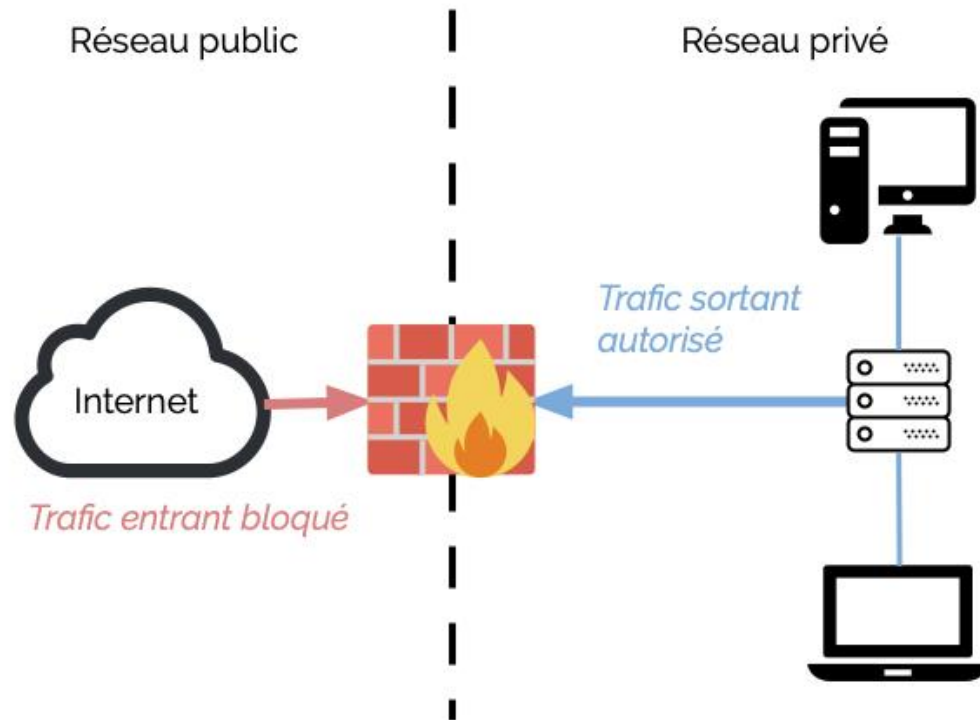


Politique de sécurité : Définition

- L'analyse des **informations** qui **circulent** ou qui sont **stockées** (analyse de leur importance pour l'entreprise, analyse du cout que représenterait leur perte),
- L'analyse des **menaces** que l'on peut objectivement envisager,
- La définition des **priorités** de l'entreprise et sa stratégie influent sur le choix des procédures internes que devront **respecter** tous les utilisateurs,
- La définition des **mécanismes de protection** à mettre en œuvre (les outils **antivirus**, les **pares-feu**, les **patches** ou programmes de correction).

Pare-feu (1)

- Le firewall (**matériel** ou **logiciel**) est chargé de filtrer les accès entre l'**Internet** et le **LAN** ou entre deux LANs.
- Il doit protéger les **accès** aux **applications** et aux **données** à l'intérieur du réseau d'entreprise.



Pare-feu (2)

- La localisation du firewall est **stratégique**, souvent c'est un **routeur** intégrant des fonctionnalités de **filtrage** appelé: Bastion, et possédant autant d'**interfaces** que de réseaux connectés.
- Il fonctionne principalement grâce à un ensemble de **règles** définissant les connexions **autorisées** (allow ou permit) et **interdites** (deny).
- Le pare-feu peut **rejeter** une demande extérieure, sans prévenir l'utilisateur concerné (drop).
- Le pare-feu exécute son filtrage sur chaque requête **entrante** ou **sortante** du trafic inter-réseaux.

Pare-feu (3)

Le filtrage effectué par un **pare-feu** peut porter sur:

- Adresses **MAC** source ou destination
- Adresses IP source ou destination
- Ports TCP ou UDP source ou destination
- Flags de l'en-tête **TCP** (SYN, ACK, ...)
- Type de message **ICMP**; le type de message ou le contenu **HTTP**, **SMTP**, **POP**..

Proxy (1)

- Un **Proxy** server joue le rôle de **mandataire** pour les autres machines locales et exécute les requêtes pour le **compte** de ces dernières.
- Un serveur **mandataire** est configure pour un ou plusieurs protocoles de niveau applicatif (http, ftp...) et permet de **sécuriser** les accès **extérieurs** (**filtrage** applicatif, **masquage** des @ des clients, **enregistrement** des connexions, ...).
- Les proxys configure pour **http** permettent le stockage des **pages web** dans un cache pour accélérer le transfert des informations fréquemment consultées vers les clients connectes.

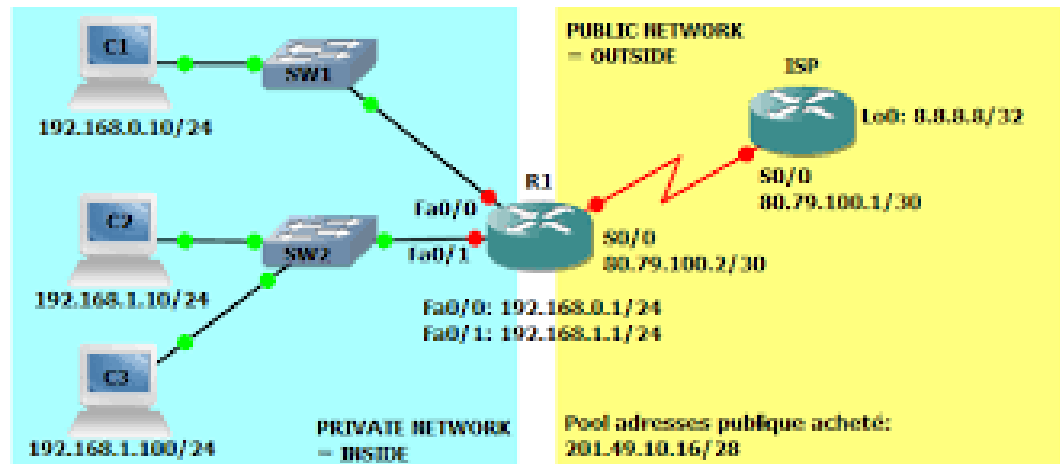


Proxy: avantages (2)

- Avoir un **point** de passage obligé permettant de bien vérifier si les **règles de sécurité** spécifiées dans la politique sécurité sont bien **appliquées**,
- **Auditer/tracer** de façon "centrale" ce trafic entre le réseau **interne** et **externe** peut aider à prévoir les évolutions du réseau (statistiques possibles),
- Eventuellement d'avoir une vue de la **consommation** Internet des différents **utilisateurs/services**
- Possibilité de mettre en œuvre des **outils** spécifiques que l'on ne pourrait **activer** sur tous les systèmes (exemple : systèmes d'**authentification** à mots de passe uniques, **statistiques/comptabilité**, etc.),

Traduction D'adresses : NAT

- Network Address Translation :est un dispositif de sécurité complémentaire au **filtrage**
- La NAT masque les adresses **privées**; par conséquent plus visibles de l'extérieur.
- Est apparue à l'origine pour palier au **manque** croissant d'adresses **IPv4** publiques.
- Partager une connexion **NAT** permet de relier plusieurs machines à Internet (ou à un autre réseau) au travers d'une **seule machine** (la passerelle).



Zone Démilitarisée : DMZ (1)

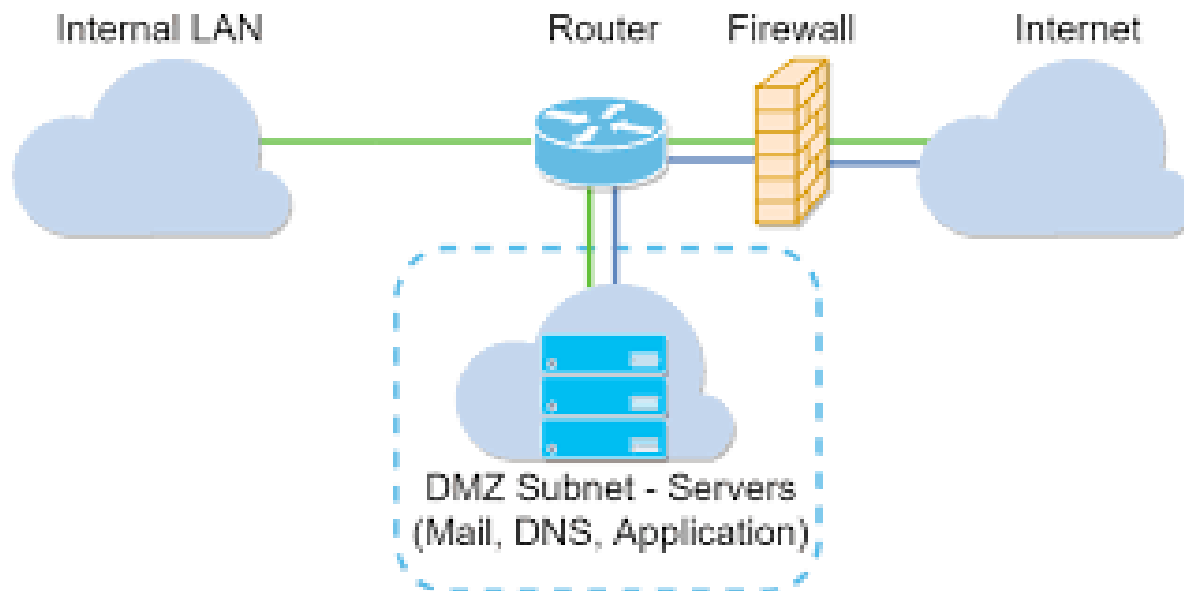


- **DMZ** est une zone de réseau **privée** ne faisant partie ni du **LAN** privé ni de l'**Internet**.
- A la manière d'une zone franche au-delà de la frontière, la **DMZ** permet de **regrouper** des **ressources** nécessitant un niveau de protection intermédiaire.
- Comme un réseau privé, elle est isolée par un firewall mais avec des règles de filtrage moins contraignantes.

Zone Démilitarisée : DMZ (2)

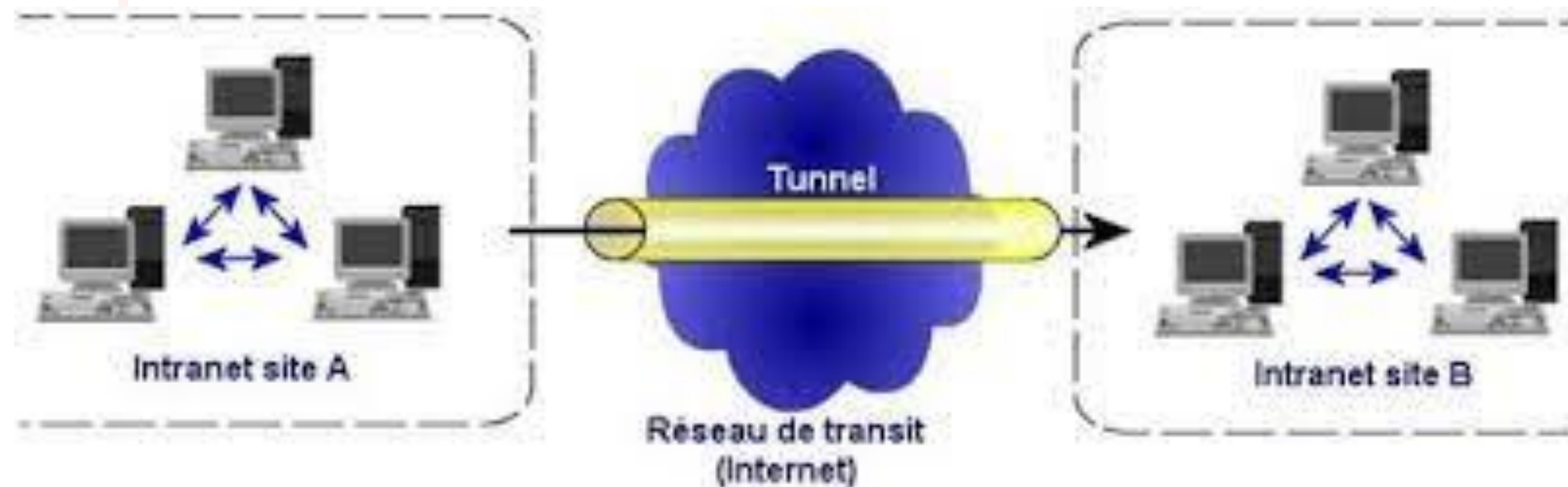
Objectif:

On utilise une **DMZ** pour rendre accessible depuis l'extérieur un ensemble de **services** tels que serveur de **messagerie**, serveur **FTP**, portail **Web**...



VPN & Protocole Ipsec (1)

- VPN est une technologie ayant pour but d'établir une communication **sécurisée** (tunnel) entre des entités éloignées, séparées par un réseau non sécurisé voire **public** (Internet) d'une manière **quasi-transparente**.
- Les postes **distants** faisant partie du même **VPN** communiquent de manière sécurisée comme s'ils étaient dans le même espace **privé**, mais celui-ci est **virtuel**.





VPN & Protocole Ipsec (2)

Quelques propriétés générales des tunnels destinés aux VPNs :

- Les données transitant sont **chiffrées** (confidentialité) et **protégées** (intégrité),
- Les **2** extrémités sont **authentifiées**,
- Les adresses sources et destinations sont chiffrées, avec **IPSec**.
- ils peuvent présenter, suivant le protocole, des qualités anti-re-jeux ou **empêcher** les attaques type **man-in-the-middle**

VPN & Protocole Ipsec (3)

Principe de fonctionnement

Une connexion VPN met en jeu les composants suivants:

- **Serveur VPN:** ordinateur qui accepte les connexions **VPN** et peut fournir une connexion Routeur-Routeur.
- **Client VPN:** ordinateur qui **initie** une connexion VPN vers un serveur VPN.
- **Tunnel:** la partie de la connexion ou les **paquets** sont **encapsulés** et **cryptés** basé sur les concepts suivants:
 - *Tunnelisation,*
 - *Chiffrement,*
 - *Authentification.*

VPN & Protocole Ipsec (4)

- **IPSec** (Internet Protocol Security, RFC 2401) est un protocole de la couche **3** du modèle **OSI** offrant différents **services** de sécurité tels que le **chiffrement** et l'**authentification**...etc.
- Il fut, à l'origine, développé pour le protocole **IPv6**. Comme IPv6 n'est pas encore déployé à grande échelle, alors **IPSec** a été porté vers la version actuelle **IPv4**.
- Il propose plusieurs choix et options qui lui permettent de répondre de façon adaptée aux besoins des **entreprises**, nomades, extranets, etc...
- Son intérêt principal est le mode **tunneling** (encapsulation d'IP) qui lui permet de créer des **VPNs**.

VPN & Protocole Ipsec (5)

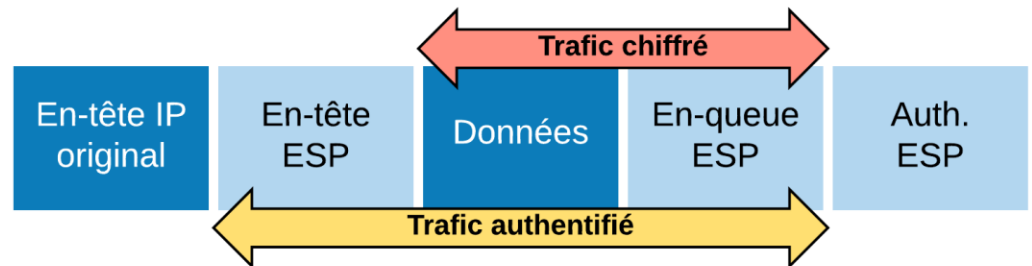
- Les **échanges** de données via **IPsec** s'appuient essentiellement sur **2** protocoles différents suivant les besoins en sécurité des utilisateurs.
 - **AH** (Authentication Header), qui vise à établir l'identité des extrémités de façon certaine (en **signant** les paquets). Il **ne garantit** aucune confidentialité des données.
 - **ESP** (Encapsulating Security Payload), pour le **chiffrement** des données (confidentialité). Il garantit également l'**authenticité** des données (une redondance par rapport à AH).
 - Ces **2** protocoles, **AH** et **ESP**, peuvent être utilisés **séparément** ou **combinés**,

VPN & Protocole Ipsec (6)

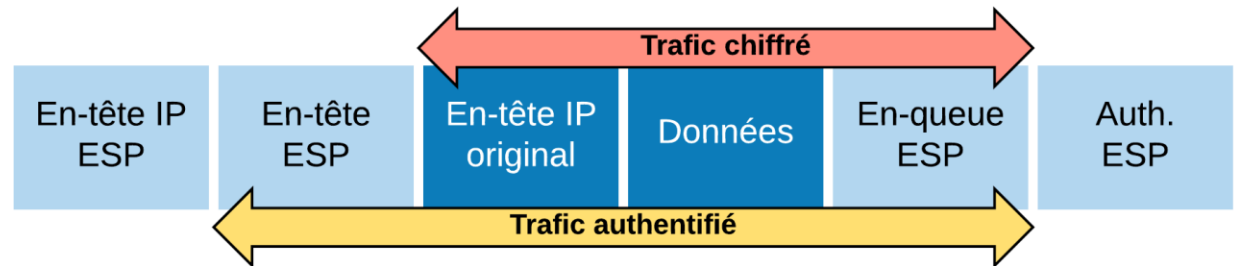
Paquet original



IPSEC (ESP)
mode transport



IPSEC (ESP)
mode tunnel



Intérêt Ipsec (7)

- Un datagramme **IPSec** circule avec les adresses des passerelles des extrémités du **tunnel** en **encapsulant** ceux des utilisateurs d'un **site** à l'autre.
- Il est ainsi impossible de **connaître** les adresses **IP internes** en **espionnant** le trafic sur **Internet**.
- L'intérêt de la solution des **IPSec tunnels** réside dans la **transparence** vis-à-vis les utilisateurs. Aucun **logiciel** n'est nécessaire sur leurs machines.
- Via le mode **IPSec Transport**, les utilisateurs mobiles peuvent se connecter sans la passerelle et il faut installer un logiciel **client** spécifique pour gérer les paramètres de **sécurité**, le **chiffrement** et calculer les **signatures**.

Plan



1. Sécurisation des Données ou cryptographie
2. Politique de sécurité
- 3. Analyse et de Détection des intrusions**
 1. Démarche
 2. NMAP
 3. Burp Suite
 4. SQLmap
 5. TCPdump
 6. Wireshark
 7. Snort
 8. AcunetixWeb

Analyse et de Détection des intrusions

Principe: La meilleure **défense** est l'**attaque** !

- **Test d'intrusion** "penetration test" ou "**pentest**" est une méthode d'**évaluation** de la sécurité d'un système ou d'un réseau informatique,
- Consiste à **simuler** une attaque d'un pirate, voire d'un logiciel malveillant.
- On détermine alors les **risques** potentiels dus à une **mauvaise configuration** d'un système, d'un **défaut de programmation** ou encore d'une **vulnérabilité** liée à la solution testée.
- Son **intérêt** est d'apporter des **corrections** et **rectifications** par l'introduction des moyens adéquats pour une meilleur sécurisation.

Analyse et de Détection des intrusions

TYPES DE TESTS

Black box



**Aucune information
fournie avant le test**

- Le test le plus réaliste
- Simule le scénario d'une attaque réelle de hacker, à "l'aveugle"

Grey box



**Quelques informations
fournies avant le test**

- Accès à des informations partielles telles que les adresses IP, les identifiants utilisateurs
- Tentatives d'escalade des niveaux d'accès (utilisateur, administrateur...)

White box



**Toutes les informations
sont fournies avant le
test**

- Connaissance des données internes du système cible
- Informations telles que les diagrammes de réseau, les identifiants de connexion...
- Test précis et rigoureux
- Simule une attaque en interne / la fuite d'informations sensibles

Analyse et de Détection des intrusions: Demarche (1)

A La phase préparatoire

- 1 collecte d'informations publiques
Whois
- 2 cartographie du réseau cible
Nmap / Siphon / Dsniff / finger
- 3 identification des vulnérabilités
**Nessus / Internet Scanner
SARA / SAINT / Retina**
- 4 consolidation des informations



B La phase de réalisation

- 1 conception des attaques
- 2 exécution des scenarii
 - intrusion -
**Netcat / finger / rusers / Exploit
Sniffer/ Tcpdump / Siphon
Ethereal**
 - élévation des privilèges -
John the ripper / Exploit / Dsniff
- 3 consolidation des données



C La phase de restitution

- 1 synthèse des données obtenues
- 2 définition d'un plan d'actions correctrices
- 3 présentation des résultats

NMAP (1)

- **Network Mapper (Nmap)** est un **scanner de ports**, libre créé par Fyodor et distribué par Insecure.org,
- Il sert à scanner, explorer et réaliser un **audit** ou un inventaire matériel de grands réseaux, Conçu pour détecter les **ports ouverts**, identifier les **services hébergés** et obtenir des informations sur le **système d'exploitation** d'un ordinateur distant,
- Est une **référence** pour les administrateurs réseau pour réaliser un **audit** de sécurité sur tout les éléments du réseau,
- Il est disponible pour toutes les plateformes,
- Est doté une **interface graphique** fonctionnelle (**Zenmap** ou **NMapWin**) donne **accès** visuel à de très nombreuses **informations** et les sauvegarde dans un fichier.

NMAP (2)

The screenshot displays the Zenmap interface for Nmap. At the top, the 'Target' field contains 'www.google.com www.facebook.com twitt' and the 'Command' field shows 'nmap -T4 -A -F -PN www.google.com www.facebook.com twitter.com microsoft.com insecure.org slashdot.org craigslist.o'. The 'Topology' tab is selected, showing a network graph with nodes representing IP addresses and hostnames, connected by lines. A sidebar on the left lists the scanned hosts, including '72.51.26.227', 'www.03.01.ash1.t', 'mh-in-f99.google.', '128.121.146.100', 'www.defcon.org', 'www.craigslist.org', 'www.blackhat.cor', '207.46.232.182', 'youtube.com (208', 'rr.pmtpa.wikimedi', 'insecure.org (64.1', 'slashdot.org (216', and 'scanme.nmap.org'. The right sidebar contains controls for 'Action', 'Interpolation' (Frames: 60, Polar selected), 'Layout', and 'View' (address, hostname, icon checked). Navigation and zoom controls are at the bottom right.

OS	Host
	72.51.26.227
	www.03.01.ash1.t
	mh-in-f99.google.
	128.121.146.100
	www.defcon.org
	www.craigslist.org
	www.blackhat.cor
	207.46.232.182
	youtube.com (208
	rr.pmtpa.wikimedi
	insecure.org (64.1
	slashdot.org (216
	scanme.nmap.org

NMAP (3)

Exemples de tests:

- Voir les ports **TCP ouverts** (pas de log sur la machine cible car utilisation de message SYN):
nmap -sS 192.168.1.39
- Voir les ports **UDP ouverts**: **nmap -sU 192.168.1.39**
- Connaître le **nom** du **système** d'exploitation du PC distant:
nmap -O 192.168.1.39
- Usurper une adresse IP: Pour scanner **192.168.1.33** par l'interface **eth1** (locale) en se faisant passer pour **192.168.15.15** depuis le **port 80**:
nmap -S 192.168.15.15 -g 80 -e eth1 -P0 192.168.1.33

Burp Suite (1)

- **Burp Suite** est une application, développée par PortSwigger Ltd, qui peut être utilisée pour la sécurisation ou effectuer des **tests de pénétration** sur les **applications web**.
- Peut être utilisée comme un serveur **proxy**, afin de manipuler le **trafic** qui le traverse, entre le **navigateur web** et le **serveur** (MITM).
- Grâce à cette fonctionnalité, il est possible d'**injecter** des **données non-conformes** afin de provoquer un comportement **anormal** de l'application et donc d'en identifier les **bugs** et **vulnérabilités** associées.
- **Outil d'intrusion**: offre la possibilité de créer des requêtes **HTTP nuisible** pour l'application. Il peut également aider à la détection des **injections SQL**.

Burp Suite (2)

The screenshot displays the Burp Suite Free Edition v1.6 interface. The top menu bar includes 'Browse and run installed applications', 'Burp Intruder Repeater Window Help', and standard window controls. Below the menu is a toolbar with buttons for 'Target', 'Proxy', 'Spider', 'Scanner', 'Intruder', 'Repeater', 'Sequencer', 'Decoder', 'Comparer', 'Extender', 'Options', and 'Alerts'. A secondary toolbar contains 'Site map' and 'Scope' buttons. A filter bar indicates: 'Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders'. The main interface is split into two panes. The left pane shows a 'Site map' with a list of URLs, including 'http://192.168.0.160' which is highlighted. A red annotation 'Sitemap & outbound Links' points to this list. The right pane shows a table of requests. A red annotation 'Requests' points to this table. The selected request is for 'http://192.168.0.160' with method 'GET' and URL '/jquery.min.js'. Below the table, the 'Request' tab is active, showing the raw request details. A red annotation 'Request/Response Details' points to this section.

Site map & outbound Links

Host	Method	URL	Params	Stat...	Length	MIME type	Title
http://192.168.0.160	GET	/animatedcollapse.js		200	12338	script	
http://192.168.0.160	GET	/jquery.min.js		200	57770	script	
http://192.168.0.160	GET	/AppSensorDemo/				HTML	
http://192.168.0.160	GET	/ESAPI-java-SwingSe...				HTML	
http://192.168.0.160	GET	/OWASP-CSRFGuard-...				HTML	
http://192.168.0.160	GET	/WackoPicko				HTML	
http://192.168.0.160	GET	/WebGoat/attack				HTML	
http://192.168.0.160	GET	/awstats/awstats.pl				HTML	
http://192.168.0.160	GET	/awstats/awstats.pl?...	<input checked="" type="checkbox"/>			HTML	
http://192.168.0.160	GET	/bodgeit/				HTML	
http://192.168.0.160	GET	/cyclone/				HTML	

Request/Response Details

Request: GET /jquery.min.js HTTP/1.1
Host: 192.168.0.160
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close

Burp Suite (3)

La suite Burp incorpore les composants suivants :

- Un **proxy local** (en mode interception) qui va permettre d'inspecter et modifier le **trafic** entre votre **navigateur** (firefox, chrome, etc.) et l'**application cible**.
- Un scanner d'applications **Web** performant.
- Un outil (spider/crawler) permettant de récupérer les **champs** d'une **page Web** dans le but de modifier certains **paramètres**,
- Un outil d'**intrusion**, pour effectuer des **attaques** spécifiques afin de trouver et d'exploiter des **vulnérabilités**.
- Un outil de **répétition** permettant la modification avant l'envoi de vos requêtes.
- Un **séquenceur** pour tester la randomisation des sessions avec **jetons** (token).

SQLmap (1)

- **SQLmap** permet d'effectuer automatiquement des **requêtes SQL** pour détecter les **vulnérabilités** d'un serveur **Web**.
- Il essaye trouver des **injections** possibles au travers des champs **HTTP** (méthodes **GET** et **POST**) à partir d'une **URL** contenant un **caractère invalide**,
- Identification des composants de la cible (**OS, SGBD...**) afin de récupérer des **données** telles que le **nom des tables**, les **logins**, les **mots de passe** ou de prendre le **contrôle** du système.
- Globalement, il permet d'automatiser des **attaques** très complexes ("bruteforce") nécessitant des centaines de requêtes pour obtenir les **informations** dans la **BDD** visée.

SQLmap (2)

Une fois le **site cible** est trouvé; on peut effectuer:

- Pour découvrir le **SE**, le serveur **Web** et la **BDD** de la cible:
*python sqlmap.py -u " **adresse-ip**"*
- Pour récupérer le nom de la **BDD** cible:
*python sqlmap.py -u " **adresse-ip**" -dbs*
- Pour afficher la **liste** des **tables**:
*python sqlmap.py -u " **adresse-ip**" -tables -D nom BDD*
- Pour afficher le **contenu** d'une **table**:
*python sqlmap.py -u " **adresse-ip**" ?dump -D nom BDD
-T nom table*

TCPdump

Outil en ligne de commande permettant d'écouter le réseau:
#tcpdump-uw -i INTERFACE-NUMBER -n -s0

```
192.168.214.103 - PuTTY
~ # tcpdump-uw -i 1 -n -s0
tcpdump-uw:
listening on vmk0, link-type EN10MB (Ethernet),
17:58:30.886164 IP 192.168.214.44.49658 > 192.168.214.103.22
17:58:30.886723 IP 192.168.214.103.22 > 192.168.214.44.49658
17:58:30.886932 IP 192.168.214.103.22 > 192.168.214.44.49658
17:58:30.887602 IP 192.168.214.44.49658 > 192.168.214.103.22
17:58:30.888042 IP 192.168.214.103.22 > 192.168.214.44.49658
17:58:30.888615 IP 192.168.214.44.49658 > 192.168.214.103.22
```

Timestamp **Sender IP** **Destination IP**

Sender TCP port number **Server TCP port number**

Wireshark

logiciel **open-source** permettant la **capture** et l'**analyse** de **trafic** réseau en mode graphique.

The screenshot displays the Wireshark interface with a packet capture of a test.pcap file. The main pane shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, and Info. The selected packet (No. 17) is a TCP SYN packet from 192.168.0.1 to 192.168.0.2 on port 5000. The bottom pane shows the detailed view of this packet, including its identification (0x1847), flags (0x00), and header checksum (0xa109). The packet bytes are shown in hexadecimal and ASCII format.

No.	Time	Source	Destination	Protocol	Info
3	0.023217	192.168.0.2	192.168.0.1	ICMP	Destination unreachable (port un...
4	1.025659	192.168.0.2	igmp.mcast.net	IGMP	V3 Membership Report
5	1.044366	192.168.0.2	192.168.0.1	DNS	Standard query SRV _ldap._tcp.nbg
6	1.048652	192.168.0.2	239.255.255.250	UDP	Source port: 3193 Destination po
7	1.050784	192.168.0.2	192.168.0.1	DNS	Standard query SOA nb10061d.wm004
8	1.055053	192.168.0.1	192.168.0.2	UDP	Source port: 1900 Destination po
9	1.082038	192.168.0.2	192.168.0.255	NBNS	Registration NB NB10061D<00>
10	*REF*	192.168.0.2	192.168.0.1	DNS	Standard query A proxyconf.wm004.
11	0.114211	192.168.0.2	192.168.0.1	TCP	3196 > http [SYN] Seq=0 Len=0 MSS
12	0.115337	192.168.0.1	192.168.0.2	TCP	http > 3196 [SYN, ACK] Seq=0 Ack=
13	0.115380	192.168.0.2	192.168.0.1	TCP	3196 > http [ACK] Seq=1 Ack=1 Win
14	0.115506	192.168.0.2	192.168.0.1	TCP	3196 > http [PSH, ACK] Seq=1 Ack=
15	0.117364	192.168.0.1	192.168.0.2	TCP	http > 3196 [ACK] Seq=1 Ack=256 W
16	0.120476	192.168.0.1	192.168.0.2	TCP	[TCP Window Update] http > 3196 [
17	0.136410	192.168.0.1	192.168.0.2	TCP	1025 > 5000 [SYN] Seq=0 Len=0 MSS

Identification: 0x1847 (6215)
Flags: 0x00
Fragment offset: 0
Time to live: 128
Protocol: UDP (0x11)
Header checksum: 0xa109 [correct]
Source: 192.168.0.2 (192.168.0.2)
Destination: 192.168.0.1 (192.168.0.1)

```
0000 00 09 5b 2d 75 9a 00 0b 5d 20 cd 02 08 00 45 00  ..[-u... ] ....E.  
0010 00 49 18 47 00 00 80 11 a1 09 c0 a8 00 02 c0 a8  ..I.G... ..  
0020 00 01 0b d2 00 35 00 35 46 69 00 21 01 00 00 01  .....5.5 Fi.!...  
0030 00 00 00 00 00 00 09 70 72 6f 78 79 63 6f 6e 66  .....p roxyconf  
0040 05 77 77 30 30 34 07 73 69 65 6d 65 6e 73 03 6e  ..wm004.s iemens.n  
0050 65 74 00 00 01 00 01  et.....
```

File: "D:/test.pcap" 14 KB 00:00:02 | P: 120 D: 120 M: 0

Snort & ACID

Système de **détection d'intrusion** libre publié sous licence GNU GPL

The screenshot shows a Mozilla browser window displaying the ACID Query Results page. The browser's address bar shows the URL `http://localhost/acid/acid_qry_main.php`. The page title is "ACID Query Results".

At the top of the page, there are navigation links for "Home", "Search", and "AG Maintenance", along with a "[Back]" link. Below this, a message states "Added 0 alert(s) to the Alert cache".

The "Queried DB on" section shows the query time as "Thu January 09, 2003 11:58:25". A table of criteria is displayed:

Meta Criteria	time >= [01 / 08 / 2003] [09 : * : *]
IP Criteria	any
Layer 4 Criteria	none
Payload Criteria	any

A "Summary Statistics" box on the right lists the following items:

- Sensors
- Unique Alerts (classifications)
- Unique addresses: source | destination
- Unique IP links
- Source Port: TCP | UDP
- Destination Port: TCP | UDP
- Time profile of alerts

Below the statistics, it says "Displaying alerts 101-128 of 128 total". A table of alerts is shown with the following columns: ID, Signature, Timestamp, Source Address, Dest. Address, and Layer 4 Proto.

ID	Signature	Timestamp	Source Address	Dest. Address	Layer 4 Proto
<input type="checkbox"/> #100-(4-75426)	WEB-IIS cmd.exe access	2003-01-09 05:58:30	195.70.42.41:62195	192.168.1.20:80	TCP
<input type="checkbox"/> #101-(4-75427)	WEB-IIS cmd.exe access	2003-01-09 05:58:31	195.70.42.41:62207	192.168.1.20:80	TCP
<input type="checkbox"/> #102-(4-75428)	WEB-IIS cmd.exe access	2003-01-09 05:58:31	195.70.42.41:62217	192.168.1.20:80	TCP
<input type="checkbox"/> #103-(4-75429)	WEB-IIS cmd.exe access	2003-01-09 05:58:32	195.70.42.41:62228	192.168.1.20:80	TCP
<input type="checkbox"/> #104-(4-75430)	WEB-IIS cmd.exe access	2003-01-09 05:58:33	195.70.42.41:62241	192.168.1.20:80	TCP
<input type="checkbox"/> #105-(4-75431)	WEB-IIS cmd.exe access	2003-01-09 05:58:33	195.70.42.41:62251	192.168.1.20:80	TCP

The browser's status bar at the bottom indicates "Document: Done (7.431 secs)".

AcunetixWeb

Ensemble d'outils permettant d'augmenter la sécurité des sites Web en assurant l'analyse des contenus JavaScript et la sécurité d'Ajax et du web 2.0. Il permet de scanner les requêtes SQL et SQL Injection, ainsi que le CSS.

The screenshot displays the Acunetix Web Vulnerability Scanner (Consultant edition) interface. The main window shows a list of scan results for a target URL: `http://testphp.acunetix.com/00/`. The results are categorized into Alerts (140) and Site Structure. The Alerts list includes:

- Apache Mod_Rewrite Off-By-One Buffer Overflow Vu...
- PHP version older than 4.4.1 (1)
- PHP Zend_Hash_Del_Key_Or_Index vulnerability (1)
- PHP HTML Entity Encoder Heap Overflow Vulnerabil...
- Unfiltered Header Injection in Apache 1.3.34(2.0.57)...
- Cross Site Scripting (94)
- SQL injection (16)
- Apache version older than 1.3.34 (1)
- Cookie manipulation (1)
- User credentials are sent in clear text (2)
- Broken links (1)
- Hidden form input named price was found (7)
- Apache version up to 1.3.37 has a local overflow...
- TRACE Method Enabled (1)
- Application error message (23)

The Site Structure shows a directory listing for `/` with files like `ajax`, `flash`, `images`, `secured`, `artists.php`, `cart.php`, `categories.php`, `donation.php`, `favicon.ico`, `guestbook.php`, `index.php`, and `interstate.php`.

The detailed view of the SQL Injection vulnerability is shown in a red-bordered window titled "SQL Injection". It includes the following sections:

- Vulnerability description:** This script is possibly vulnerable to SQL injection attacks. SQL injection is a vulnerability that allows an attacker to alter backend SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.
- Impact:** This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.
- Affected files:** This vulnerability affects `artists.php`.
- The impact of this vulnerability:** An attacker may execute arbitrary SQL statements on the vulnerable system. This may compromise the integrity of your database and/or expose sensitive information.
- Attack details:** The GET variable `artist` has been set to `%00'`.

The status bar at the bottom indicates "Scanning 1 website(s)..." and "Number of websites left to scan: 1".

Références

- Réseaux, Andrew Tanenbaum, InterEditions