RÉSEAUX ET SÉCURITÉ INFORMATIQUES

MICKAËL CHOISNARD
UNIVERSITÉ DE BOURGOGNE

Cours MIGS 2 novembre 2015

INTRODUCTION

La sécurité de ma machine, je m'en fous : y'a rien de précieux sur ma machine... personne n'a intérêt à me pirater !

J'ai Linux, donc je suis tranquille niveau sécurité

Attaque ssh sur serveur kundera sur 24h

root (1.93.26.17): 62 Time(s)
unknown (static.35.185.76.144.clients.your-server.de): 48 Time(s)
unknown (hr-ams-004.multiplay.co.uk): 32 Time(s)
root (61.174.50.252): 16 Time(s)
unknown (95.211.205.193): 8 Time(s)
root (61.174.51.216): 6 Time(s)
root (122.225.109.100): 3 Time(s)
root (195-154-211-26.rev.poneytelecom.eu): 3 Time(s)
unknown (106.120.78.169): 3 Time(s)
unknown (111.93.147.197): 3 Time(s)
unknown (189.58.106.82): 3 Time(s)
unknown (host186-214-static.29-79-b.business.telecomitalia.it): 3 Time(s)
root (122.225.109.200): 2 Time(s)
unknown (103.27.236.39): 2 Time(s)
unknown (220.130.143.67): 2 Time(s)
bin (115.238.55.163): 1 Time(s) licence2 (iem-252.rp.u-bourgogne.fr): 1 Time(s)
root (103.27.236.39): 1 Time(s)
root (122.225.109.112): 1 Time(s)
root (122.225.109.123): 1 Time(s)
root (61.174.51.218): 1 Time(s)
unknown (14.164.145.137): 1 Time(s)
unknown (187.12.251.54): 1 Time(s)

La sécurité porte sur

- Les informations
- Le système
- Le réseau

Technique d'attaque et d'intrusion

- Attaque : n'importe quelle action qui compromet la sécurité des informations.
- Intrusion : Prise de contrôle partielle ou totale d'un système distant.
- Description d'une attaque :
  - Recherche d'informations : réseau, serveurs, routeurs, . . .
  - Recherche de vulnérabilités : système d'exploitation, serveurs applicatifs, . . .
  - Tentative d'exploitation des vulnérabilités à distance puis localement
  - Installation de backdoor (passage secret, cheval de troie)
  - Installation de sniffer (analyseur de trames)
  - Suppression des traces.
  - Attaque par déni de service (DoS).

But des attaques

Source

Destination

Situation Normale

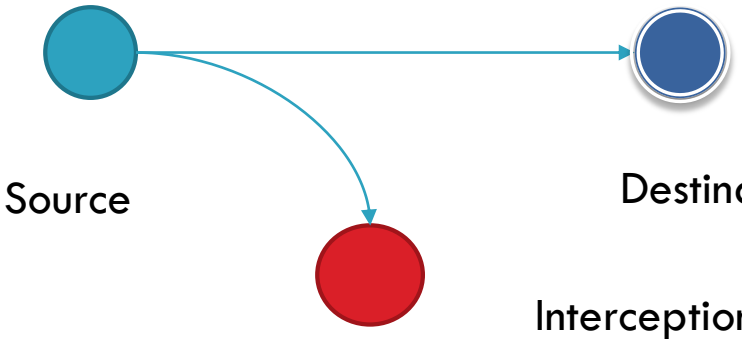
Les attaques Déni de Service « DoS »

Source

Destination

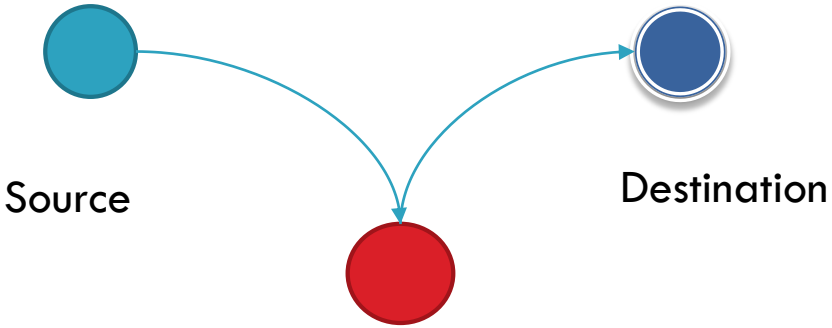
Interruption : vise la disponibilité des informations

Les attaques d'interception



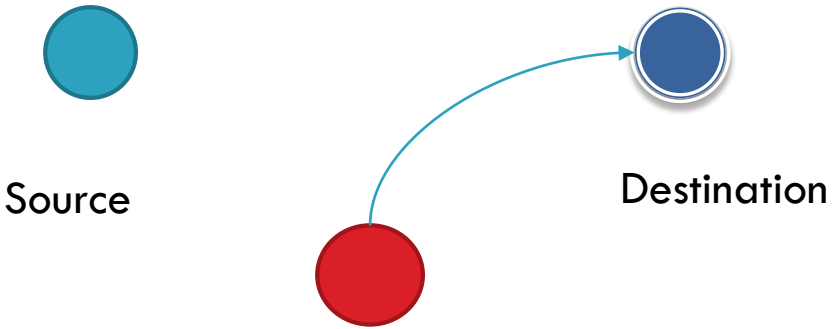
Interception : vise la confidentialité des informations (capture de contenu, analyse de traffic,…)

Les attaques « Man in the middle »



Modification : vise
l'intégrité des informations
(modification, rejeu, …)

Les attaques



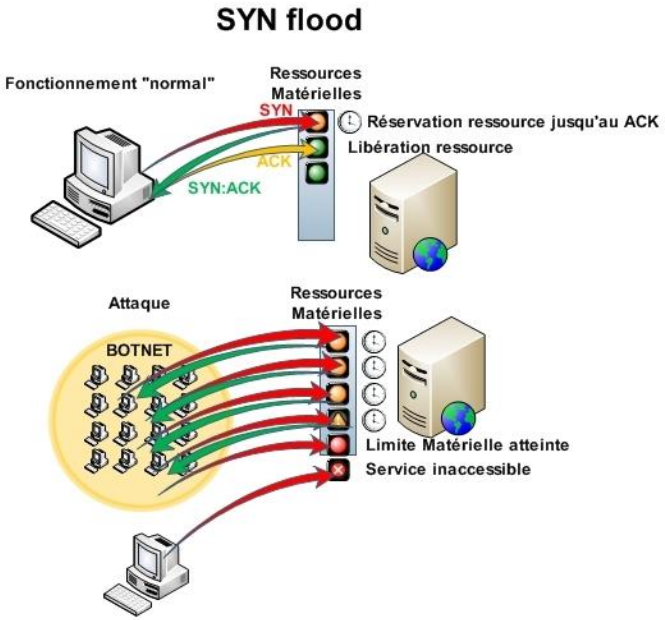
Fabrication : vise l'authenticité des information (mascarade)

Port informatique

- Un port est un numéro unique codé sur 16 bits (65536 ports différents possibles)
- Certains sont réservés

Port	Service ou Application rattachée
21	FTP (Transfert de fichiers)
23	Telnet (Administration système)
25	SMTP (Envoi des emails)
53	DNS (Transformation des noms en adresses IP)
80	HTTP (Consultation des pages web)
110	POP3 (Réception des emails)
119	NNTP (Newsgroups)
443	HTTPS (Internet sécurisé)

Attaque DOS Syn Flood



Phishing (hameçonnage ou filoutage)

- technique par laquelle des personnes malveillantes se font passer pour de grandes sociétés ou des organismes financiers qui vous sont familiers en envoyant des mèls frauduleux et récupèrent des mots de passe de comptes bancaires ou numéros de cartes de crédit pour détourner des fonds.

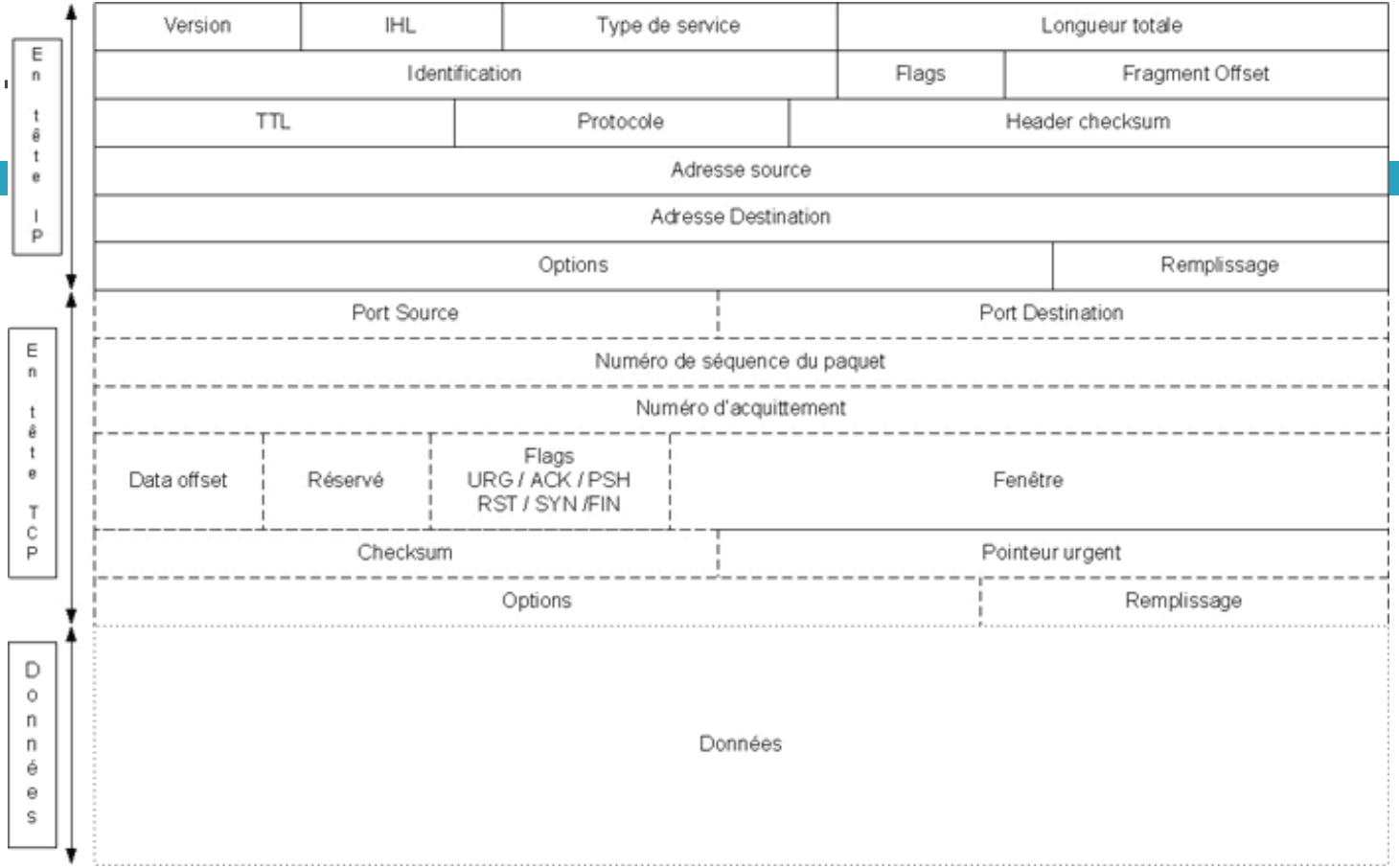
Technique de recherche d'information

- Recherche d'information publiques
  - DNS (dig), whois, …
- Découverte du réseau et du filtrage IP.
  - traceroute, ping, hping, netcat, . . .
- Découverte des systèmes d'exploitation.
  - nessus, nmap, xprobe, queso, . . .
- Découverte de services ouverts.
  - nmap, udp-scan, nessus, . . .
- Découverte des versions logicielles.
  - telnet, netcat, . . .

Who is


afnic
Accès rapide
Votre nom de domaine
Produits et services
L'AFNIC en bref
Résoudre un litige
Expertises
Page d'accueil > Produits et services > Services > Whois
Le .fr
Le .re
Autres domaines de premier niveau français
Services
DNSSEC
Service QUalifié d'Accès aux "données Whois" (SQUAW)
Whois
Aide
Mentions spéciales Whois
ZoneCheck
Convertisseur IDN
Liste quotidienne des noms de domaine enregistrés
Afnic Conseil
Formations
WHOIS
Le nom de domaine "u-bourgogne.fr" est déjà déposé.
Résultat de votre recherche
Nom de domaine : u-bourgogne.fr
État : Actif (consulter aussi le site web)
Bureau d'enregistrement : GIP RENATER
Date de création : 1 janvier 1995 00:00
Date anniversaire : 01 janvier
Serveurs de noms (DNS)
- Serveur n° 1: ns1.u-bourgogne.fr
- Serveur n° 2: dns.univ-lyon1.fr
Titulaire : UNIVERSITE DIJON BOURGOGNE
centre Informatique
Esplanade Erasme
21078 Dijon
France
Téléphone :+33 3 80 39 52 10
Courrier électronique :browaeys@u-bourgogne.fr
Joignabilité :NotIdentified
Eligibilité :Ok
Contact administratif : Sophie Bejean
Univ. de Bourgogne
B.P. 27877
21078 Dijon
France

Paquet


Entête IP
Version
IHL
Type de service
Longueur totale
Identification
Flags
Fragment Offset
TTL
Protocole
Header checksum
Adresse source
Adresse Destination
Options
Remplissage
Entête TCP
Port Source
Port Destination
Numéro de séquence du paquet
Numéro d'acquittement
Data offset
Réservé
Flags
URG / ACK / PSH
RST / SYN /FIN
Fenêtre
Checksum
Pointeur urgent
Options
Remplissage
Données
Données

Balayage

- Découverte de machines :
  - But : découvrir les machines d'un réseau donné.
  - Principe : envoyer un paquet à toutes les adresses. analyser le paquet retour
  - Outils. nmap
- Découverte de ports ouverts :
  - But. découvrir les services/ports ouverts sur une machine donnée.
  - Principe. envoyer des paquets.
  - analyser les paquet retour (ou leur absence)
- Outils.
  - nmap
  - telnet
  - netcat

Attaque sur les réseaux locaux

- Écoute du réseau. Capturer le contenu des paquets qui ne nous sont pas destinés.
  - Tcpdump/wireshark
  - sniff
- Usurpation d'adresses (IP et MAC). Forger et envoyer des paquets avec une fausse adresse IP. . .
  - dsniff
- Vol de session. Forger des paquets permettant la prise de contrôle d'une connexion déjà établie.
  - juggernaut
  - hunt

Mécanismes de défense

- • **Chiffrement** : algorithme généralement basé sur des clefs et transformant les données. Sa sécurité est dépendante du niveau de sécurité des clefs.
- • **Signature** numérique: données ajoutées pour vérifier l'intégrité ou l'origine des données.
- • **Bourrage de trafic** : données ajoutées pour assurer la confidentialité, notamment au niveau du volume du trafic.
- • **Notarisation** : utilisation d'un tiers de confiance pour assurer certains services de sécurité.
- • **Contrôle d'accès** : vérifie les droits d'accès d'un acteur aux données. N'empêche pas l'exploitation d'une vulnérabilité.

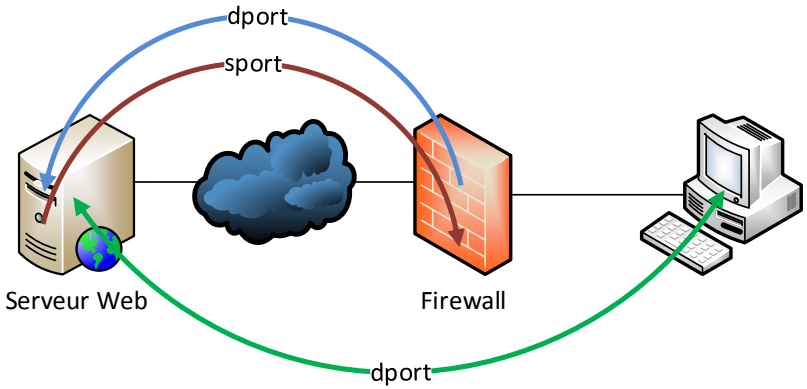
Mécanismes de défense

- **Antivirus** : logiciel censé protéger ordinateur contre les logiciels (ou fichiers potentiellement exécutables) néfastes. Ne protège pas contre un intrus qui emploie un logiciel légitime, ou contre un utilisateur légitime qui accède à une ressource alors qu'il n'est pas autorisé à le faire.
- **Le pare-feu** : un élément (logiciel ou matériel) du réseau informatique contrôlant les communications qui le traversent. Il a pour fonction de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les communications autorisés ou interdits. N'empêche pas un attaquant d'utiliser une connexion autorisée pour attaquer le système. Ne protège pas contre une attaque venant du réseau intérieur (qui ne le traverse pas).
- **Détection d'intrusion** : repère les activités anormales ou suspectes sur le réseau surveillé. Ne détecte pas les accès incorrects mais autorisés par un utilisateur légitime. Mauvaise détection : taux de faux positifs, faux négatifs.
- **Journalisation** ("logs") : Enregistrement des activités de chaque acteurs. Permet de constater que des attaques ont eu lieu, de les analyser et potentiellement de faire en sorte qu'elles ne se reproduisent pas.
- **Analyse des vulnérabilité** ("security audit") : identification des points de vulnérabilité du système. Ne détecte pas les attaques ayant déjà eu lieu, ou lorsqu'elles auront lieu.

Etude de cas Firewall Netfilter

- Implémentation noyau du firewall sous linux
- Une seule commande : iptables mais …beaucoup d'options
- Firewall statefull (garde des traces des requêtes)
- Politique par défaut

Netfilter suite



Netfilter suite

- On efface toutes règles existantes

  iptables -X

  iptables -F

  iptables -t nat -X

  iptables -t nat -F

- Politique par défaut

  iptables -P INPUT DROP

  iptables -P FORWARD DROP

  iptables -P OUTPUT DROP

Netfilter suite suite

- On ouvre l'accès au web au serveur et au client

```
# requetes DNS
iptables -A OUTPUT -o $public -p tcp --dport 53 -j ACCEPT
iptables -A INPUT -i $public -p tcp --sport 53 -j ACCEPT
iptables -A OUTPUT -o $public -p udp --dport 53 -j ACCEPT
iptables -A INPUT -i $public -p udp --sport 53 -j ACCEPT
# Pour avoir du net
iptables -A INPUT -i $public -p tcp --sport http -j ACCEPT
iptables -A OUTPUT -o $public -p tcp --dport http -j ACCEPT
# Pour du net sur le client
iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -i $prive -p tcp --dport http -j ACCEPT
```

Netfilter divers

Translation adresse

iptables -A POSTROUTING -t nat -s $reseauprive -j MASQUERADE

Translation de port

iptables -t nat -A PREROUTING -i $public -p tcp --dport 8085 -j DNAT --to 192.168.10.15:80

iptables -A FORWARD -i $public -p tcp -d 192.168.10.15 --dport 80 -j ACCEPT

Règles d'hygiène SSI

- Il convient d'utiliser un compte ne possédant pas les privilèges « administrateur »
- Éviter de se connecter à des sites suspects
- Éviter de télécharger des logiciels dont l'innocuité n'est pas garantie
- Changer de mot de passe régulièrement

Mot de passe

- Attention à la longueur
- Bien choisir
  - Pas dans le dictionnaire
  - Mot de passe différent du login
  - Pas de memo sur le clavier
  - Utiliser des caractères exotiques +;()
- Changer régulièrement

Intégrité assurée

- Logiciel antivirus avec mise à jour automatique
- Sauvegardes régulières des données
- Clonage du système
- Utilisation de clés USB personnelles

5 réflexes à avoir lors de la réception d'un courriel

- N'ayez pas une confiance aveugle dans le nom de l'expéditeur
- Méfiez-vous des pièces jointes
- Ne répondez jamais à une demande d'informations confidentielles
- Passez votre souris au-dessus des liens, faites attention aux caractères accentués dans le texte ainsi qu'à la qualité du français dans le texte ou de la langue pratiquée par votre interlocuteur
- Paramétrez correctement votre logiciel de messagerie
  - Ne jamais accepter de recevoir des messages au format HTML ou XML
  - interdisez l'exécution automatique des ActiveX et des plug-ins

Liens

- Le CERTA : http://www.cert.ssi.gouv.fr/
- L'ANSSI : http://www.ssi.gouv.fr/