

RSX112

Sécurité des réseaux

Stéphane LARCHER

Piratage informatique

```
for object to mirror_mod.mirror_object
operation == "MIRROR_X":
    mirror_mod.use_x = True
    mirror_mod.use_y = False
    mirror_mod.use_z = False
operation == "MIRROR_Y":
    mirror_mod.use_x = False
    mirror_mod.use_y = True
    mirror_mod.use_z = False
operation == "MIRROR_Z":
    mirror_mod.use_x = False
    mirror_mod.use_y = False
    mirror_mod.use_z = True

#selection at the end -add
mirror_ob.select= 1
mirror_ob.select=1
context.scene.objects.active = mirror_ob
("Selected" + str(mirror_ob.name))
mirror_ob.select = 0
= bpy.context.selected_objects
data.objects[one.name].select

print("please select exactly one mirror")

-- OPERATOR CLASSES -----

bpy.types.Operator):
    X mirror to the selected
    object.mirror_mirror_x"
    mirror X"
```

La problématique

Lors de l'envoi d'un message, nous ne voulons pas que qu'il puisse être

intercepté et
lu
confidentialité

Modifié
Intégrité

Injecté d'un
faux
message
authentification

Réinjecté par
un ancien
message
anti-rejeu

La problématique

**La
disponibilité**

L'intégrité

**La
confidentialité**

La preuve

La problématique





Définition

Définitions

Le piratage

Pillage du système informatique

Le Hacker

Récupération
d'une information
non publique

Définitions

Faire appel à un spécialiste pour tester la sécurité

Les hackers
professionnels

Les « Whites Hats »

Dans la peau de
l'attaquant

Vérification de l'accessibilité
des données

Définitions

Qui est l'ennemi

Les hackers
black hats

Les hackers
grey hats

Les hackers
white hats

Les script
kiddies

Les hackers
universitaires

Définitions

Test d'intrusion pour tester la sécurité



Les tests en black box

l'hacker qui vient auditer le système n'a aucune information



Les tests en grey box

possession d'un identifiant pour l'accès



Les tests en white box

système ouvert pour un test plus approfondi



L'attaque

L'attaque,

L'attaquant doit conserver son anonymat parce qu'il y a blocage des Ips et référencement des Ips malveillantes

port-Knocking

modification du comportement des firewall

Utilisation d'un ordinateur tier piraté

Se rendre anonyme avec un proxy
solution TOR

Changement régulier de l'ip de l'attaquant



L'attaque,

L'attaquant doit trouver une porte d'entrée

Netcat

n'importe quel
type de
connexion à
un service sur
un port donné

Telnet

connexion
TCP/IP avec
un serveur
distant

Nmap

scanner des
ports

Scapy

interception de
paquets sur un
réseau
la génération de
paquets dans
un grand
nombre de
protocoles

Metasploit

framework
puissant
testant les
vulnérabilités
d'un système



L'attaque,

D'autre moins facile à trouver

Des (gros) dictionnaires permettant de lancer des attaques sur dictionnaire

Des outils permettant de réaliser des attaques de type force brute

Des keyloggers, permettant de récupérer les informations tapées au clavier sur l'ordinateur de sa victime

Quelques virus ou trojans faciles à mettre en place

De quoi lancer des attaques de type DoS

Des scripts de log-wiper pour effacer leurs traces dans les logs d'un système

Quelques modules lkm à injecter dans un kernel

L'attaque,

Trouver à partir de la partie visible de l'entreprise une adresse IP

whois

base de données pour les noms de domaine

Host

repérage de l'adresse IP du site WEB

traceroute

liste de tous les nœuds

Google (!)

il est l'ennemi de ceux qui ont oublié de se faire discrets



L'attaque,

Découvrir les caractéristiques du réseau

Connaissance du
système
d'exploitation d'un
serveur

Connaître sa
topologie

Prise
d'empreinte TCP/IP

Les réseaux complets
avec une adresse de
sous-réseau et son
masque

Capturer ainsi les
écrans des
machines cibles

Frappe utilisateur
Voir les fenêtres de la
victime en temps réel

L'attaque,

Profiter de la faille humaine

Le social engineering

Sensibilisation du personnel aux questions de sécurité

Etude des réseaux sociaux

Ouvrir les postes du réseau

Wireshark

étude du réseau

Ecoute du wifi

beaucoup de réseaux wifi sont non chiffrés

L'attaque,

L'attaque par le WEB

Utilisation des failles connus des sites web

 Injections SQL

 par requêtes

 XSS (cross-site scripting)

L'attaque par la force

Tester toutes les combinaisons de mot de passe

Saturation de la bande passante

Saturation des buffers pour une application

Attaque de dénis de service (DoS)



Les parades

Les parades

La protection

Un antivirus à jour

Système d'information à jour de manière globale

Réduire la surface d'attaque en supprimant les fonctionnalités des OS inutilisées

Les parades

Sauvegarde

La fréquence
pour un RPO (Recovery Point Objective) le plus acceptable

Le type de sauvegarde

totales
partielles
incrémentielles

Le type de stockage

les supports devraient idéalement être redondants et hors site avec une rotation établie en fonction de la politique de sécurité

Sécurité

Les données sauvegardées doivent être chiffrées et accessibles uniquement aux personnes autorisées

Les parades

VPN

généralement fourni par un routeur, le VPN (Virtual Private Network) chiffre et sécurise les communications entre sites distants ou avec les utilisateurs nomades disposant d'un accès

Pare-feu

Seul le trafic autorisé peut entrer ou sortir de l'entreprise

IPS

un IPS (Intrusion Prevention System) surveille le trafic entrant et sortant à la recherche de logiciels malveillants, de signatures d'attaques réseau, etc

Les parades

ESA

Appareils dédiés à la sécurité de la messagerie électronique comme l'ESA de Cisco qui filtre les spams et les e-mails suspects.

WSA Filtrages des sites Internet malveillants connus ou suspects

Serveur AAA

Serveurs disposent d'une base de données des personnes autorisées à accéder aux périphériques réseau

Les parades

Authentification, autorisation et traçabilité (AAA)

Les services à utiliser pour renforcer la sécurité

Authentication

Qui est autorisé à se connecter ?

Authorization

Quelles sont les actions autorisées ?

Accounting

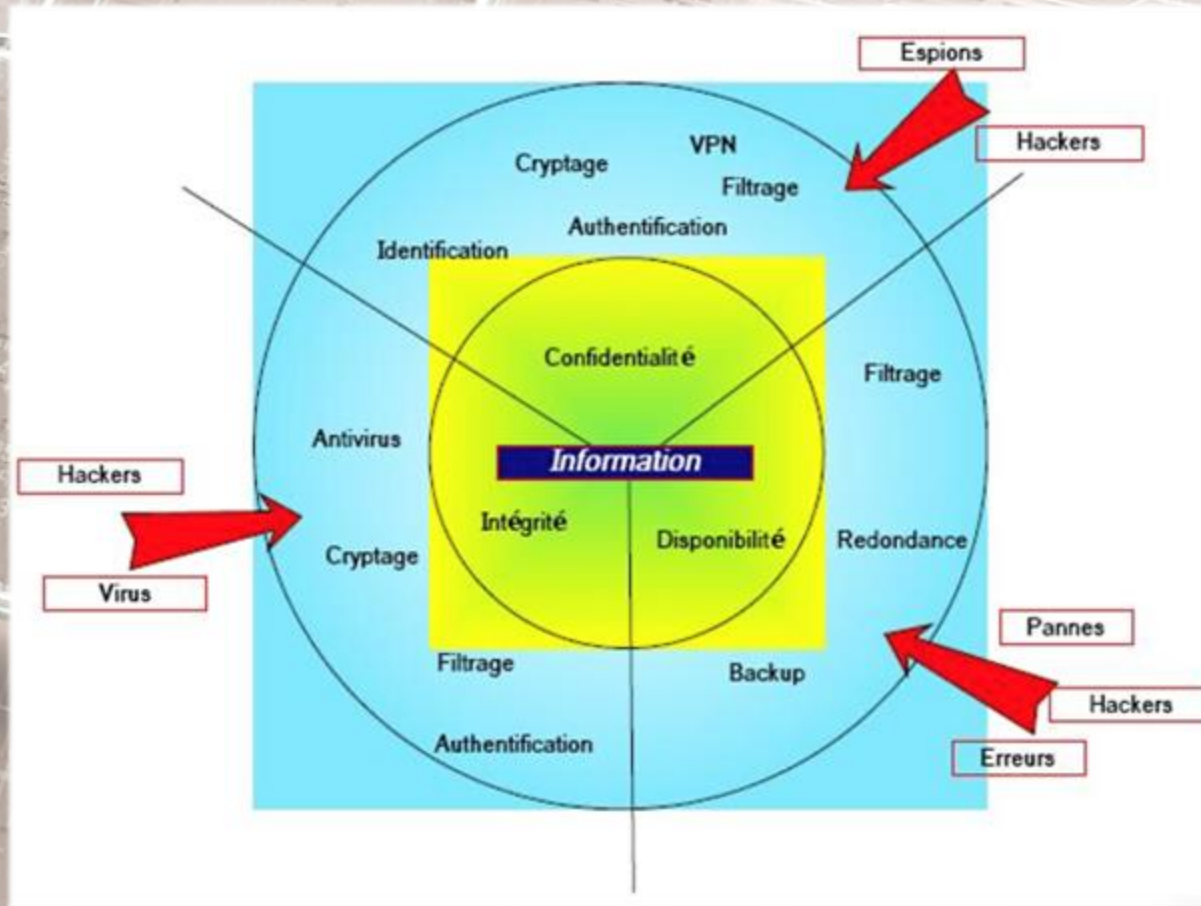
Les actions importantes sont-elles tracées ?

Quand est-il autorisé à se connecter ?

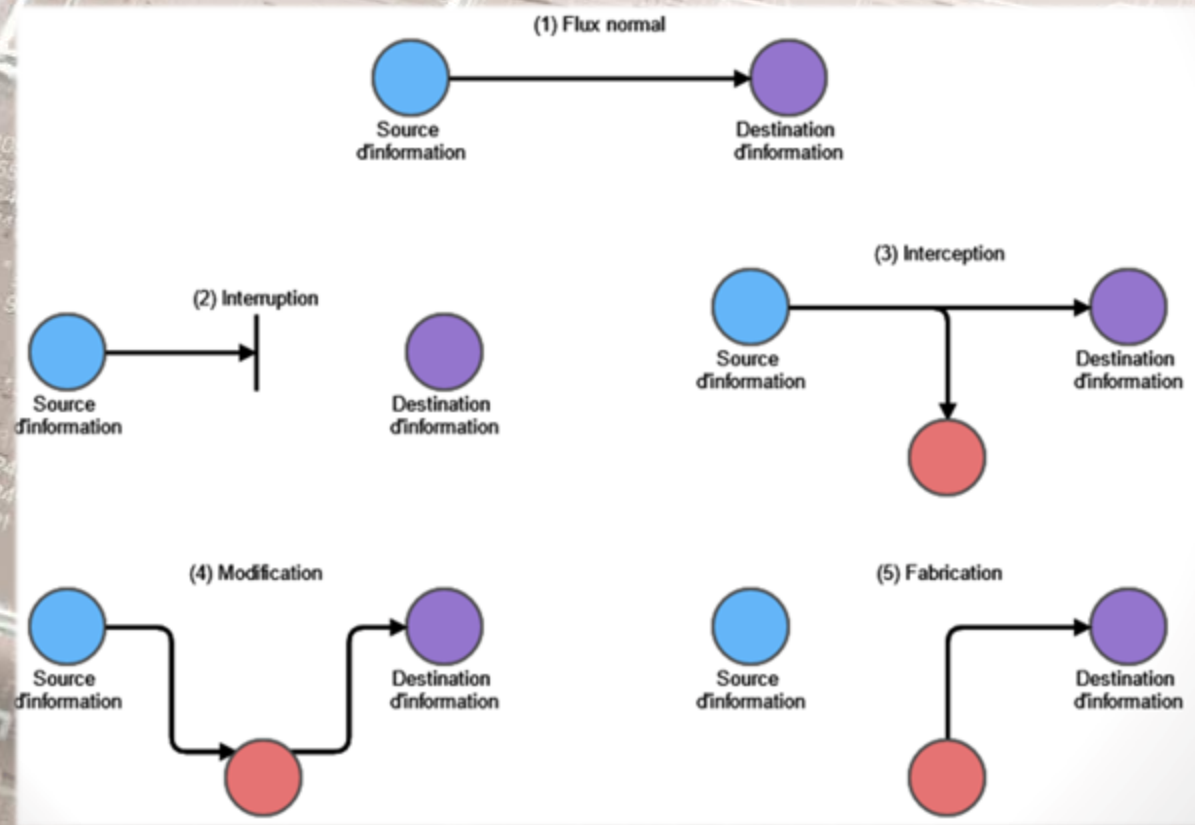
The image features a close-up, high-angle shot of a metallic padlock resting on a complex, brown-toned printed circuit board (PCB). The padlock is positioned diagonally, with its shackle pointing towards the top left. The PCB is densely packed with intricate white circuit traces and various electronic components, including small integrated circuits and resistors. The lighting creates a sense of depth, highlighting the textures of the metal padlock and the fine details of the circuitry. The overall color palette is muted, dominated by browns, greys, and metallic tones, giving it a technical and industrial feel.

La sécurité du réseau

La sécurité du réseau



La sécurité du réseau



La sécurité du réseau

