Atouts et limites des pares-feu personnels

Cédric Blancher <blancher@cartel-securite.fr>

—

Symposium sur la Sécurité des Technologies de l'Information et de la Communication

11 juin 2003

Plan

- Concepts de base
  - Présentation du concept de firewall personnel
  - Champs d'application
- Le firewall personnel dans le monde réel
  - Fonctionnalités générales
  - Particularités et classification des produits
- Limites du concept
  - Limites intrinsèques
  - Limites héritées (indépendantes)
- Intégrer efficacement l'outil
  - Les bases d'une bonne implémentation

Problématique du filtrage des postes isolés

- Utilisation essentiellement cliente
- Difficulté de mise en œuvre à l'aide de filtres classiques
- Manque d'outils adaptés
- ➥ Nouvelle approche

Filtrage par application

- Le critère est l'application générant le flux
- Liste blanche, liste noire, comportement par défaut

Champs d'application

- Poste personnel relié à Internet
- Poste de travail en réseau d'entreprise
- Portable
- etc.

- Concepts de base
  - Présentation du concept de firewall personnel
  - Champs d'application
- Le firewall personnel dans le monde réel
  - Fonctionnalités générales
  - Particularités et classification des produits
- Limites du concept
  - Limites intrinsèques
  - Limites héritées (indépendantes)
- Intégrer efficacement l'outil
  - Les bases d'une bonne implémentation

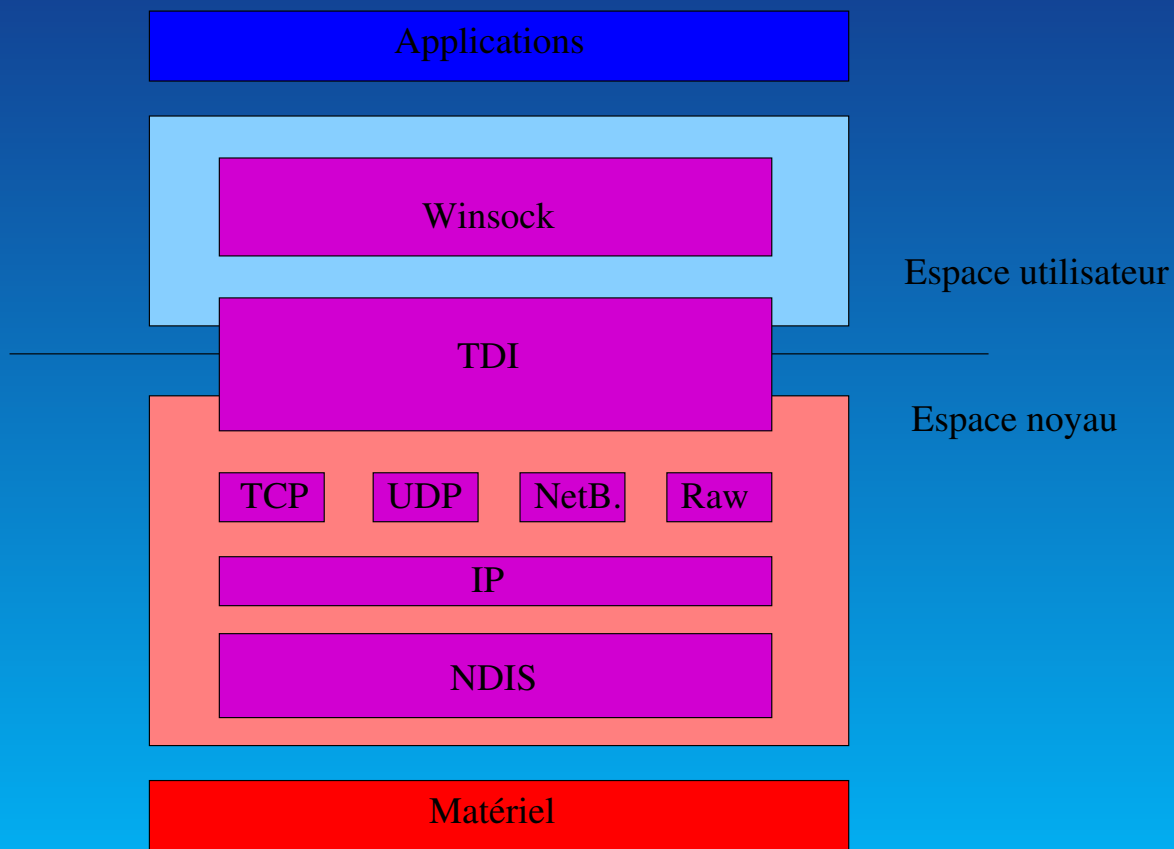
Identification d'une application

- Nom de l'application
- Chemin dans le système de fichiers
- Somme MD5 de l'exécutable

Configuration

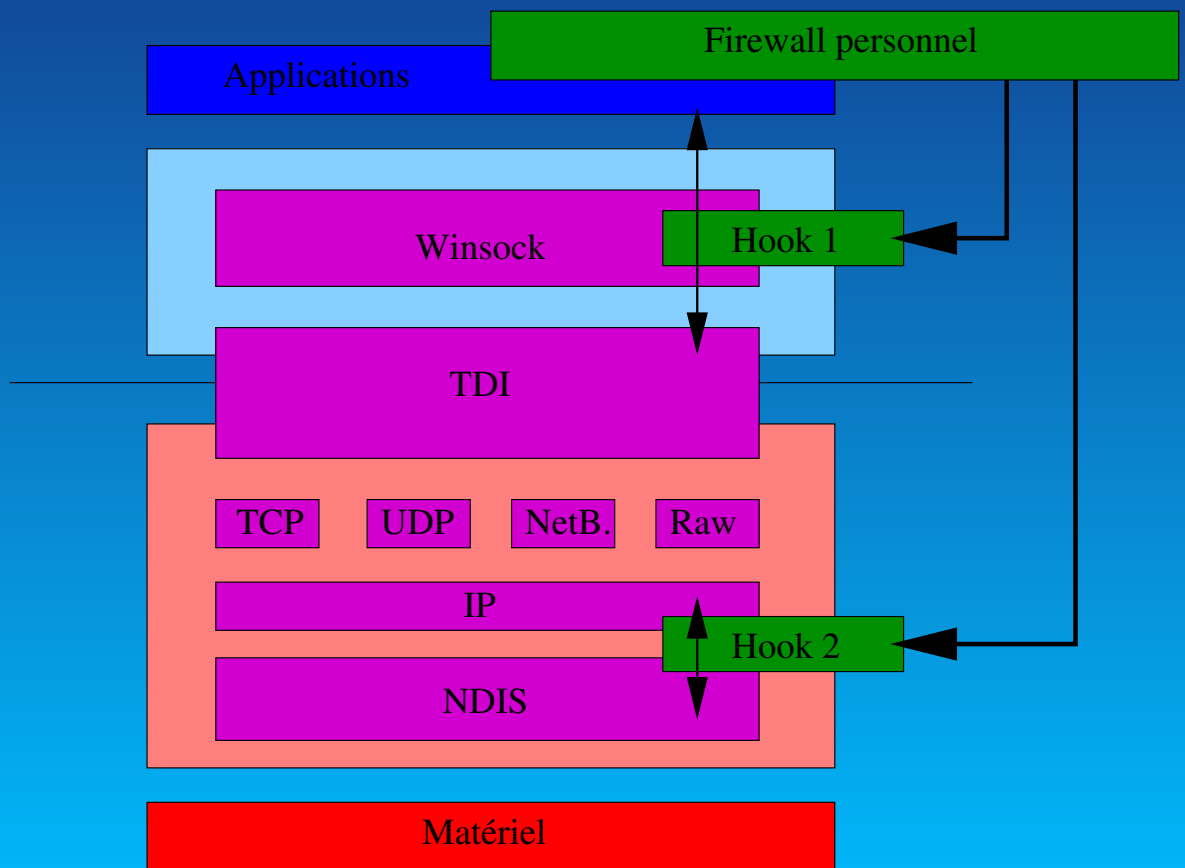
- Jeu de règles par défaut
- Méthode interactive d'autorisation des applications et flux
- Configuration simple et remontée d'alerte

La pile réseau générique Win32



TDI : Transport Driver Interface
NDIS : Network Driver Interface Specification

Interception des appels socket et paquets reçus par deux hooks



Deux classes de produits

- Produits simples : oui/non
- Produits évolués : oui/non + restriction de flux

Tous les produits proposent un suivi d'état de niveau 4 pour TCP
Fonctionnalités très différentes selon les produits
Aucun produit ne propose de suivi de session pour ALG (FTP, H323, etc.)

- Concepts de base
  - Présentation du concept de firewall personnel
  - Champs d'application
- Le firewall personnel dans le monde réel
  - Fonctionnalités générales
  - Particularités et classification des produits
- Limites du concept
  - Limites intrinsèques
  - Limites héritées (indépendantes)
- Intégrer efficacement l'outil
  - Les bases d'une bonne implémentation

Limites de deux ordres

- Inhérentes : le concept est confronté à la réalité de sa mise en œuvre
- Indépendante : limites imposées par le socle système sous-jacent

Limites inhérentes

- Utilisateur non compétent
- Signalisation peu explicite et rébarbative
- Jeu de règles par défaut faible
- Possibilité de filtrage parfois limitées
- Difficulté de limiter certaines application (e.g. navigateur)

Limites indépendantes

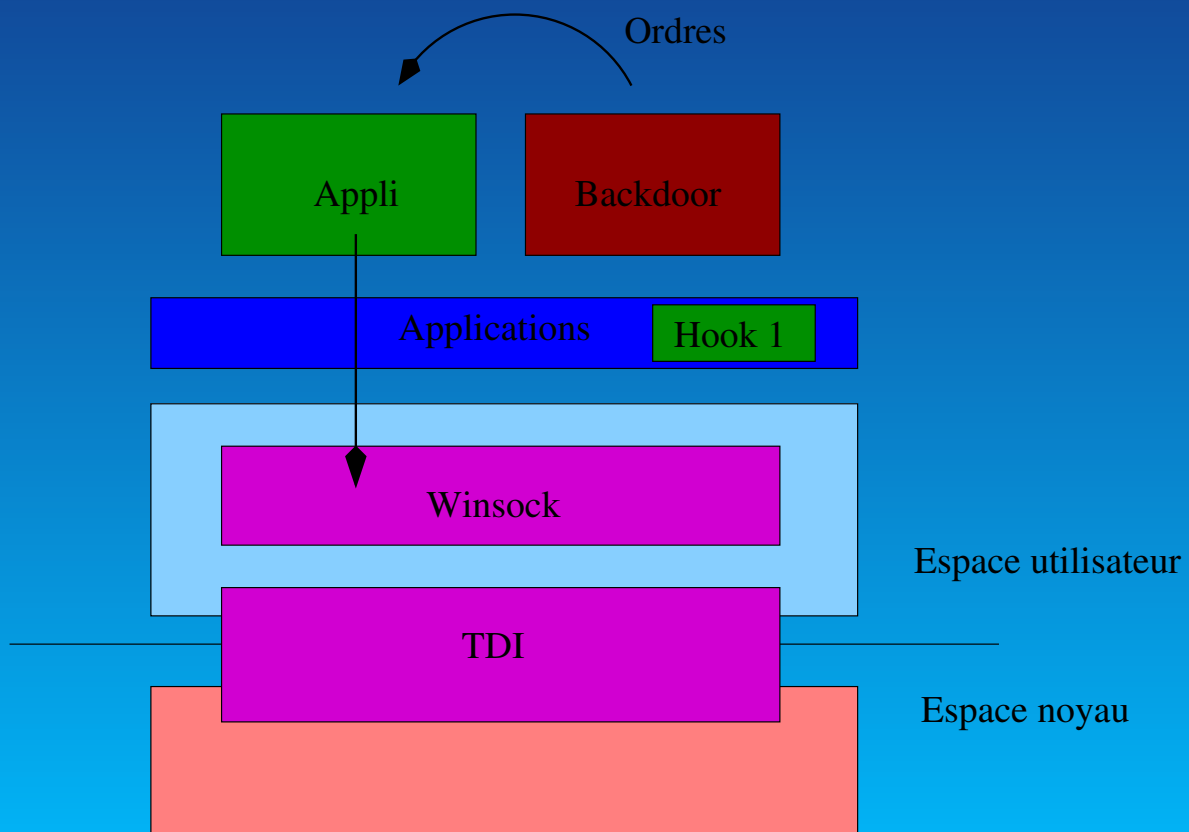
- OS faible ne gérant pas la notion de droits
- OS mal configuré : FAT32, utilisation de comptes superutilisateur, etc.
- Présence de bibliothèques de capture
- “Fonctionnalités” de communication inter-processus

Trois axes d'attaque

- Passer au dessus du firewall via une application autorisée
- Passer en dessous du firewall via une bibliothèque adaptée
- Attaquer le firewall lui-même en tant qu'applicatif

⇒ Les trois méthodes sont exploitables

Passer au dessus

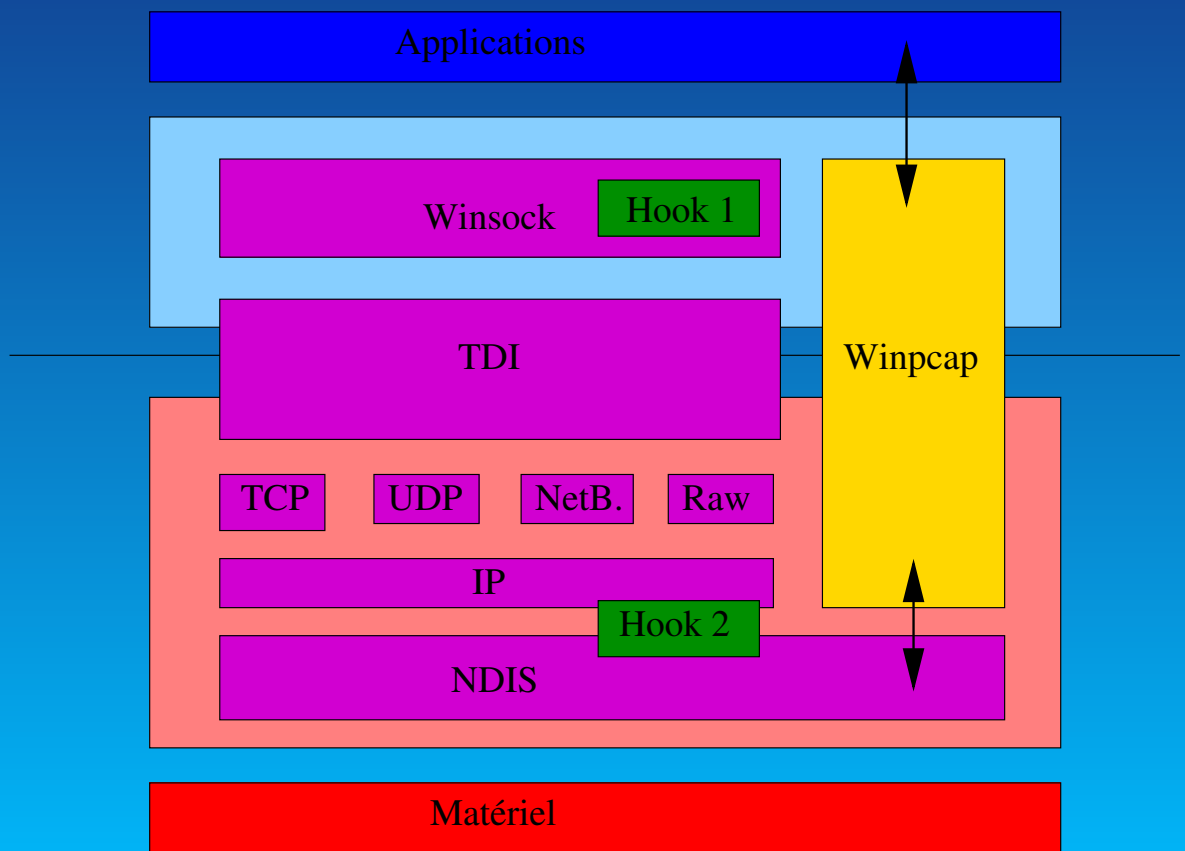


Passer au dessus

- Utilisation de macros et autres applets
- Utilisation des liens OLE et ActiveX (cf. JAB)
- Appel CreateRemoteThread permettant de l'injection de code à la volée

↪ La méthode la plus efficace et la plus difficile à contrer

Passer en dessous



Passer en dessous

- Injection de paquets au plus bas niveau
- Capture de trames au niveau NDIS

➥ Nécessite l'installation d'une bibliothèque de capture/injection

Attaquer le firewall

- Exploitation de jeux de règles faibles
- Altération du fichier de configuration
- Arrêt du processus
- Exploitation du logiciel en lui-même

➥ Possible sur OS faible (Win9x/Me) ou mal configuré (FAT32/XP Family par défaut)

- Concepts de base
  - Présentation du concept de firewall personnel
  - Champs d'application
- Le firewall personnel dans le monde réel
  - Fonctionnalités générales
  - Particularités et classification des produits
- Limites du concept
  - Limites intrinsèques
  - Limites héritées (indépendantes)
- Intégrer efficacement l'outil
  - Les bases d'une bonne implémentation

Une implémentation correcte

- Éviter les limites indépendantes
- Éviter les limites inhérentes
- Généraliser la politique de sécurité
- ➥ Un travail tout azimut

Éviter les limites indépendantes

- Utiliser de vrais OS, avec la notion de droits
- Les installer et les configurer correctement
- Configurer l'attribution des privilèges
- Limiter les bibliothèques et applications disponibles
- Éviter les applications trop "communicantes"

↪ Travail en amont sur le socle applicatif

Éviter les limites inhérentes

- Choisir son outil en fonction de ses besoins
- Éviter les outils simplissimes
- Bien configurer son outil
- Ne pas croire le blabla marketting
- ➥ Travail sur le dispositif de protection

Généraliser la politique de sécurité

- Répéter le filtrage sur les équipements réseau
- Mettre en place des filtres applicatifs
- Mettre en place des antivirus
- ➥ Travail en aval sur le réseau
- ➥ Gérer les problèmes localisés entre la chaise et le clavier : sensibilisation, formation !

En résumé :

- Un concept séduisant mais limité par les plateformes sous-jacentes
- Une brique insuffisante en elle-même, mais partie du dispositif global de protection du SI

<PUB>

- MISC : magazine français, spécialisé en sécurité informatique[a]

</PUB>

[a] http://www.miscmag.com/