Introduction

Mise en œuvre du protocole natif chez Microsoft
Communication entre machine hétérogènes
Administration centralisée

Mise en œuvre du protocole SMB / CIFS
pour le partage de fichiers (et d'imprimantes)

SMB / CIFS

Samba est une réimplémentation de SMB/CIFS …
ce qui permet la communication MS Windows / *nix

Netbios
Mode de nommage dans un voisinage réseaux
API (couche 4) sur les ports 137, 138 et 139

couche 1 – physique
couche 2 – **IP**
couche 3 – NetBT
(implémentation de NetBIOS sur IP)

Résolution de noms par *broadcast*
(sauf si serveur WINS)

définitions

NetBIOS : NetBEUI – NetBT
Nom netbios – nom hôte

```
$ nmblookup -A <ip>
```


Jadis
NetBIOS était initialement implémenté sans IP → NetBEUI

NetBIOS
15 + 1 caractères pour le rôle
(*try nmblookup and see NetBIOS-suffix*)

La machine déclare au minimum **2 noms**; le nom de machine et celui du *workhroup*

Résolution de nom 1
/etc/nsswitchs
DNS – WINS – broadcast

installation / dæmons

installation

samba · samba-common · smbclient

dæmons

smbd · nmbd · windbindd

Rôle des dæmons

smdb : partage des ressources
administre l'authentification
nmbd : dæmon netBIOS
résolution de noms
permet la participation au voisinage réseau
windbindd : démarré si samba fait partie d'un AD

lancement à grands coups de
`invoke-rc.d samba` ou
`/etc/inint.d/samba`

configuration

configuration centralisée dans

`/etc/samba/smb.conf`

sections
variables
`$testparm <mysmb.conf> > smb.conf`

`smbd -b | grep smb.conf`

Sections
global – homes – printers

Commentaires # ou ;

Variables
Scripts personnalisés et *include*
Variables disponibles : voir `man smb.conf`

Notion de voisinage réseau

browsing list

voisinage réseau

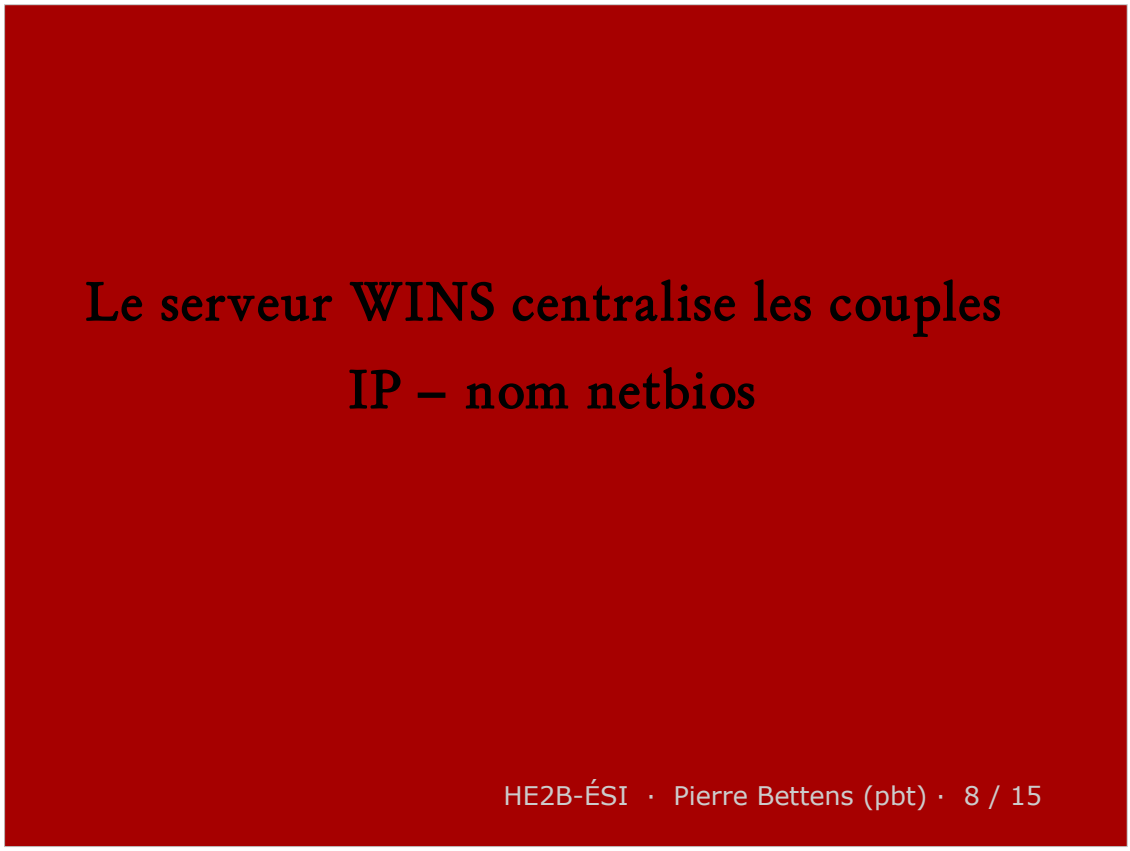
master browser

élection

Visualiser les partages sur un même segment (sinon interroger via IP sur le port 139)

C'est la machine qui informe le maitre explorateur (annonce `__MS_BROWSE__`).

Élection → entraine une inertie pour la liste d'exploration → serveur **WINS**



Rôle

Centralise les correspondances IP – nom
Limite les *broadcasts*
Permet une liste d'exploration « derrière les routeurs »

authentification

types d'authentification

share – user – server – domain

passwd backend

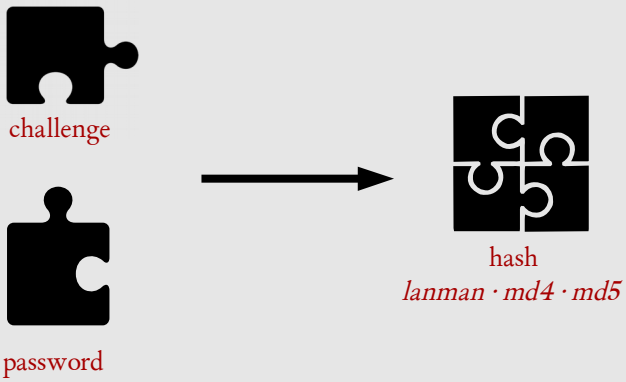
smbpasswd – tdbsam – ldap

Type d'authentification
share – user – server – domain

passwd backend
smbpasswd
possibilité de synchronisation
tdbsam
/var/lib/samba
rôle de PDC

protocole *challenge / response*

présentation



Protocole challenge / response

1/ client : *negociate_message*
2/ server : *challenge_message*
3/ client : calcul du hash *authenticate_message*
4/ server : accept ?

Dans la négociation les deux parties s'échangent une clé de session (pour éviter le vol)

protocoles *challenge / response*

ntlm v1

- hash du mot de passe
  - LanMan → DES
  - NTLM → MD4
- challenge © hash → 24 bytes

Protocoles ntlm

ntlm v1

- Challenge = 8 bytes (64 bits)
- les hashs sont stockés dans /etc/samba/smbpasswd (si c'est le backend)
- hash
  - LanMan hash
    DES des 14 caractères encodés en « ASCII»
  - NT hash
    MD4 encodés en UTF16
  - Les hashs font 16 bytes (128 bits)

Voir Wikipedia pour les détails
https://en.wikipedia.org/wiki/NT_LAN_Manager

authentification |||

protocoles *challenge / response*

ntlm v2

- hash mot de passe (MD4)
- hash *user* et *domain* (HMAC MD5)
- …

Kerberos

Protocoles ntlm

ntlm v2

Introduit avec NT4 SP4
Longueur variable > 24 bytes

Détails : http://davenport.sourceforge.net/ntlm.html

On pourra «forcer » un type d'authentification avec

```
encrypt password = yes
lanman auth = no
ntlm auth = no
client lanman auth = no
client ntlmv2 = yes
```

Kerberos

Nécessite une ? de confiance (l'AD)
trusted-third-party scheme

utilitaires

· `smbpasswd` · `smbclient` ·
· ~~`smbmount`~~ · `mount` ·
· interface graphique ·

À compléter

Liens

Site officiel samba.org

Comprendre NTLM chez davenport

Référence

TCP / IP Network administration (Craig Hunt)

… et les pages de manuel

Transparents dans le cadre de mes cours à HE2B-ÉSI.

Qui suis-je ?

Pierre Bettens (pbt)
pbettens@he2b.be
http://blog.namok.be · http://esi.namok.be

Images

500px Łukasz Kuczborski
DeviantArt Spence122
The noun project dnlhtz SuperAtic labs