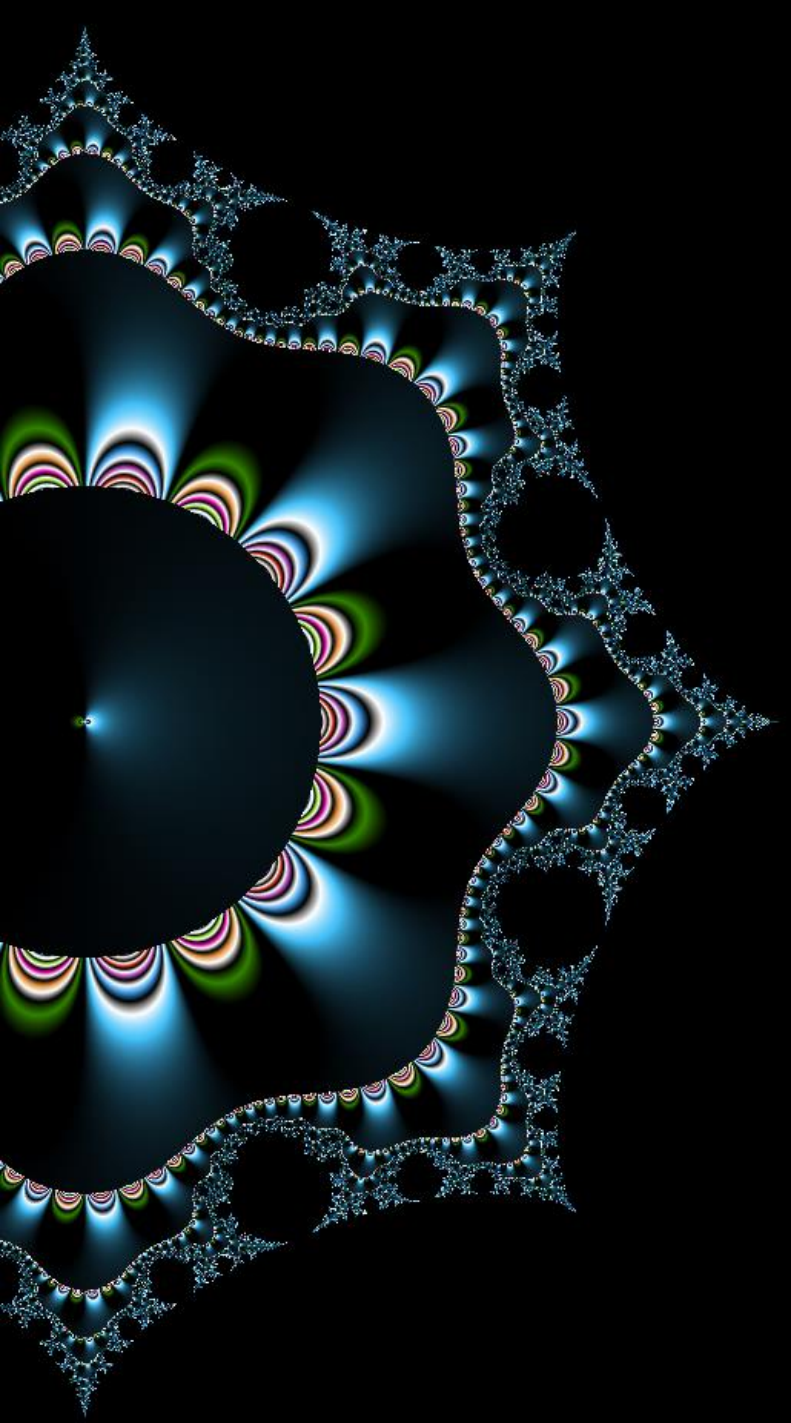


# 04 Contrôle d’accès

Accès restreint aux ressources

Corinne HENIN

www.arsouyes.org

# Accès à un SI

A un site web, un bâtiment, …

# Identification

Qui je suis ?

*« Corinne HENIN »*

# Authentification

Preuve ?

*« j'ai ma carte d'identité »*

# Contrôle d’accès

Je peux faire/voir quoi ?

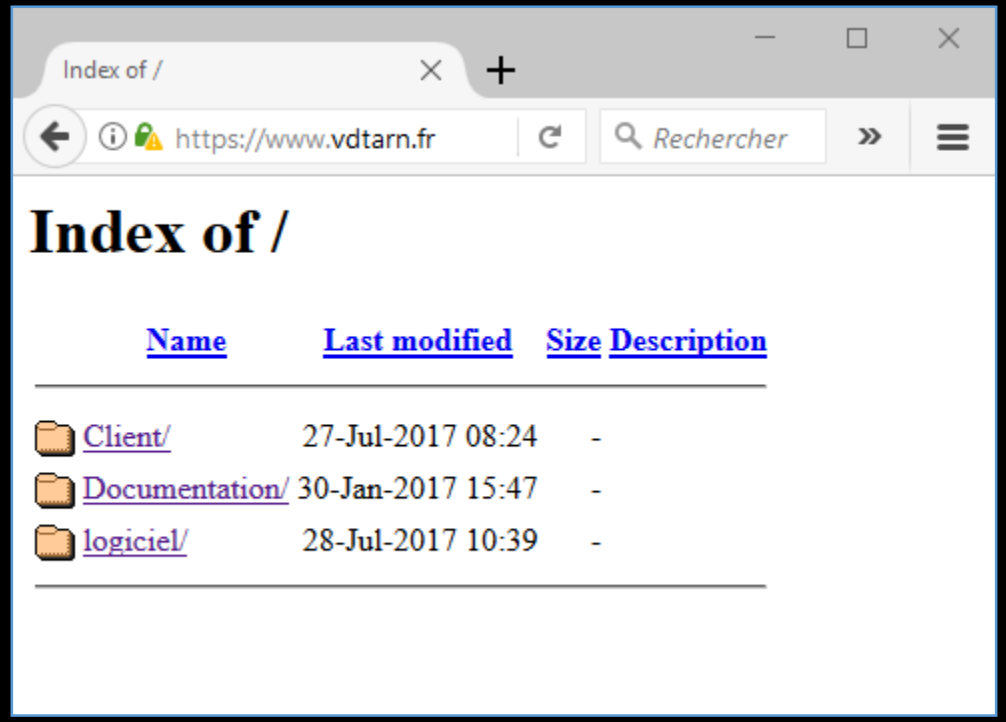
*« accéder au secrétariat de l’instruction du TJ »*

# Echecs de contrôle d’accès

Directory listing, Direct access (url, id, ...), Fopen

# Directory listing

```
<VirtualHost *:80>

  ServerName  intranet.example.com

  Options +Indexes

</VirtualHost>
```



# Insecure Direct Object Reference (IDOR)

```
$ wget http://intranet.example.com/upload/secret.pem

$ wget http://api.example.com/Keys/1f5d6s2d1

$ wget http://shop.example.com/account/?customerid=1
```

# Fopen / Path traversal

```php
<?php

$file = "./some/dir/to/" . $_GET["file"] ;
$fp   = fopen($file) ;
$data = fread($fp, filesize($file)) ;
fclose($data) ;
echo $data ;

// readfile, file, file_get_contents, …
```

# Featured Backdoors

## Mode debug

```php
<?php

        $debug = isset($_GET["debug"]) ;
        $user  = $_SESSION["user"] ;

        if ($user->isAdmin() || $debug ) {
                do_admin_stuff($_GET, $_POST) ;
        }
```

# Featured Backdoors

## commandes cachées

**TCP/32764 router backdoor**

**Firmware Sercomm**

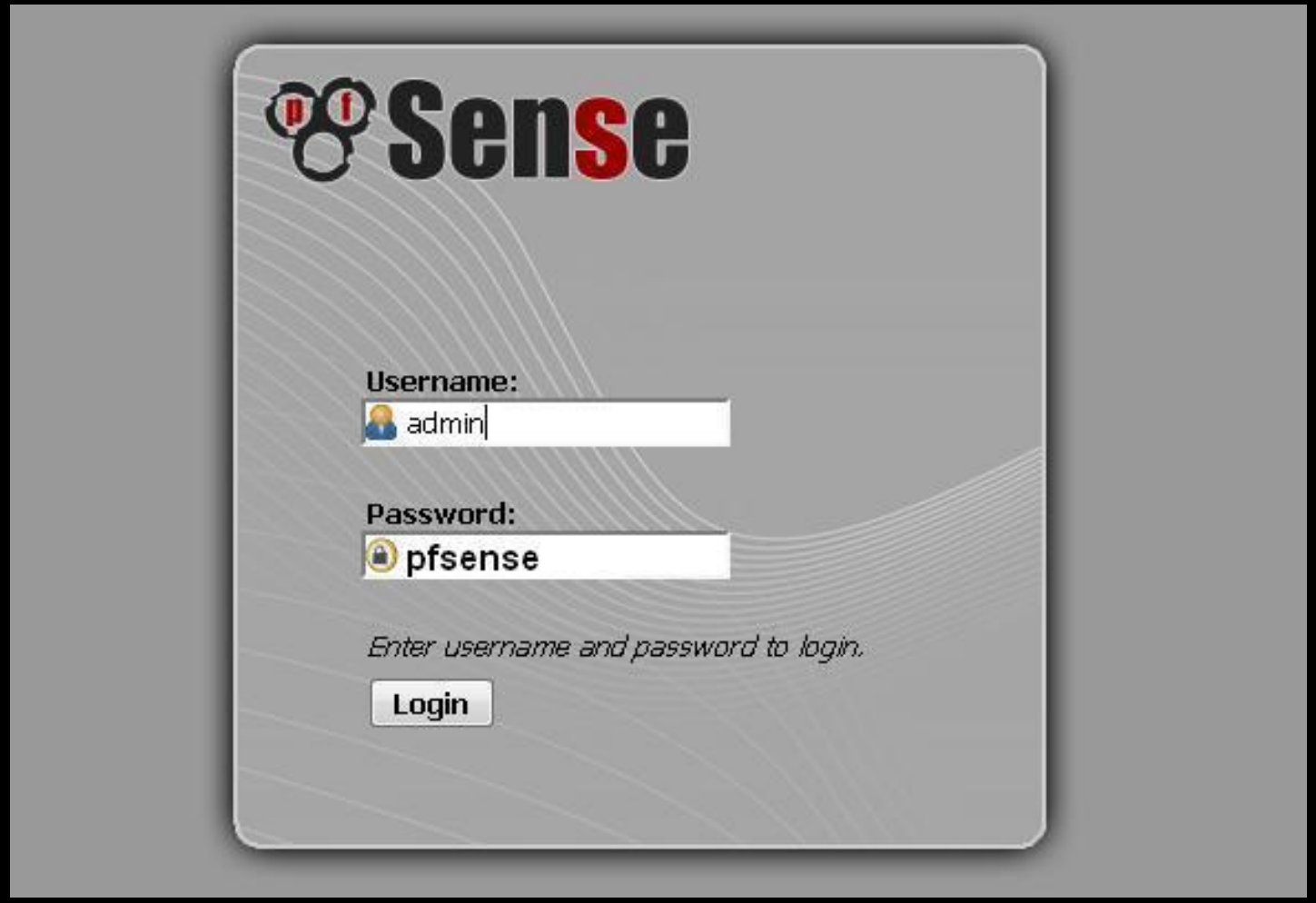
*CISCO Linksys Netgear Diamond*

**Commandes à distance**

*root sans authentification*

# Featured Backdoors

## compte par défaut



# Echecs d’authentification

Adresse IP, HTTP Referer, HTTP Host, Cookies…

# Adresse IP

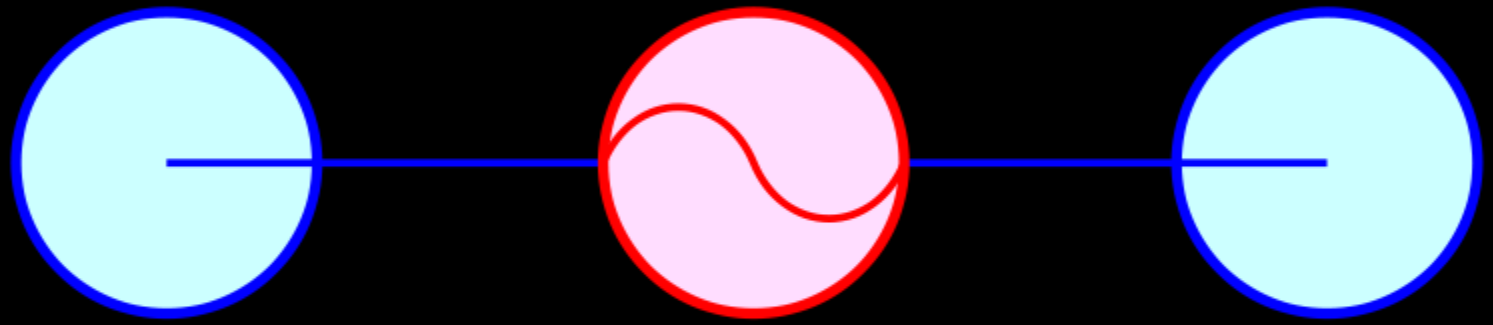
```
<VirtualHost *:80>

  ServerName  secured.example.com

  <Location />
    Require ip 87.98.129.198
    Require ip 192.168.0.0/24
    Require host trusted.example.com
    Require forward-dns other.example.com
    Require local
  </Location>

</VirtualHost>
```

# Géolocalisation

```
<VirtualHost *:80>

  ServerName  secured.example.com

  GeoIPEnable On
  GeoIPDBFile /path/to/GeoIP.dat

  <Location />
    Deny from GEOIP_COUNTRY_CODE=CN
    Deny from GEOIP_COUNTRY_CODE=RU
  </Location>

</VirtualHost>
```

# Limitations sur les adresses

## Man in the middle



# Limitations sur les adresses

## Spoofing

X-Forwarded-for : ip, proxy, …

*Provenance déclarative*

# Limitations sur les adresses

## Geoip

Pas digne de confiance

*VPN, proxies*

Pas fiable

*US > 44% des ips*

Dépendant

*Mise à jour des Bdd*

Pas précis

*Précision pays 99,8%, état 90%, ville 80%*

# En-tête HTTP : HOST

```
<VirtualHost *:80>

  ServerName  intranet.example.com

  Require expr "%{HTTP_HOST} == 'intranet.example.com'"

</VirtualHost>
```

# En-tête HTTP : Referer

```
<VirtualHost *:80>

  ServerName  intranet.example.com

  Require expr
        "%{HTTP_REFERER} -strmatch '*://%{HTTP_HOST}/*'"

</VirtualHost>
```

# En-tête HTTP : User Agent

```
<VirtualHost *:80>

  ServerName  intranet.example.com

  Require expr "! %{HTTP_USER_AGENT} -strmatch '*NESSUS*'"

</VirtualHost>
```

# Cookies

```php
<?php

function setAsAdmin() {
    $_COOKIES['admin'] = true ;
}

function isAdmin() {
    return @$_COOKIES['admin'] === true ;
}
```

# Limitations sur les en-têtes

Forgées par le client

# Role Based Access Control

Contrôle d’accès à base de rôles

# Utilisateurs / Subjects

Qui est contrôlé

*« Corinne HENIN »*

# Droits / Permissions

*Ce qui est contrôlé*

*« accéder au secrétariat de l'instruction »*

# Groupes / Roles

## Ensemble de droits

*« accès à l'instruction »,*
*« accès au service des scellés »…*

## *Ensemble de personnes*

*« Experts judiciaires en catégorie G.02.05 »*
*« Corinne HENIN », « Thibaut HENIN », …*

# Variante Hiérarchique

## Héritage entre les rôles

*« G – Médecine Légale, criminalistique et sciences criminelles »*

*« G.02 – Investigations scientifiques et techniques »*

*« G.02.05 – Documents informatiques »*

# Variante Contrainte

Un seul rôle a la fois

« Expert Judiciaire » / « Partie Civile »

# Principe du moindre privilège

Droits minimums

*(pour chaque groupe)*

Groupes minimums

*(pour chaque utilisateur)*