Hygiène numérique pour l'administrateur système

@aeris, 13 mai 2017

Aeris

Groupe cyber-terroriste individuel auto-radicalisé sur Internet

Mail / Jabber : aeris@imirhil.fr
Mastodon :
aeris@social.imirhil.fr

Blog : https://blog.imirhil.fr/
Conférences :
https://confs.imirhil.fr/

GPG : EFB7 4277 ECE4 E222
OTR : 5769 616D 2D3D AC72

Devops chez Cozy Cloud

Sommaire

⚠️ Disclaimer ⚠️

La sécurité est un processus, pas un produit
— *Bruce Schneier*

⚠️ Disclaimer ⚠️

> La sécurité est un processus, pas un produit
> — *Bruce Schneier*

#define MODÈLE_DE_MENACE

- NSA, système de sauvegarde mondial ?
- Miroslav, cybercriminel russe ?
- MIRAI, logiciel digital ?
- Kévin, script kiddie ?
- Marcel, votre boss ?
- Marion, votre collègue ?

⚠️ Disclaimer ⚠️

> La sécurité est un processus, pas un produit
> — *Bruce Schneier*

#define MODÈLE_DE_MENACE

- NSA, système de sauvegarde mondial ?
- Miroslav, cybercriminel russe ?
- MIRAI, logiciel digital ?
- Kévin, script kiddie ?
- Marcel, votre boss ?
- Marion, votre collègue ?

Adapter à **vos** besoins et contextes

- Le code de l'arme nucléaire US de 1963 à 2004 ?

⚠️ Disclaimer ⚠️

> La sécurité est un processus, pas un produit
> — *Bruce Schneier*

#define MODÈLE_DE_MENACE

- NSA, système de sauvegarde mondial ?
- Miroslav, cybercriminel russe ?
- MIRAI, logiciel digital ?
- Kévin, script kiddie ?
- Marcel, votre boss ?
- Marion, votre collègue ?

Adapter à **vos** besoins et **vos** contextes

- Le code de l'arme nucléaire US de 1963 à 2004 ? 00 00 00 00

⚠️ Disclaimer ⚠️

Ici, on considèrera :

- une sécurité « standard »
- pour un admin sys « standard »
- dans un contexte « standard »

On va parler uniquement **InfoSec** et pas du tout **OpSec**

Si vous avez des besoins spécifiques :

- Electronic Frontier Foundation
- Café vie privée
- Reporters sans Frontière

Installation de l'OS

Choix de l'OS (1/)

On parle de serveurs, donc :

- Un système stable
  - Du **GNU/Linux** ou du ***BSD**
  - Éviter les rolling-release (Gentoo, Arch…)
  - Éviter les distribs « kleenex » entre 2 versions (Ubuntu…)

Choix de l'OS (1/)

On parle de serveurs, donc :

- Un système stable
  - Du **GNU/Linux** ou du ***BSD**
  - Éviter les rolling-release (Gentoo, Arch…)
  - Éviter les distribs « kleenex » entre 2 versions (Ubuntu…)
- Un système **standard**
  - L'exotisme, c'est bien pour les vacances seulement (Alpine…)

Choix de l'OS (1/)

On parle de serveurs, donc :

- Un système stable
  - Du **GNU/Linux** ou du ***BSD**
  - Éviter les rolling-release (Gentoo, Arch…)
  - Éviter les distribs « kleenex » entre 2 versions (Ubuntu…)
- Un système **standard**
  - L'exotisme, c'est bien pour les vacances seulement (Alpine…)
- Un système **à jour en terme de sécurité**
  - Les LTS ne sont bizarrement pas forcément l'idéal
  - Surtout sur la fin

Choix de l'OS (2/)

FreeBSD®

CentOS

redhat®
LINUX

(Pour la suite, on va essentiellement parler Debian)

Installation de l'OS (1/)

- Installez **vous-même** (pas d'installeur OVH/Online)
  - Ça évite d'avoir n'importe quoi à la fin
  - On maîtrise ce qu'on installe (`~/.p` chez OVH)

Installation de l'OS (1/)

- Installez **vous-même** (pas d'installeur OVH/Online)
  - Ça évite d'avoir n'importe quoi à la fin
  - On maîtrise ce qu'on installe (`~/.p` chez OVH)
- N'hésitez pas à passer en mode ***expert***
  - Évite d'installer des choses inutiles
    Debian « next/next/next » : 925Mo, 480 paquets
    Debian « manuelle » : 625Mo, 248 paquets
    Debian « minimale » : 194Mo, 163 paquets

Installation de l'OS (1/)

- Installez **vous-même** (pas d'installeur OVH/Online)
  - Ça évite d'avoir n'importe quoi à la fin
  - On maîtrise ce qu'on installe (`~/.p` chez OVH)
- N'hésitez pas à passer en mode ***expert***
  - Évite d'installer des choses inutiles
    Debian « next/next/next » : 925Mo, 480 paquets
    Debian « manuelle » : 625Mo, 248 paquets
    Debian « minimale » : 194Mo, 163 paquets
- Désactivez l'installation des ***recommends*** et des ***suggests***
  - Évite d'installer des choses inutiles aussi

```
/etc/apt/apt.conf.d/60recommends
APT::Install-Recommends "0";
APT::Install-Suggests "0";
```

Installation de l'OS (2/)

Chiffrement ou pas **chiffrement des disques** ?

- Pour un **serveur** : bof
  - FDE difficile (problème du boot)
  - Ne protège que d'une saisie (offline), aucune utilité online
  - Limiter le chiffrement au strict nécessaire
- Pour une **machine utilisateur** : obligatoire !
  - Protection contre le vol/la perte
  - On éteint la machine !
- Dans tous les cas, privilégier ***LVM on LUKS***
  - Chiffrement intégral du disque (peu de métadonnées)
  - Une seule phrase de passe même si plusieurs partitions
  - Plus modulable

Installation de l'OS (3/)

- Activez les **mises-à-jour de sécurité et de publication**

```
/etc/apt/sources.list.d/debian.list
deb http://deb.debian.org/debian/ jessie main
deb http://deb.debian.org/debian/ jessie-updates main
deb http://deb.debian.org/debian-security/ jessie/updates main
```

- Inscrivez-vous auprès de la **liste de diffusion des alertes de sécurité**

https://lists.debian.org/debian-security-announce/

Sécurisation minimale

Sécurisation minimale (1/)

- Installez un **firewall**
  - *iptables* fait bien le boulot
  - Par défaut, on rejette tout le trafic entrant
  - On ne laisse passer explicitement que ce dont on a réellement besoin
    - HTTP (80), HTTPS (443), SSH (22/XXXX), mail (25/587/993)…

Sécurisation minimale (1/)

- Installez un **firewall**
  - *iptables* fait bien le boulot
  - Par défaut, on rejette tout le trafic entrant
  - On ne laisse passer explicitement que ce dont on a réellement besoin
    - HTTP (80), HTTPS (443), SSH (22/XXXX), mail (25/587/993)…
- L'ennemi est dorénavant **dans votre réseau**
  - Internet of shit (imprimantes, caméras, frigos, dildos…)
  - Mobilité (débilephones, ami à la maison…)

```
iptables-save -t filter
filter
:INPUT DROP
:FORWARD DROP
:OUTPUT DROP

# Windows, ça spam…
-A INPUT -p udp -d 255.255.255.255 -j DROP
-A INPUT -p udp -d X.X.X.255 -j DROP
-A INPUT -p udp -m multiport --dport netbios-ns,netbios-dgm,netbios-ssn -j DROP

-A INPUT -i lo -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p tcp -m tcp --dport ssh -j ACCEPT
-A INPUT -p tcp -m tcp --dport http -j ACCEPT
-A INPUT -p tcp -m tcp --dport https -j ACCEPT
-A INPUT -p tcp -m tcp --dport smtp -j ACCEPT
-A INPUT -p tcp -m tcp --dport submission -j ACCEPT
-A INPUT -p tcp -m tcp --dport imaps -j ACCEPT

-A OUTPUT -o lo -j ACCEPT
-A OUTPUT -p icmp -j ACCEPT
-A OUTPUT -m conntrack --ctstate NEW,RELATED,ESTABLISHED -j ACCEPT

COMMIT
```

Sécurisation minimale (3/)

- On désactive les **connexions par mot de passe** de SSH
  - Clef SSH only
  - Suffisamment robuste (RSA > 3072 bits ou ED25519 ❤️)
  - On en profite pour désactiver les vieux algos
  - Et pour changer le port par défaut
    - Ça n'évitera pas les attaques, mais au moins celles de Kévin
    - Ça nettoie sérieusement les logs

Sécurisation minimale (4/)

```
/etc/ssh/sshd_config
Port XXXX

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_dsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key

PermitRootLogin prohibit-password
PasswordAuthentication no

Ciphers chacha20-poly1305@openssh.com
KexAlgorithms curve25519-sha256@libssh.org
MACs umac-128-etm@openssh.com
```

Sécurisation minimale (5/)

- Activer la 2FA sur SSH (au moins pour `root`)
  - `apt install libpam-yubico`
  - https://developers.yubico.com/yubico-pam/
  - https://developers.yubico.com/yubico-pam/Yubikey_and_SSH_via_PAM.html

Sécurisation minimale (6/)

- Installation de ***fail2ban***
  - Bloque les ports via *iptables* en cas de bruteforce
  - SSH — SMTP/IMAP — HTTP
  - Pas la panacée mais ça nettoie les logs (Kévin…)
  - Gaffe à ne pas s'auto-bannir !

Sécurisation minimale (7/)

- Activation des **mises-à-jour de sécurité automatique**
  - Paquet *unattended-upgrades* + un peu de configuration https://wiki.debian.org/UnattendedUpgrades
  - Ça n'empèche certainement pas de passer sur sa machine régulièrement
  - Au moins pour redémarrer les services

Un peu de réseau (1/)

- Vérifier la source (*UDP spoofing*)

```
sysctl -w net.ipv4.conf.default.rp_filter = 1
```

Un peu de réseau (1/)

- Vérifier la source (*UDP spoofing*)

```
sysctl -w net.ipv4.conf.default.rp_filter = 1
```

- Activer les SYN cookies (limite le *SYN flooding*)

```
sysctl -w net.ipv4.tcp_syncookies = 1
```

Un peu de réseau (1/)

- Vérifier la source (*UDP spoofing*)

```
sysctl -w net.ipv4.conf.default.rp_filter = 1
```

- Activer les SYN cookies (limite le *SYN flooding*)

```
sysctl -w net.ipv4.tcp_syncookies = 1
```

- Rejeter les redirections ICMP (limite les MitM)

```
sysctl -w net.ipv4.conf.all.accept_redirects = 0
sysctl -w net.ipv4.conf.all.secure_redirects = 0
```

Un peu de réseau (1/)

- Vérifier la source (*UDP spoofing*)

```
sysctl -w net.ipv4.conf.default.rp_filter = 1
```

- Activer les SYN cookies (limite le *SYN flooding*)

```
sysctl -w net.ipv4.tcp_syncookies = 1
```

- Rejeter les redirections ICMP (limite les MitM)

```
sysctl -w net.ipv4.conf.all.accept_redirects = 0
sysctl -w net.ipv4.conf.all.secure_redirects = 0
```

- Désactiver le *source routing*

```
sysctl -w net.ipv4.conf.default.accept_source_route = 0
```

Applicatif

DNS

- Éviter les serveurs faisant autorité en tant que résolveur
  - DNS poisonning = export à l'extérieur…
  - Donc pas de *bind9*
  - Plutôt ***unbound*** ou ***knot***
  - Activer ***DNSSec*** (généralement par défaut)
  - Pour du cache, envisager un forward de confiance
    - ns0.fdn.org / ns1.fdn.org
    - ns0.ldn-fai.net

```
$ dig imirhil.fr

; <<>> DiG 9.10.3-P4-Debian <<>> imirhil.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9872
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;imirhil.fr.                    IN      A

;; ANSWER SECTION:
imirhil.fr.             3600    IN      A       62.210.124.124

;; AUTHORITY SECTION:
imirhil.fr.             604800  IN      NS      ns.imirhil.fr.
imirhil.fr.             604800  IN      NS      nssec.online.net.
imirhil.fr.             604800  IN      NS      primary.heberge.info.

;; ADDITIONAL SECTION:
ns.imirhil.fr.          555172  IN      A       62.210.124.124
ns.imirhil.fr.          555172  IN      AAAA    2001:bc8:3f23:100::1

;; Query time: 37 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Apr 03 23:56:24 CEST 2017
;; MSG SIZE  rcvd: 180
```

TLS (1/trop)

- Très dépendant des logiciels niveau config
- TL;DR : **TLSv1.2 + ECDHE+AES (+ ECDHE+CHACHA20+POLY1305)**
  - TLS<v1.2 = CBC padding attack, POODLE
  - Pas de PFS, pas de chocolat
  - DHE = lent, risqué (génération des clefs), mitm ☢
  - RC4 backdooré / 3DES faillible à sweet32
  - Le reste on n'en parle même pas (EXPORT, DES, NULL, ANONYMOUS…)
  - Taille de clef >3072 bits pour RSA (4096 bits en pratique)
  - SHA-1 pas un problème (utilisé pour du MAC) et en même temps un problème (authentification)
- Si compatibilité nécessaire, TLSv1.1 mais avec EtM
  - POODLE si pas de support client

HTTPD (1/)

- Masquer le n° de version, l'OS…

```
# apache
ServerTokens Prod
ServerSignature Off
# nginx
server_tokens off;
```

- Désactiver *mod_status*

```
a2dismod status && systemctl apache2 restart
```

- Désactiver le listing des répertoires

```
# apache
Options -Indexes
# nginx
# Par défaut (autoindex on;)
```

HTTPD (2/)

- **HTTPS** partout, activer **HSTS**
  - Let's Encrypt — https://hstspreload.org/

```
Strict-Transport-Security "max-age=31536000; includeSubDomains; preload"
```

- Activer les ***Content Security Policy***
  - Minimisation des droits (idéalement *none* ou *self*)
  - On évite les *inline*

```
Content-Security-Policy "default-src 'none'; style-src 'self';
                         script-src 'self'; img-src 'self';"
```

- D'autres en-têtes de sécurité

```
X-Content-Type-Options "nosniff"
X-Frame-Options "DENY"
X-XSS-Protection "1; mode=block"
```

SMTP / IMAPS / Submission

- Ne pas utiliser le port *SMTP* (25) pour l'envoi, mais ***Submission*** (587)
  - 25 (STARTTLS) = non authentifié, entrant only, anti-spam, greylist…
  - 587 (TLS) = authentifié, open bar
- ***Greylisting*** (*postgrey*)
- ***Antispam*** (*amavis*, *spamassassin*… Bon courage…)
- ***SPF*** & ***DKIM*** (*opendkim*)
  - (*DMARC* casse toute liste de diffusion)
- Bien vérifier qu'on n'est pas un **relai ouvert**
  - https://mxtoolbox.com/diagnostic.aspx
  - http://www.mailradar.com/openrelay/
- ***postfix*** + ***dovecot*** 💞

Les nouveaux dangers

ZMap / Scans.io / Shodan (1/)

ZMap / Scans.io / Shodan

Scan **TOUT** IPv4 chaque jour (ou presque)

Open-data sur les données

API accessibles

ZMap / Scans.io / Shodan (1/)

ZMap / Scans.io / Shodan

Scan **TOUT** IPv4 chaque jour (ou presque)

Open-data sur les données

API accessibles

Système en ligne = ETA exposition publique < 48h

ZMap / Scans.io / Shodan (1/)

ZMap / Scans.io / Shodan

Scan **TOUT** IPv4 chaque jour (ou presque)

Open-data sur les données

API accessibles

Système en ligne = ETA exposition publique < 48h

0day ou faille = ETA exploitation < 48h

Shodan Developers Book View All... Show API Key

SHODAN port:554 has_screenshot:true

Explore Downloads Reports Enterprise Access Contact Us My Account Upgrade

Exploits Maps Images Like 128 Download Results Create Report

91.78.224.215

ppp91-78-224-215.pppoe.mtu-net.ru

MTS Broadband

Added on 2017-04-17 17:28:56 GMT

Russian Federation, Moscow

Details

RTSP/1.0 200 OK

CSeq: 1

Shodan | Developers | Book | View All... | Show API Key

SHODAN

port:5900 has_screenshot:true

Explore | Downloads | Reports | Enterprise Access | Contact Us | My Account | Upgrade

Exploits | Maps | Images | Share Search | Download Results | Create Report

TOTAL RESULTS

2,700

TOP COUNTRIES

United States	380
China	248
Germany	161
Korea, Repu...	131
Russian Fed...	127

TOP ORGANIZATIONS

Administraci...	73
Beijing hsoft ...	67
Deutsche Tel...	64
Lg Powerco...	47
HiNet	27

TOP OPERATING SYSTEMS

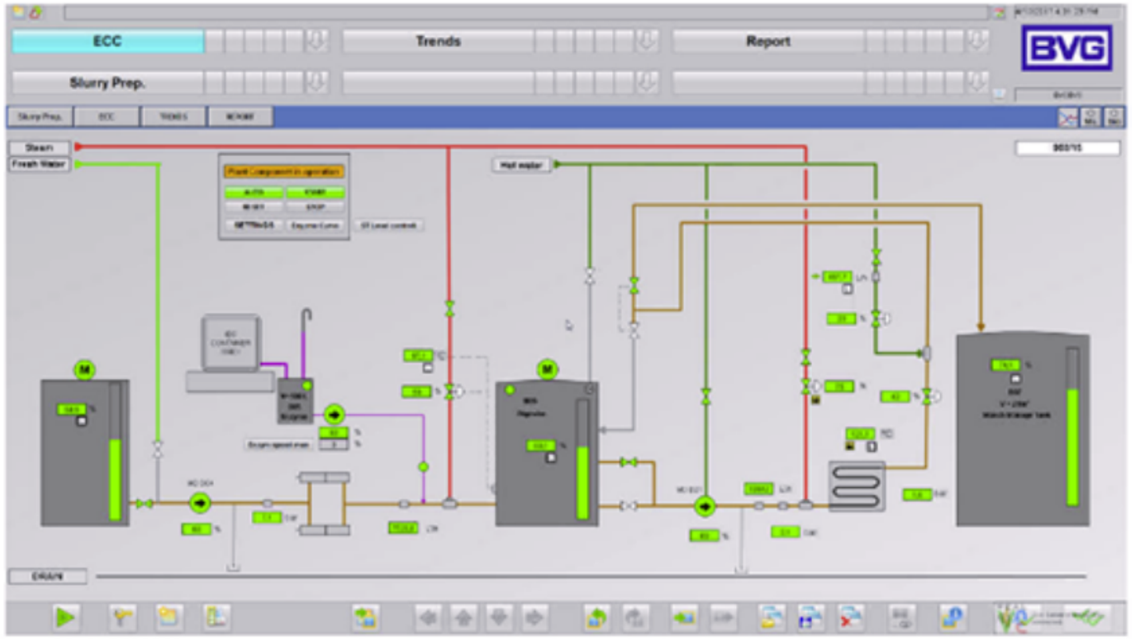
178.160.78.112

Hrvatski Telekom d.d.

Added on 2017-04-17 14:31:56 GMT

Croatia

Details



RFB 004.001

authentication disabled

Shodan | Developers | Book | View All... | Show API Key

SHODAN

yunohost/admin

Explore | Downloads | Reports | Enterprise Access | Contact Us | My Account | Upgrade

Exploits | Maps | Share Search | Download Results | Create Report

TOTAL RESULTS

1,113

TOP COUNTRIES

France	740
United Kingd...	76
United States	75
Germany	49
Netherlands	42

TOP SERVICES

HTTP	1,098
HTTPS	12
HTTP (8080)	2
8086	1

TOP ORGANIZATIONS

OVH SAS	257

302 Found
213.32.67.125
125.ip-213-32-67.eu
OVH SAS
Added on 2017-04-17 17:39:27 GMT
France
Details

```
HTTP/1.1 302 Moved Temporarily
Server: nginx
Date: Mon, 17 Apr 2017 17:36:16 GMT
Content-Type: text/html
Content-Length: 154
Connection: keep-alive
Location: https://213.32.67.125/yunohost/admin
```

302 Found
37.59.108.22
22.ip-37-59-108.eu
OVH SAS
Added on 2017-04-17 17:26:09 GMT
France
Details

```
HTTP/1.1 302 Moved Temporarily
Server: nginx
Date: Mon, 17 Apr 2017 17:25:58 GMT
Content-Type: text/html
Content-Length: 154
Connection: keep-alive
Location: https://37.59.108.22/yunohost/admin
```

302 Found
62.210.208.198
62-210-208-198.rev.poneytelecom.eu
ONLINE SAS
Added on 2017-04-17 17:08:51 GMT
France

```
HTTP/1.1 302 Moved Temporarily
Server: nginx
Date: Mon, 17 Apr 2017 17:08:48 GMT
Content-Type: text/html
```

Shodan | Developers | Book | View All... | Show API Key

SHODAN

X-Cozy-Login-Page

Explore | Downloads | Reports | Enterprise Access | Contact Us | My Account | Upgrade

Exploits | Maps | Share Search | Download Results | Create Report

TOTAL RESULTS

527

TOP COUNTRIES

France	373
United Kingd...	38
Germany	32
Canada	20
Italy	18

TOP SERVICES

HTTPS	469
HTTP	51
9443	3
HTTPS (8443)	1
Splunk	1

TOP ORGANIZATIONS

Cozy - Votre nuage personnel privé

151.80.223.138
ip138.ip-151-80-223.eu
OVH SAS
Added on 2017-04-17 17:13:11 GMT
Italy
Details

SSL Certificate

Issued By:
|- Common Name: **Let's Encrypt Authority X3**
|- Organization: **Let's Encrypt**
Issued To:
|- Common Name: **cozycloud.poinsaint-brissac.ovh**

Supported SSL Versions

TLSv1, TLSv1.1, TLSv1.2

```
HTTP/1.1 200 OK
Server: nginx/1.6.2
Date: Mon, 17 Apr 2017 17:12:57 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 2700
Connection: keep-alive
Vary: Accept-Encoding
X-Powered-By: Express
X-Cozy-Login-Page: true
ETag: W/"xEt2bQ/0h0H1jjAoi36DOg=="
Strict-Transport-Security: ma...
```

Cozy - Your Private Personal Cloud

Shodan | Developers | Book | View All... | Show API Key

SHODAN /nextcloud

Explore | Downloads | Reports | Enterprise Access | Contact Us | My Account | Upgrade

Exploits | Maps | Share Search | Download Results | Create Report

TOTAL RESULTS

773

TOP COUNTRIES

Germany	249
United States	141
China	66
France	48
Netherlands	36

TOP SERVICES

HTTPS	442
HTTP	167
NAS Web Int...	14
444	11
8081	8

TOP ORGANIZATIONS

01cloud

83.90.151.3
x1-6-24-7f-20-00-5f-3a.cpe.webspeed.dk
YouSee
Added on 2017-04-17 17:52:34 GMT
Denmark, Copenhagen
Details

Supported SSL Versions
TLSv1.2

```
HTTP/1.1 400 Bad Request
Server: nginx
Date: Mon, 17 Apr 2017 17:51:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Set-Cookie: oc2o9ns2zb4l=pkduv1sabvb8udic43h26sgka5; path=/nextcloud; secure; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
...
```

218.216.163.62

pc2a062.ztv.ne.jp
Ztv Co.,ltd
Added on 2017-04-17 17:43:51 GMT
Japan, Tsu
Details

```
HTTP/1.1 200 OK
Date: Mon, 17 Apr 2017 17:43:49 GMT
Server: Apache/2.4.23 (Unix) OpenSSL/1.0.1t PHP/5.6.25
Transfer-Encoding: chunked
Content-Type: text/html;charset=ISO-8859-1

515
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
```

ZMap / Scans.io / Shodan (3/)

Parade :

- Contenu vierge sur le vhost par défaut
- Pas de SAN sur TLS

Certificate Transparency (CT)

crt.sh : base de données *append-only* des émissions de certificats

crt.sh Identity Search

Group by Issuer

Criteria	Common Name LIKE '%.imirhil.fr'

Certificates

crt.sh ID	Logged At ⇧	Not Before	Identity	Issuer Name
121783787	2017-04-17	2017-04-17	aeris.imirhil.fr	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
111745888	2017-04-02	2017-04-02	social.imirhil.fr	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
111155563	2017-04-01	2017-04-01	nsa.imirhil.fr	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
111136627	2017-04-01	2017-04-01	status.imirhil.fr	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
111136611	2017-04-01	2017-04-01	paste.imirhil.fr	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
111136598	2017-04-01	2017-04-01	poche.imirhil.fr	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
111136580	2017-04-01	2017-04-01	links.imirhil.fr	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
111136547	2017-04-01	2017-04-01	cloud.imirhil.fr	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
111136509	2017-04-01	2017-04-01	confs.imirhil.fr	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
111136448	2017-04-01	2017-04-01	ask.imirhil.fr	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
97310478	2017-02-27	2017-02-27	radicale.imirhil.fr	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
83056849	2017-02-01	2017-02-01	tls.imirhil.fr	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
83056789	2017-02-01	2017-02-01	stats.imirhil.fr	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
83056728	2017-02-01	2017-02-01	blog.imirhil.fr	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
80296806	2017-01-25	2017-01-25	aeris.imirhil.fr	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
78828425	2017-01-20	2017-01-20	status.imirhil.fr	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
78611929	2017-01-19	2017-01-19	confs.imirhil.fr	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
72047014	2017-01-01	2017-01-01	nsa.imirhil.fr	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
72046991	2017-01-01	2017-01-01	paste.imirhil.fr	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
72046975	2017-01-01	2017-01-01	poche.imirhil.fr	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
72046938	2017-01-01	2017-01-01	links.imirhil.fr	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
72046896	2017-01-01	2017-01-01	cloud.imirhil.fr	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
72046817	2017-01-01	2017-01-01	ask.imirhil.fr	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Certificate Transparency (CT)

Parade :

- ~~Ne pas utiliser de CA *CT-aware*~~
- Utiliser une CA personnelle pour les choses critiques

Docker / Snap / Go

Tendance au « tout packagé »

- Trucs exotiques (Alpine…)
- Transforme le développeur en mainteneur
- YOLO BYIE

Docker / Snap / Go

Tendance au « tout packagé »

- Trucs exotiques (Alpine…)
- Transforme le développeur en mainteneur
- YOLO BYIE (You Only Live Once, But You Infect Everybody)

Branch: master ▾ discourse_docker / image / base / install-nginx Find file Copy path

xfalcox Fixes ngx_brotli compilation 1cd6aa5 on 28 Dec 2016

2 contributors

Executable File | 44 lines (30 sloc) | 1.99 KB Raw Blame History

```
9  git clone https://github.com/bagder/libbrotli
10 cd libbrotli
11 ./autogen.sh
12 ./configure
13 make install
14
15 cd /tmp
17
18 # this is the reason we are compiling by hand...
19 git clone https://github.com/google/ngx_brotli.git
20
21 curl -O https://nginx.org/download/nginx-$VERSION.tar.gz
22 tar zxf nginx-$VERSION.tar.gz
23 cd nginx-$VERSION
24
25 # so we get nginx user and so on
26 apt-get install -y nginx libpcre3 libpcre3-dev
27 # we don't want to accidentally upgrade nginx and undo our work
28 apt-mark hold nginx
29
30 # now ngx_brotli has brotli as a submodule
31 cd /tmp/ngx_brotli && git submodule update --init && cd /tmp/nginx-$VERSION
32
33 # ignoring depracations with -Wno-deprecated-declarations while we wait for this https://github.com/google/ngx_brotli/issues/39#iss
34 ./configure --with-cc-opt='-g -O2 -fPIE -fstack-protector-strong -Wformat -Werror=format-security -Wdate-time -D_FORTIFY_SOURCE=2 -
35
```

Branch: master ▾ discourse_docker / image / base / install-nginx Find file Copy path

xfalcox Fixes ngx_brotli compilation 1cd6aa5 on 28 Dec 2016

2 contributors

Executable File | 44 lines (30 sloc) | 1.99 KB Raw Blame History

```
9  git clone https://github.com/bagder/libbrotli
10 cd libbrotli
11 ./autogen.sh
12 ./configure
13 make install
14
15 cd /tmp
17
18 # this is the reason we are compiling by hand...
19 git clone https://github.com/google/ngx_brotli.git
20
21 curl -O https://nginx.org/download/nginx-$VERSION.tar.gz
22 tar zxf nginx-$VERSION.tar.gz
23 cd nginx-$VERSION
24
25 # so we get nginx user and so on
26 apt-get install -y nginx libpcre3 libpcre3-dev
27 # we don't want to accidentally upgrade nginx and undo our work
28 apt-mark hold nginx
29
30 # now ngx_brotli has brotli as a submodule
31 cd /tmp/ngx_brotli && git submodule update --init && cd /tmp/nginx-$VERSION
32
33 # ignoring depracations with -Wno-deprecated-declarations while we wait for this https://github.com/google/ngx_brotli/issues/39#iss
34 ./configure --with-cc-opt='-g -O2 -fPIE -fstack-protector-strong -Wformat -Werror=format-security -Wdate-time -D_FORTIFY_SOURCE=2 -
35
```

Version/intégrité ? `/tmp` (ugo=rwX+t) ? `make install` ? `apt install/hold` ?

Docker / Snap / Go

Besoin d’isoler une application : LXC

Docker / Snap / Go

Besoin d'isoler une application : LXC

⚠️ Conteneurisation : pas d'isolation

Une appli root du conteneur qui s'échappe = un attaquant root sur la machine physique

Docker / Snap / Go

Besoin d'isoler une application : LXC

⚠️ Conteneurisation : pas d'isolation

Une appli root du conteneur qui s'échappe = un attaquant root sur la machine physique

Si multi-tenant, virtualisation lourde obligatoire (Xen, Qemu/KVM, VirtualBox, VMWare…)

X.509 / TLS

X.509 et le problème des CA

- Contexte de moins en moins *safe*
  - Mobilité : wifi public, 3G/4G
  - FAI : mitm, dns spoof…
    - Bouygues Télécom
    - SFR
  - Compromission des CA
    - StartSSL / WoSign : 2.000 *mis-issued*
    - Symantec : 300.000 *mis-issued*
    - Symantec & BlueCoat
    - Let's Encrypt : « Paypal »

X.509 et le problème des CA

- Contexte de moins en moins *safe*
  - Mobilité : wifi public, 3G/4G
  - FAI : mitm, dns spoof…
    - Bouygues Télécom
    - SFR
  - Compromission des CA
    - StartSSL / WoSign : 2.000 *mis-issued*
    - Symantec : 300.000 *mis-issued*
    - Symantec & BlueCoat
    - Let's Encrypt : « Paypal »

Le système des CA a vécu…

Nécessité de remettre l'administrateur au cœur du cercle de confiance

HTTP Public Key Pinning (HPKP)

Déclare dans les en-têtes HTTP des épingles à vérifier à la prochaine visite

```
$ curl -sI https://imirhil.fr/ | grep public-key-pins
public-key-pins: max-age=5184000;
        pin-sha256="wdkD38iQQzxE7g0RpmN8VoaIqX7YmPWwoueD9Iqawfg=";
        pin-sha256="grcO0hHONi6YWf7AUdq1kPpDIVx6FIsKHLI3UugAhug="
```

On peut épingler :

- La racine : protège de l'émission d'un certificat par une autre CA
- L'intermédiaire : bof + risque de changement (Let's Encrypt)
- La feuille : peut être galère en cas de CDN

HTTP Public Key Pinning (HPKP)

Déclare dans les en-têtes HTTP des épingles à vérifier à la prochaine visite

```
$ curl -sI https://imirhil.fr/ | grep public-key-pins
public-key-pins: max-age=5184000;
        pin-sha256="wdkD38iQQzxE7g0RpmN8VoaIqX7YmPWwoueD9Iqawfg=";
        pin-sha256="grcO0hHONi6YWf7AUdq1kPpDIVx6FIsKHLI3UugAhug="
```

On peut épingler :

- La racine : protège de l'émission d'un certificat par une autre CA
- L'intermédiaire : bof + risque de changement (Let's Encrypt)
- La feuille : peut être galère en cas de CDN

Épingle de secours obligatoire

Une fois déployé, **beaucoup** réfléchir avant toute modification
Config cassée = anciens visiteurs KO durant **max-age**

DANE/TLSA (2/)

- Nécessite DNSSec 😣
- Double chaîne de certification
  - Applicatif (HTTP, XMPP, SMTP…)
  - DNS

DANE/TLSA (2/)

- Nécessite DNSSec 😣
- Double chaîne de certification
  - Applicatif (HTTP, XMPP, SMTP…)
  - DNS
- Aucun intérêt si clefs sur machine applicative
  - applicatif powned ⇒ DNSSec powned ⇒ TLSA powned

DANE/TLSA (2/)

- Nécessite DNSSec ☹
- Double chaîne de certification
  - Applicatif (HTTP, XMPP, SMTP…)
  - DNS
- Aucun intérêt si clefs sur machine applicative
  - applicatif powned ⇒ DNSSec powned ⇒ TLSA powned
  - stealth master DNS

DANE/TLSA (2/)

- Nécessite DNSSec ☹
- Double chaîne de certification
  - Applicatif (HTTP, XMPP, SMTP…)
  - DNS
- Aucun intérêt si clefs sur machine applicative
  - applicatif powned ⇒ DNSSec powned ⇒ TLSA powned
  - stealth master DNS
- OpenDNSSec
  - https://www.octopuce.fr/documentation-interne-a-octopuce-sur-dnssec/

Questions ?