

sh mac address-table

sh mac address-table count

```
1      0896.addd.7fc0      DYNAMIC      Gi0/1
1      74d4.35e2.01b5      DYNAMIC      Fa0/13
1      74d4.35e6.4d38      DYNAMIC      Fa0/23
1      74d4.35e6.bbd4      DYNAMIC      Fa0/1
Total Mac Addresses for this criterion: 24
SW1#sh mac address-table c
SW1#sh mac address-table count

Mac Entries for Vlan 1:
-----
Dynamic Address Count   : 4
Static Address Count    : 0
Total Mac Addresses     : 4

Total Mac Address Space Available: 8043
```

mac-address aging [*Durée en seconde*]

sh processes [*cpu*] [*history*]

Commandes sécurisations des ports :

switchport port-security (Active le port-security)

switchport port-security maximum [Valeur] (Modifie le nombre de MAC Address pouvant être apprises sur ce port)

switchport port-security violation [*protect/restrict/shutdown*] (Défini le mode de protection de port)

Commande visualisation sécurisation des ports :

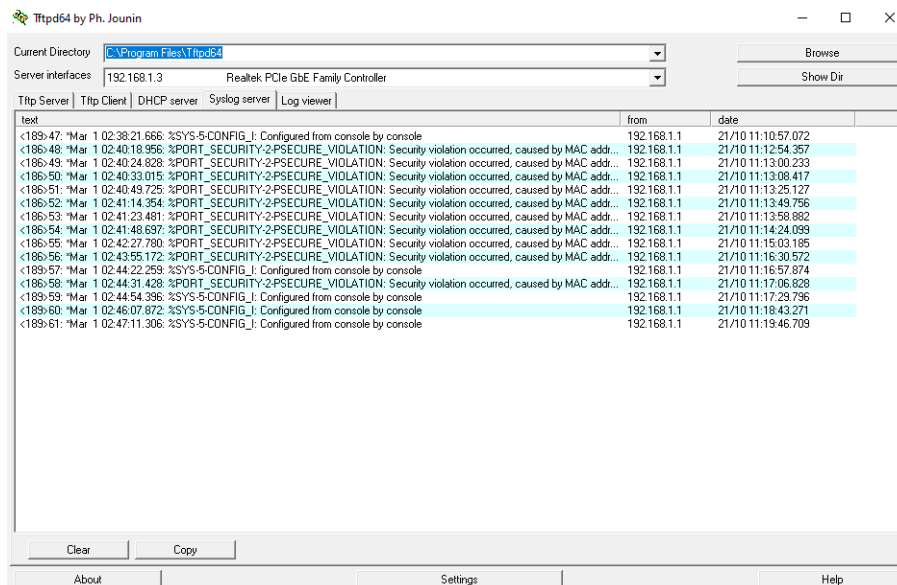
sh port-security | interface [0-24]

```
SW1#sh port-security
*Mar  1 02:47:11.306: %SYS-5-CONFIG_I: Configured from console by
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Secur
              (Count)         (Count)         (Count)
-----
      Fa0/1              1              1              436
-----
Total Addresses in System (excluding one mac per port)      : 0
Max Addresses limit in System (excluding one mac per port) : 8192
```

Commande kali pour lancer l'attaque CAM Overflow :

sudo macof -i [Nom de l'interface réseau kali] -n [Nombre d'adresses MAC à envoyer vers le switch]

Remonté de logs vers un serveur SYSLOG :



Visualisation d'un scan du réseau via la remontée de logs et un security-port défini en shutdown :

```
<186>63: *Mar 1 02:48:25.176: %PORT_SECURITY-2/PSECURE_VIOLATION: Security violation occurred, caused by MAC address 0800.2744.637d on port FastEthernet0/1. 192.168.1.1 21/10 11:21:00.581
<189>64: *Mar 1 02:48:26.183: %LINEPROTO-5/UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down 192.168.1.1 21/10 11:21:00.583
<187>65: *Mar 1 02:48:27.181: %LINK-3/UPDOWN: Interface FastEthernet0/1, changed state to down 192.168.1.1 21/10 11:21:02.580
```

Dans les logs on voit que le port a subi une attaque CAM Overflow et a été mis en mode errdisable

Commande pour activer un port suite à un errdisable :

errdisable recovery cause [Raison de l'errdisable]

errdisable recovery interval [Délai souhaité en seconde]

Visualisation dans la remontée de logs la réactivation du port suite au errdisable :

```
<189>67: *Mar 1 02:52:05.294: %PM-4-ERR_RECOVER: Attempting to recover from psecure-violation err-disable state on Fa0/1 192.168.1.1 21/10 11:24:40.691
<187>68: *Mar 1 02:52:08.875: %LINK-3/UPDOWN: Interface FastEthernet0/1, changed state to up 192.168.1.1 21/10 11:24:44.275
<189>69: *Mar 1 02:52:09.882: %LINEPROTO-5/UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up 192.168.1.1 21/10 11:24:44.277
```