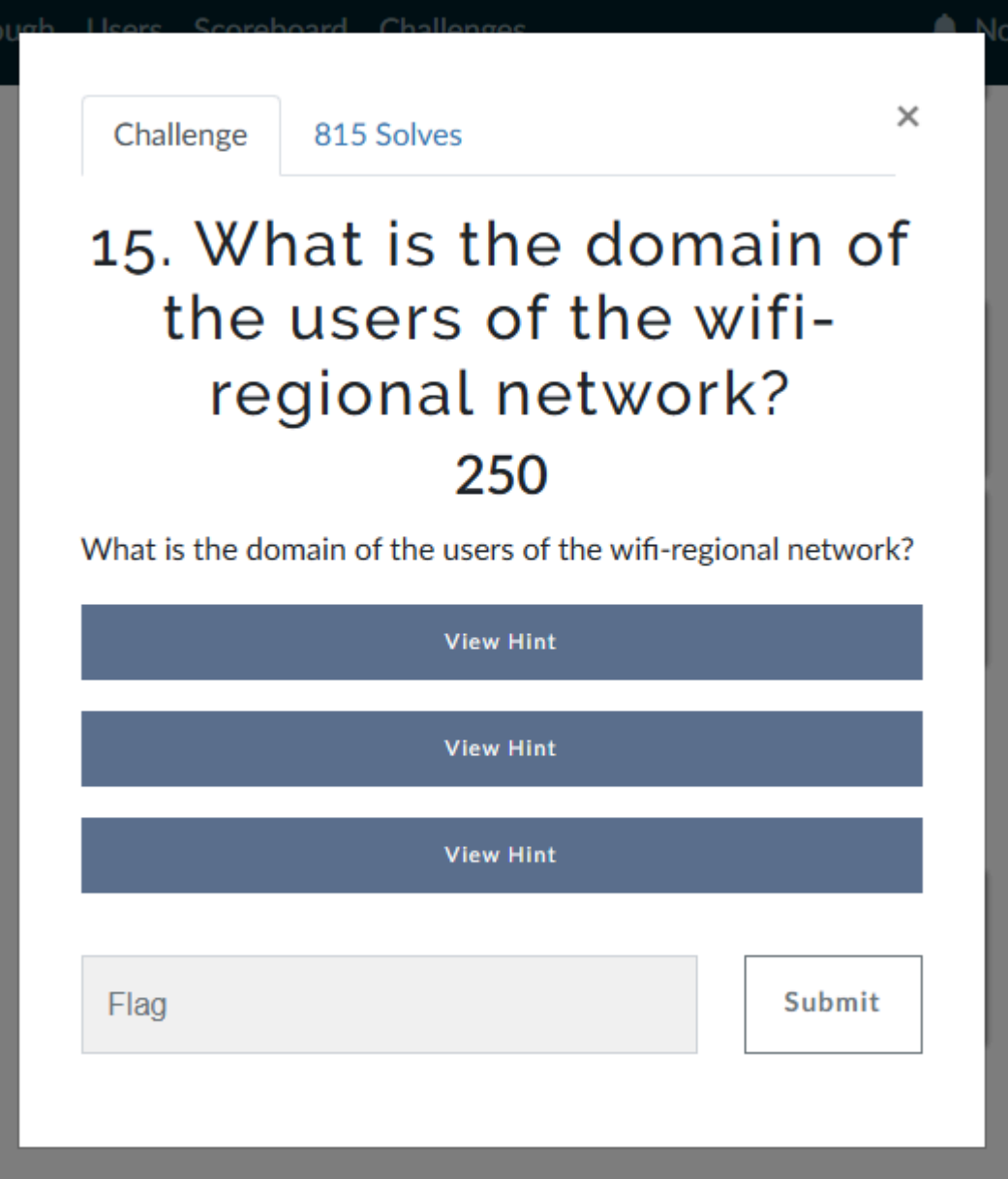


Actividad extra por no poder terminar o dar por realizado la 18, por su dificultad en el formulario de conexión.



The screenshot shows a challenge interface with a dark header containing navigation links: 'ough', 'Users', 'Scoreboard', and 'Challenges'. The challenge title is '15. What is the domain of the users of the wifi-regional network?' with a score of '250'. Below the title is the question text: 'What is the domain of the users of the wifi-regional network?'. There are three blue buttons labeled 'View Hint'. At the bottom, there is a 'Flag' button and a 'Submit' button.

Challenge 815 Solves

15. What is the domain of the users of the wifi-regional network?

250

What is the domain of the users of the wifi-regional network?

View Hint

View Hint

View Hint

Flag Submit

Leyendo la primera pista, nos recomienda usar WireShark.


```
564 10.092459 IntelCor_ac:53:50 Ubiquiti_71:22:16 TLSv1.2 79 Application Data
565 10.092480 Ubiquiti_71:22:16 IntelCor_ac:53:50 TLSv1.2 77 Application Data
567 10.092713 IntelCor_ac:53:50 Ubiquiti_71:22:16 EAP 44 Response, Protected EAP (EAP-PEAP)
568 10.092727 Ubiquiti_71:22:16 IntelCor_ac:53:50 EAP 42 Success
577 10.101188 Ubiquiti_7a:33:28 IntelCor_a9:de:55 EAP 43 Request, Identity
578 10.101191 Ubiquiti_7a:33:28 IntelCor_bd:64:54 EAP 43 Request, Identity
579 10.101194 IntelCor_bd:64:54 Ubiquiti_7a:33:28 EAP 63 Response, Identity
...
Frame 579: 63 bytes on wire (504 bits), 63 bytes captured (504 bits)
IEEE 802.11 QoS Data, Flags: .....T
Logical-Link Control
802.1X Authentication
Extensible Authentication Protocol
Code: Response (2)
Id: 199
Length: 25
Type: Identity (1)
Identity: CONTOSOREG\anonymous

0000 88 01 2c 00 f0 9f c2 7a 33 28 64 32 a8 bd 64 54 ..,....z 3(d2...dT
0010 f0 9f c2 7a 33 28 00 00 00 00 aa aa 03 00 00 00 ...z3(.....
0020 88 0e 01 00 00 19 02 c7 00 19 01 43 4f 4e 54 4f ..... ..CONTOSOREG\anonymous
0030 53 4f 52 45 47 5c 61 6e 6f 6e 79 6d 6f 75 73
```

Challenge

831 Solves

X

16. What is the email address of the servers certificate?

250

What is the email address of the server certificate?

View Hint

View Hint

Flag

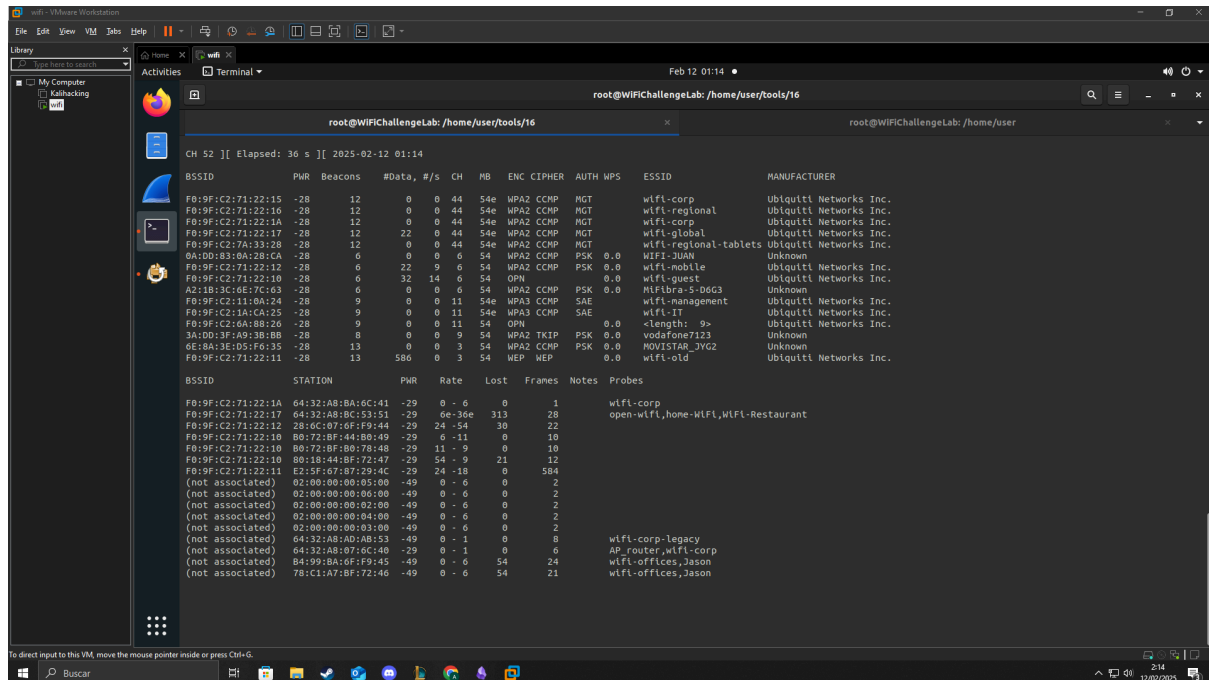
Submit

Leyendo la pista podemos utilizar un script que tenemos dentro de la carpeta de tools.

```
root@WiFiChallengeLab:/home/user/tools# ls
a1rgeddon  assless-chaps  cREAP  eapeak  extra-phishing-pages  hcxtools  hostapd-mana  ncapfilter.sh  UnicastDeauth  wifl_db  wiflpumpkin3  wpa_sycophant
air-hammer  borate.ap  EAP-buster  eaphammer  hashcat-6.0.0  hostapd-2.11  ndk4  reaver-wps-for-k-t6x  wacker  wiflphisher  wiflte2
root@WiFiChallengeLab:/home/user/tools#
```

Este se encarga de filtrar e indicarnos el certificado utilizado en las redes.

Por desconocimiento volvemos a realizar un análisis de más o menos un minuto para asegurar la captura de todo el contenido de la red Wifi.



Este script solo tiene dos argumentos en nuestro -f para indicarle el .cap y -C para obtener los certificados.

(Para realizar el comando de pcapFilter tuve problemas, es recomendable realizarlo en canales específicos, si realizas un cap con muchos Certs, al no mostrarlos por terminal intentara crear un archivo el cual nunca me aparecio, por comodidad mejor utilizarlo en canales con pocas conexiones)



Challenge

832 Solves



16. What is the email address of the servers certificate?

250

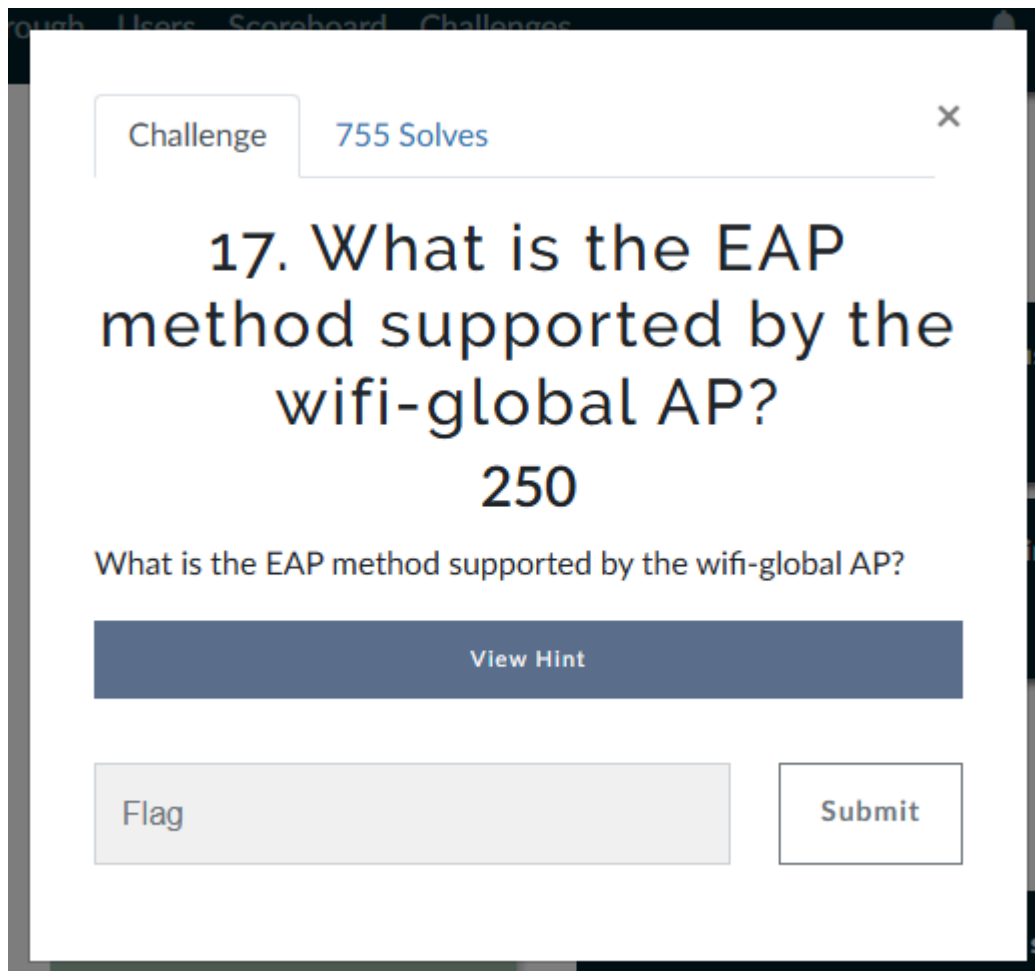
What is the email address of the server certificate?

View Hint

View Hint

server@WiFiChallenge.com

Submit



Para este caso leyendo la hint, nos recomiendan usar EAP_buster, herramienta ya descargada en el sistema.

```
root@wifiChallengeLab:~/home/user/tools/EAP_buster# bash EAP_buster.sh -h
EAP_buster by BlackArrow [https://github.com/blackarrowsec/EAP_buster]

WARNING
You need to use legitimate EAP identities in order to start the 802.1X authentication process and get reliable results (EAP identities can be collected using sniffing tools such as c
rEAP, just make sure you use a real identity and not an anonymous one => https://github.com/Sn1zz/crEAP)

Syntax: EAP_buster.sh <EAP_ESSID> <EAP_identity> <wifi_interface>
```

Wifi global utiliza el mismo canal que las dos actividades anteriores por lo que podemos aprovechar el .cap anterior.

(Despues de pegarme con crEAP.py, ya que al parecer tenemos que descargarnos un github (<https://github.com/Tylous/Scapy-com>) y realizar un “cd Scapy-com && python setup.py install”, tras esto tenemos la herramienta lista para utilizarla, tuve que realizar un par de .cap’s ya que por extraños motivos no me daba el User ID para usarlo en EAP_buster.sh)

```

root@WiFiChallengeLab:/home/user/Downloads# ./crEAP.py -r act17EAP-01.cap

      _____
     /  _  _  _  \
    /  _  _  _  \
   /  _  _  _  \
  /  _  _  _  \
 /  _  _  _  \
/  _  _  _  \
>
crEAP is a utility which will identify WPA Enterprise Mode Encryption types and if
insecure protocols are in use, crEAP will harvest usernames and handshakes.

Version: 1.4

[-] Searching for EAPOL packets from PCAP act17EAP-01.cap

[!] EAP-TLS Response ID Detected
[-] BSSID:      wifi-global
[-] Auth ID:    183
[-] User ID:    GLOBAL\GlobalAdmin
[-] Unique Harvested Users:
['GLOBAL\\GlobalAdmin']

```

Tras conseguir esto podemos utilizar la herramienta para obtener la flag.

```

root@WiFiChallengeLab:/home/user/tools/EAP_buster# bash EAP_buster.sh wifi-global "GLOBAL\GlobalAdmin" wlan1
EAP_buster by BlackArrow [https://github.com/blackarrowsec/EAP_buster]

WARNING
You need to use legitimate EAP identities in order to start the 802.1X authentication process and get reliable results (EAP identities can be collected using sniffing tools such as crEAP, just make sure you use a real identity and not an anonymous one => https://github.com/Snizz/crEAP)

not supported => EAP-TLS
not supported => EAP-PEAP_MSCHAPv2
not supported => EAP-PEAP_TLS
checking EAP-PEAP_GTC support ...

```

action process and get reliable results (EAP identities can be collected using sniffing tools such as crEAP, just make sure you use a real identity and not an anonymous one => <https://github.com/Snizz/crEAP>)

```

not supported => EAP-TLS
not supported => EAP-PEAP_MSCHAPv2
not supported => EAP-PEAP_TLS
not supported => EAP-PEAP_GTC
not supported => EAP-PEAP_OTP
not supported => EAP-PEAP_MD5-Challenge
not supported => EAP-TTLS_EAP-MD5-Challenge
not supported => EAP-TTLS_EAP-GTC
not supported => EAP-TTLS_EAP-OTP
not supported => EAP-TTLS_EAP-MSCHAPv2
not supported => EAP-TTLS_EAP-TLS
not supported => EAP-TTLS_MSCHAPv2
not supported => EAP-TTLS_MSCHAP
not supported => EAP-TTLS_PAP
not supported => EAP-TTLS_CHAP
not supported => EAP-FAST_MSCHAPv2
not supported => EAP-FAST_GTC
not supported => EAP-FAST_OTP

```

Al terminar nos encontramos con que no encontro nada, pero aun asi acabe probando y acerté con la primera, la cual era la que nos salia en crEAP.py:

```
root@WiFiChallengeLab:/home/user/Downloads# ./crEAP.py -r act17EAP-01.cap

      _____
     /  _  _  _  \
    /  _  _  _  \
   /  _  _  _  \
  /  _  _  _  \
 /  _  _  _  \
/  _  _  _  \
 \  _  _  _  /
  \  _  _  _ /
   \  _  _  /
    \  _  _ /
     \  _  /
      \_/_/

crEAP is a utility which will identify WPA Enterprise Mode Encryption types and if
insecure protocols are in use, crEAP will harvest usernames and handshakes.

Version: 1.4

[-] Searching for EAPOL packets from PCAP act17EAP-01.cap

[!] EAP-TLS Response ID Detected
[-] BSSID:      wifi-global
[-] Auth ID:    183
[-] User ID:    GLOBAL\GlobalAdmin
[-] Unique Harvested Users:
['GLOBAL\\GlobalAdmin']
```

Recon MGT

15. What is the domain of the ✓

250

16. What is the email address ✓

250

17. What is the EAP method s ✓

250