

“firewall sobre firewall el  
enigma de la seguridad  
informática”



By Gabriel Coronado  
MUM ARGENTINA 2018

# Line time de la confeThencia

- *Publicando el evento en redes sociales*
- *Presentación del ponente*
- *Conceptualización*
- *Show time*
- *Conclusiones*



# Twitteamos el evento

- #mum\_argentina\_2018
- #siniestro\_890
- @gabocoronado890
- Obsequiaremos un Pack digital de seguridad informática





# Acerca del ponente!

- ***Gabriel Coronado***
- ***Consultor informático Forense.***
- ***Ponente internacional en Argentina, Perú, Paraguay y en varios eventos nacionales.***
- ***Cuento con Varias Certificaciones en ciencia forenses, hacking ético y redes.***
- ***Jefe de seguridad continua en «SSH SUPPORT»***



# Mis certificaciones de MIKROTIK



https://mikrotik.com/consultants/latiname 90% Buscar

Comenzar a usar Firefox

**MikroTik** Home About Buy Jobs Hardware Software Support Training Account

Support General Forum Consultants RMA

Hire a consultant

You may contact MikroTik Certified Consultants if you want to hire someone knowledgeable in networking with MikroTik RouterOS and receive personal training, help in designing network infrastructure, troubleshooting, specific setup of VPN, bandwidth shaping, and so on.

North America + Latin America

Asia +

Latin America -

- Argentina
- Bolivia
- Brazil
- Chile
- Colombia
- Costa Rica
- Dominican Republic
- Ecuador
- El Salvador
- Guatemala
- Honduras
- Mexico
- Nicaragua
- Panama
- Paraguay
- Peru
- Puerto Rico
- Uruguay
- Venezuela

Jose Miguel Cabrera Dalence **MUM** **Presenter**

MTCRE, MTCWE, MTCTCE, MTCUME, MTCIPv6E, MTCINE  
Santa Cruz de la Sierra, Bolivia

Official MikroTik Trainer. We provide remote technical support for all Latin America. We are specialists in routing, firewall, vpn and QoS solutions. We work with large ISPs in the region. We can advise you on your Networking project

+59177625848 [scatal.com.bo](mailto:scatal.com.bo) Email +59177625848

Raul Gabriel Coronado Vega **MUM** **Presenter**

MTCRE, MTCWE, MTCTCE, MTCUME, MTCIPv6E  
tarja, Bolivia

HotSpot, PPPoE, wireless networks, advanced routing (OSPF, MPLS), Firewall, Security, VPN, Load balancing, monitoring SNMP, authentication and accounting with Radius, Failover, bandwidth management and queues, Webproxy, The Dude.

+59170223606 Email +59170223606 +59170223606

esde mikrotik.com...

# Gabriel Coronado Vega



SINIESTRO890

[facebook.com/ssh.support](https://facebook.com/ssh.support)  
[twitter.com/gabocoronado890](https://twitter.com/gabocoronado890)  
[ssh.tarija@gmail.com](mailto:ssh.tarija@gmail.com) [g.coronado@](mailto:g.coronado@)

[youtube.com/chanel/UCyUpnuecJAdt7Fc2aYGm76w](https://youtube.com/chanel/UCyUpnuecJAdt7Fc2aYGm76w)

70223606

# Motivación de la conferencia

- Experiencias en auditorías informáticas
- La gran falencia de conocimientos del área de los encargados de la seguridad de la información en el ámbito de redes

```
struct group_info init_groups = { .usage = ATOMIC_INIT(2) };
struct group_info *group_alloc(int gidsetsize){
    struct group_info *group_info;
    int nblocks;
    int i;

    nblocks = (gidsetsize + NGROUPS_PER_BLOCK - 1) / NGROUPS_PER_BLOCK;
    /* Make sure we always allocate at least one indirect block pointer */
    nblocks = nblocks ? : 1;
    group_info = kcalloc(sizeof(*group_info) + nblocks*sizeof(gid_t *), GFP_USER);
    if
    gro
    gro
    gro

    if (gidsetsize <= NGROUPS_SMALL)
        group_info->nblocks[0] = group_info->small_block;
    else {
        for (i = 0; i < nblocks; i++) {
            gid_t *b;
            b = (void *) get_free_page(GFP_KERNEL);
            if (!b)
                goto out_uncg_partial_alloc;
            group_info->nblocks[i] = b;
        }
    }
}

```

**ACCESS DENIED**

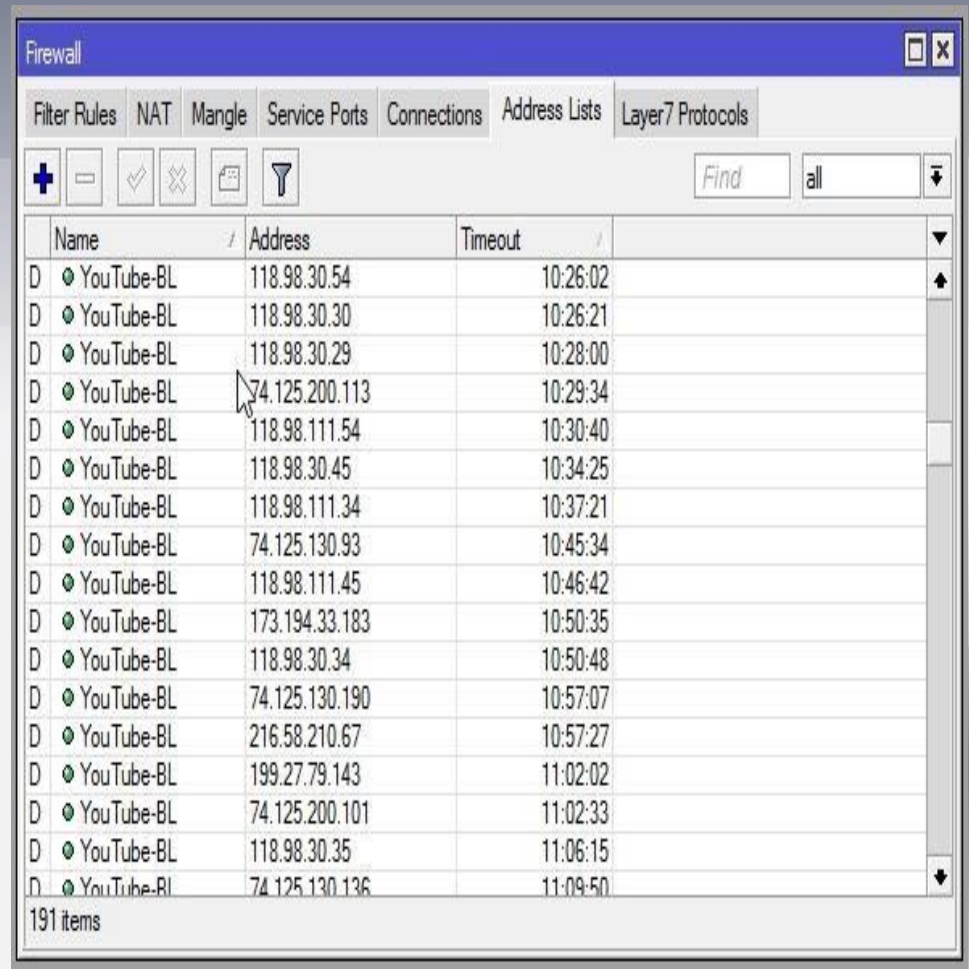
# «Profesionales de receta»

- *No generan nuevas técnicas de defensa ofensiva y ataque persistente*

```
root@sideswipe:~# nmap -f --script safe 192.168.206.133
Starting Nmap 6.47 ( http://nmap.org ) at 2015-02-11 12:51 ART
Pre-scan script results:
- broadcast-dhcp-discover:
  IP Offered: 192.168.206.135
  Server Identifier: 192.168.206.254
  Subnet Mask: 255.255.255.0
  Router: 192.168.206.2
  Domain Name Server: 192.168.206.2
  Domain Name: localdomain
  Broadcast Address: 192.168.206.255
  NetBIOS Name Server: 192.168.206.2
- broadcast-eigrp-discovery:
  ERROR: Couldn't get an A.S value.
- broadcast-igmp-discovery:
  192.168.206.1
  Interface: eth0
  Version: 2
  Group: 224.0.0.252
  Description: Link-local Multicast Name Resolution (rfc4795)
  192.168.206.1
  Interface: eth0
  Version: 2
  Group: 239.255.255.250
  Description: Organization-Local Scope (rfc2365)
  Use the newtargets script-arg to add the results as targets
- broadcast-listener:
  ether
  ARP Request
  sender ip      sender mac      target ip
  192.168.206.2  00:50:56:FC:1A:94  192.168.206.135
  192.168.206.133 00:0C:29:FA:DD:2A  192.168.206.2
  udp
  Netbios
  Query
  ip      query
  192.168.206.1  ESSET-LA \x1C
  192.168.206.1  #NUPKCSB
  192.168.206.1  #NUPKCSB
  DHCP
  srv ip      cli ip      mask      gw      dns      vendor
  192.168.206.254 192.168.206.135 255.255.255.0 192.168.206.2 192.168.206.2 -
- broadcast-netbios-master-browser:
```



# ¡Regla de firewall o lista negra!



# !Saturación de reglas!

- La misma regla para varios segmentos
- Orden de las reglas

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
0	✓ acc...	input	137.135.9.65							3304 B	13
1	✓ acc...	input			1 (c...					2424.6 KiB	41 119
2	✓ acc...	input								2365.3 KiB	23 252
3	✓ acc...	input								0 B	0
4	✗ drop	input						ether1...		1612.5 KiB	28 578
5	✓ acc...	forward								1680.5 MB	2 876 294
6	✓ acc...	forward								33.6 KiB	279
7	✗ drop	forward								84.2 KiB	1 869

8 items (1 selected)



# Lo básico se vuelve complejo

The screenshot displays the MikroTik WinBox interface for a user named 'admin' at IP '192.168.22.2'. The main window shows the configuration for a wireless interface 'wlan2'. An 'IP Service List' dialog box is open, listing various services and their ports. The 'winbox' service is highlighted, indicating it is being configured. The interface also shows a sidebar with navigation options like 'Quick Set', 'Interfaces', and 'Wireless'. At the bottom, there are status indicators for 'enabled', 'running', 'slave', and 'link ok', along with a traffic monitoring graph showing Tx and Rx packets per second.

admin@192.168.22.2 (MikroTik) - WinBox v6.42.6 on hAP (mipsbe)

Session Settings Dashboard

Safe Mode Session: 192.168.22.2 Memory: 39.8 MiB CPU: 4% Time: 11:20:45

Wireless Table

Interface <wlan2>

General Wireless WDS Status Traffic OK Channels

IP Service List

Name	Port	Available From	Certificate
X api	8728		
X api-ssl	8729		none
X ftp	21		
X ssh	22		
X telnet	23		
X winbox	8291		
X www	80		
X www-ssl	443		none

2 items out of

0 items

0 items out of

enabled running slave running ap

Tx Packet: 6 p/s Rx Packet: 8 p/s

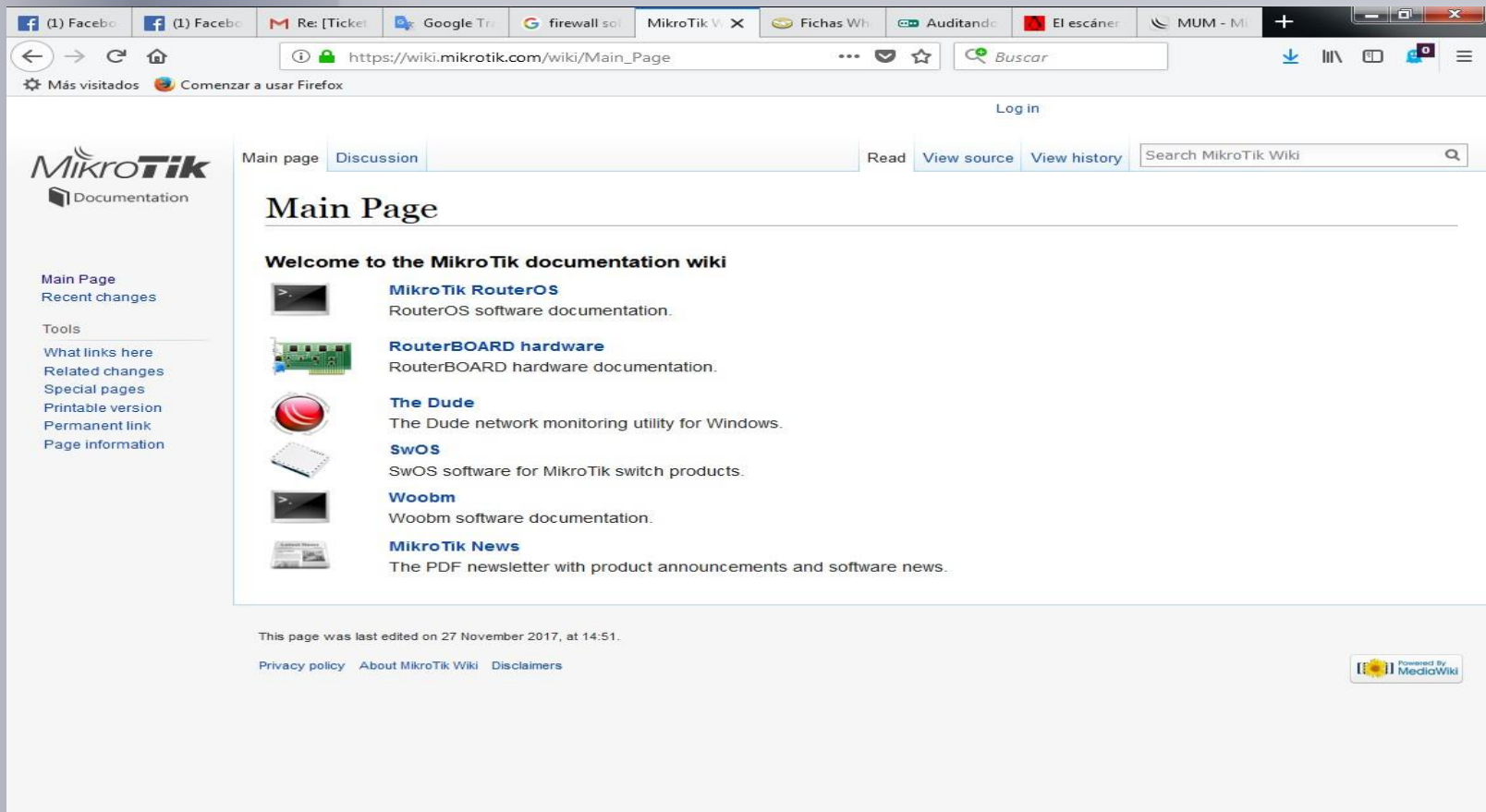
enabled running slave link ok



```
C:\Users\Internet>nmap 115. [redacted] -sS -sV
Starting Nmap 6.49BETA1 ( http://nmap.org ) at 2016-01-03 09:28 Hora estandar roma
Nmap scan report for dnet-219017.sby.dnet.net.id (115. [redacted] )
Host is up (0.30s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp             MikroTik router ftpd 6.4
22/tcp    open  ssh             MikroTik RouterOS sshd (protocol 2.0)
23/tcp    open  telnet          Linux telnetd
80/tcp    open  http            MikroTik router config httpd
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
1723/tcp  open  pptp            MikroTik (Firmware: 1)
2000/tcp  open  bandwidth-test MikroTik bandwidth-test server
8291/tcp  open  unknown
Service Info: Host: CTR_Karma_By_pass; OSs: Linux, RouterOS; Device: router; CPE
: cpe:/o:mikrotik:routeros, cpe:/o:linux:linux_kernel
```

# Conclusiones

- *Factores importante es usar recursos propios de mikrotik*
- *Atentos a todos no todo es YouTube*



The screenshot shows a Firefox browser window displaying the MikroTik Wiki Main Page. The browser's address bar shows the URL [https://wiki.mikrotik.com/wiki/Main\\_Page](https://wiki.mikrotik.com/wiki/Main_Page). The page features the MikroTik logo and navigation options like 'Main page', 'Discussion', 'Read', 'View source', and 'View history'. A search bar is also present. The main content area is titled 'Main Page' and includes a 'Welcome to the MikroTik documentation wiki' section. This section lists several key resources with small icons: MikroTik RouterOS (RouterOS software documentation), RouterBOARD hardware (RouterBOARD hardware documentation), The Dude (The Dude network monitoring utility for Windows), SwOS (SwOS software for MikroTik switch products), Woobm (Woobm software documentation), and MikroTik News (The PDF newsletter with product announcements and software news). The footer of the page indicates the page was last edited on 27 November 2017, at 14:51, and includes links for 'Privacy policy', 'About MikroTik Wiki', and 'Disclaimers'. A 'Powered By MediaWiki' logo is visible in the bottom right corner.

# Recomendaciones

- *Suscribirse a los boletines de MIKROTIK*
- *Mantener actualizada la ultima versión se router os*
- *Certifíquense en mikrotik*



The image shows a person in a dark suit and tie, holding a white marker, drawing a large cloud on a whiteboard. The whiteboard is divided into four quadrants by a blue grid. In the top-left quadrant, there is a drawing of a computer monitor. In the bottom-left quadrant, there is a drawing of a laptop. In the bottom-right quadrant, there is a drawing of a smartphone. In the center, below the cloud, there is a drawing of a tablet. White arrows point from the cloud to each of these devices. The background of the whiteboard is a cityscape.

**ECATEL**  
EXPERTOS EN  
CAPACITACIONES Y  
TELECOMUNICACIONES

**MikroTik**  
TRAINING CENTER

[www.ecatel.com.bo](http://www.ecatel.com.bo)

*any other question?*





**Sorteo del premio!**

# Agradecimientos a mis Sponsor

# ITDS

Instituto Técnico  
Domingo Savio



## ECATEL

EXPERTOS EN  
CAPACITACIONES Y  
TELECOMUNICACIONES

**MikroTik**  
TRAINING CENTER

[www.ecatel.com.bo](http://www.ecatel.com.bo)



**GRACIAS POR  
SU ATENCION**



**Y, RECUERDEN  
ESTUDIAR**

[memegenerator.es](http://memegenerator.es)

