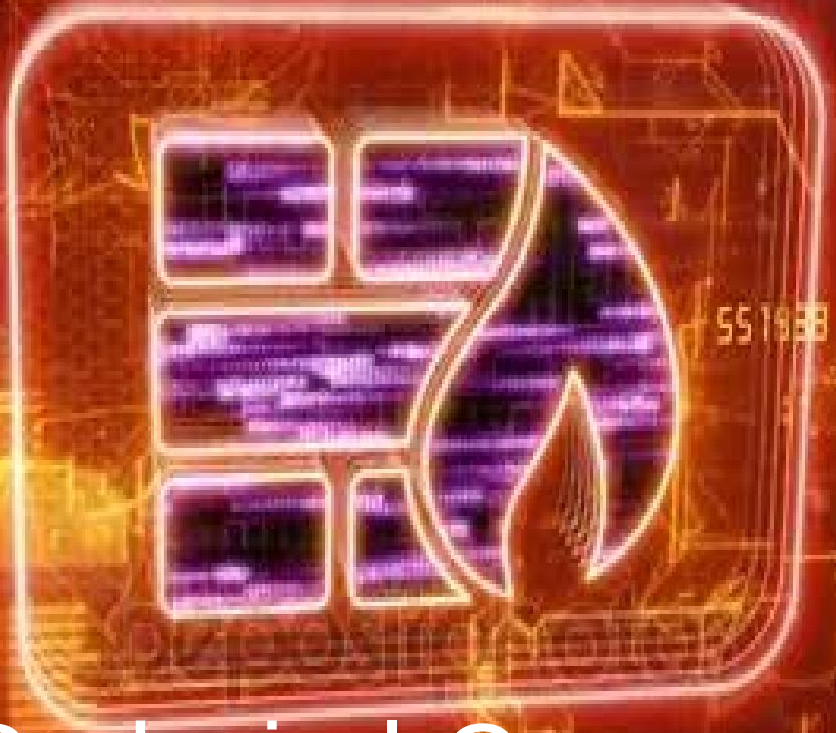
“firewall sobre firewall el enigma de la seguridad informática”



By Gabriel Coronado

MUM ARGENTINA **2018**

Line time de la confeThencia

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

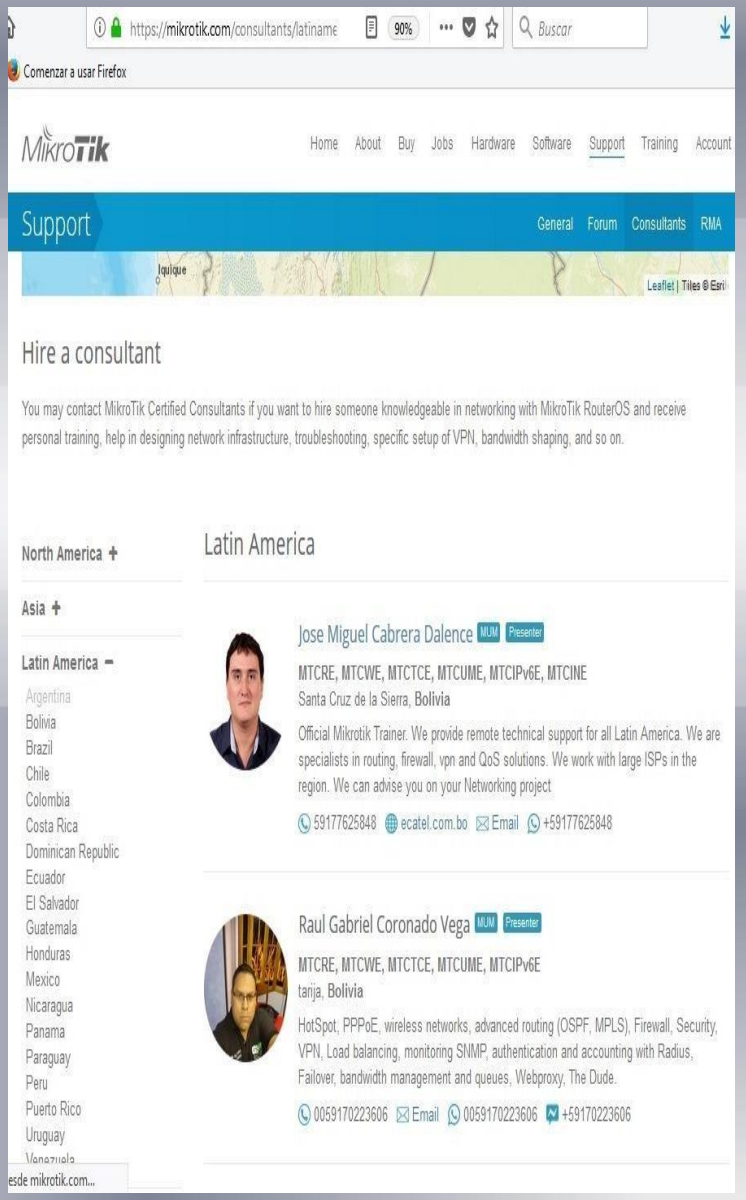
Twitteamos el evento

- #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»**

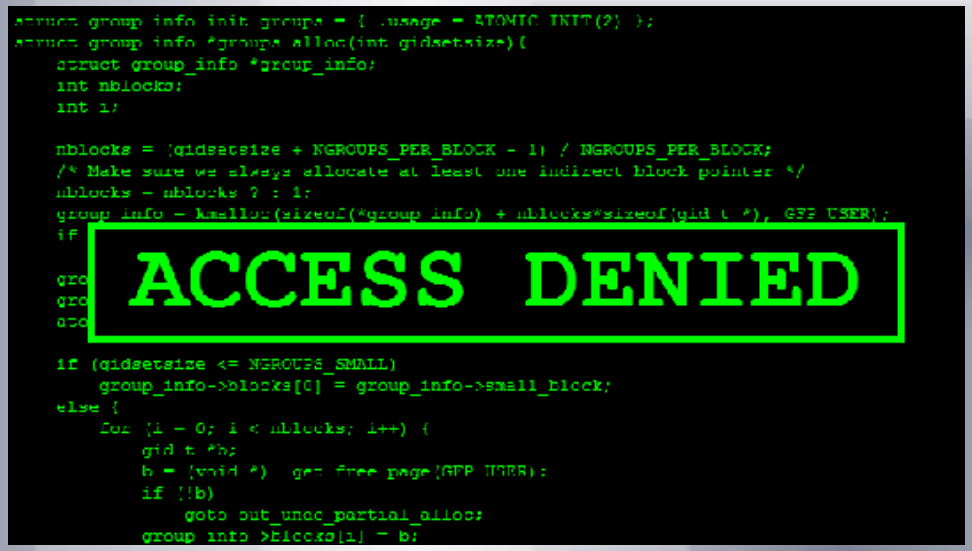
Mis certificaciones de MIKROTIK




Gabriel Coronado Vega
SINIESTRO890
facebook.com/ssh.support
twitter.com/gabocoronado890
ssh.tarija@gmail.com g. coronado@
youtube.com/chanel/UCyUpnuecJAdt7Fc2aYGm76w
70223606

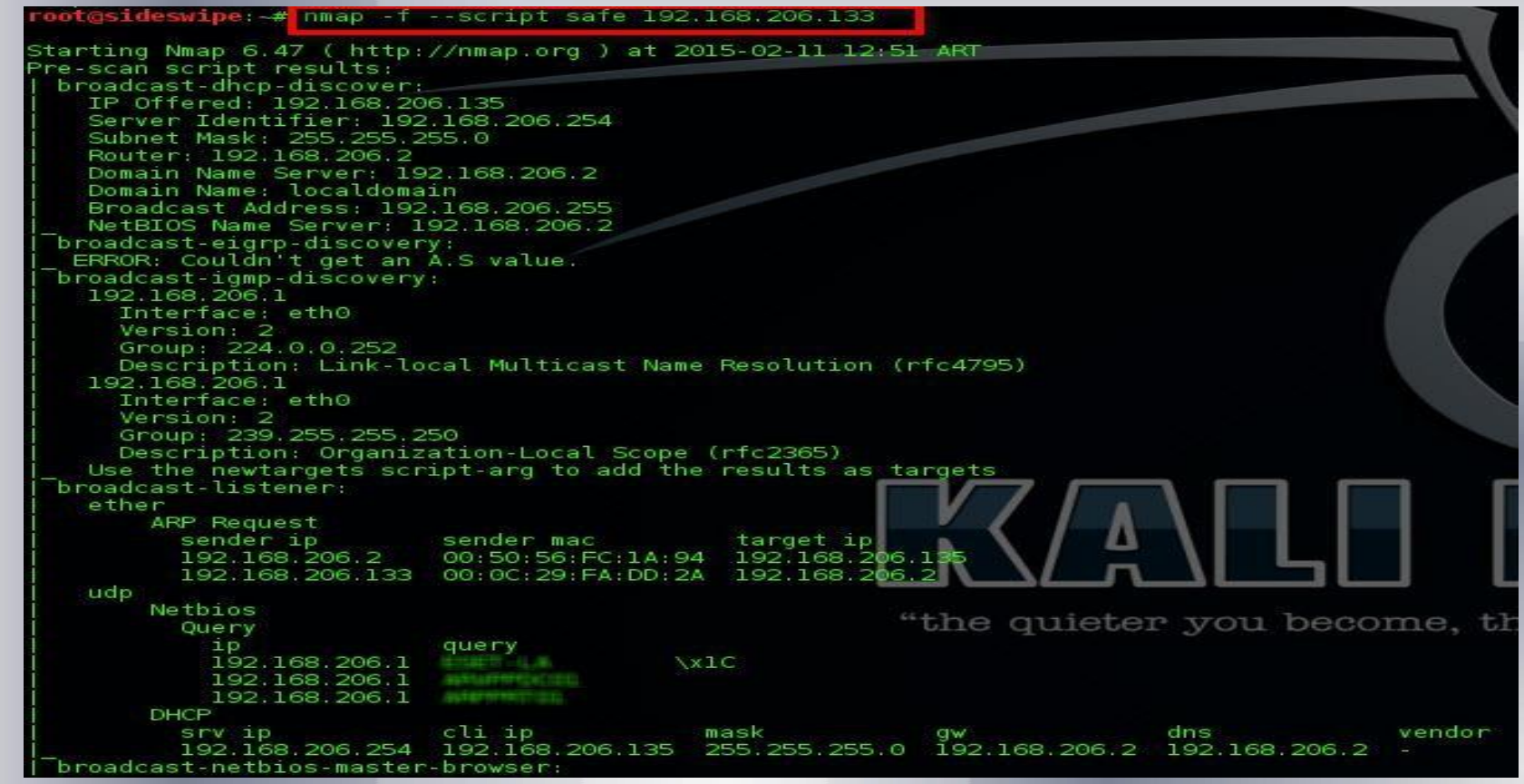
Motivacion de la conferencia

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

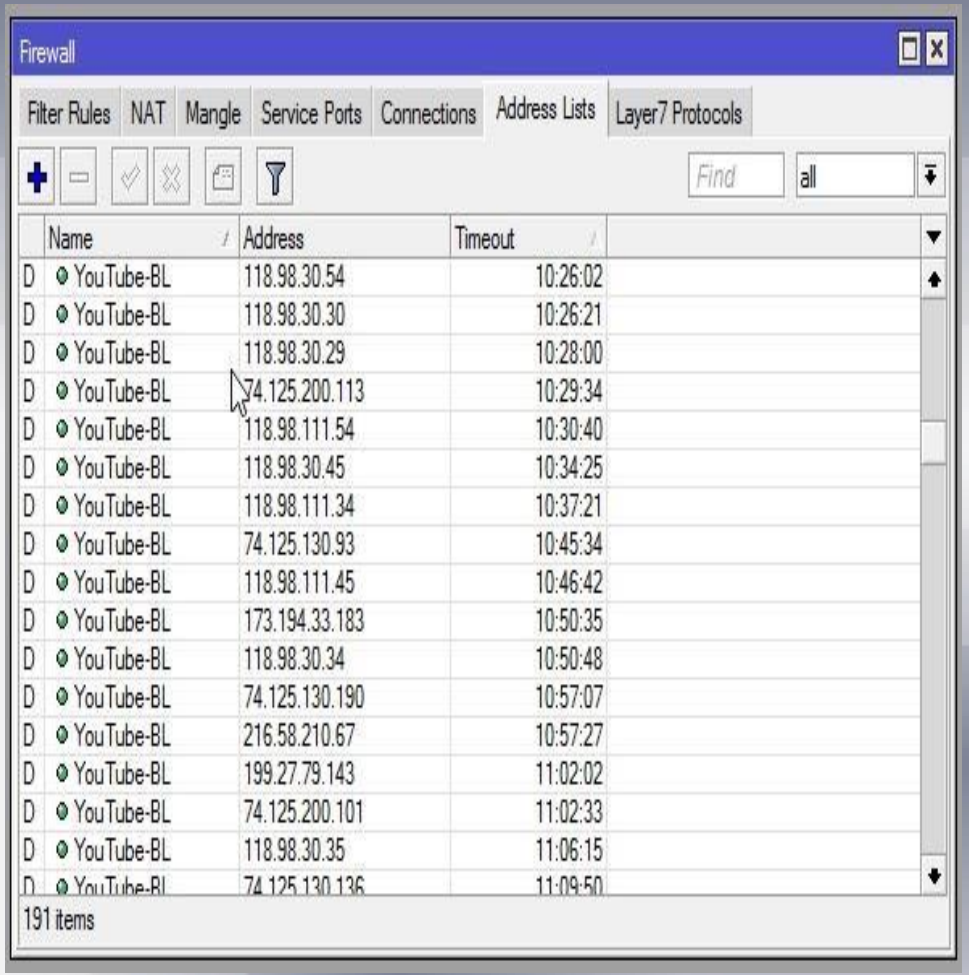


«Profesionales de receta»

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

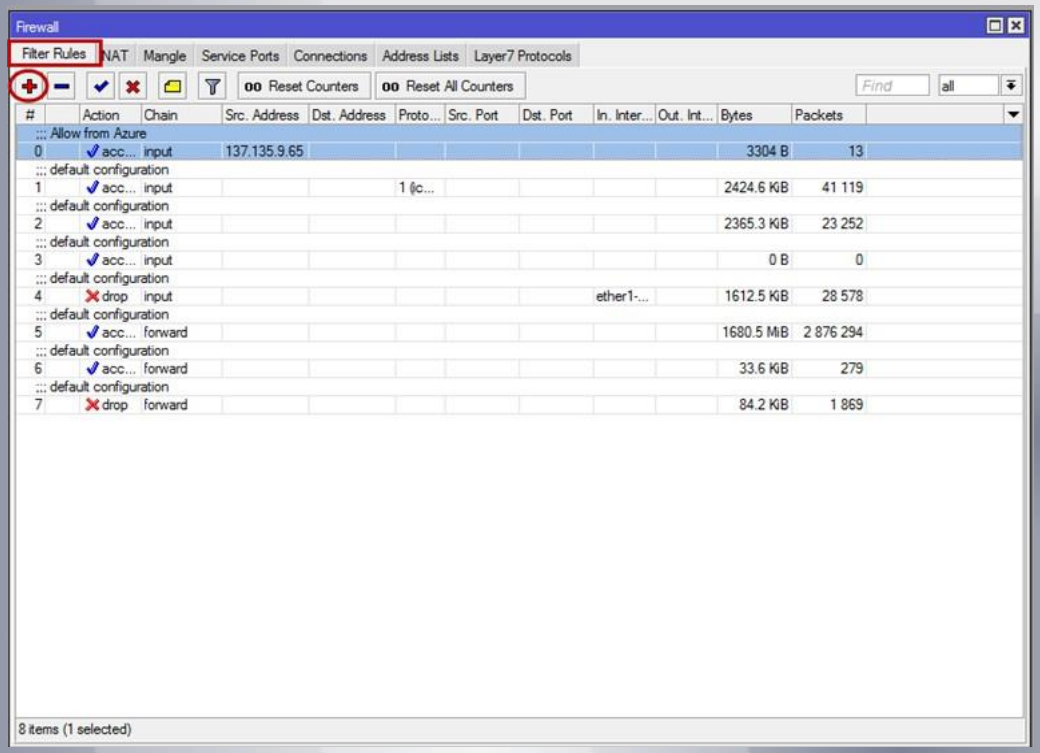


¡Regla de firewall o lista negra!



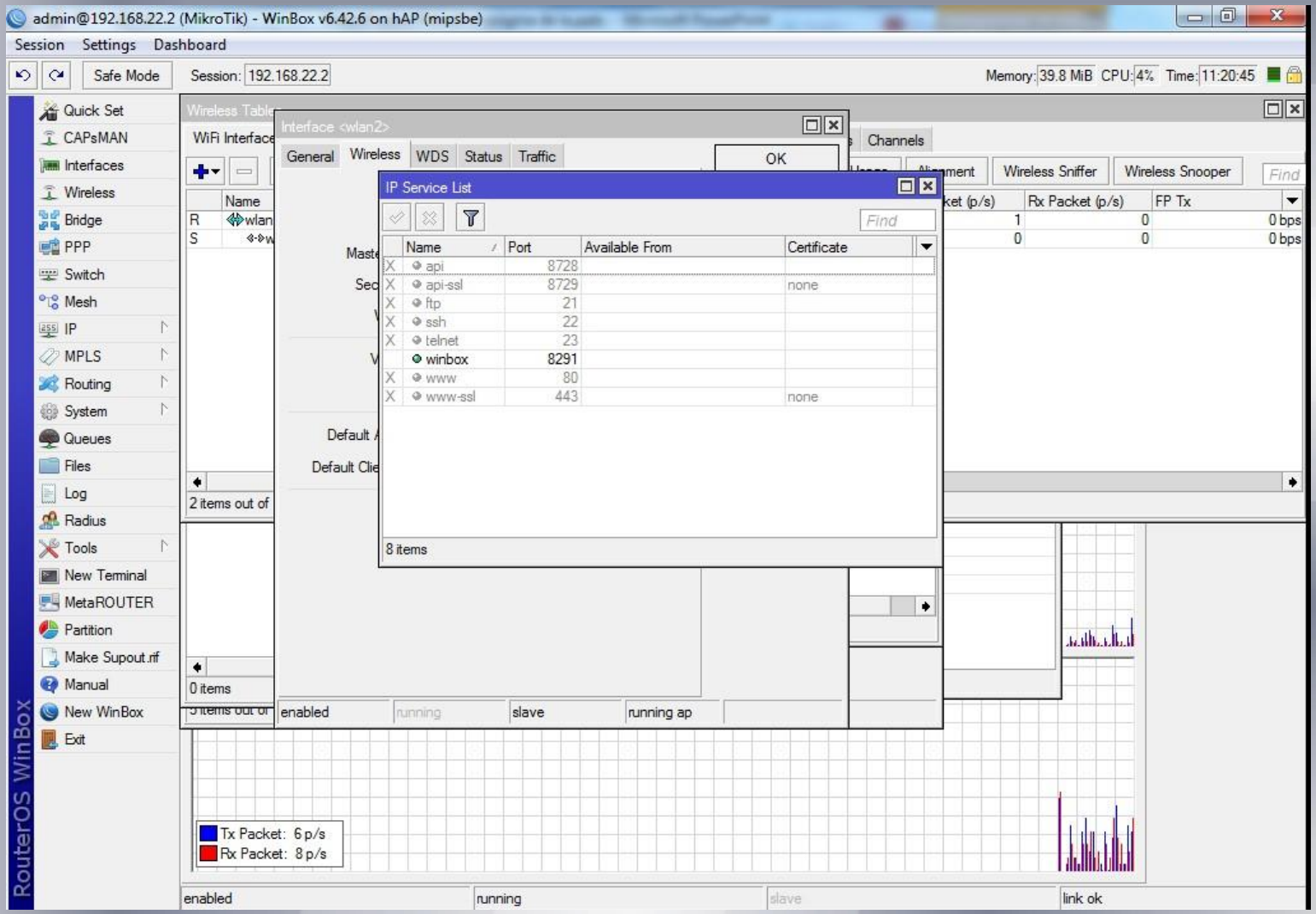
!Saturación de reglas!

- 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...	Connection State	Bytes	Packets
;;; special dummy rule to show fasttrack counters													
0	D	acc...	forward									0 B	0
;;; IN - Permitir conexiones establecidas y relacionadas													
1		acc...	input								established related	24.3 KiB	200
;;; IN - Rechazar conexiones invalidas													
2		drop	input								invalid	15.0 KiB	246
;;; IN - Detectar y descartar escaneo de puertos													
3		drop	input			6 (tcp)						0 B	0
;;; IN - Suprimir DoS													
4		tarpit	input			6 (tcp)						0 B	0
;;; IN - Detectar DoS													
5		add...	input			6 (tcp)						0 B	0
;;; IN - Salto a chain ICMP													
6		jump	input			1 (ic...						0 B	0
;;; IN - Denegar DNS por la wan													
7		drop	input			6 (tcp)		53	wlan1			0 B	0
8		drop	input			17 (u...		53	wlan1			0 B	0
;;; IN - Winbox													
9		acc...	input			6 (tcp)		8291				92 B	2
;;; IN - Permitir PPTP													
10		acc...	input			6 (tcp)		1723				0 B	0
11		acc...	input			47 (g...						0 B	0
;;; IN - IPs permitidas Administrar Router													
12		acc...	input									1591.3 KiB	19 690
;;; IN - Descartar todo lo demas													
13		drop	input									419.6 KiB	5 781
14		acc...	ICMP			1 (ic...						0 B	0
15		acc...	ICMP			1 (ic...						0 B	0
16		acc...	ICMP			1 (ic...						0 B	0
17		acc...	ICMP			1 (ic...						0 B	0
18		acc...	ICMP			1 (ic...						0 B	0

Lo básico se vuelve complejo

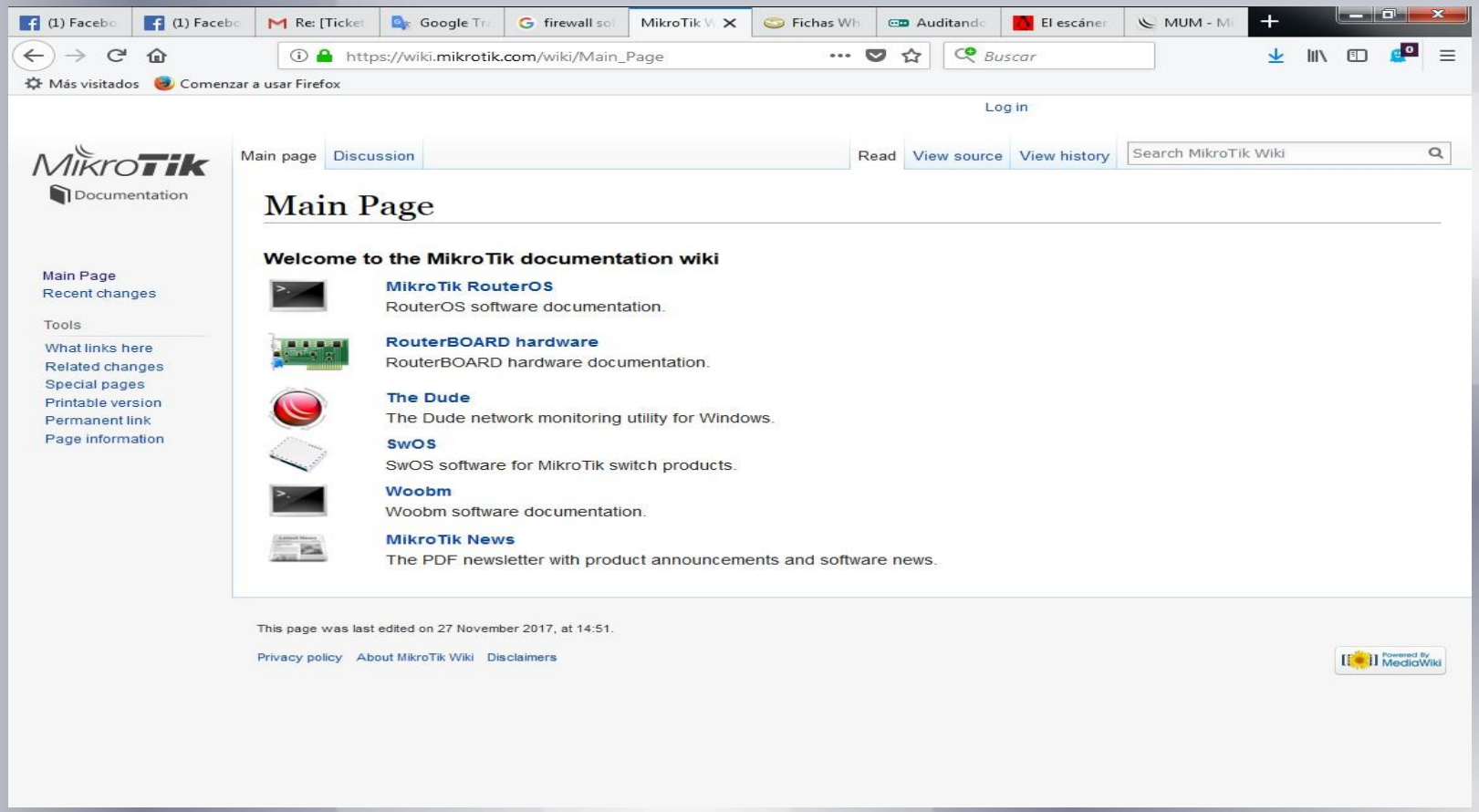



```
C:\Users\Internet>nmap 115.[redacted] -sS -sV

Starting Nmap 6.49BETA1 ( http://nmap.org ) at 2016-01-03 09:28 Hora estβndar ro
mance
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***



Recomendaciones

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

any other question?

Sorteo del premio!

Agradecimientos a mis Sponsor

ITDS

Instituto Técnico
Domingo Savio


GRACIAS POR
SU ATENCION
Y RECUERDEN
ESTUDIAR
memegenerator.es

MikroTik