Gabriel Coronado Vega

- Gerente general «SSH SUPPORT» TARIJA BOLIVIA
- Consultor informático Forense
- Certificaciones mikrotik «MTCNA, MTCWE, MTCTCE, MTCUME»
- Speaker internacional «ARGENTINA, PERU, BOLVIA»

Gabriel Coronado Vega

SSH SUPPORT

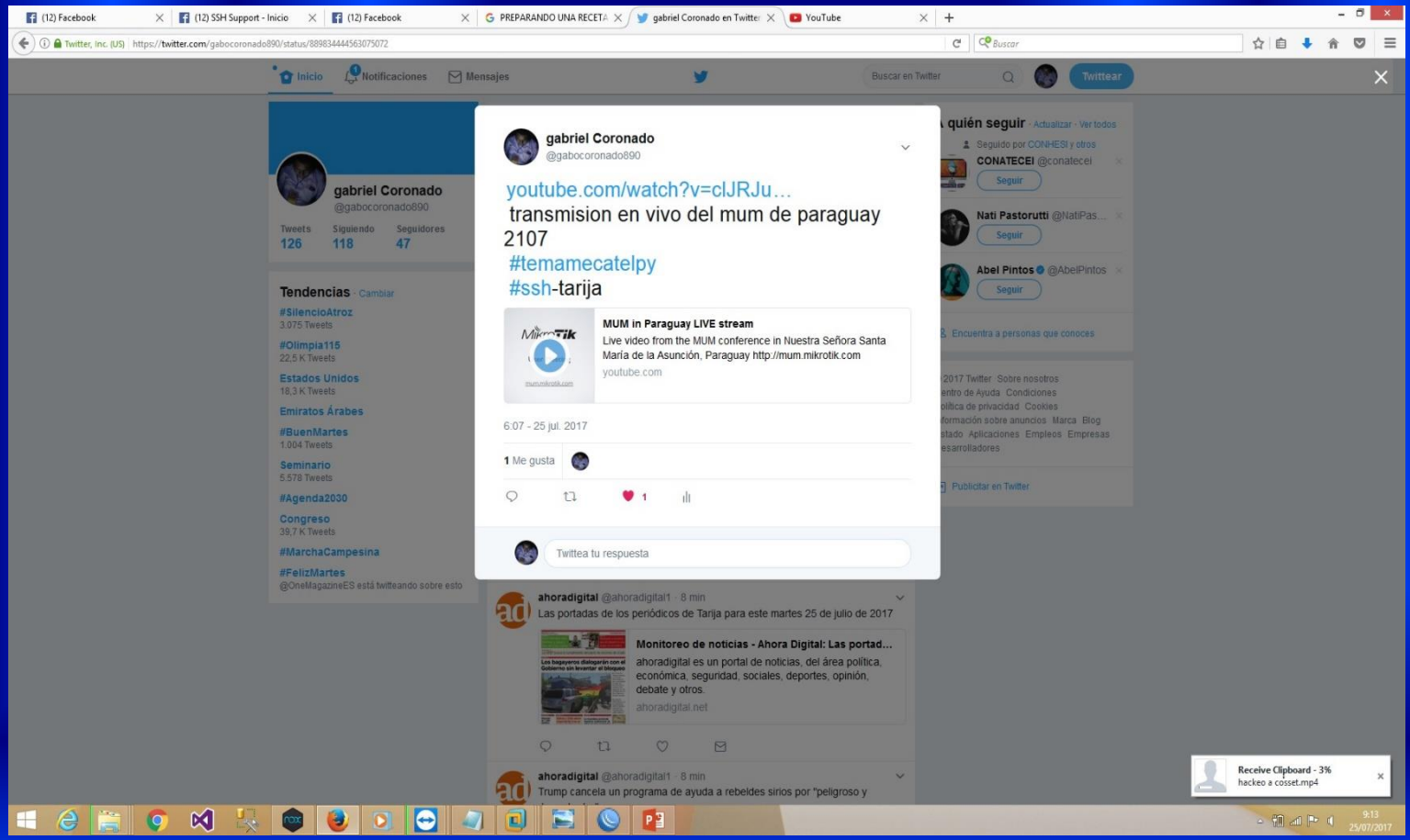

MUM
MIKROTIK USER MEETING


Gabriel Coronado Vega
GHOST890
facebook.com/ssh.support
twitter.com/gabocoronado890
ssh.tarija@gmail.com g. coronado@
youtube.com/chanel/UCyUpnuecJAdt7Fc2a
70223606

NUESTRO MORFE DIARIO!

Twitter!!!

- *Sorpresa al final!*



TEAM

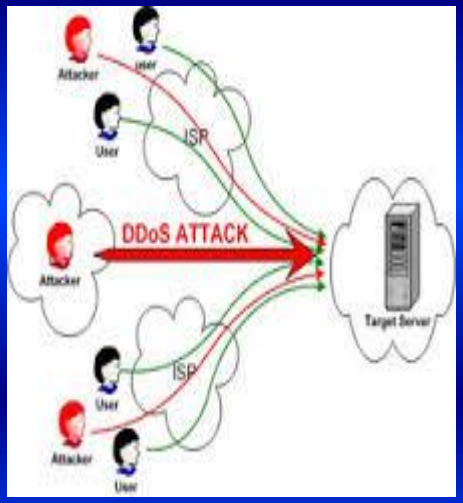
«HARDENING EN MIKROTIK»

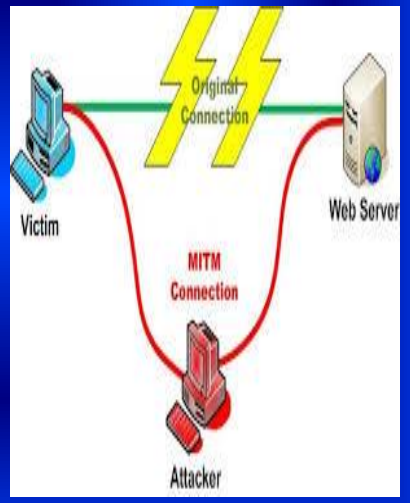
DEFINICION

- ***Reglas o políticas de seguridad que se utilizan para poder proteger un determinado ámbito informático.***
- ***La seguridad informática es elemental al momento de realizar cualquier implementación.***

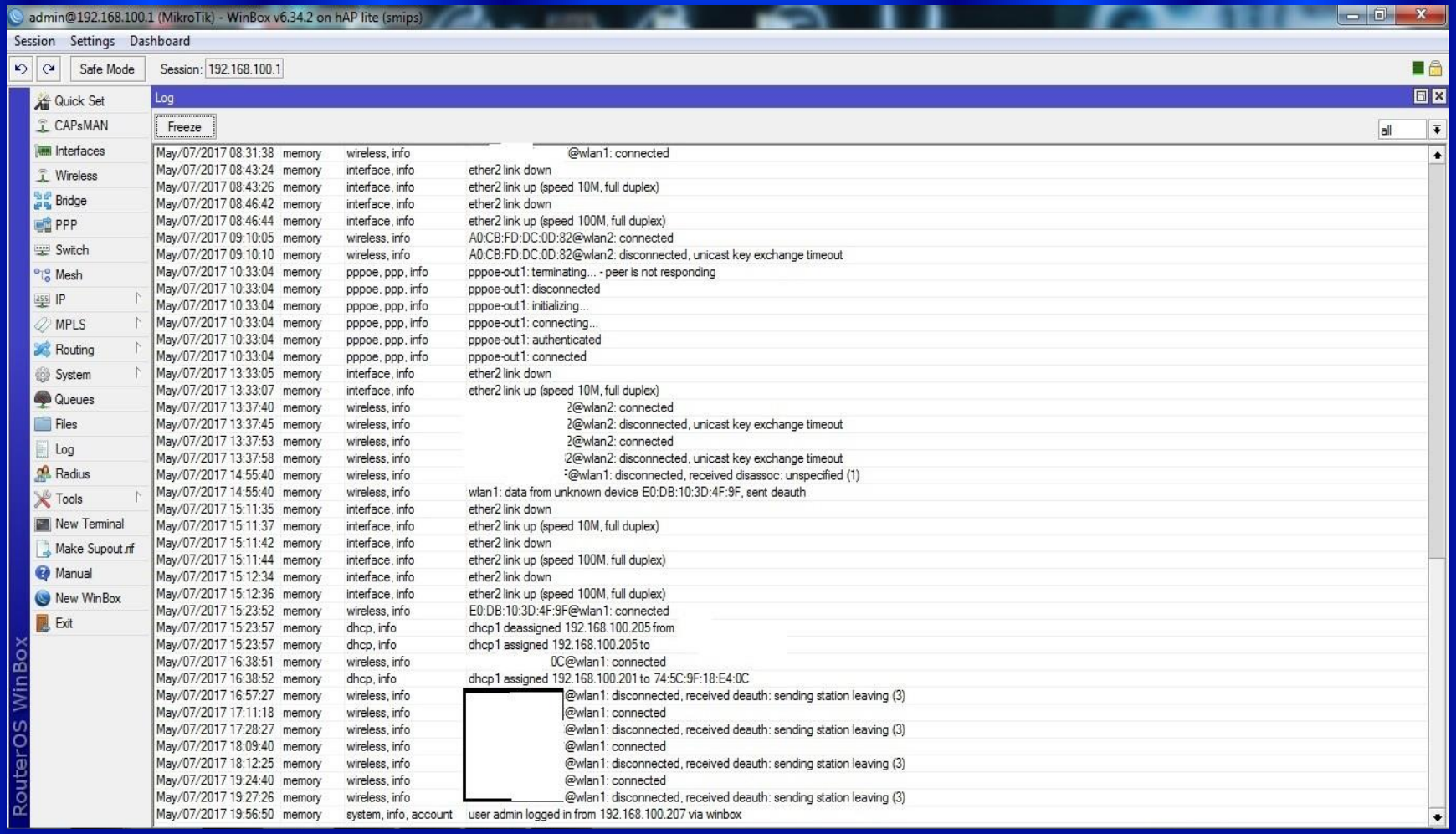
«Tipos de ataques»

- ***man-in-the-middle***
- ***Ataques de fuerza bruta***
- ***Denegación de servicios***
- ***Atacando la capa 8 del modelo osi***

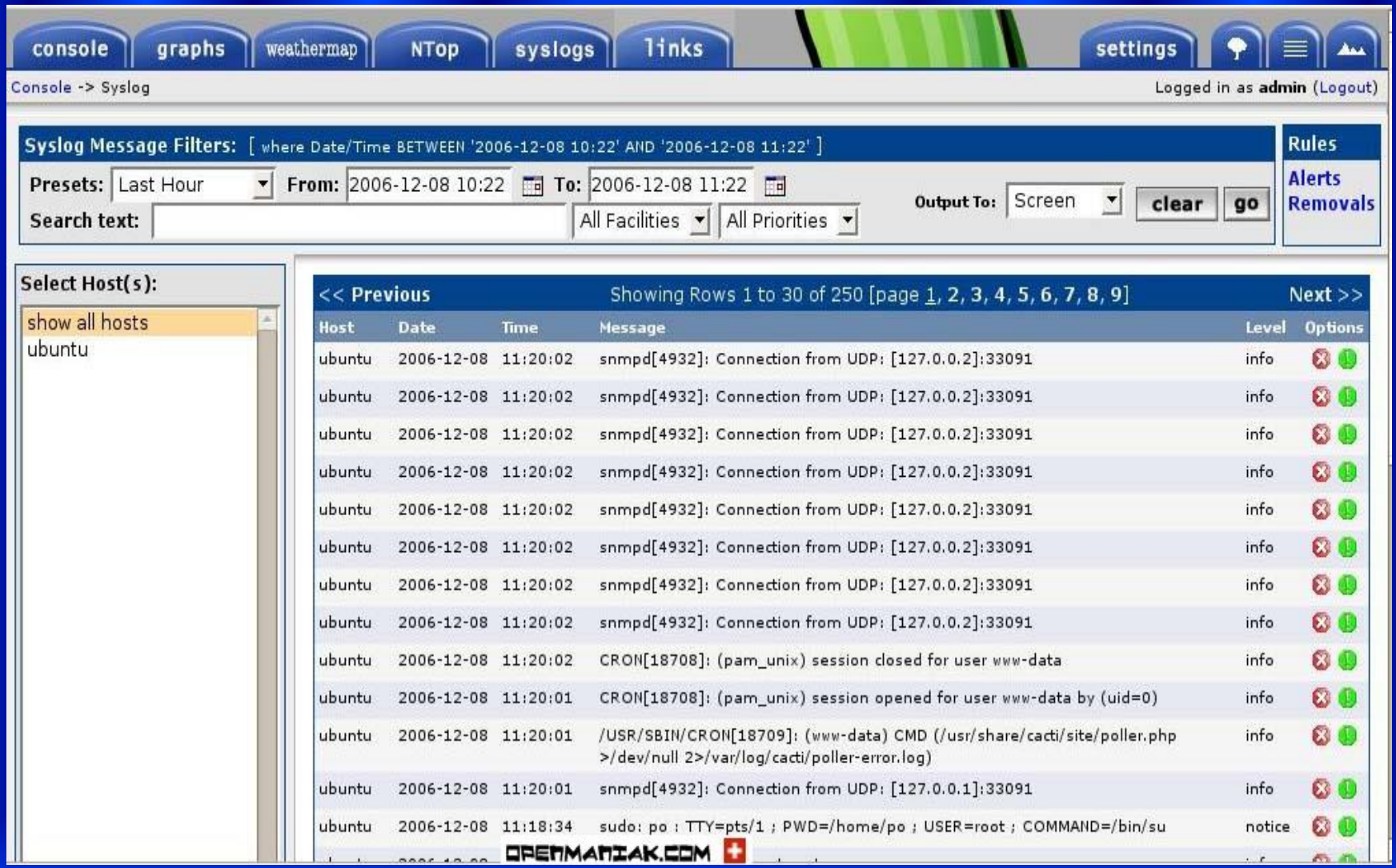




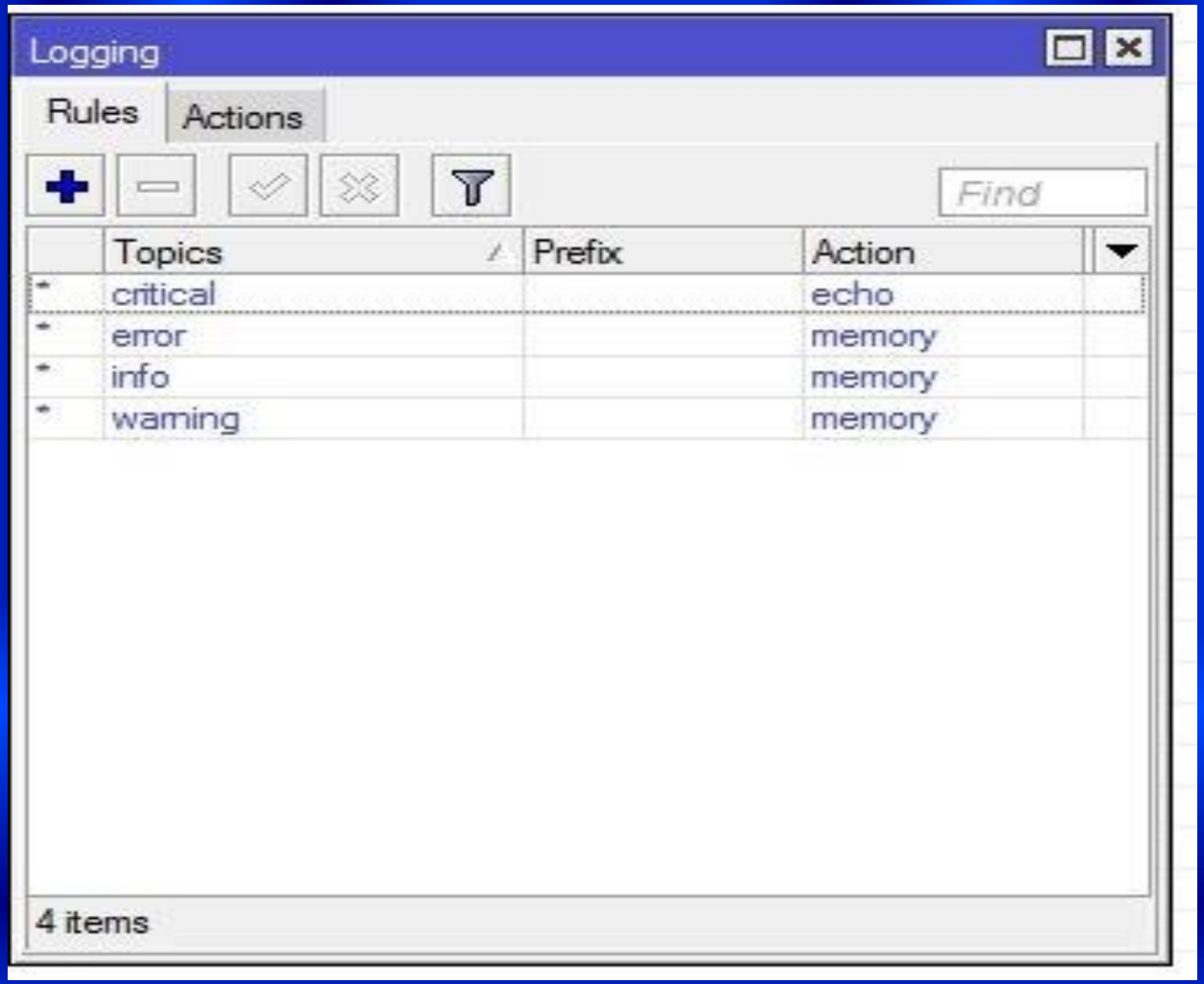
«NUESTRO MEJOR ALIADO»



"PARA ALGO DE MAYOR PERFORM"



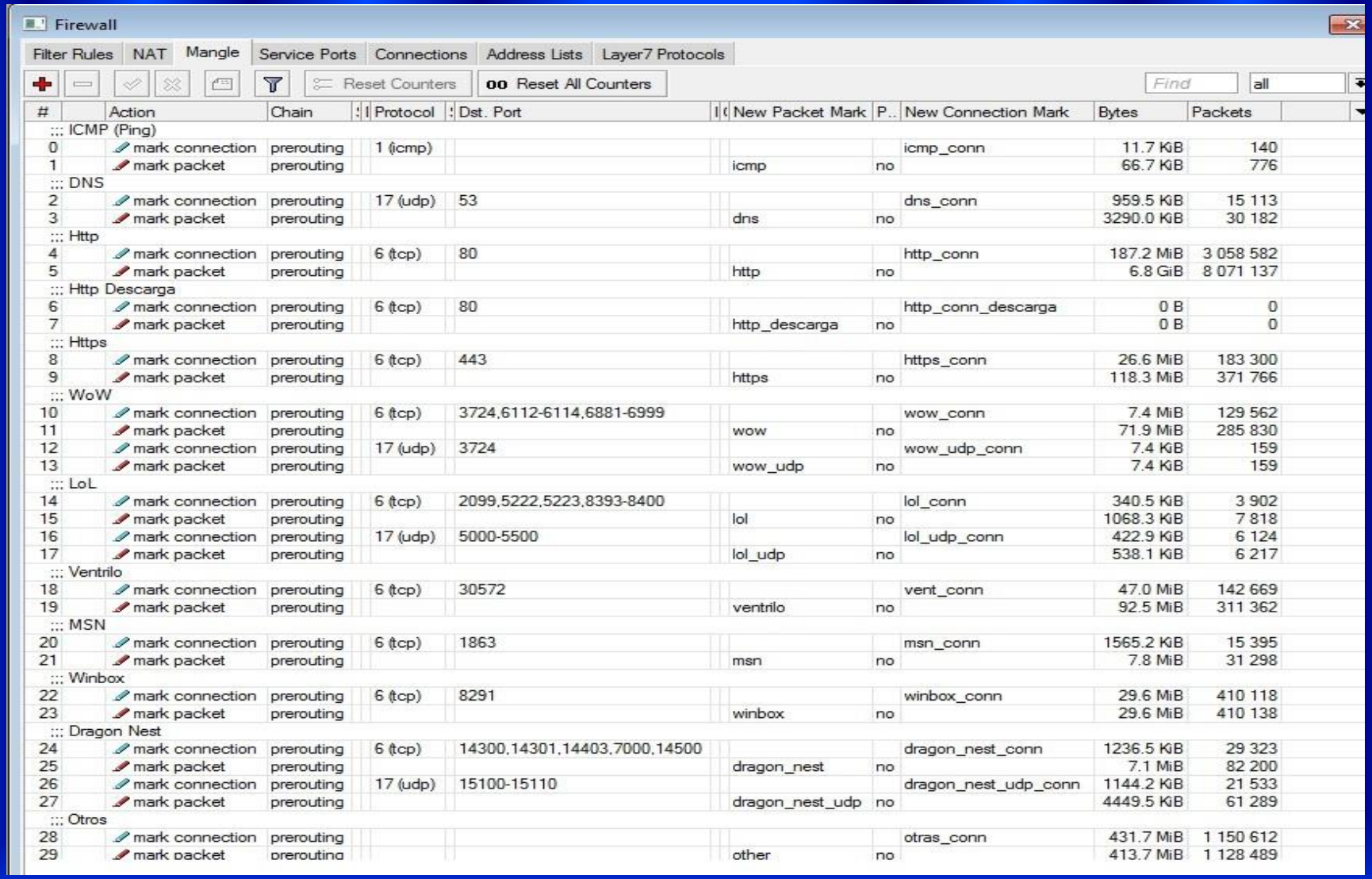
«LA YAPITA»


Logging
Rules
Actions
Find
Topics
Prefix
Action
critical
echo
error
memory
info
memory
warning
memory
4 items

«ATAQUE DDOS»

- A nivel mundial en el top 10.

"REGLAS DE FIREWALL"



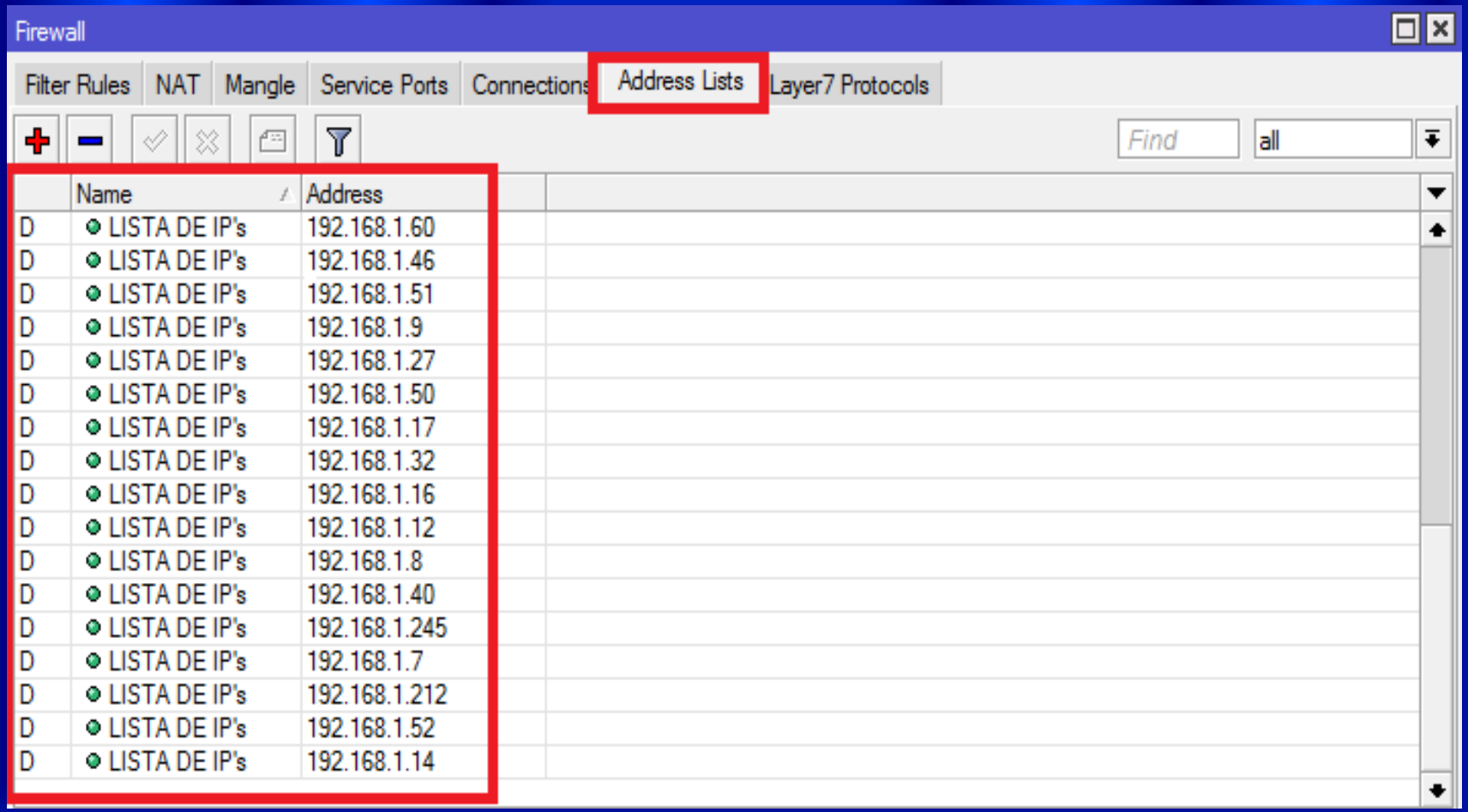
Firewall

Filter Rules | NAT | Mangle | Service Ports | Connections | Address Lists | Layer7 Protocols

Reset Counters | Reset All Counters | Find | all

#	Action	Chain	Protocol	Dst. Port	New Packet Mark	P..	New Connection Mark	Bytes	Packets
;;; ICMP (Ping)									
0	mark connection	prerouting	1 (icmp)				icmp_conn	11.7 KiB	140
1	mark packet	prerouting			icmp	no		66.7 KiB	776
;;; DNS									
2	mark connection	prerouting	17 (udp)	53			dns_conn	959.5 KiB	15 113
3	mark packet	prerouting			dns	no		3290.0 KiB	30 182
;;; Http									
4	mark connection	prerouting	6 (tcp)	80			http_conn	187.2 MiB	3 058 582
5	mark packet	prerouting			http	no		6.8 GiB	8 071 137
;;; Http Descarga									
6	mark connection	prerouting	6 (tcp)	80			http_conn_descarga	0 B	0
7	mark packet	prerouting			http_descarga	no		0 B	0
;;; Https									
8	mark connection	prerouting	6 (tcp)	443			https_conn	26.6 MiB	183 300
9	mark packet	prerouting			https	no		118.3 MiB	371 766
;;; WoW									
10	mark connection	prerouting	6 (tcp)	3724,6112-6114,6881-6999			wow_conn	7.4 MiB	129 562
11	mark packet	prerouting			wow	no		71.9 MiB	285 830
12	mark connection	prerouting	17 (udp)	3724			wow_udp_conn	7.4 KiB	159
13	mark packet	prerouting			wow_udp	no		7.4 KiB	159
;;; LoL									
14	mark connection	prerouting	6 (tcp)	2099,5222,5223,8393-8400			lol_conn	340.5 KiB	3 902
15	mark packet	prerouting			lol	no		1068.3 KiB	7 818
16	mark connection	prerouting	17 (udp)	5000-5500			lol_udp_conn	422.9 KiB	6 124
17	mark packet	prerouting			lol_udp	no		538.1 KiB	6 217
;;; Ventrilo									
18	mark connection	prerouting	6 (tcp)	30572			vent_conn	47.0 MiB	142 669
19	mark packet	prerouting			ventrilo	no		92.5 MiB	311 362
;;; MSN									
20	mark connection	prerouting	6 (tcp)	1863			msn_conn	1565.2 KiB	15 395
21	mark packet	prerouting			msn	no		7.8 MiB	31 298
;;; Winbox									
22	mark connection	prerouting	6 (tcp)	8291			winbox_conn	29.6 MiB	410 118
23	mark packet	prerouting			winbox	no		29.6 MiB	410 138
;;; Dragon Nest									
24	mark connection	prerouting	6 (tcp)	14300,14301,14403,7000,14500			dragon_nest_conn	1236.5 KiB	29 323
25	mark packet	prerouting			dragon_nest	no		7.1 MiB	82 200
26	mark connection	prerouting	17 (udp)	15100-15110			dragon_nest_udp_conn	1144.2 KiB	21 533
27	mark packet	prerouting			dragon_nest_udp	no		4449.5 KiB	61 289
;;; Otros									
28	mark connection	prerouting					otras_conn	431.7 MiB	1 150 612
29	mark packet	prerouting			other	no		413.7 MiB	1 128 489

"LISTAS DE DIRECCIONES"



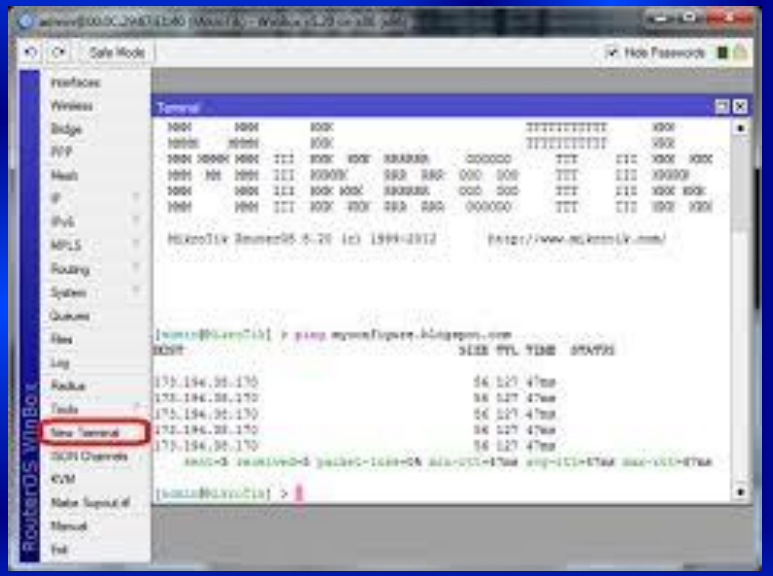
"FIREWALL vs ADDRESS LIST"

“PROFESIONALES DE RECETA”

«KALI?»

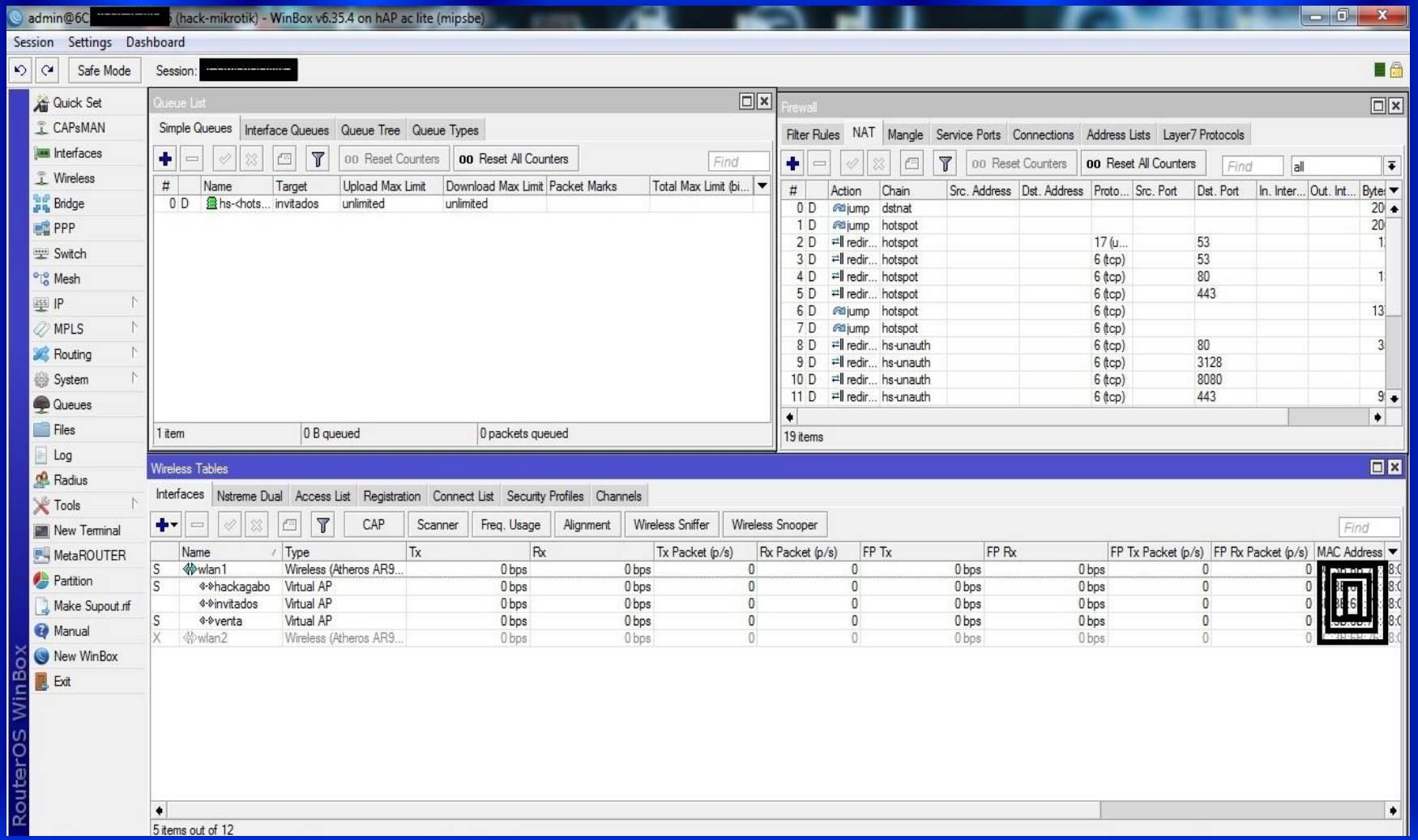
«CONTRAMEDIDAS»

- ***Pensar como el atacante***
- ***Mantener las normas de seguridad mínimas en nuestros equipos mikrotik***



«¿Como vamos con el *twitter*?»

«AL ATAQUE»

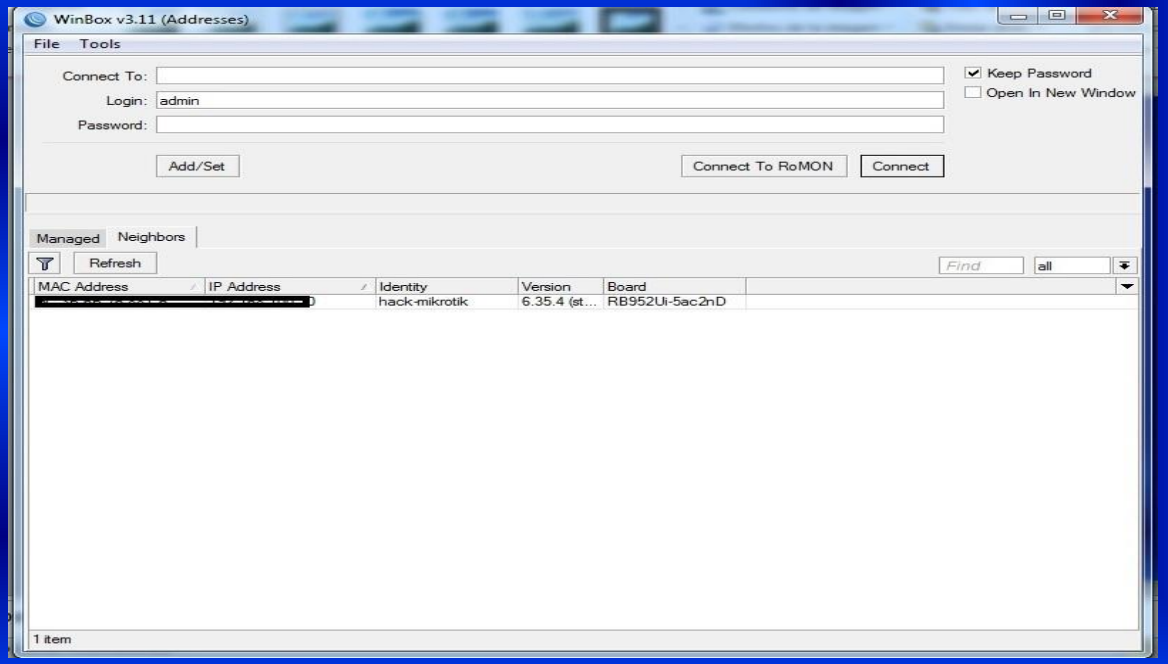

admin@6C [redacted] (hack-mikrotik) - WinBox v6.35.4 on hAP ac lite (mipsbe)
Session Settings Dashboard
Safe Mode
Session: [redacted]
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Partition
Make Supout.rif
Manual
New WinBox
Exit
RouterOS WinBox
Queue List
Simple Queues
Interface Queues
Queue Tree
Queue Types
Reset Counters
Reset All Counters
Find
Name Target Upload Max Limit Download Max Limit Packet Marks Total Max Limit (bi...
0 D hs-chots... invitados unlimited unlimited
1 item
0 B queued
0 packets queued
Firewall
Filter Rules
NAT
Mangle
Service Ports
Connections
Address Lists
Layer7 Protocols
Reset Counters
Reset All Counters
Find
all
Action Chain Src. Address Dst. Address Proto... Src. Port Dst. Port In. Inter... Out. Int... Byte
0 D jump dstnat 20
1 D jump hotspot 20
2 D redir... hotspot 17 (u... 53 1
3 D redir... hotspot 6 (tcp) 53
4 D redir... hotspot 6 (tcp) 80 1
5 D redir... hotspot 6 (tcp) 443
6 D jump hotspot 6 (tcp) 13
7 D jump hotspot 6 (tcp)
8 D redir... hs-unauth 6 (tcp) 80 3
9 D redir... hs-unauth 6 (tcp) 3128
10 D redir... hs-unauth 6 (tcp) 8080
11 D redir... hs-unauth 6 (tcp) 443 9
19 items
Wireless Tables
Interfaces
Nstreme Dual
Access List
Registration
Connect List
Security Profiles
Channels
CAP
Scanner
Freq. Usage
Alignment
Wireless Sniffer
Wireless Snooper
Find
Name Type Tx Rx Tx Packet (p/s) Rx Packet (p/s) FP Tx FP Rx FP Tx Packet (p/s) FP Rx Packet (p/s) MAC Address
S wlan1 Wireless (Atheros AR9... 0 bps 0 bps 0 0 0 bps 0 bps 0 0
S hackagabo Virtual AP 0 bps 0 bps 0 0 0 bps 0 bps 0 0
invitados Virtual AP 0 bps 0 bps 0 0 0 bps 0 bps 0 0
S venta Virtual AP 0 bps 0 bps 0 0 0 bps 0 bps 0 0
X wlan2 Wireless (Atheros AR9... 0 bps 0 bps 0 0 0 bps 0 bps 0 0
5 items out of 12

«ATAQUE DE FUERZA BRUTA»

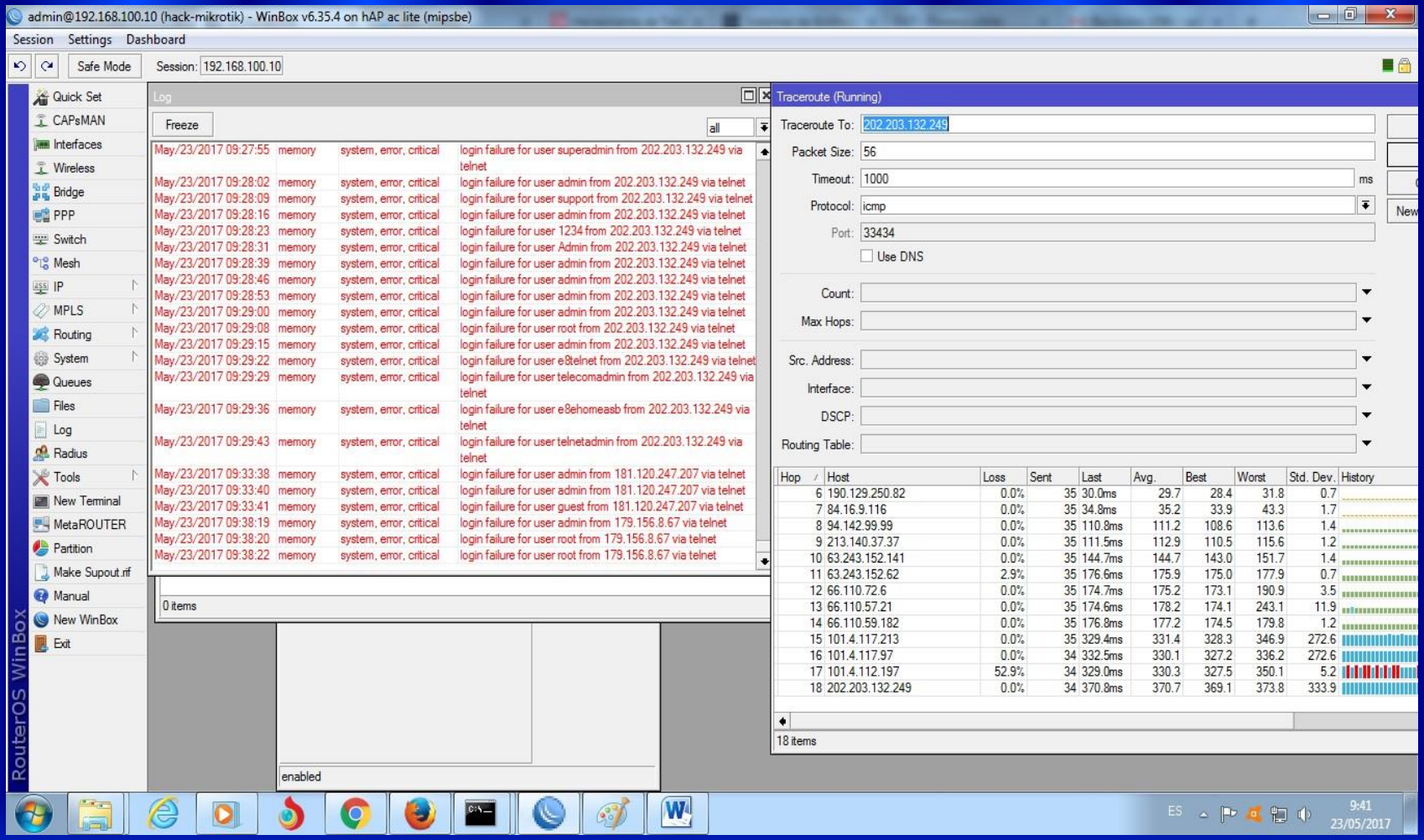
- *Descripción*
- *Tendencia*
- *Vulnerabilidad*

«VENTAJAS DE WINBOX»

- *WinBox tiene protocolo propietario*
- *Mas complejo de ser atacado*
- *Ssh, telnet, web, propensos a intrusiones.*



CUANDO TE QUIEREN DAR PALO!

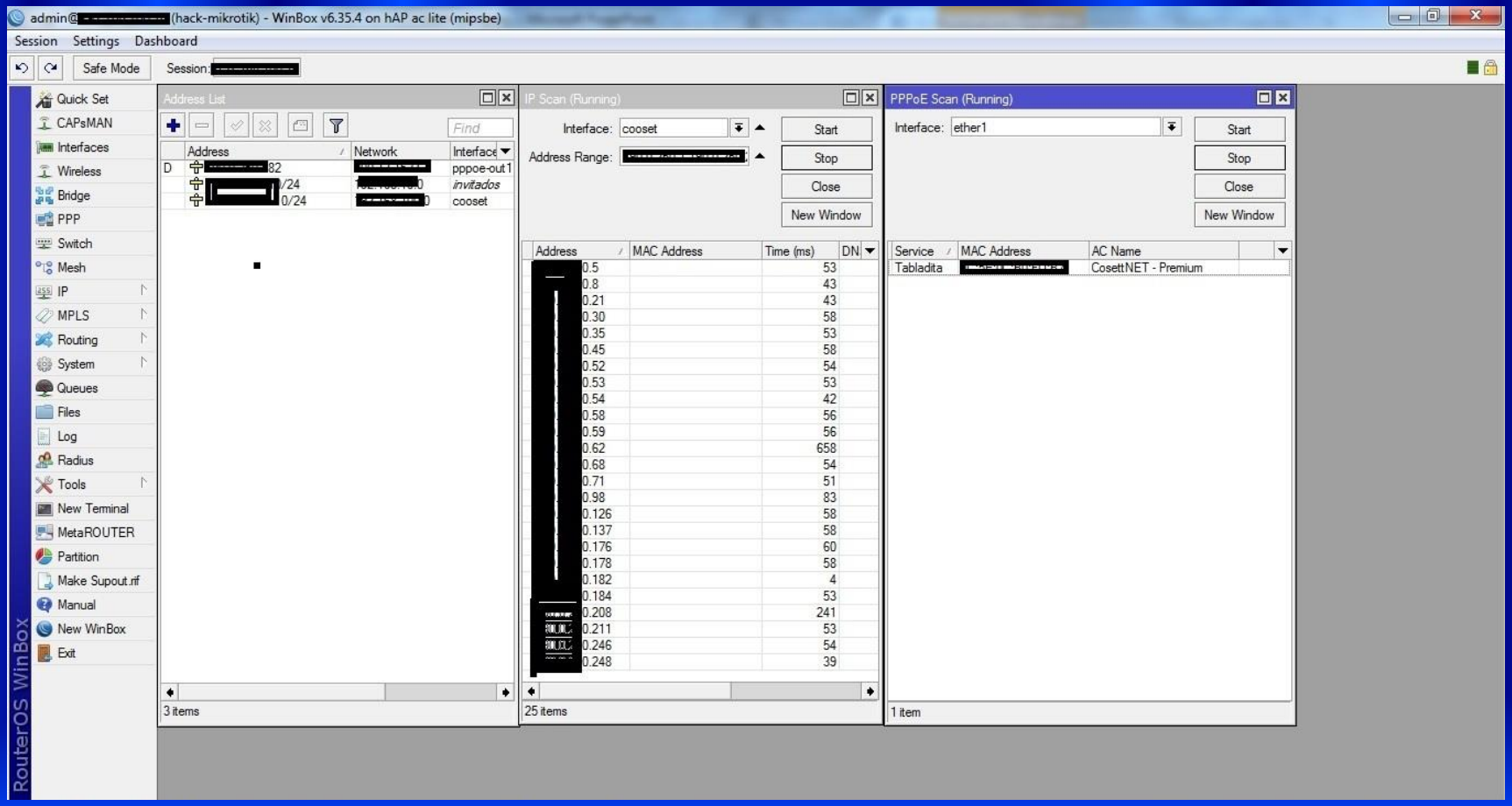


«ATACANDO LA CAPA 8»

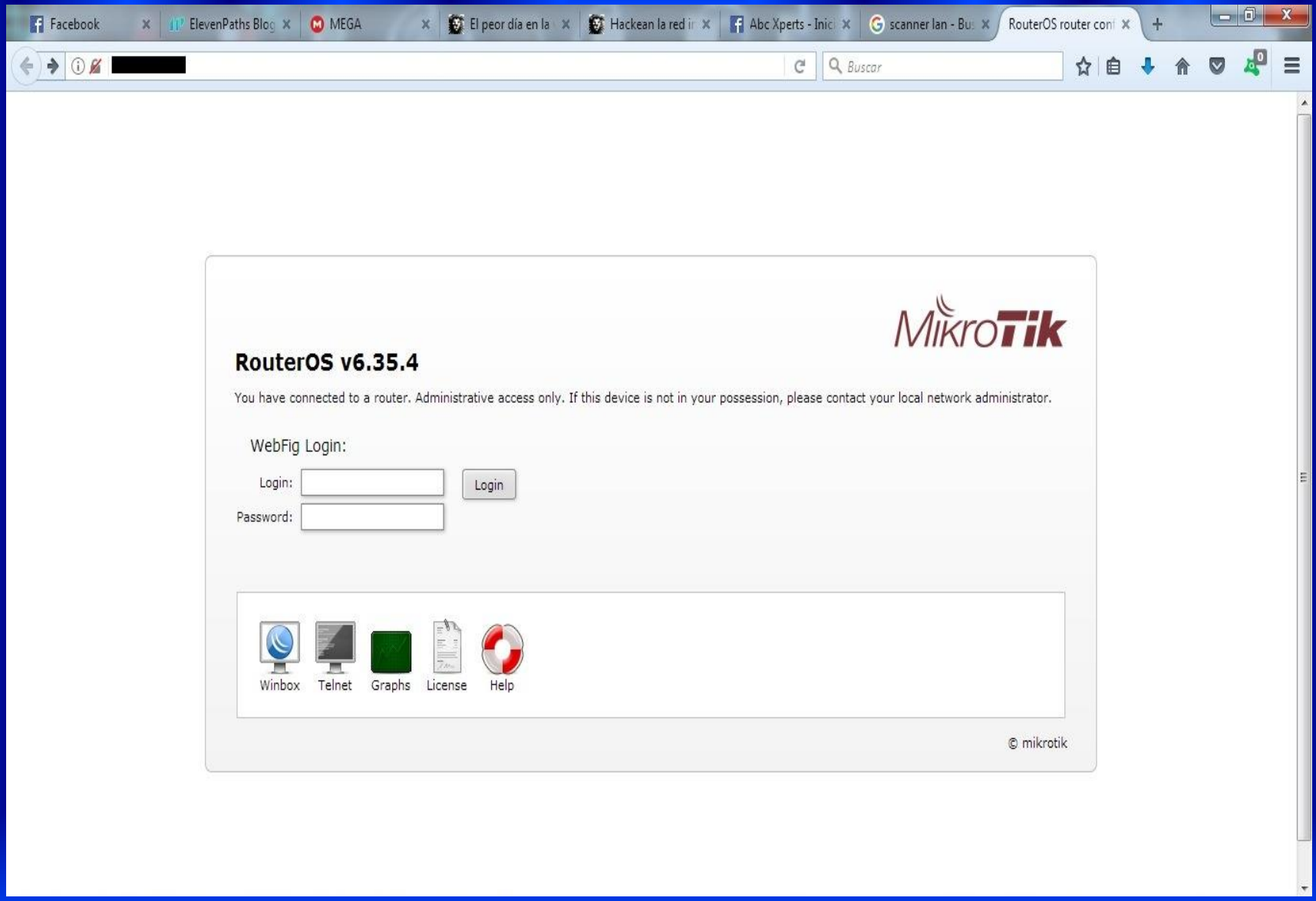
- *La capa mas débil*
- *La mas vulnerable*
- *Ingeniería social*

«HACKEANDO CON MIKROTIK»

- *Desde lo mas básico*



«FUSION A.F.B CON SQL INYECTION»



WINDOWS 10!

DONACION DE SESION!

ATAQUE EN TIEMPO REAL

YA PARA CONCLUIR!

Acerca de nosotros

Somos una empresa dedicada a brindar soporte en soluciones con MikroTik

También somos un centro autorizado de certificacion. Con nuestros cursos podrás capacitarte y obtener las certificaciones de MikroTik.

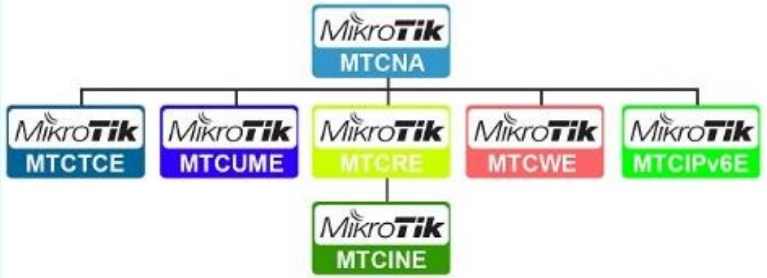
Proximos Cursos

MTCNA	MTCTCE
26 Ago 2017	29 Ago 2017

Reserva ahora con

448.000 Gs.

Certificaciones



Contáctenos

EcaTel SRL

info@ecatel.com.py

0973 691525

EcatelSRL

BIENVENIDOS


Gracias