



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





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!

Bolivia

Saice Tarijeño



SABORES
COLORES
de Bolivia

Twitter!!!

- *Sorpresa al final!*

The screenshot shows a web browser window displaying the Twitter profile of gabriel Coronado (@gabocoronado890). The profile page includes the user's name, bio, and statistics (126 tweets, 118 following, 47 followers). A tweet is highlighted, featuring a video player for a 'MUM in Paraguay LIVE stream'. The tweet text reads: 'youtube.com/watch?v=clJRJu... transmision en vivo del mum de paraguay 2107 #temamecatelpy #ssh-tarja'. Below the tweet, there is a reply section with one response from 'ahoradigital' (@ahoradigital1) dated 8 minutes ago. The browser's address bar shows the URL 'https://twitter.com/gabocoronado890/status/889834444563075072'. The Windows taskbar is visible at the bottom, showing various application icons and the system clock at 9:13 on 25/07/2017.

TEAM





«HARDENING EN MIKROTIK»



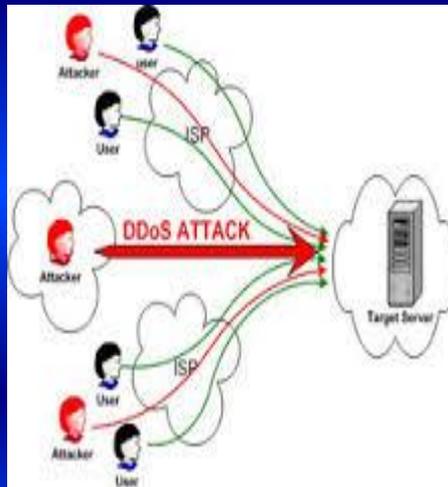
DEFINICION

- *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»

admin@192.168.100.1 (MikroTik) - WinBox v6.34.2 on hAP lite (smips)

Session Settings Dashboard

Safe Mode Session: 192.168.100.1

RouterOS WinBox

Quick Set CAPsMAN Interfaces Wireless Bridge PPP Switch Mesh IP MPLS Routing System Queues Files Log Radius Tools New Terminal Make Spoutout Manual New WinBox Exit

Log

Freeze all

May/07/2017 08:31:38	memory	wireless, info	@wlan1: connected
May/07/2017 08:43:24	memory	interface, info	ether2 link down
May/07/2017 08:43:26	memory	interface, info	ether2 link up (speed 10M, full duplex)
May/07/2017 08:46:42	memory	interface, info	ether2 link down
May/07/2017 08:46:44	memory	interface, info	ether2 link up (speed 100M, full duplex)
May/07/2017 09:10:05	memory	wireless, info	A0:CB:FD:DC:0D:82@wlan2: connected
May/07/2017 09:10:10	memory	wireless, info	A0:CB:FD:DC:0D:82@wlan2: disconnected, unicast key exchange timeout
May/07/2017 10:33:04	memory	pppoe, ppp, info	pppoe-out1: terminating... - peer is not responding
May/07/2017 10:33:04	memory	pppoe, ppp, info	pppoe-out1: disconnected
May/07/2017 10:33:04	memory	pppoe, ppp, info	pppoe-out1: initializing...
May/07/2017 10:33:04	memory	pppoe, ppp, info	pppoe-out1: connecting...
May/07/2017 10:33:04	memory	pppoe, ppp, info	pppoe-out1: authenticated
May/07/2017 10:33:04	memory	pppoe, ppp, info	pppoe-out1: connected
May/07/2017 13:33:05	memory	interface, info	ether2 link down
May/07/2017 13:33:07	memory	interface, info	ether2 link up (speed 10M, full duplex)
May/07/2017 13:37:40	memory	wireless, info	2@wlan2: connected
May/07/2017 13:37:45	memory	wireless, info	2@wlan2: disconnected, unicast key exchange timeout
May/07/2017 13:37:53	memory	wireless, info	2@wlan2: connected
May/07/2017 13:37:58	memory	wireless, info	2@wlan2: disconnected, received disassoc: unspecified (1)
May/07/2017 14:55:40	memory	wireless, info	:@wlan1: disconnected, received disassoc: unspecified (1)
May/07/2017 14:55:40	memory	wireless, info	wlan1: data from unknown device E0:DB:10:3D:4F:9F, sent deauth
May/07/2017 15:11:35	memory	interface, info	ether2 link down
May/07/2017 15:11:37	memory	interface, info	ether2 link up (speed 10M, full duplex)
May/07/2017 15:11:42	memory	interface, info	ether2 link down
May/07/2017 15:11:44	memory	interface, info	ether2 link up (speed 100M, full duplex)
May/07/2017 15:12:34	memory	interface, info	ether2 link down
May/07/2017 15:12:36	memory	interface, info	ether2 link up (speed 100M, full duplex)
May/07/2017 15:23:52	memory	wireless, info	E0:DB:10:3D:4F:9F@wlan1: connected
May/07/2017 15:23:57	memory	dhcp, info	dhcp1 deassigned 192.168.100.205 from
May/07/2017 15:23:57	memory	dhcp, info	dhcp1 assigned 192.168.100.205 to
May/07/2017 16:38:51	memory	wireless, info	0C@wlan1: connected
May/07/2017 16:38:52	memory	dhcp, info	dhcp1 assigned 192.168.100.201 to 74:5C:9F:18:E4:0C
May/07/2017 16:57:27	memory	wireless, info	@wlan1: disconnected, received deauth: sending station leaving (3)
May/07/2017 17:11:18	memory	wireless, info	@wlan1: connected
May/07/2017 17:28:27	memory	wireless, info	@wlan1: disconnected, received deauth: sending station leaving (3)
May/07/2017 18:09:40	memory	wireless, info	@wlan1: connected
May/07/2017 18:12:25	memory	wireless, info	@wlan1: disconnected, received deauth: sending station leaving (3)
May/07/2017 19:24:40	memory	wireless, info	@wlan1: connected
May/07/2017 19:27:26	memory	wireless, info	@wlan1: disconnected, received deauth: sending station leaving (3)
May/07/2017 19:56:50	memory	system, info, account	user admin logged in from 192.168.100.207 via winbox

"PARA ALGO DE MAYOR PERFORM"

The screenshot displays the Nagios Core Syslog interface. At the top, there are navigation buttons for 'console', 'graphs', 'weathermap', 'NTop', 'syslogs', 'links', 'settings', and a menu icon. The current view is 'Console -> Syslog', and the user is logged in as 'admin'. The Syslog Message Filters section shows a filter for messages between '2006-12-08 10:22' and '2006-12-08 11:22'. The 'Presets' dropdown is set to 'Last Hour'. The 'From' and 'To' fields are filled with the respective timestamps. The 'Search text' field is empty. The 'Output To' dropdown is set to 'Screen'. There are 'clear' and 'go' buttons. On the right, there are 'Alerts' and 'Removals' buttons. Below the filters, there is a 'Select Host(s):' section with a list containing 'show all hosts' and 'ubuntu'. The main area shows a table of log messages with columns for Host, Date, Time, Message, Level, and Options. The table shows 30 rows of messages, including SNMP connections and CRON jobs. The footer of the interface includes the text 'OPENMANIAK.COM' and a small red cross icon.

console graphs weathermap NTop syslogs links settings

Console -> Syslog Logged in as admin (Logout)

Syslog Message Filters: [where Date/Time BETWEEN '2006-12-08 10:22' AND '2006-12-08 11:22']

Presets: Last Hour From: 2006-12-08 10:22 To: 2006-12-08 11:22

Search text: All Facilities All Priorities Output To: Screen clear go Alerts Removals

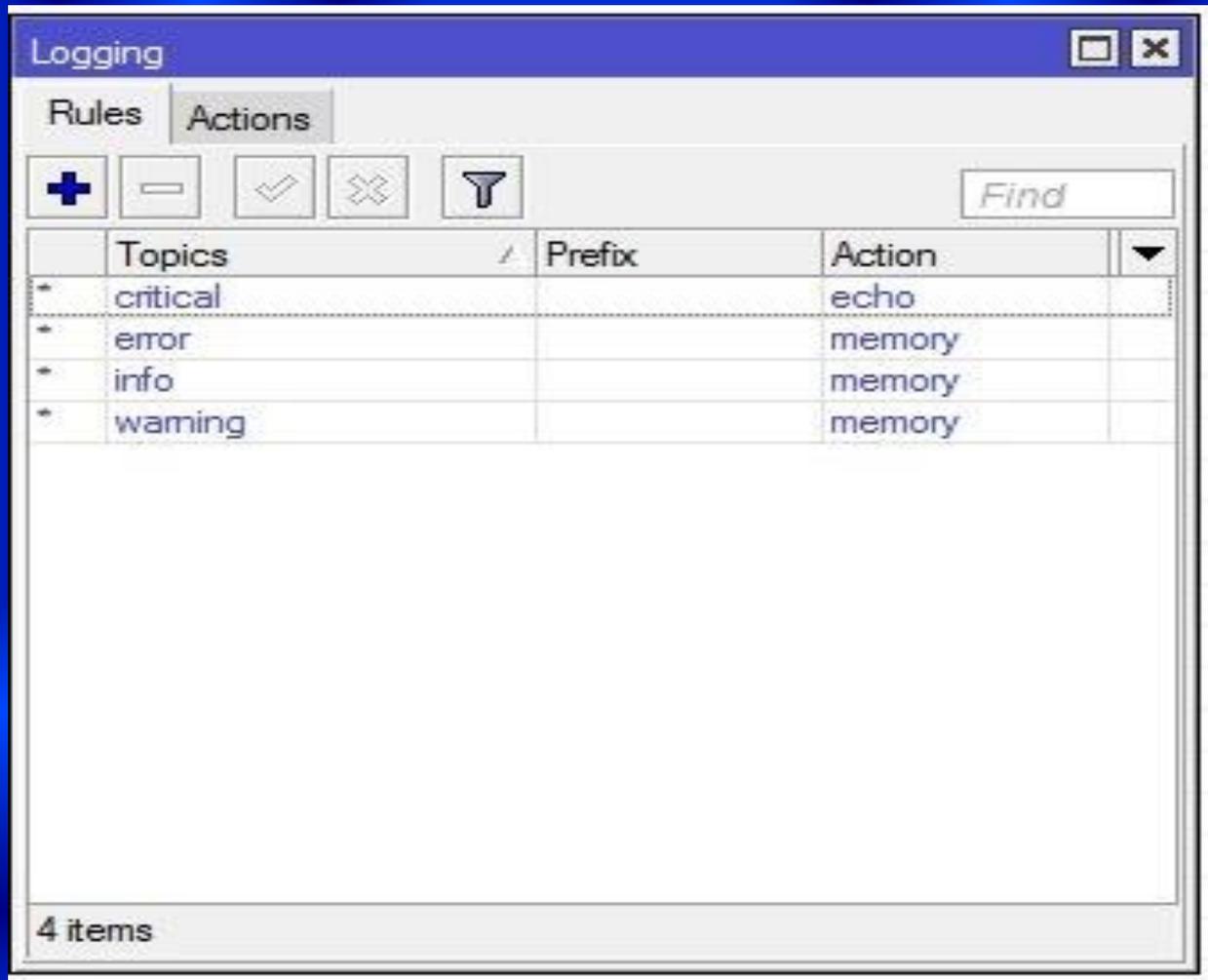
Select Host(s): show all hosts ubuntu

<< Previous Showing Rows 1 to 30 of 250 [page 1, 2, 3, 4, 5, 6, 7, 8, 9] Next >>

Host	Date	Time	Message	Level	Options
ubuntu	2006-12-08	11:20:02	snmpd[4932]: Connection from UDP: [127.0.0.2]:33091	info	
ubuntu	2006-12-08	11:20:02	snmpd[4932]: Connection from UDP: [127.0.0.2]:33091	info	
ubuntu	2006-12-08	11:20:02	snmpd[4932]: Connection from UDP: [127.0.0.2]:33091	info	
ubuntu	2006-12-08	11:20:02	snmpd[4932]: Connection from UDP: [127.0.0.2]:33091	info	
ubuntu	2006-12-08	11:20:02	snmpd[4932]: Connection from UDP: [127.0.0.2]:33091	info	
ubuntu	2006-12-08	11:20:02	snmpd[4932]: Connection from UDP: [127.0.0.2]:33091	info	
ubuntu	2006-12-08	11:20:02	snmpd[4932]: Connection from UDP: [127.0.0.2]:33091	info	
ubuntu	2006-12-08	11:20:02	snmpd[4932]: Connection from UDP: [127.0.0.2]:33091	info	
ubuntu	2006-12-08	11:20:02	CRON[18708]: (pam_unix) session closed for user www-data	info	
ubuntu	2006-12-08	11:20:01	CRON[18708]: (pam_unix) session opened for user www-data by (uid=0)	info	
ubuntu	2006-12-08	11:20:01	/USR/SBIN/CRON[18709]: (www-data) CMD (/usr/share/cacti/site/poller.php >/dev/null 2>/var/log/cacti/poller-error.log)	info	
ubuntu	2006-12-08	11:20:01	snmpd[4932]: Connection from UDP: [127.0.0.1]:33091	info	
ubuntu	2006-12-08	11:18:34	sudo: po : TTY=pts/1 ; PWD=/home/po ; USER=root ; COMMAND=/bin/su	notice	

OPENMANIAK.COM

«LA YAPITA»



The screenshot shows a window titled "Logging" with a tabbed interface. The "Actions" tab is selected. The window contains a toolbar with icons for adding (+), removing (-), checking (✓), unchecking (✗), and filtering (funnel), along with a "Find" search box. Below the toolbar is a table with four columns: "Topics", "Prefix", "Action", and a dropdown arrow. The table lists four items, each with a "*" in the first column. The "Topics" column contains "critical", "error", "info", and "warning". The "Action" column contains "echo" for "critical" and "memory" for the other three. The status bar at the bottom left indicates "4 items".

	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”

#	Action	Chain	Protocol	Dst. Port	New Packet Mark	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

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

+ - ✓ ✗ ☰ 🔍 Find all

	Name	Address
D	LISTA DE IP's	192.168.1.60
D	LISTA DE IP's	192.168.1.46
D	LISTA DE IP's	192.168.1.51
D	LISTA DE IP's	192.168.1.9
D	LISTA DE IP's	192.168.1.27
D	LISTA DE IP's	192.168.1.50
D	LISTA DE IP's	192.168.1.17
D	LISTA DE IP's	192.168.1.32
D	LISTA DE IP's	192.168.1.16
D	LISTA DE IP's	192.168.1.12
D	LISTA DE IP's	192.168.1.8
D	LISTA DE IP's	192.168.1.40
D	LISTA DE IP's	192.168.1.245
D	LISTA DE IP's	192.168.1.7
D	LISTA DE IP's	192.168.1.212
D	LISTA DE IP's	192.168.1.52
D	LISTA DE IP's	192.168.1.14

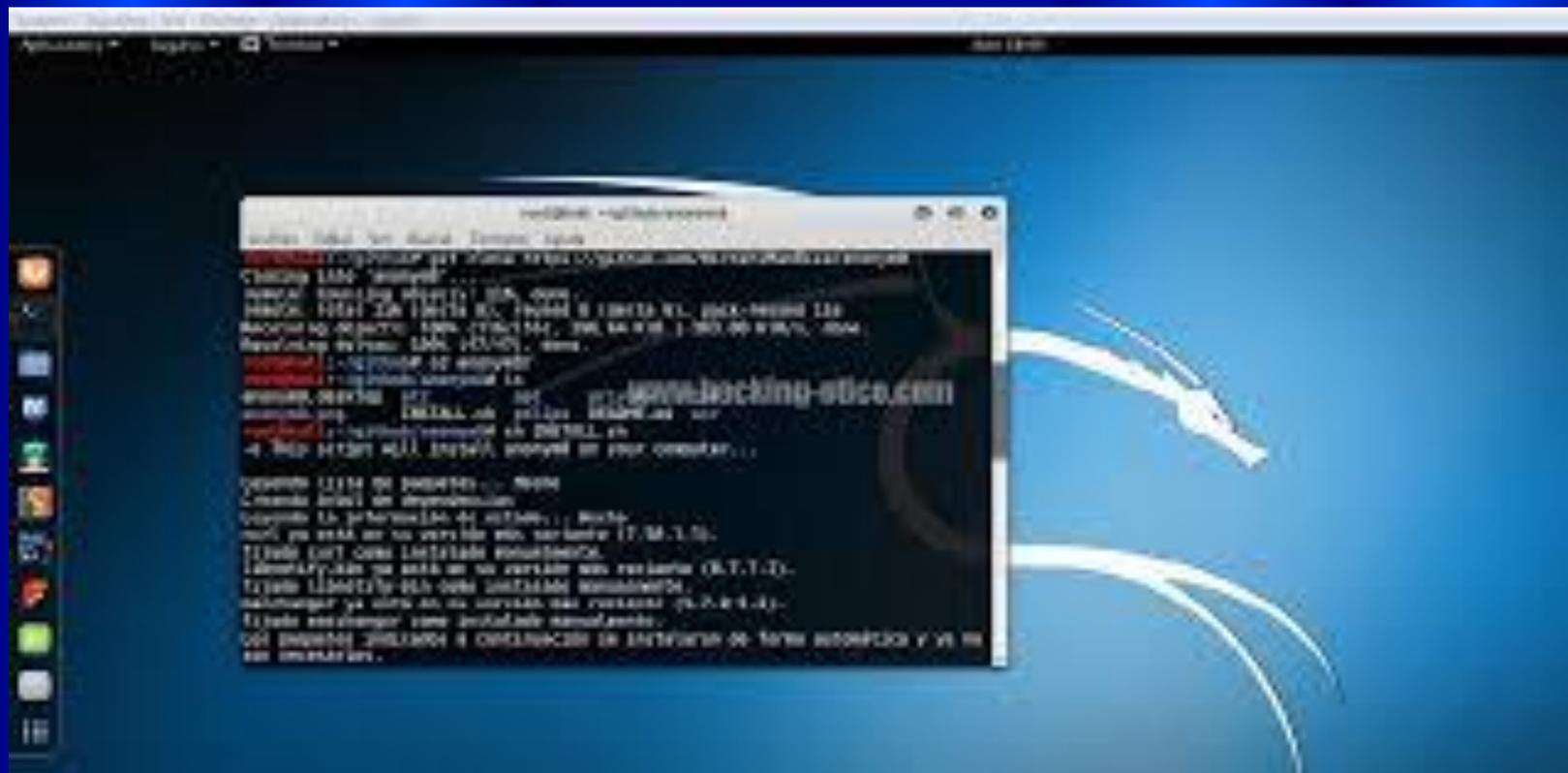
“FIREWALL vs ADDRESS LIST”



“PROFESIONALES DE RECETA”

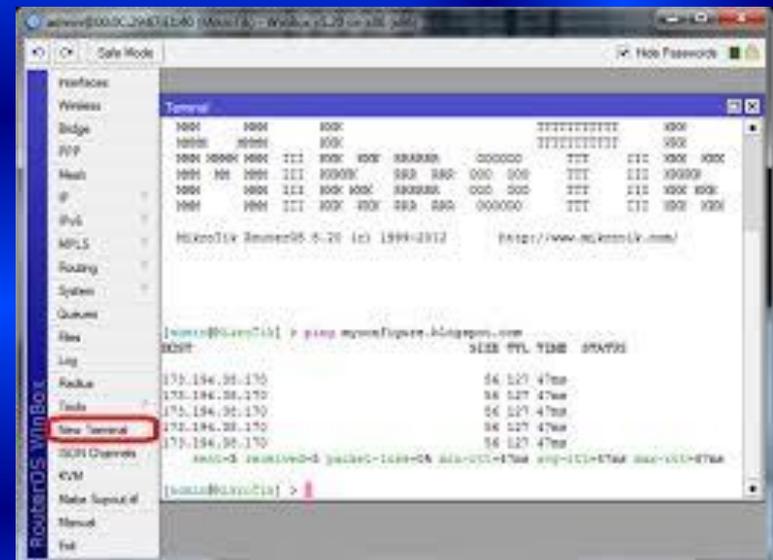


«KALI?»



«CONTRAMEDIDAS»

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



«¿Como vamos con el twitter?»



«AL ATAQUE»

admin@6C (hack-mikrotik) - WinBox v6.35.4 on hAP ac lite (mipsbe)

Session Settings Dashboard

Safe Mode Session: [REDACTED]

Queue List

Simple Queues Interface Queues Queue Tree Queue Types

00 Reset Counters 00 Reset All Counters Find

#	Name	Target	Upload Max Limit	Download Max Limit	Packet Marks	Total Max Limit (bi...
0 D	hs-<hots... invitados		unlimited	unlimited		

1 item 0 B queued 0 packets queued

Firewall

Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols

00 Reset Counters 00 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			1
4 D	redir...	hotspot			6 (tcp)		80			1
5 D	redir...	hotspot			6 (tcp)		443			1
6 D	jump	hotspot			6 (tcp)					13
7 D	jump	hotspot			6 (tcp)					13
8 D	redir...	hs-unauth			6 (tcp)		80			3
9 D	redir...	hs-unauth			6 (tcp)		3128			3
10 D	redir...	hs-unauth			6 (tcp)		8080			3
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
wlan1	Wireless (Atheros AR9...	0 bps	0 bps	0	0	0	0 bps	0 bps	0	8:C:00:06:27:00
hackagabo	Virtual AP	0 bps	0 bps	0	0	0	0 bps	0 bps	0	8:C:00:06:27:00
invitados	Virtual AP	0 bps	0 bps	0	0	0	0 bps	0 bps	0	8:C:00:06:27:00
venta	Virtual AP	0 bps	0 bps	0	0	0	0 bps	0 bps	0	8:C:00:06:27:00
wlan2	Wireless (Atheros AR9...	0 bps	0 bps	0	0	0	0 bps	0 bps	0	8:C:00:06:27:00

5 items out of 12

RouterOS WinBox

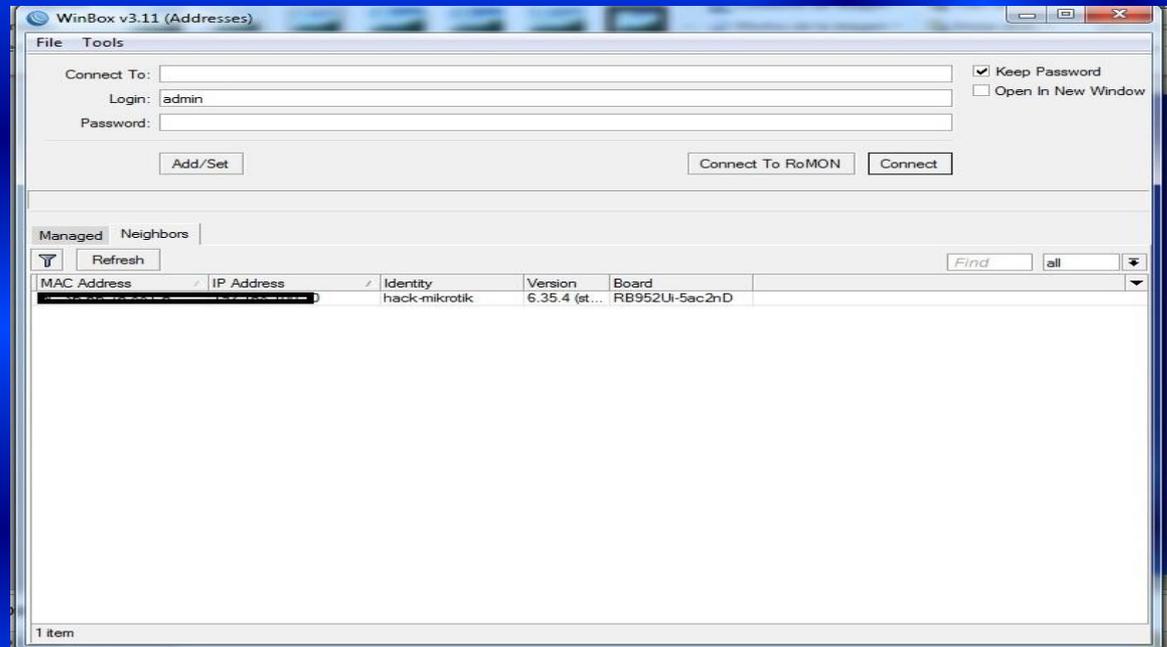
«ATAQUE DE FUERZA BRUTA»

- *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!

The screenshot displays the Mikrotik WinBox interface. The top window shows the user 'admin@192.168.100.10' connected to a Mikrotik device. The main window is divided into several panes:

- Log:** A list of system error messages indicating login failures for various users (superadmin, admin, support, 1234, Admin, root, e8telnet, telecomadmin, e8homeasb, telnetadmin) from the source IP 202.203.132.249 via telnet. The log entries are dated May 23, 2017, between 09:27:55 and 09:38:22.
- Traceroute (Running):** A configuration window for a traceroute to 202.203.132.249. The configuration includes a packet size of 56, a timeout of 1000 ms, and the use of ICMP protocol on port 33434. The 'Use DNS' checkbox is unchecked.
- Traceroute Results:** A table showing the results of the traceroute. The table has columns for Hop, Host, Loss, Sent, Last, Avg, Best, Worst, Std. Dev., and History. The results show a path of 18 hops, with a significant loss of 52.9% at hop 17 (101.4.112.197).

Hop	Host	Loss	Sent	Last	Avg	Best	Worst	Std. Dev.	History
6	190.129.250.82	0.0%	35	30.0ms	29.7	28.4	31.8	0.7	
7	84.16.9.116	0.0%	35	34.8ms	35.2	33.9	43.3	1.7	
8	94.142.99.99	0.0%	35	110.8ms	111.2	108.6	113.6	1.4	
9	213.140.37.37	0.0%	35	111.5ms	112.9	110.5	115.6	1.2	
10	63.243.152.141	0.0%	35	144.7ms	144.7	143.0	151.7	1.4	
11	63.243.152.62	2.9%	35	176.6ms	175.9	175.0	177.9	0.7	
12	66.110.72.6	0.0%	35	174.7ms	175.2	173.1	190.9	3.5	
13	66.110.57.21	0.0%	35	174.6ms	178.2	174.1	243.1	11.9	
14	66.110.59.182	0.0%	35	176.8ms	177.2	174.5	179.8	1.2	
15	101.4.117.213	0.0%	35	329.4ms	331.4	328.3	346.9	272.6	
16	101.4.117.97	0.0%	34	332.5ms	330.1	327.2	336.2	272.6	
17	101.4.112.197	52.9%	34	329.0ms	330.3	327.5	350.1	5.2	
18	202.203.132.249	0.0%	34	370.8ms	370.7	369.1	373.8	333.9	

«ATACANDO LA CAPA 8»

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



«HACKEANDO CON MIKROTIK»

- *Desde lo mas básico*

The screenshot displays the Mikrotik WinBox interface. On the left is a sidebar menu with categories like Quick Set, CAPsMAN, Interfaces, Wireless, Bridge, PPP, Switch, Mesh, IP, MPLS, Routing, System, Queues, Files, Log, Radius, Tools, New Terminal, MetaROUTER, Partition, Make Supout.rf, Manual, New WinBox, and Exit. The main workspace is divided into three panels:

- Address List:** Shows a table with columns for Address, Network, and Interface. It lists three entries with addresses ending in .82, .724, and .0/24, and interfaces named pppoe-out1, invitados, and cooset.
- IP Scan (Running):** Shows the interface 'cooset' and an address range. Below is a table of scan results:

Address	MAC Address	Time (ms)	DN
0.5		53	
0.8		43	
0.21		43	
0.30		58	
0.35		53	
0.45		58	
0.52		54	
0.53		53	
0.54		42	
0.58		56	
0.59		56	
0.62		658	
0.68		54	
0.71		51	
0.98		83	
0.126		58	
0.137		58	
0.176		60	
0.178		58	
0.182		4	
0.184		53	
0.208		241	
0.211		53	
0.246		54	
0.248		39	

- PPPoE Scan (Running):** Shows the interface 'ether1'. Below is a table with columns for Service, MAC Address, and AC Name:

Service	MAC Address	AC Name
Tabladita	[REDACTED]	CosettNET - Premium

At the bottom of each panel, the number of items is displayed: 3 items for Address List, 25 items for IP Scan, and 1 item for PPPoE Scan.

«FUSION A.F.B CON SQL INYECTION»

RouterOS v6.35.4

You have connected to a router. Administrative access only. If this device is not in your possession, please contact your local network administrator.

WebFig Login:

Login: Login

Password:

Winbox Telnet Graphs License Help

© mikrotik

WINDOWS 10!

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 certificación. Con nuestros cursos podrás capacitarte y obtener las certificaciones de MikroTik.

Proximos Cursos

MTCNA

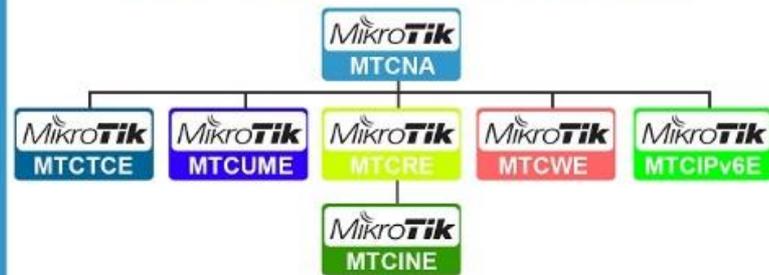
26 Ago 2017

MTCTCE

29 Ago 2017

Reserva ahora con
448.000 Gs.

Certificaciones



Contáctenos



info@ecatel.com.py

 0973 691525

 EcatelSRL



BIENVENIDOS



Gracias

