

Microsoft®



Microsoft
Windows 95

Mikrotik Security

Amenazas comunes

Por David gonzalez herrera
www.tikacademy.com

TikAcademy 

Agenda

- presentación
- ¿Qué es Amenaza de Seguridad?
- Ataques comunes en RouterOS
- Algunas formas de mitigación

AmyLee

(2007-2019)



Amen y cuiden a sus mascotas!.

Ellos son los únicos seres 100% inocentes de la creación; te amarán toda la vida y nunca te pedirán nada a cambio.

¿Quiénes somos?

TikAcademy

- Nace en 2015
- Academia MikroTik desde 2016
- Miles de horas de capacitación impartidas
- Cursos personalizados
- Traducción y revisión del material de capacitación de MikroTik
- Conferencias internacionales

Servicios

- Implementación de soluciones
- Consultoría y capacitación
- Auditoría de e infraestructura
- Diseño de soluciones basadas en MikroTik
- Capacitación y Certificación en otros fabricantes

¿Quiénes somos?

DAVID GONZÁLEZ HERRERA

- Instructor Mikrotik
- Instructor
- Consultor Mikrotik
- Especialista en Virtualización y Linux
- Certificado BGP (LACNIC)
- Implementación de la Infraestructura de Gateways de Pago
- Migración de Otros Fabricantes a Mikrotik.

PROYECTOS



bmind®

TikAcademy

Somos Más

Primera Edición

El Workbook de
MikroTik RouterOS

GRAN LANZAMIENTO!
VENTAS +57-312-770-4122

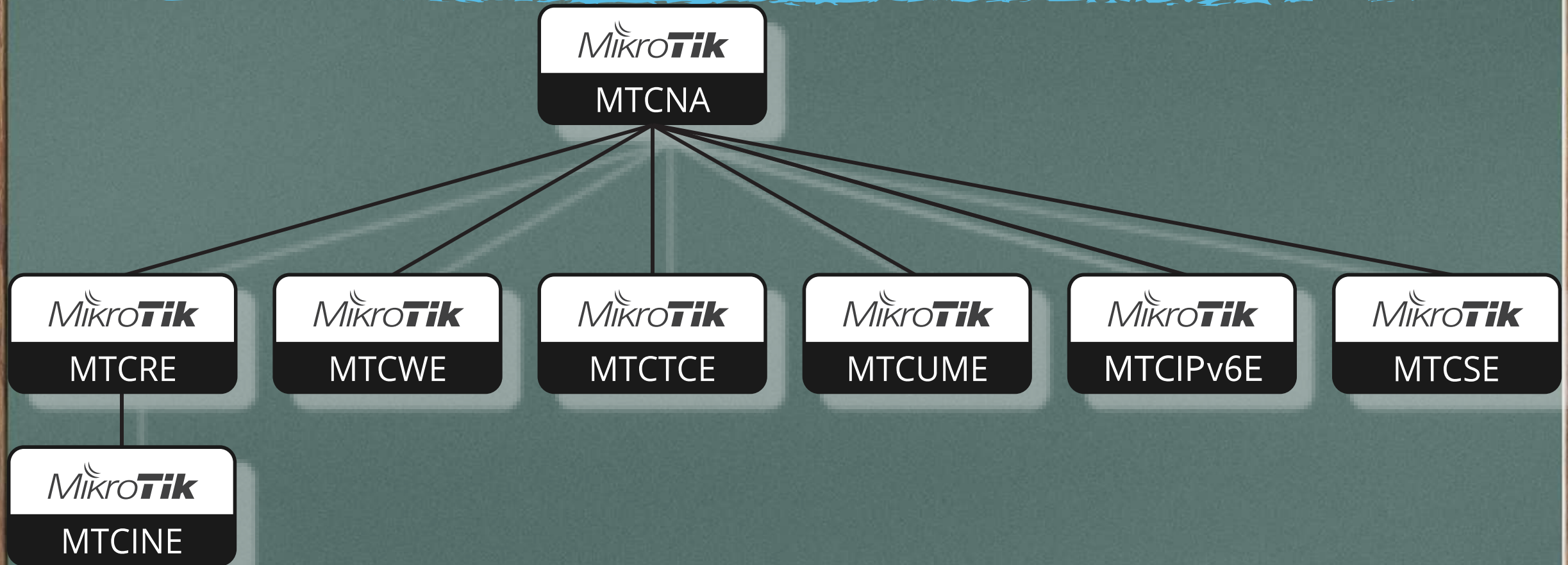


David González Herrero es un consultor empujador en las áreas de programación, cableado, configuración y mantenimiento de redes. Es un profesional certificado de Ubiquiti y Mikrotik. Durante los últimos años ha desempeñado como responsable de la construcción de redes y como asesor para varias plataformas internacionales. En el año 2016 fundó la academia de formación TikAcademy con la intención de brindar cursos de certificación en manejo e implementación de dispositivos Mikrotik en todo el territorio colombiano y el extranjero. Producto de su experiencia como instructor y conferencista, ha diseñado este material con el fin de compartir su conocimiento y responder a la constante necesidad de capacitación de todos los interesados en el manejo e implementación de dispositivos destinados a la intercomunicación y tráfico de datos.

MikroTik

Autor: David González Herrero (TR0384)
TikAcademy - MikroTik Colombia
www.tikacademy.com

CURSOS MIKROTIK – TIKACADEMY



CURSOS MIKROTIK – TIKACADEMY





¿que es una amenaza de seguridad?

¿Conoce las métodos de Ataque?
¿Está preparado?

¿Qué es una amenaza de seguridad?

- La seguridad informática, también conocida como ciberseguridad o seguridad de tecnología de la información, es el área relacionada con la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida en una computadora o circulante a través de las redes de computadoras.
- Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información.

"What is Computer security?", Matt Bishop, IEEE Security and Privacy Magazine 1(1):67 - 69, 2003.

DOI: 10.1109/MSECP.2003.1176998

¿Qué es una amenaza de seguridad?

- La ciberseguridad comprende software (bases de datos, metadatos, archivos), hardware, redes de computadoras y todo lo que la organización valore y signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada.

"What is Computer security?", Matt Bishop, IEEE Security and Privacy Magazine 1(1):67 - 69, 2003.
DOI: 10.1109/MSECP.2003.1176998

AMENAZAS

- Hacking
- Ingeniería Social
- DDoS
- Virus
- Ransomware
- Troyanos
- Malware
- Phishing
- Spoofing
- Spam
- Spyware
- Gusanos
- Botnets



¿Qué es una amenaza de seguridad?

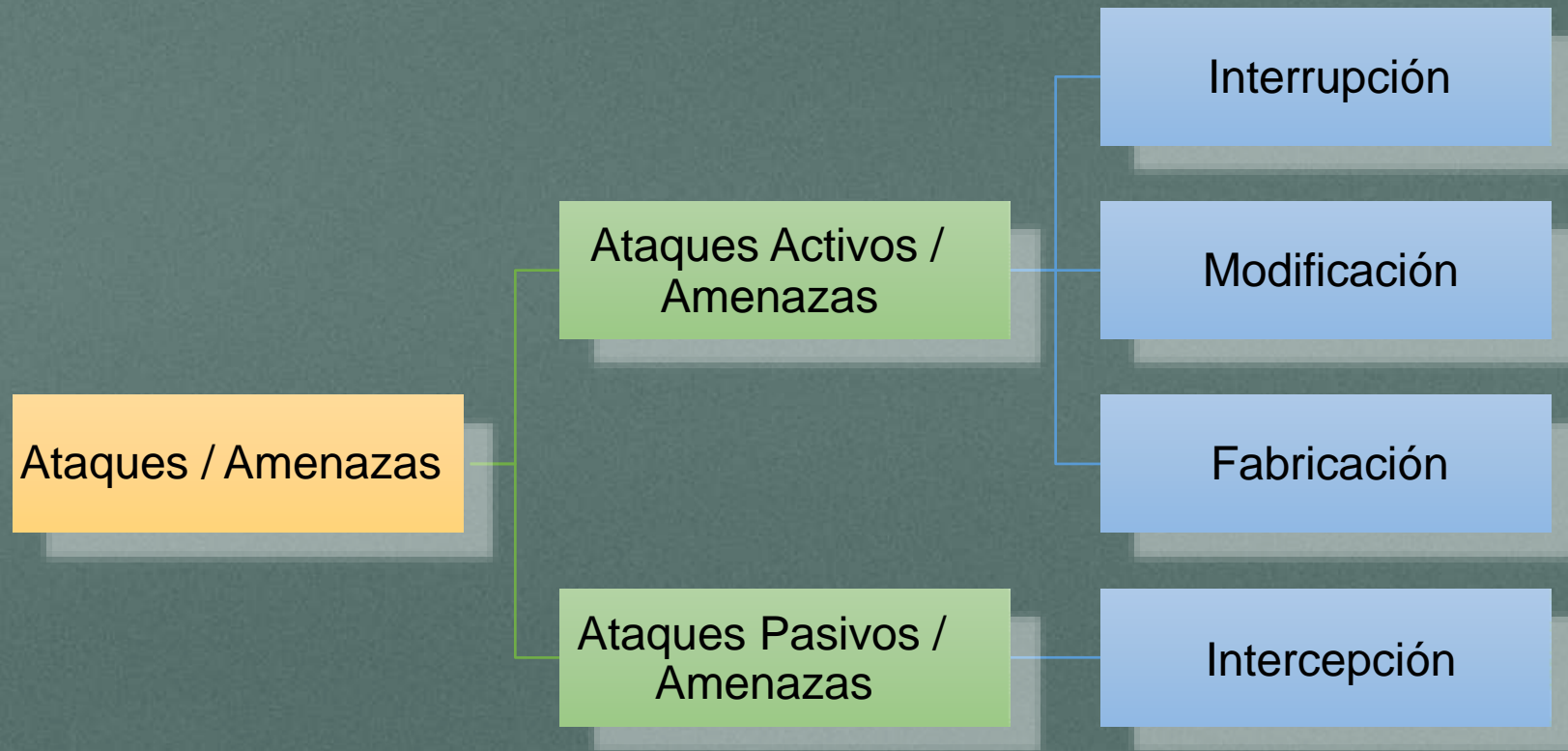
▪ Amenaza Externa

- Aquella que se origina desde el exterior de la organización con el fin de robar, destruir o modificar información confidencial de esa institución.
- Algunas veces, no tienen una meta fija, solo explotan un fallo encontrado

▪ Amenaza Interna

- Aquella originada desde dentro de la organización o institución que comúnmente es causada y explotada por empleados inconformes a quienes se les ha negado un ascenso, aumento salarial o se les avisa la terminación del contrato.
- Aprovecha el conocimiento interno para causar daño a la infraestructura o información

¿Qué es una amenaza de seguridad?



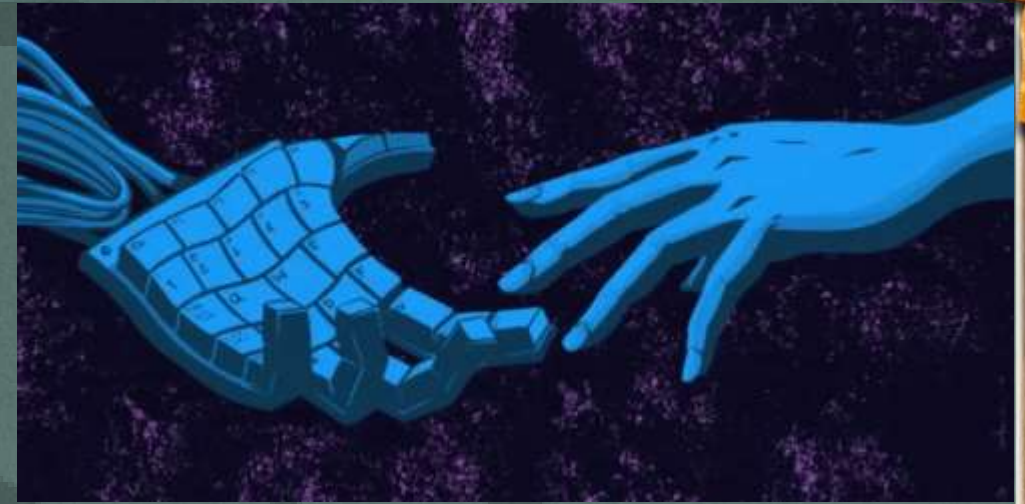
¿PLANEACIÓN???...



Crear un plan, una estrategia de protección de los recursos de la red y la información

PREVENCIÓN

tomar medidas que prevengan que sus activos sean dañados (o robados)



DETECCIÓN

tomar medidas que le permitan detectar por quien, como y cuando un activo fue accedido, robado o dañado

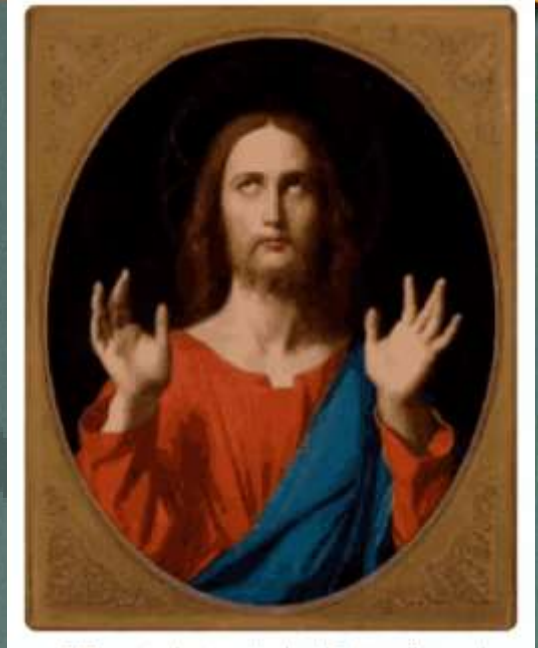


MITIGACIÓN

Analizar como protegerse de las amenazas y tomar medidas que le permitan recuperar sus activos. Educar a sus usuarios sobre las posibles amenazas.



ORACIÓN



Cuando todo lo demás no se hizo y se enteró del
tema hoy y aquí

FIREWALL EN ROUTEROS

Desde donde parte la seguridad

firewall en RouterOS

- RouterOS implementa un firewall de estado. Este tipo de firewall es un firewall capaz de hacer seguimiento de conexiones ICMP, UDP y TCP.
- Esto significa que el firewall puede identificar si un paquete está relacionado a un paquete anterior.
- Organizado en cadenas secuencialmente procesadas
- Sigue el principio IF-THEN
- Puede hacer seguimiento del estado operacional de conexiones.

firewall en RouterOS

Connection Tracking

- Provee información sobre conexiones
- Utiliza bastantes recursos de CPU
- Debe ser habilitado para Filter y NAT

Firewall

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

Tracking

	Src. Address	Dst. Address	Protocol	Conn.
C	0.0.0.0	239.255.255.250	2 (igmp)	
C	0.0.0.0	224.0.0.251	2 (igmp)	
SACd	1.240.113.29:52157	181.63.192.192:51413	17 (udp)	
SACd	3.86.144.234:49165	181.63.192.192:51413	17 (udp)	
SACd	5.189.157.90:9888	181.63.192.192:51413	17 (udp)	
SACd	5.189.157.90:11989	181.63.192.192:51413	17 (udp)	
SACd	5.189.157.90:12040	181.63.192.192:51413	17 (udp)	
SACd	5.189.157.90:12057	181.63.192.192:51413	17 (udp)	
SACd	5.189.160.21:2171	181.63.192.192:51413	17 (udp)	
SACd	5.189.160.21:2188	181.63.192.192:51413	17 (udp)	
SACd	5.189.160.21:60205	181.63.192.192:51413	17 (udp)	
SACd	5.189.183.129:51320	181.63.192.192:51413	17 (udp)	
SCd	31.29.192.54:49001	181.63.192.192:51413	17 (udp)	
SACd	35.236.105.29:6992	181.63.192.192:51413	17 (udp)	
SCd	49.206.211.182:54287	181.63.192.192:51413	17 (udp)	

435 items

Connection Tracking

Enabled: auto

☒ Loose TCP Tracking

TCP Syn Sent Timeout: 00:00:05

TCP Syn Received Timeout: 00:00:05

TCP Established Timeout: 1d 00:00:00

TCP Fin Wait Timeout: 00:00:10

TCP Close Wait Timeout: 00:00:10

TCP Last Ack Timeout: 00:00:10

TCP Time Wait: 00:00:10

TCP Close: 00:00:10

TCP Max Retransmit Timeout: 00:05:00

TCP Unacked Timeout: 00:05:00

UDP Timeout: 00:00:10

UDP Stream Timeout: 00:03:00

ICMP Timeout: 00:00:10

Generic Timeout: 00:10:00

firewall en RouterOS

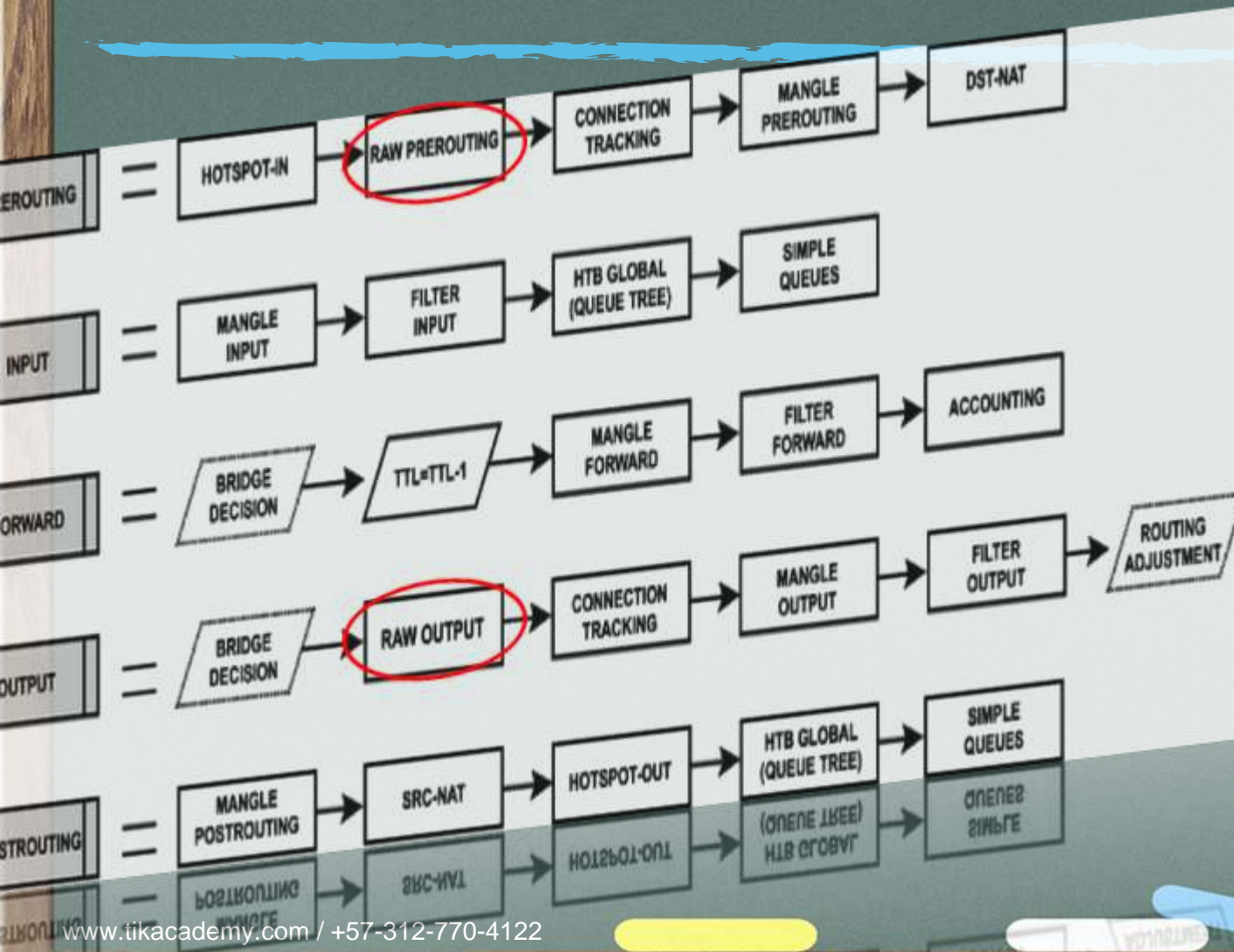


TABLA RAW

- Solo en Prerouting y Output
- Evita Connection Tracking
- Reduce consumo de CPU

Ataques a Mikrotik RouterOS

¿Sabía sobre ellos?

Ataques a Mikrotik RouterOS

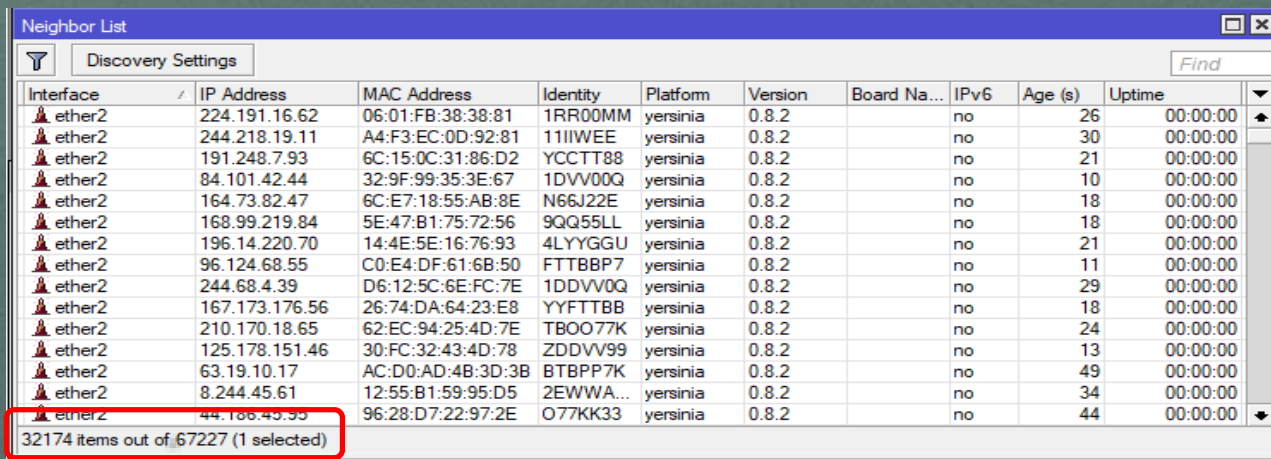
- Ataque de Fuerza Bruta
 - Pretende lograr acceso no autorizado a dispositivos
 - Automáticamente prueba combinaciones de usuario/clave
 - Agota tanto recursos de red como de máquina
 - Potencialmente peligroso si las contraseñas son débiles

Et...	Protocol	Src.	Dest.	Tx Rate	Rx Rate	Tx Pack	Rx Pack
800 (ip)	6 (tcp)	192.168.1.254:39202	192.168.1.1:22 (ssh)	0 bps	0 bps		
800 (ip)	6 (tcp)	192.168.1.254:45605	192.168.1.1:22 (ssh)	0 bps	0 bps		
800 (ip)	6 (tcp)	192.168.1.254:38707	192.168.1.1:22 (ssh)	0 bps	0 bps		
800 (ip)	6 (tcp)	192.168.1.254:40363	192.168.1.1:22 (ssh)	0 bps	0 bps		
800 (ip)	6 (tcp)	192.168.1.254:57012	192.168.1.1:22 (ssh)	0 bps	0 bps		
800 (ip)	6 (tcp)	192.168.1.254:51584	192.168.1.1:22 (ssh)	0 bps	0 bps		
800 (ip)	6 (tcp)	192.168.1.254:40917	192.168.1.1:22 (ssh)	0 bps	0 bps		
800 (ip)	6 (tcp)	192.168.1.254:59630	192.168.1.1:22 (ssh)	0 bps	0 bps		
800 (ip)	6 (tcp)	192.168.1.254:42983	192.168.1.1:22 (ssh)	0 bps	0 bps		
800 (ip)	6 (tcp)	192.168.1.254:56839	192.168.1.1:22 (ssh)	0 bps	0 bps		
800 (ip)	6 (tcp)	192.168.1.254:42752	192.168.1.1:22 (ssh)	0 bps	0 bps		
800 (ip)	6 (tcp)	192.168.1.254:58035	192.168.1.1:22 (ssh)	0 bps	0 bps		
800 (ip)	6 (tcp)	192.168.1.254:34975	192.168.1.1:22 (ssh)	0 bps	0 bps		
800 (ip)	6 (tcp)	192.168.1.254:52383	192.168.1.1:22 (ssh)	0 bps	0 bps		
800 (ip)	6 (tcp)	192.168.1.254:57142	192.168.1.1:22 (ssh)	0 bps	0 bps		
Total Tx: 0 bps				Total Rx: 0 bps			
Total Tx Packet: 0				Total Rx Packet: 0			

Et...	Protocol	Src.	Dest.	Tx Rate	Rx Rate
800 (ip)	6 (tcp)	192.168.1.254:40876	192.168.1.1:23 (telnet)	592 bps	1120 bps
800 (ip)	6 (tcp)	192.168.1.254:57657	192.168.1.1:23 (telnet)	968 bps	1056 bps
800 (ip)	6 (tcp)	192.168.1.254:44580	192.168.1.1:23 (telnet)	2.2 kbps	528 bps
800 (ip)	6 (tcp)	192.168.1.254:53595	192.168.1.1:23 (telnet)	0 bps	0 bps
800 (ip)	6 (tcp)	192.168.1.254:45764	192.168.1.1:23 (telnet)	0 bps	0 bps
800 (ip)	6 (tcp)	192.168.1.254:51001	192.168.1.1:23 (telnet)	0 bps	0 bps

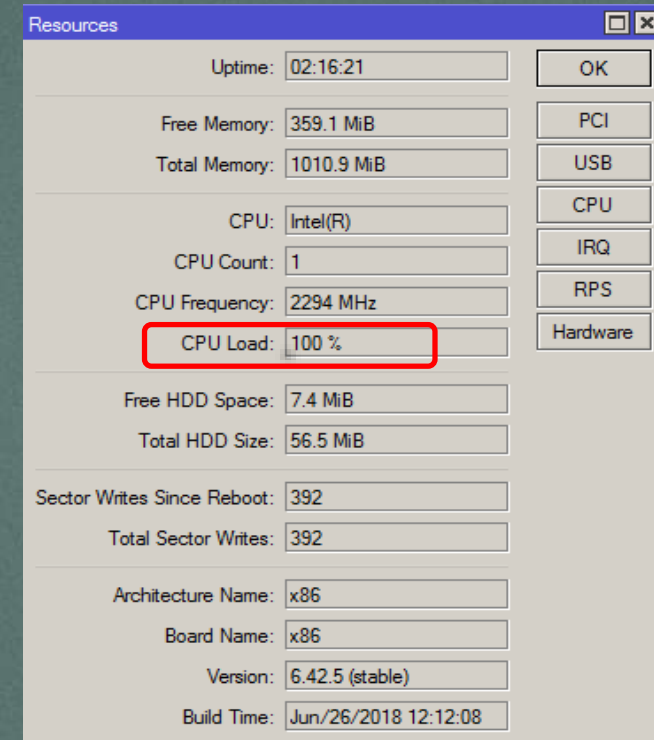
Ataques a MikroTik RouterOS

- Inundación MNDP
 - Utiliza el puerto UDP 5678
 - Saturar el dispositivo con anuncios de vecinos falsos
 - Consume recursos hasta hacer reiniciar el dispositivo



Interface	IP Address	MAC Address	Identity	Platform	Version	Board Na...	IPv6	Age (s)	Uptime
ether2	224.191.16.62	06:01:FB:38:38:81	1RR00MM	yersinia	0.8.2		no	26	00:00:00
ether2	244.218.19.11	A4:F3:EC:0D:92:81	11IIWEE	yersinia	0.8.2		no	30	00:00:00
ether2	191.248.7.93	6C:15:0C:31:86:D2	YCCTT88	yersinia	0.8.2		no	21	00:00:00
ether2	84.101.42.44	32:9F:99:35:3E:67	1DVV00Q	yersinia	0.8.2		no	10	00:00:00
ether2	164.73.82.47	6C:E7:18:55:AB:8E	N66J22E	yersinia	0.8.2		no	18	00:00:00
ether2	168.99.219.84	5E:47:B1:75:72:56	9QQ55LL	yersinia	0.8.2		no	18	00:00:00
ether2	196.14.220.70	14:4E:5E:16:76:93	4LYYGGU	yersinia	0.8.2		no	21	00:00:00
ether2	96.124.68.55	C0:E4:DF:61:6B:50	FTTB8P7	yersinia	0.8.2		no	11	00:00:00
ether2	244.68.4.39	D6:12:5C:6E:FC:7E	1DDVV0Q	yersinia	0.8.2		no	29	00:00:00
ether2	167.173.176.56	26:74:DA:64:23:E8	YYFTTB8	yersinia	0.8.2		no	18	00:00:00
ether2	210.170.18.65	62:EC:94:25:4D:7E	TBOO77K	yersinia	0.8.2		no	24	00:00:00
ether2	125.178.151.46	30:FC:32:43:4D:78	ZDDVV99	yersinia	0.8.2		no	13	00:00:00
ether2	63.19.10.17	AC:D0:AD:4B:3D:3B	BTBPP7K	yersinia	0.8.2		no	49	00:00:00
ether2	8.244.45.61	12:55:B1:59:95:D5	2EWWA...	yersinia	0.8.2		no	34	00:00:00
ether2	44.186.45.95	96:28:D7:22:97:2E	O77KK33	yersinia	0.8.2		no	44	00:00:00

32174 items out of 67227 (1 selected)



Uptime:	02:16:21	OK
Free Memory:	359.1 MiB	PCI
Total Memory:	1010.9 MiB	USB
CPU:	Intel(R)	CPU
CPU Count:	1	IRQ
CPU Frequency:	2294 MHz	RPS
CPU Load:	100 %	Hardware
Free HDD Space:	7.4 MiB	
Total HDD Size:	56.5 MiB	
Sector Writes Since Reboot:	392	
Total Sector Writes:	392	
Architecture Name:	x86	
Board Name:	x86	
Version:	6.42.5 (stable)	
Build Time:	Jun/26/2018 12:12:08	

Ataques a Mikrotik RouterOS

- Ataque de Inundación UDP
 - Colapsar ya sea la red o el dispositivo enviando datagramas UDP
 - No explota ninguna vulnerabilidad
 - Se usa con frecuencia para ataques DNS DDoS

Firewall

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

Tracking

	Src. Address	Dst. Address	Protocol	Conn...	Timeout	TCP State	Orig./Repl. Rate	Orig./Repl. Bytes
C	0.0.0.0:68	255.255.255.255:67	17 (udp)		00:00:04		0 bps/0 bps	328 B/0 B
C	3.10.87.19:4528	192.168.188.1:53	17 (udp)		00:00:06		0 bps/0 bps	28 B/0 B
C	6.165.214.142:2543	192.168.188.1:53	17 (udp)		00:00:06		0 bps/0 bps	28 B/0 B
C	6.220.226.255:2390	192.168.188.1:53	17 (udp)		00:00:00		0 bps/0 bps	28 B/0 B
C	10.212.198.127:2395	192.168.188.1:53	17 (udp)		00:00:00		0 bps/0 bps	28 B/0 B
C	10.218.147.58:5290	192.168.188.1:53	17 (udp)		00:00:00		0 bps/0 bps	28 B/0 B
C	10.231.192.104:5096	192.168.188.1:53	17 (udp)		00:00:00		0 bps/0 bps	28 B/0 B
C	12.160.68.226:4643	192.168.188.1:53	17 (udp)		00:00:06		0 bps/0 bps	28 B/0 B
C	12.215.174.0:4848	192.168.188.1:53	17 (udp)		00:00:00		0 bps/0 bps	28 B/0 B
C	12.215.227.34:5526	192.168.188.1:53	17 (udp)		00:00:00		0 bps/0 bps	28 B/0 B
C	13.87.111.255:4562	192.168.188.1:53	17 (udp)		00:00:06		0 bps/0 bps	28 B/0 B
C	14.182.45.142:4749	192.168.188.1:53	17 (udp)		00:00:00		0 bps/0 bps	28 B/0 B
C	19.179.224.45:5443	192.168.188.1:53	17 (udp)		00:00:00		0 bps/0 bps	28 B/0 B
C	23.185.63.210:2345	192.168.188.1:53	17 (udp)		00:00:06		0 bps/0 bps	28 B/0 B
C	24.141.150.80:2403	192.168.188.1:53	17 (udp)		00:00:01		0 bps/0 bps	28 B/0 B

161 items out of 25278

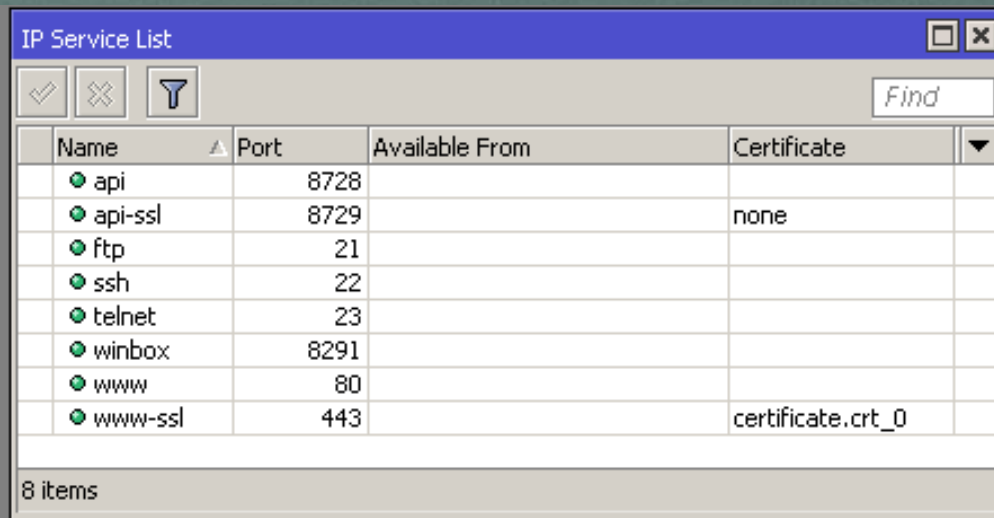
Max Entries: 163744

Resources

Uptime:	00:37:46
Free Memory:	41.4 MB
Total Memory:	96.0 MB
CPU:	QEMU
CPU Count:	1
CPU Frequency:	3592 MHz
CPU Load:	100 %
Free HDD Space:	31.4 MB
Total HDD Size:	63.5 MB
Sector Writes Since Reboot:	936
Total Sector Writes:	937
Architecture Name:	x86_64
Board Name:	CHR
Version:	6.44.3 (stable)
Build Time:	Apr/23/2019 12:37:03

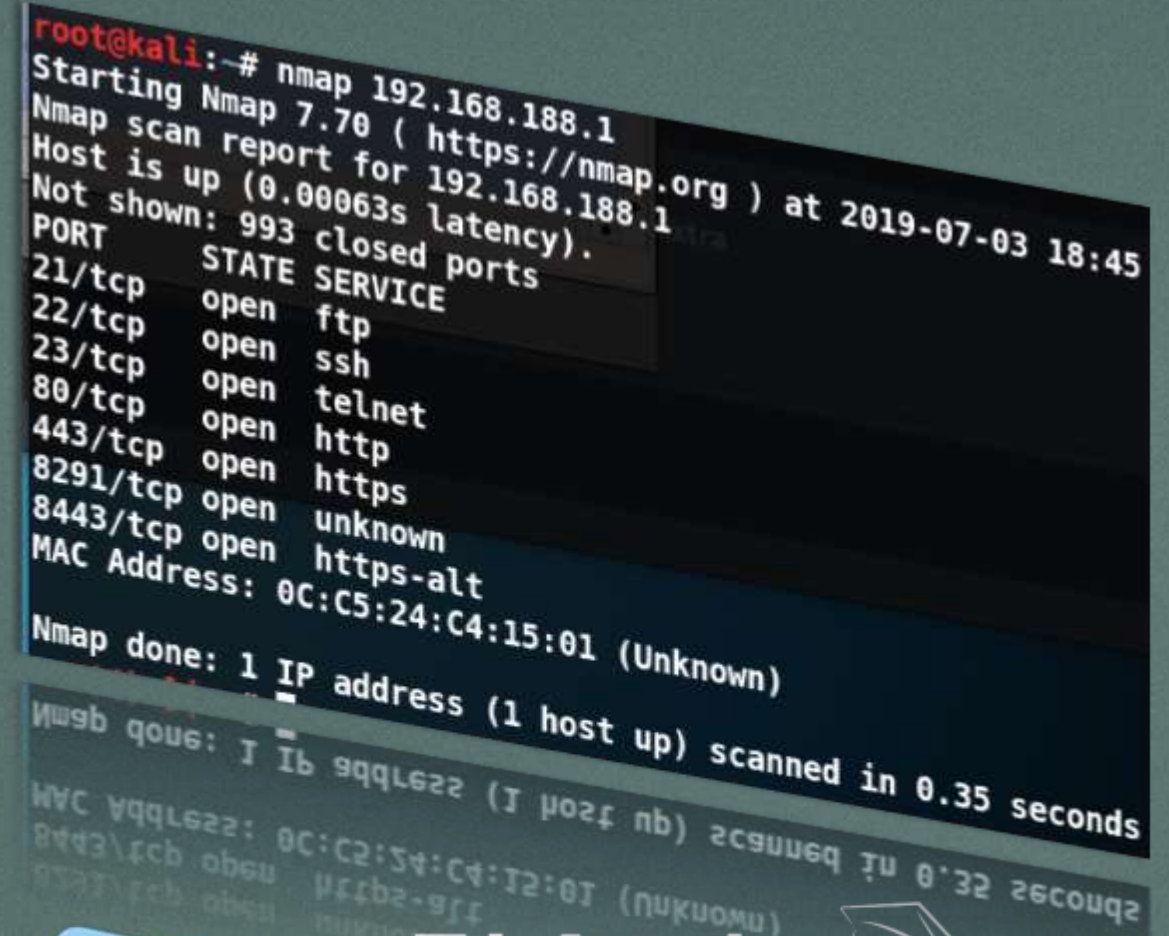
Ataques a MikroTik RouterOS

- Escaneo de Puertos
 - Aunque no es un ataque, es el inicio de uno
 - Genera tráfico inútil en la red
 - Causa sobrecarga



Name	Port	Available From	Certificate
api	8728		
api-ssl	8729		none
ftp	21		
ssh	22		
telnet	23		
winbox	8291		
www	80		
www-ssl	443		certificate.crt_0

8 items



```
root@kali:~# nmap 192.168.188.1
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-03 18:45
Nmap scan report for 192.168.188.1
Host is up (0.00063s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
443/tcp    open  https
8291/tcp  open  unknown
8443/tcp  open  https-alt
MAC Address: 0C:C5:24:C4:15:01 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
```


Ataques a Mikrotik RouterOS

- DHCP Starvation (Inanición DHCP)
 - Difunde peticiones DHCPREQUEST con direcciones MAC falsificadas.
 - Agota las IP disponibles impidiendo la conexión a clientes lícitos.
 - Consume recursos como memoria y CPU

Log			
Freeze			
Jul/01/2019 23:22:48	memory	dhcp, error	dhcp1: failed to give out IP address: pool <dhcp_pool0> is empty
Jul/01/2019 23:22:48	memory	dhcp, error	dhcp1: failed to give out IP address: pool <dhcp_pool0> is empty
Jul/01/2019 23:22:48	memory	dhcp, error	dhcp1: failed to give out IP address: pool <dhcp_pool0> is empty
Jul/01/2019 23:22:48	memory	dhcp, error	dhcp1: failed to give out IP address: pool <dhcp_pool0> is empty
Jul/01/2019 23:22:48	memory	dhcp, error	dhcp1: failed to give out IP address: pool <dhcp_pool0> is empty
Jul/01/2019 23:22:48	memory	dhcp, error	dhcp1: failed to give out IP address: pool <dhcp_pool0> is empty
Jul/01/2019 23:22:48	memory	dhcp, error	dhcp1: failed to give out IP address: pool <dhcp_pool0> is empty
Jul/01/2019 23:22:48	memory	dhcp, error	dhcp1: failed to give out IP address: pool <dhcp_pool0> is empty
Jul/01/2019 23:22:48	memory	dhcp, error	dhcp1: failed to give out IP address: pool <dhcp_pool0> is empty
Jul/01/2019 23:22:48	memory	dhcp, error	dhcp1: failed to give out IP address: pool <dhcp_pool0> is empty
Jul/01/2019 23:22:48	memory	dhcp, error	dhcp1: failed to give out IP address: pool <dhcp_pool0> is empty

Resources	
Uptime:	00:37:46
Free Memory:	41.4 MB
Total Memory:	96.0 MB
CPU:	QEMU
CPU Count:	1
CPU Frequency:	2592 MHz
CPU Load:	100 %

IP Pool			
Pools		Used Addresses	
Pool	Address	Owner	Info
dhcp_pool0	192.168.188.2	DHCP	02:51:58:1C:F7:1D
dhcp_pool0	192.168.188.3	DHCP	66:20:4C:1B:71:D7
dhcp_pool0	192.168.188.4	DHCP	A0:6C:D7:23:22:3F
dhcp_pool0	192.168.188.5	DHCP	88:68:7C:7F:81:FB
dhcp_pool0	192.168.188.6	DHCP	88:06:53:7B:D0:ED
dhcp_pool0	192.168.188.7	DHCP	68:5D:F1:15:11:9D
dhcp_pool0	192.168.188.8	DHCP	70:C3:3F:79:4B:11
dhcp_pool0	192.168.188.9	DHCP	FE:B2:49:45:D0:90
dhcp_pool0	192.168.188.10	DHCP	14:42:6E:60:9E:16
dhcp_pool0	192.168.188.11	DHCP	42:61:4A:4B:1A:45
dhcp_pool0	192.168.188.12	DHCP	BA:3F:A8:53:A0:C5
dhcp_pool0	192.168.188.13	DHCP	08:A1:5E:7F:49:FC
dhcp_pool0	192.168.188.14	DHCP	E6:F8:50:0A:5F:EB
dhcp_pool0	192.168.188.15	DHCP	34:58:CE:3D:0B:E6
dhcp_pool0	192.168.188.16	DHCP	88:3E:85:31:84:17

Ataques a Mikrotik RouterOS

- Ataque TCP SYN
 - Explota el saludo de tres vías de TCP
 - Envía enormes cantidades de paquetes TCP SYN con Src. Address falsa
 - La víctima responde con un paquete TCP/SYN-ACK

Resources

Uptime: 00:37:46

Free Memory: 41.4 MB

Total Memory: 96.0 MB

CPU: QEMU

CPU Count: 1

CPU Frequency: 3500 MHz

CPU Load: 100 %

Free HDD Space: 31.4 MB

Total HDD Size: 63.5 MB

Sector Writes Since Reboot: 936

Total Sector Writes: 937

Architecture Name: x86_64

Board Name: CHR

Version: 6.44.3 (stable)

Build Time: Apr/23/2019 12:37:03

Firewall

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

Tracking Find

	Src. Address	Dst. Address	Proto...	Connecti...	Timeout	TCP State	Orig./Repl. Rate	Orig./Repl. Bytes
C	1.1.196.241:29889	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	bps/0 bps	160 B/0 B
C	1.1.213.148:31538	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	bps/0 bps	160 B/0 B
C	1.6.33.104:36289	192.168.1.1:80	6 (tcp)		00:00:02	syn sent	bps/0 bps	160 B/0 B
C	1.6.132.187:64285	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	bps/0 bps	160 B/0 B
C	1.6.175.4:42697	192.168.1.1:80	6 (tcp)		00:00:04	syn sent	bps/0 bps	160 B/0 B
C	1.8.165.191:9503	192.168.1.1:80	6 (tcp)		00:00:01	syn sent	bps/0 bps	160 B/0 B
C	1.8.173.46:62682	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	bps/0 bps	160 B/0 B
C	1.8.244.152:36349	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	bps/0 bps	160 B/0 B
C	1.9.212.87:40970	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	bps/0 bps	160 B/0 B
C	1.10.67.244:57959	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	bps/0 bps	160 B/0 B
C	1.10.102.91:5321	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	bps/0 bps	160 B/0 B
C	1.13.67.211:9280	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	bps/0 bps	160 B/0 B
C	1.13.189.198:14185	192.168.1.1:80	6 (tcp)		00:00:01	syn sent	bps/0 bps	160 B/0 B
C	1.16.48.178:25762	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	bps/0 bps	160 B/0 B
C	1.18.139.155:61426	192.168.1.1:80	6 (tcp)		00:00:00	syn sent	bps/0 bps	160 B/0 B
C	1.19.155.158:13113	192.168.1.1:80	6 (tcp)		00:00:03	syn sent	bps/0 bps	160 B/0 B
C	1.19.209.175:32379	192.168.1.1:80	6 (tcp)		00:00:03	syn sent	bps/0 bps	160 B/0 B
C	1.21.42.131:47210	192.168.1.1:80	6 (tcp)		00:00:01	syn sent	bps/0 bps	160 B/0 B

48601 items out of 300864 Max Entries: 1048576

Algunas formas de mitigación

¿Sabía sobre ellos?

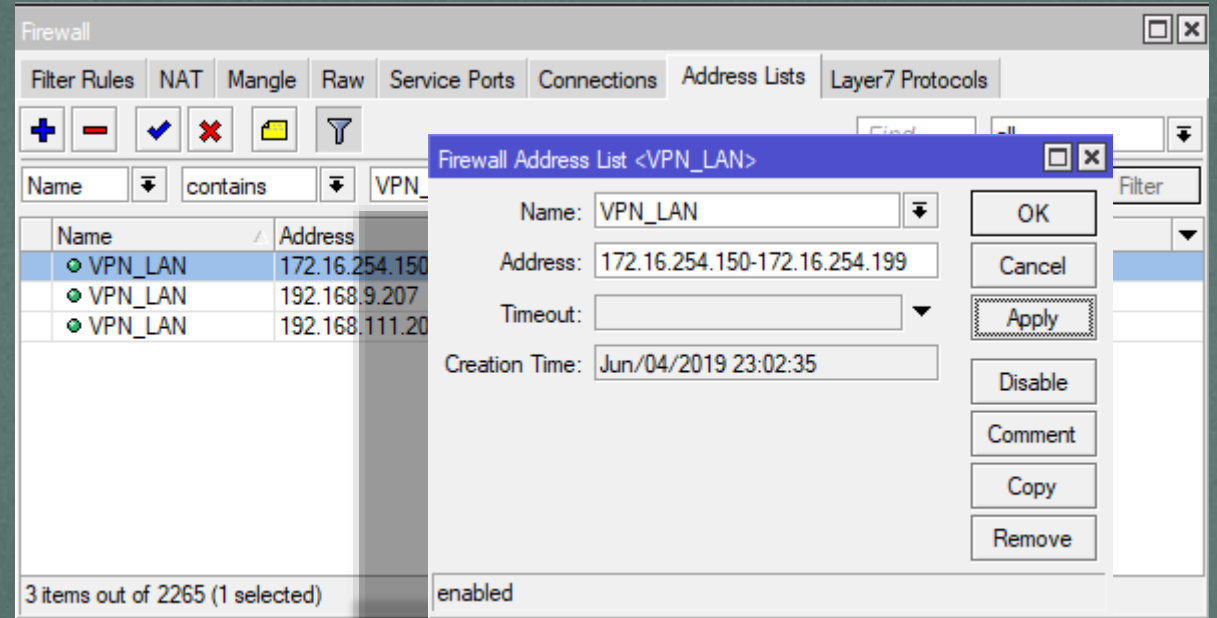
ALGUNAS FORMAS DE MITIGACIÓN

- Descartar conexiones inválidas
- El firewall funciona solo con conexiones nuevas
- Descartar paquetes entrantes no NAT'eados
- Hacer seguimiento y bloqueo de ICMP
 - ICMP no es solo PING
- Descartar paquetes no-LAN
- Restringir acceso a servicios no usados
- Descartar todo el trafico no deseado

ALGUNAS FORMAS DE MITIGACIÓN

Implementar Address Lists

- Las listas de direcciones para organizar y agrupar IPs desde e implementar control de acceso
- Al ser un contendedor ayuda a simplificar las reglas del firewall
- Tienen la capacidad de resolver nombres de DNS, muy útil



ALGUNAS FORMAS DE MITIGACIÓN

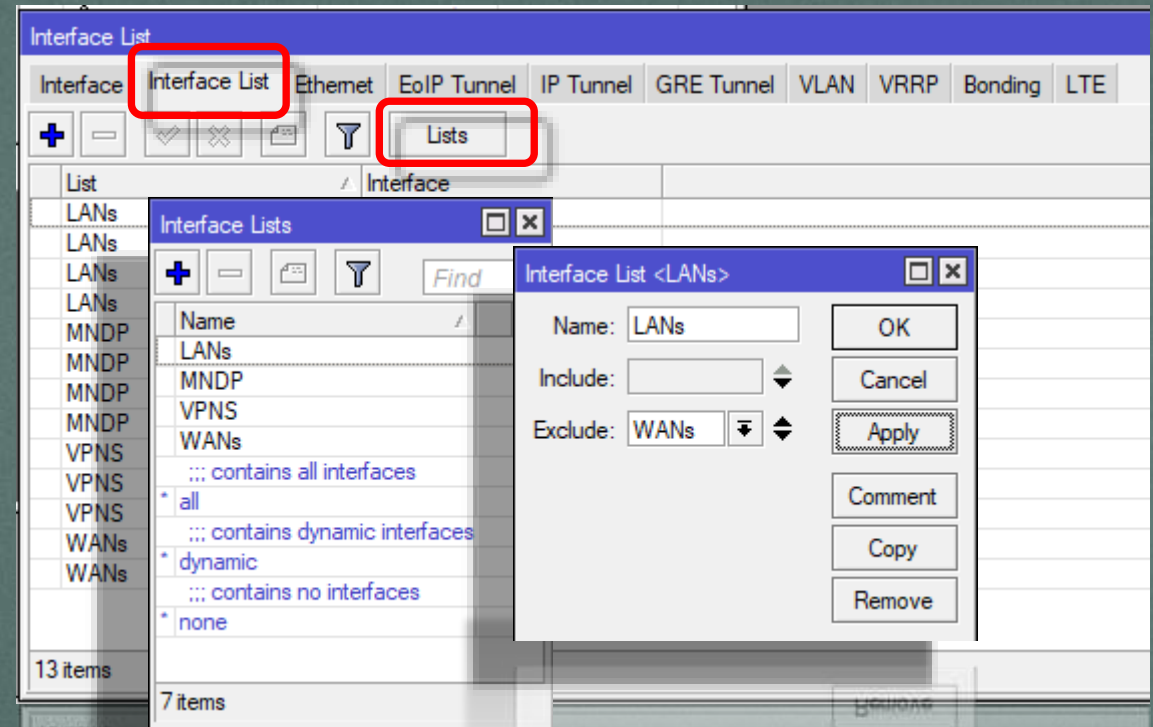
Descartar IPs según la RFC1918 conforme al área

0.0.0.0/8	"Esta" red	192.0.2.0/24	TEST-NET-1
10.0.0.0/8	Uso privado	192.168.0.0/16	Uso privado
100.64.0.0/10	NAT de clase Carrier	198.18.0.0/15	Prueba de Interconexión
127.0.0.0/8	Loopback	198.51.100.0/24	TEST-NET-2
127.0.53.53	Ocurrencia de Colisión de Nombre	203.0.113.0/24	TEST-NET-3
169.254.0.0/16	Link local	224.0.0.0/4	Multicast
172.16.0.0/12	Uso privado	240.0.0.0/4	Reservada para uso futuro
192.0.0.0/24	Asignación de Protocolos IETF	255.255.255.255/32	Broadcast Limitado

ALGUNAS FORMAS DE MITIGACIÓN

Implementar Interface Lists

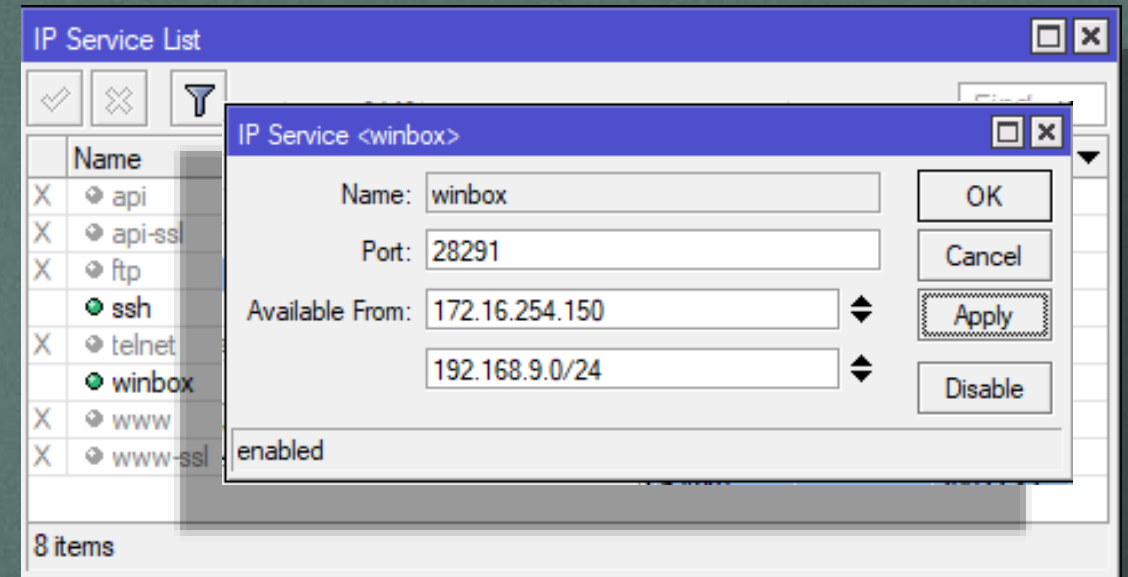
- Al igual que las listas de direcciones son contenedores
- Se pueden usar para mitigar ataques MNDP/CDP/LLDP
- Simplifican reglas de firewall



ALGUNAS FORMAS DE MITIGACIÓN

Desactivar servicios no usados

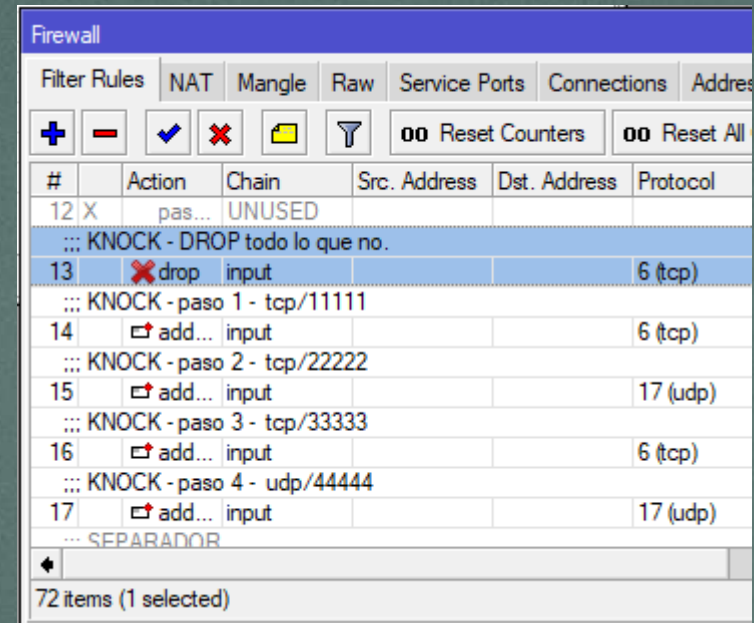
- RouterOS brinda varios métodos para conectarse a el entre ellos Winbox, SSH, Telnet, www, ftp
- Deshabilite los servicios no utilizados para reducir los puntos de entrada de ataques.



ALGUNAS FORMAS DE MITIGACIÓN

Implementar Port Knocking de servicios sensibles

- Contactar un puerto(s) con un paquete especial
- Si se cumple la secuencia se habilita otro puerto
- Ejemplo
 - Si toco puerto tcp/2222
 - Si toco puerto udp/4444
 - Abre puerto tcp/8291 (Winbox)



The screenshot shows the Mikrotik WinBox Firewall Filter Rules configuration. The 'Filter Rules' tab is selected. The table lists several rules for a Port Knocking sequence. Rule 12 is 'pas...' and is 'UNUSED'. Rule 13 is 'KNOCK - DROP todo lo que no.' with action 'drop' and protocol '6 (tcp)'. Rules 14 through 17 are 'KNOCK - paso 1' through 'KNOCK - paso 4' with actions 'add...' and protocols '6 (tcp)', '17 (udp)', '6 (tcp)', and '17 (udp)' respectively. A 'SEPARADOR' rule follows. The bottom status bar indicates '72 items (1 selected)'.

#	Action	Chain	Src. Address	Dst. Address	Protocol
12	pas...	UNUSED			
...	KNOCK - DROP todo lo que no.				
13	drop	input			6 (tcp)
...	KNOCK - paso 1 - tcp/11111				
14	add...	input			6 (tcp)
...	KNOCK - paso 2 - tcp/22222				
15	add...	input			17 (udp)
...	KNOCK - paso 3 - tcp/33333				
16	add...	input			6 (tcp)
...	KNOCK - paso 4 - udp/44444				
17	add...	input			17 (udp)
...	SEPARADOR				

CURSO DE SEGURIDAD MIKROTIK

- El curso sobre seguridad basado en Mikrotik RouterOS
- Por primera vez en Colombia.
- Precio especial solo en el MUM
- Inscripciones Abiertas en nuestro stand
- Septiembre



TikAcademy

Somos Más

Primera Edición

El Workbook de
MikroTik RouterOS

GRAN LANZAMIENTO!
VENTAS +57-312-770-4122



David González Herrero es un consultor empujador en las áreas de programación, cableado, configuración de routers y configuración de Ubiquiti. Durante los últimos años ha desempeñado como responsable de la construcción de redes de acceso para varias plataformas internacionales. En 2016 fundó la academia de formación TikAcademy con la intención de brindar cursos de certificación en manejo e implementación de dispositivos Mikrotik en todo el territorio colombiano y el extranjero. Producto de su experiencia como instructor y conferencista, ha diseñado este material con el fin de compartir su conocimiento y responder a la constante necesidad de capacitación de todos los interesados en el manejo e implementación de dispositivos destinados a la intercomunicación y tráfico de datos.

MikroTik

Autor: David González Herrero (TR0384)
TikAcademy - MikroTik Colombia
www.tikacademy.com

RECUERDEN:

- HAY QUE LEER,
COMPRENDER
- HACER BACKUPS



Scan me



- CHARLEMOS EN NUESTRO STAND
- SOMOS TIKACADEMY, SOMOS MÁS!



+57-312-770-4122



WWW.TIKACADEMY.COM

GRACIAS!