
Microsoft
Microsoft
Windows 95

Mikrotik Security

Amenazas comunes

Por David gonzalez herrera
www.tikacademy.com

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 seres100% 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 206
- 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
- Deseño 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

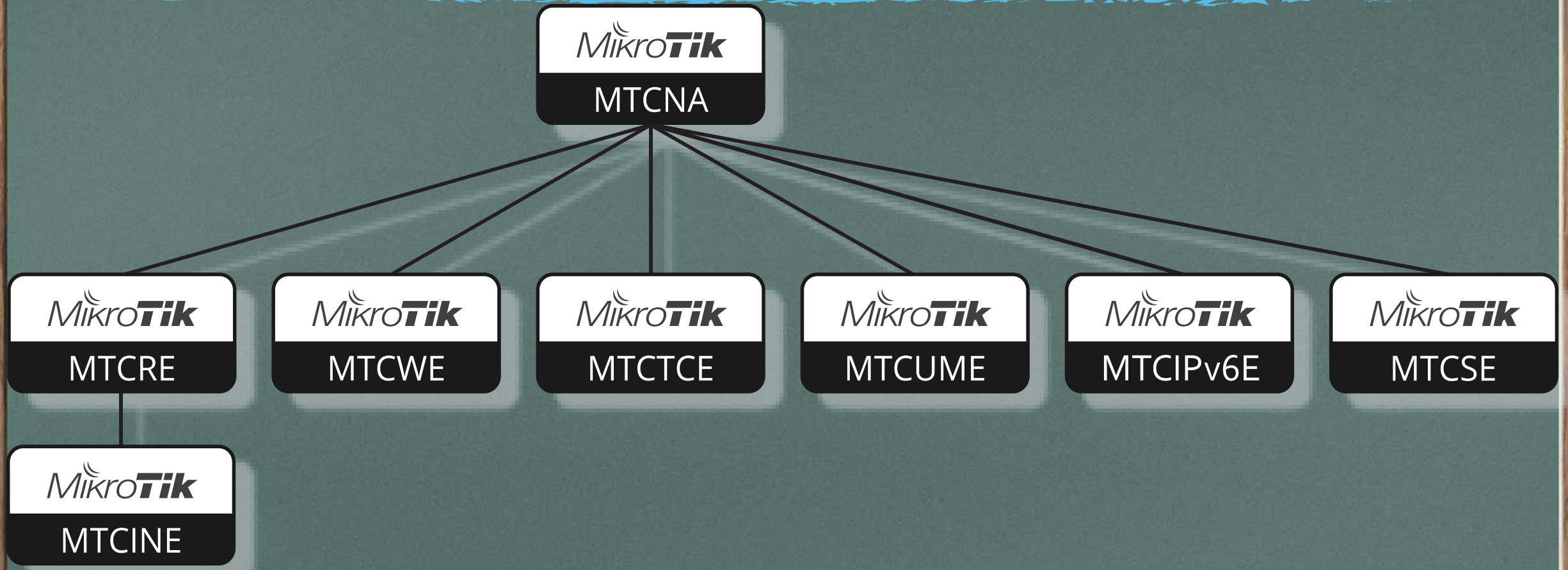
El Workbook de MikroTik RouterOS

David González Herrera [illegible] implementador em[illegible]o en las áreas de programación, cabl[illegible]rado [illegible]nacional certificado de Ubiquiti, Mikrotik, durante los últ[illegible] desempeñado como [illegible] instructor de [illegible] para varias plataformas [illegible]nacional. [illegible] 2016 [illegible] la academia de formación TikAcademy con la [illegible] ofrecer [illegible] cursos de certificación en manejo e implementación [illegible] Mikrotik y Ubiquiti 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 Herrera (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

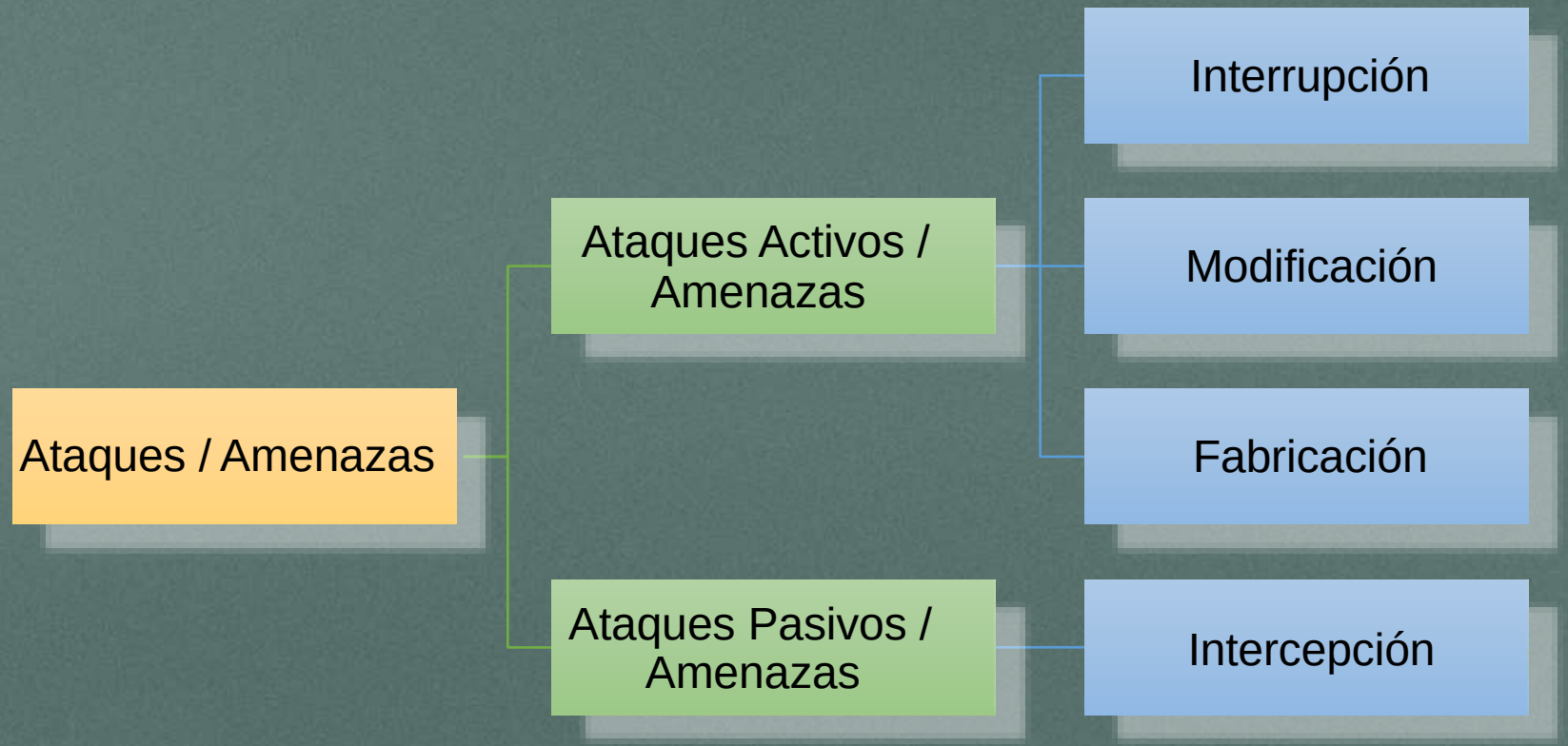
- Hacking
- Ingeniería Social
- DDoS
- Virus
- Ransomware
- Troyanos
- Malware
- Phishing
- Spoofing
- Spam
- Spyware
- Gusanos
- Botnets

¿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

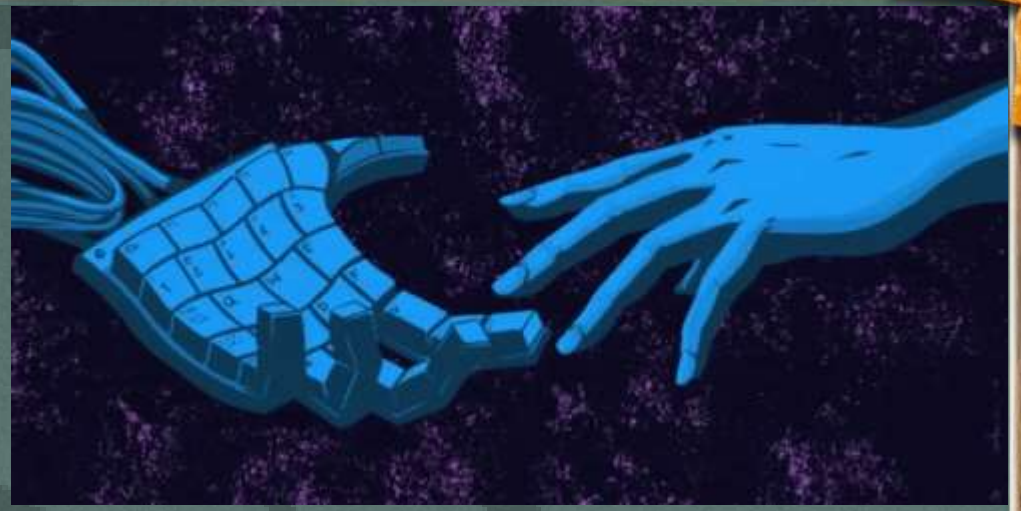
¿Qué es una amenaza de seguridad?



¿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

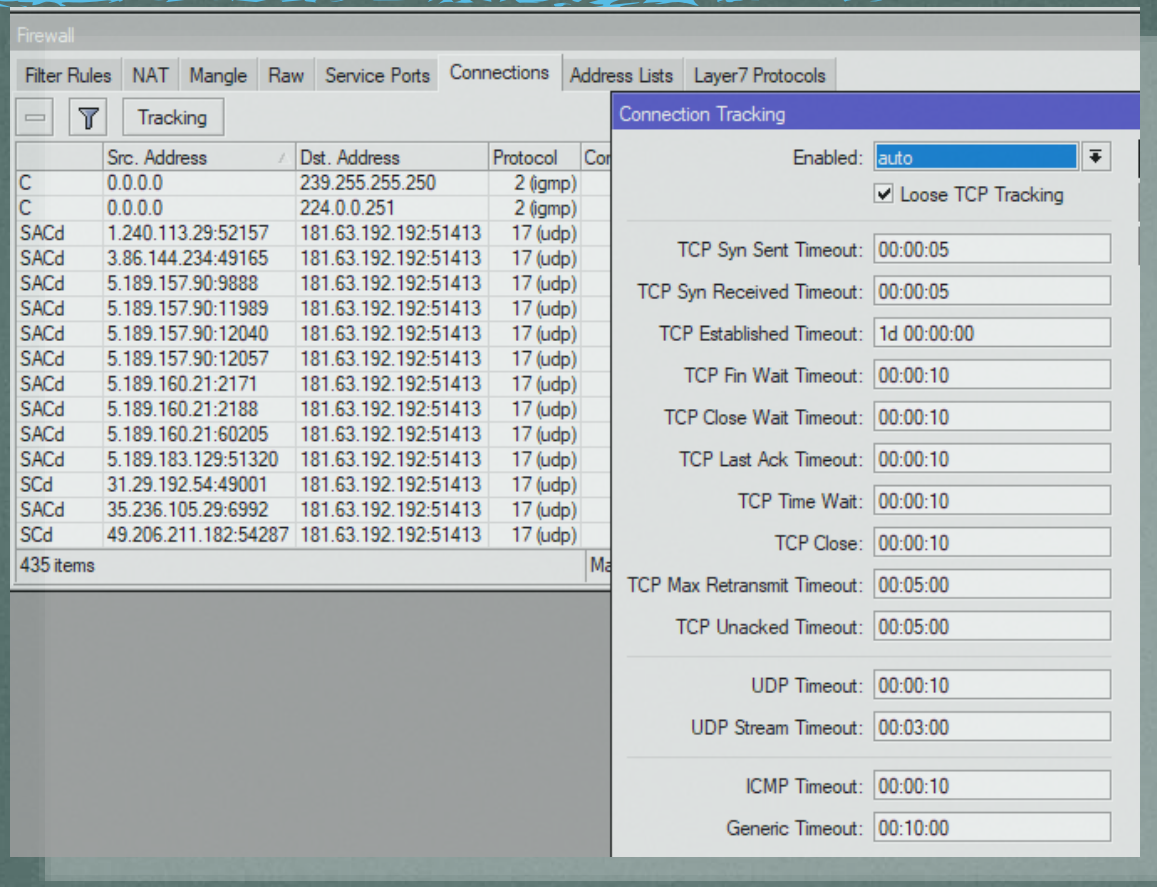
firewall en RouterOS

- 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 en RouterOS

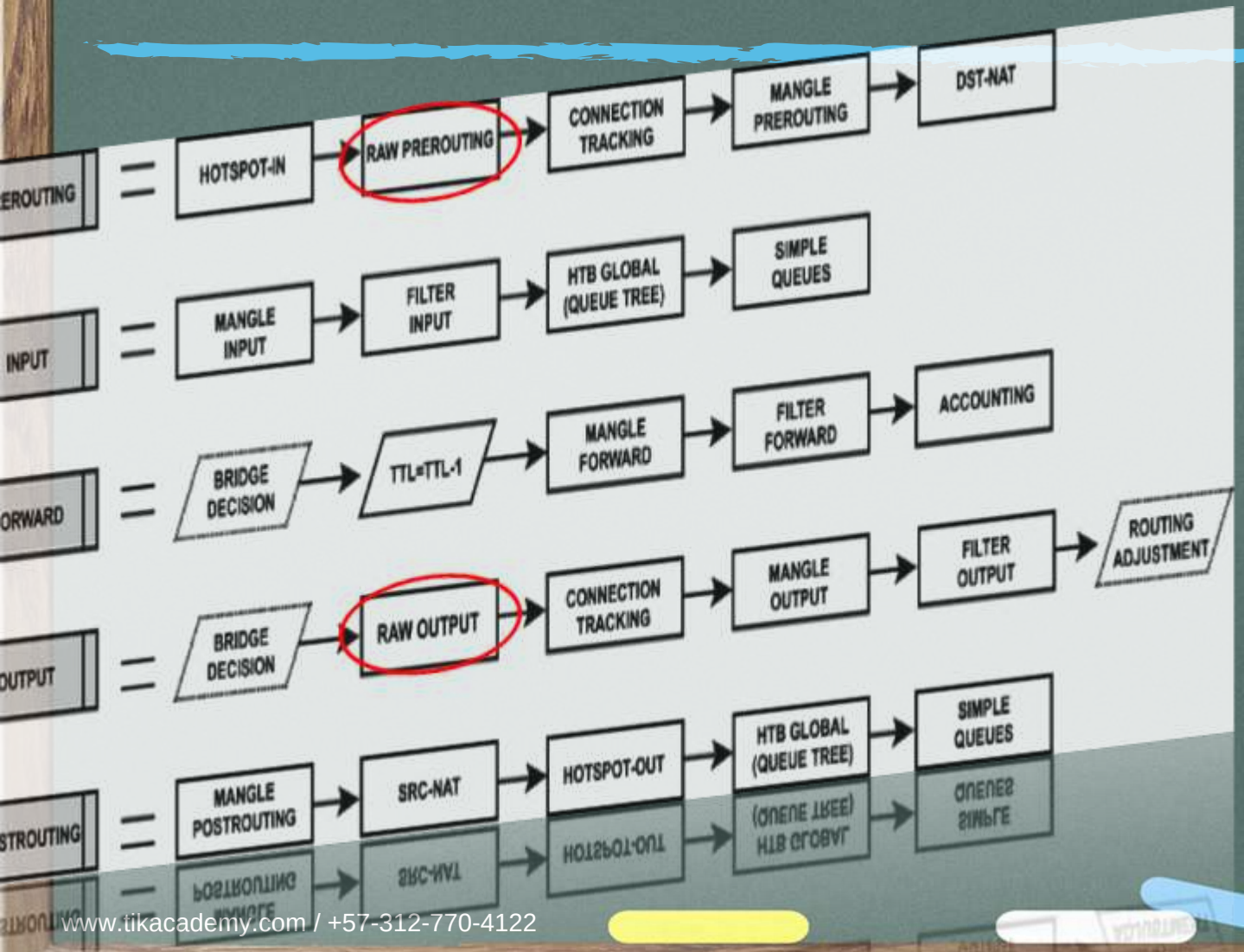


TABLA RAW

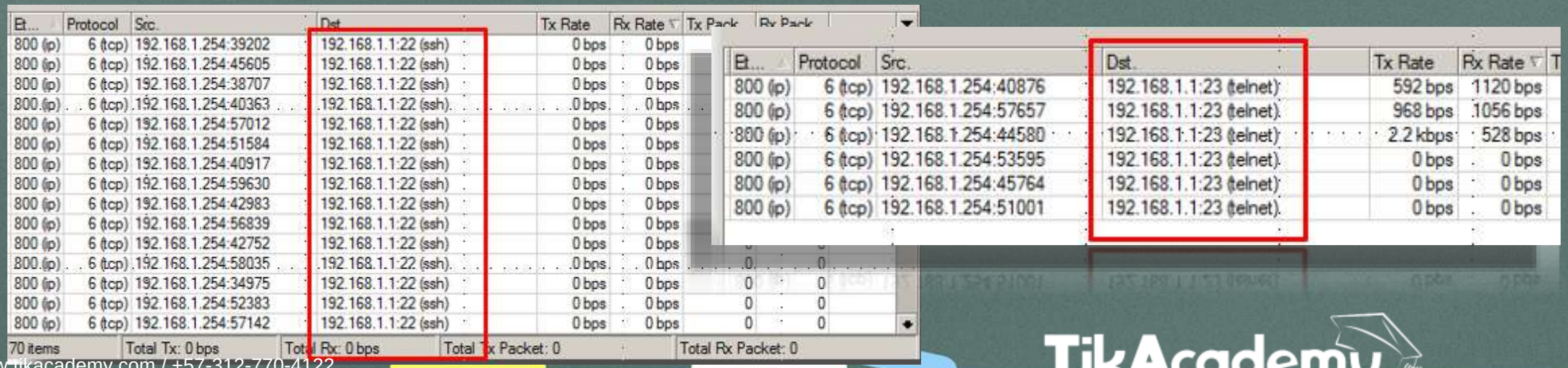
- Solo en Prerouting y Output
- Evita Connection Tracking
- Reduce consumo de CPU

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



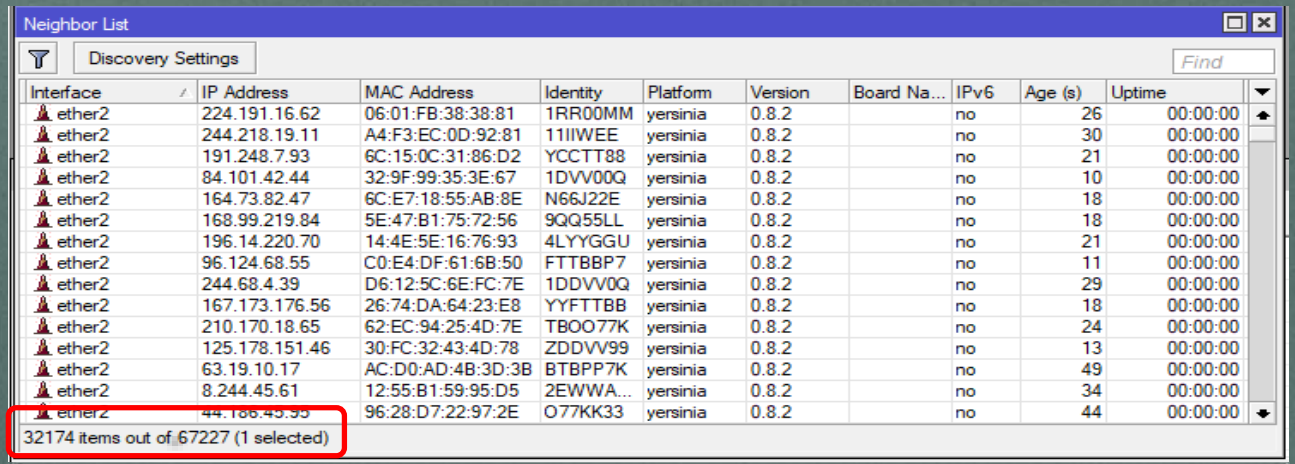
Et...	Protocol	Src.	Dst.	Tx Rate	Rx Rate
800 (ip)	6 (tcp)	192.168.1.254:40876	192.168.1.1:23 (telnet)	592 bps	1120 bps
800 (ip)	6 (tcp)	192.168.1.254:57657	192.168.1.1:23 (telnet)	968 bps	1056 bps
800 (ip)	6 (tcp)	192.168.1.254:44580	192.168.1.1:23 (telnet)	2.2 kbps	528 bps
800 (ip)	6 (tcp)	192.168.1.254:53595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

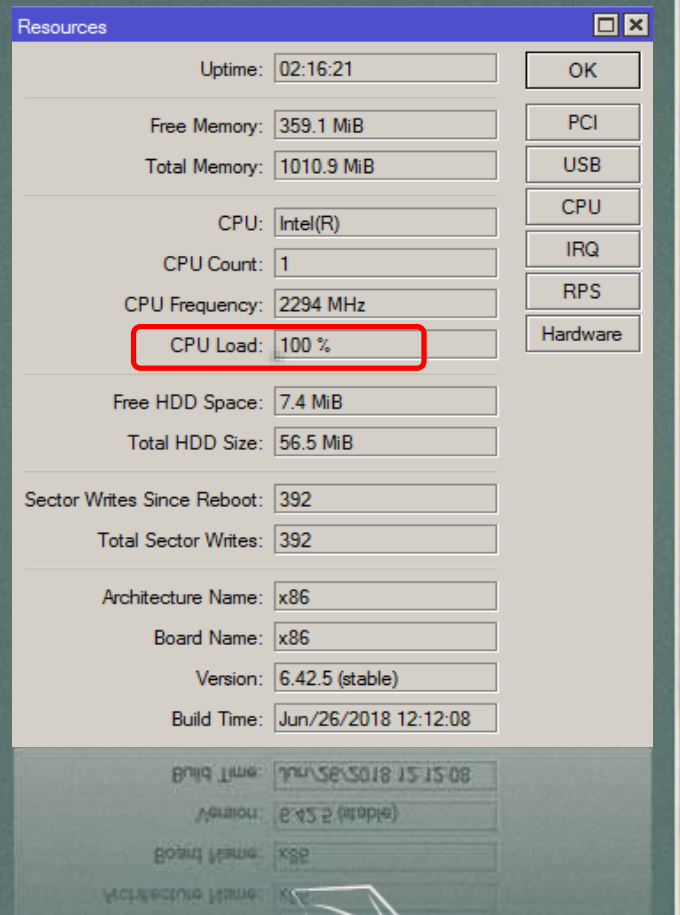
Et...	Protocol	Src.	Dst.	Tx Rate	Rx Rate
800 (ip)	6 (tcp)	192.168.1.254:39202	192.168.1.1:22 (ssh)	0 bps	0 bps
800 (ip)	6 (tcp)	192.168.1.254:45605	192.168.1.1:22 (ssh)	0 bps	0 bps
800 (ip)	6 (tcp)	192.168.1.254:38707	192.168.1.1:22 (ssh)	0 bps	0 bps
800 (ip)	6 (tcp)	192.168.1.254:40363	192.168.1.1:22 (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

70 items | Total Tx: 0 bps | Total Rx: 0 bps | Total Tx Packet: 0 | Total Rx Packet: 0

Ataques a MikroTik RouterOS

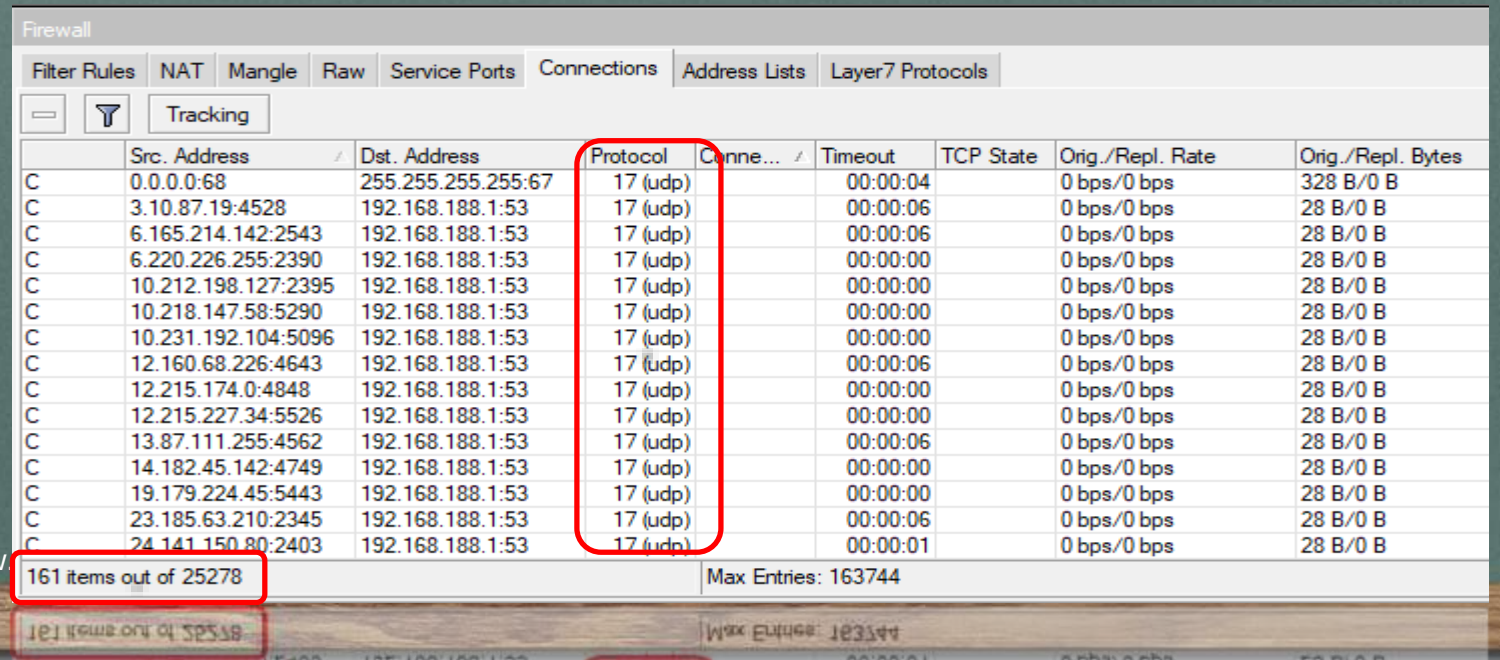
- Inundación MNDP
  - Utiliza el puerto UDP 5678
  - Saturar el dispositivo con anuncios de vecinos falsos
  - Consume recursos hasta hacer reiniciar el dispositivoW

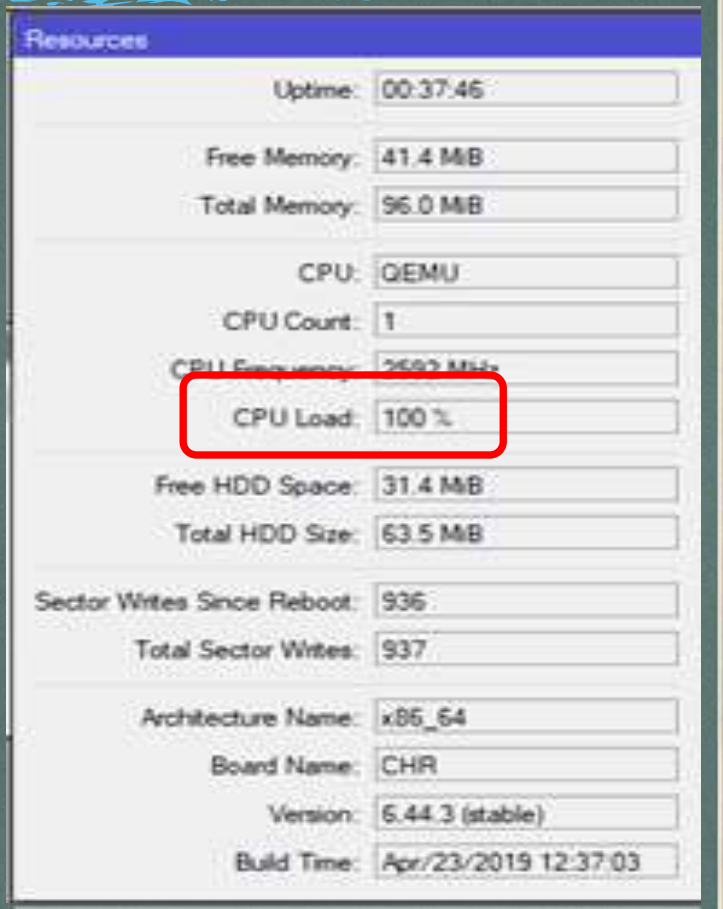




Ataques a MikroTik RouterOS

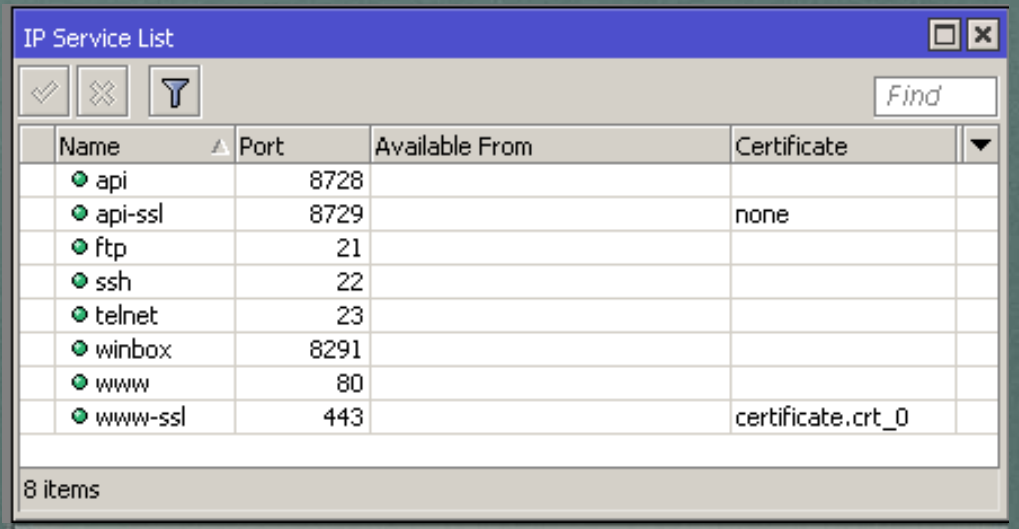
- Ataque de Inundación UDP
  - Colapsar ya sea la red o el dispositivo enviando datagramas UDP
  - No explota ninguna vulnerabilidad
  - Se usa con frecuencia para ataques DNS DDoS





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

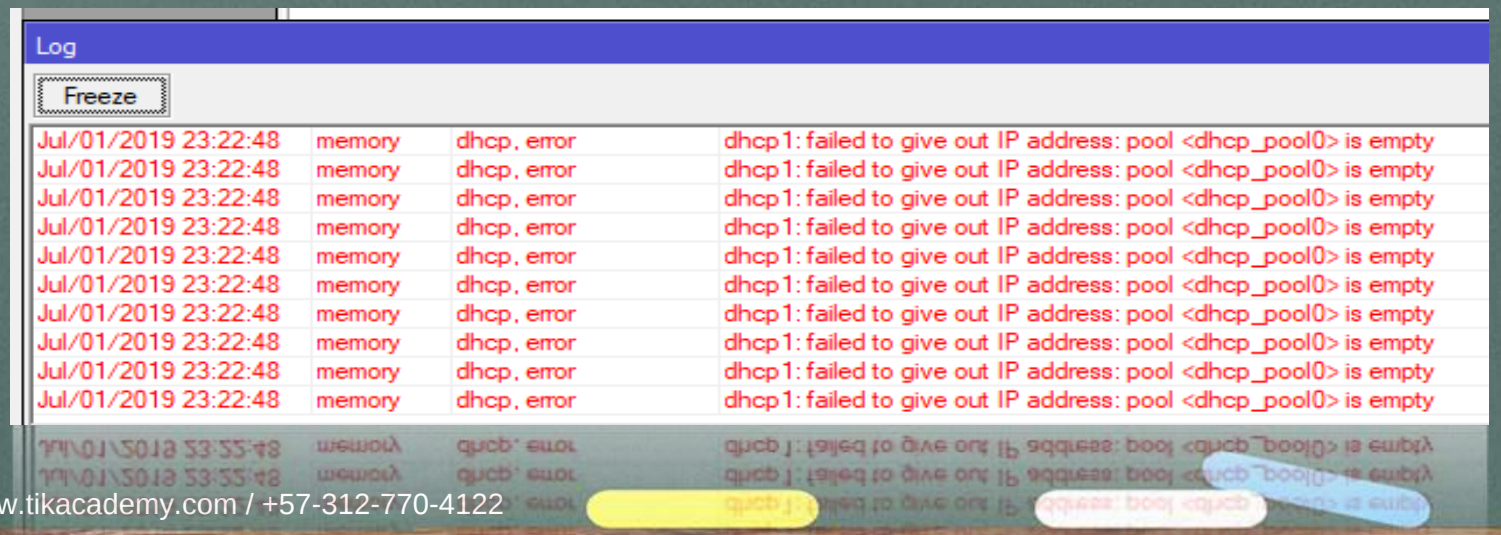


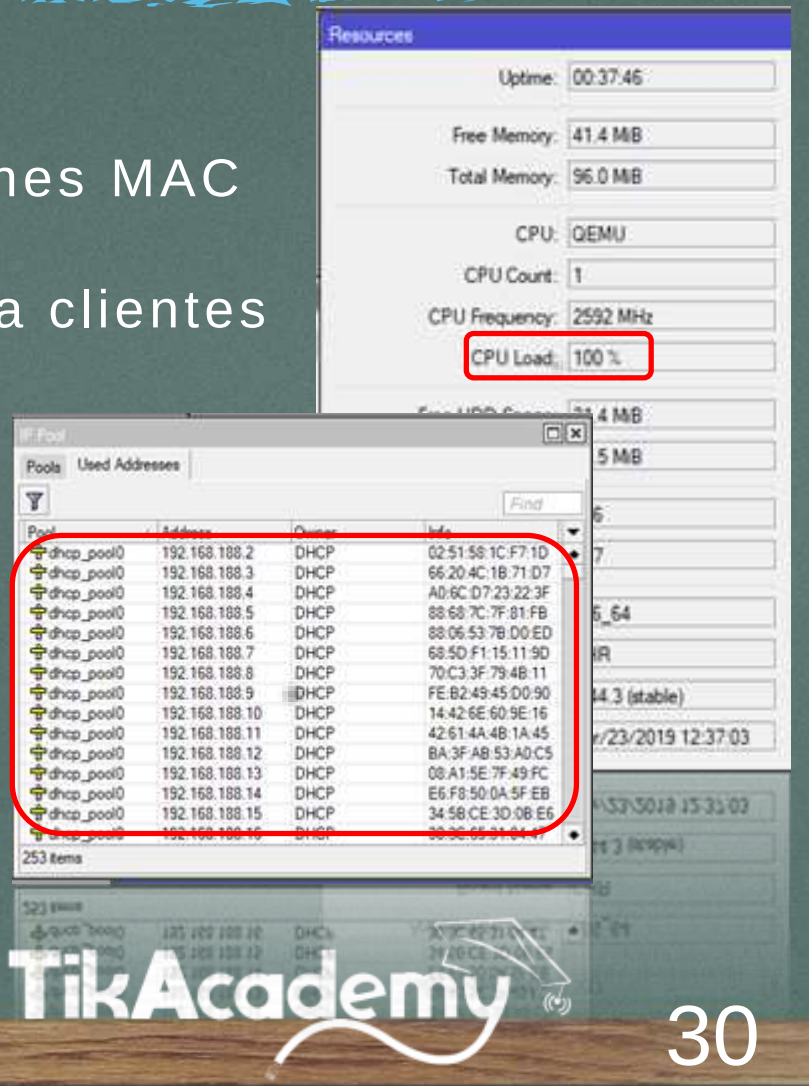

```
root@kali:~# nmap 192.168.188.1
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-03 18:45
Nmap scan report for 192.168.188.1
Host is up (0.00063s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
80/tcp   open  http
443/tcp  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

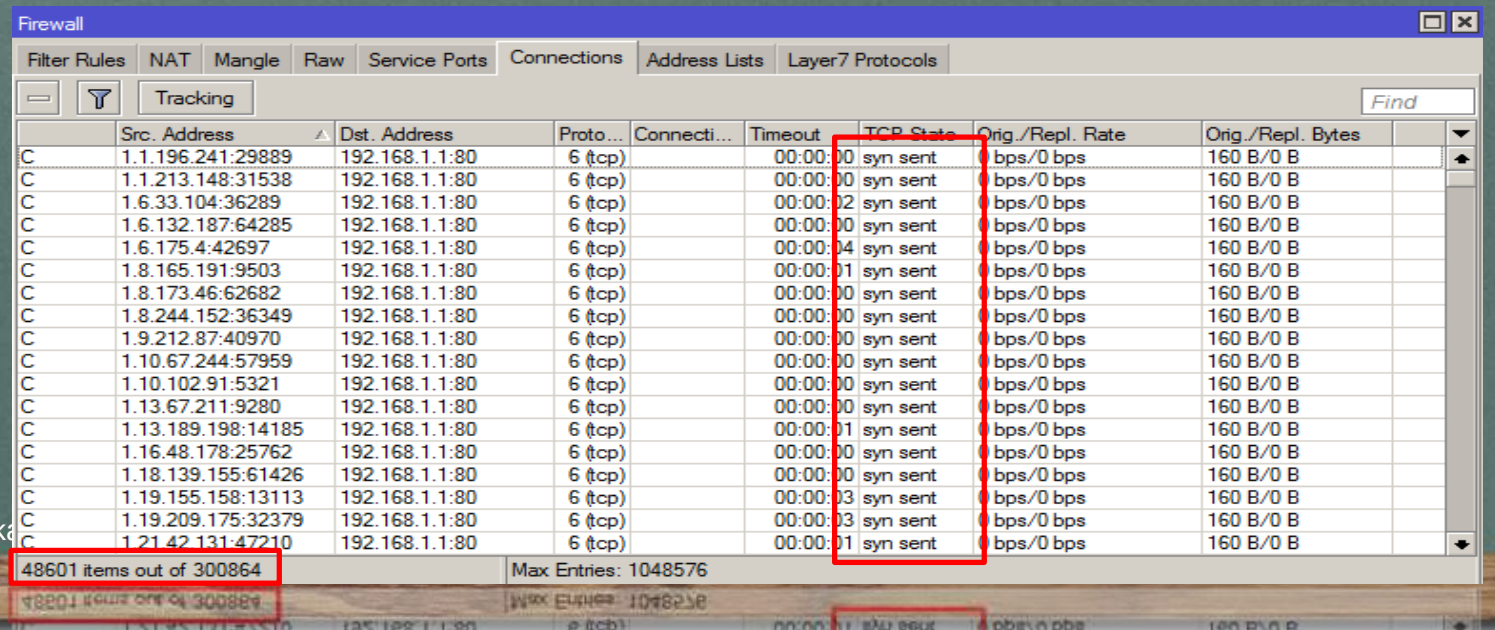
- DHCP Starvation (Inanición DHCP)
  - Difunde peticiones DHCPREQUEST con direcciones MAC falsificadas.
  - Agota las IP disponibles impidiendo la conexión a clientes lícitos.
  - Consume recursos como memoria y CPU

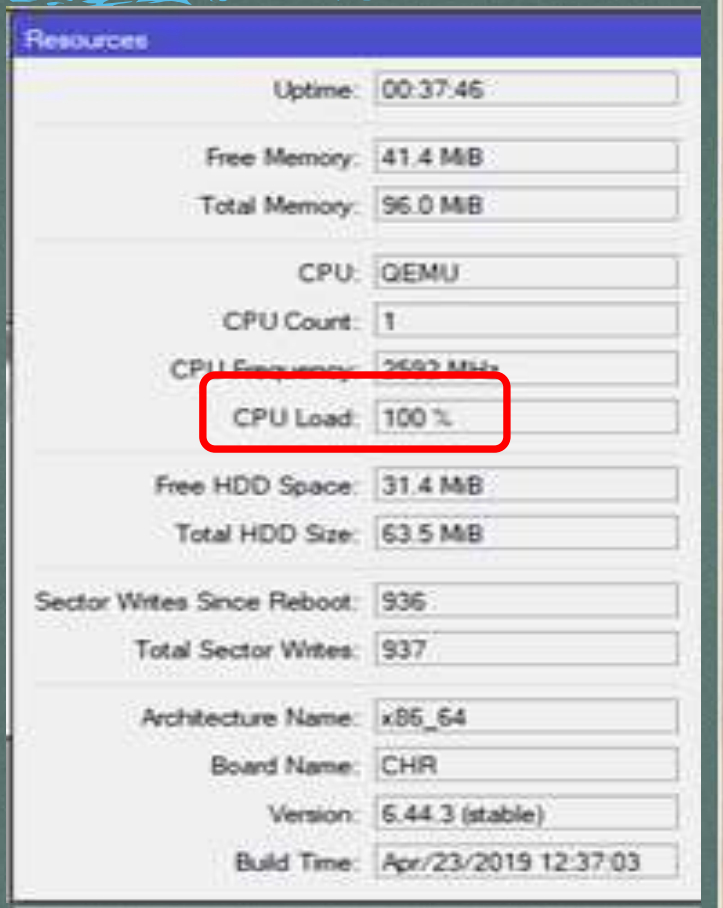




Ataques a MikroTik RouterOS

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





Algunas formas de mitigación

¿Sabía sobre ellos?

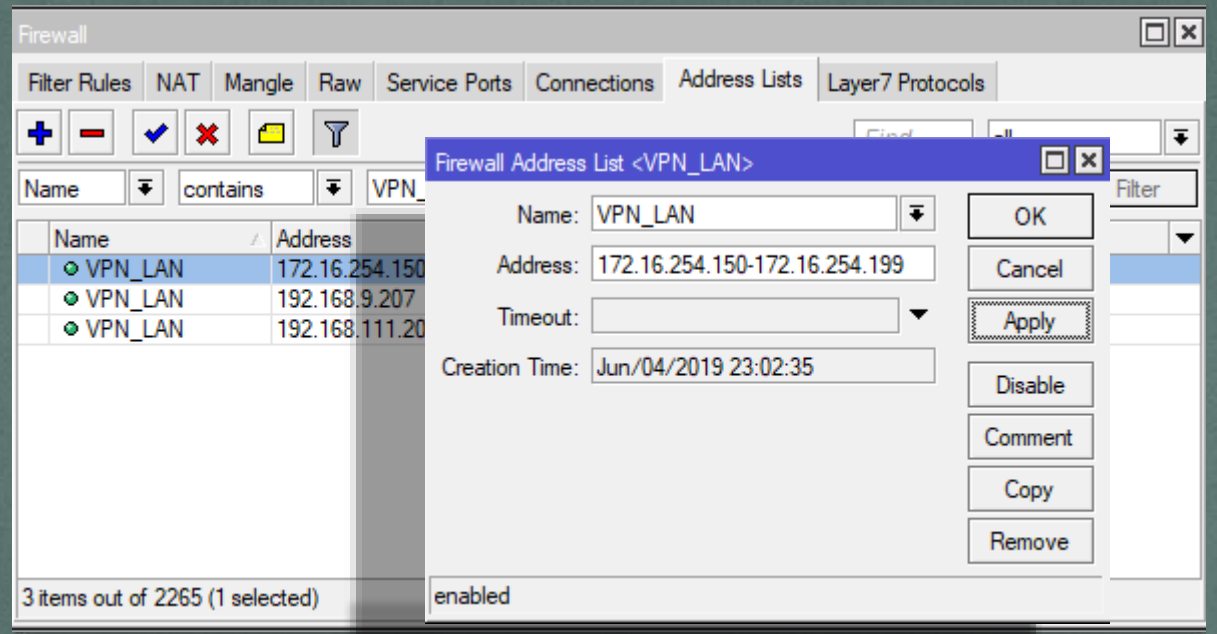
ALGUNAS FORMAS DE MITIGACIÓN

- 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

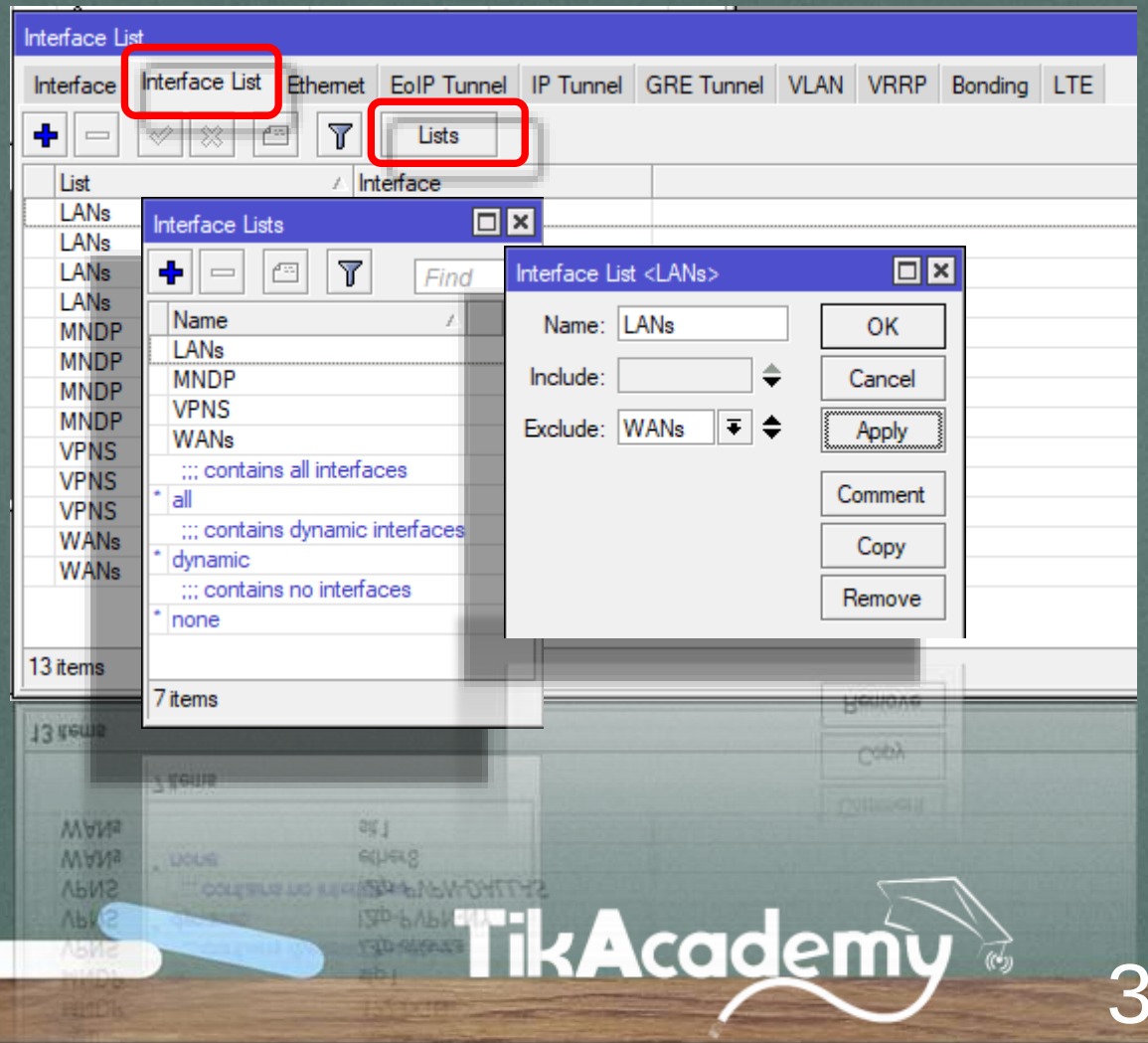
Descartar IPs según la RFC1918 conforme al área

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

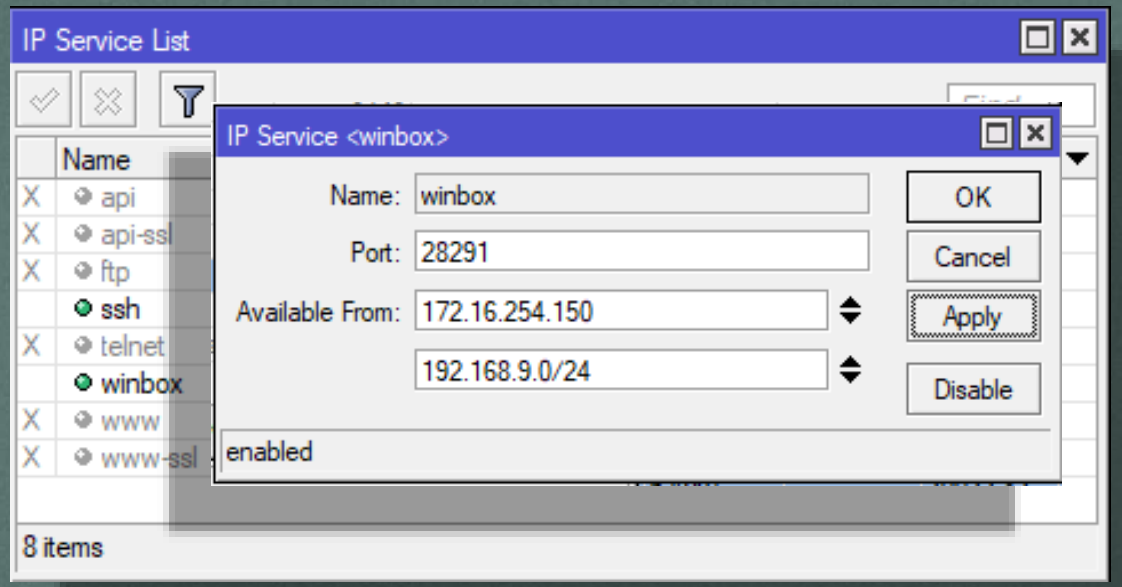
- Al igual que las listas de direcciones son contenedores
- Se pueden usar para mitigar ataques MNDP/CDP/LLDP
- Simplifican reglas de firewall



ALGUNAS FORMAS DE MITIGACIÓN

Desactivar servicios no usados

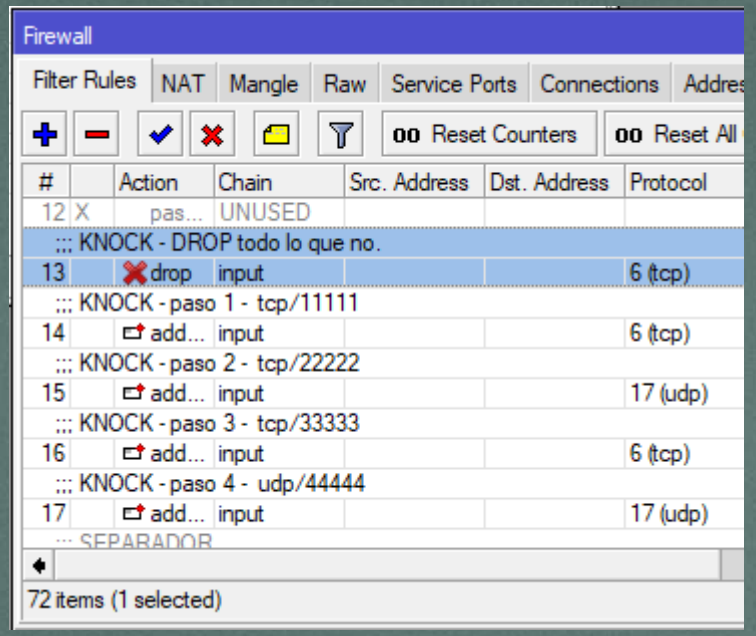
- RouterOS brinda varios métodos para conectarse a el entre ellos Winbox, SSH, Telnet, www, ftp
- Deshabilite los servicios no utilizados para reducir los puntos de entrada de ataques.



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)



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

David González Herrera [illegible] implementador em[illegible]o en las áreas de programación, cabl[illegible]rado [illegible]nacional certificado de Ubiquiti, Mikrotik, durante los últ[illegible] desempeñado como [illegible] instructor de [illegible] para varias plataformas [illegible]nacional. [illegible] 2016 [illegible] la academia de formación TikAcademy con la [illegible] ofrecer [illegible] cursos de certificación en manejo e implementación [illegible] Mikrotik y Ubiquiti 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 Herrera (TR0384)
TikAcademy - MikroTik Colombia
www.tikacademy.com

RECUERDEN:

- HAY QUE LEER,
COMPRENDER
- HACER BACKUPS

Scan me

TikAcademy
Somos Más

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

+57-312-770-4122

WWW.TIKACADEMY.COM

GRACIAS!