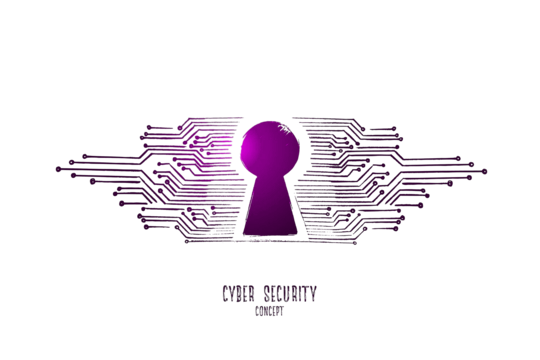
Bastionado de redes 

y sistemas.



**U2\_A9 Fuerza Bruta y Port Knocking Requisitos de finalización**

**Francisco Iván Ramírez Ortega**

**Javier Díaz Machado**

Curso 2023 - 2024

**IES El Rincón**

Curso de especialización en Ciberseguridad en entornos de las tecnologías de la información.

# Fuerza Bruta y Port Knocking Requisitos de finalización

# Introducción

MikroTik es una empresa que desarrolla hardware y software para redes de datos. Su producto más conocido es **RouterOS**, un sistema operativo de enrutamiento que convierte un PC estándar en un enrutador dedicado con todas las funciones. Además de RouterOS, MikroTik también fabrica hardware específico para routers, como routers, switches y dispositivos inalámbricos.

RouterOS, el sistema operativo de MikroTik, es extremadamente versátil y se utiliza en una amplia gama de aplicaciones, incluyendo:

1. **Enrutamiento de red**: RouterOS se utiliza para enrutar el tráfico entre redes, ya sea en redes domésticas, empresariales o de proveedores de servicios de Internet (ISP).
2. **Firewall y seguridad**: RouterOS incluye características de firewall avanzadas que permiten a los administradores de red controlar y asegurar el tráfico que pasa a través del enrutador.
3. **Conectividad inalámbrica**: MikroTik fabrica una variedad de dispositivos inalámbricos, como puntos de acceso Wi-Fi y radios para enlaces punto a punto y punto a multipunto. Estos dispositivos son comúnmente utilizados para proporcionar conectividad inalámbrica en redes empresariales, ISP y proyectos de telecomunicaciones.
4. **Administración de ancho de banda**: RouterOS incluye características de administración de ancho de banda que permiten a los administradores de red controlar y limitar el ancho de banda utilizado por diferentes tipos de tráfico.
5. **Redes privadas virtuales (VPN)**: RouterOS es compatible con una variedad de protocolos VPN, lo que permite a los usuarios crear redes privadas virtuales seguras sobre Internet pública.
6. **Hotspot y gestión de acceso**: RouterOS incluye funciones de hotspot que permiten a los proveedores de servicios de Internet ofrecer acceso a Internet de pago o gratuito a través de redes Wi-Fi públicas.

**Winbox** es una aplicación de software con interfaz gráfica que se utiliza para administrar dispositivos MikroTik.

# Objetivo

1. 1. Añadir las reglas de port Knocking en el firewall de mikrotik y probar el acceso por ssh al router
2. <https://help.mikrotik.com/docs/display/ROS/Port+knocking>
3. 2. General los paquetes necesarios para prever al menos un caso de prevención por fuerza bruta
4. <https://help.mikrotik.com/docs/display/ROS/Bruteforce+prevention>
5. Subir el informe con las correspondientes demostraciones

| Herramientas |
| --- |
| * [Winbox](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwirxe3u-aiEAxUT_rsIHVIECPcQFnoECAkQAQ&url=https%3A%2F%2Fmikrotik.com%2Fdownload&usg=AOvVaw2JCoTY2tqWuPue5n6W40Ts&opi=89978449) (snap install winbox) |
|  |

**ÍNDICE**

[**Fuerza Bruta y Port Knocking Requisitos de finalización 2**](#_xfpg6pduf6p7)

[**Introducción 2**](#_b9oaw39qdr1r)

[**Objetivo 3**](#_3uoprqr5rx0x)

[**Herramientas 3**](#_wzp689uhopv7)

[**Bibliografía 5**](#_fxv8jhomw7i7)

| Practica |
| --- |
| Listar servicios |
| ip/firewall print o nmap |
|  |
|  |
|  |
| Configuración de port knocking |
| # mar/07/2024 14:48:24 by RouterOS 6.48.6  # software id = RKJI-MH9J  #  # model = RB750Gr3  # serial number = HCY08F2T22W  /interface bridge  add admin-mac=18:FD:74:72:88:EC auto-mac=no comment=defconf name=bridge  add name=bridgeLocal  /interface list  add comment=defconf name=WAN  add comment=defconf name=LAN  /interface wireless security-profiles  set [ find default=yes ] supplicant-identity=MikroTik  /ip pool  add name=default-dhcp ranges=192.168.88.10-192.168.88.254  /ip dhcp-server  add address-pool=default-dhcp disabled=no interface=bridgeLocal name=defconf  /interface bridge port  add bridge=bridgeLocal comment=defconf interface=ether2  add bridge=bridgeLocal comment=defconf interface=ether3  add bridge=bridgeLocal comment=defconf interface=ether4  add bridge=bridgeLocal comment=defconf interface=ether5  /ip neighbor discovery-settings  set discover-interface-list=LAN  /interface list member  add comment=defconf interface=bridgeLocal list=LAN  add comment=defconf interface=ether1 list=WAN  add disabled=yes interface=ether2 list=LAN  /ip address  add address=192.168.88.1/24 comment=defconf interface=bridgeLocal network=\  192.168.88.0  /ip dhcp-client  add comment=defconf disabled=no interface=ether1  add comment=defconf disabled=no interface=bridgeLocal  /ip dhcp-server network  add address=192.168.88.0/24 comment=defconf gateway=192.168.88.1  /ip dns  set allow-remote-requests=yes  /ip dns static  add address=192.168.88.1 comment=defconf name=router.lan  /ip firewall filter  add action=add-src-to-address-list address-list=69 address-list-timeout=30s \  chain=input dst-port=69 in-interface-list=LAN protocol=tcp  add action=add-src-to-address-list address-list=666 address-list-timeout=30s \  chain=input dst-port=666 in-interface-list=LAN protocol=tcp \  src-address-list=69  add action=add-src-to-address-list address-list=secured address-list-timeout=\  30m chain=input dst-port=80 in-interface-list=LAN protocol=tcp \  src-address-list=666  add action=accept chain=input in-interface-list=LAN protocol=icmp \  src-address-list=secured  add action=drop chain=input in-interface-list=LAN protocol=icmp  /ip firewall nat  add action=masquerade chain=srcnat comment="defconf: masquerade" \  ipsec-policy=out,none out-interface-list=WAN  /system clock  set time-zone-name=Europe/Madrid  /system identity  set name=RouterOS  /tool mac-server  set allowed-interface-list=LAN  /tool mac-server mac-winbox  set allowed-interface-list=LAN |
| Pruebas |
| Primero, hacemos ping a la IP de la puerta de enlace:    No nos devuelve ningún resultado, ya que el mikrotik rechazó los paquetes.    Probamos a hacer un nmap (también desde la máquina local) y vemos que también nos lo rechaza.      Ahora, probemos haciendo port knocking. En nuestro caso, lo hicimos desde la conexión del winbox:      Y como podemos ver, tras hacer port knocking, nos deja hacerle ping a la puerta de enlace:    También podemos ver a qué listas se añadió nuestra IP. |
| Configuración del mikrotik |
| Aquí tenemos la configuración del dispositivo:  # mar/08/2024 12:31:02 by RouterOS 6.48.6  # software id = RKJI-MH9J  #  # model = RB750Gr3  # serial number = HCY08F2T22W  /interface bridge  add admin-mac=18:FD:74:72:88:EC auto-mac=no comment=defconf name=bridge  add name=bridgeLocal  /interface list  add comment=defconf name=WAN  add comment=defconf name=LAN  /interface wireless security-profiles  set [ find default=yes ] supplicant-identity=MikroTik  /ip pool  add name=default-dhcp ranges=192.168.88.10-192.168.88.254  /ip dhcp-server  add address-pool=default-dhcp disabled=no interface=bridgeLocal name=defconf  /interface bridge port  add bridge=bridgeLocal comment=defconf interface=ether2  add bridge=bridgeLocal comment=defconf interface=ether3  add bridge=bridgeLocal comment=defconf interface=ether4  add bridge=bridgeLocal comment=defconf interface=ether5  /ip neighbor discovery-settings  set discover-interface-list=LAN  /interface list member  add comment=defconf interface=bridgeLocal list=LAN  add comment=defconf interface=ether1 list=WAN  add disabled=yes interface=ether2 list=LAN  /ip address  add address=192.168.88.1/24 comment=defconf interface=bridgeLocal network=\  192.168.88.0  /ip dhcp-client  add comment=defconf disabled=no interface=ether1  add comment=defconf disabled=no interface=bridgeLocal  /ip dhcp-server network  add address=192.168.88.0/24 comment=defconf gateway=192.168.88.1  /ip dns  set allow-remote-requests=yes  /ip dns static  add address=192.168.88.1 comment=defconf name=router.lan  /ip firewall filter  add action=add-src-to-address-list address-list=69 address-list-timeout=30s \  chain=input dst-port=69 in-interface-list=LAN protocol=tcp  add action=add-src-to-address-list address-list=666 address-list-timeout=30s \  chain=input dst-port=666 in-interface-list=LAN protocol=tcp \  src-address-list=69  add action=add-src-to-address-list address-list=secured address-list-timeout=\  30m chain=input dst-port=80 in-interface-list=LAN protocol=tcp \  src-address-list=666  add action=accept chain=input in-interface-list=LAN protocol=icmp \  src-address-list=secured  add action=drop chain=input in-interface-list=LAN protocol=icmp  /ip firewall nat  add action=masquerade chain=srcnat comment="defconf: masquerade" \  ipsec-policy=out,none out-interface-list=WAN  /system clock  set time-zone-name=Atlantic/Canary  /system identity  set name=RouterOS  /tool mac-server  set allowed-interface-list=LAN  /tool mac-server mac-winbox  set allowed-interface-list=LAN |
|  |
|  |
| Finalmente aceptamos |
|  |
|  |
|  |

| Bibliografía |
| --- |
| C[omandos](https://www.mkesolutions.net/pdf/routeros-cheat-sheet-v1.1.pdf) |
|  |
|  |