RouterOS Güvenliği

MUM İstanbul 2018

Osman Kazdal

Sekuritim Bilişim

MikroTik
ROUTING THE WORLD

Ben Kimim?

Osman Kazdal

- MikroTik Certified Consultant
- MikroTik Certified Trainer
- CISSP
- Sekuritim Kurucusu

Sekuritim Bilişim

- Value Added Master Distributor
- Eğitim Merkezi
- Danışmanlık
- Kurulum
- Destek
- 2008 yılında kurulmuştur.
- Ataşehir İstanbul

MikroTik MASTER DISTRIBUTOR

MikroTik TRAINING CENTER

FlashStart® INTERNET PROTECTION partner

İletişim

- Email: info@sekuritim.com
- Telefon: 0216 302 22 21
- Web: https://sekuritim.com
- Online satış: https://shop.sekuritim.com
- Facebook: https://facebook.com/sekuritim
- Twitter: https://twitter.com/sekuritim
- Reddit: https://www.reddit.com/r/Sekuritim/

Training Center

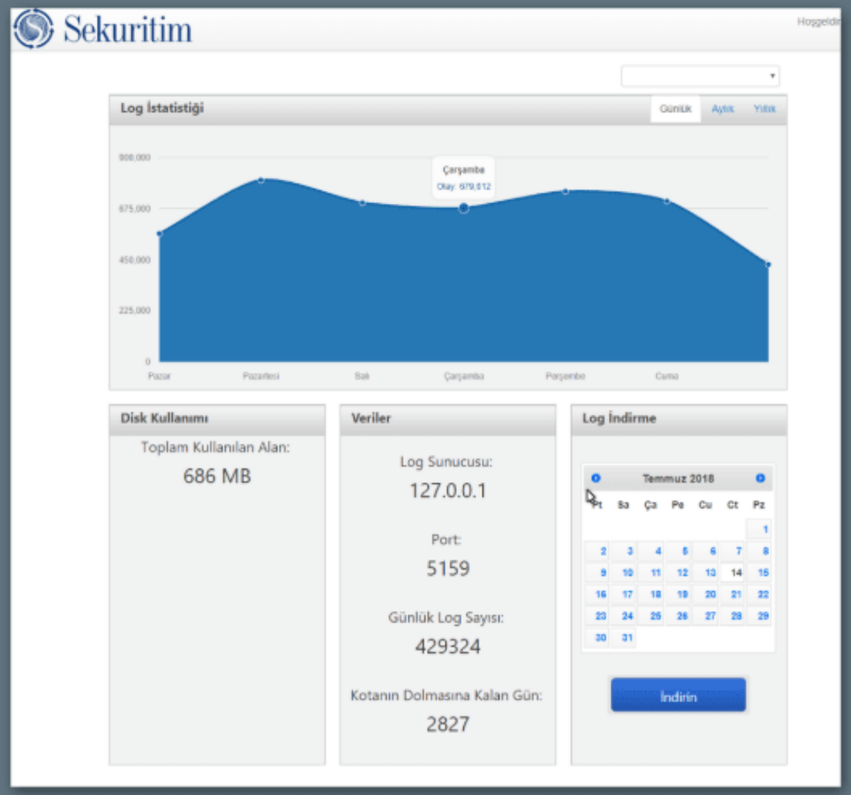
- Tüm MikroTik Sertifikasyon eğitimleri
- Türkiye'nin ilk MikroTik eğitmeni
- İstanbul merkezli, Türkiye'nin her yerinde
- Eğitim programı: https://sekuritim.com/#trainings
- Bilgi için: training@sekuritim.com

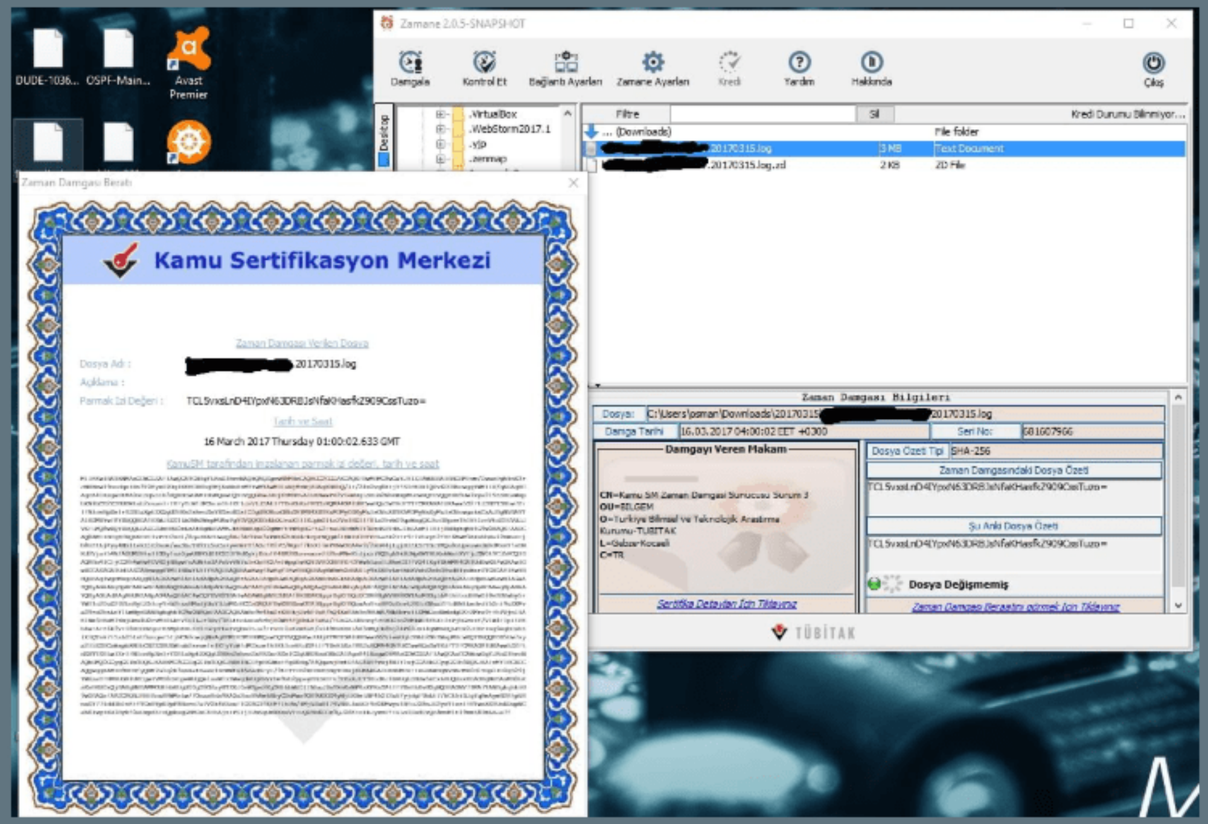
Standımıza Bekliyoruz

LTE Ürünleri

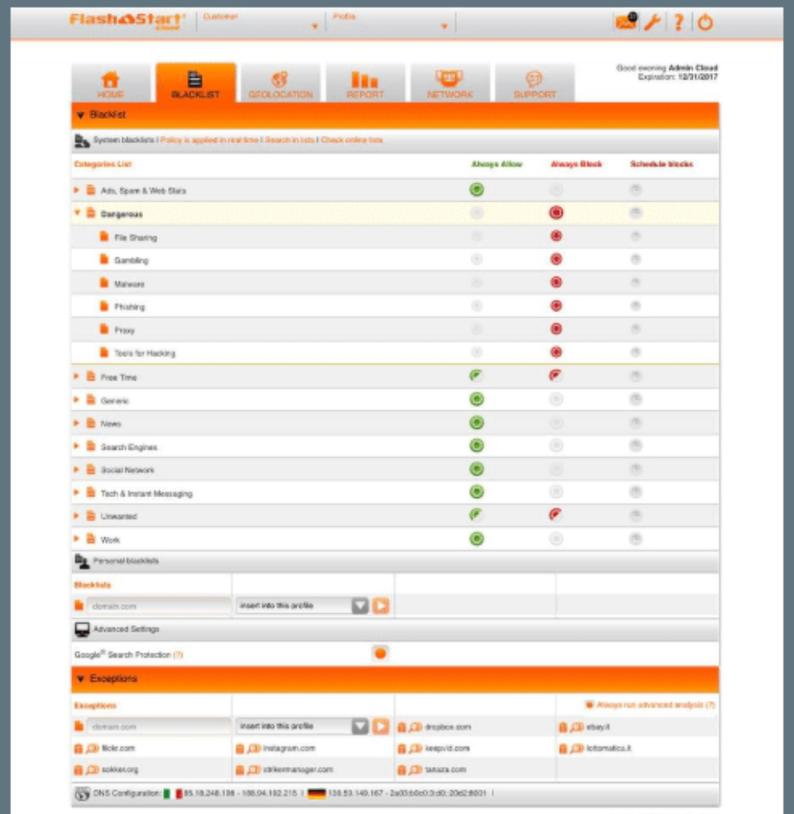
Hotspot Çözümü

5651 Loglama Çözümü





FlashStart İçerik Filtreleme



Referanslarımız

Sony Eurasia
Turkcell Superonline
Vodafone
TEB Yatırım
Panço Giyim
Çayla Restoranları
Çaytaş
Esenyurt Üniversitesi
MyFi
Netspeed
Telekom19

RouterOS Güvenliği

Nasıl saldırıyorlar?
Neden saldırıyorlar?
Kendimizi nasıl koruruz?

Demo

Saldırının Aşamaları

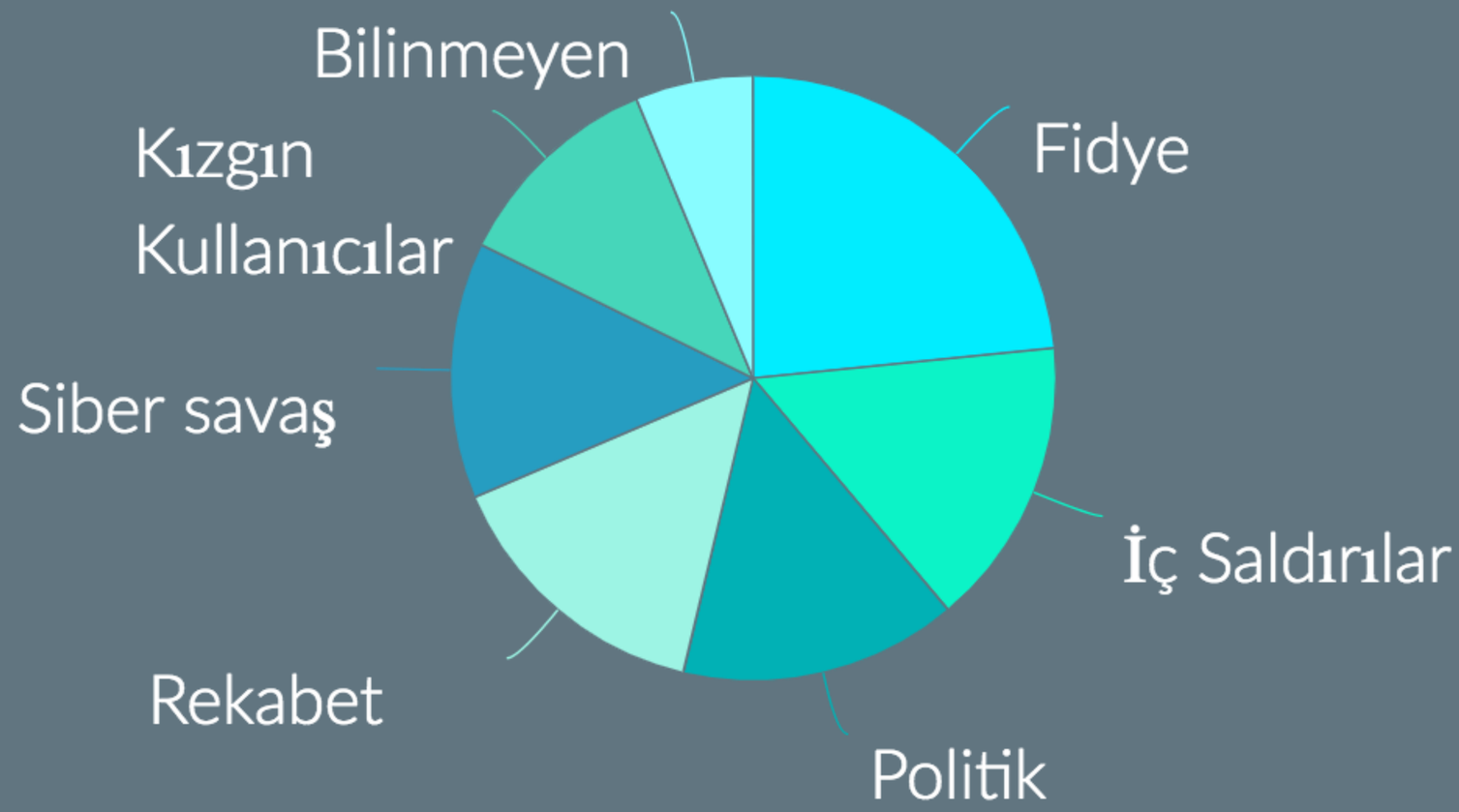
- Port tarama ile MikroTik router tespit edilmesi
- Winbox açığının kullanılarak şifrelerin ele geçirilmesi
- Router'ın ele geçirilmesi

Ne yaptılar?

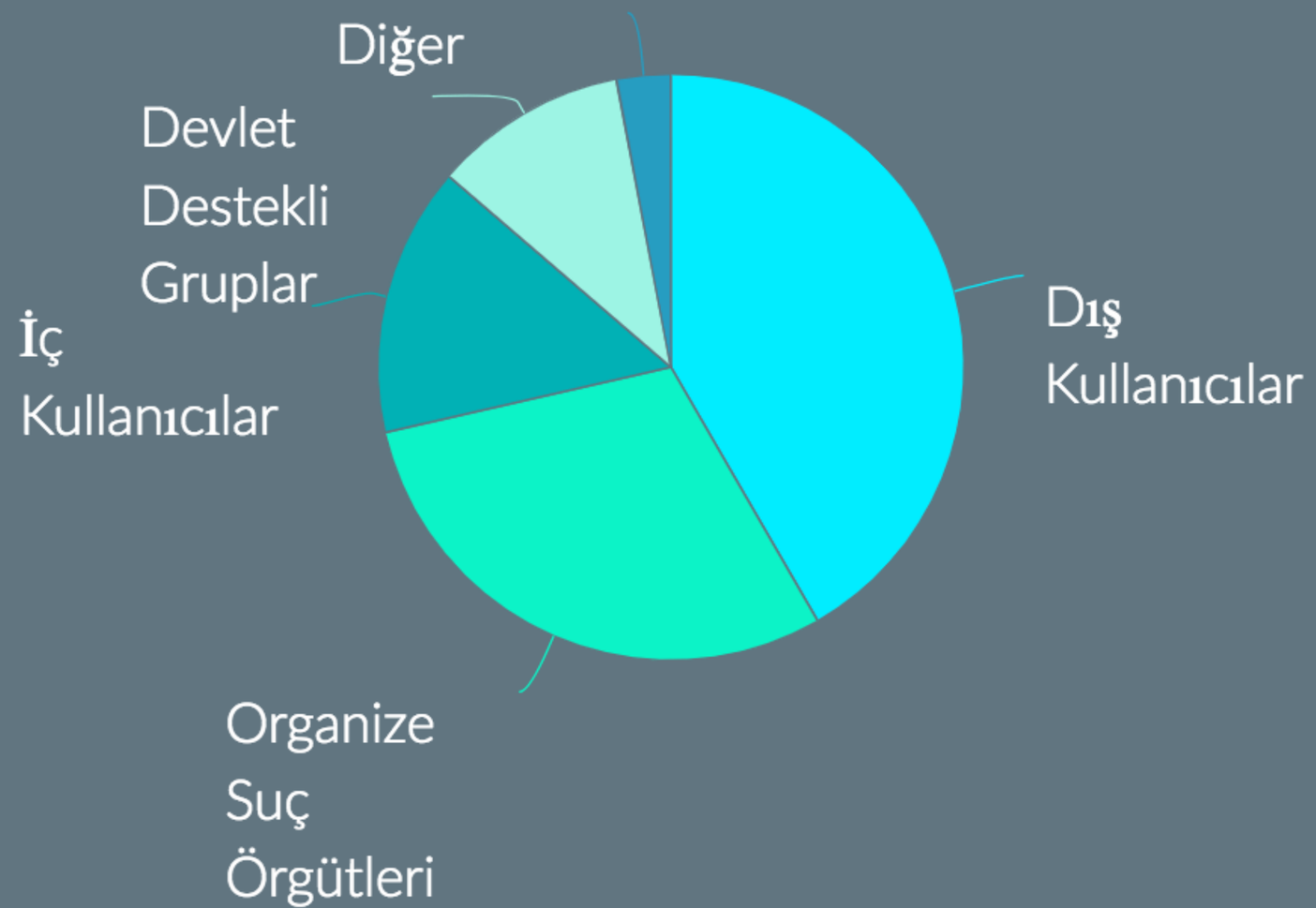
```
/ip firewall filter
add action=tarpit chain=input comment="Add you ip addess to allow-ip in Address Lists." dst-port=30553 protocol=tcp
add action=add-src-to-address-list address-list=allow-ip address-list-timeout=1h chain=input comment="The security flaw for Haj
ime is closed by the firewall." packet-size=1083 protocol=icmp
add action=accept chain=input comment="Please update RotherOS and change password." src-address-list=allow-ip
add action=drop chain=input comment=" Thanks are accepted on WebMoney Z399578297824" dst-port=53 protocol=udp
add action=drop chain=input comment="or BTC 14qiYkk3nUgsdqQawiMLC1bUGDZWHowix1" dst-port=53,8728,8729,21,22,23,80,443,8291 prot
ocol=tcp
add action=passthrough chain=input
/system note
set note="The security flaw for Hajime is closed by the firewall. Please update RotherOS. Gratitude is accepted on WebMoney Z39
9578297824 or BTC 14qiYkk3nUgsdqQawiMLC1bUGDZWHowix1"
```

https://forum.mikrotik.com/viewtopic.php?t=134804

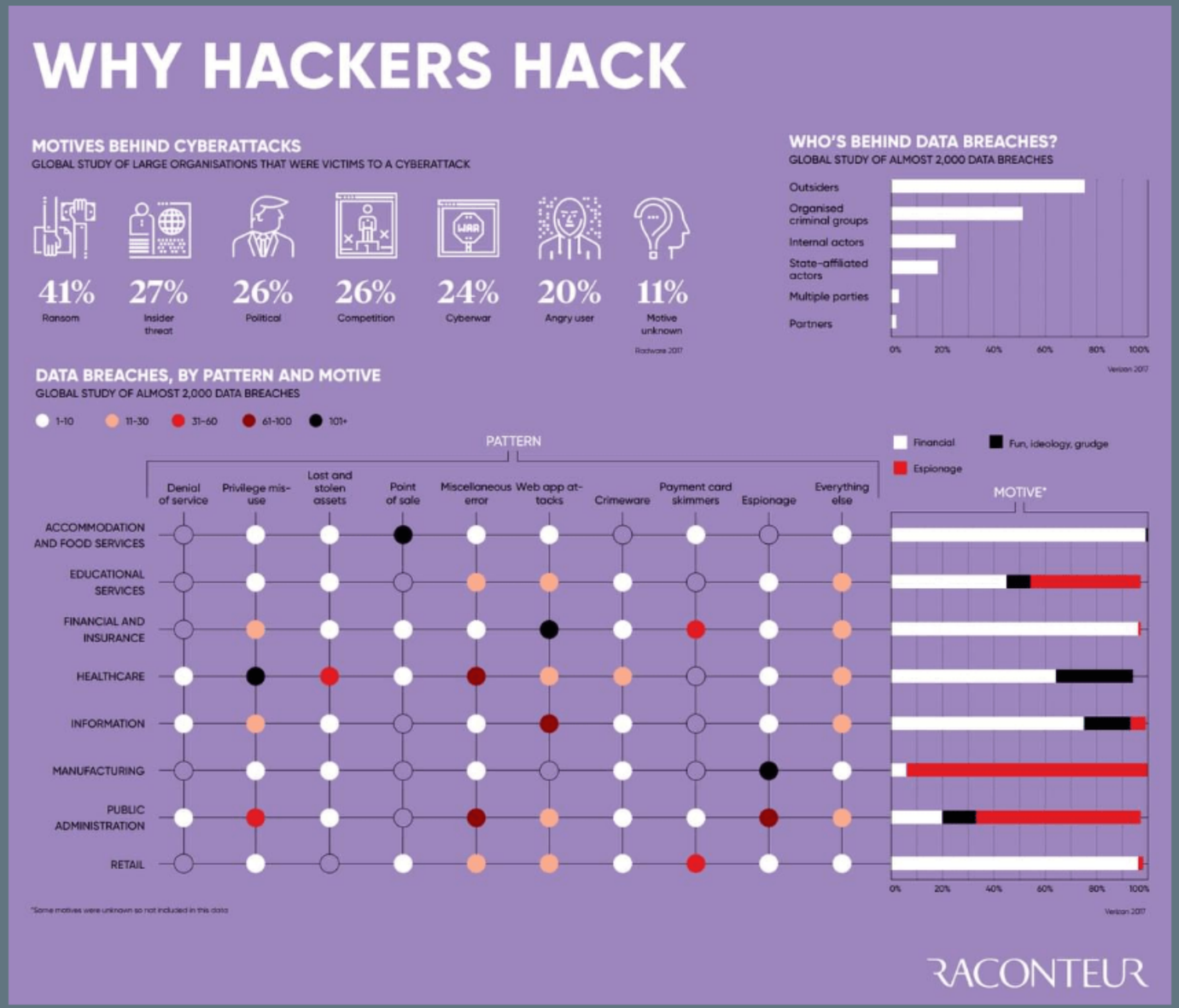
Neden Saldırıyorlar?



Kim Saldırıyor?



Infograph



http://rcnt.eu/2mj57

Sık Görülen Saldırılar

- Portscanning
- Şifre Saldırıları - Brute force
- Uygulama Saldırıları - Winbox saldırısı
- Web Uygulama Saldırıları
- DoS & DDoS
- Zero Day saldırıları

MikroTik Web Servis Açığı

- https://wikileaks.org/ciav7p1/
- 7 Mart 2017'de yayınlandı.
- 9 Mart 2017'de MikroTik açığın giderildiği yeni sürümleri çıkardı.
- Etkilenmemek için güncel RouterOS kullanılmalı.
- İhtiyacınız yoksa www servisini kapatınız.

MikroTik Web Servis Açığı

- VPNFilter
- Hajime Botnet
- Slingshot

Funny command

```
$ ./tools/getROSbin.py 6.38.4 mipsbe /nova/bin/www www_binary
$ ./StackClash_mips.py 192.168.8.1 80 www_binary "echo hello world > /dev/lcd"
```

https://github.com/BigNerd95/Chimay-Red

MikroTik Winbox Açığı

How to use

Note that this script will NOT run with Python2.x. Use only Python 3+

Winbox (TCP/IP)

```
$ python3 WinboxExploit.py 172.17.17.17

User: admin
Pass: Th3P4ssWord
```

MAC server Winbox (Layer 2)
You can extract files even if the device doesn't have an IP address :-)

```
$ python3 MACServerDiscover.py
Looking for Mikrotik devices (MAC servers)

    aa:bb:cc:dd:ee:ff

    aa:bb:cc:dd:ee:aa
```

```
$ python3 MACServerExploit.py aa:bb:cc:dd:ee:ff

User: admin
Pass: Th3P4ssWord
```

https://github.com/BasuCert/WinboxPoC

- 23 Nisan 2018'de açığa çıktı.
- Aynı gün açığın giderildiği RouterOS sürümü yayınlandı.
- Uygulaması çok kolay olduğundan etkisi çok fazla.
- Güncel RouterOS sürümü kullanılmalı.
- Winbox erişimi filtrelenmelidir

Port Tarama

```
λ nmap -sS 192.168.1.1

Starting Nmap 7.31 ( https://nmap.org ) at 2018-10-11 22:23 Turkey Standard Time
Nmap scan report for 192.168.1.1
Host is up (0.0038s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
443/tcp  open  https
2000/tcp open  cisco-sccp
8080/tcp open  http-proxy
8291/tcp open  unknown
MAC Address: [redacted] (Routerboard.com)

Nmap done: 1 IP address (1 host up) scanned in 14.25 seconds
```

- En çok kullanılan hedef tespit yöntemidir.
- MikroTik ürünler 80 ve 8291 portları taranarak bulundu.
- IP Firewall ve IP services ayarları ile engellenebilir

Şifre Saldırıları

Oct/12/2018 23:38:32	memory	system, error, critical	login failure for user user from 103.89.89.228 via ssh
Oct/12/2018 23:38:32	memory	system, error, critical	login failure for user support from 103.89.89.228 via ssh
Oct/12/2018 23:38:32	memory	system, error, critical	login failure for user guest from 103.89.89.228 via ssh
Oct/12/2018 23:38:33	memory	system, error, critical	login failure for user root from 103.89.89.228 via ssh
Oct/12/2018 23:38:33	memory	system, error, critical	login failure for user user from 103.89.89.228 via ssh
Oct/12/2018 23:42:17	memory	certificate, info	got CRL with bad signature, issued by AddTrust External CA Root::SE:A
Oct/12/2018 23:42:17	memory	certificate, info	got CRL with bad signature, issued by GlobalSign Organization Validatio
Oct/13/2018 00:08:39	memory	system, error, critical	login failure for user root from 103.89.89.228 via ssh
Oct/13/2018 00:08:40	memory	system, error, critical	login failure for user user from 103.89.89.228 via ssh
Oct/13/2018 00:08:44	memory	system, error, critical	login failure for user support from 103.89.89.228 via ssh
Oct/13/2018 00:08:48	memory	system, error, critical	login failure for user user from 103.89.89.228 via ssh
Oct/13/2018 00:08:49	memory	system, error, critical	login failure for user guest from 103.89.89.228 via ssh

- Brute force şifre saldırıları
- Winbox açığı kullanıldığında şifre saldırıları yapmadan şifreler açığa çıktı.
- Şifre saldırılarına karşı karmaşık şifreler kullanılmalıdır
- IP Firewall ve IP services ayarlarından router'a bağlanabilecek IP adresleri kısıtlanmalıdır.

DoS & DDoS Saldırıları

Zero Day Saldırıları

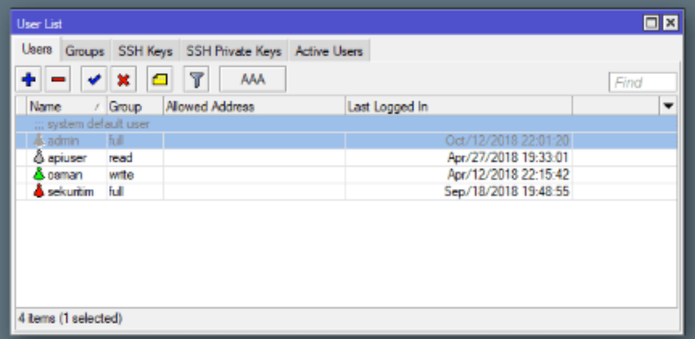
- Bu yıl ve 2019 yılında saldırıların devam etmesi bekleniyor.
- 2017 Mart ayından beri artık MikroTik ürünler tüm hacker gruplarının hedefleri arasına girmiş durumda.
- Yeni açıklar her an çıkabilir.

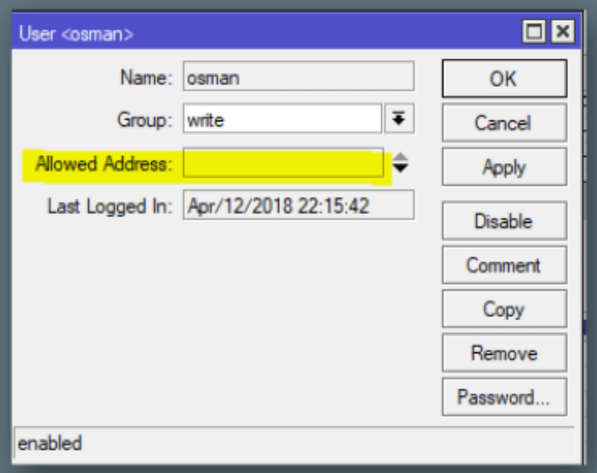
Ne Yapacağız?

Güncelleme

- İlk yapılması gereken RouterOS'un güncel sürümlere yükseltilmesidir.
- RouterBoot güncellemesini unutmayınız.
- Yeni güncellemeleri takip etmenizi ve changelog dokümanını incelemenizi tavsiye ediyoruz.
- https://blog.mikrotik.com
- https://wiki.mikrotik.com/wiki/Manual:Securing_Your_Router#Router_services
- https://forum.mikrotik.com

Kullanıcı Yönetimi

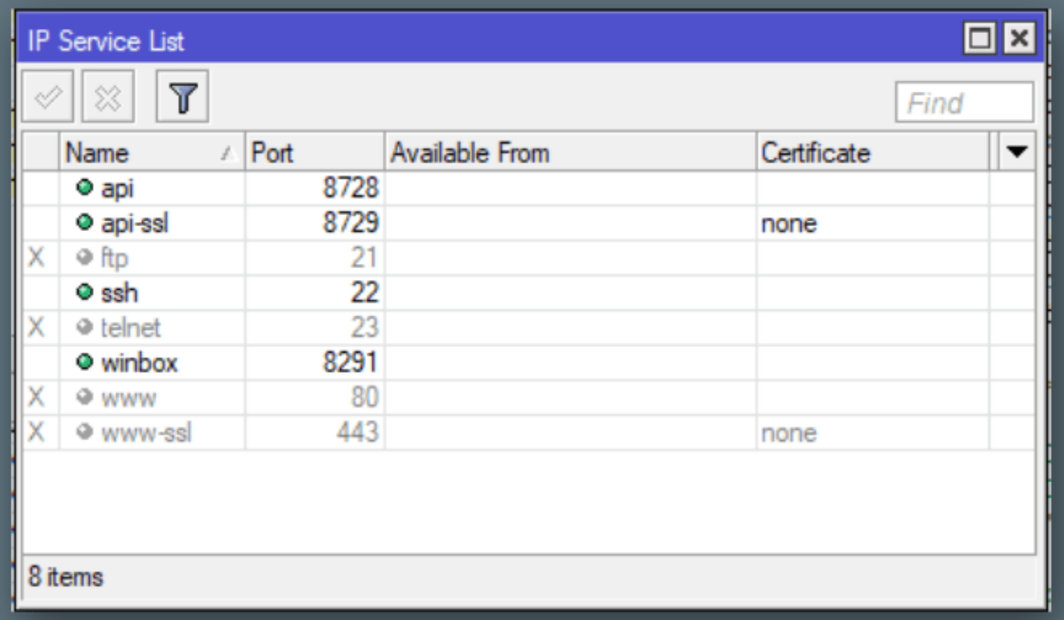




- admin kullanıcı adını değiştiriniz
- Tüm kullanıcılar için karmaşık şifreler kullanınız
- Grup ayarları ile yetkilendirme sistemini kullanınız. Tüm kullanıcıların ful yetki ihtiyacı var mı?
- 'Available From' ayarları ile kullanıcıların belli IP adreslerinden bağlamalarını sağlayabilirsiniz.

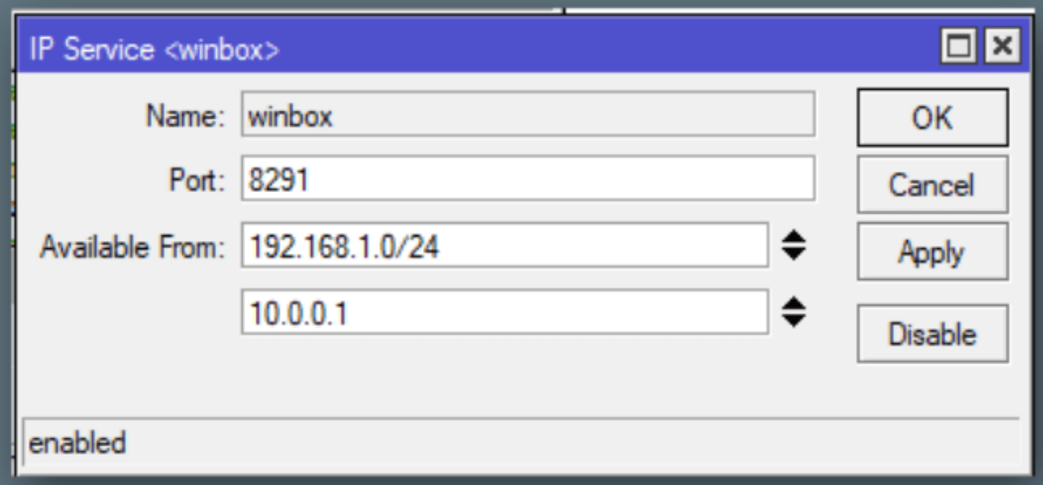
IP Services

- Kullanmadığınız servisleri kapatınız
- Sadece güvenli servisleri kullanınız (ftp, telnet, www kullanmayınız.)
- API kullanmıyorsanız kapatınız



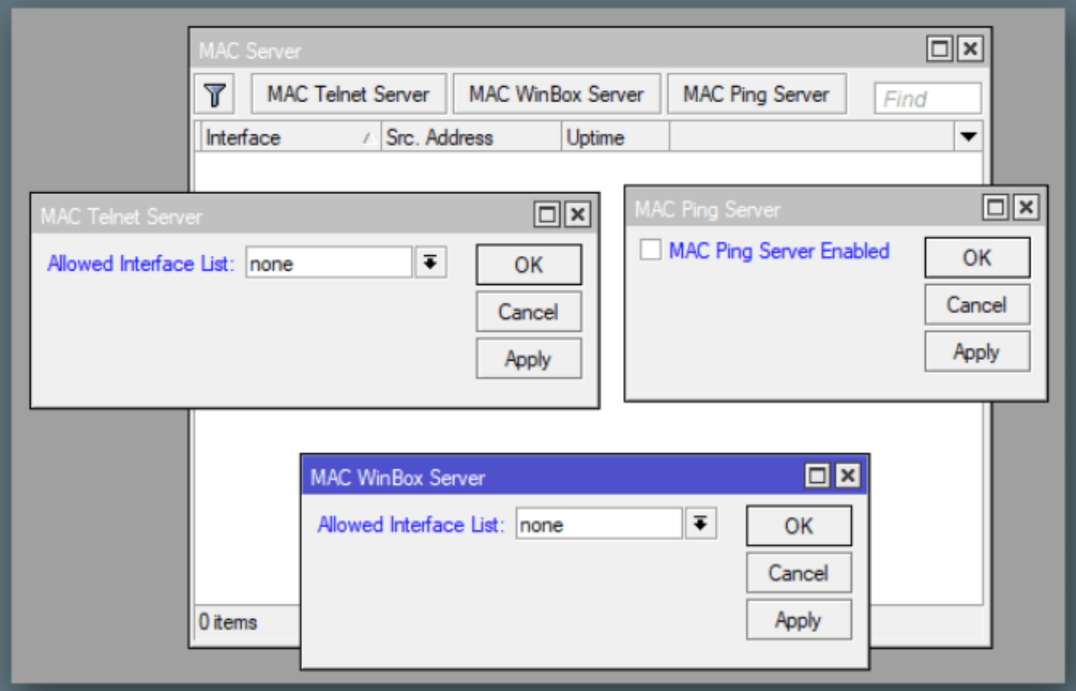
IP Services

- 'Available From' alanını kullanınız
- Servislere hangi IP adreslerinden bağlanılabileceğini limitleyebilirsiniz.
- Servislerin çalıştığı default portları değiştirebilirsiniz.
- Bu dönemde 8291 portunu değiştirmek routerlarınızın bulunmasını engelleyecektir.



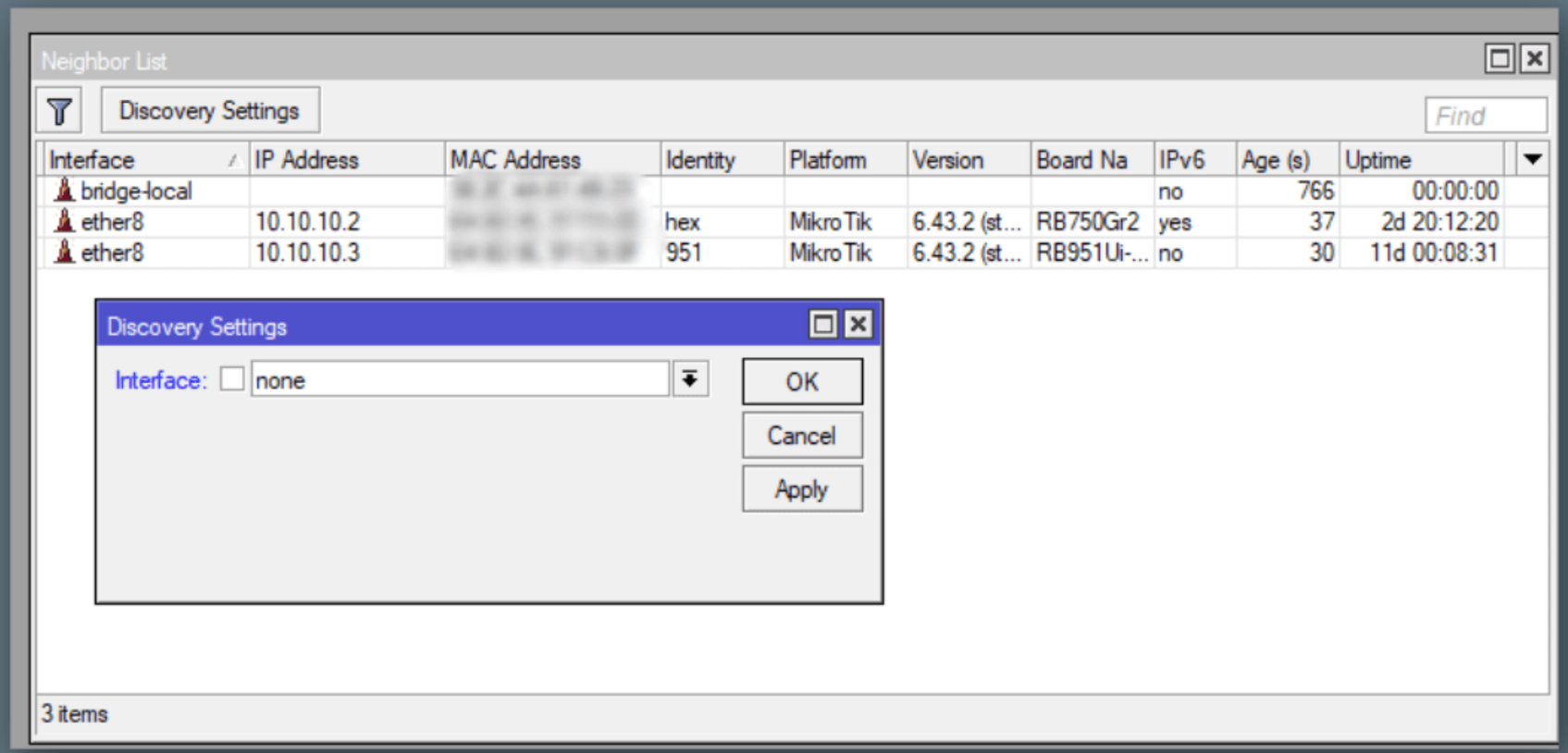
MAC Erişimi

- Tüm MAC erişimleri routerlar canlı ortamda çalışırken kapatılmalıdır.
- MAC-telnet, MAC-winbox, MAC-ping servislerini kapatınız.



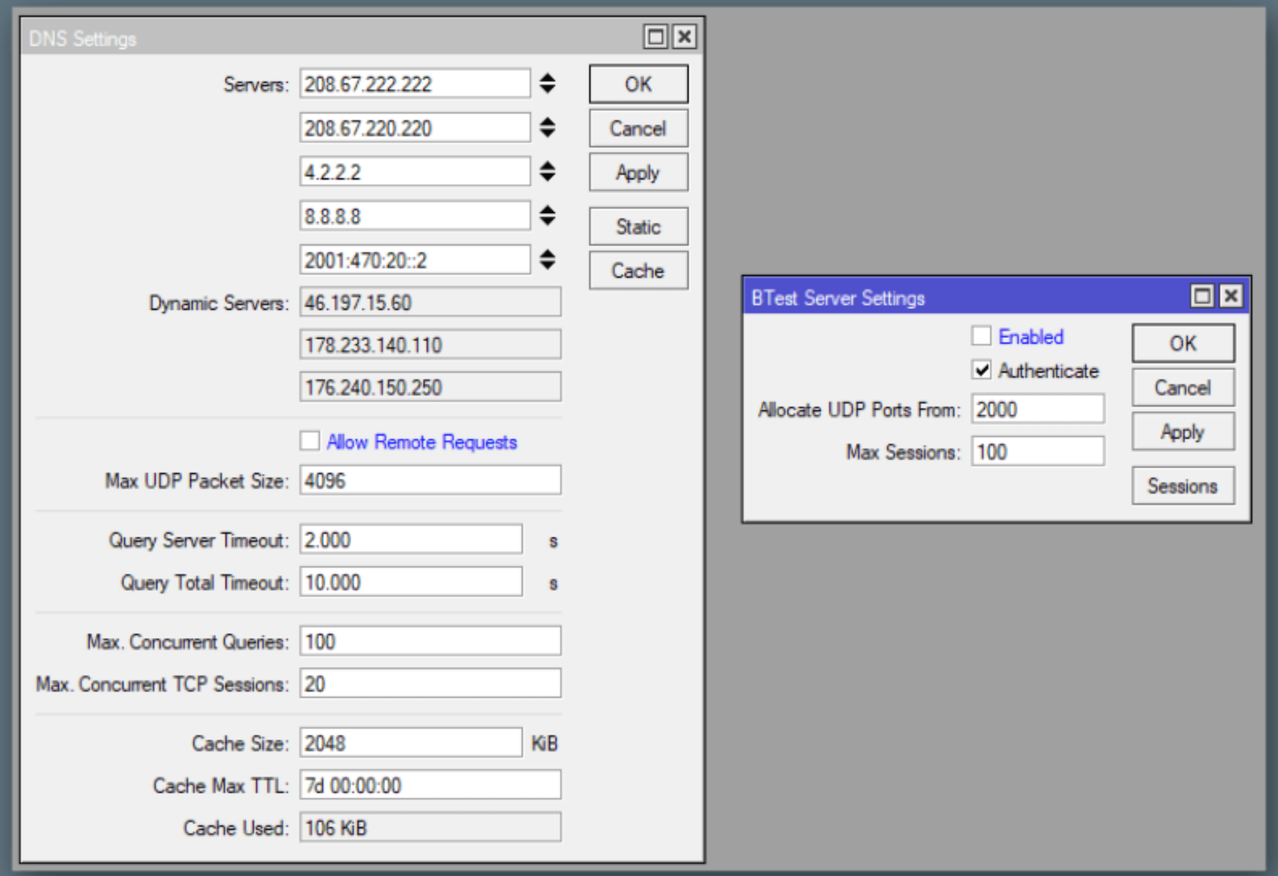
Tools MAC Server menüsü

Neighbor Discovery



IP Neighbors Menüsü

BW server ve DNS Cache



Tools BW server Menüsü
IP DNS Menüsü

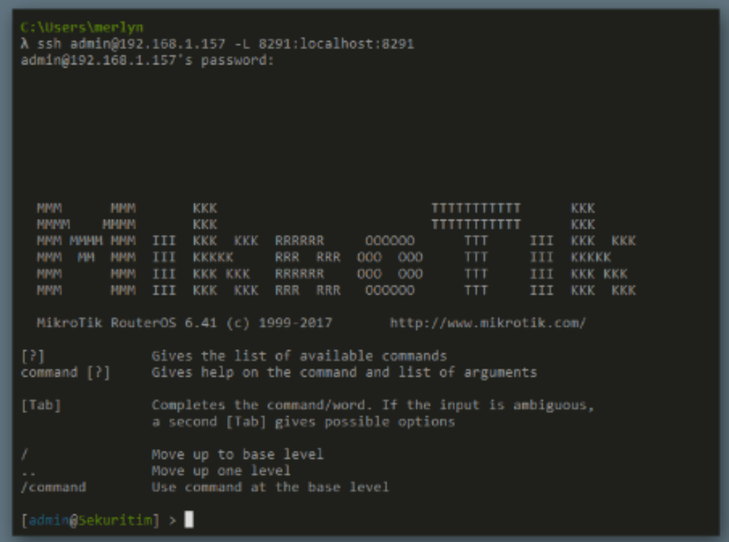
SSH Erişimi

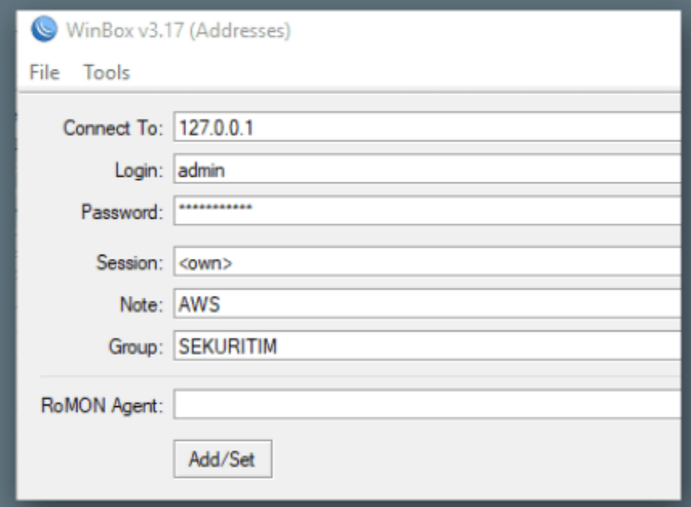
- SSH kullanılarak dosya transfer ve terminal erişimi sağlayabilirsiniz.
- SSH tünelleme kullanarak router üzerindeki diğer servislere ve router arkasındaki her türlü kaynağa bağlanabilirsiniz.
- Bu sebepten güçlü kripto kullanınız.
- Şifre yerine ssh anahtarları kullanabilirsiniz.

```
/ip ssh set strong-crypto=yes
```

SSH Tünelleme

Winbox ve router arkasındaki tüm kaynaklara ssh tünel üzerinden erişilebilir



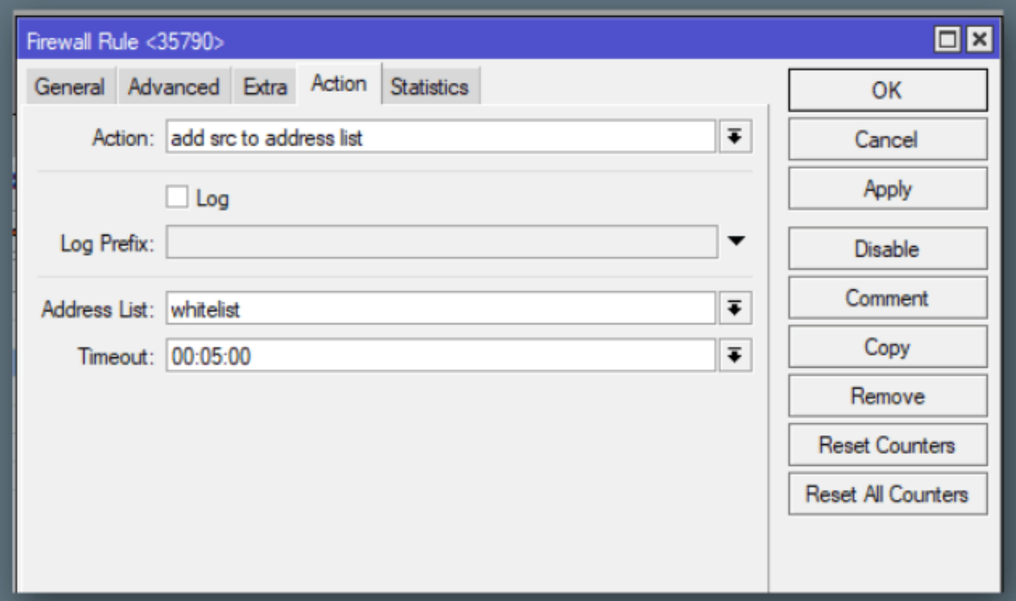


Firewall

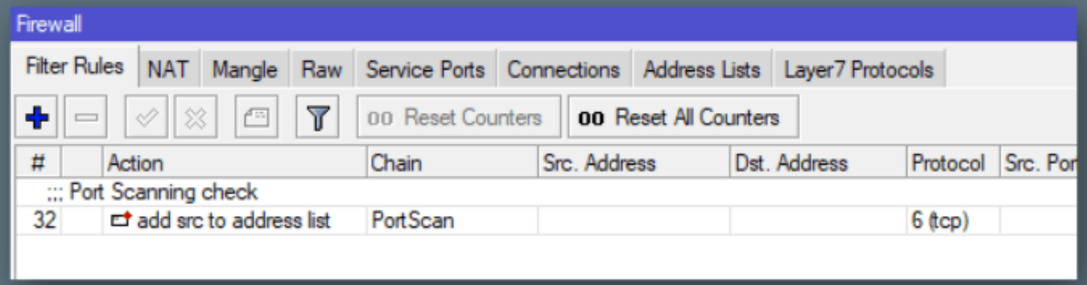
- Firewall yükünü azaltmak için sadece 'new' paketleri filtreleyen kurallar uygulayınız.
- 'Established' ve 'related' kuralların uygulayınız.
- 'Invalid' Paketleri drop ediniz.
- Sadece gerekli trafiğe izin veriniz. Geri kalan herşeyi drop ediniz.
- Firewall kurallarında comment kullanınız.
- Router'ın herhangi bir servis portu internete açılmamalıdır.
- Servislere 3 hatalı denemede otomatik bloklama ayarlanabilir.

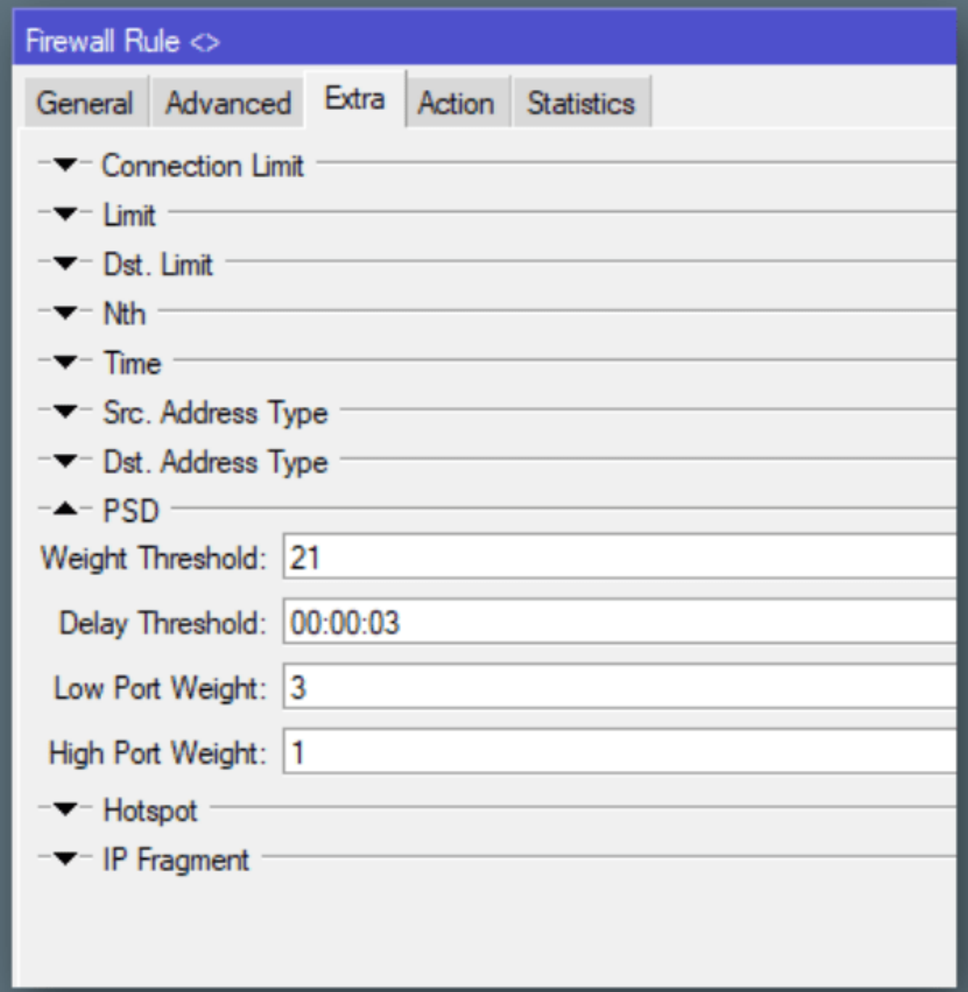
Port Knocking

- Router'a özel bir paket göndererek geçici süreliğine erişim açılmasını sağlayabilirsiniz.
- Paket boyutu, port numaraları, paket içeriği kullanılarak özel paket oluşturulabilir.
- Birden fazla paket ile port knocking ayarlanabilir.



Port Scan Detection





Firewall Kuralları

Firewall

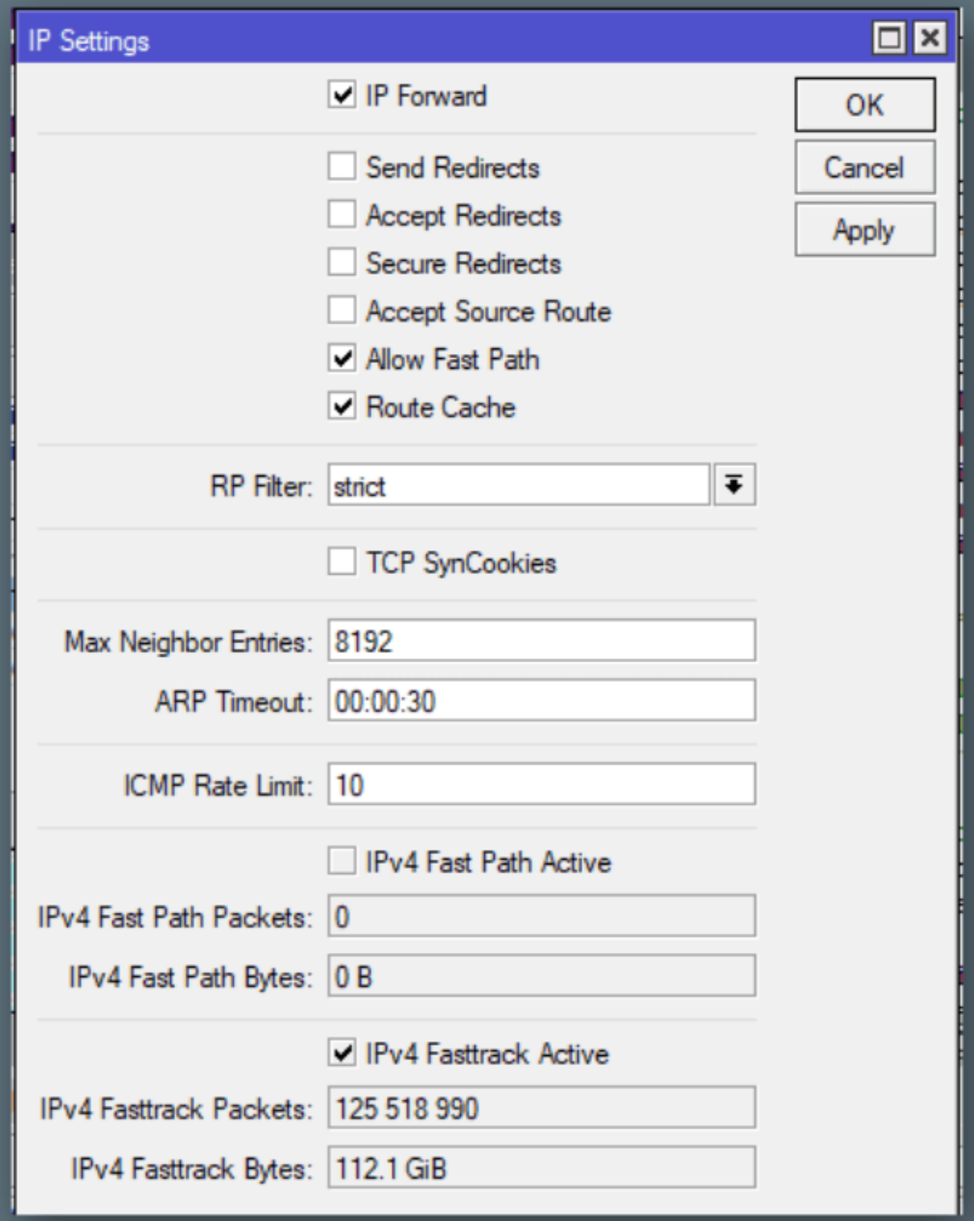
Filter Rules | NAT | Mangle | Raw | Service Ports | Connections | Address Lists | Layer7 Protocols

00 Reset Counters | 00 Reset All Counters | Find | all

#		Action	Chain	Src. Address	Dst. Address	Proto	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
;;; INVALID DROP												
0		drop	input								1051 B	13
;;; ESTABLISHED RELATED ACCEPT												
1		acc	input								1504.7 KiB	4 348
;;; PSD												
2		add...	forward			6 (tcp)					132 B	3
;;; Portknocking												
3		add...	input			6 (tcp)		35790			0 B	0
;;; WHITELIST												
4		acc	input								1153.7 KiB	17 836
;;; PSD												
5		jump	input			6 (tcp)					1280 B	26
;;; Service Attack												
6		jump	input			6 (tcp)		21,22,23,...			460 B	9
;;; DEFAULT DROP												
7		drop	input								14.8 KiB	245
;;; blacklist brute force												
8		add...	Service_at...			6 (tcp)		21,22,23,...			0 B	0
;;; brute force attempt#3												
9		add...	Service_at...			6 (tcp)		21,22,23,...			104 B	2
;;; brute force attempt#2												
10		add...	Service_at...			6 (tcp)		21,22,23,...			260 B	5
;;; brute force attempt#1												
11		add...	Service_at...			6 (tcp)		21,22,23,...			460 B	9
12		add...	PSD			6 (tcp)					44 B	1

13 items

RPFilter


IP Settings
IP Forward
OK
Cancel
Apply
Send Redirects
Accept Redirects
Secure Redirects
Accept Source Route
Allow Fast Path
Route Cache
RP Filter: strict
TCP SynCookies
Max Neighbor Entries: 8192
ARP Timeout: 00:00:30
ICMP Rate Limit: 10
IPv4 Fast Path Active
IPv4 Fast Path Packets: 0
IPv4 Fast Path Bytes: 0 B
IPv4 Fasttrack Active
IPv4 Fasttrack Packets: 125 518 990
IPv4 Fasttrack Bytes: 112.1 GiB

Son Önerilerimiz

- Kendi güvenlik standartlarınızı ve güvenlik yapılandırmalarınızı oluşturunuz.
- Standartlarınızı tüm routerlara uygulayınız.
- Trafik analizi ve bir SIEM sistemi saldırıları önceden tespit etmek için çok yararlı olacaktır.
- Log izleme scriptini inceleyiniz.
- https://wiki.mikrotik.com/wiki/Monitor_logs,_send_email_alert_/_run_script

Teşekkürler

Sunuma linkten ulaşabilirsiniz.
https://app.slidebean.com/p/HcmB8EKo1m/RouterOS-Gvenlii