MBUM #2

MikroTik Beer User Meeting

Zabezpieczenie routerów MikroTik.
Omówienie ostatnio ujawnionych luk.

Michał Filipek

Michał Filipek

MTCNA MTCRE MTCWE MTCIPv6E MTCINE MTCTCE

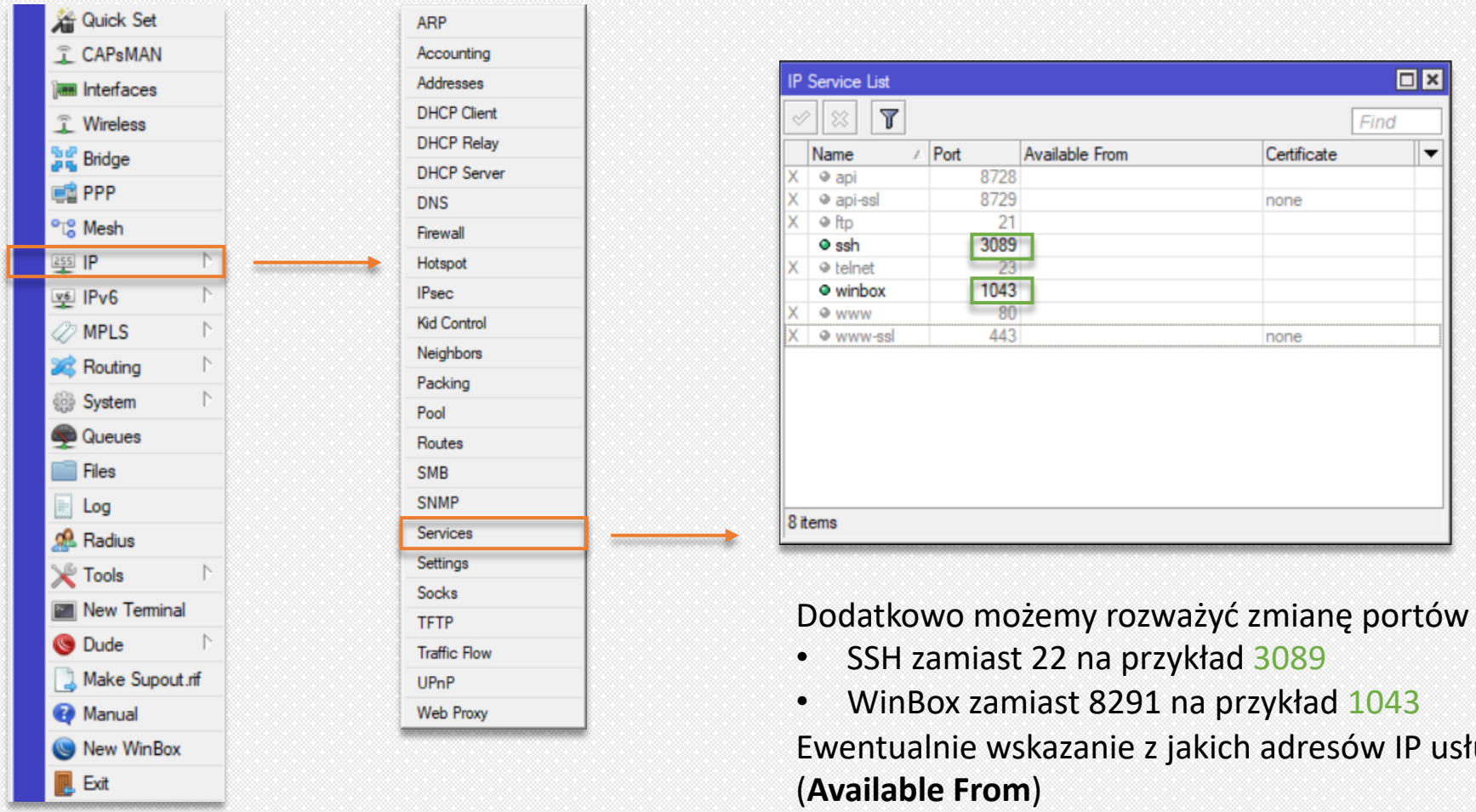
Ukończył Politechnikę Warszawską na kierunku Informatyka. Na przestrzeni ostatnich 12 lat pracował dla firm telekomunikacyjnych na stanowiskach: VoIP Engineer, Specjalista ds. Sieci i Systemów Telekomunikacyjnych, Specjalista ds. Utrzymania Sieci, Network Architect. Trener i współzałożyciel największego centrum szkoleniowego MikroTik w tej części Europy: Mikrotik Warsaw Training Center. Prowadzi szkolenia z zakresu działania sieci IP, telefonii VoIP oraz ISDN, ponadto świadczy usługi doradcze dla firm telekomunikacyjnych, technologicznych i innych.

michal@mwtc.pl

Agenda

- Metody dostępu do urządzenia
- Zabezpieczenie dostępu do routera
- Konta użytkowników
- Dodatkowe mechanizmy zwiększające bezpieczeństwo
- Omówienie podatności WinBox opublikowanej w kwietniu 2018
- Czy można było się uchronić przed atakiem ?
- W jaki sposób sprawdzić, czy zostałem ofiarą ataku ?
- Demonstracja wykorzystania podatności

Metody dostępu do urządzenia



Dodatkowo możemy rozważyć zmianę portów na jakich pracują usługi:

- SSH zamiast 22 na przykład 3089
- WinBox zamiast 8291 na przykład 1043

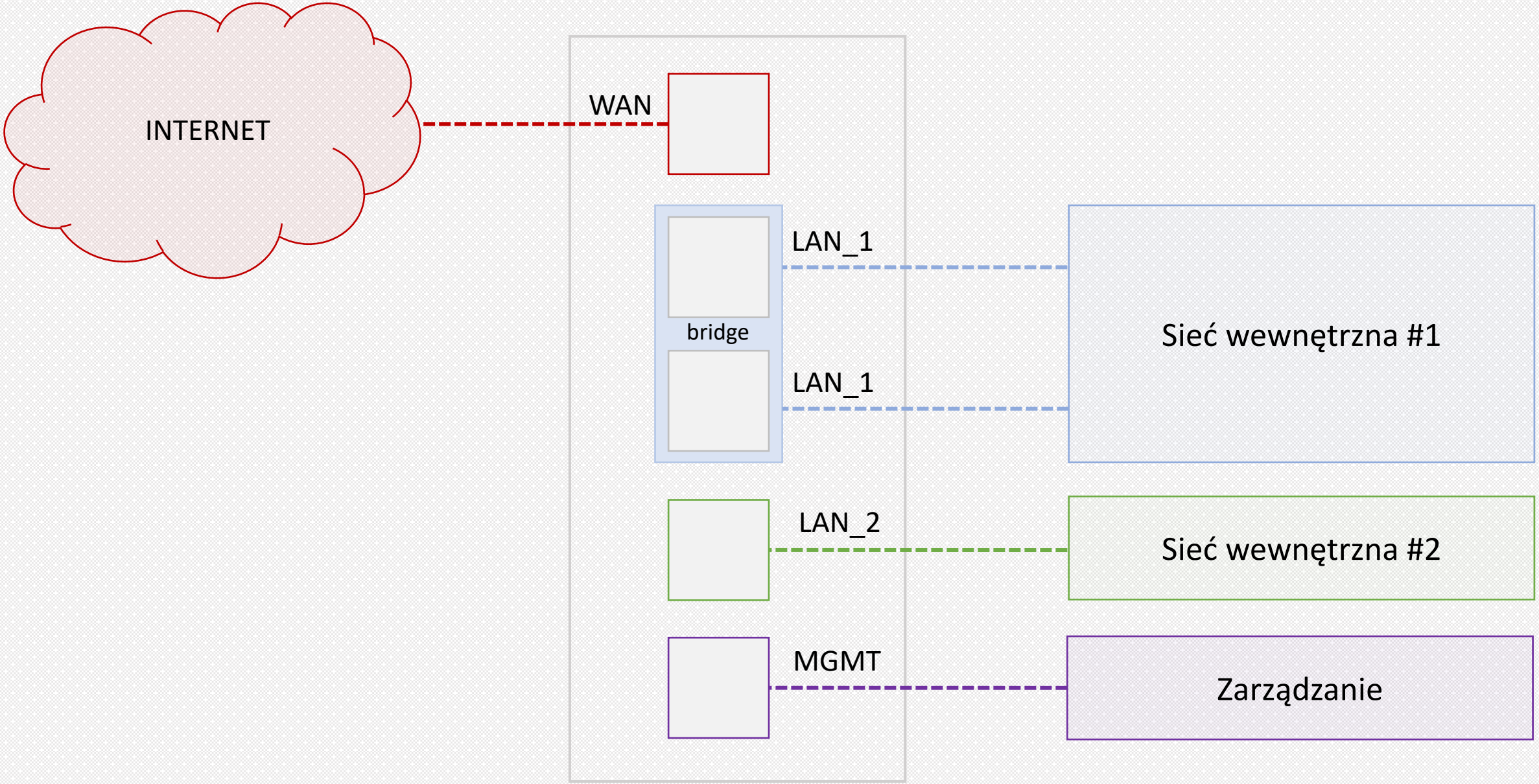
Ewentualnie wskazanie z jakich adresów IP usługa będzie dostępna (**Available From**)

Metody dostępu do urządzenia oraz inne usługi

Należy upewnić się, że poniższe usługi są wyłączone:

/tool *bandwidth-server set enabled=no*
/ip dns *set allow-remote-requests=no*
/ip socks *set enabled=no*
/ip upnp *set enable=no*
/ip cloud *set ddns-enable=no update-time=no*
/lcd *set enabled=no*
/ip proxy *set enabled=no*

Dostęp do urządzenia



Dostęp z sieci bezpośrednio podłączonych do routera (MAC-ADDRESS)

Administracyjne wyłączenie wszystkich interface'ów urządzenia jakie nie są obecnie wykorzystywane
/interface set 2,3 disabled=yes

Czy wszystkie sieci wewnętrzne są sieciami zaufanymi?
Można wyznaczyć jeden port na urządzeniu służący jedynie do zarządzania urządzeniem.

Protokół **MNDP** (MikroTik Neighbor Discovery Protocol) – pozwala na wykrywanie innych urządzeń znajdujących się w tej samej domenie rozgłoszeniowej co nasz router. Dodatkowo router, który ma uruchomione MNDP (uruchamiany ten protokół per interface, a nie całe urządzenie) sam staje się wykrywalny. Sugerowane jest wyłączenie działania protokołu na wszystkich interface'ach za wyjątkiem interface'u do zarządzania oraz zaufanych sieci **(/ip neighbor**).

Dostęp do urządzenia z wykorzystaniem jego adresu **MAC** (nie potrzebujemy posiadać adresu IP, dostęp możliwy jedynie w ramach tej samej domeny rozgłoszeniowej, dalej konieczne jest podanie prawidłowego loginu i hasła). W tym wypadku postępujemy podobnie jak w przypadku protokołu MNDP, czyli wyłączamy dostęp na wszystkich interface'ach poza zaufanymi **(/tool mac-server**).

Dostęp z zewnątrz do routera (internet)

Szczegółowo zaplanować w jaki sposób będzie można z zewnątrz podłączyć się do routera:

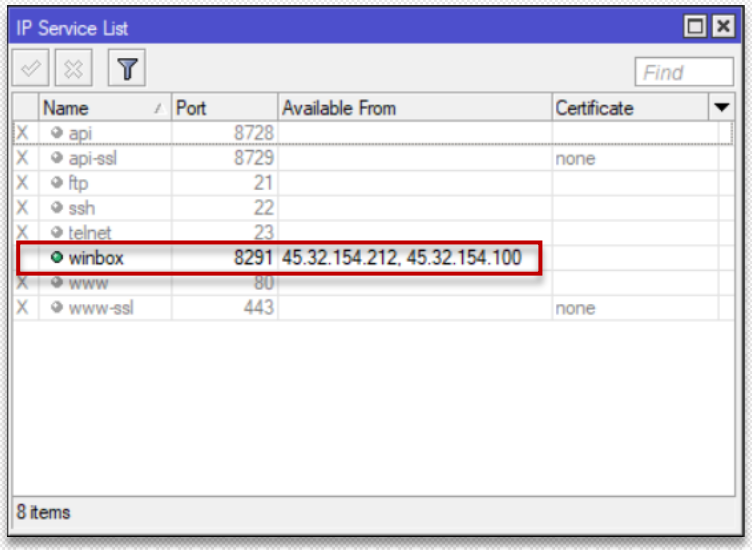
- Z konkretnych adresów IP
- Za pomocą VPN
- Port knocking (nie mamy stałego adresu IP oraz brak VPN na urządzeniu , z którego będziemy się łączyć do routera)

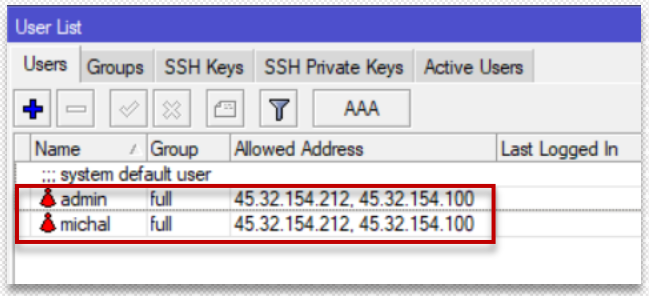
Dostęp z zewnątrz do routera (internet)

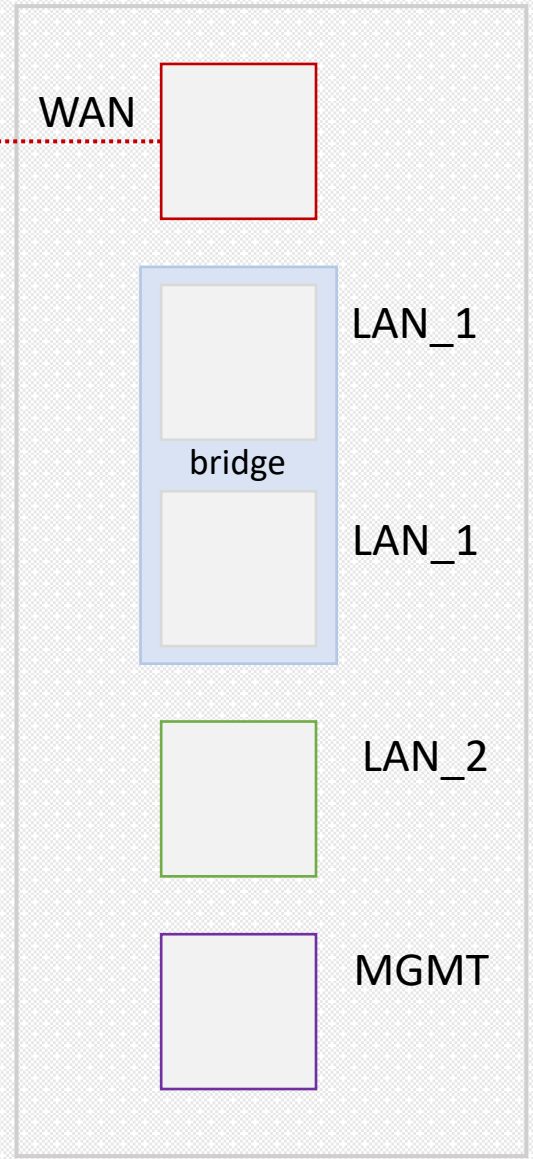
Z konkretnych adresów IP

Próba logowania

/ip firewall filter **/ip services** **/users**







/ip firewall filter *add chain=input comment="Accept Established, Related" connection-state=established,related action=accept*
/ip firewall filter *add chain=input src-address=45.32.154.212 action=accept*
/ip firewall filter *add chain=input src-address=45.32.154.100 action=accept*
/ip firewall filter *add chain=input action=drop*

Dostęp z zewnątrz do routera (internet)

VPN

Zmienny adres IP

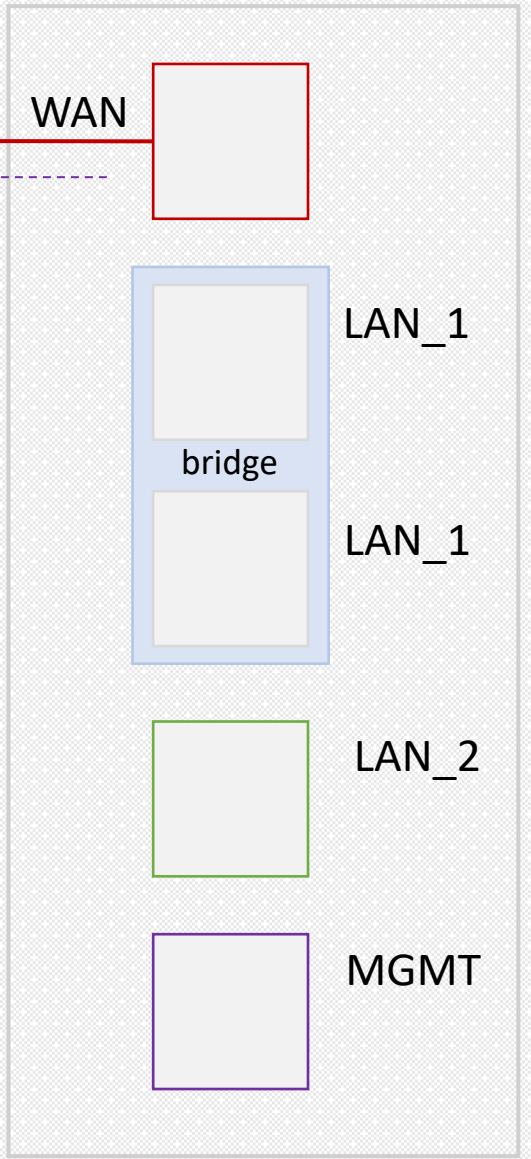
INTERNET

172.16.10.10

Adresacja Punkt-Punkt

SSTP

172.16.10.1



***/ip firewall filter** add chain=input comment="Accept Established, Related" connection-state=established,related action=accept*

***/ip firewall filter** add chain=input comment="SSTP VPN" protocol=tcp dst-port=443 action=accept*

***/ip firewall filter** add chain=input src-address=172.16.10.10/32 action=accept*

***/ip firewall filter** add chain=input action=drop*

Dostęp z zewnątrz do routera (internet)

Port Knocking

Zmienny adres IP

INTERNET

WAN

Próba połaczenia na port 2133/tcp

Próba połaczenia na port 7117/tcp

Logowanie Winbox

LAN_1

bridge

LAN_1

LAN_2

MGMT

***/ip firewall filter** add chain=input comment="Accept Established, Related" connection-state=established,related action=accept*
***/ip firewall filter** add chain=input protocol=tcp dst-port=2133 action=add-src-to-address-list address-list=port-knocking-stage1 address-list-timeout=00:01:00*
***/ip firewall filter** add chain=input protocol=tcp dst-port=7117 src-address-list=port-knocking-stage1 action=add-src-to-address-list address-list=port-knocking-stage2 address-list-timeout=00:01:00*
***/ip firewall filter** add chain=input src-address-list=port-knocking-stage2 protocol=tcp dst-port=8291 action=accept*
***/ip firewall filter** add chain=input action=drop*

Stosując port knocking powinniśmy zabezpieczyć się przed Skanowaniem Portów !!!

Konta użytkowników

- Utworzenie nowego użytkownika typu administrator (group: full)
- Wyłączenie konta admin
- Stosowanie odpowiednio złożonych haseł
- Wykorzystanie zewnętrznego systemu do autentykacji/autoryzacji użytkowników (Radius)

Dodatkowe mechanizmy zwiększające bezpieczeństwo

- Reverse Path Filtering (ochrona przed spoofing'iem wysyłanym z naszych sieci)
  /ip settings set rp-filter=strict
- Ustawienie silnej kryptografii dla połączeń ssh
  ***/ip ssh** set strong-crypto=yes*
- Korzystanie z zewnętrznego systemu kolekcji i analizy logów (SYSLOG,GRAYLOG można połączyć logi syslog z funkcjonalnością GeoIP i moniorować czy na nasze urządzenie nie loguje się ktoś z podejrzanego adresu)
- Regularne wykonywanie kopii konfiguracji (można użyć skryptu) urządzenia i weryfikacja, gdy nastąpi modyfikacja

Podatności na ataki

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2018-14847	287		Bypass	2018-08-02	2018-10-12	5.0	None	Remote	Low	Not required	Partial	None	None
Winbox for MikroTik RouterOS through 6.42 allows remote attackers to bypass authentication and read arbitrary files by modifying a request to change one byte related to a Session ID.														
2	CVE-2018-7445	119		Exec Code Overflow	2018-03-19	2018-04-24	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
A buffer overflow was found in the MikroTik RouterOS SMB service when processing NetBIOS session request messages. Remote attackers with access to the service can exploit this vulnerability and gain code execution on the system. The overflow occurs before authentication takes place, so it is possible for an unauthenticated remote attacker to exploit it. All architectures and all devices running RouterOS before versions 6.41.3/6.42rc27 are vulnerable.														
3	CVE-2018-1159	119		Overflow Mem. Corr.	2018-08-23	2018-10-12	4.0	None	Remote	Low	Single system	None	None	Partial
Mikrotik RouterOS before 6.42.7 and 6.40.9 is vulnerable to a memory corruption vulnerability. An authenticated remote attacker can crash the HTTP server by rapidly authenticating and disconnecting.														
4	CVE-2018-1158	400			2018-08-23	2018-10-12	4.0	None	Remote	Low	Single system	None	None	Partial
Mikrotik RouterOS before 6.42.7 and 6.40.9 is vulnerable to a stack exhaustion vulnerability. An authenticated remote attacker can crash the HTTP server via recursive parsing of JSON.														
5	CVE-2018-1157	400			2018-08-23	2018-10-12	6.8	None	Remote	Low	Single system	None	None	Complete
Mikrotik RouterOS before 6.42.7 and 6.40.9 is vulnerable to a memory exhaustion vulnerability. An authenticated remote attacker can crash the HTTP server and in some circumstances reboot the system via a crafted HTTP POST request.														
6	CVE-2018-1156	119		Exec Code Overflow	2018-08-23	2018-10-12	9.0	None	Remote	Low	Single system	Complete	Complete	Complete
Mikrotik RouterOS before 6.42.7 and 6.40.9 is vulnerable to stack buffer overflow through the license upgrade interface. This vulnerability could theoretically allow a remote authenticated attacker execute arbitrary code on the system.														

Podatność na atak - WinBox

- Dotyczy RouterOS w wersji od 6.29 do 6.42.1(current), 6.40.8(bugfix)
- Ujawniona w okolicach 20.04.2018
- Szybka reakcja producenta i wypuszczenie poprawki
- Umożliwia pobranie bazy danych użytkowników i haseł
- Umożliwia zapisanie plików na naszym urządzeniu w dowolnym miejscu
- Ze względu na bardzo słabą metodę przechowywania hasła (metoda XoR), odczytanie hasła z pliku jest bardzo łatwe

Czy można było uniknąć bycia zaatakowanym?

Tak, jeżeli dostęp z zewnątrz był zabezpieczony
przez firewall ☺

W jaki sposób sprawdzić, czy nie zostałem zaatakowany ?

- Udane próby logowania z adresów zagranicznych o dziwnych porach dnia i nocy (koniecznie logowane na zewnętrznego syslog'a, ponieważ na zaatakowanym MikroTik'u logi zostaną prawdopodobnie skasowane) – jest to najbardziej wiarygodna metoda weryfikacji
- Zmieniona konfiguracja /system/logging urządzenia
  /system logging *action set 0 memory-lines=1*
- Zmieniona konfiguracja urządzenia, a w szczególności:
  - Uruchomiona usługi telnet
  - Włączone socks
  - Włączone web-proxy
  - Włączone DNS (allow-remote-request)

Powyższe metody nie odpowiedzą w 100%, czy doszło do ataku, są jedynie zbiorem najczęściej spotkanych objawów !!!

Dziękuję za uwagę ☺

https://mbum.pl