Boas práticas operacionais com RouterOS

NIC.br – 27/10/2021

São Paulo / SP

Wardner Maia

Introdução

Wardner Maia

Engenheiro – Eletrotécnica e Eletrônica com especialização em Telecomunicações;

Provedor de Acesso desde 1995;

Treinamentos para ISPs desde 2002;

Diretor técnico da MD Brasil IT & Telecom;

Diretor do LACNIC.

Introdução

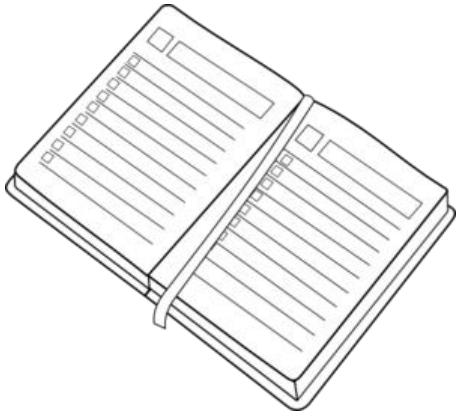
MD Brasil IT & Telecom

Serviços de Cloud & Datacenter;
Soluções para ISPs;
Treinamentos e capacitação em TI;
Serviços de consultoria.

OBS: Provedor de acesso de dezembro de 1995 à março de 2021;

http://mdbrasil.com.br http://mikrotikbrasil.com.br

Agenda



Introdução;

Boas práticas “na largada”

Segurança - administração de usuários, senhas e segurança física;

Facilidades que podem causar dificuldades

Segurança de serviços

Boas práticas operacionais

Introdução

Introdução

Porta de entrada para a grande maioria dos ISPs brasileiros devido ao excelente custo benefício;

Interface amigável que torna exponencial a curva de aprendizado de protocolos de Internet

Um verdadeiro "canivete suiço" que se aplica a muitas situações

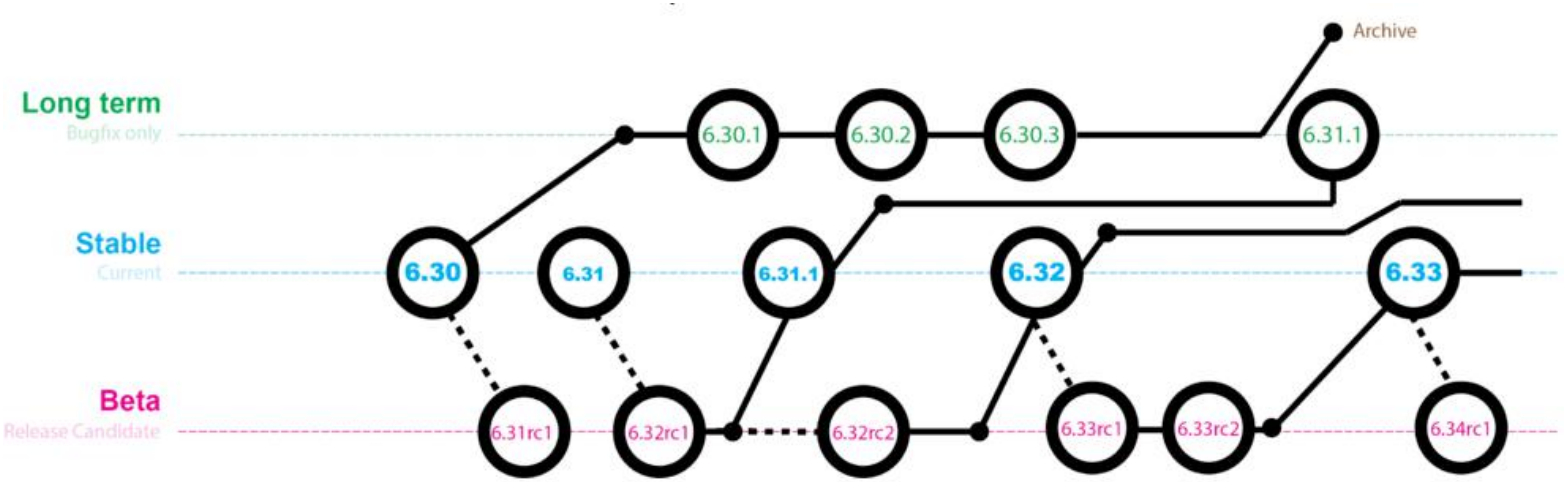
Escalabilidade - hardwares não tem acompanhado as necessidades de banda

Foco global não sintonizado com as necessidades brasileiras (wireless x fibra)

Boas práticas na “largada”

Boas práticas iniciais

Escolha a versão correta

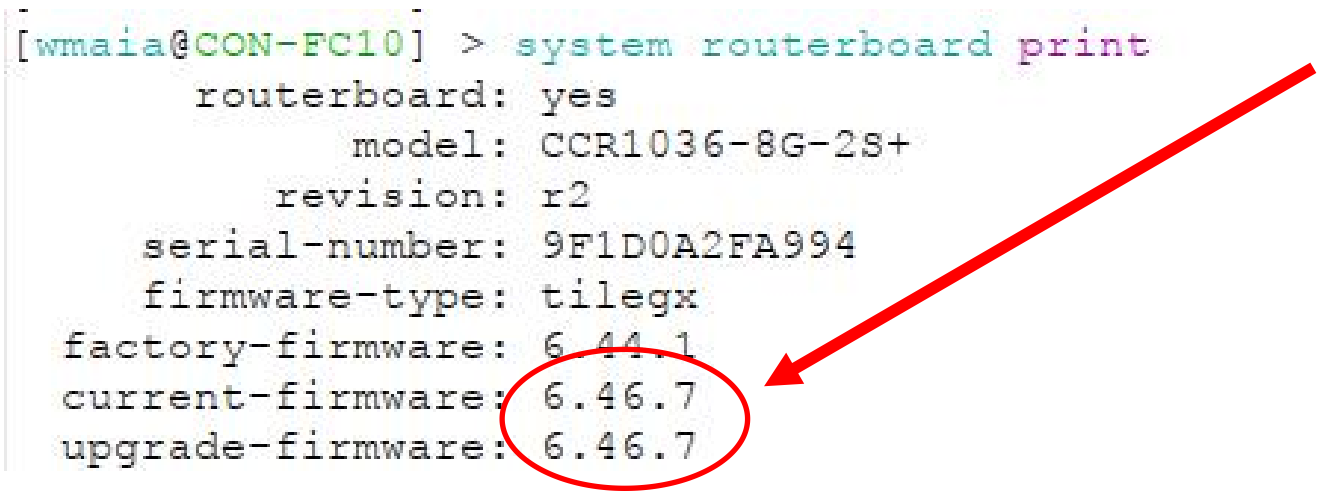


Preferencialmente escolha a versão **Long term** que é a que não sofre impacto da implementação de novas funcionalidades

Boas práticas iniciais

Lembre-se de atualizar o Boot Loader

Sempre que há uma nova instalação ou atualização o upgrade do boot loader **não** é automático o que pode levar a falhas ou algum tipo de funcionamento anômalo.



Boas práticas iniciais

Livre-se dos pacotes desnecessários

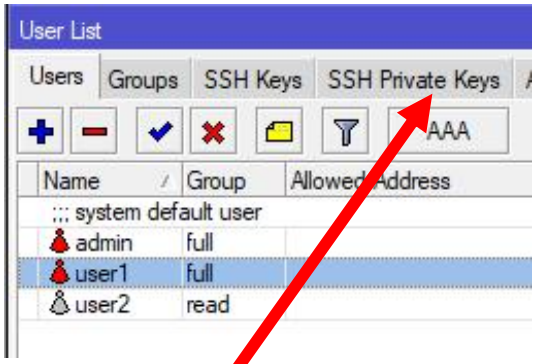
O RouterOS tem pacotes para várias funções. Um pacote que não esteja sendo usado pode ser um potencial problema de segurança ou mesmo implicar em upgrades desnecessários

```
[wmaia@CON-FC10] > system package print
Flags: X - disabled
 #    NAME                      VERSION                  SCHEDULED
 0    ntp                       6.46.7
 1    ppp                       6.46.7
 2    dhcp                      6.46.7
 3    ipv6                      6.46.7
 4    security                  6.46.7
 5    advanced-tools            6.46.7
 6    system                    6.46.7
 7    routing                   6.46.7
```


Elimine pacotes desnecessários com
/system package remove # (requer reboot)

Usuários e senhas

Usuários e senhas



Atenção para a base de usuários locais

Evite deixar usuários locais nos roteadores.

Preferencialmente use a autenticação via RADIUS principalmente em equipamentos remotos (ERBs por exemplo)

Se necessário cadastrar usuário local, considere a criação de um porém restringindo por ssh e utilizando uma chave RSA

Usuários e senhas

Criando uma chave RSA para uso no Mikrotik

```
maia@xps:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/maia/.ssh/id_rsa): mdadm-ssh
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in mdadm-ssh.
Your public key has been saved in mdadm-ssh.pub.
The key fingerprint is:
SHA256:6A4QANxds2fmF/BsWp5v0C2vUc+qZUT24MKm2x0eleE maia@xps
The key's randomart image is:
+---[RSA 2048]----+
|= . . .o .       |
| o . .  o +      |
|  .    . + *  +. |
|   .   .= =.++ooo|
|  .   . So =+ooEo|
|   . .    .ooo+o.|
|    . .   .  +=.o|
|     o     o.=o+ |
|      .   . oo+  |
+----[SHA256]-----+
maia@xps:~$
```

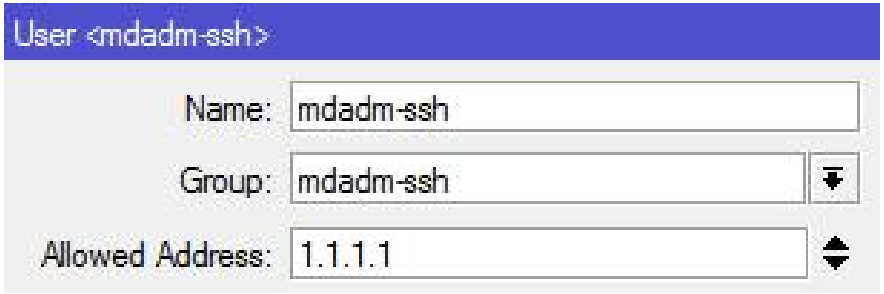
Usuários e senhas

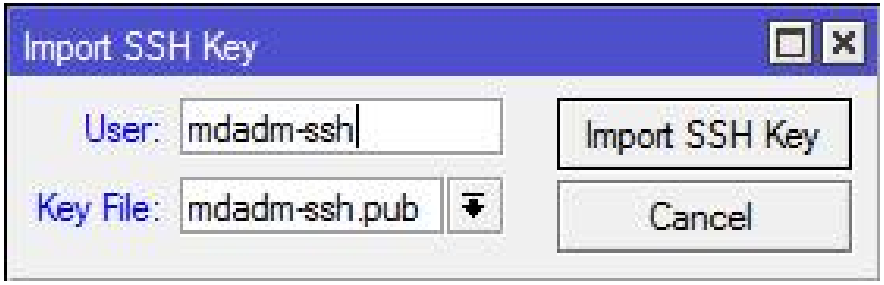
Fazendo o upload para o Roteador

```
maia@xps:~$ ftp 192.168.1.1
Connected to 192.168.1.1.
220 AP-Maia FTP server (MikroTik 6.38.5) ready
Name (192.168.1.1:maia): admin
331 Password required for admin
Password:
230 User admin logged in
Remote system type is UNIX.
ftp> put mdadm-ssh.pub
local: mdadm-ssh.pub remote: mdadm-ssh.pub
200 PORT command successful
150 Opening ASCII mode data connection for '/mdadm-ssh.pub'
226 ASCII transfer complete
391 bytes sent in 0.03 secs (14.3910 kB/s)
ftp>
```

Usuários e senhas

Criando um usuário com acesso restrito



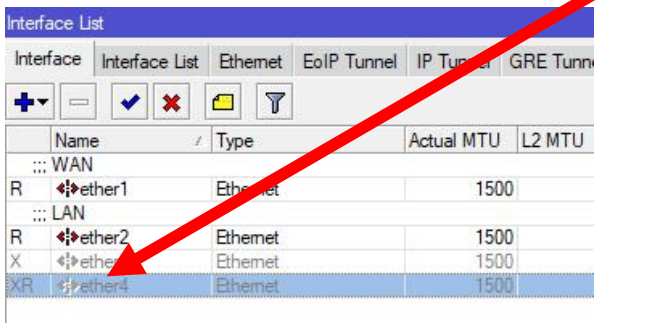



```
maia@xps:~$ ssh -l mdadm-ssh -p 6922 -i /home/maia/mdadm-ssh 192.168.1.1
mdadm-ssh@192.168.1.1's password:
```

Segurança Física

Segurança Física

Equipamentos em ambientes externos e ou nas dependências de clientes



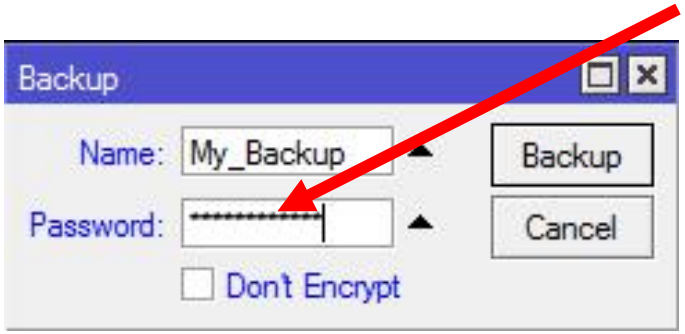
Desabilitar interfaces não utilizadas:

- Interfaces habilitadas sem necessidade podem ser utilizadas por atacantes para obter informações importantes da rede.

- Mesmo em setups teoricamente seguros, o acesso a interfaces pode ser porta de entrada para explorações mais profundas.

Segurança Física

Equipamentos em ambientes externos e ou nas dependências de clientes

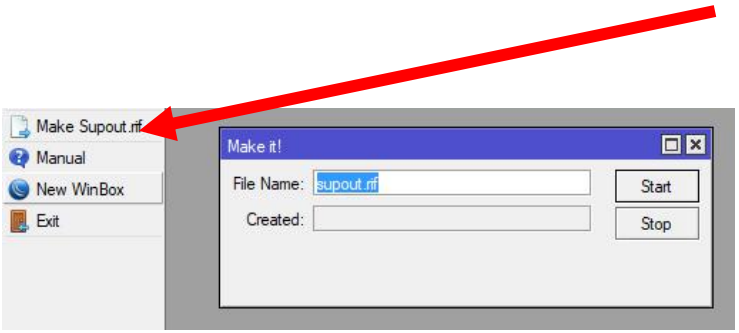


Não deixar arquivos de backup nos roteadores

- Arquivos de backup podem conter informações sensíveis da rede (alguns até com usuários/senhas).
- Criação de Backup automático quando uma RouterBoard é resetada facilita o trabalho dos atacantes
- Por padrão o backup **NÃO** é criptografado, a menos que seja definida uma senha (a partir da 6.43) .

Segurança Física

Equipamentos em ambientes externos e ou nas dependências de clientes



Não deixar arquivos suppout.rif nos roteadores

- Arquivos suppout.rif servem para debugar problemas diversos. Pode ser criado manualmente ou é criado automaticamente em certas situações;

- Informações visualizadas pelo site da Mikrotik;

- Existe porém na Internet um script Perl, que obtém as informações relevantes do mesmo:

https://pastebin.com/pa30DNfw

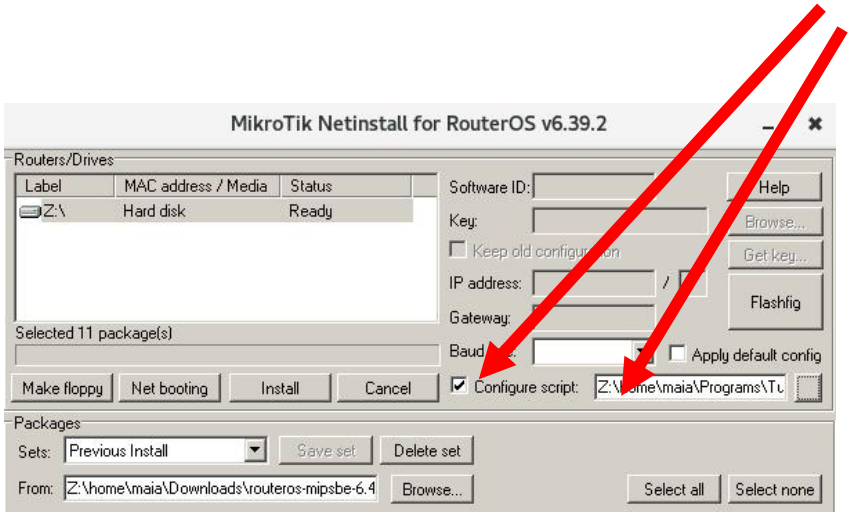
Segurança Física

Mitigação

Não deixar arquivos de backup nos roteadores

Não deixar arquivos suppout.rif nos roteadores

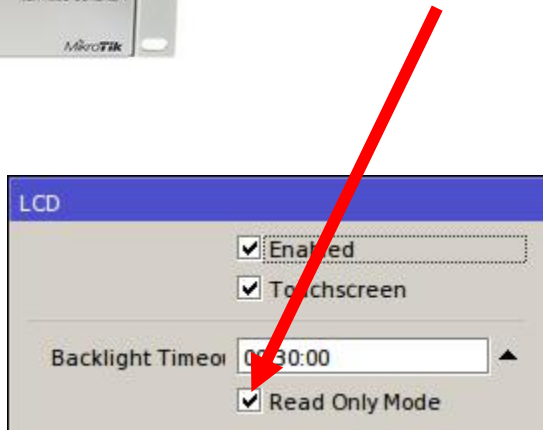
Podendo esses arquivos serem criados automaticamente, a solução é um script persistente que limpe esses arquivos a cada boot, o que pode ser feito via Netinstall

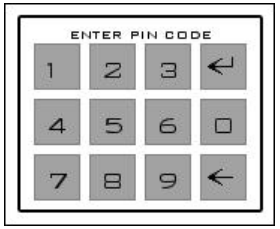


Segurança Física

LCD

Se você realmente necessita o LCD ativo, assegure-se de que o mesmo esteja em modo read-only. Caso contrário o PIN (default = 1234) vai ser solicitado e o atacante pode fazer coisas como adicionar um IP, rebotar e até resetar o roteador.



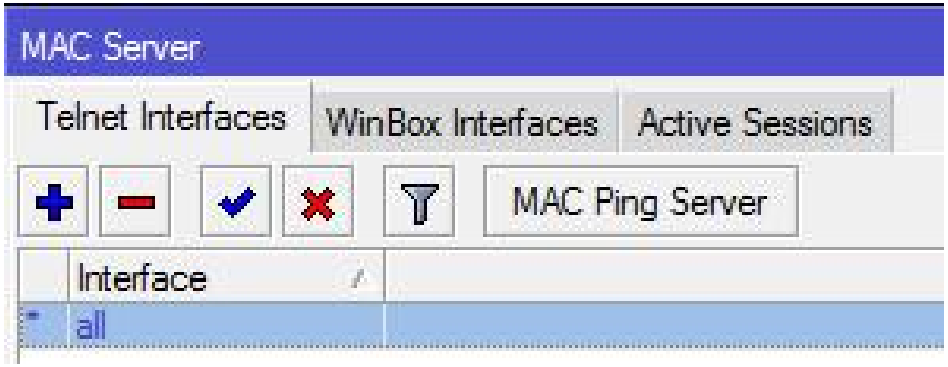


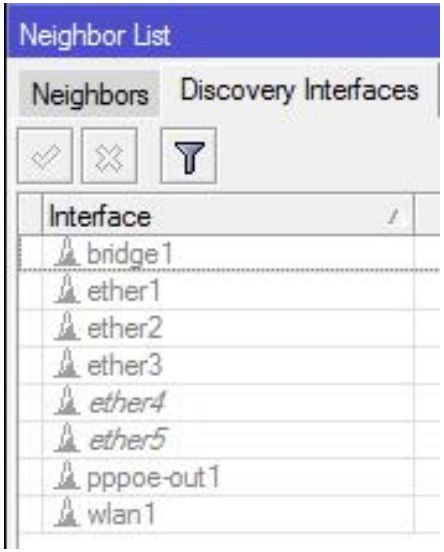
Facilidades que podem causar dificuldades...

Preferencialmente desabilitar

MAC-Server

Desabilite o MAC-Server para Telnet e Winbox sempre que possível. Se necessário, habilite somente em interfaces específicas





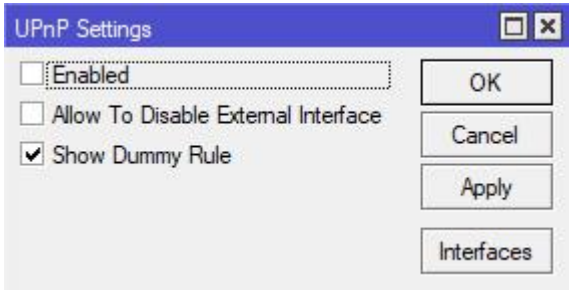
MNDP

Desabilite as interfaces de descoberta sempre que possível para evitar ataques MNDP (Equivalente ao CDP da Cisco)

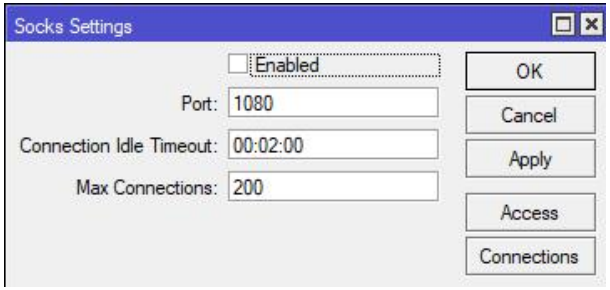
Manter desabilitados

Serviços desabilitados por padrão e que devem permanecer desabilitados:

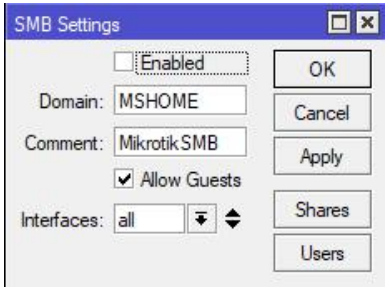
/ip upnp



/ip socks



/ip smb



Se você não tem certeza dos serviços que estão rodando em sua caixa, tente descobri-los com nmap:

```
maia@xps:~$ sudo nmap -A -T4 192.168.88.1
[sudo] password for maia:

Starting Nmap 7.01 ( https://nmap.org ) at 2017-03-29 15:22 CEST
```

Segurança de Serviços

Segurança de Serviços

Resultados do nmap

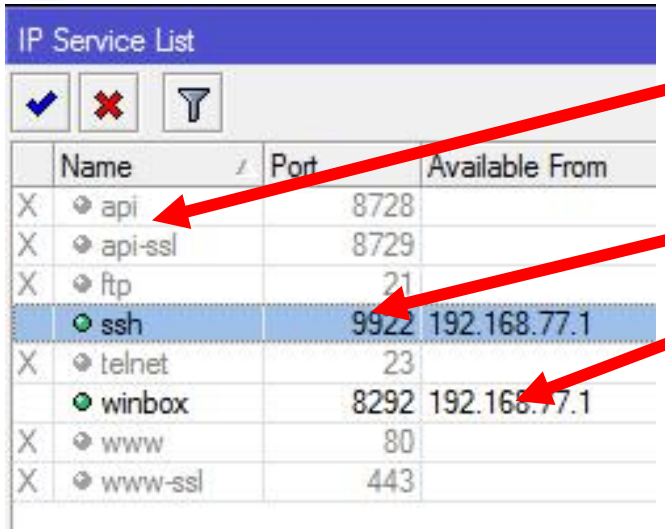
```
maia@maia-5520:~/Programs/Mikrotik-Exploit$ sudo nmap -sS -sV 192.168.1.14
[sudo] password for maia:

Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-15 21:33 -02
Nmap scan report for 192.168.1.14
Host is up (0.00065s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE        VERSION
21/tcp   open  ftp            MikroTik router ftpd 6.40.9
22/tcp   open  ssh            MikroTik RouterOS sshd (protocol 2.0)
23/tcp   open  telnet         Linux telnetd
80/tcp   open  http           MikroTik router config httpd
2000/tcp open  bandwidth-test MikroTik bandwidth-test server
8291/tcp open  unknown
MAC Address: 08:00:27:29:DE:24 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Linux, RouterOS; Device: router; CPE: cpe:/o:mikrotik:routeros, cpe:/o:linux:linux_kernel
```

Portas TCP abertas por padrão: 21, 22, 23, 80, 2000 e 8291

Segurança de Serviços

IP Services



Desabilite serviços desnecessários;

Mude as portas default;

Restrinja o acesso a determinados IPs

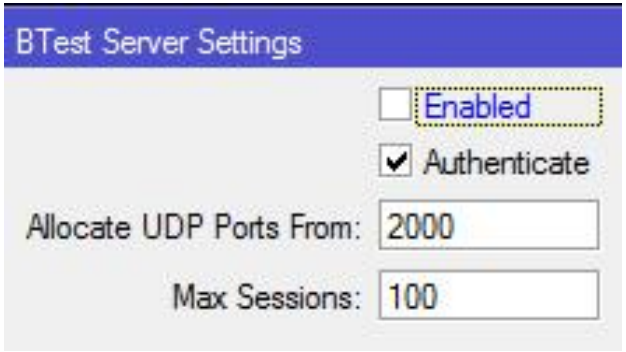
Pode parecer paranoia, mas além de restringir por IP, para serviços ativos, é importante também restringir no Firewall (ver próximo slide)

Segurança de Serviços

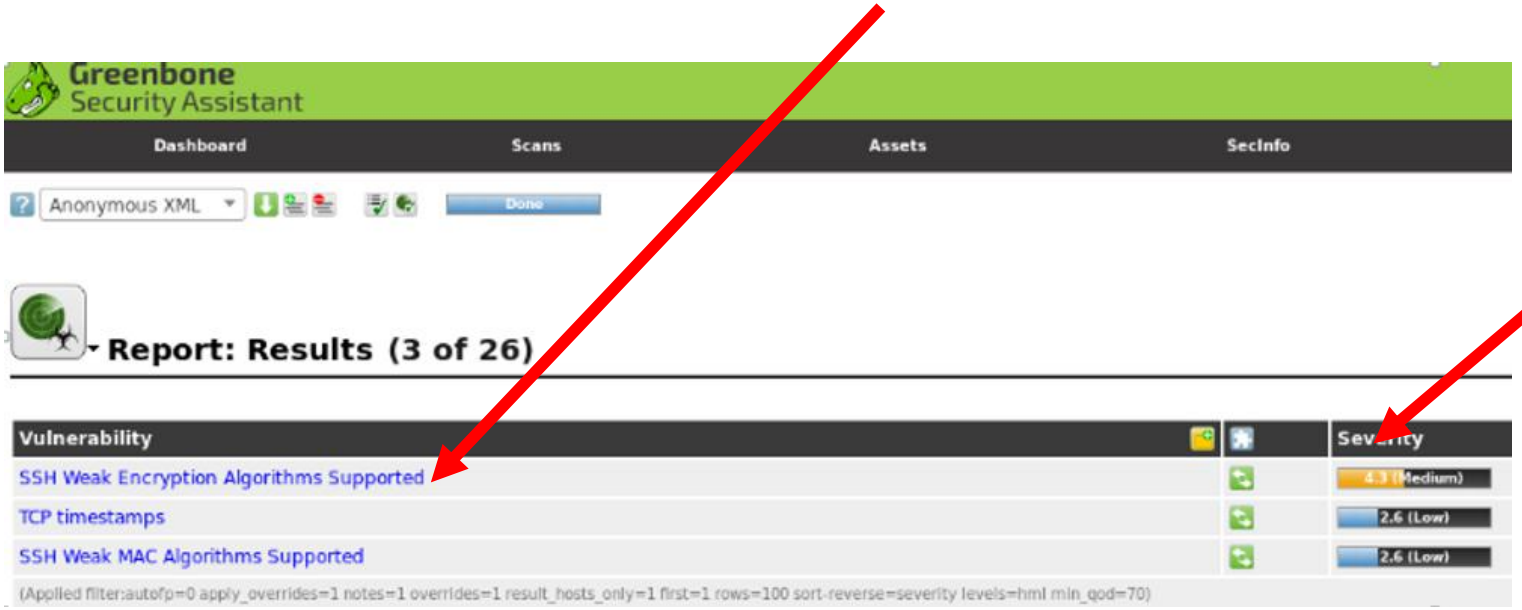
Bandwidth Test Server

Não há razão para deixar o BW-test habilitado.

Habilite-o somente quando for utilizar e volte a desabilita-lo



Resultados do OpenVAS



somente uma vulnerabilidade de severidade média

Segurança de Serviços

Habilitar Criptografia Forte

A criptografia forte é **desabilitada por padrão** (e daí a vulnerabilidade mostrada pelo OpenVAS). Sempre que as as aplicações da caixa justificarem, a criptografia forte deve ser habilitada.

```
[mdadm-ssh@AP-Maia] > ip ssh set strong-crypto=yes
[mdadm-ssh@AP-Maia] >
```

Todo canivete Suiço pode ser útil, mas se utilizado corretamente...

Um bom canivete suiço, porém com seus limites...

Dividir serviços

Embora seja atrativo, não é uma boa ideia concentrar vários serviços em uma caixa única.

- Roteador de borda é roteador de borda

- BRAS é BRAS

- Firewall é Firewall

Não culpe o seu Mikrotik por decisões equivocadas 

Links para consulta

Mum Milan 2017
https://mum.mikrotik.com/presentations/EU17/presentation_4088_1492591370.pdf

Mum Berlin 2018
https://mum.mikrotik.com/2018/EU/agenda/EN

MUM Brazil 2018
https://mum.mikrotik.com/2018/BR/agenda/EN

MUM Mexico 2019
https://mum.mikrotik.com/2019/MX/agenda/EN

Obrigado!

maia@mdbrasil.com.br