Контролирано разрешаване на достъп чрез SMS

MikroTik Net Camp 2021

Несебър

Петър Димитров

За мен - Петър Димитров

- MikroTik Trainer: от 2013 г.
- Ubiquiti Trainer: от 2018 г.
- Предлагани обучения:

Въведение в компютърните мрежи, Мониторинг с The Dude

MTCNA, MTCSWE, MTCRE, MTCINE, MTCWE,

MTCEWE, MTCTCE, MTCUME, MTCSE, MTCIPv6E

UBWS, UBWA, UBRSS, UBRSA, UNS, UEWA

Контролирано разрешаване на достъп чрез SMS, Петър Димитров

- В корпоративна среда често се налага външна фирма да достъпва за поддръжка машини в корпоративната мрежа
- От гледна точка на сигурност и контрол е уместно това да се случва чрез изрично осигуряване на временен достъп
- Често достъпа е уместно да се управлява от отговорно лице извън IT

Изисквания

- Определени мениджъри от компанията да могат да дават достъп на определени външни фирми достъп до конкретни вътрешни ресурси за определено време
- Процеса да е в две стъпки чрез SMS-и:
  - Мениджър изпраща заявка за достъп, включваща кой до какво за колко време да има достъп.
  - След извършване на необходимите проверки, ако операцията е разрешена, мениджъра получава еднократен временен код, с който чрез втори SMS потвърждава достъпа.

Подход

- Устройство с модем и SIM карта ще получава, обработва и изпраща SMS-и
- Същото устройство ще проверява дали заявките са допустими
- В случай на успешно потвърждаване на достъп, устройството ще изпълнява чрез ssh команда за добавяне на адрес (или мрежа) в адресна листа на друго устройство, което чрез firewall управлява достъпа

Необходими компоненти

- Настройка на /tool sms
- Механизъм за проверка
  - дали времето за достъп е в определен разумен интервал
  - дали номера, от който идва SMS-а, има право да дава достъп
    - на съответната външна компания
    - до съответния вътрешен ресурс
  - дали потвърждението идва от същия номер, който е поискал достъпа

Реализация

- Чрез SMS ще бъде извикван скрипт, към който ще се подават параметрите от SMS-а
- Скрипта ще прави необходимите проверки и при успех ще генерира втори скрипт, който да се извиква с втория SMS. Същевременно ще се добавя и scheduler, който да изтрие втория скрипт и себе си след определено време.
- И двата скрипта ще трият SMS-а, с който са стартирани

Реализация проверки

- Проверката за времето ще е твърдо указана в скрипта
- За лесно поддържане и управление на достъпа, правата кой може да дава достъп на кого и кой може да дава достъп до къде ще се управляват с коментари в /ip firewall address-list

Команди чрез ssh

- В документацията на MikroTik е описано как се изпълняват отдалечено команди през ssh
- На рутера, където е firewall-а и ще добавяме адреси в адресна листа, имаме потребител с вкаран публичния RSA ключ
- На рутера, обработващ SMS-ите, сме добавили двойката публичен/частен RSA ключ за ползване от потребителя, с който ще работим

Особености

- Owner на първия скрипт трябва да бъде потребителя, който разполага с RSA ключовете
- Ако редактирате скрипта с друг потребител, не забравяйте да смените след това owner-а

Настройка на инструмента SMS

```
/tool sms
set allowed-number=+359xxxxxxxxx,+359yyyyyyyyy \
port=lte1 receive-enabled=yes secret=pass
```

Основен скрипт

```
:foreach i in=[/tool sms inbox find] do={
  :local rand1 ([/tool fetch url="https://www.random.org/passwords/\?num=1&len=8&format=plain&rnd=new" output=user as-value]->"data")
  :local rand ("r" . ([:pick $rand1 1 ([:len $rand1] - 1)]))
  :local sdr [/tool sms inbox get value-name=phone $i]
  :local err 0
  :local errmsg
  :local dstaccess 0
  :local srcaccess 0
  if (($hours < 1) or ($hours > 72)) do={
    set err 1
    set errmsg "Invalid number of hours $hours - should be between 1 and 72"
    } else={
      :foreach j in=[/ip firewall address-list find] do={
        if  (([/ip firewall address-list get value-name=list $j] = ($dst . "-access")) and ([:find [/ip firewall address-list get value-name=comment $j]  $sdr -1] > 0)) do={set dstaccess 1}
      }
      if ($dstaccess = 1) do={
        :foreach j in=[/ip firewall address-list find] do={
          if  (([/ip firewall address-list get value-name=list $j] = $src) and ([:find [/ip firewall address-list get value-name=comment $j]  $sdr -1] > 0)) do={set srcaccess 1}
        }
        if ($srcaccess = 1) do={
            :log info message="$sdr requested access from $src to $dst for $hours hours."
          } else={
          set err 1
          set errmsg "$sdr has no permission to grant access from $src"
          }
        } else={
        set err 1
        set errmsg "$sdr has no permission to grant access to $dst"
        }
    }
```

Основен скрипт

```
if ($err = 0) do={
    /system script add name=$rand dont-require-permissions=yes source=":local phone \"$sdr\"\r\
      \n:local rand $rand\r\
      \n:local asrc [/ip firewall address-list get value-name=address [find list=$src]]\r\
      \n:local adst (\"$dst\" . \"-access\")\r\
      \n:local asecs ($hours * 3600)\r\
      \n:local sdr [/tool sms inbox get value-name=phone [find message~\"$rand\"]]\r\
      \nif (\$sdr = \$phone) do={\r\
      \n:log info message=(\$phone . \" granted access from \" . \$asrc .\" to \" . \$adst . \" for \" . \$asecs .\" seconds.\")\r\
      \n:local acmd \"/ip firewall address-list add address=\$asrc list=\$adst timeout=\$asecs\"\r\
      \n:log info message=(\"executing command: \" . \$acmd)\r\
      \n/system ssh-exec address=192.168.100.254 user=admin command=\$acmd
      \n/tool sms send lte1 phone-number=\$phone message=\"Access granted.\"
      \n} else={:log warning message=(\"Access requested by \" . \$phone . \" but \" . \$sdr .\" tried to give it!\")}\r\
      \n/tool sms inbox remove [find phone=\$sdr]"
    /system scheduler add name=("remove" . $rand) start-date=[/system clock get date] start-time=([/system clock get time] +10m) on-event=("/system script remove " . $rand . "\r\
      \n/system scheduler remove remove". $rand)
    :log info message=("phone-number=" . $sdr . "message=" . $rand)
    /tool sms send lte1 phone-number=$sdr message=$rand
    } else={
    :log warning message=$errmsg
    /tool sms send lte1 phone-number=$sdr message=$errmsg
    }
  /tool sms inbox remove $i
}
```

Конфигурация в адресни листи

```
/ip firewall address-list
add address=0.0.0.1 comment="Petar Dimitrov +359xxxxxxxxx, \
Someone Else +359yyyyyyyyy" list=printer-access
add address=0.0.0.1 comment="Petar Dimitrov +359xxxxxxxxx" \
list=video-access
add address=0.0.0.1 comment="Someone Else +359yyyyyyyyy" \
list=coffee-access
add address=192.168.100.101 comment="Petar Dimitrov +359xxxxxxxxx, \
Someone Else +359yyyyyyyyy" list=firma1
add address=192.168.100.102 comment="Petar Dimitrov +359xxxxxxxxx" \
list=firma2
add address=192.168.100.103 comment="Someone Else +359yyyyyyyyy" \
list=firma3
```

Формат на SMS-и

- Първи SMS:

  :cmd pass script accctrl src=firma1 dst=printer hours=4

- Втори SMS:

  :cmd pass script получен-код

Време е за тестове!

Благодаря за вниманието!