Wrocław, 08.12.2020

Bezpieczeństwo sieci komputerowych

Laboratorium 5

Bezpieczeństwo infrastruktury sieciowej

Prowadzący: dr inż. Marcin Markowski

Autorka: Agnieszka Płoszaj 218353

Zadanie zostało wykonane przy wykorzystaniu komputera z systemem windows 10 i programu *Cisco Packet Tracer 7.3.1*.

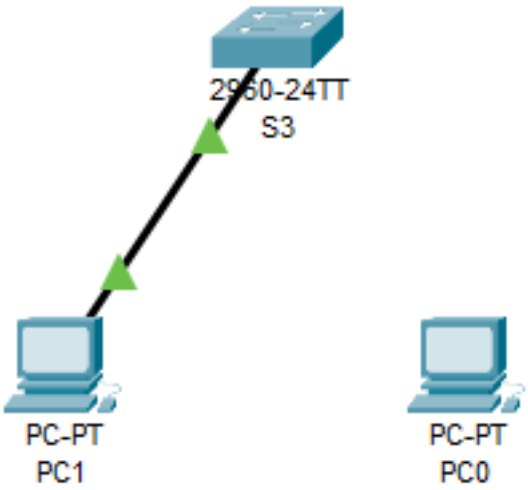
Zadanie 1

Na początek został skonfigurowany mechanizm bezpieczeństwa na porcie fa0/5:
int fastethernet 0/5
switchport mode access
switchport port-security.
Określenie liczby uprawnionych adresów MAC dla portu:
switchport port-security maximum 1.
Konfiguracja 'lepka', czyli pierwszy adres jaki pojawi się na porcie zostanie zapisany i zapamiętany:
switchport port-security mac-address sticky.
Określenie sposobu reakcji na przekroczenie limitu (w tym przypadku wyłączenie portu):
switchport port-security violation shutdown.

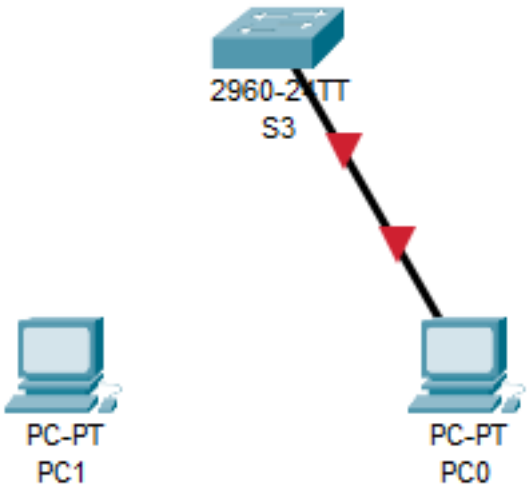
Użycie wszystkich powyższych poleceń zostało pokazane na ilustracji 1. Topologia do zadania 1 została przedstawiona na ilustracji 2 oraz 3. Na ilustracji 2 została pokazana topologia po konfiguracji i podłączeniu pierwszego komputera, natomiast ilustracja 3 pokazuje topologię po podłączeniu drugiego komputera.
Ilustracja 4 przedstawia konfigurację portu po podłączeniu pierwszego komputera.
Ilustracja 5 przedstawia konfigurację portu po podłączeniu drugiego komputera. Reakcja przełącznika jest zgodna z oczekiwaniami (oraz określeniem sposobu reakcji na przekroczenie limitu jednego adresu MAC). Port został wyłączony.

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S3
S3(config)#int fastethernet 0/5
S3(config-if)#switchport mode access
S3(config-if)#switchport port-security
S3(config-if)#switchport port-security maximum 1
S3(config-if)#switchport port-security mac-address sticky
S3(config-if)#switchport port-security violation shutdown
```

Ilustracja 1 Konfiguracja portu fa0/5



Ilustracja 2 Topologia – komputer 1



Ilustracja 3 Topologia – komputer 2

```
S3#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)         (Count)
-----------------------------------------------------------------------
        Fa0/5         1           1                  0          Shutdown
-----------------------------------------------------------------------
S3#show port-security int fa0/5
Port Security               : Enabled
Port Status                 : Secure-up
Violation Mode              : Shutdown
Aging Time                  : 0 mins
Aging Type                  : Absolute
SecureStatic Address Aging  : Disabled
Maximum MAC Addresses       : 1
Total MAC Addresses         : 1
Configured MAC Addresses    : 0
Sticky MAC Addresses        : 1
Last Source Address:Vlan    : 0090.0C59.B656:1
Security Violation Count    : 0
```

Ilustracja 4 Konfiguracja portu po podłączeniu pierwszego komputera

```
S3#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
-----------------------------------------------------------------------
        Fa0/5        1           1                  1          Shutdown
-----------------------------------------------------------------------
S3#show port-security int fa0/5
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0001.972C.195C:1
Security Violation Count   : 1
```

Ilustracja 5 Konfiguracja portu po podłączeniu drugiego komputera

Zadanie 2

Na początek został skonfigurowany router (poprzez utworzenie 2 kont użytkowników z hasłem niezabezpieczonym (ilustracja 6) oraz konfigurację interfejsów sieciowych (ilustracja 7))
Następnie został skonfigurowany dostęp do urządzenia. Na początek wyłączono dostęp przez nie używane linie, a następnie umożliwiono dostęp przez telnet. Niestety nie można było utworzyć bezpiecznego hasła (md5) (co zostało pokazane na ilustracji 8). Aktualna topologia została pokazana na ilustracji 9.

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R3
R3(config)#username ploszaj password agnieszka
R3(config)#username ap password 218353
```

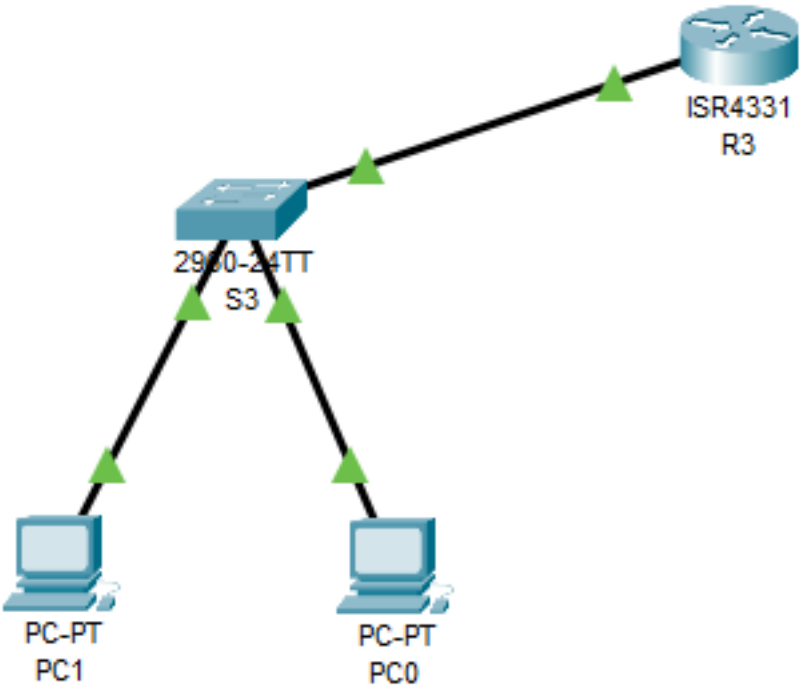
Ilustracja 6 Utworzenie 2 kont użytkowników

```
R3(config)#int g0/0/0
R3(config-if)#ip address 192.168.3.1 255.255.255.0
R3(config-if)#no shut

R3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up
```

Ilustracja 7 Konfiguracja interfejsu sieciowego

```
R3(config)#line aux 0
R3(config-line)#no password
R3(config-line)#login
% Login disabled on line 0, until 'password' is set
R3(config-line)#exit
R3(config)#line vty 0 4
R3(config-line)#no transport input
R3(config-line)#transport input telnet
R3(config-line)#secret agnieszka
                   ^
% Invalid input detected at '^' marker.

R3(config-line)#?
Virtual Line configuration commands:
  access-class   Filter connections based on an IP access list
  accounting     Accounting parameters
  databits       Set number of data bits per character
  exec-timeout   Set the EXEC timeout
  exit           Exit from line configuration mode
  flowcontrol    Set the flow control
  history        Enable and control the command history function
  ipv6           IPv6 options
  logging        Modify message logging facilities
  login          Enable password checking
  motd-banner    Enable the display of the MOTD banner
  no             Negate a command or set its defaults
  parity         Set terminal parity
  password       Set a password
  privilege      Change privilege level for line
  session-limit  Set maximum number of sessions
  speed          Set the transmit and receive speeds
  stopbits       Set async line stop bits
  transport      Define transport protocols for line
R3(config-line)#password agnieszka
R3(config-line)#login
```

Ilustracja 8 Konfiguracja dostępu do urządzenia



Ilustracja 9 Topologia

Następnie przy pomocy polecenia
show run
zostały wyświetlone hasła (ilustracja 10). Hasła zostały zapisane jawnym tekstem. Włączono więc proste szyfrowanie haseł, poprzez użycie polecenia
service password-encryption
(Ilustracja 11) i ponownie użyto polecenia
show run.
Jak można zaobserwować na ilustracji 12, hasła nie są już podawane jawnym tekstem.

```
username ap password 0 218353
username ploszaj password 0 agnieszka
.
        line aux 0
         login
        !
        line vty 0 4
         password agnieszka
         login
         transport input telnet
```

Ilustracja 10 Hasła – tekst jawny

```
R3#
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#service password-encryption
```

Ilustracja 11 Proste szyfrowanie haseł

```
username ap password 7 08731D165A4C56
username ploszaj password 7 08204B40001C160D190A
        line aux 0
         login
        !
        line vty 0 4
         password 7 08204B40001C160D190A
         login
         transport input telnet
```

Ilustracja 12 Hasła – zaszyfrowane

W następnej kolejności został skonfigurowany dostęp do routera wyłącznie przez ssh (ilustracja 13) poprzez przypisanie domeny
ip domain-name agnieszka.local,
wygenerowanie klucza RSA o długości 512
crypto key generate rsa,
zablokowanie wszystkich protokołów
no transport protocol
oraz umożliwienie dostępu przez ssh
transport input ssh
Następnie zostało utworzone nowe konto użytkownika z hasłem zabezpieczonym przez MD5 (ilustracja 14) i przy pomocy polecenia show run wyświetlone hasło (ilustracja 15).

```
R3#
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ip domain-name agnieszka.local
R3(config)#crypto key generate rsa
% You already have RSA keys defined named R3.agnieszka.local .
% Do you really want to replace them? [yes/no]: yes
The name for the keys will be: R3.agnieszka.local
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 512
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]
```

Ilustracja 13 Przypisanie domeny oraz wygenerowanie klucza RSA

```
R3(config)#username aploszaj secret pagnieszka
```

Ilustracja 14 Utworzenie konta użytkownika

```
username ap password 7 08731D165A4C56
username aploszaj secret 5 $1$mERr$yqEjzLMzRYD5i//URp6gL.
username ploszaj password 7 08204B40001C160D190A
!
line aux 0
 login
!
line vty 0 4
 password 7 08204B40001C160D190A
 login local
 transport input ssh
```

Ilustracja 15 Hasła – zaszyfrowane

Zadanie 3

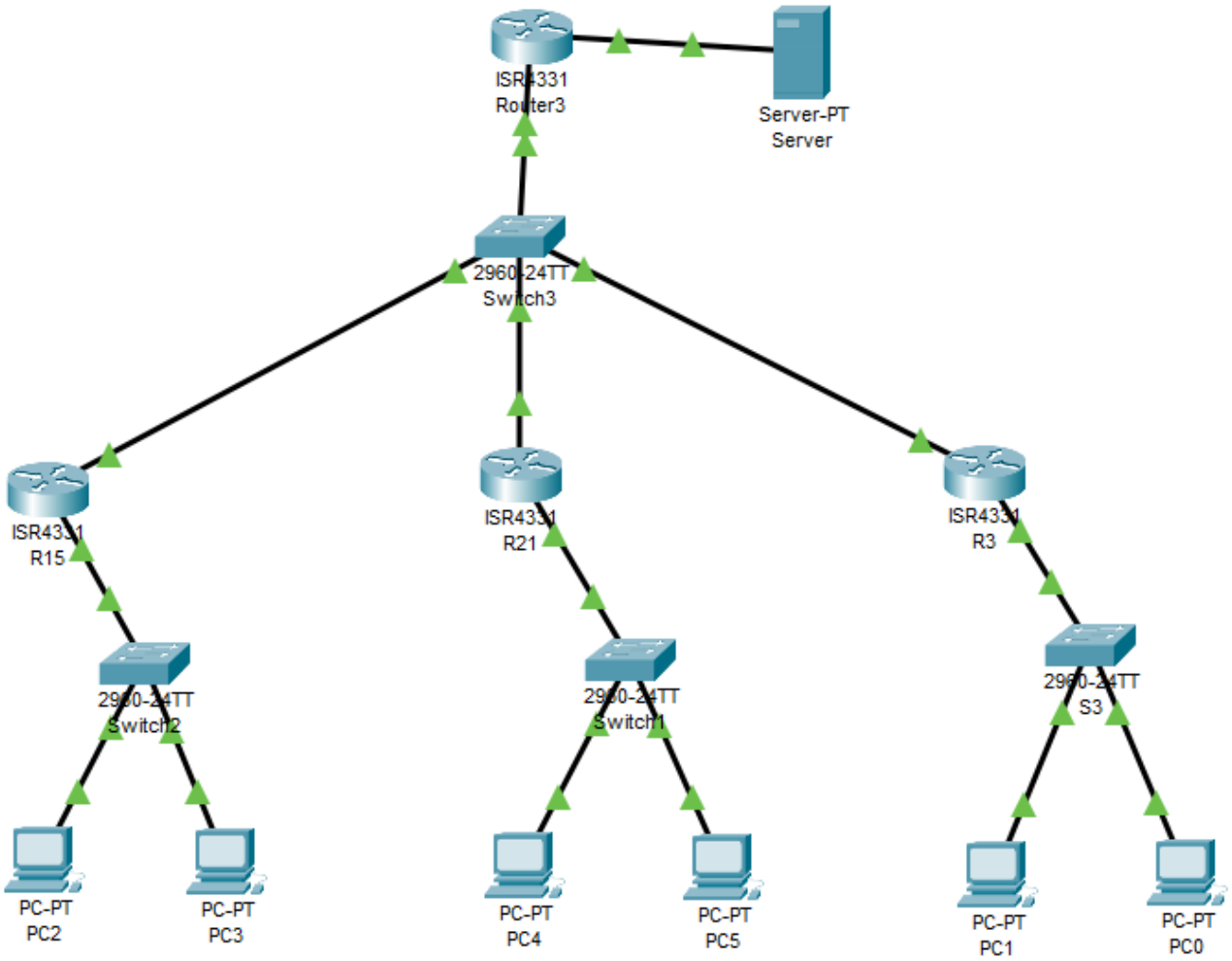
Na początek została skonfigurowana topologia (ilustracja 18). Zostały skonfigurowane interfejsy zgodnie z adresami w instrukcji (ilustracja 16 i 17). Następnie został skonfigurowany routing (RIP) (ilustracja 19). W następnej kolejności został skonfigurowany passive-interface oraz uwierzytelnienie routingu początkowo na routerze „głównym", a następnie na R21 oraz R3 (na początku poprzez RIP, jednak z powodu braku „ip rip" (ilustracja 20) poprzez OSPF (ilustracja 21 i 22)). Niestety routery nie otrzymują informacji o trasie do serwera oraz pozostałych routerów. Na ilustracjach 23 oraz 24 zostały pokazane fragmenty wyników polecenia show run. Na ilustracji 25 został pokazany wynik polecenia *tracert* z PC2 (wynik *traceout* z routera R15 został pokazany na ilustracji 26).

```
Router(config)#int g0/0/1
Router(config-if)#ip address 192.168.15.3 255.255.255.0
```

Ilustracja 16 Interfejs zewnętrzny routera R15

```
Router(config)#int g0/0/1
Router(config-if)#ip address 192.168.21.3 255.255.255.0
```

Ilustracja 17 Interfejs zewnętrzny routera R21



Ilustracja 18 Topologia

```
Router(config)#route rip
Router(config-router)#version 2
Router(config-router)#network 10.10.15.0
Router(config-router)#version 2
Router(config-router)#network 192.168.3.0
Router(config-router)#network 192.168.15.0 255.255.255.0
                                           ^
% Invalid input detected at '^' marker.

Router(config-router)#network 192.168.21.0
```

Ilustracja 19 RIP

```
Router(config-if)#ip rip authentication mode md5
                  ^
% Invalid input detected at '^' marker.
```

Ilustracja 20 ip rip

```
Router(config-router)#network 192.168.3.0 255.255.255.0 area 10
Router(config-router)#network 192.168.15.0 255.255.255.0 area 10
Router(config-router)#network 192.168.21.0 255.255.255.0 area 10
Router(config-router)#passive-interface g0/0/1
```

Ilustracja 21 ospf

```
Router(config)#int g0/0/0
Router(config-if)#ip ospf authentication message-digest
Router(config-if)#ip ospf message-digest-key 1 md5 ploszaj
Router(config-if)#exit
```

Ilustracja 22 ospf

```
key chain KLUCZ_RIP
 key 1
  key-string ploszaj
!
interface GigabitEthernet0/0/0
 ip address 10.10.15.3 255.255.255.0
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 ploszaj
 duplex auto
 speed auto
```

Ilustracja 23 show run

```
router ospf 10
 log-adjacency-changes
 passive-interface GigabitEthernet0/0/1
 network 192.168.3.0 0.0.0.255 area 10
 network 192.168.15.0 0.0.0.255 area 10
 network 192.168.21.0 0.0.0.255 area 10
 network 10.10.15.0 0.0.0.255 area 10
!
router rip
 version 2
 passive-interface GigabitEthernet0/0/1
 network 10.0.0.0
 network 192.168.3.0
 network 192.168.15.0
 network 192.168.21.0
```

Ilustracja 24 show run

```
C:\>tracert 10.10.15.3

Tracing route to 10.10.15.3 over a maximum of 30 hops:

  1    *        *        *        Request timed out.
  2    *        *        *        Request timed out.
  3    *        *        *        Request timed out.
```

Ilustracja 25 tracert

```
R15#tracerout 10.10.15.3
Type escape sequence to abort.
Tracing the route to 10.10.15.3

  1    *      *      *
  2    *      *      *
  3    *      *      *
  4    *      *      *
```

Ilustracja 26 tracerout

Na koniec wykonano komendę
auto secure.
Jak można zobaczyć na ilustracji 27, po pokazaniu szeregu informacji odnośnie działania powyższej komendy następuje pytanie czy router jest podłączony do internetu. W pierwszym przypadku wybrano opcję „tak” i jak widać, następnym krokiem byłby wybór interfejsu podłączonego do internetu. W drugim przypadku wybrano opcję „nie” i na ilustracji 28 przedstawiono fragment odpowiadający wyłączonym i włączonym usługom.

```
Router#auto secure

                         --- AutoSecure Configuration ---
*** AutoSecure configuration enhances the security of
the router, but it will not make it absolutely resistant
to all security attacks ***

AutoSecure will modify the configuration of your device.
All configuration changes will be shown. For a detailed
explanation of how the configuration changes enhance security
and any possible side effects, please refer to Cisco.com for
Autosecure documentation.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.

Gathering information about the router for AutoSecure

Is this router connected to internet? [no]: yes
Enter the number of interfaces facing the internet [1]: 1
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   10.10.15.3      YES manual up                    up
GigabitEthernet0/0/1   unassigned      YES unset  up                    up
GigabitEthernet0/0/2   unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
```

Ilustracja 27 auto secure

```
Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol

Disabling the bootp server
Disabling the http server
Disabling the finger service
Disabling source routing
Disabling gratuitous arp
```

Ilustracja 28 auto secure