

Министерство образования Республики Беларусь
Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет инфокоммуникаций
Кафедра защиты информации

Практическая работа №5
«Уязвимости удаленного доступа к настройкам сетевого
оборудования. Протокол AAA»
Шифр 672

Проверила:
Белоусова Е.С.

Выполнила:
ст. гр. 961401
Акулова П.Г..

Минск 2022

Цель: проанализировать уязвимости удаленного доступа к настройкам сетевого оборудования посредством Telnet и SSH соединения, изучить способы подключения sniffера к сети и его использования для перехвата трафика; изучить процессы протокола AAA, овладеть навыками конфигурации аутентификации, авторизации и учета удаленного доступа пользователей к сетевому оборудованию по SSH-соединению.

1. Исходные данные для смоделированной сети

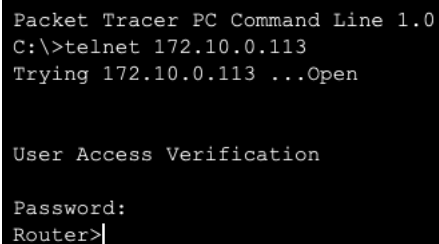
Вторая цифра	Пароль для подключения	Номер сессии	Имя домена	Число попыток SSH соединения	Время ожидания SSH соединения
7	1010	7	Citadel	5	25

2. Настройка консольного и Telnet подключения на Router0

Router0:

```
line con 0
  exec-timeout 60 0
  password 1010
  login
!
line aux 0
!
line vty 0 4
  exec-timeout 60 0
  password 1010
  login
line vty 5 15
  exec-timeout 60 0
  password 1010
  login
.
```

Подключение с PC15:



```
Packet Tracer PC Command Line 1.0
C:\>telnet 172.10.0.113
Trying 172.10.0.113 ...Open

User Access Verification

Password:
Router>
```

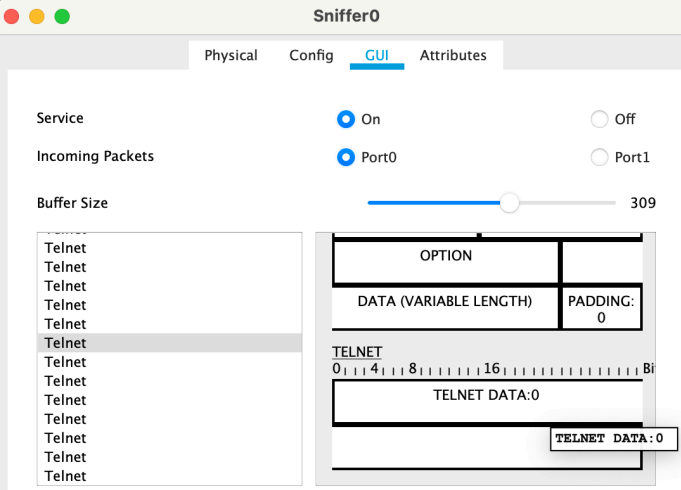
3. Настройка SPAN

Switch3:

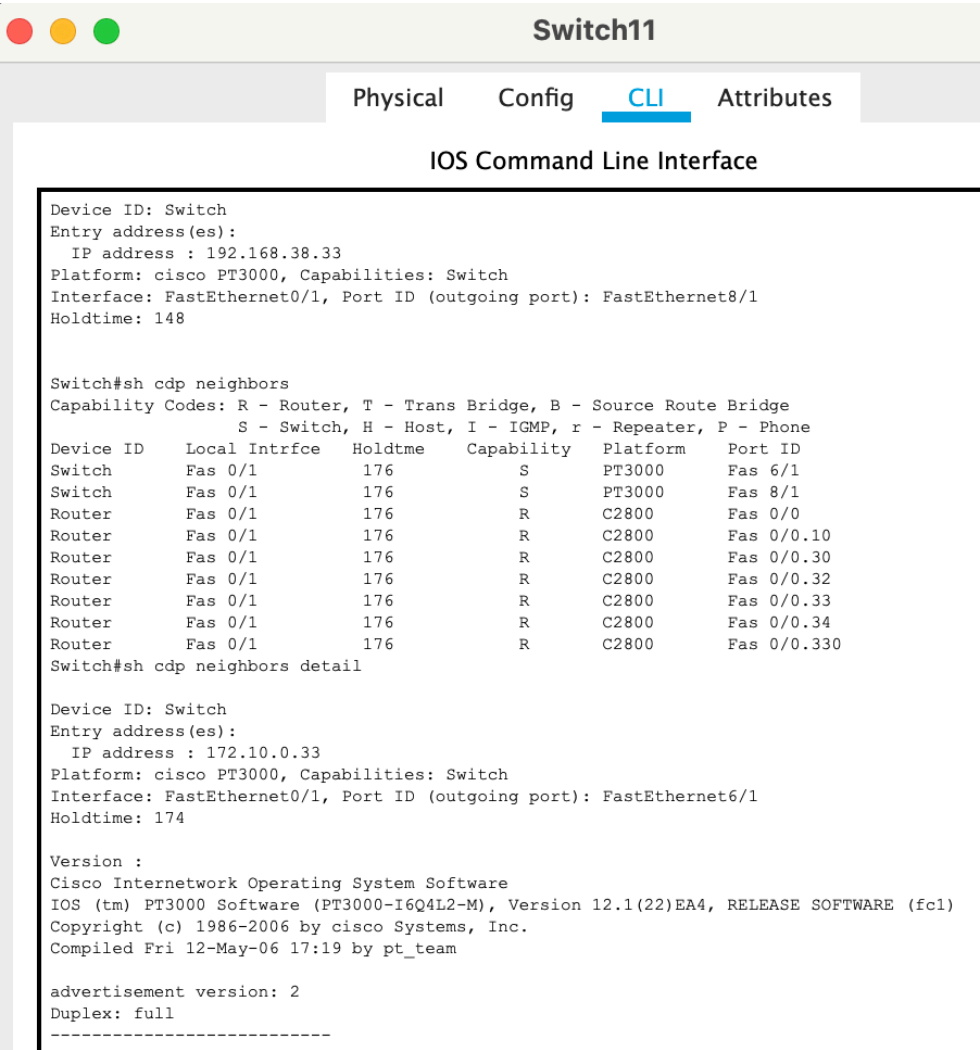
4.Перехват пароля при подключении с помощью Telnet

5.Уязвимости CDP протокола

Перехват CDP пакетов:



Switch11(атакующий):



6. Настройка шифрования паролей на маршрутизаторе

```
Router(config)#enable password 10101
Router(config)#enable secret 1010
Router(config)#service password-encryption
```

```
enable secret 5 $1$mERr$Nn1WTu2B8cY1oM2PIytzT.  
enable password 7 08701C1F5948
```

Type 7 Password: 08701C1F5948

Crack Password

Plain text: 10101

Усиление пароля:

```
Router(config)#enable password 10101672
Router(config)#enable secret 1010672
Router(config)#service password-encryption
```

```
enable secret 5 $1$mERr$Qb1latydRVXs2cQR8pX.8.
enable password 7 08701C1F5948534040
```

Type 7 Password: 08701C1F5948534040

Crack Password

Plain text: 10101672

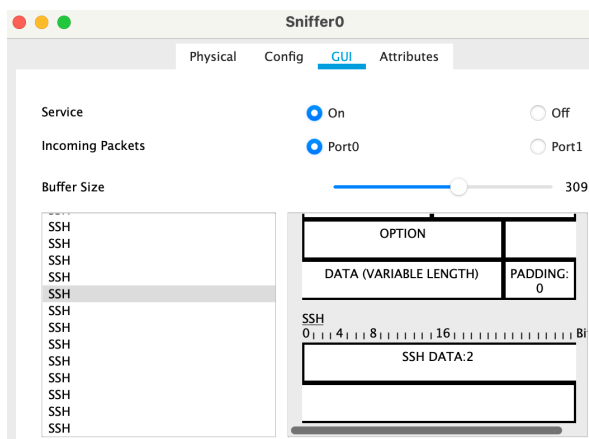
7. Настройка SSH

Добавление нового пользователя:

```
Router(config)#username Admin privilege 15 secret 1010672
Router(config)#username Engineer privilege 5 secret 1010672
Router(config)#username Operator privilege 3 secret 1010672
```

Проверка SSH соединения (PC15):

```
C:\>ssh -l Admin 172.10.0.113
Password:
Router0#
```



8. Настройка SSH на Router3 с помощью RADIUS Router3: 172.10.0.137

```
Router(config)#hostname Router3
Router3(config)#ip domain-name
Router3(config)#ip domain-name Building1
Router3(config)#cry
Router3(config)#crypto k
Router3(config)#crypto key g
Router3(config)#crypto key generate rsa
The name for the keys will be: Router3.Building1
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]: 768
% Generating 768 bit RSA keys, keys will be non-exportable...[OK]
```

```
Router3(config)#ip ssh ver
*Mar 1 0:3:11.930: %SSH-5-ENABLED: SSH 1.99 has been enabled
Router3(config)#ip ssh version 2
Router3(config)#aaa new
Router3(config)#aaa new-model
Router3(config)#rad
Router3(config)#radius-server
Router3(config)#radius-server h
Router3(config)#radius-server host 172.10.0.138 key 1010672
Router3(config)#aaa authent
Router3(config)#aaa authentication 1
Router3(config)#aaa authentication login ssh group r
Router3(config)#aaa authentication login ssh group radius
Router3(config)#line vty 0 15
Router3(config-line)#tr
Router3(config-line)#transport i
Router3(config-line)#transport input ssh
Router3(config-line)#l
Router3(config-line)#log
Router3(config-line)#login authent
Router3(config-line)#login authentication ssh
Router3(config-line)#do wr
Building configuration...
[OK]
Router3(config-line)#exit
Router3(config)#aaa authori
Router3(config)#aaa authorization exec ssh group radius local
Router3(config)#line vty 0 15
Router3(config-line)#accou
Router3(config-line)#accounting exec ssh
Router3(config-line)#exit
Router3(config)#aaa acc
Router3(config)#aaa accounting exec ssh star
Router3(config)#aaa accounting exec ssh start-stop gr
Router3(config)#aaa accounting exec ssh start-stop group radi
Router3(config)#aaa accounting exec ssh start-stop group radius
Router3(config)#aaa accounting exec console star
Router3(config)#aaa accounting exec console start-stop group rad
Router3(config)#aaa accounting exec console start-stop group radius
```

Проверка подключения

```
Packet Tracer PC Command Line 1.0
C:\>ssh -l Akulova1 172.10.0.137

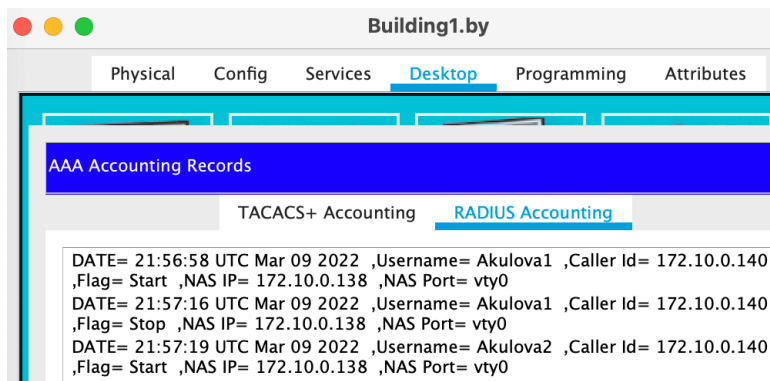
Password:
Router3>exi

[Connection to 172.10.0.137 closed by foreign host]
C:\>ssh -l Akulova2 172.10.0.137

Password:
Router3>|
```

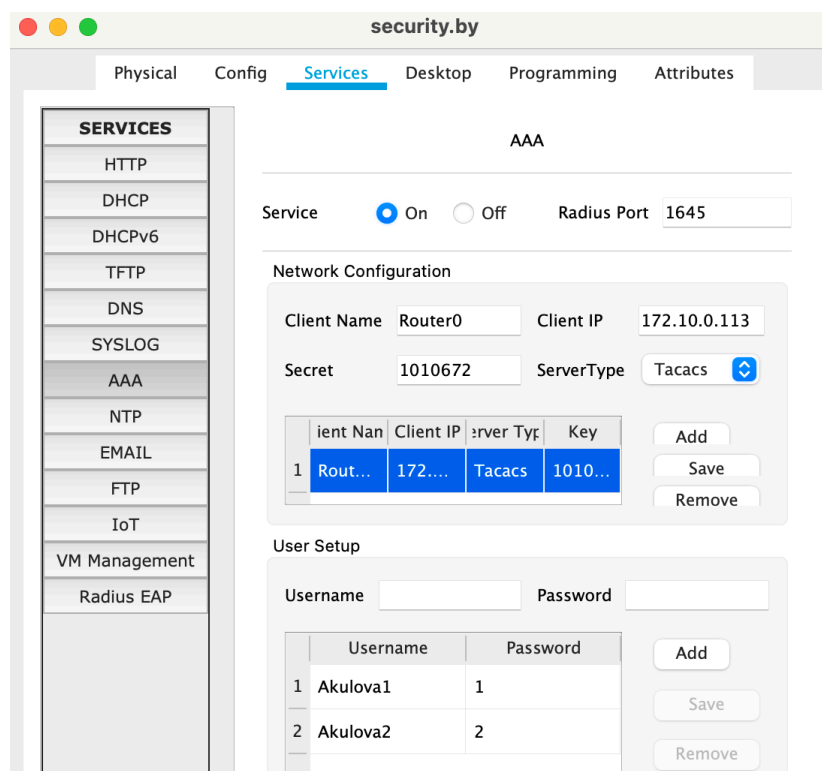
The screenshot shows the Packet Tracer Sniffer1 GUI. The 'GUI' tab is selected. The 'Service' is set to 'On' and 'Incoming Packets' is set to 'Port0'. The 'Buffer Size' is set to 00. The packet list on the left shows a RADIUS packet. The packet details on the right show the following fields:

IP			
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 Bits			
VER:4	IHL:5	DSCP:0x00	TL:29
ID:0x000c		FLAGS:0x0	FRAG OFFSET:0x000
TTL:128	PRO:0x11	CHKSUM	
SRC IP:172.10.0.138			
DST IP:172.10.0.137			
DATA (VARIABLE LENGTH)			



9. Настройка SSH на Router0 с помощью TACACS

Router0: 172.10.0.113



Вывод: в ходе выполнения практической работы были изучены различные способы дистанционного доступа к среде интерфейса командной строки: консольное подключение, telnet и SSH, осуществлен перехват информации в сети через снифферы, осуществлена защита подключения через пароли, шифрование паролей, настройка SSH через RADIUS и TACACS-сервера, SSH оказался намного более безопасным способом доступа чем telnet, т.к. сообщения SSH не показывают пароли доступа.

