

1)

```
root@AAA-1:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.18 netmask 255.255.255.0 broadcast 0.0.0.0
    inet6 fe80::42:90ff:fe39:c100 prefixlen 64 scopeid 0x20<link>
    ether 06:23:66:15:aa:04 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 656 (656.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

2)

```
root@AAA-1:~# netstat -anu
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp      0      0 127.0.0.1:18120         0.0.0.0:*
udp      0      0 0.0.0.0:1812          0.0.0.0:*
udp      0      0 0.0.0.0:1813          0.0.0.0:*
udp      0      0 0.0.0.0:56089         0.0.0.0:*
udp6     0      0 :::54648              :::*
udp6     0      0 :::1812               :::*
udp6     0      0 :::1813               :::*
root@AAA-1:~# netstat -anu | grep -E "1812|1813"
udp      0      0 127.0.0.1:18120         0.0.0.0:*
udp      0      0 0.0.0.0:1812          0.0.0.0:*
udp      0      0 0.0.0.0:1813          0.0.0.0:*
udp6     0      0 :::1812               :::*
udp6     0      0 :::1813               :::*
```

Na imagem em cima pode-se visualizar os Sockets UDP ativos e depois filtrei pelos serviços Radius (porta 1812) e Radius-acct (porta 1813).

3)

```
root@AAA-1:~# service --status-all
[ + ] freeradius
[ ? ] hwclock.sh
[ - ] procps
[ + ] tacacs_plus
root@AAA-1:~# uname -a
Linux AAA-1 5.15.0-130-generic #140~20.04.1-Ubuntu SMP Wed Dec 18 21:35:34 UTC 2024 x86_64
x86_64 x86_64 GNU/Linux
```

```

root@AAA-1:~# ls -l /etc/freeradius
total 4
drwxr-xr-x 9 freerad freerad 4096 Apr  3 15:34 3.0
root@AAA-1:~# ls -l /etc/freeradius/3.0
total 144
-rw-r----- 1 freerad freerad 20807 Apr 17 2019 README.rst
drwxr-xr-x 2 freerad freerad 4096 Apr  3 15:34 certs
-rw-r--r-- 1 freerad freerad 7689 Jan  1 1970 clients.conf
-rw-r----- 1 freerad freerad 1440 Apr 17 2019 dictionary
-rw-r----- 1 freerad freerad 2661 Apr 17 2019 experimental.conf
lrwxrwxrwx 1 freerad freerad 28 Apr  3 15:35 hints -> mods-config/preprocess/hints
lrwxrwxrwx 1 freerad freerad 33 Apr  3 15:35 huntgroups -> mods-config/preprocess/huntgroups
drwxr-xr-x 2 freerad freerad 4096 Apr  3 15:34 mods-available
drwxr-xr-x 9 freerad freerad 4096 Apr  3 15:34 mods-config
drwxr-xr-x 2 freerad freerad 4096 Apr  3 15:34 mods-enabled
-rw-r----- 1 freerad freerad 52 Apr 17 2019 panic.gdb
drwxr-xr-x 2 freerad freerad 4096 Apr  3 15:34 policy.d
-rw-r----- 1 freerad freerad 28361 Apr 17 2019 proxy.conf
-rw-r----- 1 freerad freerad 26897 Apr 17 2019 radiusd.conf
drwxr-xr-x 2 freerad freerad 4096 Apr  3 15:34 sites-available
drwxr-xr-x 2 freerad freerad 4096 Apr  3 15:34 sites-enabled
-rw-r----- 1 freerad freerad 3470 Apr 17 2019 templates.conf
-rw-r----- 1 freerad freerad 8536 Apr 17 2019 trigger.conf
lrwxrwxrwx 1 freerad freerad 27 Apr  3 15:35 users -> mods-config/files/authorize
root@AAA-1:~# █

```

Como se pode verificar na imagem acima, está presente o ficheiro users, ou seja, onde estão guardadas as contas dos utilizadores autenticados pelo Radius, como é o caso do bob e da alice.

<https://lycansec.wordpress.com/2020/05/15/instalando-um-servidor-radius-v3-no-linux-para-testes-simples-de-redes-enterprise/>

```

GNU nano 2.9.3 /etc/
alice    Cleartext-Password := "gns3"
        Reply-Message = "Hello, %{User-Name}"

bob      Cleartext-Password := "gns3"
        Reply-Message = "Hello, %{User-Name}"

dantunes Cleartext-Password := "segurancap5"
        Reply-Message = "Hello, %{User-Name}, Autenticacao bem sucedida!!" █

```

4)

```

client R1-6615{
    ipaddr = 192.168.100.250
    secret = radiuspass
    shortname = R1-6615
}
█

```

5)

```
R1-6615#debug aaa authentication
AAA Authentication debugging is on
R1-6615#debug aaa authorization
AAA Authorization debugging is on
R1-6615#debug aaa accounting
AAA Accounting debugging is on
R1-6615#terminal monitor
% Console already monitors
R1-6615#
```

6)

```
R1-6615(config)#username diogo secret utilizadorlocal
R1-6615(config)#
R1-6615(config)#radius server radius1
R1-6615(config-radius-server)#$4 192.168.100.18 auth-port 1812 acct-port 1813
R1-6615(config-radius-server)#key radiuspass
R1-6615(config-radius-server)#exit
R1-6615(config)#aaa authentication login default group radius local
R1-6615(config)#
R1-6615(config-line)#line con 0
R1-6615(config-line)#privilege level 15
R1-6615(config-line)#
line vty 0 4
password 7 095F4B0E0C17161C080D053F27253B
transport input telnet ssh
!
```

1	0.000000	-	06:23:66:15:aa:f1	06:23:66:15:aa:f1	LOOP	60 Reply
2	1.334206	-	192.168.100.250	192.168.100.18	RADIUS	102 Access-Request id=5
3	2.335694	-	192.168.100.18	192.168.100.250	RADIUS	109 Access-Reject id=5
4	6.371715	-	192.168.100.250	192.168.100.18	RADIUS	102 Access-Request id=5, Duplicate Request
5	7.372253	-	192.168.100.18	192.168.100.250	RADIUS	109 Access-Reject id=5, Duplicate Response
6	7.557132	-	06:23:66:15:aa:04	06:23:66:15:aa:f1	ARP	42 Who has 192.168.100.250? Tell 192.168.100.18
7	7.564084	-	06:23:66:15:aa:f1	06:23:66:15:aa:04	ARP	60 192.168.100.250 is at 06:23:66:15:aa:f1
8	9.994338	-	06:23:66:15:aa:f1	06:23:66:15:aa:f1	LOOP	60 Reply
9	11.416703	-	192.168.100.250	192.168.100.18	RADIUS	102 Access-Request id=5, Duplicate Request
10	12.418127	-	192.168.100.18	192.168.100.250	RADIUS	109 Access-Reject id=5, Duplicate Response
11	16.452450	-	192.168.100.250	192.168.100.18	RADIUS	102 Access-Request id=5, Duplicate Request
12	17.453513	-	192.168.100.18	192.168.100.250	RADIUS	109 Access-Reject id=5, Duplicate Response
13	19.996200	-	06:23:66:15:aa:f1	06:23:66:15:aa:f1	LOOP	60 Reply
14	22.560571	-	06:23:66:15:aa:f1	Broadcast	ARP	60 Who has 192.168.100.100? Tell 192.168.100.250

```
R1-6615#test aaa group radius dantunes segurancap5 legacy
Attempting authentication test to server-group radius using radius
No authoritative response from any server.

R1-6615#
000066: *Apr  3 20:07:05.653 UTC: %SEC_LOGIN-1-QUIET_MODE_ON: Still timeleft for watching f
ailures is 2 secs, [user: dantunes] [Source: 192.168.100.15] [localport: 22] [Reason: Login
Authentication Failed] [ACL: sl_def_acl] at 20:07:05 UTC Thu Apr 3 2025
R1-6615#
```

```
(dantunes@192.168.100.250) Password:
(dantunes@192.168.100.250) Password:
(dantunes@192.168.100.250) Password:
Connection closed by 192.168.100.250 port 22
root@A1:~#
```

Como se pode verificar, nas PDUS, existe o pedido Access-Request, no entanto é sempre rejeitado.

7)

```
root@AAA-1:~# service freeradius reload
* Checking FreeRADIUS daemon configuration... [ OK ]
* FreeRADIUS daemon is running
* Reloading FreeRADIUS daemon freeradius [ OK ]
root@AAA-1:~#
```

O script freeradius pode ser encontrado ou visualizado com o comando `/etc/init.d/freeradius`.

```
reload)
    configtest || exit 150

    if status_of_proc -p "$PIDFILE" "$PROG" "$DESCR"; then
        log_daemon_msg "Reloading $DESCR" "$PROG"

        start-stop-daemon --stop --signal HUP --quiet --pidfile $PIDFILE || ret=$?
        log_end_msg $ret
    fi
;;
```

Na imagem acima pode-se verificar o script relativo ao comando reload. No caso deve ser usado o comando `service freeradius reload`.

Na imagem acima pode-se verificar o script relativo ao comando status. No caso deve ser usado o comando `service freeradius status`.

```
root@AAA-1:~# service freeradius status
* freeradius is running
root@AAA-1:~#
```

```
root@A1:~# ssh dantunes@192.168.100.250
```

Wavelength

```
(dantunes@192.168.100.250) Password:
Hello, dantunes, Autenticacao bem sucedida!!!
Acesso apenas a pessoas autorizadas!!!!
```

```
Bem Vindo ao modo EXEC!!!!
```

R1-6615>en

Password:

R1-6615#

Após executar o comando “service freeradius reload”, o serviço de Radius releu as novas configurações e assim as configurações do novo utilizador ficaram disponíveis. Consequentemente, consegui comunicar por ssh com esse utilizador.

33	4.260358	-	192.168.100.250	192.168.100.18	RADIUS	114 Access-Request id=5
34	4.261556	-	192.168.100.18	192.168.100.250	RADIUS	109 Access-Accept id=5

Como se pode verificar na captura do wireshark houve sucesso na autenticação Radius. Primeiramente o Router1 enviou um pedido de autenticação para o servidor Radius (Access-Request). Seguidamente, o servidor verificou se os dados de autenticação eram válidos comparando com as informações presentes nos ficheiros de configuração, tanto do cliente Router como do utilizador criado. Como estes eram válidos o servidor respondeu com um PDU Access-Accept.

```

▼ Attribute Value Pairs
  ▼ AVP: t=User-Name(1) l=10 val=dantunes
    Type: 1
    Length: 10
    User-Name: dantunes
  ▼ AVP: t=User-Password(2) l=18 val=Encrypted
    Type: 2
    Length: 18
    User-Password (encrypted): d6b050fa6ffc0e44cfec579a8c0054da
  ▶ AVP: t=NAS-Port(5) l=6 val=2
  ▶ AVP: t=NAS-Port-Id(87) l=6 val=tty2

Code: Access-Accept (2)
Packet identifier: 0x5 (5)
Length: 67
Authenticator: 62c99eaf6b9896a9a4a332bd4556da19
[This is a response to a request in frame 33]
[Time from request: 0.001198000 seconds]
▼ Attribute Value Pairs
  ▼ AVP: t=Reply-Message(18) l=47 val=Hello, dantunes, Autenticacao bem sucedida!!!
    Type: 18
    Length: 47
    Reply-Message: Hello, dantunes, Autenticacao bem sucedida!!!

```

A Ofuscação da Password é feita de modo a proteger a mesma a partir de MD5 e da operação XOR. Primeiramente o Request Authenticator é combinado com a shared secret, depois passando para um hash MD5. Depois a password é cifrada por blocos de 16 bytes com XOR utilizando os hashes MD5 iterativamente.

Diagrama Temporal:

- O utilizador inicia uma sessão via SSH enviando o seu username para a autenticação;
- O R1 envia um Access-Request para o servidor FreeRadius, contendo o username e a password já ofuscada e um campo Authenticator que é gerado aleatoriamente.
- O servidor FreeRadius valida os dados de configuração, comparando-os com as informações armazenadas na sua base de dados.

-Se for válido o servidor responde com um Access-Accept, enviando a resposta ao Router, que seguidamente reencaminha ao terminal onde está a ser feita a comunicação SSH, para informar ao utilizador que pode iniciar a sessão SSH.

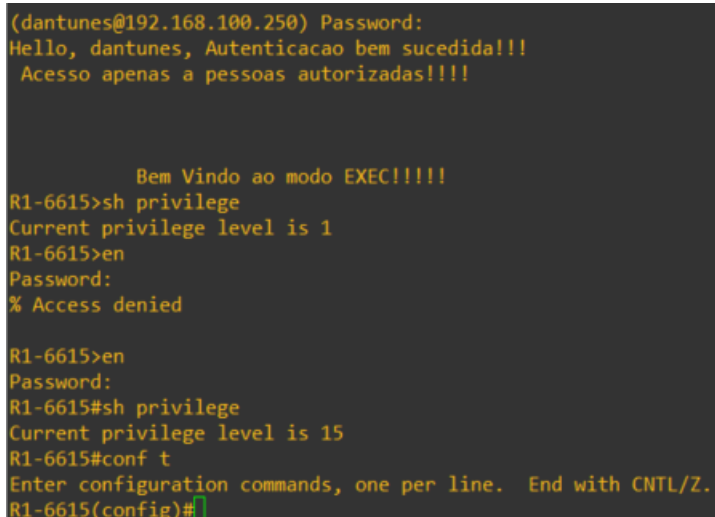
8)

Como o Authenticator é calculado?

Primeiramente, O Authenticator é um valor de 16 bytes gerado aleatoriamente, neste caso pelo R1.

Para o poder calcular faz-se a soma dos campos do Access Request, Code, Identifier, Length, Authenticator, Attributes (Parte dos dados Radius) e Shared Secret. Após a soma ou concatenação destes campos aplica-se um hash MD5.

9)



```
(dantunes@192.168.100.250) Password:
Hello, dantunes, Autenticacao bem sucedida!!!
Acesso apenas a pessoas autorizadas!!!!

      Bem Vindo ao modo EXEC!!!!
R1-6615>sh privilege
Current privilege level is 1
R1-6615>en
Password:
% Access denied

R1-6615>en
Password:
R1-6615#sh privilege
Current privilege level is 15
R1-6615#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1-6615(config)#
```

Após fazer a autenticação via SSH, pode-se verificar que o utilizador está com o nível de privilégio 1 (modo EXEC de utilizador). Após aceder ao enable colocando a password, verifica-se que o utilizador está com o nível de privilégio 15. E consequentemente verificou-se que o utilizador pode entrar no modo de configuração.

Após a autenticação RADIUS bem-sucedida, o usuário recebeu, por padrão, o nível de privilégio 1 no modo EXEC. Isso aconteceu porque o servidor RADIUS não enviou nenhum atributo de autorização específico instruindo o roteador (R1) a conceder um nível de privilégio diferente, como o nível 15.

A configuração `aaa authorization exec default group radius local` no R1 garantiu que a autorização para iniciar a sessão EXEC fosse aceita. No entanto, como não foi definida nenhuma instrução explícita para alterar o nível de acesso do usuário, o R1 aplicou automaticamente o nível padrão para usuários autenticados, que é o privilégio 1. Para obter acesso ao modo de configuração global (configure terminal), seria necessário elevar o privilégio para o nível 15 usando o comando `enable`.

AVP: Attribute-Value Pairs Access-Request

```
▼ Attribute Value Pairs
  ▼ AVP: t=User-Name(1) l=10 val=dantunes
    Type: 1
    Length: 10
    User-Name: dantunes
  ▼ AVP: t=User-Password(2) l=18 val=Encrypted
    Type: 2
    Length: 18
    User-Password (encrypted): d6b050fa6ffc0e44cfec579a8c0054da
  ▼ AVP: t=NAS-Port(5) l=6 val=2
    Type: 5
    Length: 6
    NAS-Port: 2
  ▼ AVP: t=NAS-Port-Id(87) l=6 val=tty2
    Type: 87
    Length: 6
    NAS-Port-Id: tty2
  ▼ AVP: t=NAS-Port-Type(61) l=6 val=Virtual(5)
    Type: 61
    Length: 6
    NAS-Port-Type: Virtual (5)
  ▼ AVP: t=NAS-IP-Address(4) l=6 val=192.168.100.250
    Type: 4
    Length: 6
    NAS-IP-Address: 192.168.100.250
```

AVP: Attribute-Value Pairs Access-Accept

```
[This is a response to a request in frame 33]
[Time from request: 0.001198000 seconds]
▼ Attribute Value Pairs
  ▼ AVP: t=Reply-Message(18) l=47 val=Hello, dantunes, Autenticacao bem sucedida!!!
    Type: 18
    Length: 47
    Reply-Message: Hello, dantunes, Autenticacao bem sucedida!!!
```


10)

```
R1-6615#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1-6615(config)#line vty 0 4
R1-6615(config-line)#privilege level 15
R1-6615(config-line)#
```

```
(dantunes@192.168.100.250) Password:
Hello, dantunes, Autenticacao bem sucedida!!!
Acesso apenas a pessoas autorizadas!!!!
```

```
Bem Vindo ao modo EXEC!!!!
```

```
R1-6615#sh privilege
Current privilege level is 15
R1-6615#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1-6615(config)#line vty 0 4
R1-6615(config-line)#no privilege 15
R1-6615(config-line)#^
% Invalid input detected at '^' marker.
R1-6615(config-line)#no privilege level 15
R1-6615(config-line)#do wr
Building configuration...
[OK]
R1-6615(config-line)#
```

Ao adicionar o comando `privilege level 15` à configuração das linhas VTY, estamos a instruir o roteador a atribuir automaticamente o nível de privilégio 15 a qualquer usuário que se autentique com sucesso através da linha SSH, sem considerar o que o servidor RADIUS ou a configuração local do usuário possam especificar em relação aos privilégios. Isso significa que essa configuração nas linhas VTY tem prioridade e será a primeira a ser aplicada para definir o nível de privilégio inicial.

11)

```
dantunes      Cleartext-Password := "segurancap5"
              Reply-Message = "Hello, %{User-Name}, Autenticacao bem sucedida!!!",
              Service-Type = NAS-Prompt-User,
              Cisco-AVPair = "shell:priv-lvl=15"
```

```
root@AAA-1:~# service freeradius restart
* Checking FreeRADIUS daemon configuration... [ OK ]
* Stopping FreeRADIUS daemon freeradius [ OK ]
* Starting FreeRADIUS daemon freeradius [ OK ]
root@AAA-1:~# service freeradius status
* freeradius is running
root@AAA-1:~#
```

```
R1-6615(config)#aaa authorization exec default group radius
R1-6615(config)#
```

```
(dantunes@192.168.100.250) Password:
Hello, dantunes, Autenticacao bem sucedida!!!
Acesso apenas a pessoas autorizadas!!!!
```

```
Bem Vindo ao modo EXEC!!!!
```

```
R1-6615#
```



```

--> 56 24.921684 - 192.168.100.250 192.168.100.18 RADIUS 114 Access-Request id=12
<-- 57 24.921684 - 192.168.100.18 192.168.100.250 RADIUS 140 Access-Accept id=12

```

```

Code: Access-Request (1)
Packet identifier: 0xc (12)
Length: 72
Authenticator: e99ae6097954ef6000c945a0c7f63f27
[The response to this request is in frame 57]
Attribute Value Pairs
  AVP: t=User-Name(1) l=10 val=dantunes
    Type: 1
    Length: 10
    User-Name: dantunes
  AVP: t=User-Password(2) l=18 val=Encrypted
    Type: 2
    Length: 18
    User-Password (encrypted): aab8b27563ff0e99e4d032e722b50b04
  AVP: t=NAS-Port(5) l=6 val=2
    Type: 5
    Length: 6
    NAS-Port: 2
  AVP: t=NAS-Port-Id(87) l=6 val=tty2
    Type: 87
    Length: 6
    NAS-Port-Id: tty2
  AVP: t=NAS-Port-Type(61) l=6 val=Virtual(5)
    Type: 61
    Length: 6
    NAS-Port-Type: Virtual (5)
  AVP: t=NAS-IP-Address(4) l=6 val=192.168.100.250
    Type: 4
    Length: 6
    NAS-IP-Address: 192.168.100.250

```

```

57 24.921684 - 192.168.100.18 192.168.100.250 RADIUS 140 Access-Accept id=12

```

```

Frame 57: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface -, id 0
Ethernet II, Src: 06:23:66:15:aa:04 (06:23:66:15:aa:04), Dst: 06:23:66:15:aa:f1 (06:23:66:15:aa:f1)
Internet Protocol Version 4, Src: 192.168.100.18, Dst: 192.168.100.250
User Datagram Protocol, Src Port: 1812, Dst Port: 1645
RADIUS Protocol
  Code: Access-Accept (2)
  Packet identifier: 0xc (12)
  Length: 98
  Authenticator: 0e9d7633672242427961146e0f640499
  [This is a response to a request in frame 56]
  [Time from request: 0.000000000 seconds]
  Attribute Value Pairs
    AVP: t=Reply-Message(18) l=47 val=Hello, dantunes, Autenticacao bem sucedida!!!
      Type: 18
      Length: 47
      Reply-Message: Hello, dantunes, Autenticacao bem sucedida!!!
    AVP: t=Service-Type(6) l=6 val=Exec-User(7)
      Type: 6
      Length: 6
      Service-Type: Exec-User (7)
    AVP: t=Vendor-Specific(26) l=25 vnd=ciscoSystems(9)
      Type: 26
      Length: 25
      Vendor ID: ciscoSystems (9)
      VSA: t=Cisco-AVPair(1) l=19 val=shell:priv-lvl=15

```

Na captura anterior a PDU Access-Accept apenas tinha o campo Reply-message. Agora pode-se verificar que tem também os atributos service-type e Vendor-Specific Cisco-AVPair.

O service-type, especifica o tipo de serviço autorizado para o utilizador.

O Cisco-AVPair é o atributo que define o nível de privilégio do utilizador, neste caso 15 ("shell:priv-lvl=15").

Vendor ID da Cisco para VSAs

O Vendor ID da Cisco para os seus Vendor-Specific Attributes (VSAs) RADIUS é 9. Este ID é atribuído pela IETF (Internet Engineering Task Force), que é a entidade responsável pela regulamentação dos padrões da Internet.

Podemos encontrar uma lista atualizada dos IDs de fornecedores (Vendor IDs) e outros atributos no site do IANA (Internet Assigned Numbers Authority), que é responsável pela distribuição desses IDs.

<https://www.iana.org/assignments/enterprise-numbers>

12)

```
root@AAA-1:~# service freeradius stop
* Stopping FreeRADIUS daemon freeradius:
root@AAA-1:~# 
root@A1:~# ssh dantunes@192.168.100.250

Welcome

(dantunes@192.168.100.250) Password:
(dantunes@192.168.100.250) Password:
```

Ao tentar aceder por ssh, após parar o serviço Radius, verificou-se um atraso, pois o router estava a tentar comunicar com o servidor Radius, no entanto como este está “down”, não obtia resposta. Como o router tem um tempo de espera para obter a resposta obteve-se um atraso.

Como o utilizador apenas está configurado na base de dados do servidor Radius e não está presente na base de dados local, não é possível haver autenticação.