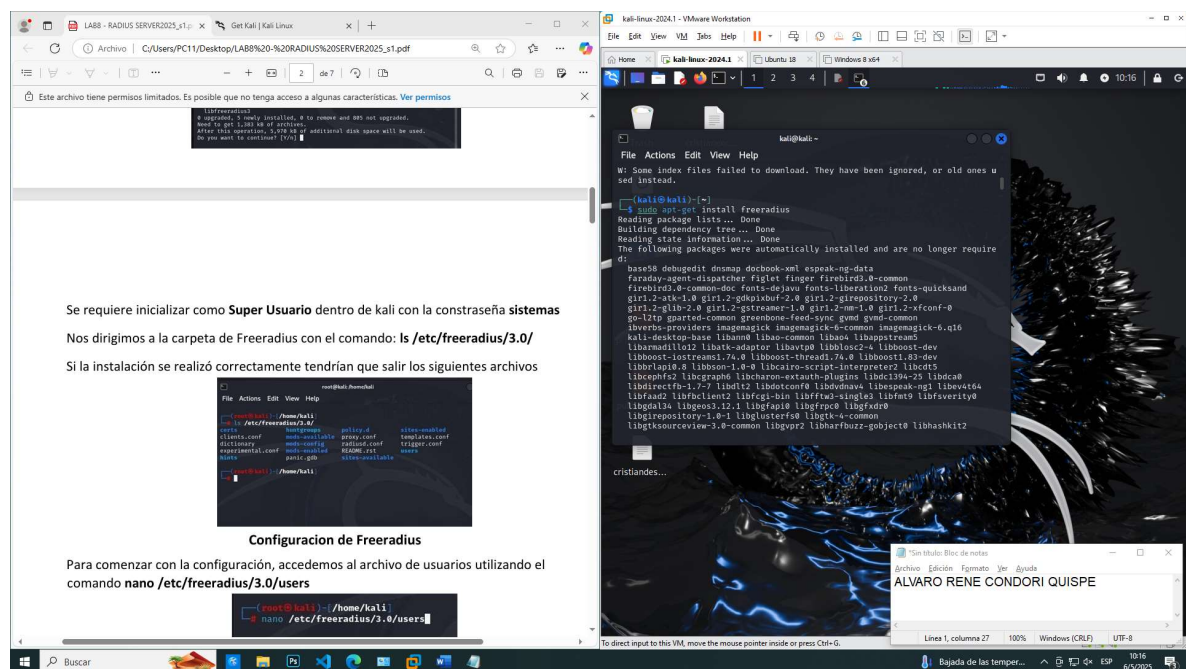


1



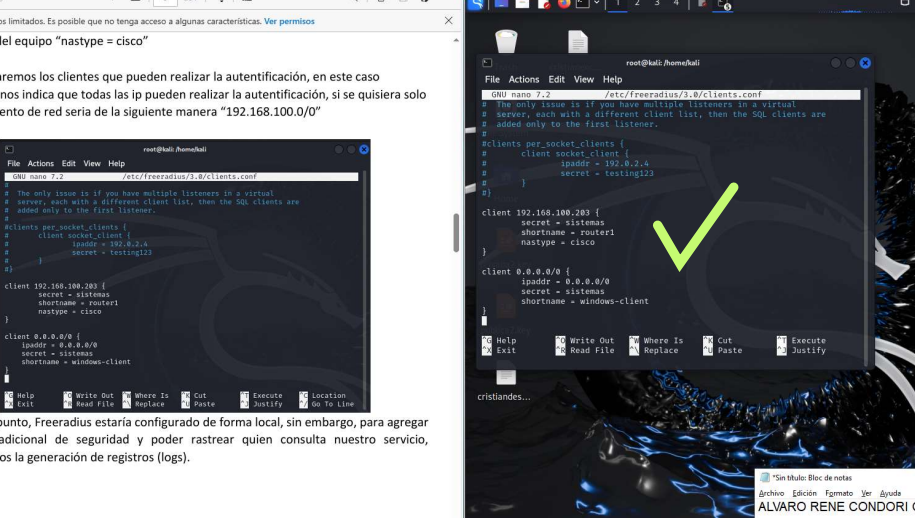
The screenshot displays two terminal windows from a Kali Linux virtual machine running on VMware Workstation.

The top terminal window shows the contents of the file `/etc/freeradius/3.0/users`, which lists several users with their respective clear-text passwords:

```
#
#   +-----+-----+
#   | Username      | Password          |
#   +-----+-----+
clients.conf    secret
dictionary     password
experimental.conf  test
#
# Add more users below this line
#
root@kali:/home/kali# nano /etc/freeradius/3.0/users
```

The bottom terminal window shows the same file being edited with the `nano` editor. It includes comments explaining the format and provides examples of user entries:

```
GNU nano 2.2 /etc/freeradius/3.0/users *
#
# RadSec-Authing - Brackets Filter,
# Framed-Filter-id = "std.ppp",
# Framed-MTU = 1500,
# Framed-Compression = Van-Jacobson-TCP-IP
#
# The canonical testing user which is in most of the
# examples.
#
#bob ClearText-Password = "hello"
# Reply-Message = "Hello, $User-Name!"
#
#pepe ClearText-Password = "pepe"
#alvaro ClearText-Password = "12345"
#admin ClearText-Password = "admin"
# Reply-Message = "bienvenido"
#
# This is an entry for a user with a space in their name.
# Note the double quotes surrounding the name. If you have
# users with spaces in their names, you must also change
# the "filter_username" policy to allow spaces.
#
Help Exit Write Out Read File Where Is Replace Cut Paste Execute Justify
```



Y la marca del equipo "natype = cisco"

Implementaremos los clientes que pueden realizar la autenticación, en este caso "0.0.0.0/0" nos indica que todas las ip pueden realizar la autenticación, si se quisiera solo en un segmento de red sería de la siguiente manera "192.168.100.0/0"

Hasta este punto, FreeRadius está configurado de forma local, sin embargo, para agregar una capa adicional de seguridad y poder rastrear quien consulta nuestro servicio, habilitaremos la generación de registros (logs).

5

LAB8 - RADIUS SERVER2025\_s1.p

C:\Users\PC1\Desktop\LAB8%20-%20RADIUS%20SERVER2025\_s1.pdf

Este archivo tiene permisos limitados. Es posible que no tenga acceso a algunas características. [Ver permisos](#)

Para ello nos dirigimos al archivo radiusd.conf con el comando: **nano**

**/etc/freeradius/3.0/radiusd.conf**

```
(root@kali) ~/home/kali
nano /etc/freeradius/3.0/radiusd.conf
```

Una vez dentro del archivo, localizamos la línea correspondiente de la autenticación (auth) y modificamos el valor predeterminado "no" a "YES"

```

# Log all (accept and reject) authentication results to the log file.
# This is the same as setting "auth_accept = yes" and
# "auth_reject = yes"
# allowed values: {no, yes}
auth = yes

# Log Access-Accept results to the log file.
# This is only used if "auth = no"
# allowed values: {no, yes}
auth_accept = no

# Log Access-Reject results to the log file.

```

Realizaremos el mismo paso anterior para la generación de logs para eventos como **auth\_badpass** y **auth\_goodpass**

```

# Log passwords with the authentication requests.
# auth_badpass - logs password if it's rejected
# auth_goodpass - logs password if it's correct
# allowed values: {no, yes}
auth_badpass = yes
auth_goodpass = yes

# Log additional text at the end of the "Login OK" messages.
# For these to work, the "auth" and "auth_goodpass" or "auth_badpass"
# configurations above have to be set to "yes".

```

kali-linux-2024.1 - VMware Workstation

File Edit View VM Help

Home kali-linux-2024.1 Ubuntu 18 Windows 8 x64

root@kali: /home/kali

```

GNU nano 2.2 /etc/freeradius/3.0/radiusd.conf
#
# Log the full User-Name attribute, as it was found in the request.
#
# allowed values: {no, yes}
#
stripped_names = no
#
# Log all (accept and reject) authentication results to the log file.
# This is the same as setting "auth_accept = yes" and
# "auth_reject = yes"
# allowed values: {no, yes}
auth = yes
#
# Log Access-Accept results to the log file.
# This is only used if "auth = no"
# allowed values: {no, yes}
auth_accept = no
#
# Log Access-Reject results to the log file.

```

cristiandes...

ALVARO RENE CONDORI QUISPE

Linea 1, columna 27 100% Windows (CRLF) UTF-8

6

LAB8 - RADIUS SERVER2025\_s1.p

C:\Users\PC1\Desktop\LAB8%20-%20RADIUS%20SERVER2025\_s1.pdf

Este archivo tiene permisos limitados. Es posible que no tenga acceso a algunas características. [Ver permisos](#)

```

# Log all (accept and reject) authentication results to the log file.
# This is the same as setting "auth_accept = yes" and
# "auth_reject = yes"
# allowed values: {no, yes}
auth = yes

# Log Access-Accept results to the log file.
# This is only used if "auth = no"
# allowed values: {no, yes}
auth_accept = no

# Log Access-Reject results to the log file.

```

Realizaremos el mismo paso anterior para la generación de logs para eventos como **auth\_badpass** y **auth\_goodpass**

```

# Log passwords with the authentication requests.
# auth_badpass - logs password if it's rejected
# auth_goodpass - logs password if it's correct
# allowed values: {no, yes}
auth_badpass = yes
auth_goodpass = yes

# Log additional text at the end of the "Login OK" messages.
# For these to work, the "auth" and "auth_goodpass" or "auth_badpass"
# configurations above have to be set to "yes".

```

"auth\_badpass = yes" Indicamos que se generen logs de cuando alguien intente autenticarse de manera incorrecta o falle en el proceso de inicio de sesión.

"auth\_goodpass = yes" Indicamos que se generen logs para todos usuarios que inicien sesión correctamente.

Procedemos a reiniciar el servicio de Freeradius para aplicar todos los cambios realizados

kali-linux-2024.1 - VMware Workstation

File Edit View VM Help

Home kali-linux-2024.1 Ubuntu 18 Windows 8 x64

root@kali: /home/kali

```

GNU nano 2.2 /etc/freeradius/3.0/radiusd.conf
#
# Log Access-Reject results to the log file.
# This is only used if "auth = no"
# allowed values: {no, yes}
auth_reject = no
#
# Log passwords with the authentication requests.
# auth_badpass - logs password if it's rejected
# auth_goodpass - logs password if it's correct
# allowed values: {no, yes}
auth_badpass = yes
auth_goodpass = yes
#
# Log additional text at the end of the "Login OK" messages.
# For these to work, the "auth" and "auth_goodpass" or "auth_badpass"
# configurations above have to be set to "yes".

```

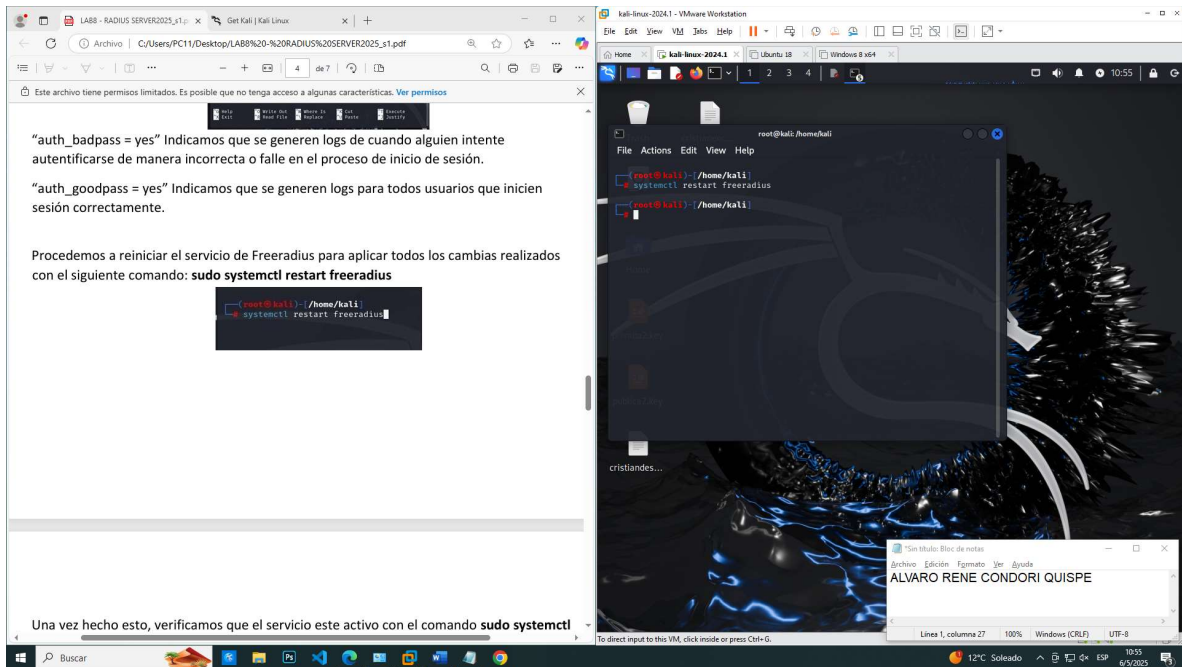
cristiandes...

ALVARO RENE CONDORI QUISPE

Linea 1, columna 27 100% Windows (CRLF) UTF-8



7



The screenshot shows a Kali Linux virtual machine environment. On the left, a PDF document titled "LAB8 - RADIUS SERVER2025\_s1.p" is open in a web browser. The document contains the following text:

"auth\_badpass = yes" Indicamos que se generen logs de cuando alguien intente autenticarse de manera incorrecta o falle en el proceso de inicio de sesión.

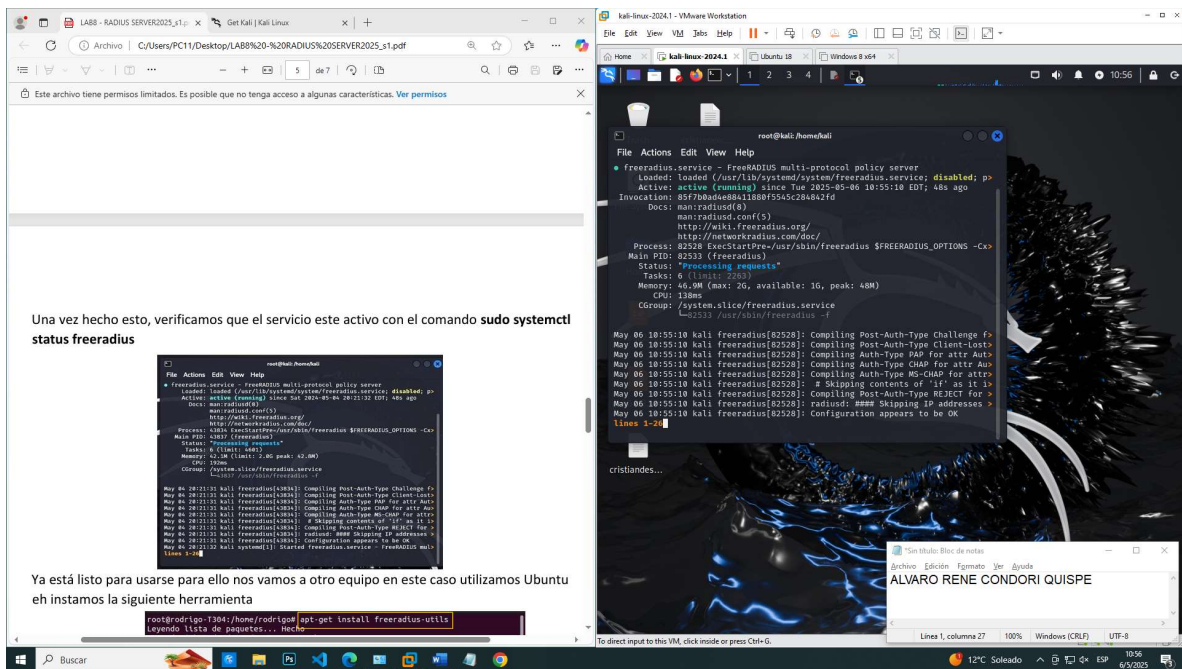
"auth\_goodpass = yes" Indicamos que se generen logs para todos usuarios que inicien sesión correctamente.

Procedemos a reiniciar el servicio de FreeRadius para aplicar todos los cambios realizados con el siguiente comando: **sudo systemctl restart freeradius**

Una vez hecho esto, verificamos que el servicio este activo con el comando **sudo systemctl**

On the right, a terminal window is open, showing the command **systemctl restart freeradius** being executed. Below the terminal, a small note window displays the text: "ALVARO RENE CONDORI QUISPE".

8



The screenshot shows a Kali Linux virtual machine environment. On the left, a PDF document titled "LAB8 - RADIUS SERVER2025\_s1.p" is open in a web browser. The document contains the following text:

Una vez hecho esto, verificamos que el servicio este activo con el comando **sudo systemctl status freeradius**

Ya está listo para usarse para ello nos vamos a otro equipo en este caso utilizamos Ubuntu eh instamos la siguiente herramienta

On the right, a terminal window is open, showing the command **sudo systemctl status freeradius** being executed. The output of the command is displayed, showing the status of the **freeradius.service** as **active (running)**. Below the terminal, a small note window displays the text: "ALVARO RENE CONDORI QUISPE".

9.

Con el siguiente comando podremos logear en el servidor radius y comprobar que anda, con el comando **radtest** "usuario" "contraseña" "ip\_del\_servidor" "puerto" "contraseña compartida".

```

root@ubuntu:/home/ubuntu# radtest root@10 12345 192.168.100.203 1812 sistemas
Sent Access-Request Id 199 from 0.0.0.0:49154 to 192.168.100.203:1812 length 77
  User-Name = "root@10"
  User-Password = "12345"
  NAS-IP-Address = 127.0.1.1
  NAS-Port = 1812
  Message-Authenticator = 0x00
  Cleartext-Password = "12345"
Received Access-Accept Id 199 from 192.168.100.203:1812 to 192.168.100.211:60184 length 20
  User-Name = "root@10"
  User-Password = "12345"
  NAS-IP-Address = 127.0.1.1
  NAS-Port = 1812
  Message-Authenticator = 0x00
  Cleartext-Password = "12345"
Sent Access-Request Id 125 from 0.0.0.0:49154 to 192.168.100.203:1812 length 77
  User-Name = "root@10"
  User-Password = "12345"
  NAS-IP-Address = 127.0.1.1
  NAS-Port = 1812
  Message-Authenticator = 0x00
  Cleartext-Password = "12345"
Received Access-Reject Id 125 from 192.168.100.203:1812 to 192.168.100.211:35943 length 20
  User-Name = "root@10"
  User-Password = "12345"
  NAS-IP-Address = 127.0.1.1
  NAS-Port = 1812
  Message-Authenticator = 0x00
  Cleartext-Password = "12345"
root@ubuntu:/home/ubuntu#

```

Haremos un logeo correcto y seguidamente se realizará un logeo incorrecto, en ambos logeos no genera un mensaje de logeo aceptado o rechazado.

```

sistemas@sistemas:~$ sudo radtest alvaro 12345 192.168.100.203 1812 sistemas
Sent Access-Request Id 245 from 0.0.0.0:49969 to 192.168.100.203:1812 length 76
  User-Name = "alvaro"
  User-Password = "12345"
  NAS-IP-Address = 127.0.1.1
  NAS-Port = 1812
  Message-Authenticator = 0x00
  Cleartext-Password = "12345"
Sent Access-Request Id 245 from 0.0.0.0:49969 to 192.168.100.203:1812 length 76
  User-Name = "alvaro"
  User-Password = "12345"
  NAS-IP-Address = 127.0.1.1
  NAS-Port = 1812
  Message-Authenticator = 0x00
  Cleartext-Password = "12345"
Sent Access-Request Id 245 from 0.0.0.0:49969 to 192.168.100.203:1812 length 76
  User-Name = "alvaro"
  User-Password = "12345"
  NAS-IP-Address = 127.0.1.1
  NAS-Port = 1812
  Message-Authenticator = 0x00
  Cleartext-Password = "12345"
(0) No reply from server for ID 245
sistemas@sistemas:~$

```

10

Nos dirigiremos a Windows 8 y abriremos la aplicación de **NTRadPing**, esta se encuentra dentro de la carpeta con el mismo nombre de la aplicación.

Dentro de la aplicación pondremos la ip del servidor radius, puerto lógico, contraseña compartida, usuario, contraseña de usuario, una vez llenado todas las casillas presionar **Send**.

The NTRadPing application window shows fields for IP, Port, Username, Password, and a Send button. The interface is in Spanish.

11.

Este archivo tiene permisos limitados. Es posible que no tenga acceso a algunas características. Ver permisos

Dentro de la aplicación pondremos la ip del servidor radius, puerto lógico, contraseña compartida, usuario, contraseña de usuario, una vez llenado todas las casillas presiona Send.

Y este nos mostrara el siguiente mensaje

RADIUS Server reply:  
[Sending authentication request to server: 192.168.100.203:1812]  
[Sending packet: 0x00000000: 0x00000000]  
[Received response from the server: 0x00000000: 0x00000000]  
[Received response from the server: 0x00000000: 0x00000000]

12

## Evaluación

1.

**sudo tail -f /var/log/freeradius/radius.log**

**pregunta 2**

