



ANONYMOUS

LOGINS FOR PENTESTER

Contenido

Introducción.....	3
Configurar FTP anónimo.....	3
Atacar FTP anónimo.....	8
Configurar SMB anónimo.....	10
Atacar a PYMES anónimas	13
Conclusión	14

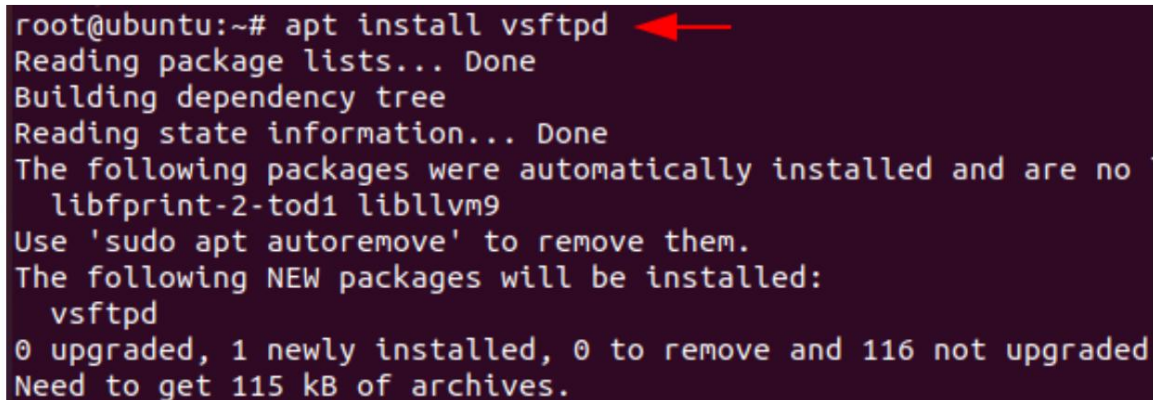
Introducción

Los inicios de sesión anónimos son una función que permite al usuario configurar un servicio al que puede acceder cualquier usuario. No necesita credenciales específicas para acceder a ese recurso. Varios servidores que desean alojar datos a los que debería poder acceder una amplia gama de usuarios mediante inicios de sesión anónimos. En la vida real, mientras se realizan pruebas de penetración de la red, un evaluador debería poder identificar el servicio anónimo y probarlo. También veremos detrás de escena cómo se configuran estos servicios anónimos en nuestra máquina de destino local que ejecuta Ubuntu. Estaremos aprendiendo sobre el servicio FTP y el servicio SMB.

Configurar FTP anónimo

Comenzaremos demostrando el proceso de configuración del acceso anónimo en el servicio FTP. Tenemos una máquina Ubuntu con acceso root. Instalamos el vsftpd usando el comando apt.

apto para instalar vsftpd



```
root@ubuntu:~# apt install vsftpd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no
  libfprint-2-tod1 libllvm9
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 116 not upgraded
Need to get 115 kB of archives.
```

Cada servicio que se instala en una máquina Linux tiene un archivo de configuración que se puede utilizar para modificar las opciones y configuraciones de ese servicio en particular. De forma predeterminada, el inicio de sesión anónimo está deshabilitado en vsftpd.

Necesitaremos editar el archivo de configuración `/etc/vsftpd.conf` para habilitar la funcionalidad de inicio de sesión anónimo. Editamos el archivo de configuración con nano, pero puedes usar cualquier editor de tu elección, como vi o sublime. Revisamos todas las demás opciones y comentarios hasta llegar a la opción `"anonymous_enabled=NO"`, que se muestra en la imagen de abajo.

```
# Example config file /etc/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
# Run standalone? vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=NO
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (:::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
```

Para habilitar el inicio de sesión anónimo en la máquina, cambie la opción "anonymous_enable=NO" a "anonymous_enable=YES". Consulte la captura de pantalla a continuación.


```
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
#
# Run standalone? vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=NO
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (:::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=YES
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
```

Simplemente habilitar el inicio de sesión anónimo o instalar un servicio no es suficiente para que funcione. Queremos un servicio FTP completamente funcional. Para hacer esto, necesitamos poder compartir archivos usando FTP y, dado que hemos habilitado el inicio de sesión anónimo, deberíamos poder descargar los archivos desde la máquina Ubuntu usando el acceso anónimo. El servicio FTP requiere un directorio cuyo contenido se pueda compartir a través de la red. Creamos un directorio en el directorio /var. Le pusimos al directorio el nombre del pub. También necesitamos cambiar la propiedad del directorio para que sea adecuado para compartir datos. Después de crear y cambiar la propiedad, ingresamos al directorio y creamos un archivo con el mensaje "Bienvenido a Hacking Articles". Llamamos al archivo de texto note.txt.

```
mkdir -p /var/ftp/pub
sudo chown nadie:nogroup /var/ftp/pub
CD /var/ftp/pub
echo "Bienvenido a artículos sobre piratería" > note.txt
```

```
root@ubuntu:~# mkdir -p /var/ftp/pub  
root@ubuntu:~# sudo chown nobody:nogroup /var/ftp/pub  
root@ubuntu:~# cd /var/ftp/pub  
root@ubuntu:/var/ftp/pub# echo "Welcome to Hacking Articles" > note.txt
```

Volviendo al archivo vsftpd.conf que estábamos editando, necesitamos agregar una configuración específica para que el inicio de sesión anónimo sea funcional. Agregamos el directorio que acabamos de crear en las configuraciones y luego agregamos la opción `no_anon_password` que dejará de solicitar una contraseña. Otra opción que agregamos es la opción `hide_ids`. Cuando se le solicite, volverá a la combinación `ftp:ftp`. Necesitamos agregar el rango de puertos que se pueden usar para FTP pasivo.

```

# sites. However, some broken FTP clients such as "ncftp" and "mirror" as
# the presence of the "-R" option, so there is a strong case for enabling
#ls_recurse_enable=YES
#
# Customization
#
# Some of vsftpd's settings don't fit the filesystem layout by
# default.
#
# This option should be the name of a directory which is empty. Also, th
# directory should not be writable by the ftp user. This directory is use
# as a secure chroot() jail at times vsftpd does not require filesystem
# access.
secure_chroot_dir=/var/run/vsftpd/empty
#
# This string is the name of the PAM service vsftpd will use.
pam_service_name=vsftpd
#
# This option specifies the location of the RSA certificate to use for SS
# encrypted connections.
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
ssl_enable=NO

#
# Uncomment this to indicate that vsftpd use a utf8 filesystem.
#utf8_filesystem=YES
#
# Point users at the directory we created earlier.
anon_root=/var/ftp/
#
# Stop prompting for a password on the command line.
no_anon_password=YES
#
# Show the user and group as ftp:ftp, regardless of the owner.
hide_ids=YES
#
# Limit the range of ports that can be used for passive FTP
pasv_min_port=40000
pasv_max_port=50000

```

Esto completa todas las configuraciones que necesitamos para configurar un servicio FTP con inicio de sesión anónimo habilitado en una máquina Ubuntu. Todo lo que se requiere es reiniciar el servicio vsftpd para que las nuevas configuraciones entren en vigor. Ahora nos referiremos a nuestra máquina Kali Linux, es decir, la máquina atacante.

nano /etc/vsftpd.conf
reinicio del servicio vsftpd

```
root@ubuntu:/var/ftp/pub# nano /etc/vsftpd.conf
root@ubuntu:/var/ftp/pub# service vsftpd restart
root@ubuntu:/var/ftp/pub#
```

Atacar FTP anónimo

Al atacar o apuntar a un sistema, uno de los pasos iniciales que toma un atacante es realizar un escaneo del objetivo. Este análisis proporciona al atacante información como puertos abiertos y servicios en ejecución. Usamos Nmap para escanear la máquina Ubuntu que acabábamos de configurar. Podemos ver que Nmap pudo identificar que el servicio FTP estaba funcional en la máquina de destino y también da otro paso en la enumeración e informa al atacante que el servicio FTP tiene el inicio de sesión anónimo habilitado.

nmap -A 192.168.1.46


```

(root@kali)-[~]
# nmap -A 192.168.1.46
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-13 14:06 EDT
Nmap scan report for 192.168.1.46
Host is up (0.00039s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
|_FTP server status:
|_Connected to ::ffff:192.168.1.2
|_Logged in as ftp
|_TYPE: ASCII
|_No session bandwidth limit
|_Session timeout in seconds is 300
|_Control connection is plain text
|_Data connections will be plain text
|_At session startup, client count was 1
|_vsFTPD 3.0.3 - secure, fast, stable
|_End of status
MAC Address: 00:0C:29:49:94:BA (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
Service Info: OS: Unix

```

Ahora que se ha confirmado que el servicio FTP se está ejecutando con el inicio de sesión anónimo habilitado, intentemos acceder al servicio. Para ello nos conectaremos al servicio FTP proporcionando la dirección IP de la máquina. Como no tenemos ninguna credencial de usuario y el inicio de sesión anónimo está habilitado, ingresaremos "Anónimo" en el campo Nombre e iniciaremos sesión. Podemos ejecutar el comando de listado de directorios ls para averiguar los archivos que se comparten a través de FTP. Vemos que hay un archivo de texto con el nombre note.txt. Podemos transferir el archivo de texto usando el comando get como se muestra a continuación. Después de la transferencia, podemos leer el archivo de texto para confirmar que hemos obtenido correctamente los datos del archivo que se creó en la máquina Ubuntu.

```

ftp192.168.1.46
Anónimo
es
pub cd
es
obtener nota.txt
adiós
nota de gato.txt

```

```
(root@kali)~[~]
# ftp 192.168.1.46
Connected to 192.168.1.46.
220 (vsFTPd 3.0.3)
Name (192.168.1.46:root): Anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 ftp      ftp          4096 May 13 11:08 pub
226 Directory send OK.
ftp> cd pub
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp          28 May 13 11:08 note.txt
226 Directory send OK.
ftp> get note.txt
local: note.txt remote: note.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for note.txt (28 bytes).
226 Transfer complete.
28 bytes received in 0.00 secs (290.8910 kB/s)
ftp> bye
221 Goodbye.

(root@kali)~[~]
# cat note.txt
Welcome to Hacking Articles
```

Configurar SMB anónimo

El siguiente servicio que se puede configurar con acceso anónimo es el servicio SMB. Como fue diseñado originalmente para sistemas Windows, necesitamos instalar el servicio samba en nuestra máquina Ubuntu. Al igual que con vsftpd, utilizamos apt para instalar el servicio samba, como se muestra a continuación.

apto para instalar samba

```
root@ubuntu:~# apt install samba
Reading package lists... Done
Building dependency tree
Reading state information... Done
samba is already the newest version (2:4.11.6+dfsg-0ubuntu1)
The following packages were automatically installed and are no longer required:
  libfprint-2-tod1 libllvm9
Use 'sudo apt autoremove' to remove them.
```

Como todos los servicios que se instalan en cualquier máquina Linux, Samba también tiene un archivo de configuración ubicado dentro del directorio /etc. Dado que estamos intentando configurar el servicio con inicio de sesión anónimo, agregaremos algunas configuraciones adicionales en comparación con la instalación básica de samba.

CD /etc/samba/

```
root@ubuntu:~# cd /etc/samba/
root@ubuntu:/etc/samba# nano smb.conf
```

Estamos usando el editor nano, pero básicamente puedes usar cualquier editor de tu elección. Bajando al archivo, agregamos las siguientes configuraciones, como el directorio que se debe usar para compartir los archivos.

Estamos creando el directorio /var/www para este propósito. Necesitamos otorgarle los permisos adecuados, como navegable y público, para que se pueda acceder mediante un inicio de sesión anónimo.

```
# Windows clients look for this share name as a source of downloadable
# printer drivers
[print$]
    comment = Printer Drivers
    path = /var/lib/samba/printers
    browseable = yes
    read only = yes
    guest ok = no
# Uncomment to allow remote administration of Windows print drivers.
# You may need to replace 'lpadmin' with the name of the group your
# admin users are members of.
# Please note that you also need to set appropriate Unix permissions
# to the drivers directory for these users to have write rights in it
;   write list = root, @lpadmin

security = user
map to guest = bad user

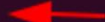
[Shares]
path = /var/www/
available = yes
read only = no
browsable = yes
public = yes
writable = yes
guest ok = yes
```

Lo siguiente que debemos hacer es crear un archivo que pueda usarse para probar la capacidad de transferencia de archivos usando SMB. Creamos un archivo de texto llamado file.txt y lo completamos con el mensaje "Bienvenido a Ignite Technologies". Deberá reiniciar el servicio para activar las configuraciones.

```
cd/var/www
es
archivo gato.txt
```



```
root@ubuntu:~# cd /var/www
root@ubuntu:/var/www# ls
file.txt  html
root@ubuntu:/var/www# cat file.txt
Welcome To Ignite Technologies
root@ubuntu:/var/www#
```



Atacar a PYMES anónimas

Como hicimos con el servicio FTP, también es posible comprobar si el servicio se está ejecutando en la máquina de destino mediante el escaneo nmap. Aunque no lo vamos a demostrar aquí. Vamos a proceder asumiendo que el servicio está funcionando en la máquina de destino. Nos conectamos al servicio mediante smbclient. En la imagen a continuación queda bastante claro que no proporcionamos una combinación de usuario o contraseña para conectarse al servicio ya que el inicio de sesión anónimo está habilitado. Luego enumeramos los recursos compartidos y encontramos el archivo.txt compartido. Transferimos el archivo a la máquina Kali Linux local y confirmamos que el SMB

El servicio de inicio de sesión anónimo está activo y funcionando.

```
clientesmb -L //192.168.1.46
smbclient //192.168.1.46/acciones
archivo gato.txt
```

```

(root@kali)-[~/Desktop]
# smbclient -L //192.168.1.46
Enter WORKGROUP\root's password:

      Sharename      Type      Comment
      ─────────      ───      ─────────
      print$         Disk      Printer Drivers
      Shares          Disk
      IPC$           IPC       IPC Service (ubuntu server (Samba, Ubuntu))
SMB1 disabled -- no workgroup available

(root@kali)-[~/Desktop]
# smbclient //192.168.1.46/shares
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> ls

.                D            0   Thu May 13 14:26:24 2021
..               D            0   Thu May 13 14:24:57 2021
html             D            0   Thu May 13 14:24:58 2021
file.txt         N            31  Thu May 13 14:26:24 2021

19992176 blocks of size 1024. 11382112 blocks available
smb: \> get file.txt
getting file \file.txt of size 31 as file.txt (5.0 KiloBytes/sec) (average 5.0
smb: \> exit

(root@kali)-[~/Desktop]
# cat file.txt
Welcome To Ignite Technologies

```

Conclusión

Los inicios de sesión anónimos son bastante comunes en entornos de la vida real y también en los desafíos de Capture the Flags. Como atacante, es importante comprender cómo funciona y qué tipo de configuración se requiere para habilitar el inicio de sesión anónimo. Sobre todo, es importante saber cómo interactuar con este tipo de acceso.

ÚNETE A NUESTRO PROGRAMAS DE ENTRENAMIENTO

