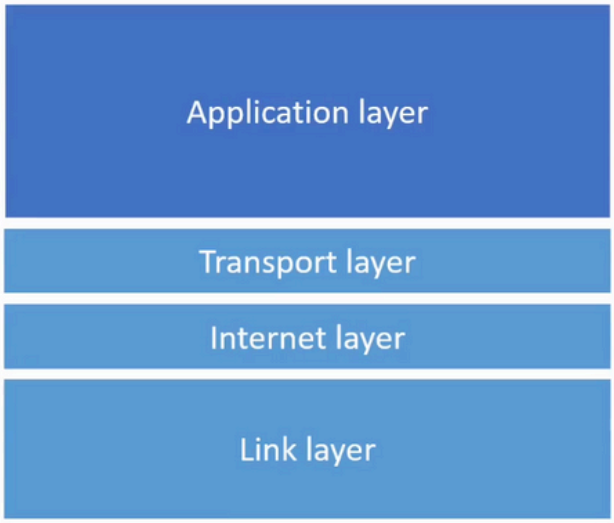
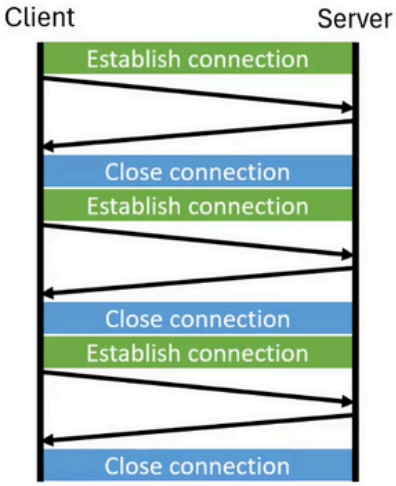
Transport layer protocols

- Hypertext Transfer Protocol (HTTP)
- Domain Name System (DNS)
- File Transfer Protocol (FTP)
- Secure Shell Protocol (SSH)
- Simple Mail Transfer Protocol (SMTP)

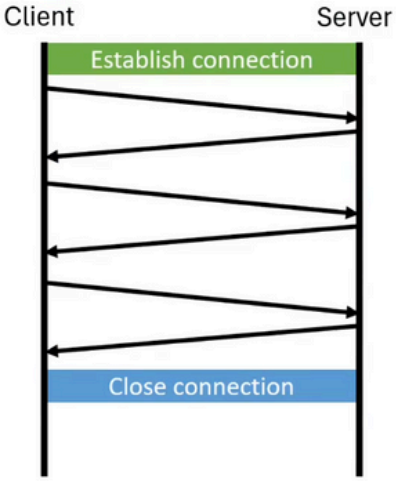


Hypertext Transfer Protocol (HTTP)

- HTTP no persistent



- HTTP persistent



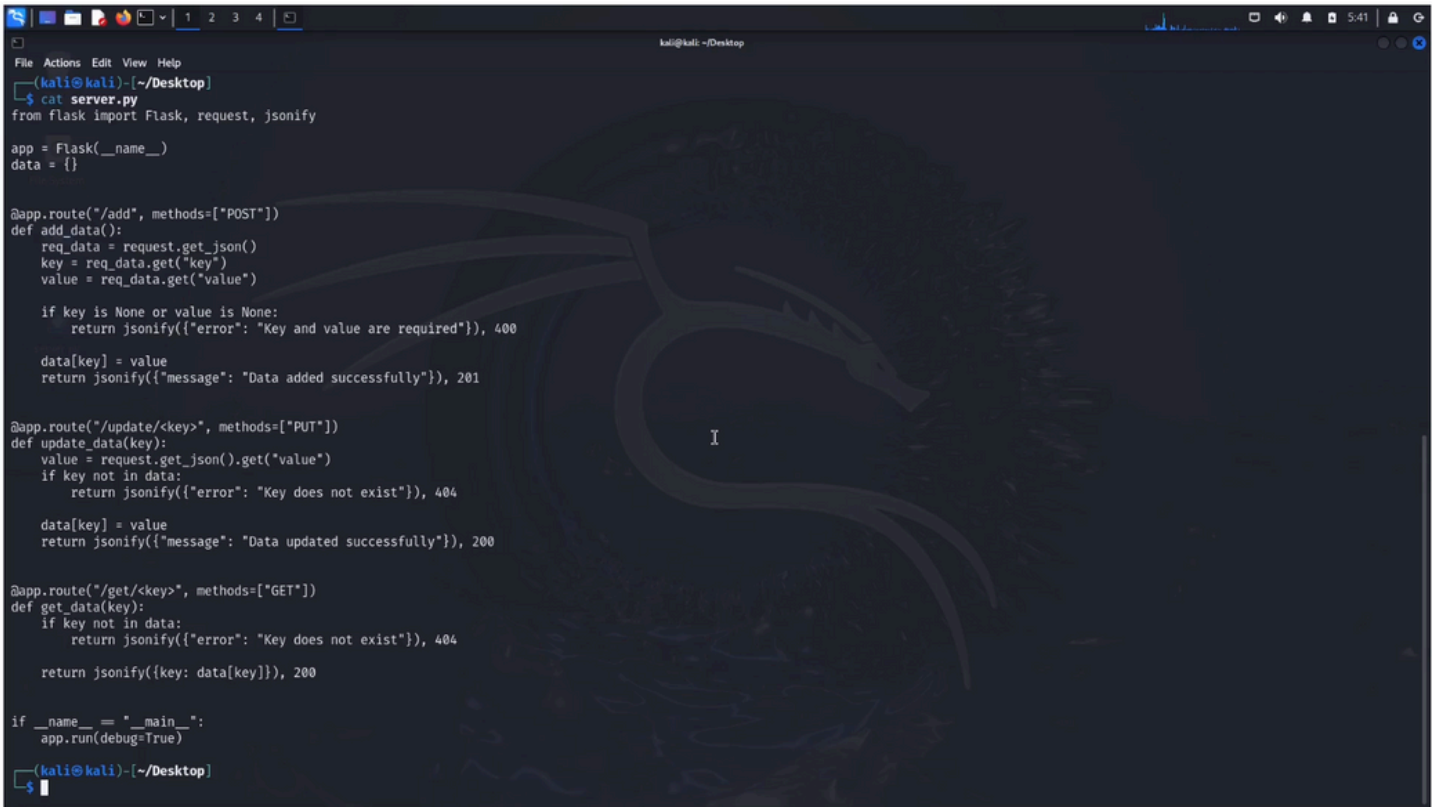
Hypertext Transfer Protocol (HTTP)

```
GET / HTTP/1.1
Host: www.example.com
User-Agent: Mozilla/5.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

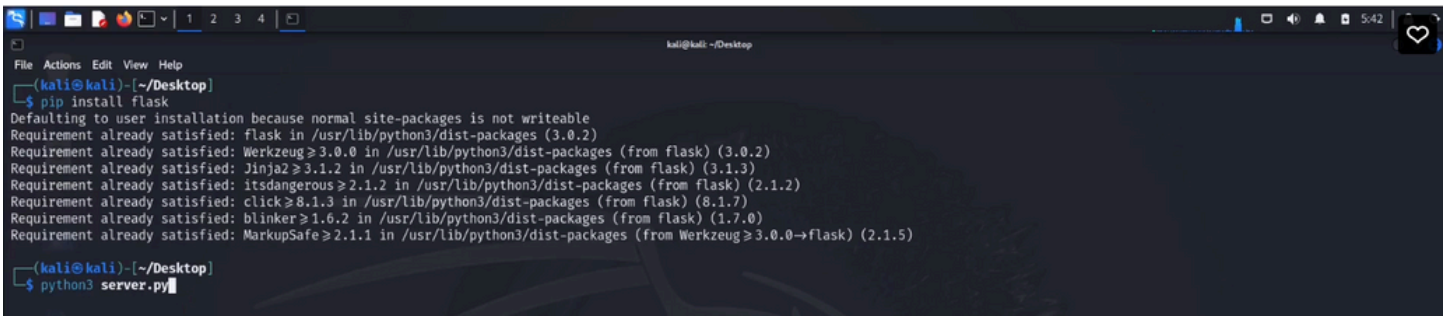
Hypertext Transfer Protocol (HTTP)

```
HTTP/1.1 200 OK
Date: Mon, 23 May 2005 22:38:34 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 155
Last-Modified: Wed, 08 Jan 2003 23:11:55 GMT
Server: Apache/1.3.3.7 (Unix) (Red-Hat/Linux)
ETag: "3f80f-1b6-3e1cb03b"
Accept-Ranges: bytes
Connection: close

<html>
  <head>
    <title>An Example Page</title>
  </head>
  <body>
    <p>Hello World, this is a very simple HTML document.</p>
  </body>
</html>
```

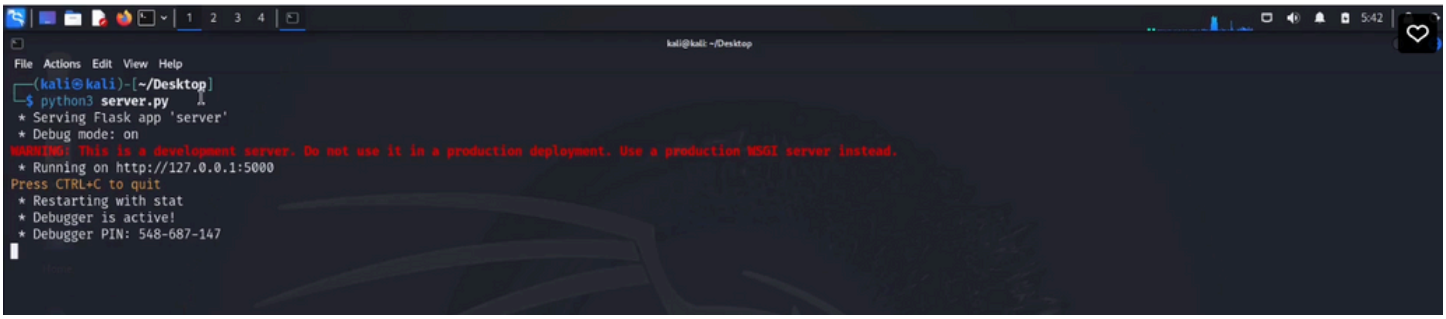
1XX (informational)
2XX (successful)
3XX (redirection)
4XX (client error)
5XX (server error)



```
File Actions Edit View Help
┌──(kali㉿kali)-[~/Desktop]
└─$ cat server.py
from flask import Flask, request, jsonify

app = Flask(__name__)
data = {}


@app.route("/add", methods=["POST"])
def add_data():
    req_data = request.get_json()
    key = req_data.get("key")
    value = req_data.get("value")

    if key is None or value is None:
        return jsonify({"error": "Key and value are required"}), 400

    data[key] = value
    return jsonify({"message": "Data added successfully"}), 201


@app.route("/update/<key>", methods=["PUT"])
def update_data(key):
    value = request.get_json().get("value")
    if key not in data:
        return jsonify({"error": "Key does not exist"}), 404

    data[key] = value
    return jsonify({"message": "Data updated successfully"}), 200


@app.route("/get/<key>", methods=["GET"])
def get_data(key):
    if key not in data:
        return jsonify({"error": "Key does not exist"}), 404

    return jsonify({key: data[key]}), 200


if __name__ == "__main__":
    app.run(debug=True)

┌──(kali㉿kali)-[~/Desktop]
└─$
```



```
File Actions Edit View Help
┌──(kali㉿kali)-[~/Desktop]
└─$ pip install flask
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: flask in /usr/lib/python3/dist-packages (3.0.2)
Requirement already satisfied: Werkzeug≥3.0.0 in /usr/lib/python3/dist-packages (from flask) (3.0.2)
Requirement already satisfied: Jinja2≥3.1.2 in /usr/lib/python3/dist-packages (from flask) (3.1.3)
Requirement already satisfied: itsdangerous≥2.1.2 in /usr/lib/python3/dist-packages (from flask) (2.1.2)
Requirement already satisfied: click≥8.1.3 in /usr/lib/python3/dist-packages (from flask) (8.1.7)
Requirement already satisfied: blinker≥1.6.2 in /usr/lib/python3/dist-packages (from flask) (1.7.0)
Requirement already satisfied: MarkupSafe≥2.1.1 in /usr/lib/python3/dist-packages (from Werkzeug≥3.0.0→flask) (2.1.5)

┌──(kali㉿kali)-[~/Desktop]
└─$ python3 server.py
```

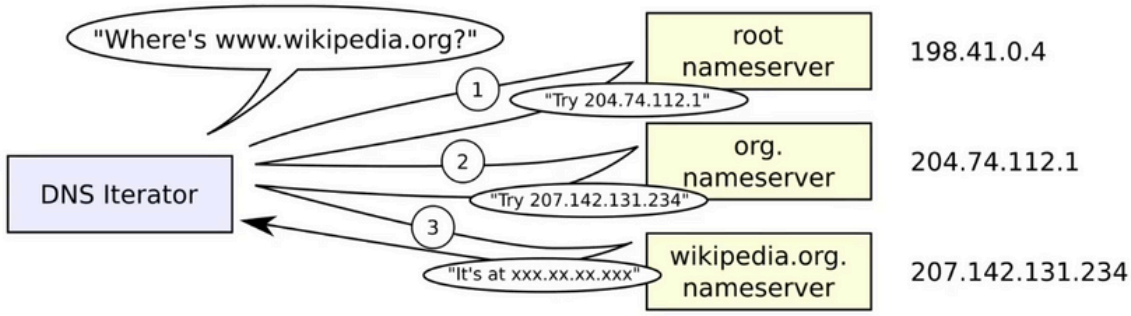


```
File Actions Edit View Help
┌──(kali㉿kali)-[~/Desktop]
└─$ python3 server.py
 * Serving Flask app 'server'
 * Debug mode: on
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
 * Running on http://127.0.0.1:5000
Press CTRL+C to quit
 * Restarting with stat
 * Debugger is active!
 * Debugger PIN: 548-687-147
```

```
File Actions Edit View Help
kali@kali: ~/Desktop ×  kali@kali: ~/Desktop ×
┌──(kali㉿kali)-[~/Desktop]
└─$ curl -X POST -H "Content-Type: application/json" -d '{"key": "1", "value": "John Doe"}' http://localhost:5000/add
{
  "message": "Data added successfully"
}

┌──(kali㉿kali)-[~/Desktop]
└─$ curl http://localhost:5000/get/1
{
  "1": "John Doe"
}

┌──(kali㉿kali)-[~/Desktop]
└─$ curl -X PUT -H "Content-Type: application/json" -d '{"value": "Jane Doe"}' http://localhost:5000/update/1
{
  "message": "Data updated successfully"
}

┌──(kali㉿kali)-[~/Desktop]
└─$ curl http://localhost:5000/get/1
{
  "1": "Jane Doe"
}

┌──(kali㉿kali)-[~/Desktop]
└─$
```

Domain Name System (DNS)

- Hierarchical and distributed naming system for computers, services, and other resources on the Internet.

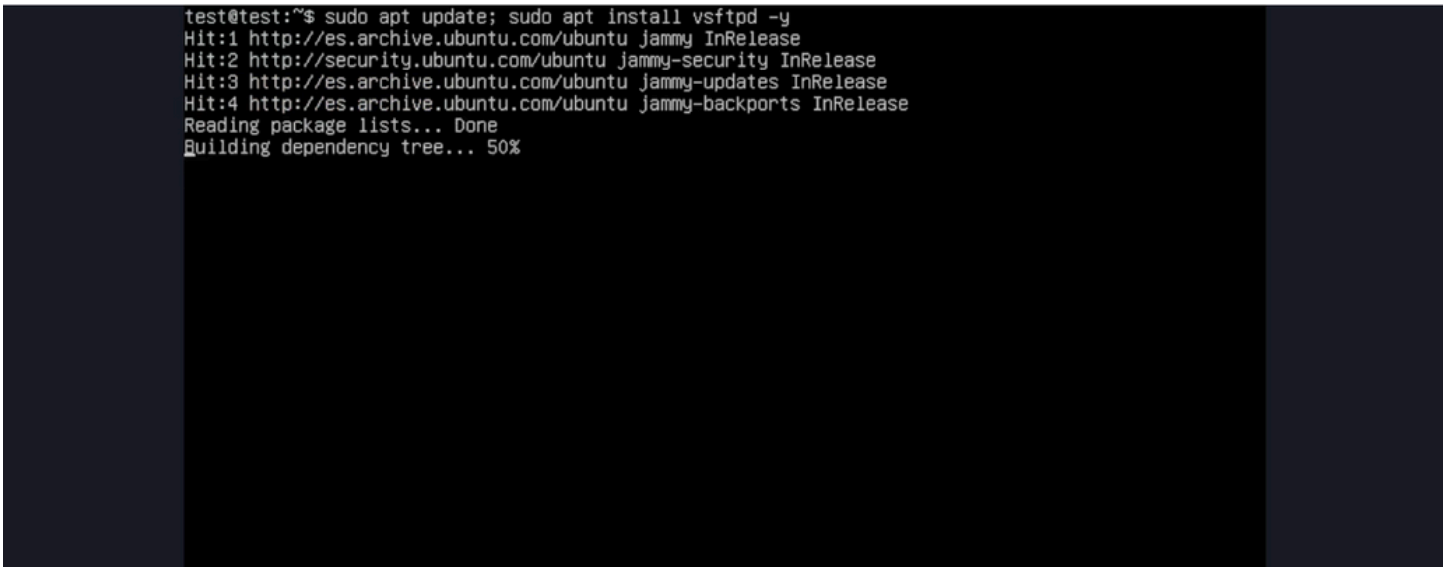


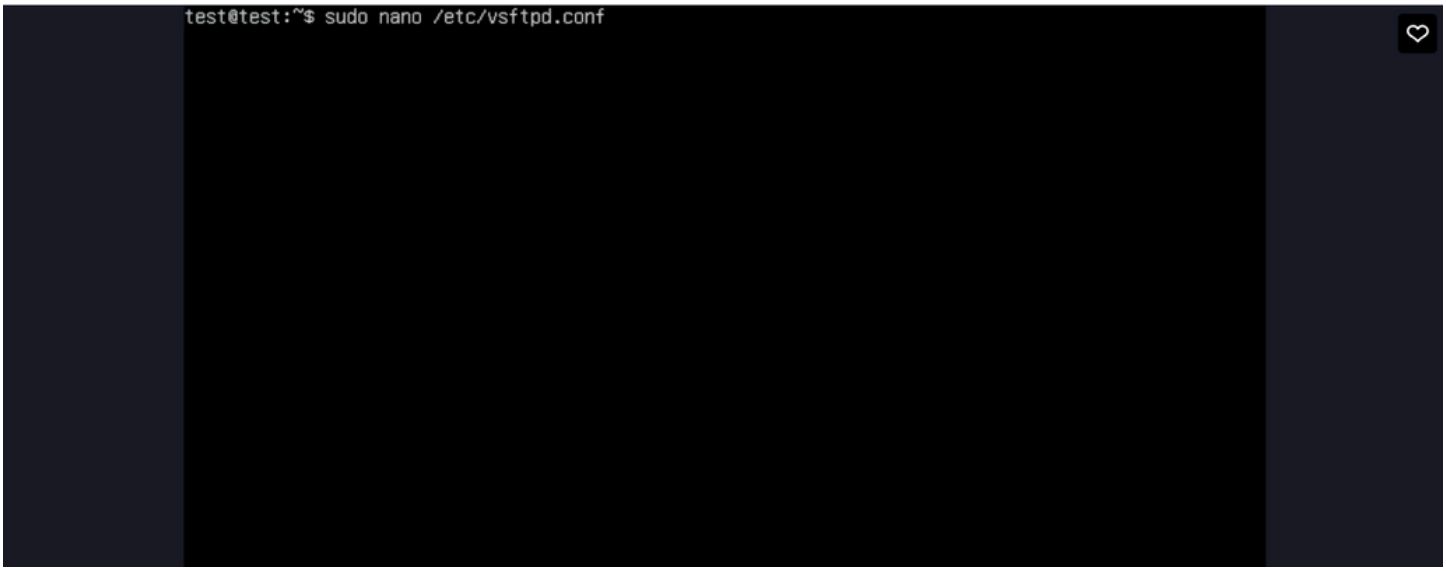
Domain Name System (DNS)

```
example.com                     NS      ns1.example.com
example.com                     NS      ns2.example.com
ns1.example.com                 A       XXX.XXX.Y.Z
ns2.example.com                 A       XXX.XXX.Y.Z
example.com                     A       XXX.XXX.Y.Z
www.example.com                 A       XXX.XXX.Y.Z
example.com                     AAAA    YYYY:ZZZZ:X:XXXX::
www.example.com                 AAAA    YYYY:ZZZZ:X:XXXX::
mail.example.com.               A       XXX.XXX.Y.Z
webmail.example.com.            A       XXX.XXX.Y.Z
ftp.example.com.                CNAME   example.com
example.com.                    MX      10 mail.example.com.
_domainkey.example.com.         TXT     "o=-"
default._domainkey.example.com  TXT     "p=;"
```

File Transfer Protocol (FTP)

- ls
- cd
- pwd
- **get**
- **put**
- mkdir
- rmdir
- **delete**
- **rename**
- chmod
- **quit**
- **help**



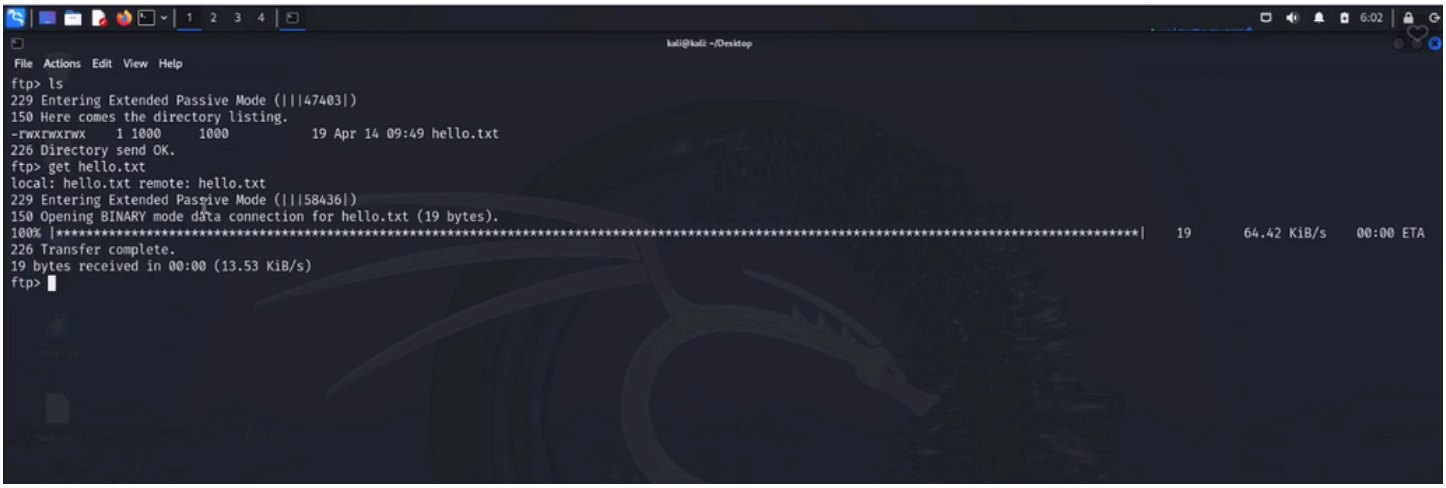


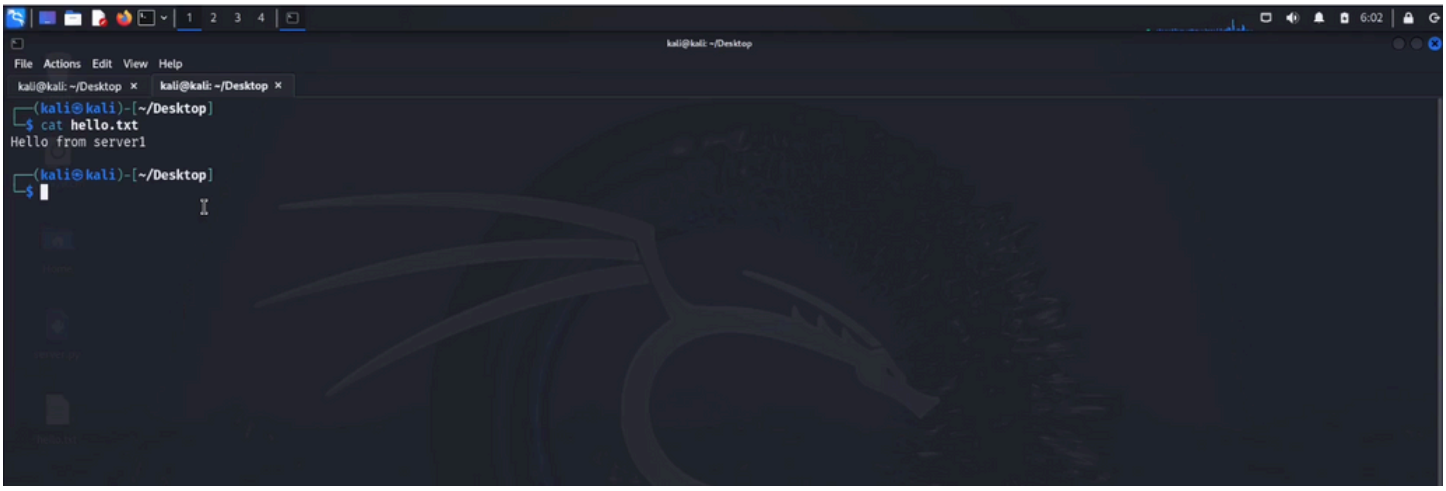
```
  GNU nano 6.2                                /etc/vsftpd.conf
# Example config file /etc/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# 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.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,


test@test:~$
```

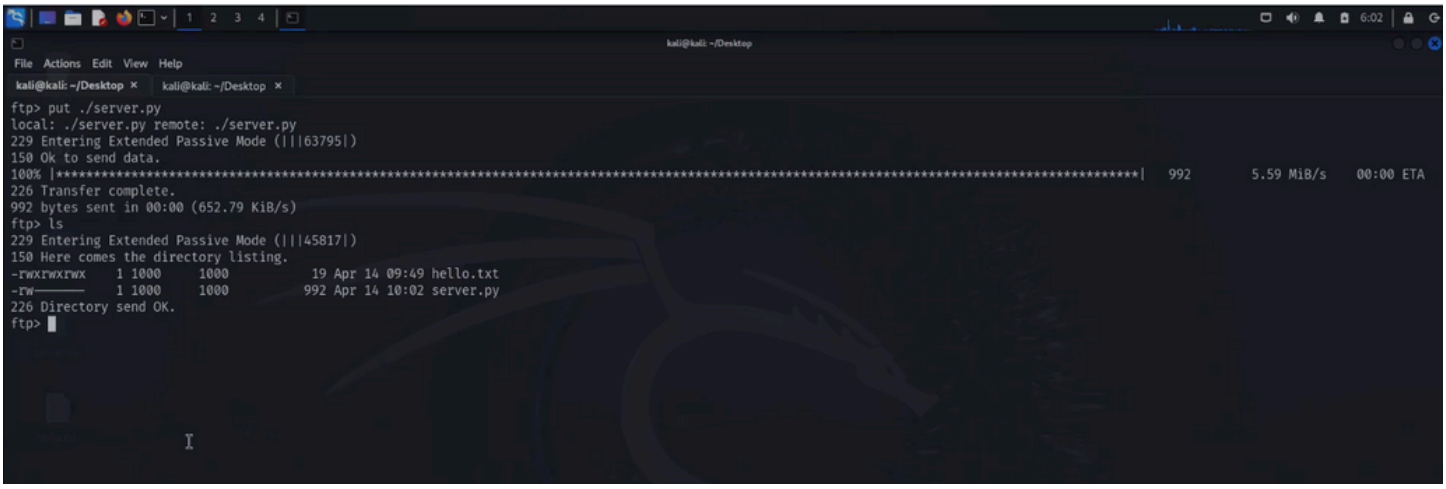
```
test@test:~$ sudo systemctl restart vsftpd.service _
```

```
test@test:~$ sudo systemctl status vsftpd.service
● vsftpd.service - vsftpd FTP server
     Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; vendor preset: enabled)
     Active: active (running) since Sun 2024-04-14 10:00:48 UTC; 5s ago
    Process: 3538 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
   Main PID: 3539 (vsftpd)
      Tasks: 1 (limit: 2220)
     Memory: 852.0K
        CPU: 3ms
     CGroup: /system.slice/vsftpd.service
             └─3539 /usr/sbin/vsftpd /etc/vsftpd.conf

Apr 14 10:00:48 test systemd[1]: Starting vsftpd FTP server...
Apr 14 10:00:48 test systemd[1]: Started vsftpd FTP server.
test@test:~$ _
```

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~/Desktop]
└─$ ftp 10.0.1.13
Connected to 10.0.1.13.
220 (vsFTPd 3.0.5)
Name (10.0.1.13:kali): test
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> help
Commands may be abbreviated.  Commands are:

!               cdup            epsv4           hash            mdelete         mput            pdir            quote           rmdir           struct          user
$               chmod           epsv6           help            mdir            mreget          pls             rate            rstatus         sunique         verbose
account         close           exit            idle            mget            msend           pmlsd           rcvbuf          runique         system          xferbuf
append          cr              features        image           mkdir           newer           preserve        recv            send            tenex           ?
ascii           debug           fget            lcd             mls             nlist           progress        reget           sendport        throttle
bell            delete          form            less            mlsd            nmap            prompt          remopts         set             trace
binary          dir             ftp             lpage           mlst            ntrans          proxy           rename          site            type
bye             disconnect      gate            lpwd            mode            open            put             reset           size            umask
case            edit            get             ls              modtime         page            pwd             restart         sndbuf          unset
cd              epsv            glob            macdef          more            passive         quit            rhelp           status          usage
ftp>
```


kali@kali: ~/Desktop
File Actions Edit View Help
ftp> ls
229 Entering Extended Passive Mode (|||47403|)
150 Here comes the directory listing.
-rwxrwxrwx 1 1000 1000 19 Apr 14 09:49 hello.txt
226 Directory send OK.
ftp> get hello.txt
local: hello.txt remote: hello.txt
229 Entering Extended Passive Mode (|||58436|)
150 Opening BINARY mode data connection for hello.txt (19 bytes).
100% |**********| 19 64.42 KiB/s 00:00 ETA
226 Transfer complete.
19 bytes received in 00:00 (13.53 KiB/s)
ftp>


kali@kali: ~/Desktop
File Actions Edit View Help
kali@kali: ~/Desktop
kali@kali: ~/Desktop
(kali㉿kali)-[~/Desktop]
$ cat hello.txt
Hello from server1
(kali㉿kali)-[~/Desktop]
$


kali@kali: ~/Desktop
File Actions Edit View Help
kali@kali: ~/Desktop
kali@kali: ~/Desktop
ftp> put ./server.py
local: ./server.py remote: ./server.py
229 Entering Extended Passive Mode (|||63795|)
150 Ok to send data.
100% |**********| 992 5.59 MiB/s 00:00 ETA
226 Transfer complete.
992 bytes sent in 00:00 (652.79 KiB/s)
ftp> ls
229 Entering Extended Passive Mode (|||45817|)
150 Here comes the directory listing.
-rwxrwxrwx 1 1000 1000 19 Apr 14 09:49 hello.txt
-rw------- 1 1000 1000 992 Apr 14 10:02 server.py
226 Directory send OK.
ftp>