RPC

1. With the rpc protocol, how many users can you find ?
   Your response Your command

```
┌──(kali㉿ntsapi)-[~]
└─$ rpcinfo -p 10.13.1.36 | wc -l
23
```

2. What is the rid of msfadmin?
   Your response Your command

```
┌──(kali㉿ntsapi)-[~]
└─$ rpcclient -U "" -N 10.13.1.36
rpcclient $> enumdomusers
user:[games] rid:[0x3f2]
```

   or

```
user_rid :      0xbb8
```

```
┌──(kali㉿ntsapi)-[~]
└─$ rpcclient -U "" 10.13.1.36
Password for [WORKGROUP\]:
rpcclient $> queryuser msfadmin
```

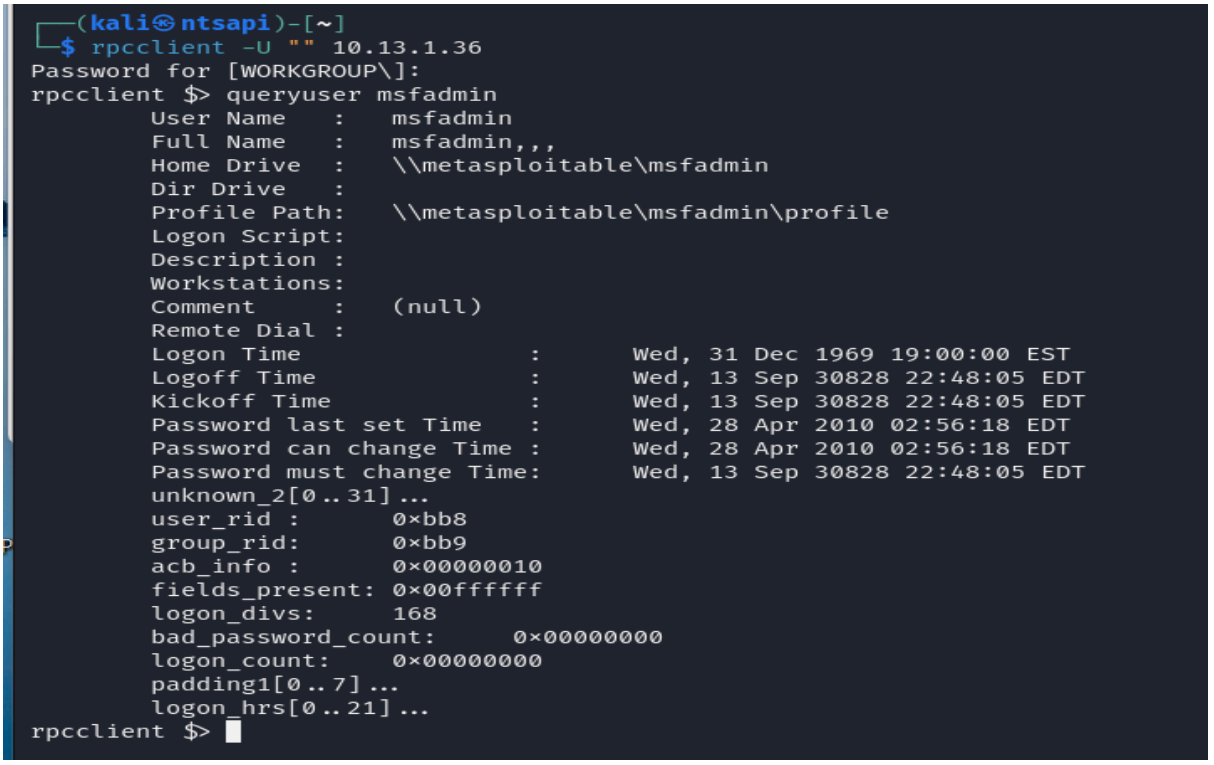
   Password: enumdomusers

3. What is the path of msfadmin's profile?
   Your response Your command
   Same command on the screenshot:
   Profile Path: \\metasploitable\msfadmin\profile

4. When did msadmin last change password?
   Your response Your command
   Same command on the screenshot
   Password last set Time : Wed, 28 Apr 2010 02:56:18 EDT

5. When should msfadmin change its password?
   Your response Your command
   Same command on the screenshot
   Password must change Time: Wed, 13 Sep 30828 22:48:05 EDT

   Details:


┌──(kali㉿ntsapi)-[~]
└─$ rpcclient -U "" 10.13.1.36
Password for [WORKGROUP\]:
rpcclient $> queryuser msfadmin
User Name : msfadmin
Full Name : msfadmin,,,
Home Drive : \\metasploitable\msfadmin
Dir Drive :
Profile Path: \\metasploitable\msfadmin\profile
Logon Script:
Description :
Workstations:
Comment : (null)
Remote Dial :
Logon Time : Wed, 31 Dec 1969 19:00:00 EST
Logoff Time : Wed, 13 Sep 30828 22:48:05 EDT
Kickoff Time : Wed, 13 Sep 30828 22:48:05 EDT
Password last set Time : Wed, 28 Apr 2010 02:56:18 EDT
Password can change Time : Wed, 28 Apr 2010 02:56:18 EDT
Password must change Time: Wed, 13 Sep 30828 22:48:05 EDT
unknown_2[0..31]...
user_rid : 0xbb8
group_rid: 0xbb9
acb_info : 0x00000010
fields_present: 0x00ffffff
logon_divs: 168
bad_password_count: 0x00000000
logon_count: 0x00000000
padding1[0..7]...
logon_hrs[0..21]...
rpcclient $>