TASK 1: Connecting to a user remotely

|  |
| --- |
| **TOOLS** : Netcate |
| Arguments that can be passed for netcate |

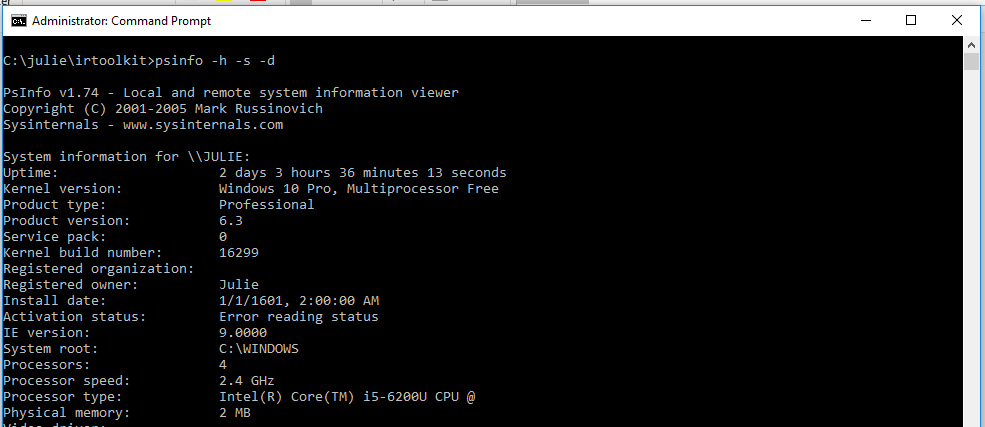
**SCREENSHOT**

****

|  |  |
| --- | --- |
| COMMAND : nc –v –l –p 2222 > volatile\_julie.txt |  |

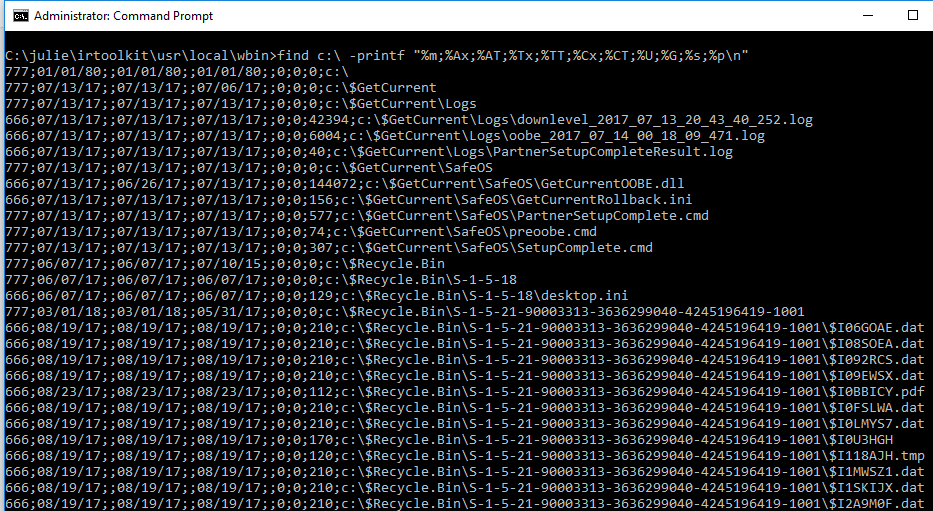
|  |  |
| --- | --- |
| TASK 2: GET SYSTEM VERSION AND PATCH LEVEL | |
| TOOLS REQUIRED TO PERFORM TASK : psinfo | |
| ARGUMENTS & FILTERS |  |
| psinfo |  |
| -h | is used to show installed hotfixes |
| -s | is used to show installed software |
| -d | is used to show disk volume information |

**Screenshort**



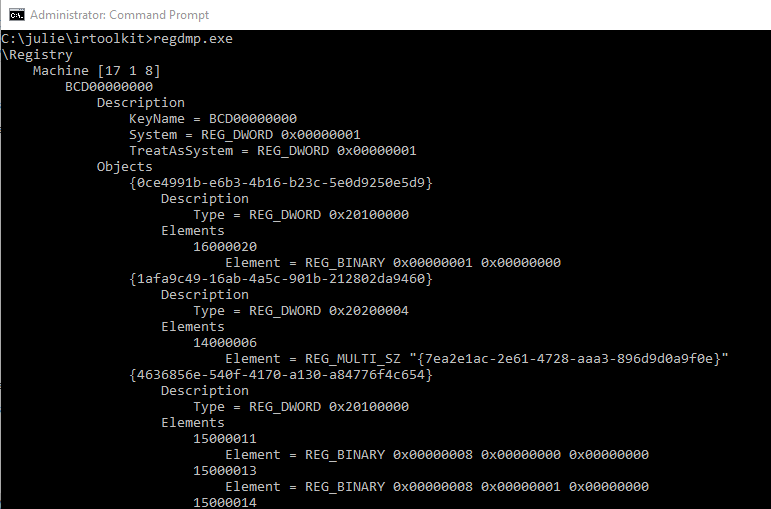
|  |
| --- |
| COMMAND : psinfo -h -s -d |

|  |  |
| --- | --- |
| TASK 3: GET FILE SYSTEM TIME AND DATE STAMPS | |
| TOOLS REQUIRED: UnxUtils | |
| ARGUMENTS |  |
| c:\ -printf “%m;%Ax;%AT;%Tx;%TT;%Cx;%CT;%U;%G;%s;%p\n” | prints the file permissions, last access date, last access time, modification date, modification time, created date, created time, user ownership, group ownership, file size, and the full path of every file on the C drive |



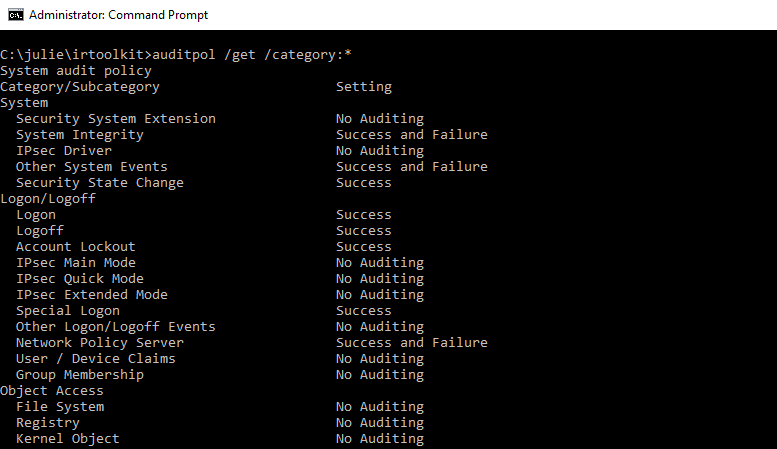
|  |
| --- |
| Command find c:\ -printf “%m;%Ax;%AT;%Tx;%TT;%Cx;%CT;%U;%G;%s;%p\n” |

|  |  |
| --- | --- |
| TASK 4 : GET REGISTRY DATA | |
| TOOLS REQUIRED TO PERFORM TASK 4: regDmp  Task : Get Registry data | |
| ARGUMENTS |  |
| regDmp | capture the complete registry |



|  |
| --- |
| **Command**: regdmp.exe |

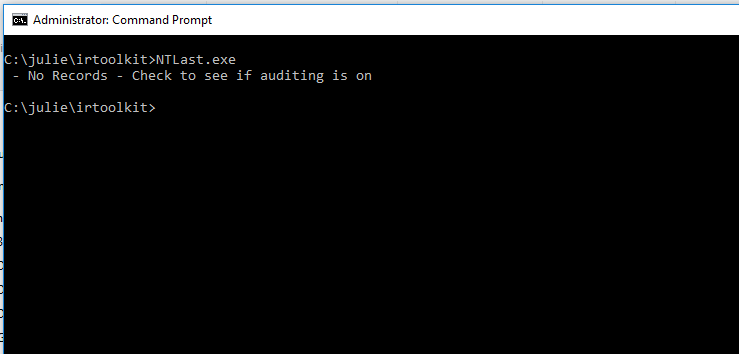


****

|  |
| --- |
| COMMAND : auditpol /get /category:\*  This command will display the current security policy in categories |

**TASK 6**: A History of Logins

|  |  |
| --- | --- |
| **TOOLS** : NTLAST | |
| Arguments that can be passed for **NTLAST** | |
| -s | Last Successful Logons |
| -f | Last Failed Logons |
| -i | Last Interactive Logons |
| -r | Last Remote Logons |
| -u [u] | Logons by User – [u] = case sensitive username |
| -v | Verbose Output - shows logon/logoff/duration |
| -mil | Military Time Output - Default matches event log time |
| -file | File name - Saved .evt sec log to open |
| -csv | Print output as CSV |
| -l | Last Successful Logon |
| -l:i | Last Interactive Logon |

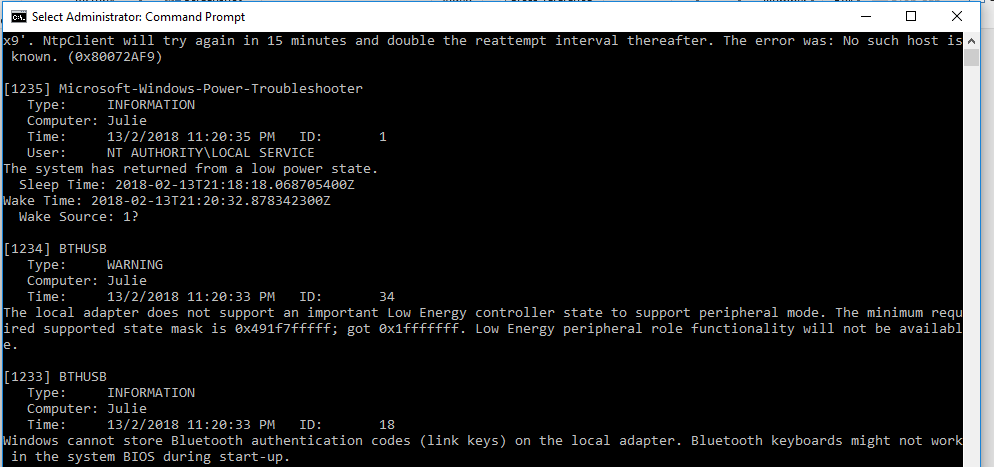


|  |
| --- |
| COMMAND : ntlast.exe |

**TASK 7**: GET SYSTEM LOG EVENTS

|  |  |
| --- | --- |
| **TOOLS** : PsLogList | |
| Arguments that can be passed for **DATE** | |
| el |enum logs | List log names |
| gl | get-log | Gets log configuration information |
| sl|set-log | Modify configuration of a log |
| qe|query-events | Query from an existing log files |
| Epl | export-log | Export a log |
| al | archive-log | Archive an exported log |
| Cl | clear-log | Clears a log |

**SCREENSHOT:**

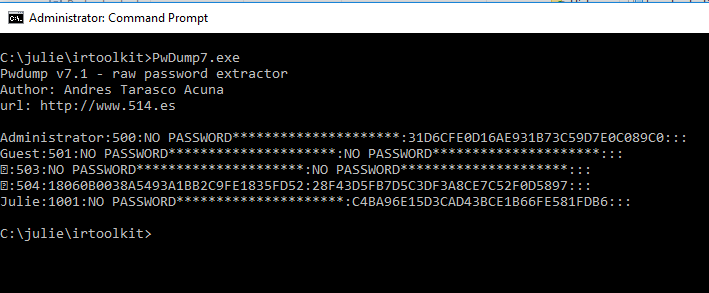
****

|  |
| --- |
| COMMAND : PsLogList  This command will export a system log to a file named logs.evtx |

TASK 8: COLLECTING DUMP FILE OF PASSWORDS

|  |  |
| --- | --- |
| **TOOLS:** PWDUMP | |
| Arguments that can be passed for **pwdump** | |
| **-h** | **the ip of the host** |
| **-u** | **the username** |
| **-p** | **the password** |

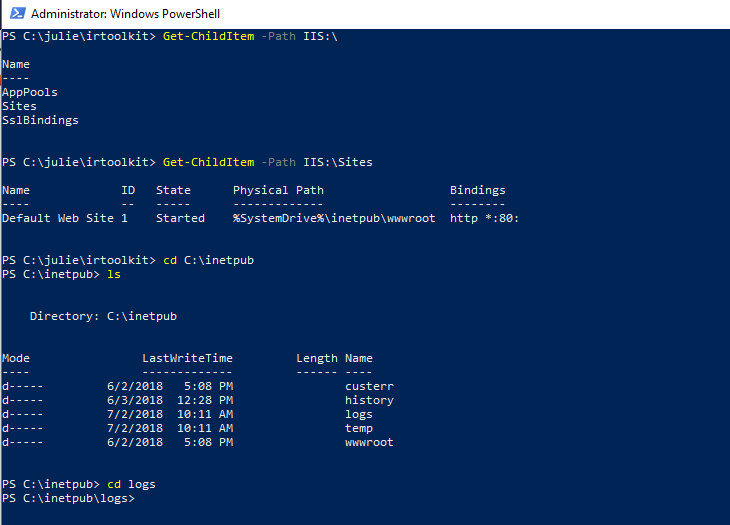
**SCREENSHOT:**

****

|  |
| --- |
| COMMAND : PwDump7.exe  This command will detect and start to dump passwords of the windows operating system |

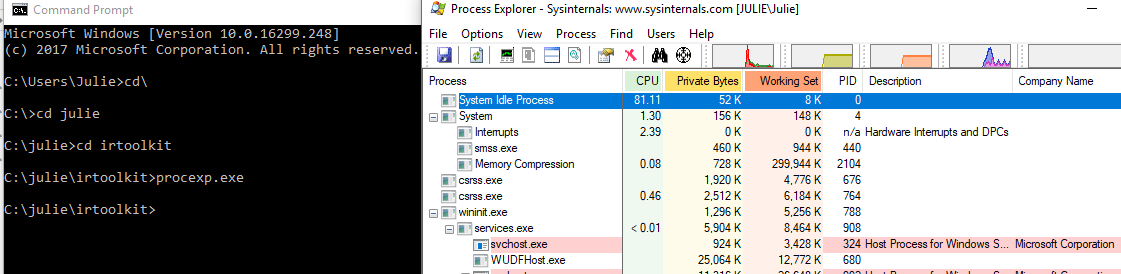
|  |
| --- |
| **TASK 9**: IIS LOGS |
| **TOOLS:** Powershell |

**SCREENSHOT:**



|  |
| --- |
| COMMAND : Get-ChildItem -Path IIS:\  This command will display files that were accessed in the last 30 minutes |

|  |
| --- |
| **TASK 10: Suspicious Files** |
|  |

****