

***COMPUTER FORENSICS LAB TWO***

***Windows Live Response***

Assignment by

**NATHAN ISHEANESU NYABVURE**

**H140177Q**

**BACHELOR OF TECHNOLOGY IN INFORMATION SECURITY AND ASSURANCE**

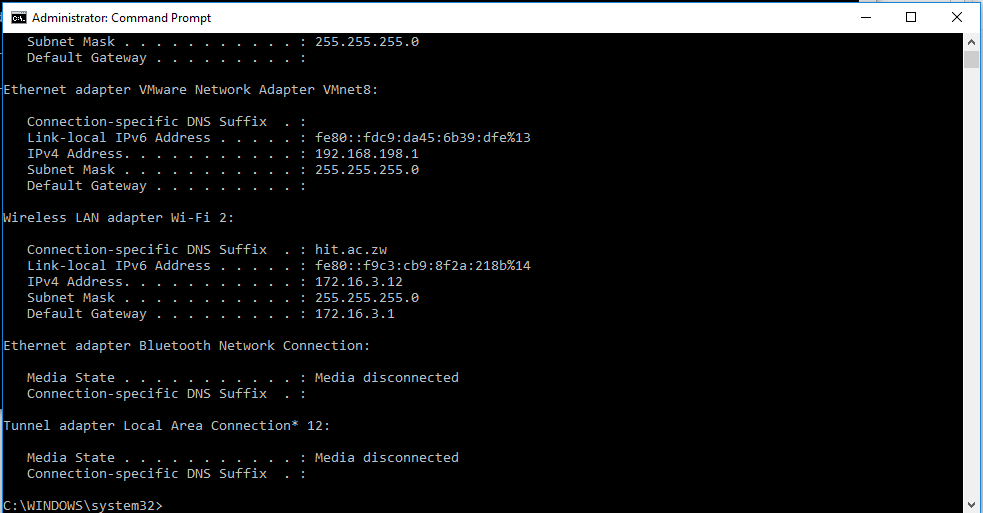
SCHOOLOF INFORMATION SCIENCES AND TECHNOLOGY

**HARARE INSTITUTE OF TECHNOLOGY**

**Lecturer: Mr T Marengereke**

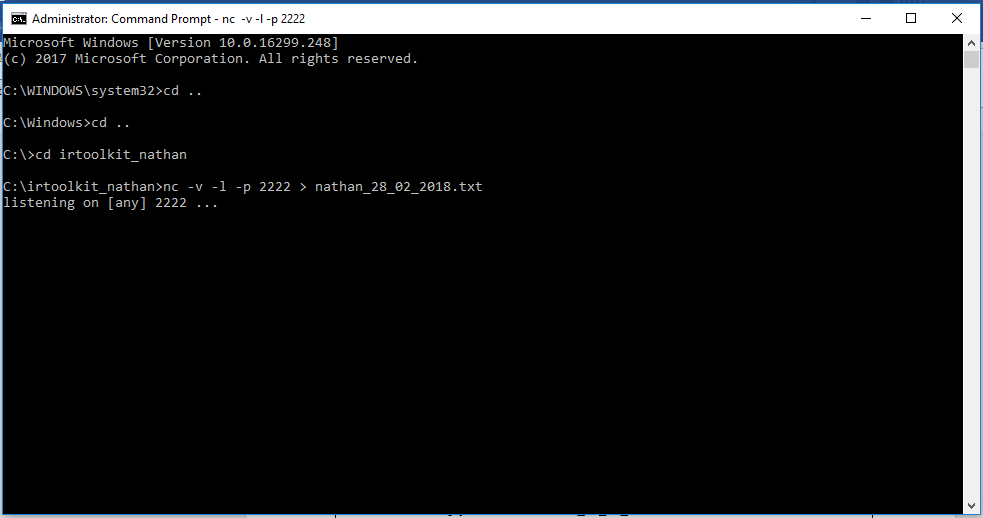
***February 2018***

|  |  |  |
| --- | --- | --- |
| Task 1: Use netcat to send files from the victim’s machine to a remote machine | | |
| TOOLS REQUIRED TO PERFORM TASK: netcat.exe | | |
| ***LIST ALL FILTERS/ ARGUMENTS THAT CAN BE PASSED FOR THE TOOL/ COMMAND*** | | |
| –v | View form remote machine | |
| -I | | It places the client machine in listen mode |
| -p | | It highlights the local port, it defines the source ports for packets |

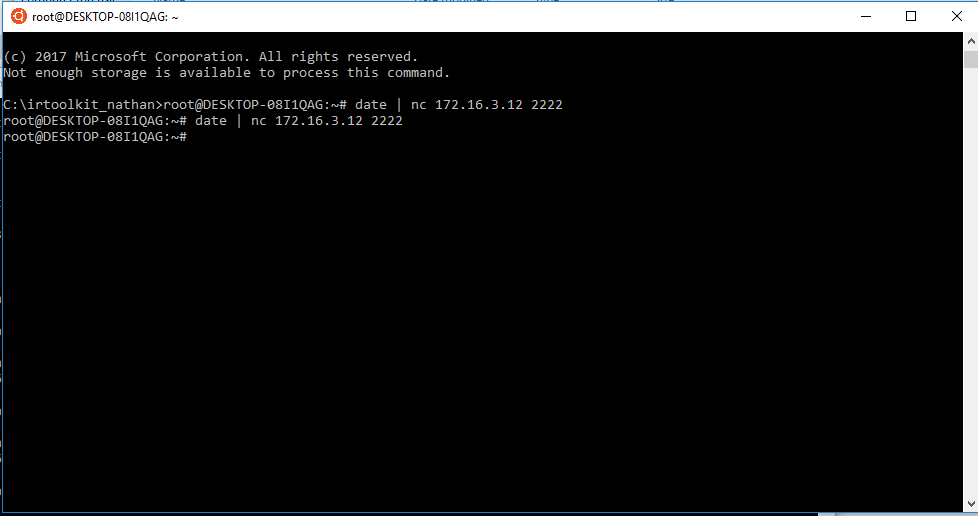
Step 1: Start a new command prompt to access your IP address   


Step 2: On the client machine run the command

***nc –v –l –p 2222 > nathan\_28\_02\_2018.txt*** to establish the netcat sever

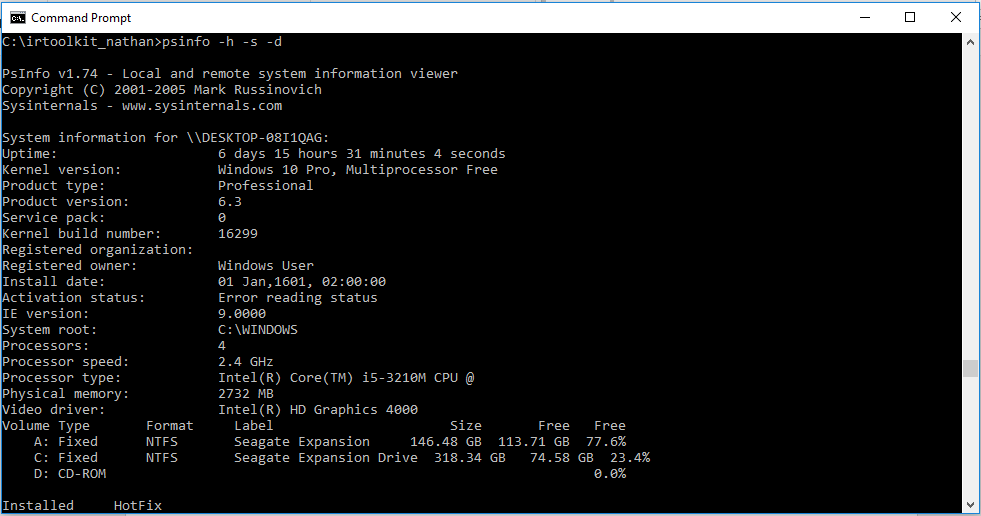


Step 3: on the remote machine open ubuntu and telnet into the machine. Press enter and a txt file with date will be created.



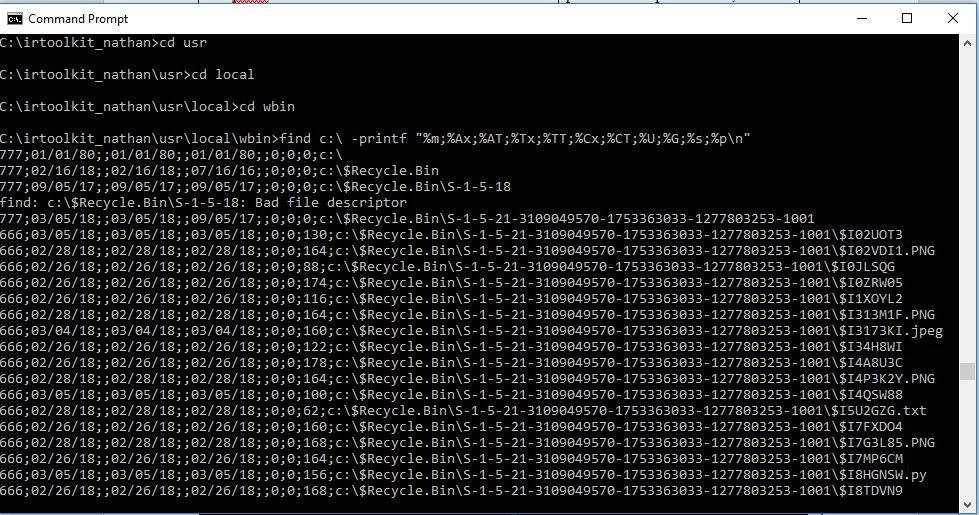
|  |
| --- |
| COMMAND: ***nc –v –l –p 2222 > nathan\_28\_02\_2018.txt***  ***“date* | *nc 172.16.3.12 2222”*** |

|  |  |
| --- | --- |
| *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 |



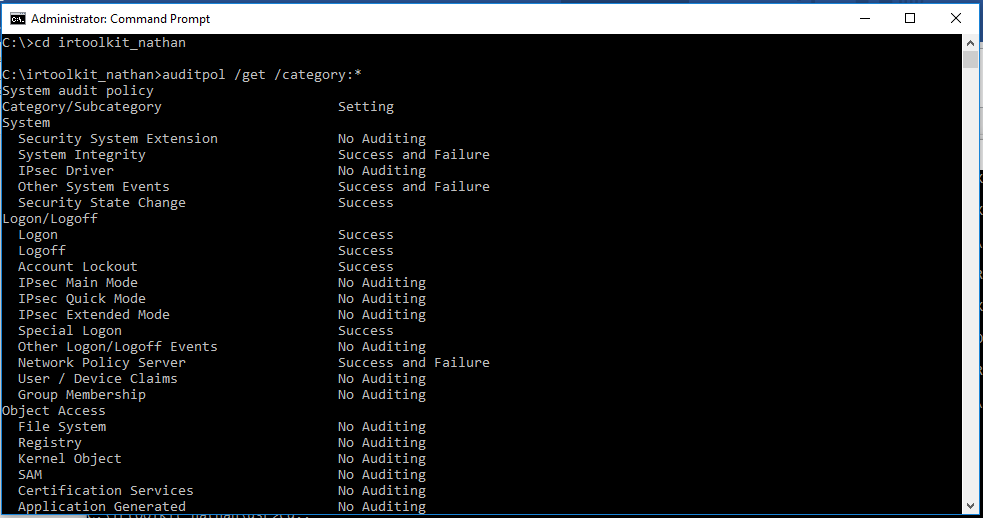
|  |
| --- |
| COMMAND : psinfo -h -s -d |

|  |  |
| --- | --- |
| *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 |



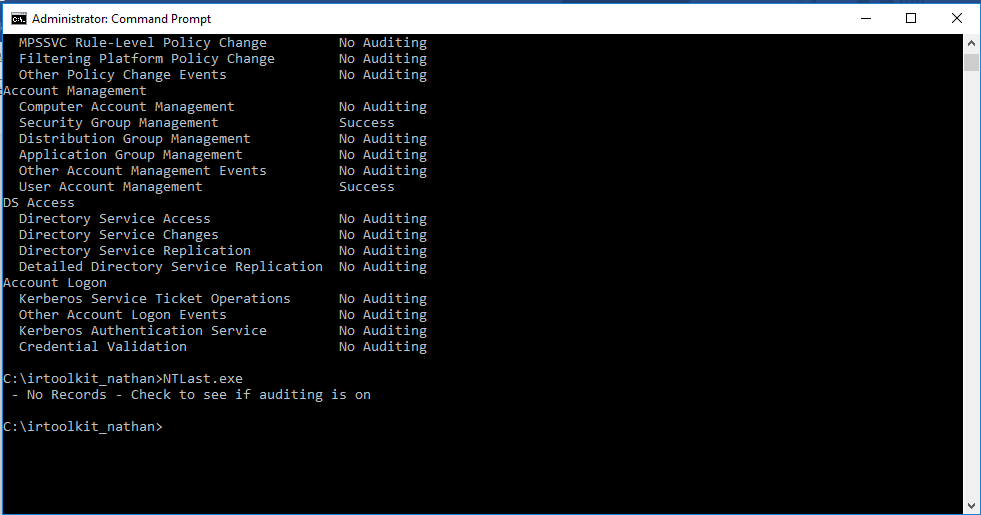
|  |
| --- |
| **Command**: usr\local\wbin>find c:\ -printf "%m;%Ax;%AT;%Tx;%TT;%Cx;%CT;%U;%G;%s;%p\n" |

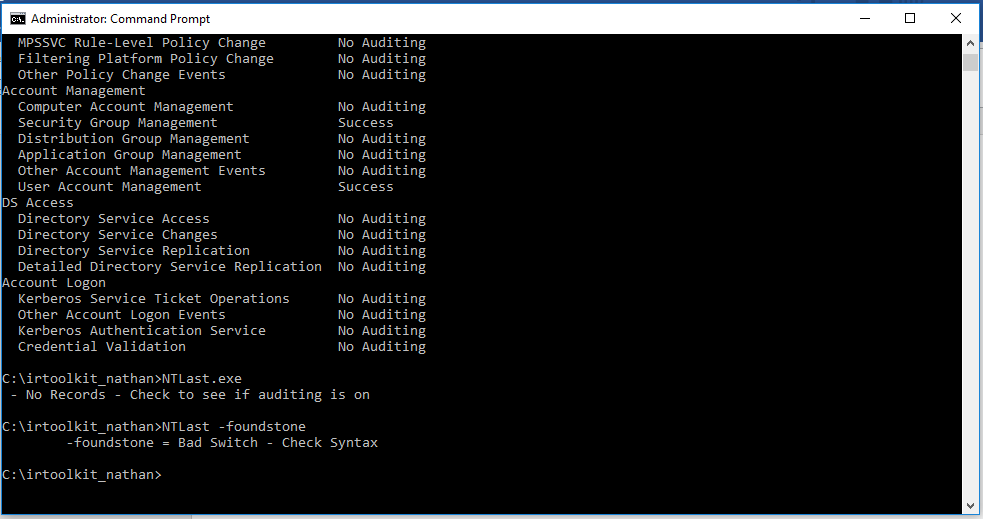
|  |  |
| --- | --- |
| *TASK 4: GET THE AUDIT POLICY* | |
| *TOOLS : AUDITPOL* | |
| **Arguments that can be passed for AUDITPOL** | |
| /? | Help |
| /get | Displays current audit policy |
| /set | Sets the audit policy |
| /list | Displays selective policy elements |
| /backup | Backups the current security policy to a file |
| /restore | Restores a policy from a backup file |
| /remove | Removes the per user audit policy for a user account |



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

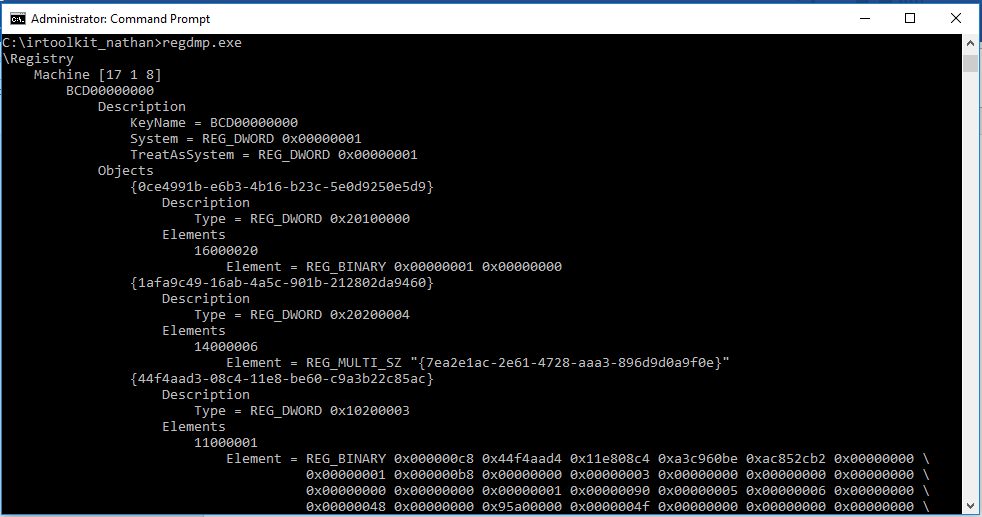
|  |  |
| --- | --- |
| *TASK 5: HISTORY OF LOGINS* | |
| *TOOLS : NTLAST* | |
| **Arguments that can be passed for NTLAST** | |
| -s | Last Successful Logons |
| -f | Last Failed Logons |
| -i | Last Interactive Logons |
| -r | Last Remote Logons |
| -u [u] | Logons by User – [u] = case sensitive username |
| -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 |





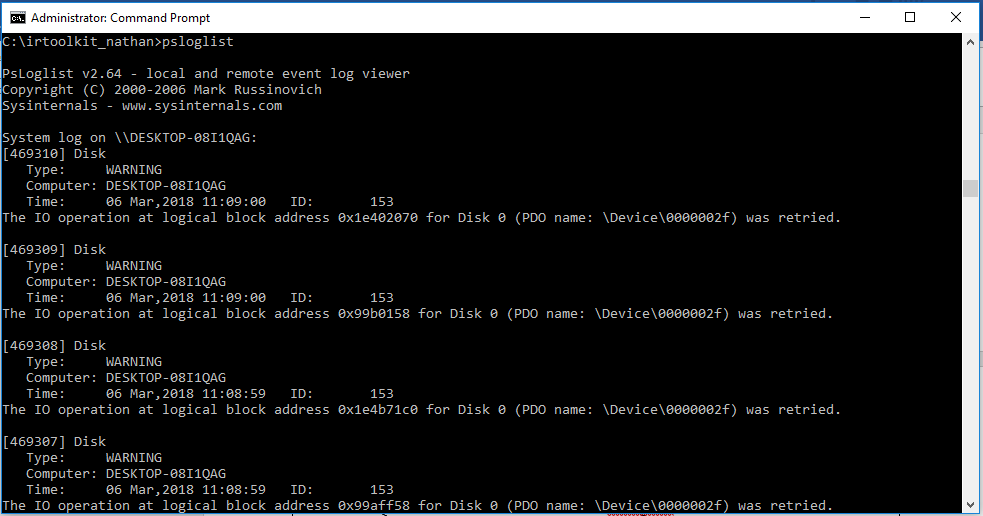
|  |
| --- |
| **Command**: NTlast, NTLast – foundstone |

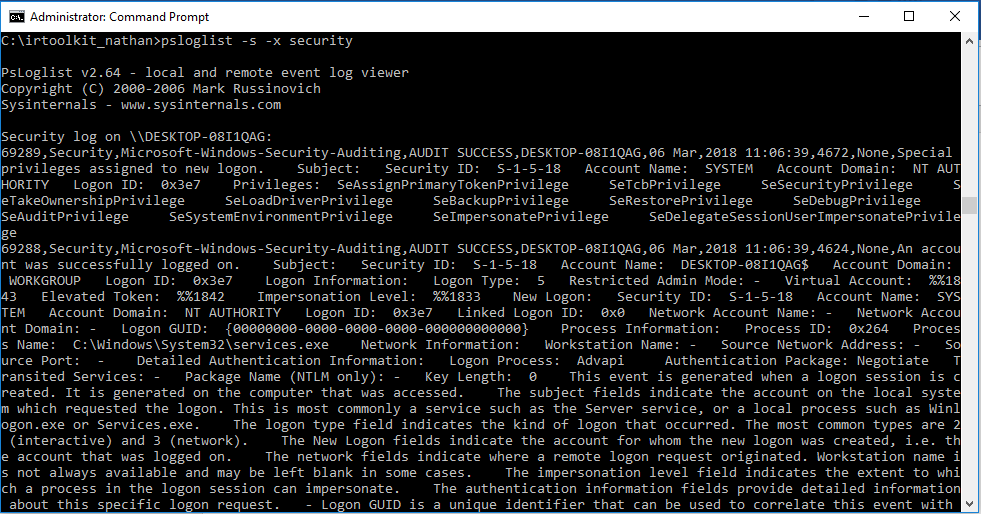
|  |  |
| --- | --- |
| *TASK 6: GET REGISTRY DATA* | |
| TOOLS REQUIRED TO PERFORM TASK 3: regDmp  Task : Get Registry data | |
| ARGUMENTS |  |
| regDmp | capture the complete registry |



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

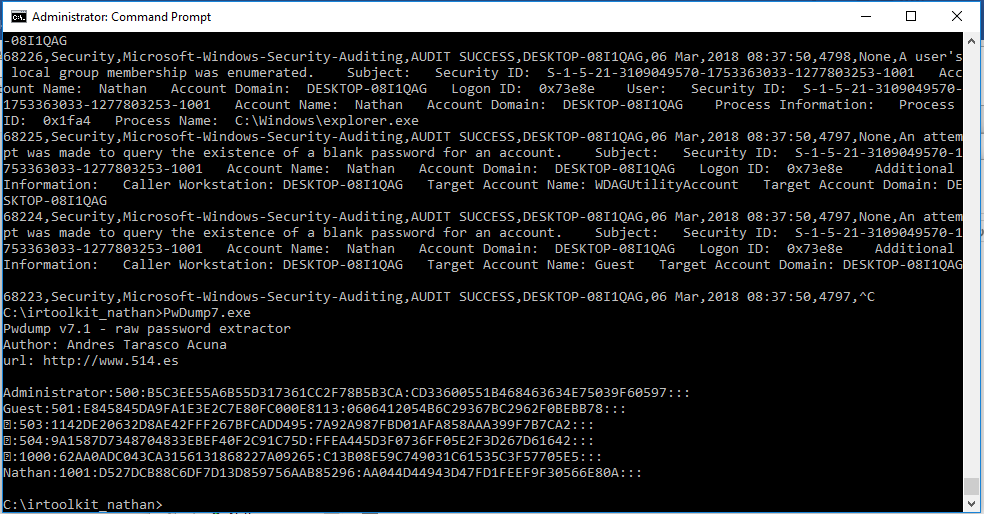
|  |
| --- |
| *TASK 7: System Event log* |
| TOOLS REQUIRED TO PERFORM TASK 3: PsLogList  Task : System Event log |





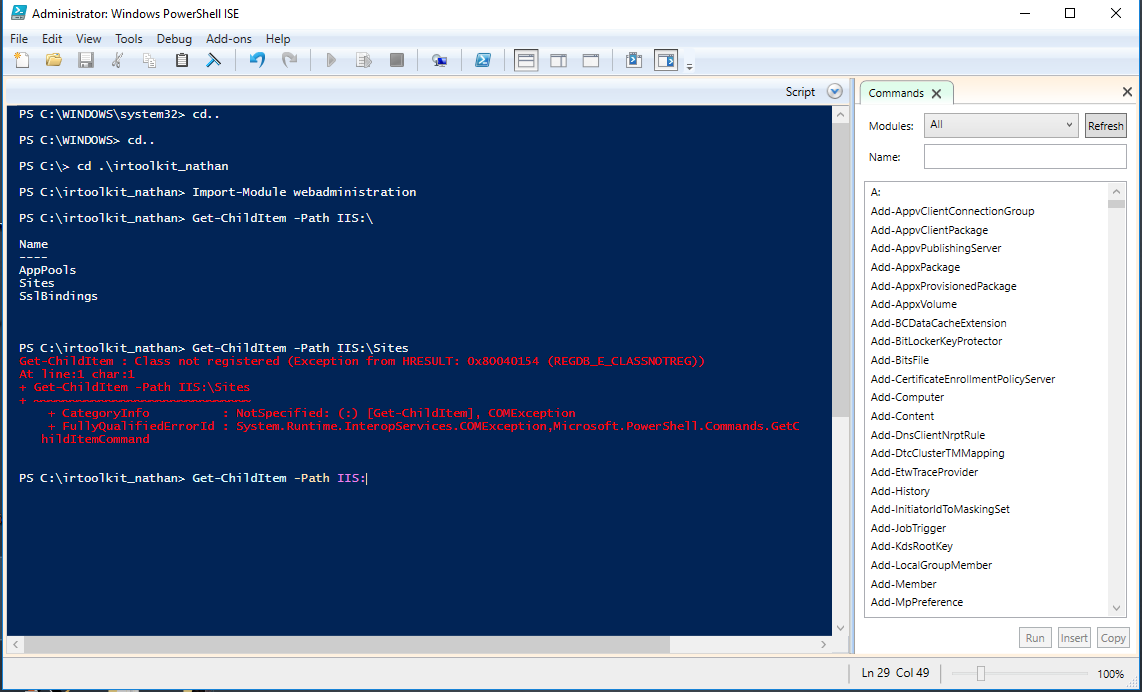
|  |
| --- |
| **Command:** psloglist  psloglist –s –x security |

|  |
| --- |
| *TASK 8: User Accounts* |
| TOOLS REQUIRED TO PERFORM TASK 3: pwdump  Task : user accounts |



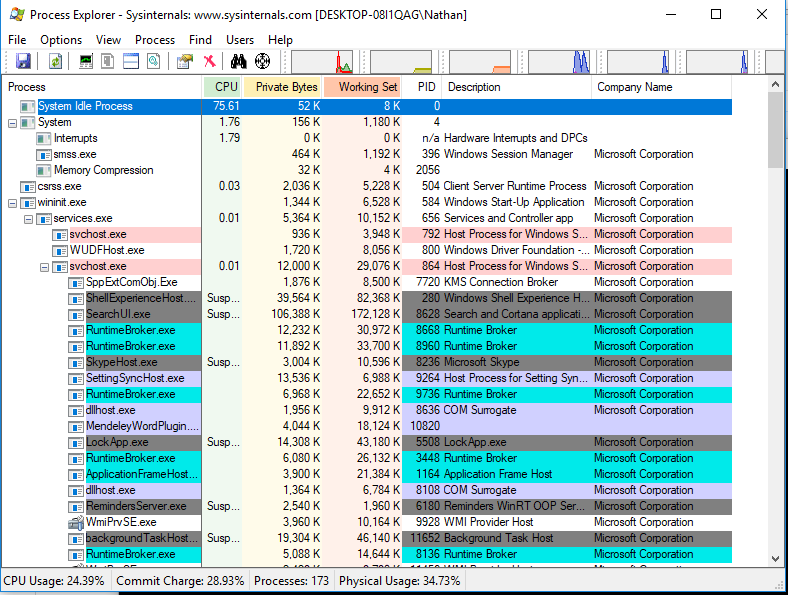
|  |
| --- |
| **Command:** PwsDump.exe |

|  |
| --- |
| *TASK 9: IIS* |
| TOOLS REQUIRED TO PERFORM TASK 3: powershell |



|  |
| --- |
| **Command:** PwsDump.exe |

|  |
| --- |
| *TASK 10: Suspicious file* |
| TOOLS REQUIRED TO PERFORM TASK : Procexp |



|  |
| --- |
| **Command:** procexp.exe |