

HARARE INSTITUTE OF TECHNOLOGY

INFORMATION SECURITY AND ASSURANCE

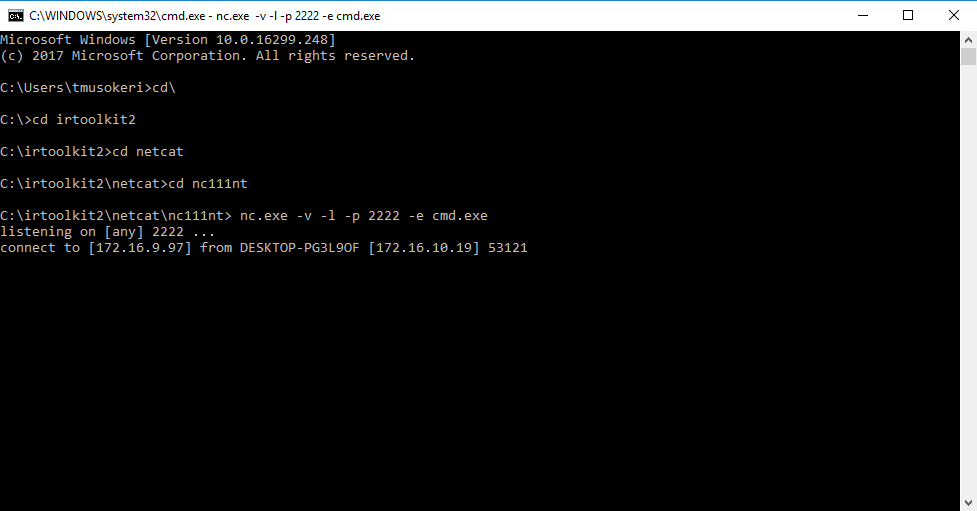
MUSOKERI TSITSI H140349Y

COMPUTER FORENSICS

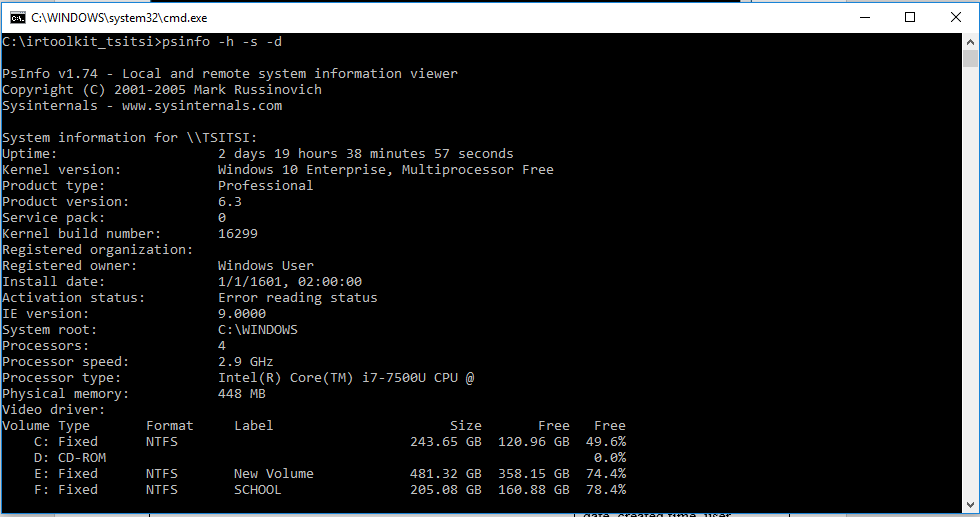
LAB TWO: ANALYZING NONVOLATILE DATA

Lecturer: MR MARENGEREKE

|  |  |
| --- | --- |
| TASK 1: Starting server netcat | |
| TOOLS REQUIRED TO PERFORM TASK : nc.exe | |
| ARGUMENTS & FILTERS |  |
| Nc.exe | Used show net cart |
| -v | is used to show installed hotfixes |
| -l | is used to show installed software |
| -p | is used to show disk volume information |

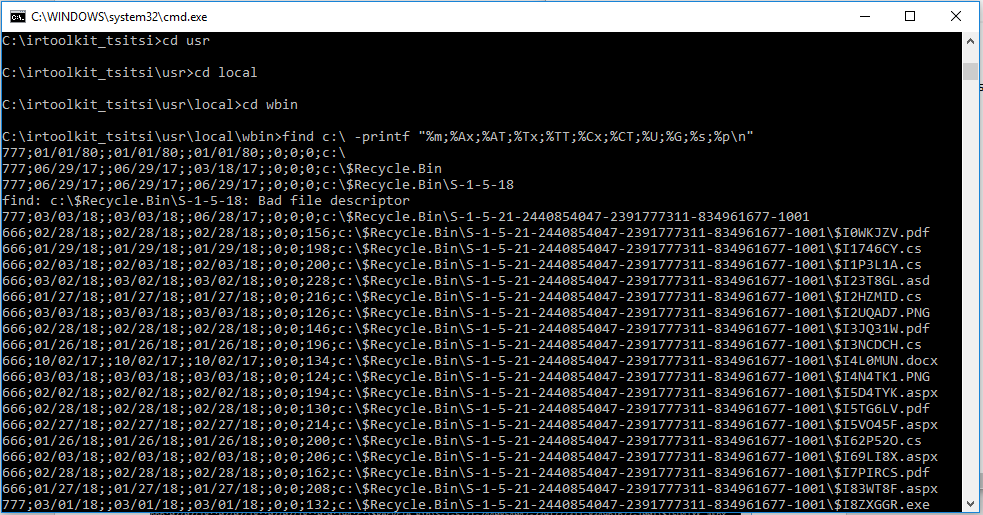


|  |  |
| --- | --- |
| TASK 2: GET SYSTEM VERSION AND PATCH LEVEL | |
| TOOLS REQUIRED TO PERFORM TASK : psinfo | |
| ARGUMENTS & FILTERS |  |
| psinfo |  |
| -h | is used to show installed hotfixes |
| -s | is used to show installed software |
| -d | is used to show disk volume information |



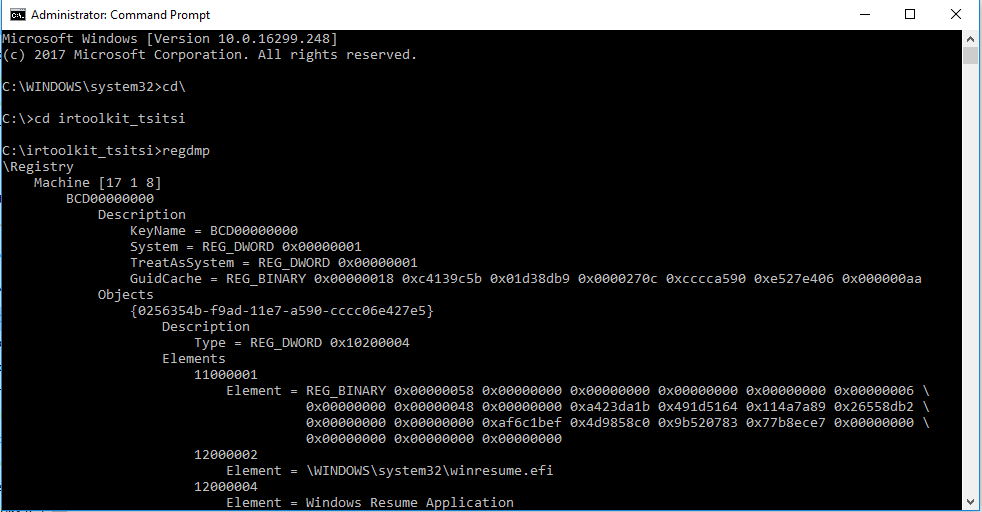
|  |
| --- |
| COMMAND: psinfo –h –s -d |

|  |  |
| --- | --- |
| TASK 3: File System Time and Date Stamps | |
| TOOLS REQUIRED TO PERFORM TASK : UnxUntils | |
| ARGUMENTS & FILTERS |  |
| find 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 |



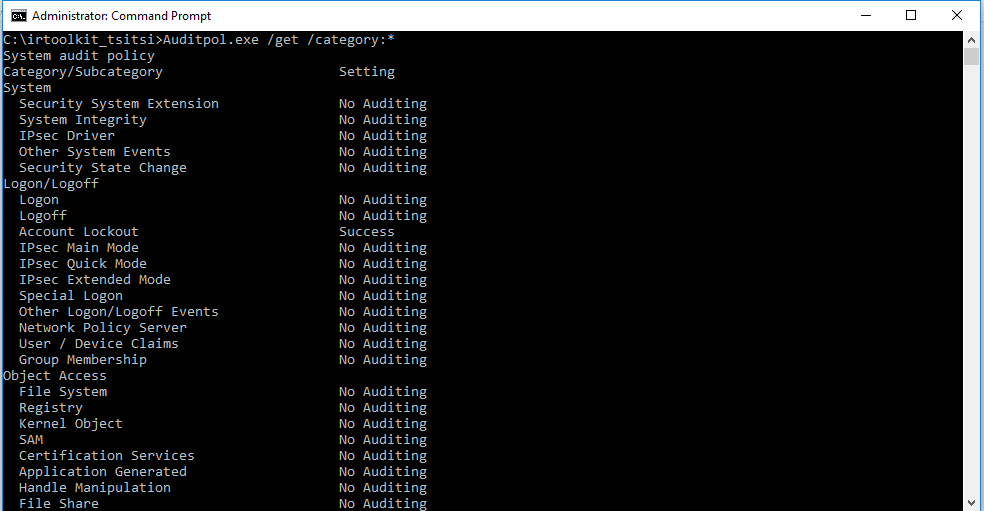
|  |
| --- |
| COMMAND: find c:\ -printf “%m;%Ax;%AT;%Tx;%TT;%Cx;%CT;%U;%G;%s;%p\n” |

|  |  |
| --- | --- |
| TASK 4: RegDump | |
| TOOLS REQUIRED TO PERFORM TASK : RegDump | |
| ARGUMENTS & FILTERS |  |
| Regdump | capture the complete registry |



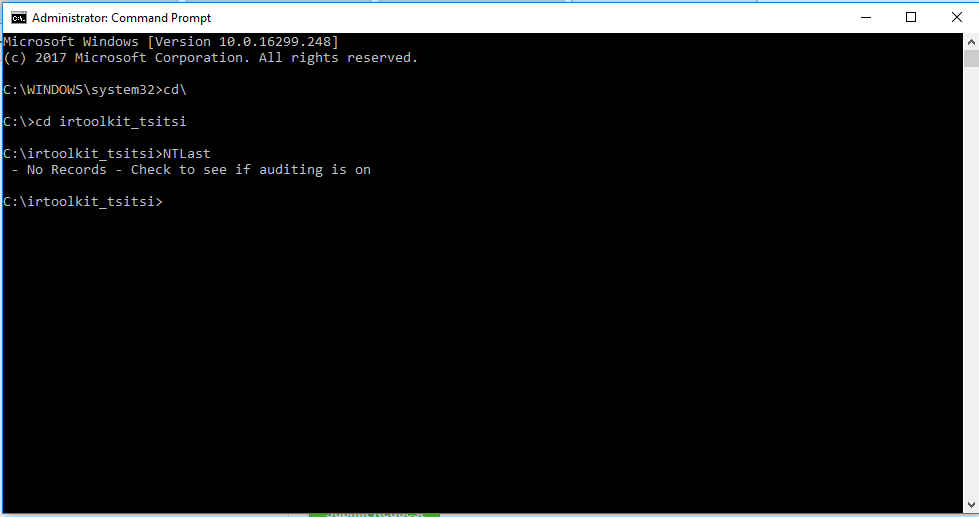
|  |
| --- |
| COMMAND :regdump.exe |

|  |  |
| --- | --- |
| **TASK 5:** 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 |



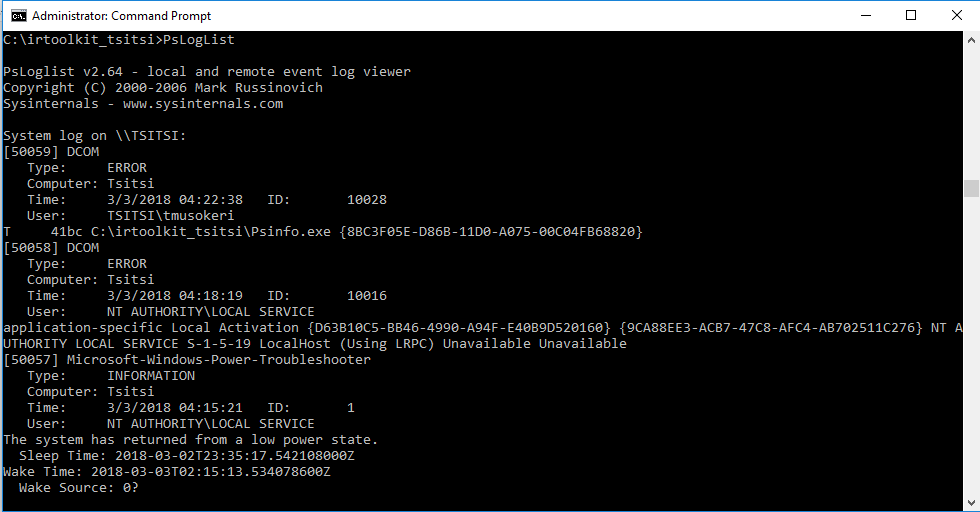
|  |
| --- |
| Command :Auditpol.exe /get /category:\* |

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



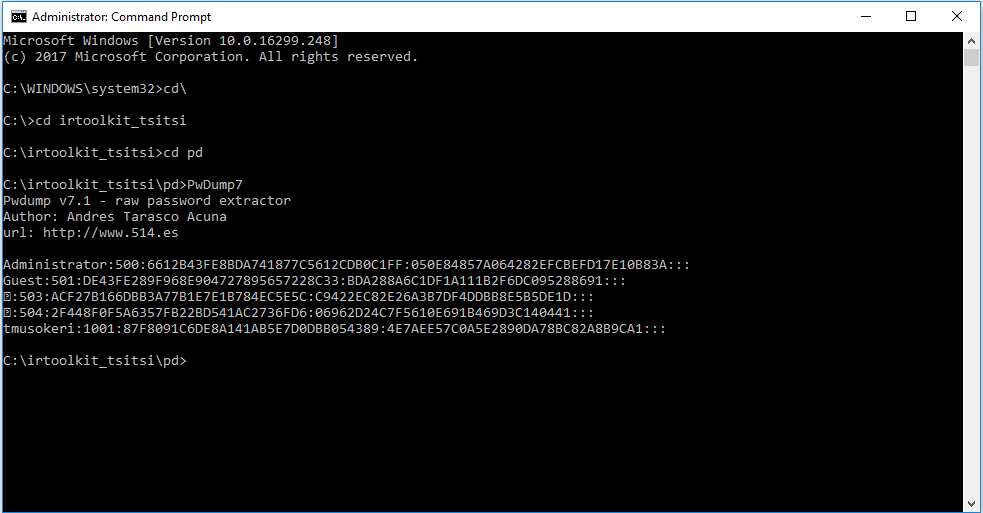
|  |
| --- |
| COMMAND :NTLast |

|  |  |
| --- | --- |
| TASK 7: System Event Logs | |
| TOOLS REQUIRED TO PERFORM TASK : PsLogList | |
| ARGUMENTS & FILTERS |  |
|  |  |

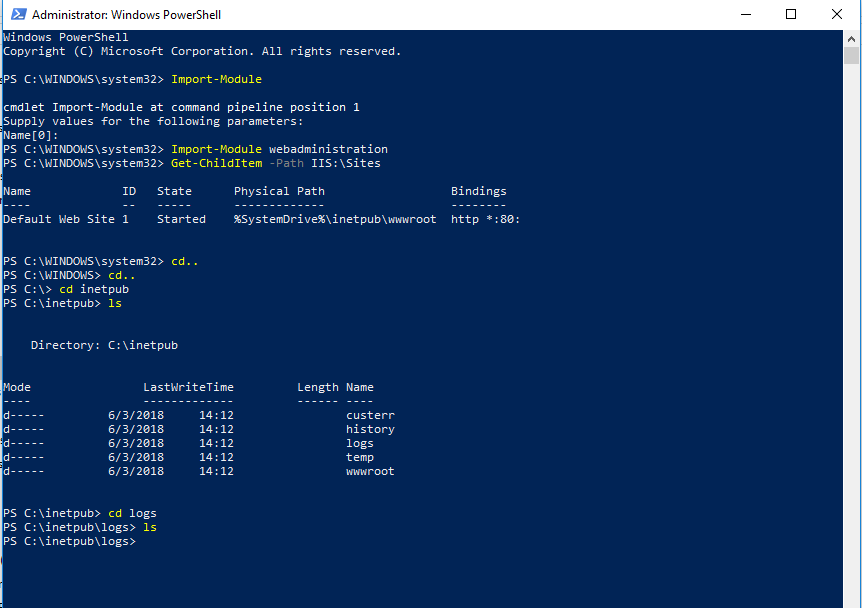


|  |
| --- |
| COMMAND: PSLogList |

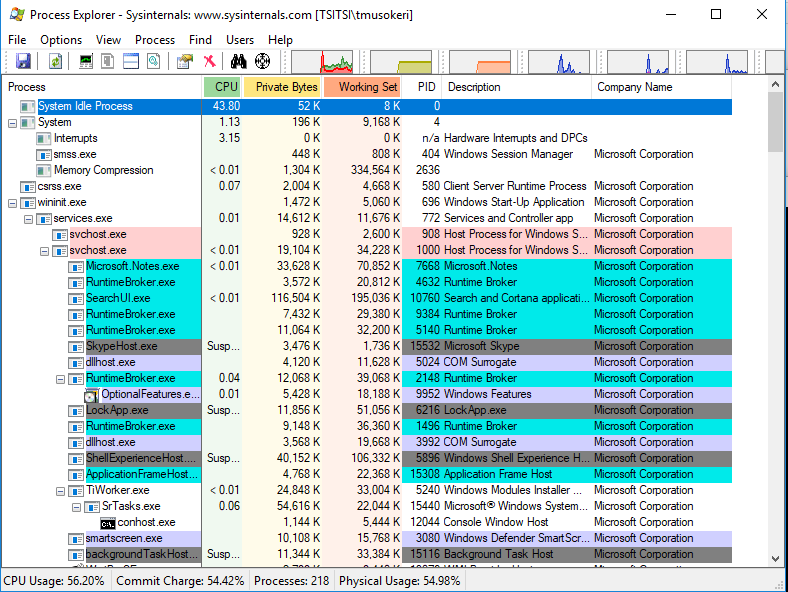
|  |  |
| --- | --- |
| TASK 8: User Accounts | |
| TOOLS REQUIRED TO PERFORM TASK : pwdump | |
| ARGUMENTS & FILTERS |  |
|  |  |



|  |  |
| --- | --- |
| TASK 9: IIS Logs | |
| TOOLS REQUIRED TO PERFORM TASK :powershell | |
| ARGUMENTS & FILTERS |  |
|  |  |



|  |  |
| --- | --- |
| TASK 10:Suspicious Files | |
| TOOLS REQUIRED TO PERFORM TASK : procexp.exe | |
| ARGUMENTS & FILTERS |  |
|  |  |



|  |
| --- |
| COMMAND:procexp.exe |