

HARARE INSTITUTE OF TECHNOLOGY

INFORMATION SECURITY AND ASSURANCE PART 4

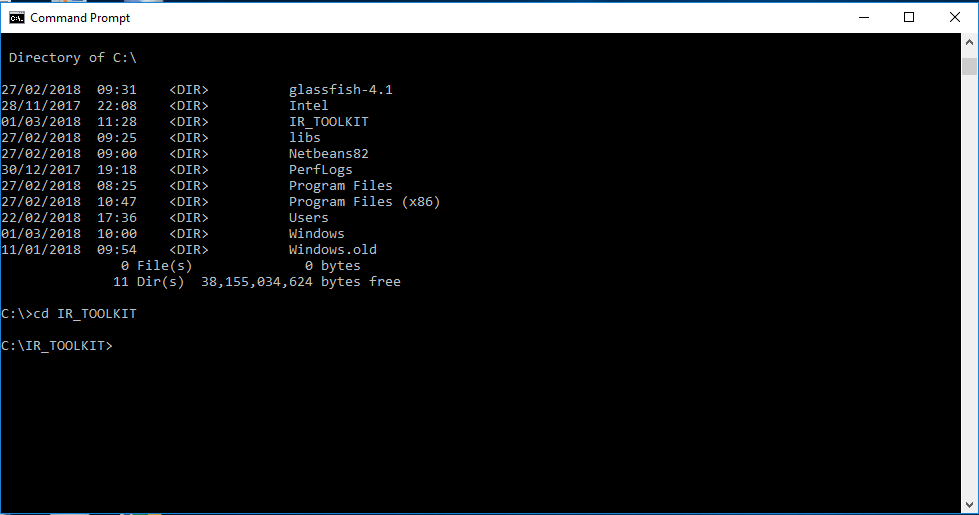
MUKORA RANGARIRAI H140173V

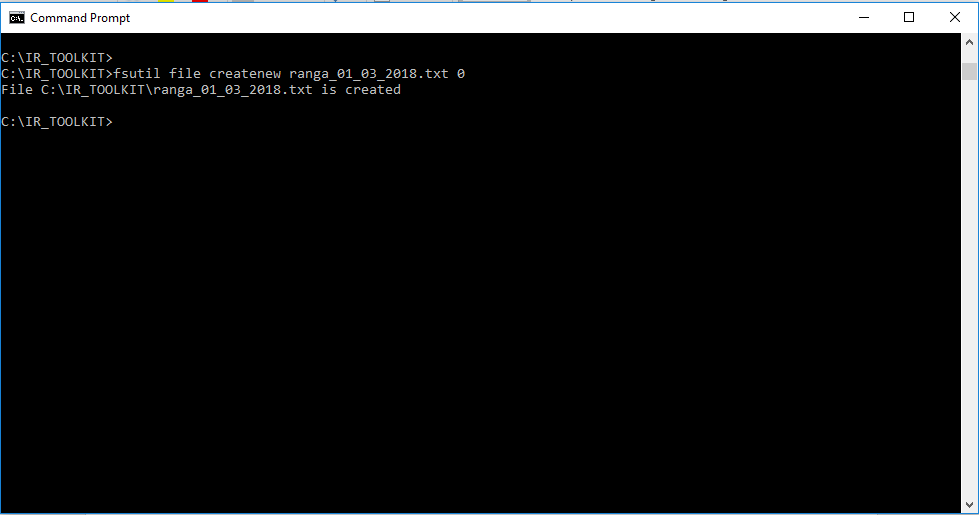
COMPUTER FORENSICS **LAB TWO**

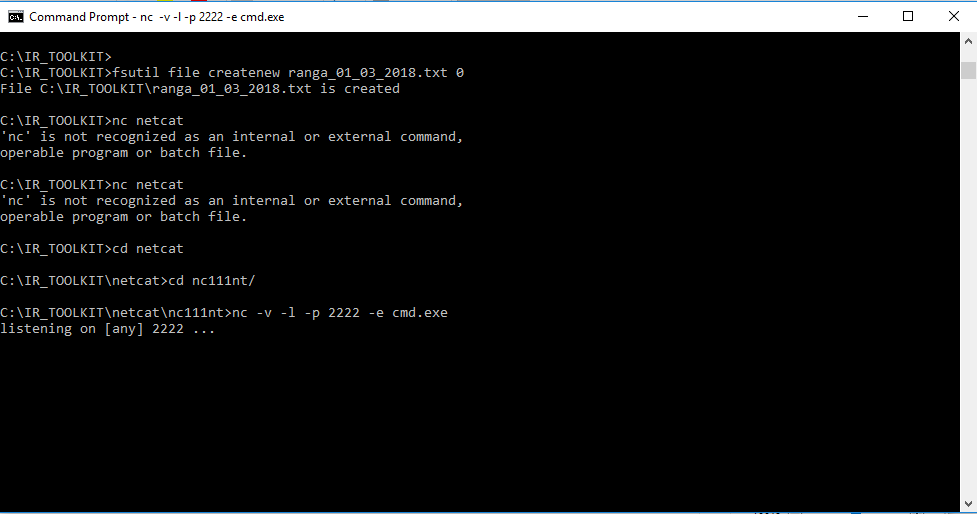
TUTOR: MR MARENGEREKE

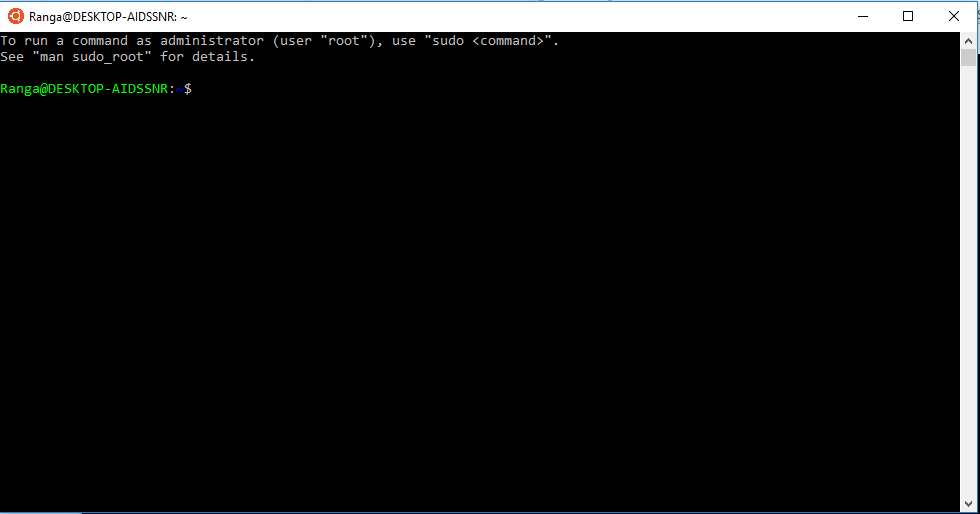
ANALYZING NONVOLATILE DATA

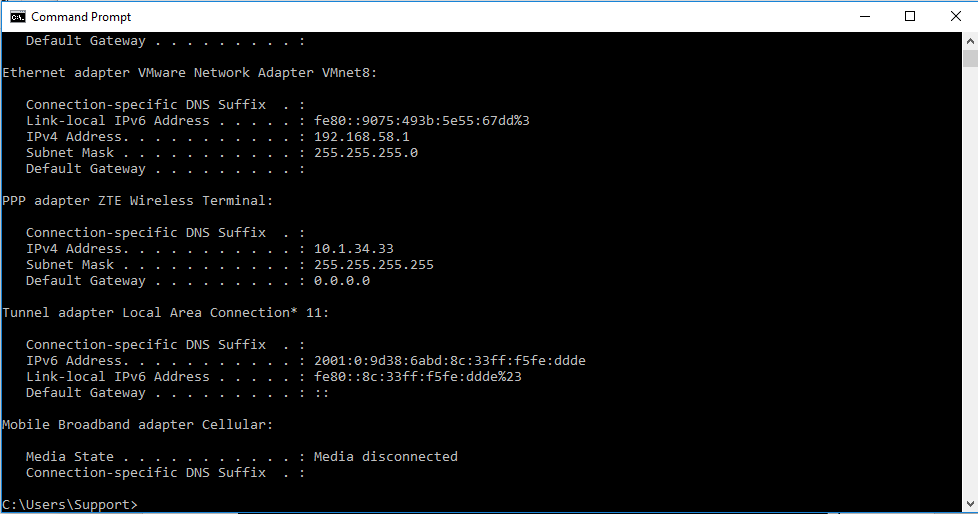
netcat



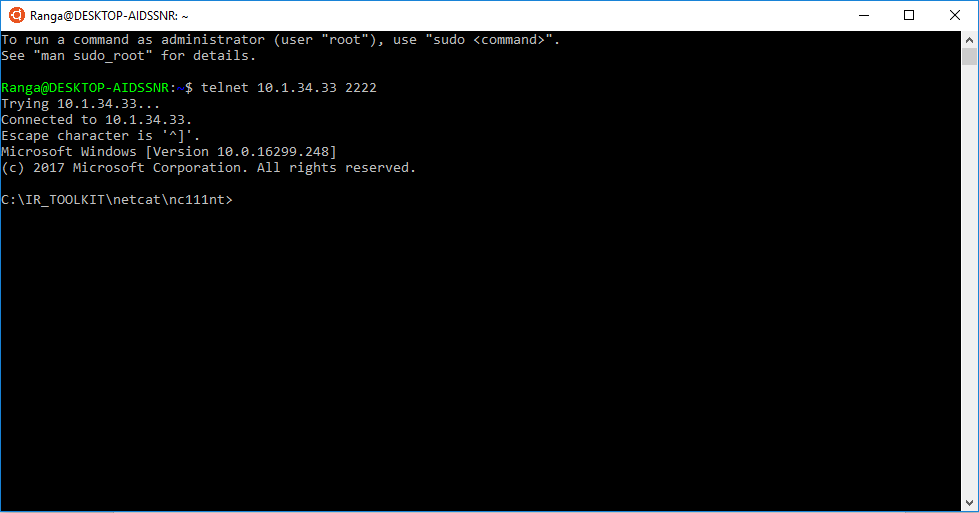




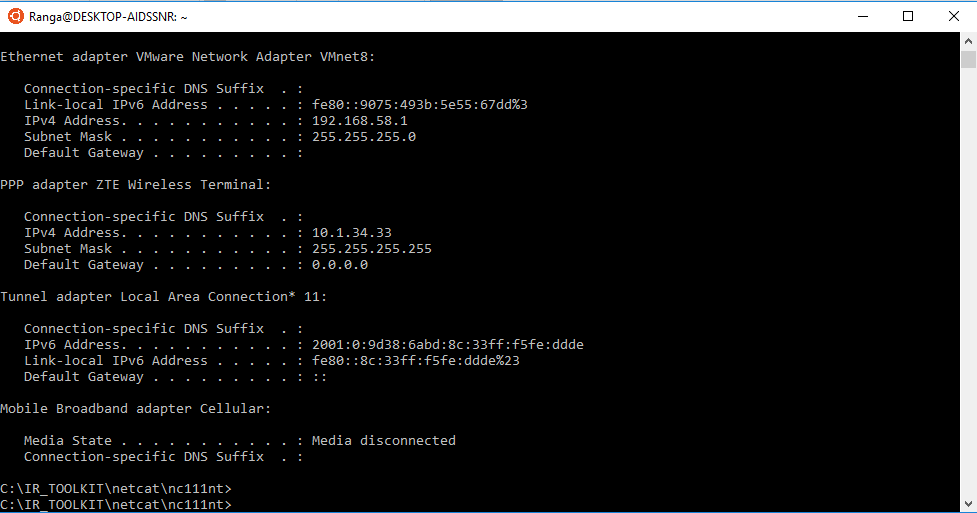




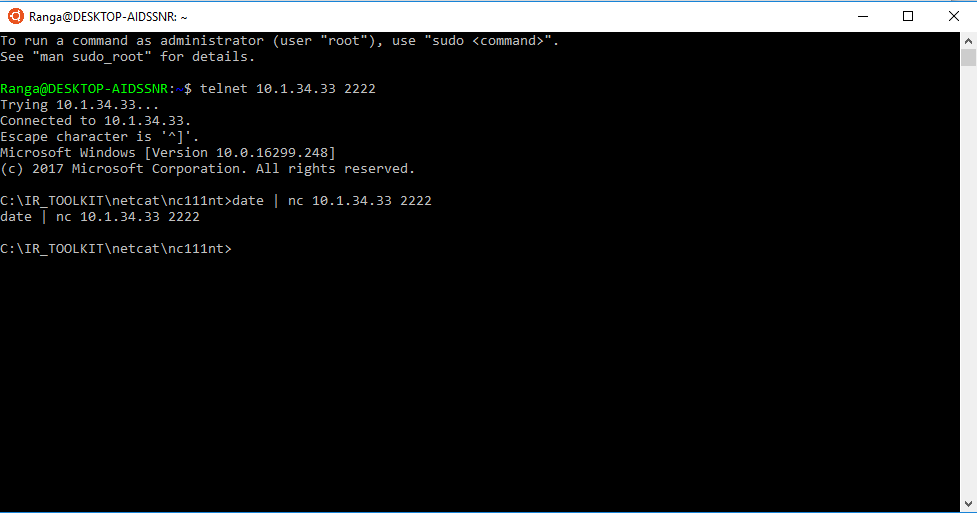
Telnetting to victim machine using IP Address and port 2222



**COMMAND:** starting serve netcat : nc –v –l –p 2222 > tendai\_29\_02\_2016.txt

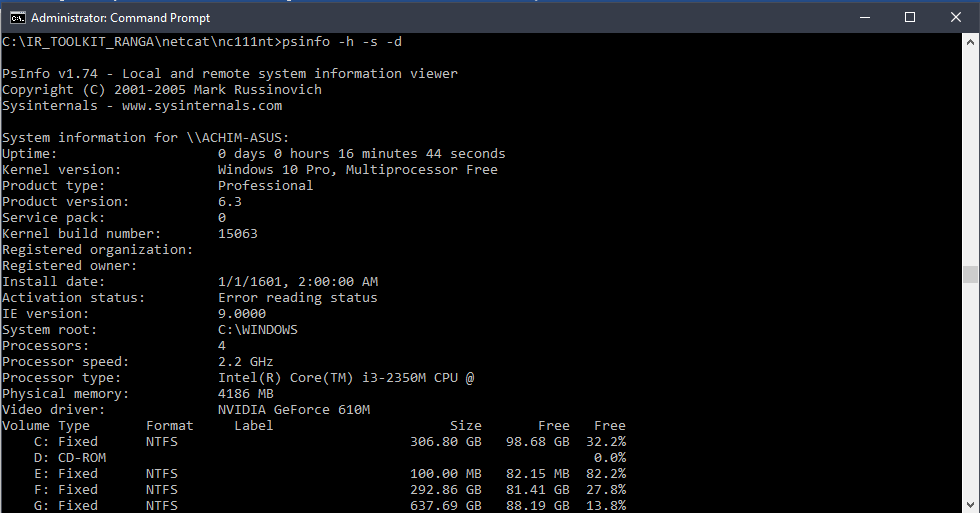


Sending date and time to forensic machine



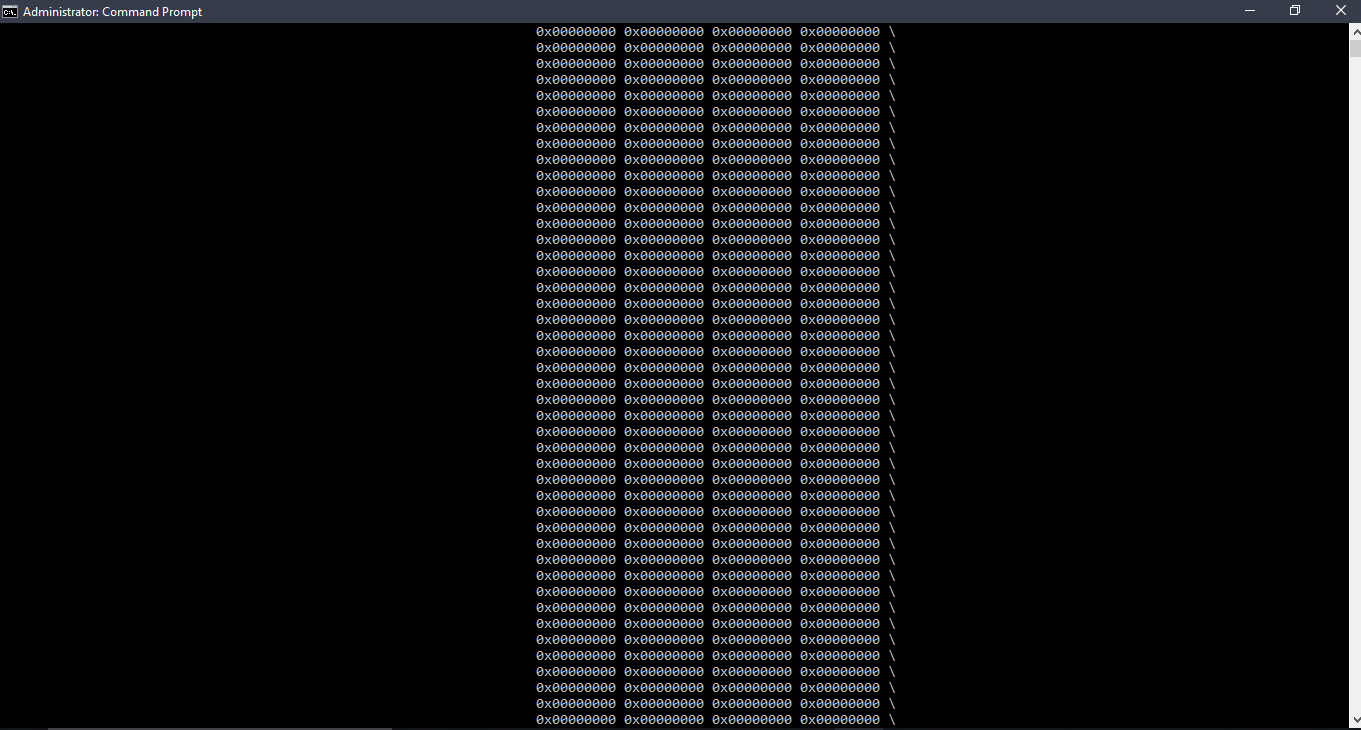
**COMMAND:** victim machine: command(date) | nc forensic\_workstation\_ip\_address 2222

System Version and Patch Level



psinfo -h -s -d

Registry Data

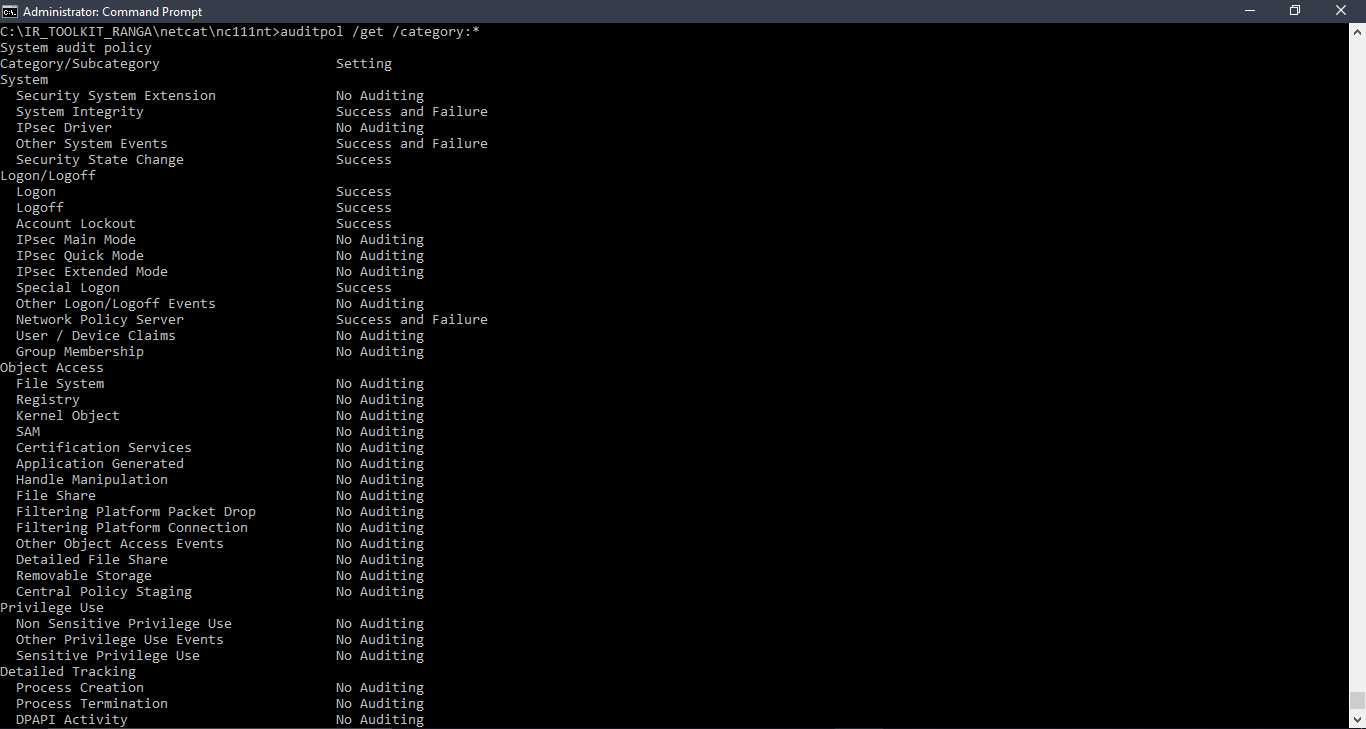


regDmp

The Auditing Policy

|  |  |
| --- | --- |
| 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 |

**SCREENSHOT:**

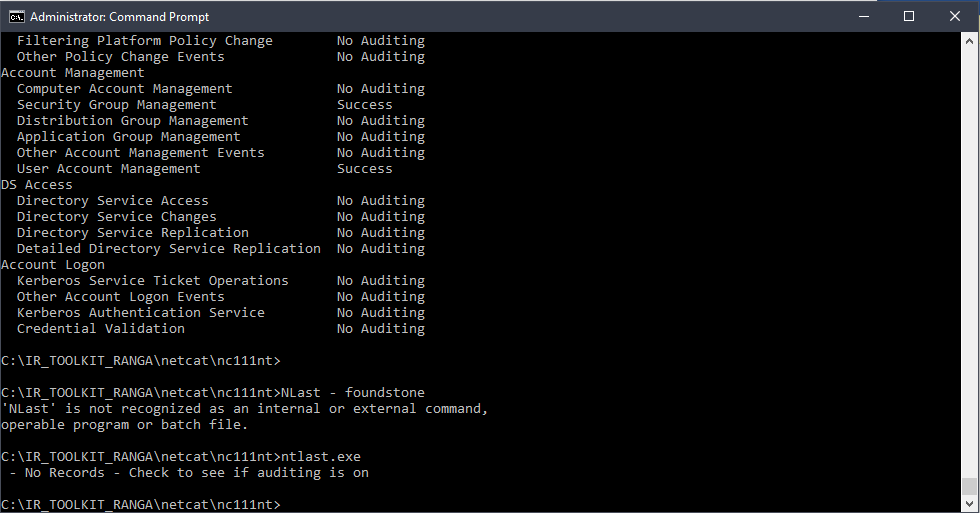


|  |
| --- |
| COMMAND: auditpol /get /category:\*  This command will display the current security policy in categories |

A History of Login

GET SYSTEM LOG IN/ LOGOUT INFORMATION

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



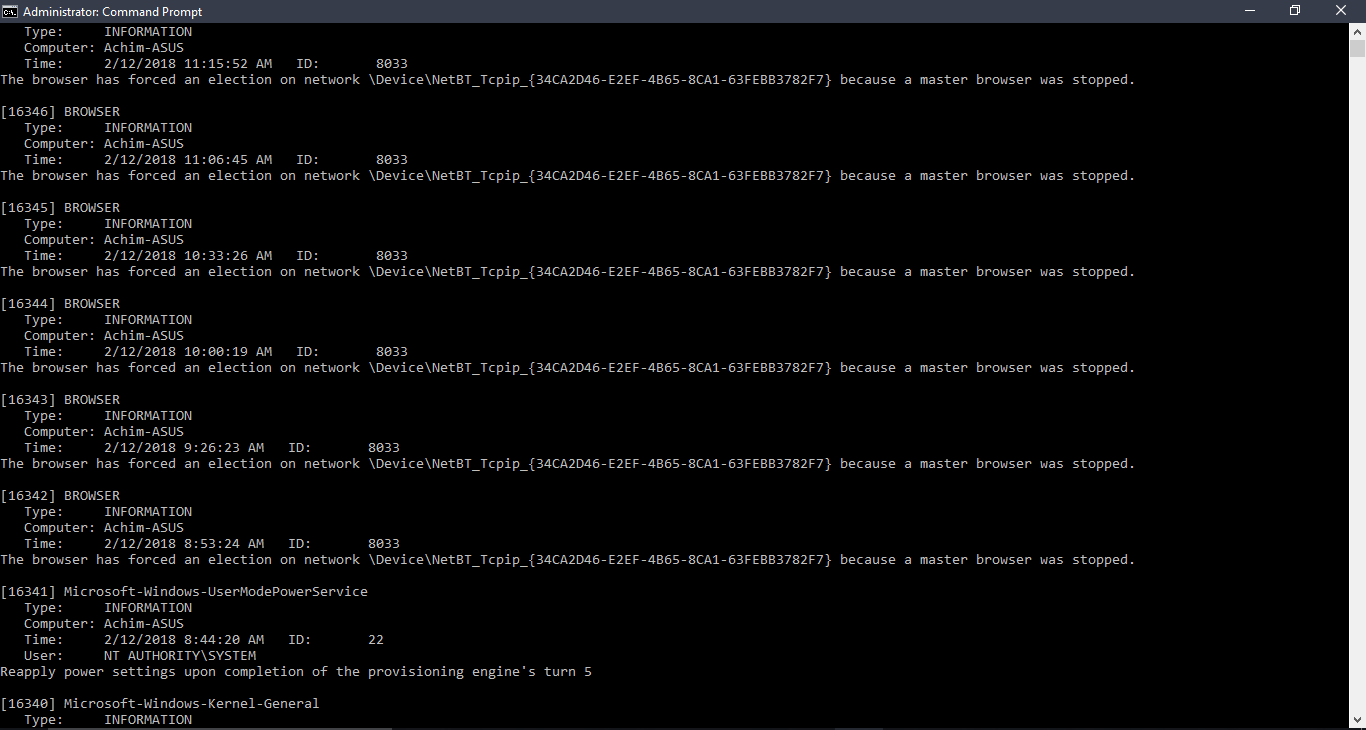
|  |
| --- |
| COMMAND: ntlast.exe |

System Event Logs

GET SYSTEM LOG EVENTS

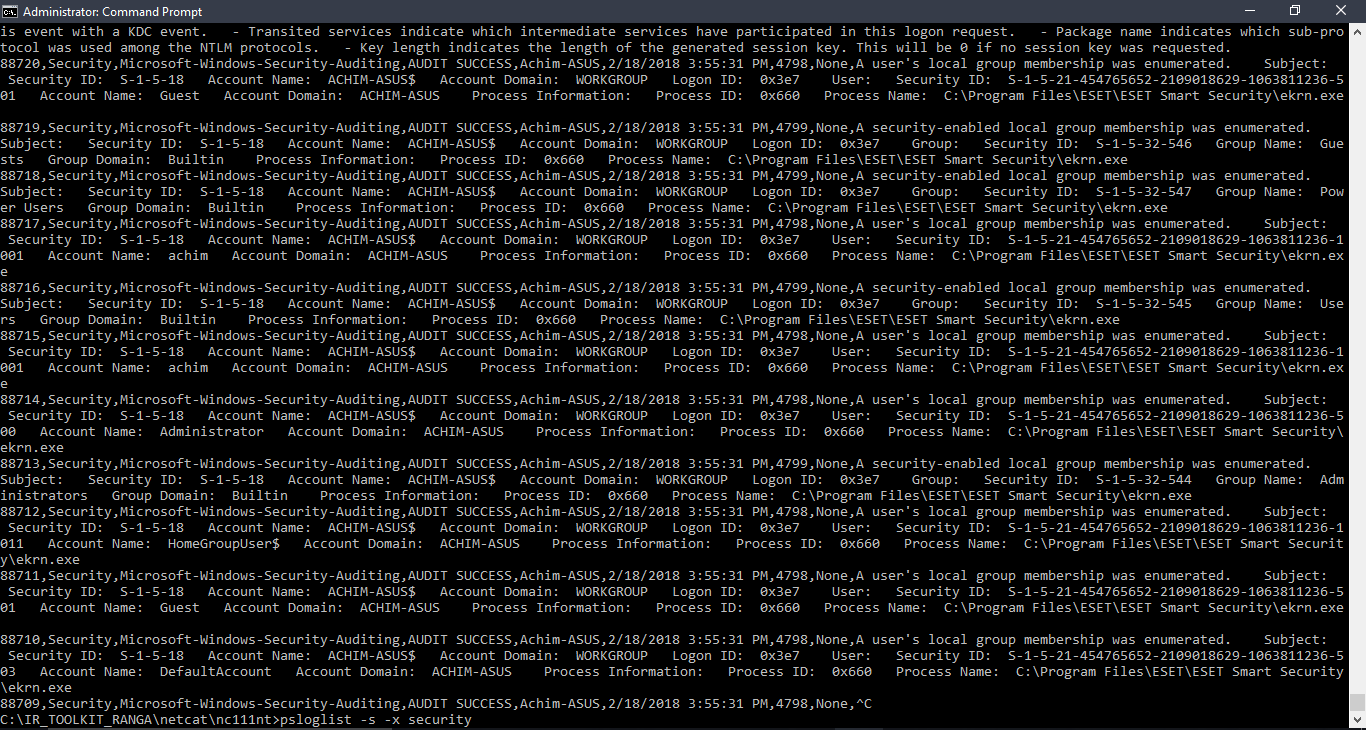
|  |  |
| --- | --- |
| **TOOLS:** WEVTUTIL | |
| Arguments that can be passed for **DATE** | |
| el |enum logs | List log names |
| gl | get-log | Gets log configuration information |
| sl|set-log | Modify configuration of a log |
| qe|query-events | Query from an existing log files |
| Epl | export-log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

**SCREENSHOT:**



|  |
| --- |
| COMMAND 1: PsLogList |

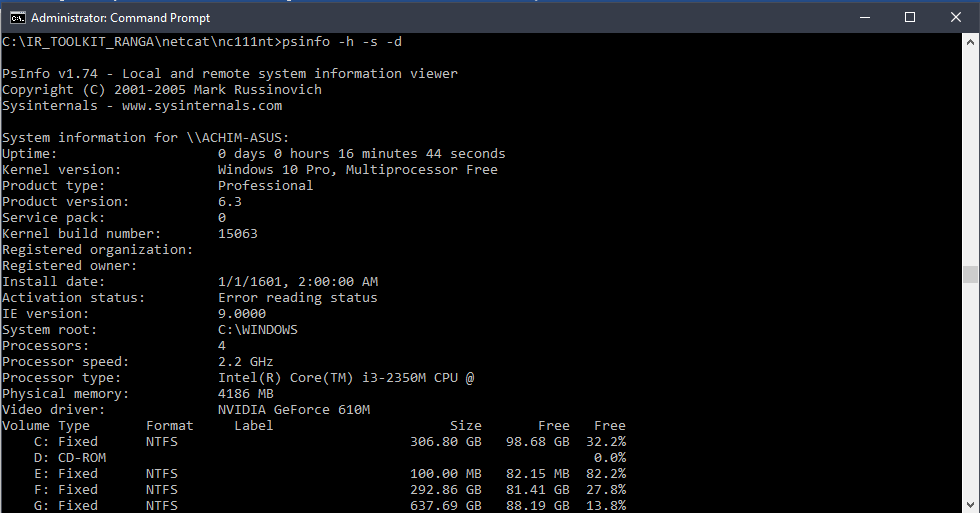
PsLogList



psloglist –s –x security

System Version and Patch Level

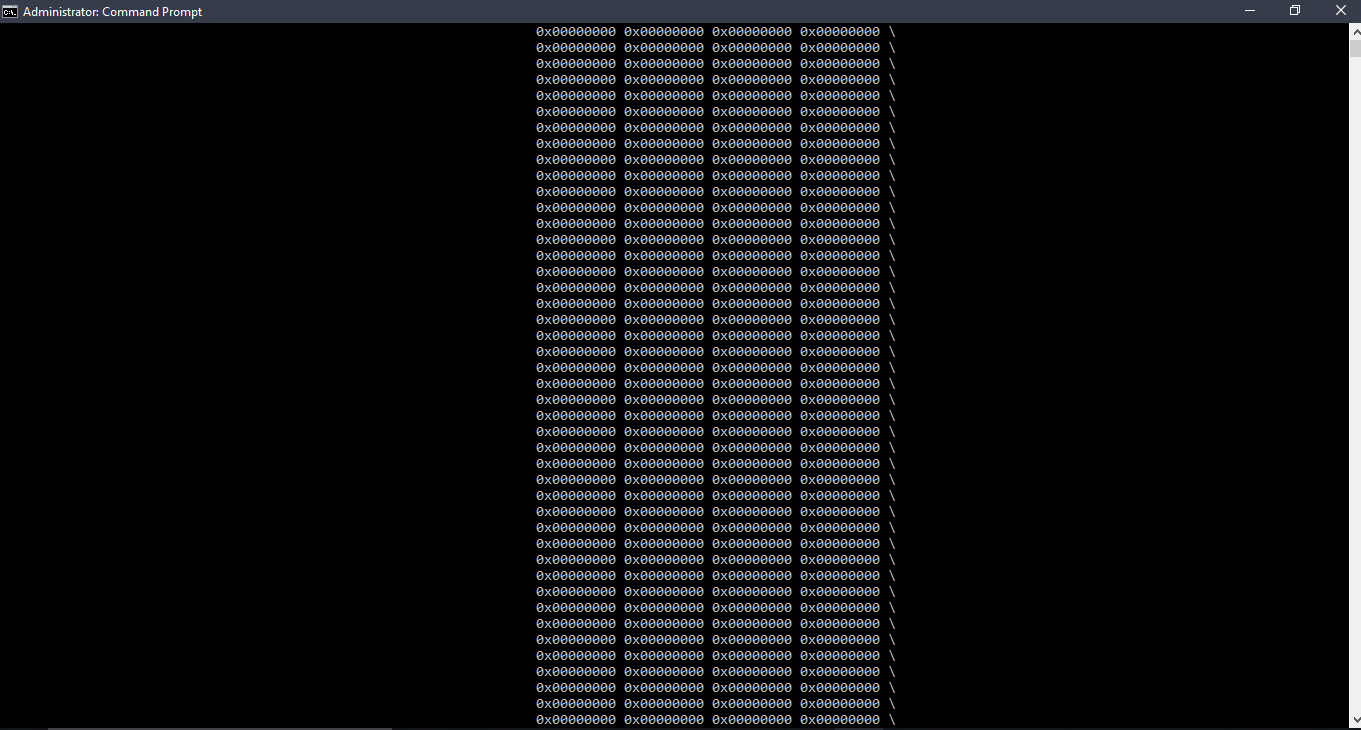
|  |  |
| --- | --- |
| GET SYSTEM VERSION AND PATCH LEVEL | |
| TOOLS REQUIRED TO PERFORM TASK: psinfo | |
| ARGUMENTS & FILTERS |  |
| psinfo |  |
| -h | is used to show installed hotfixes |
| -s | is used to show installed software |
| -d | is used to show disk volume information |



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

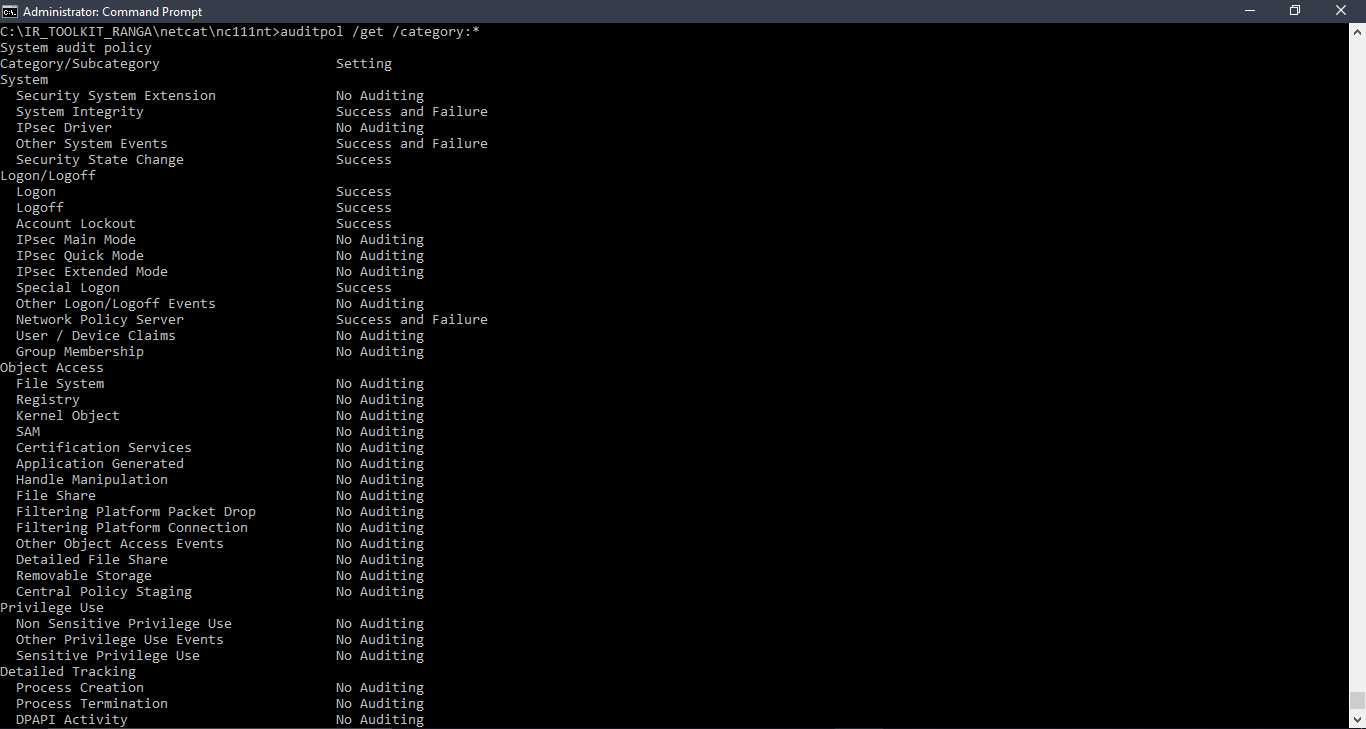
Registry Data

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



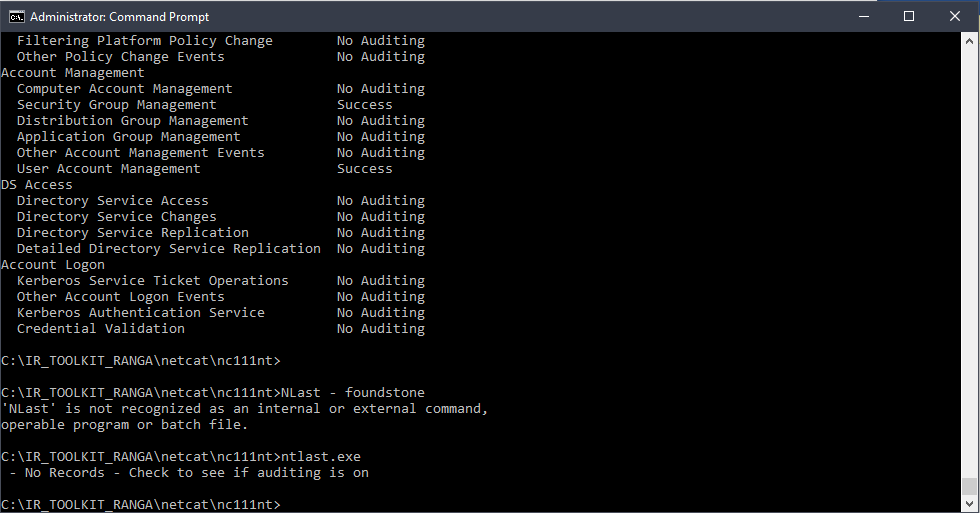
|  |
| --- |
| **Command**: regdmp |

The Auditing Policy



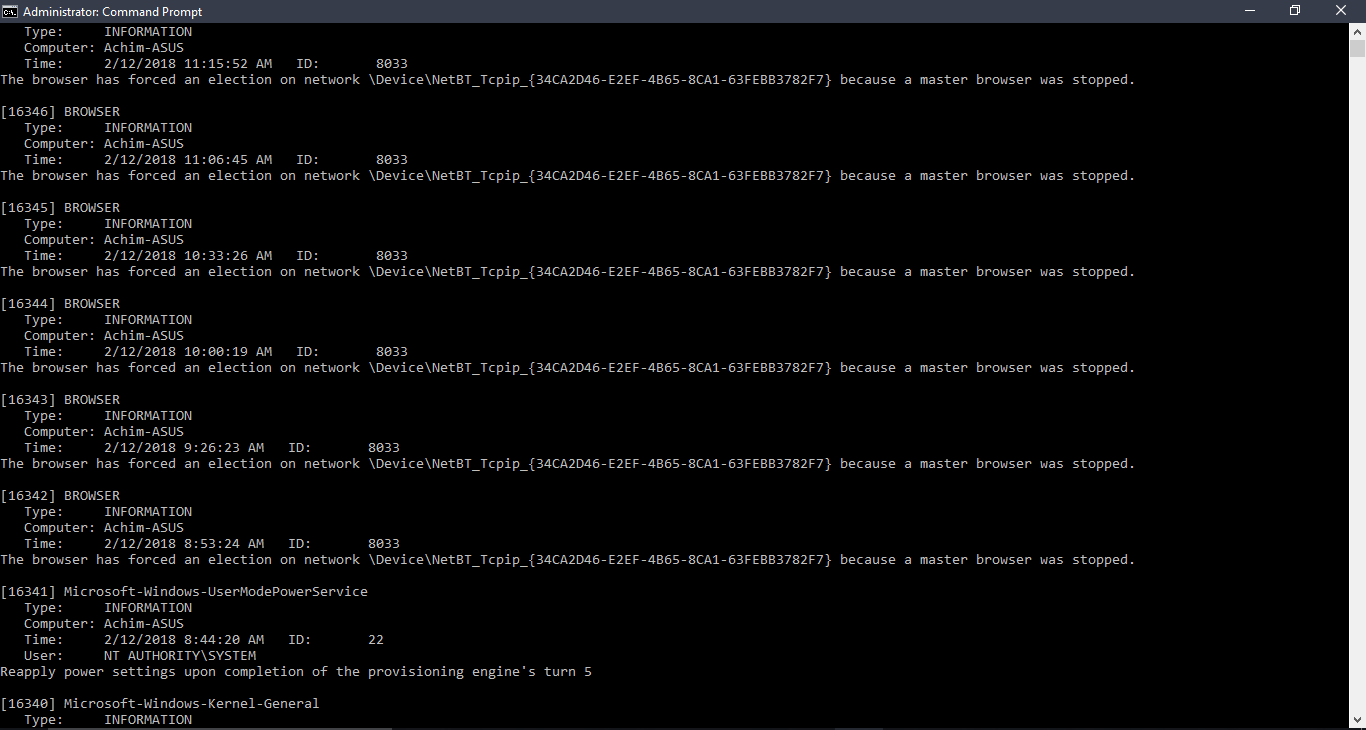
auditpol /get /category:\*

A History of Logins

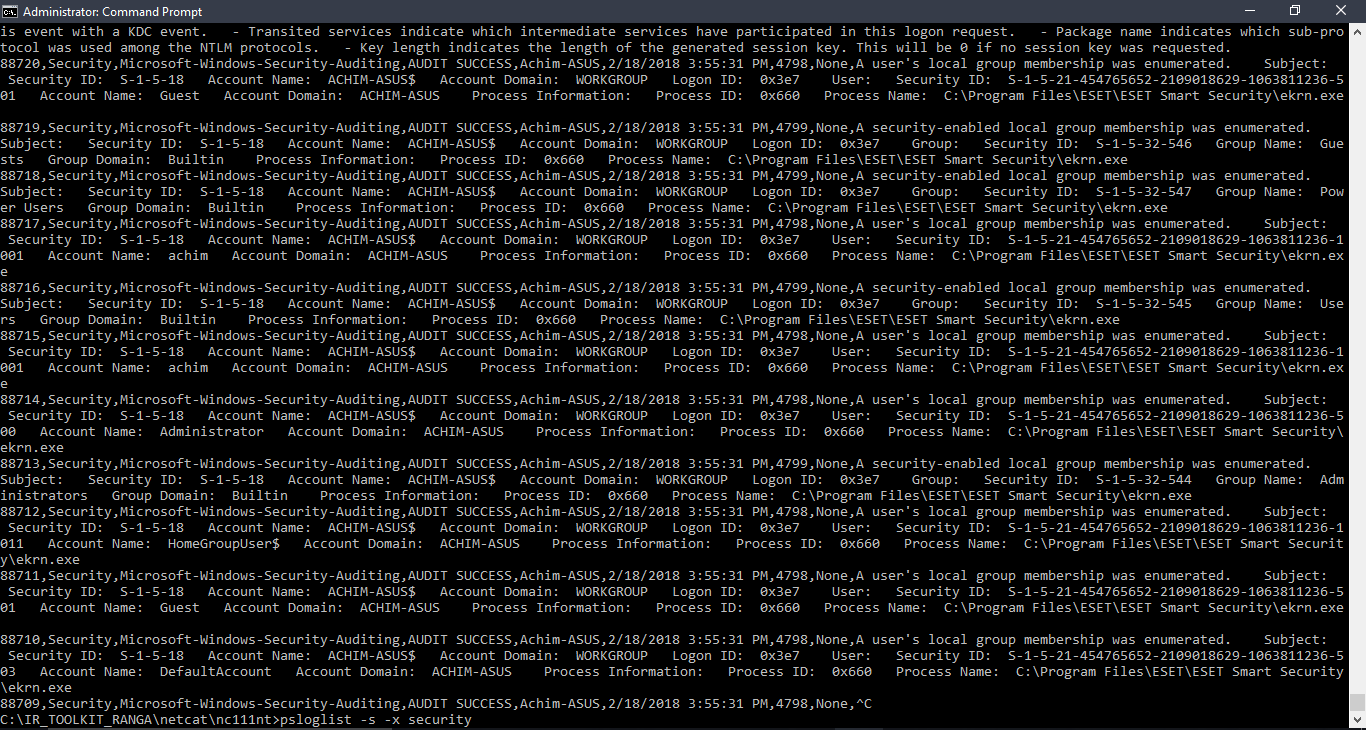


ntlast.exe

System Event Logs



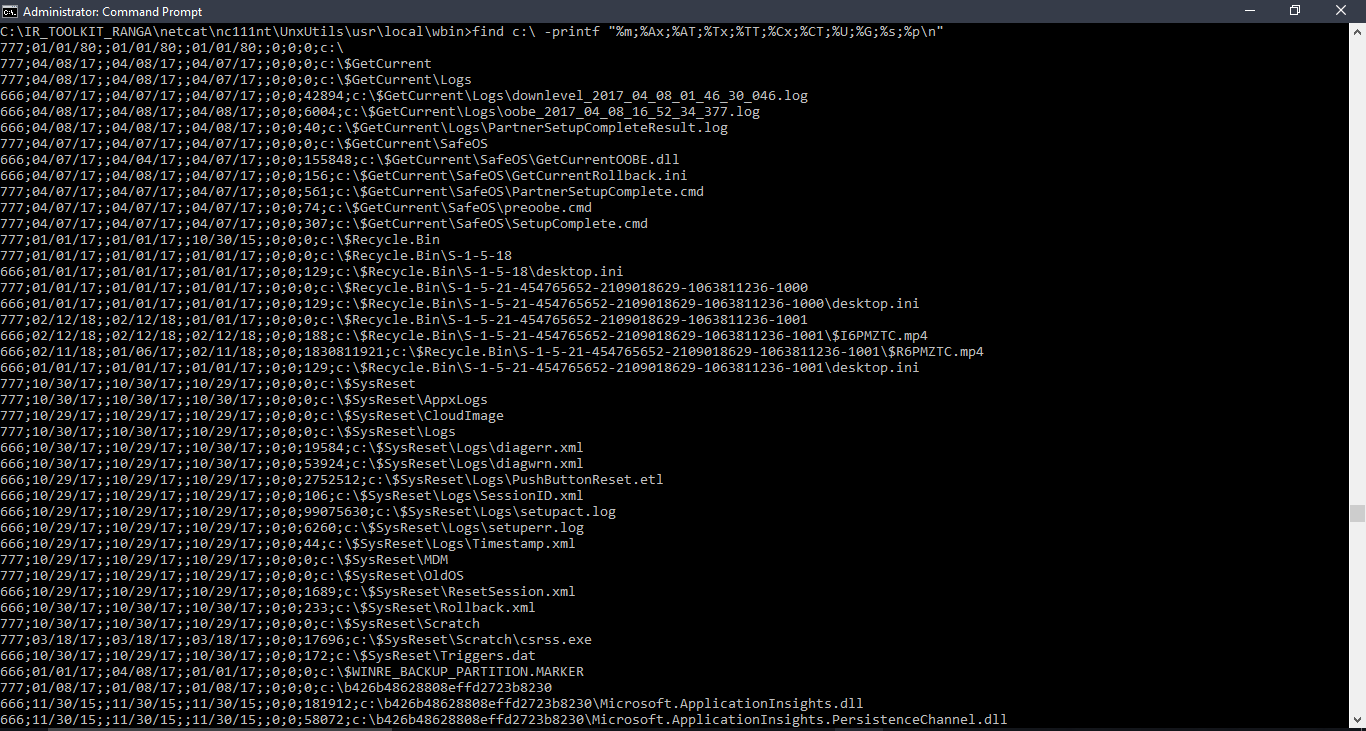
PsLogList



psloglist –s –x security

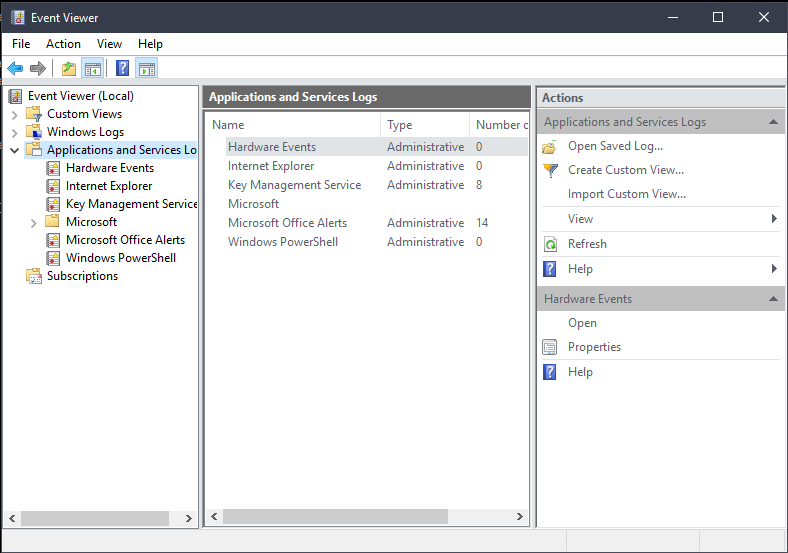
File System Time and Date Stamps

|  |  |
| --- | --- |
| 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 |



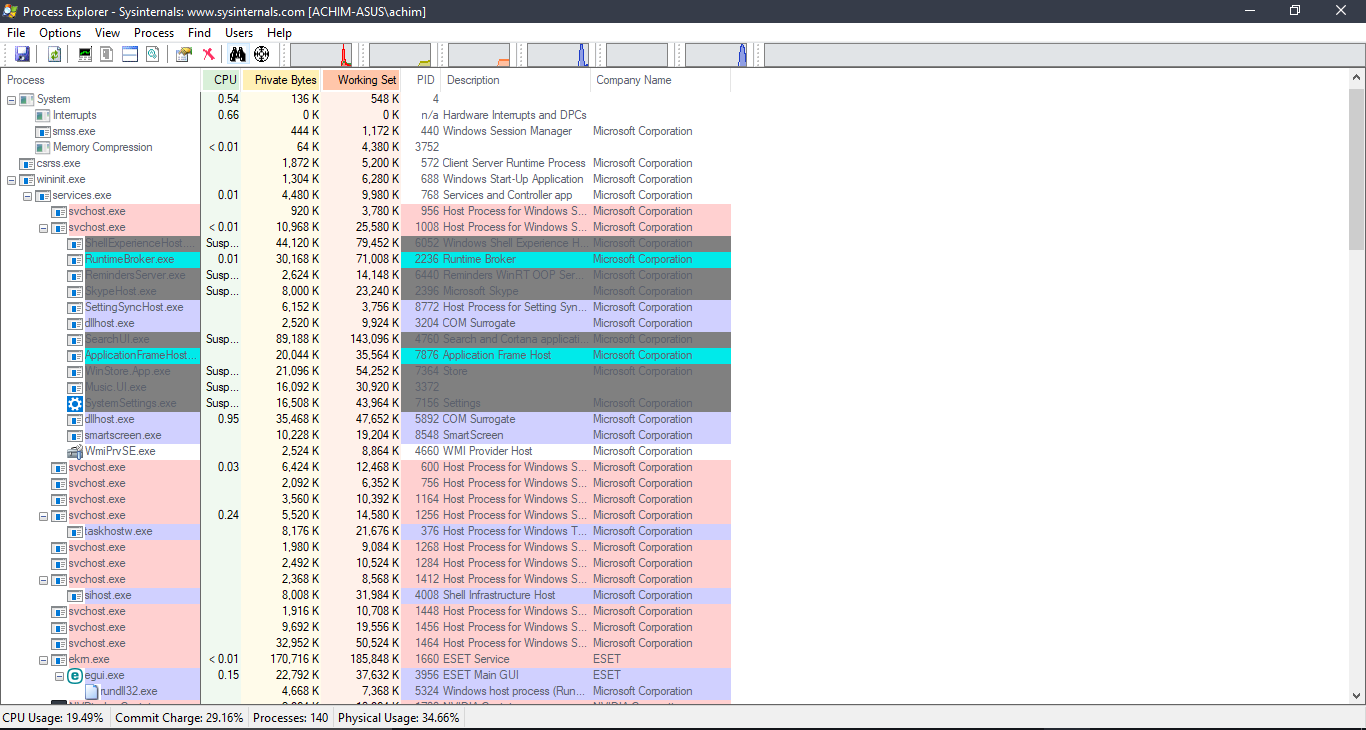
**COMMAND:** find c:\ -printf “%m;%Ax;%AT;%Tx;%TT;%Cx;%CT;%U;%G;%s;%p\n”

IIS Logs



**COMMAND:** start eventvwr

**Suspicious Files**



**COMMAND: P**rocexp.exe

User Accounts