

HARARE INSTITUTE OF TECHNOLOGY

INFORMATION SECURITY AND ASSURANCE PART 4

TAKAVADINI JENIPHER H140180W

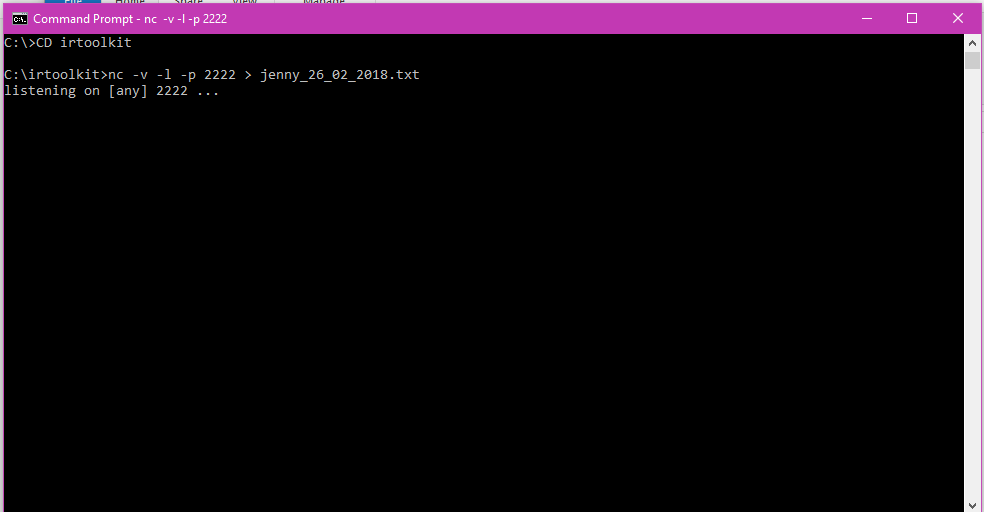
COMPUTER FORENSICS LAB2 NON VOLATILE DATA

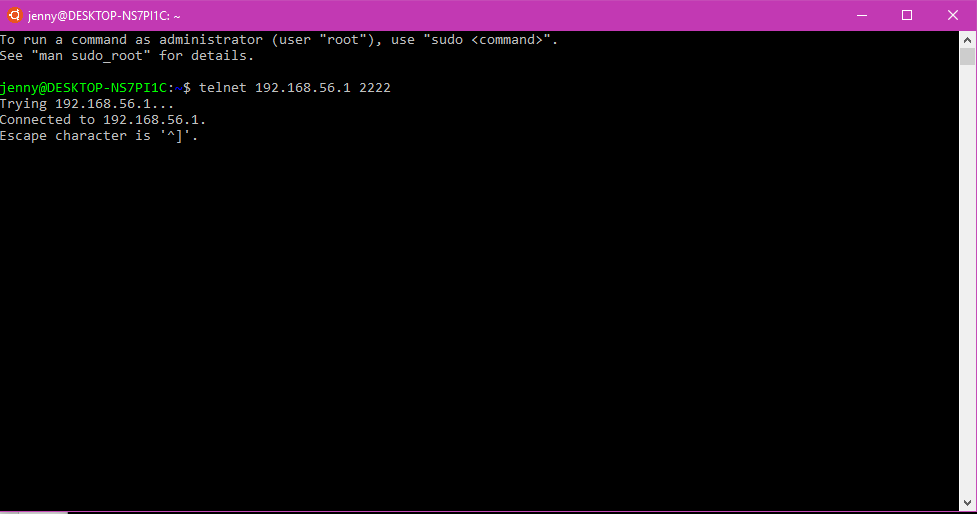
TUTOR: MR MARENGEREKE

netcat

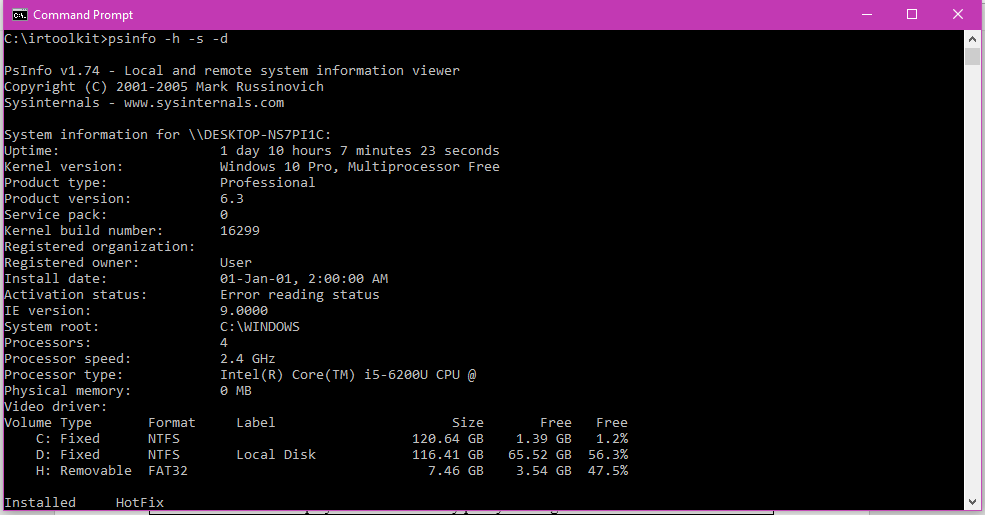
starting serve netcat : nc –v –l –p 2222 > jenny\_26\_02\_2018.txt

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



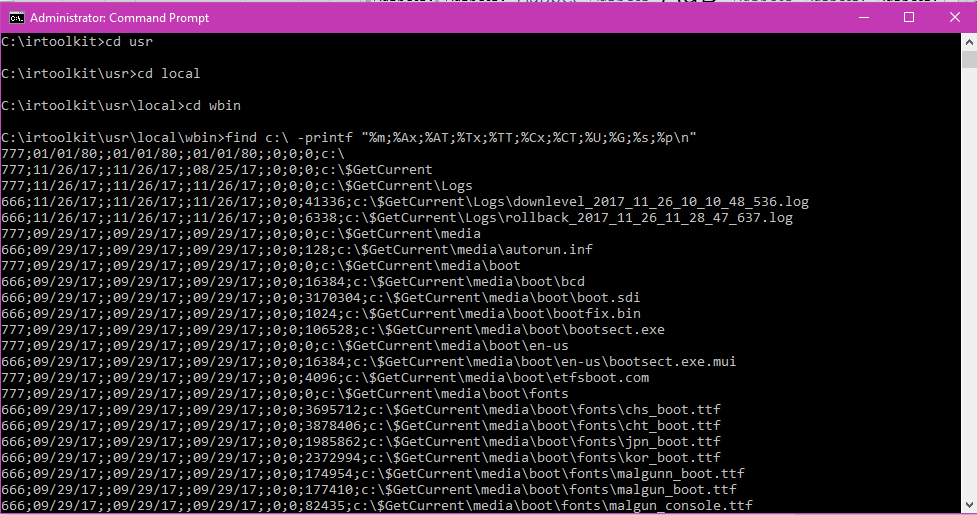


|  |  |
| --- | --- |
| GET SYSTEM VERSION AND PATCH LEVEL | |
| TOOLS REQUIRED TO PERFORM TASK : psinfo | |
| ARGUMENTS & FILTERS |  |
| psinfo |  |
| -h | is used to show installed hotfixes |
| -s | is used to show installed software |
| -d | is used to show disk volume information |



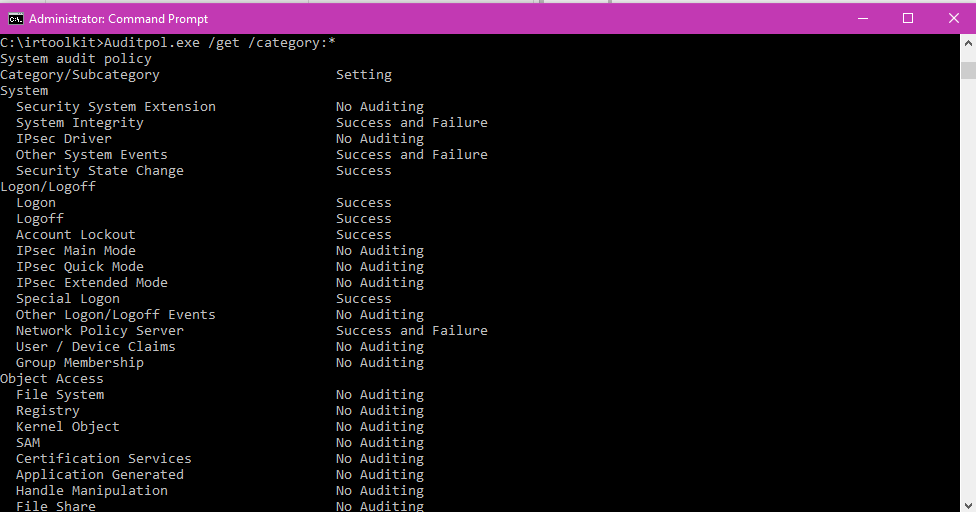
|  |
| --- |
| Command: psinfo -h -s -d |

|  |  |
| --- | --- |
| 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” |

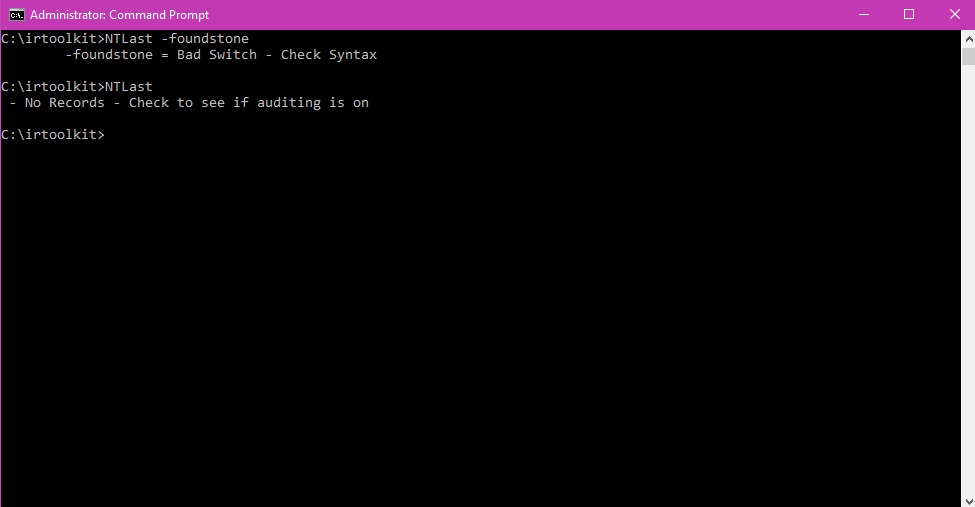
|  |  |
| --- | --- |
| GET THE AUDIT POLICY | |
| **TOOLS :** AUDITPOL | |
| **Arguments that can be passed for AUDITPOL** | |
| /? | Help |
| /get | Displays current audit policy |
| /set | Sets the audit policy |
| /list | Displays selective policy elements |
| /backup | Backups the current security 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 |

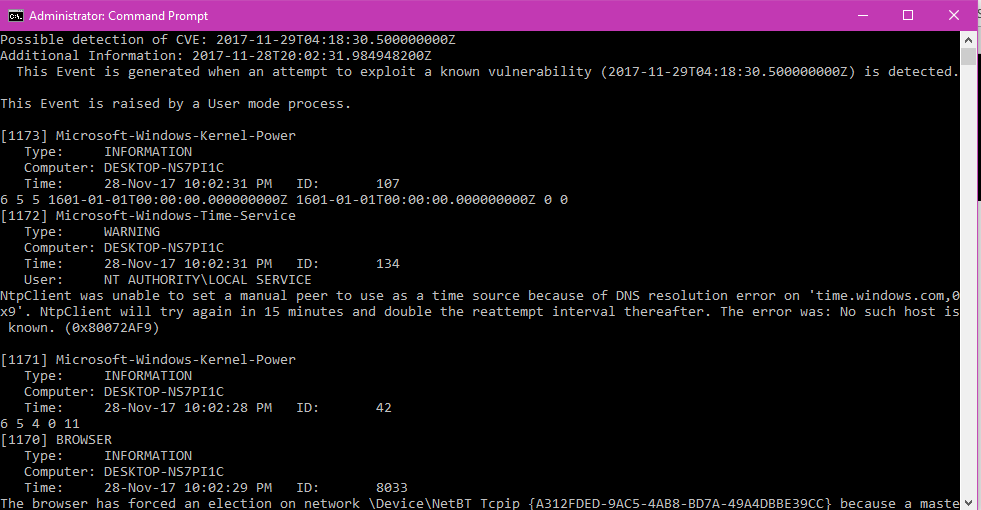
GET SYSTEM LOG IN/ LOGOUT INFORMATION

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

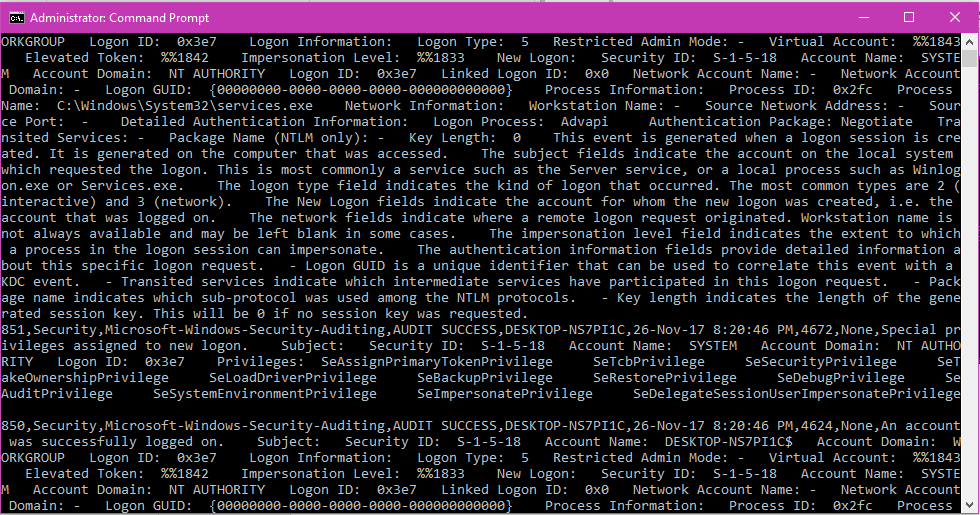


|  |
| --- |
| Command: NTLast.exe |

SYSTEM EVENT LOGS

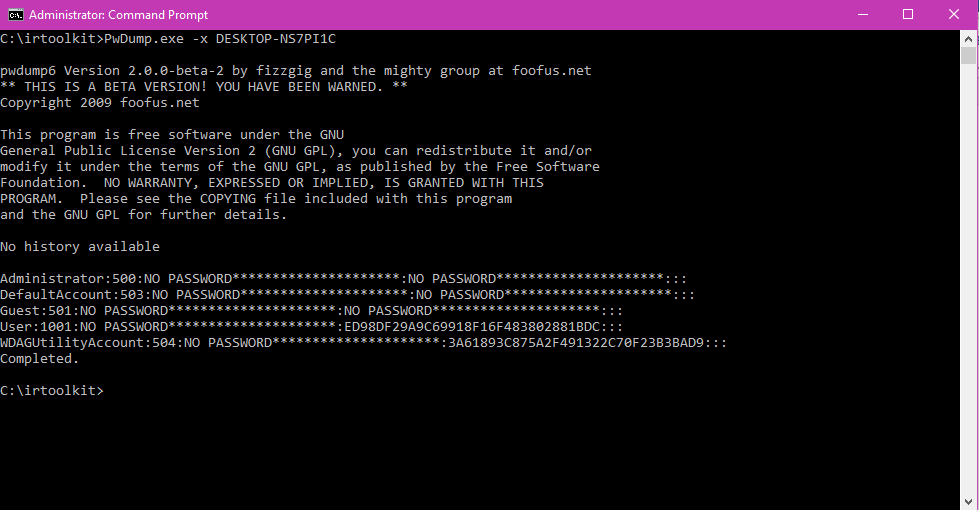


|  |
| --- |
| Command: PsLogList |



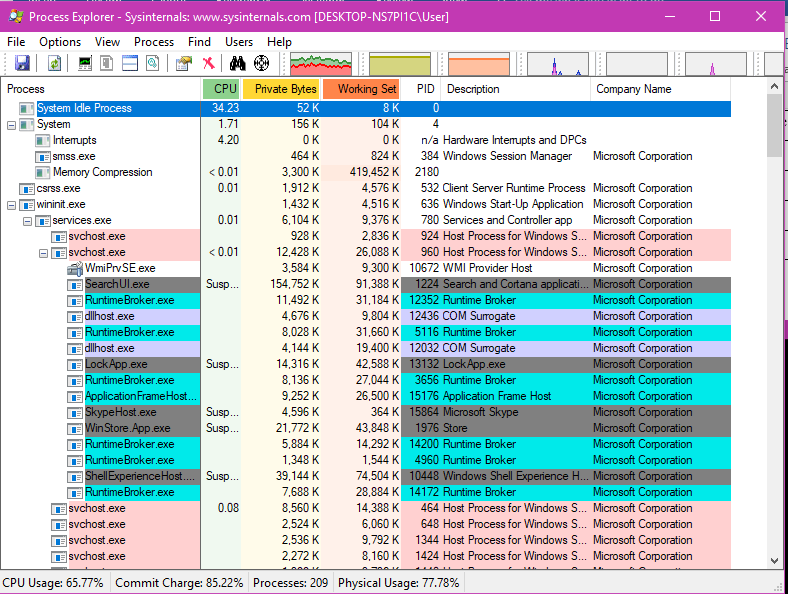
|  |
| --- |
| Command: psloglist –s –x security |

USER ACCOUNTS



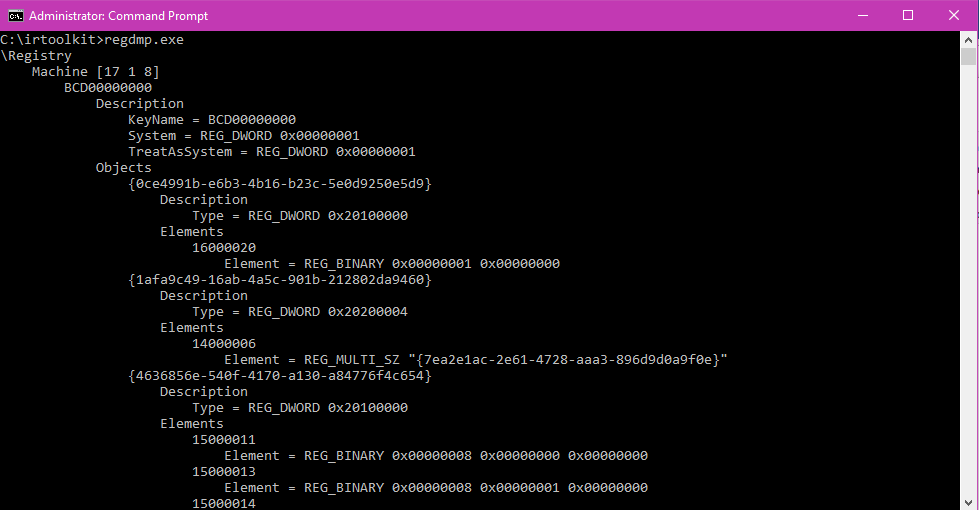
|  |
| --- |
| Command: PwDump.exe -x DESKTOP-NS7P11C (machine name) |

SUSPICIOUS FILES



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

REGISTRY DATA



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