

**SCHOOL OF INFORMATION SCIENCE AND TECHNOLOGY**

**COURSE: COMPUTER FORENSICS**

**AUTHOR: NYAMUDEZA PENELOPE**

**REG NUMBER: H140178Y**

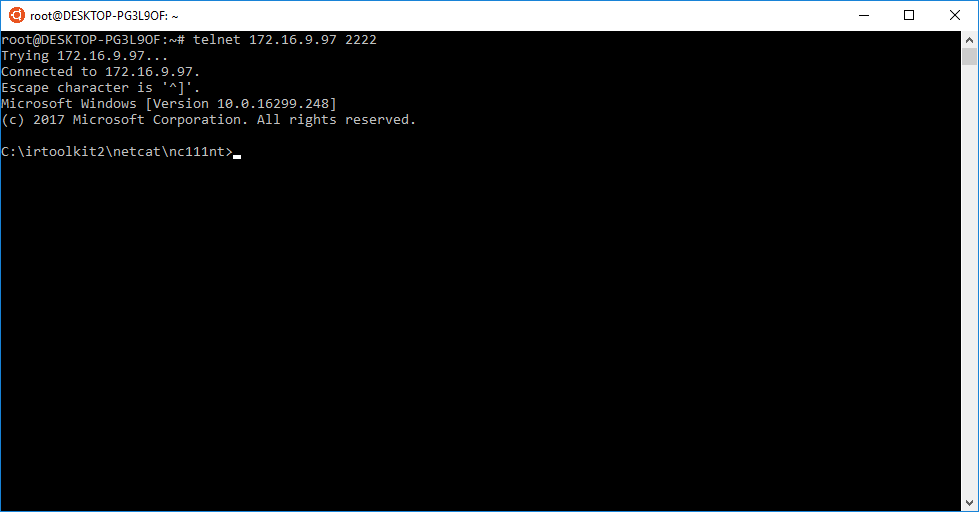
**PROGRAM: ISA**

**LAB 2: NON-VOLATILE**

**TASK 1: NETCAT**

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

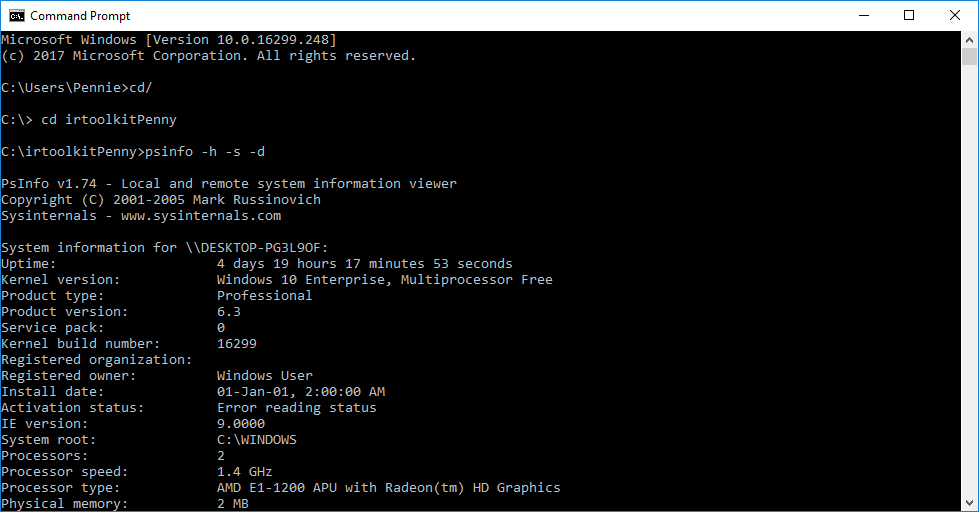
victim machine: command(date) | nc forensic\_workstation\_ip\_address 2222



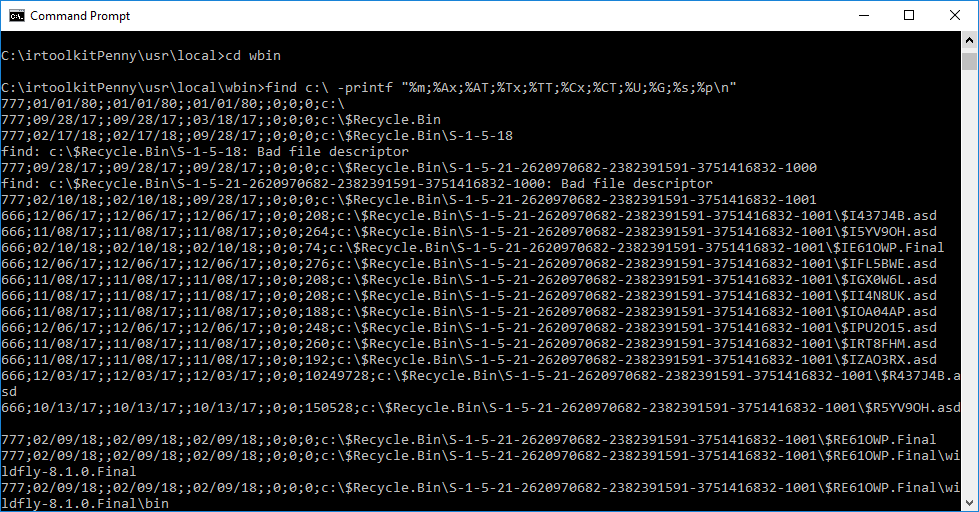
***Screenshot from the victimizing machine***

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

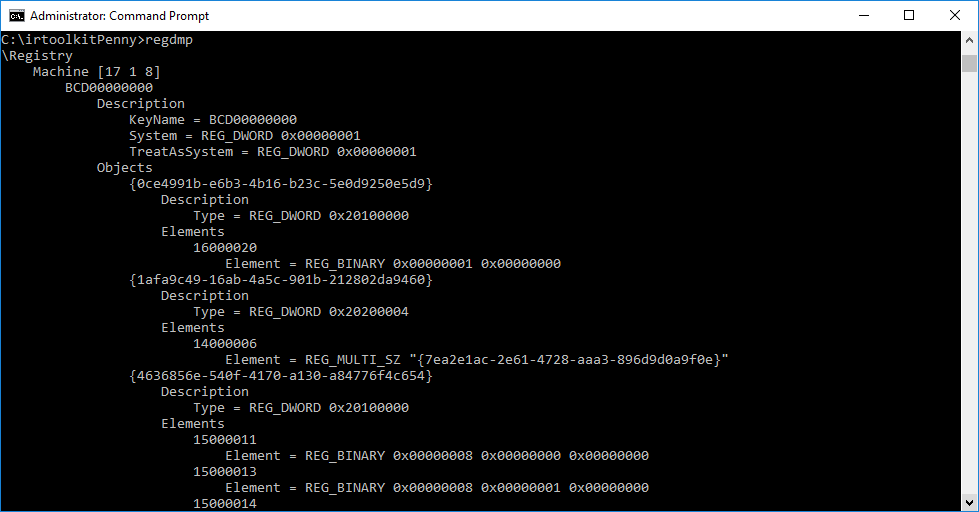


|  |  |
| --- | --- |
| **TASK 3: GET FILE SYSTEM TIME AND DATE STAMPS** | |
| TOOLS REQUIRED: UnxUtils | |
| ARGUMENTS |  |
| c:\ -printf “%m;%Ax;%AT;%Tx;%TT;%Cx;%CT;%U;%G;%s;%p\n” | prints the file permissions, last access date, last access time, modification date, modification time, created date,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

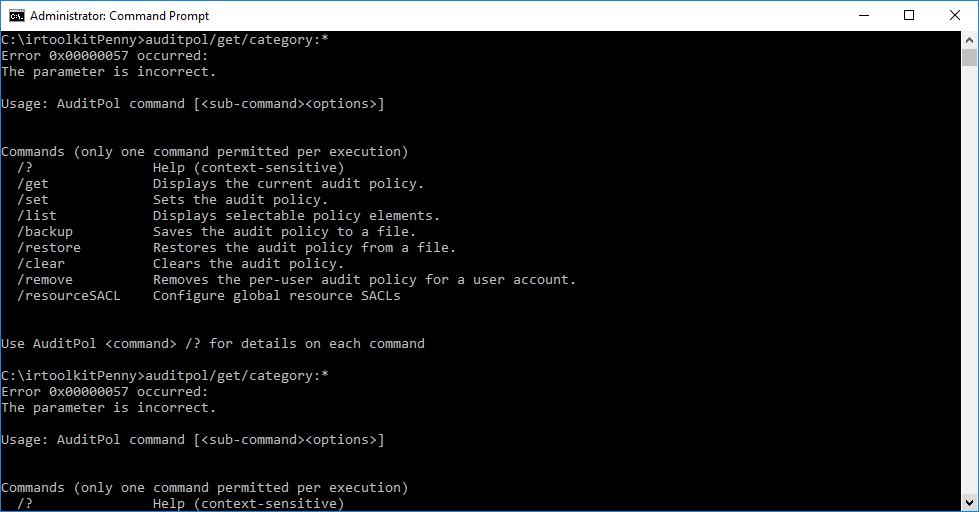


|  |
| --- |
| **Command**: find c:\ -printf “%m;%Ax;%AT;%Tx;%TT;%Cx;%CT;%U;%G;%s;%p\n” |

|  |  |
| --- | --- |
| **TASK 4 : GET REGISTRY DATA** | |
| TOOLS: regDmp | |
| ARGUMENTS |  |
| regDmp | capture the complete registry |



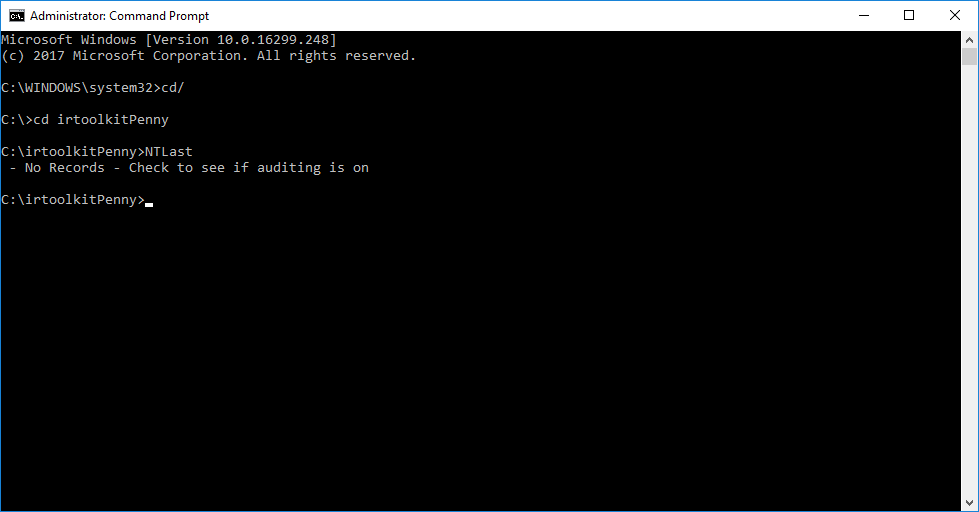
|  |  |
| --- | --- |
| **TASK 5: GET THE AUDIT POLICY** | |
| **TOOLS :** auditpol | |
| **Arguments that can be passed for AUDITPOL** | |
| /? | Help |
| /get | Displays current audit policy |
| /set | Sets the audit policy |
| /list | Displays selective policy elements |
| /backup | Backups the current 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 /get /category:\* |

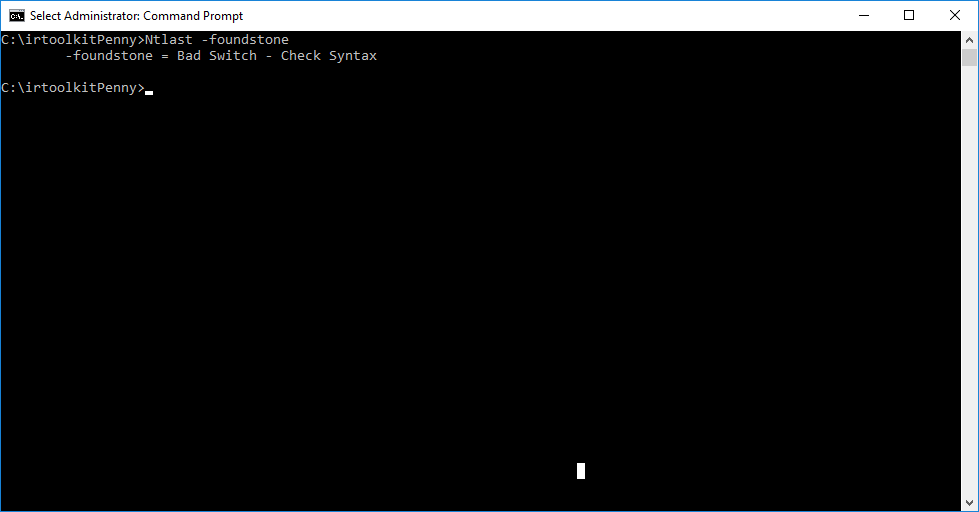
**TASK 6: HISTORY OF LOGINS**

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



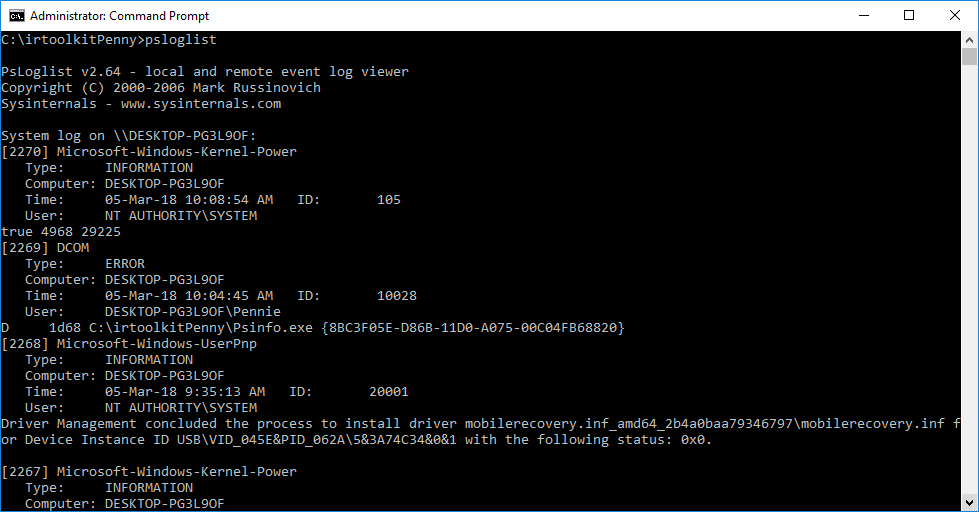
|  |
| --- |
| **Command**: NTlast |

|  |
| --- |
| **Command:** NTLast - foundstone |

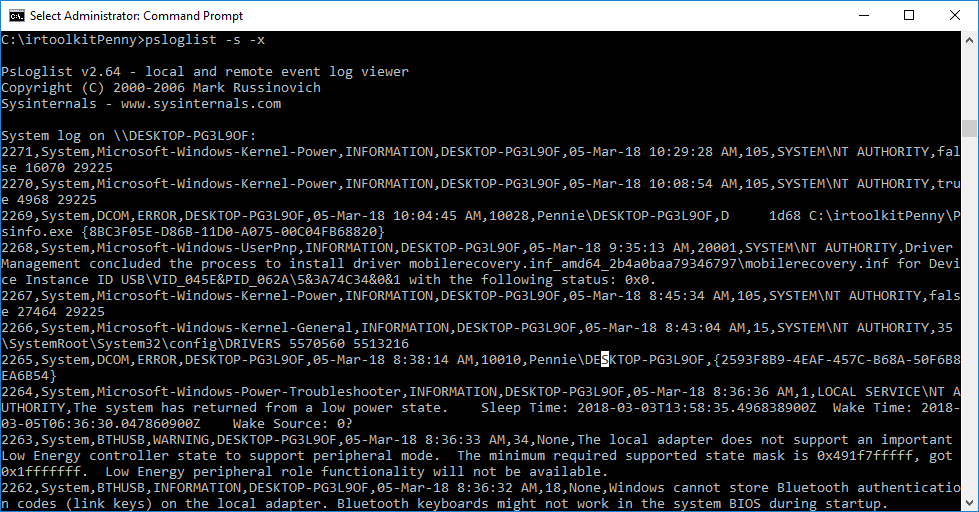


**TASK 7: SYSTEM EVENT LOGS**

|  |
| --- |
| **Command:** psloglist |

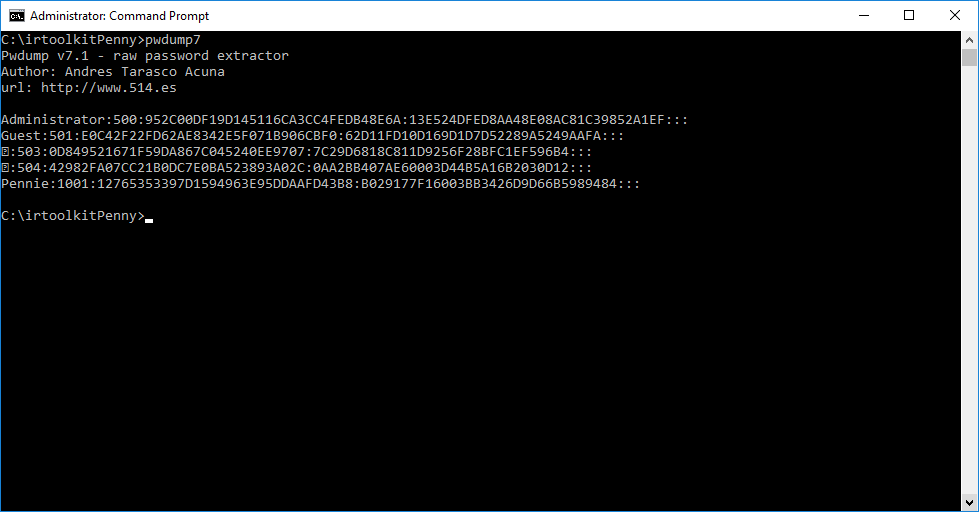


**Command**: psloglist –s –x security



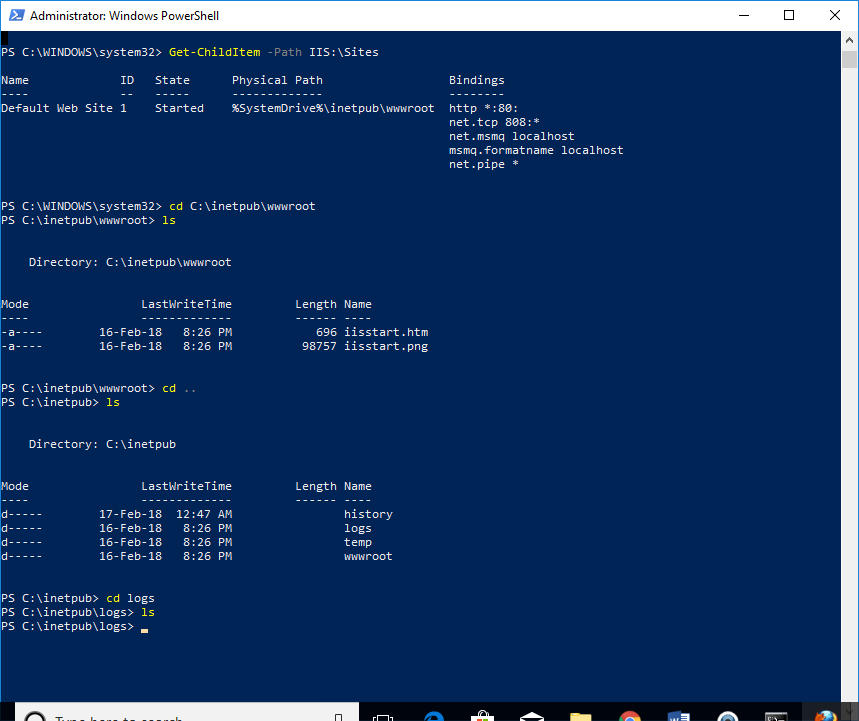
**TASK 8: USER ACCOUNTS**

|  |
| --- |
| **Command**: Pwdump |



**TASK 9: IIS Logs**

|  |  |
| --- | --- |
| **Command**: Get | Children –Path IIS:\Sites |



**TASK 10: SUSPICIOUS FILES**

**Command**: procexp.exe

