

HARARE INSTITUTE OF TECHNOLOGY

INFORMATION SECURITY AND ASSURANCE PART 4

JAPHET MUCHAZONDIDA H140172Z

COMPUTER FORENSICS LAB 2

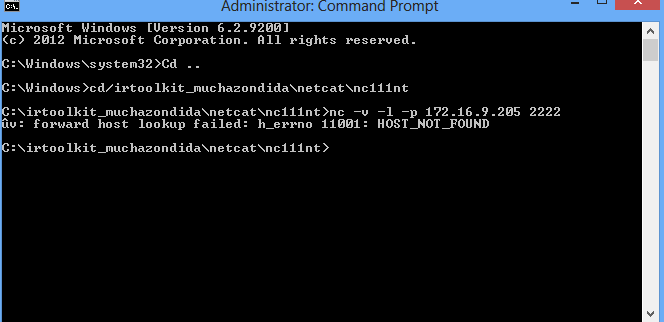
TUTOR: MR MARENGEREKE

**TASK 1: netcat**

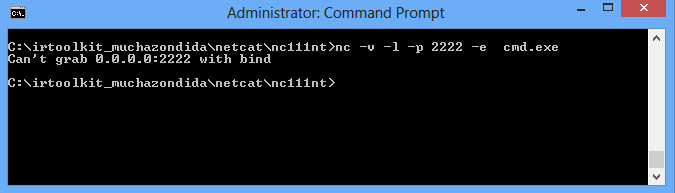
starting serve netcat : nc –v –l –p 2222 > japhet\_28\_02\_2018.txt

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

**SCREENSHOT**



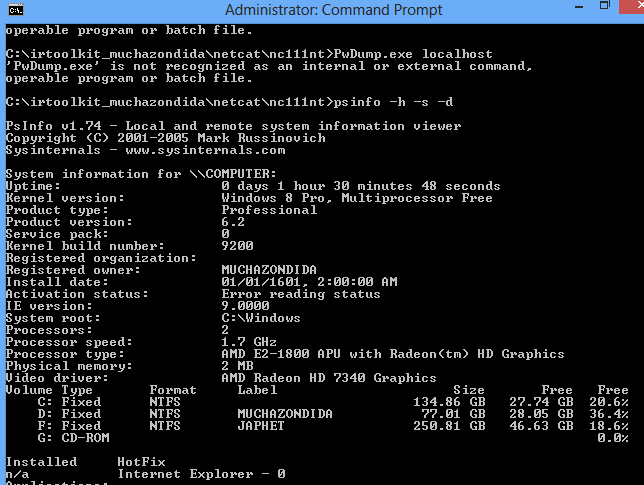
COMMAND: nc –v –l –p 2222 > japhet\_28\_02\_2018.txt



COMMAND: nc –v –l –p 2222 –e cmd.exe

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

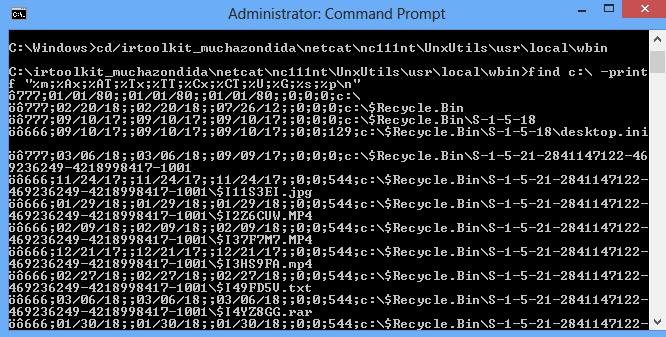
**SCREENSHOT**



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 |

**SCREENSHOT**

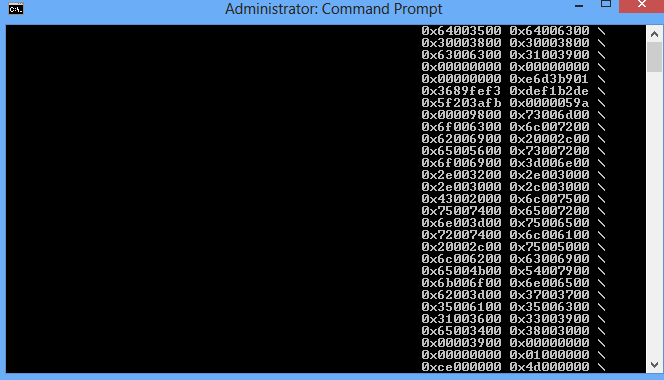


COMMAND: find c:\ -printf “%m;%Ax;%AT;%Tx;%TT;%Cx;%CT;%U;%G;%s;%p\n”

**TASK 4: Registry Data**

Tool used: regDmp.exe

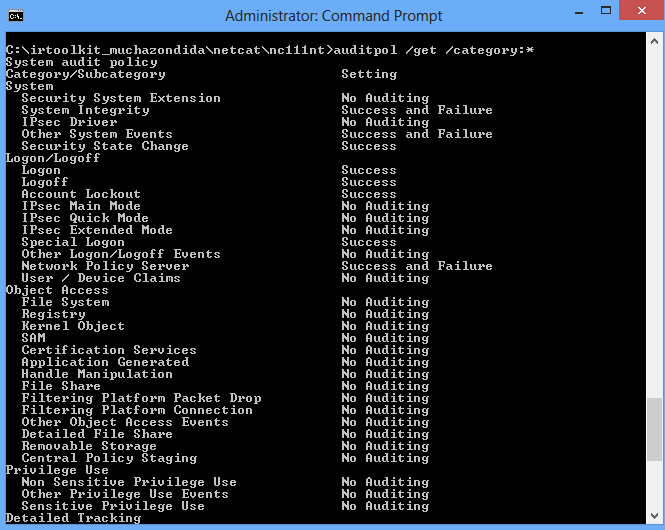
SCREENSHOT



COMMAND: regDmp

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

**SCREENSHOT**

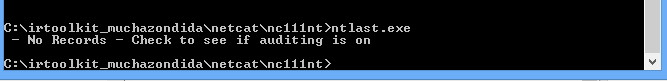


|  |
| --- |
| COMMAND : auditpol /get /category:\*  This command will display the current security policy in categories |

**TASK 6: 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 |

**SCREENSHOT**

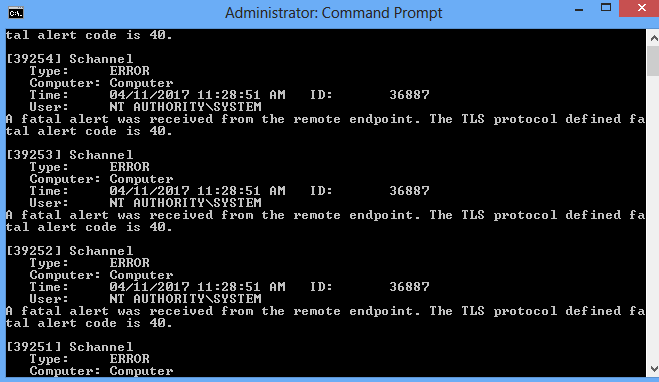


COMMAND: ntlast.exe

**TASK 7: 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 |

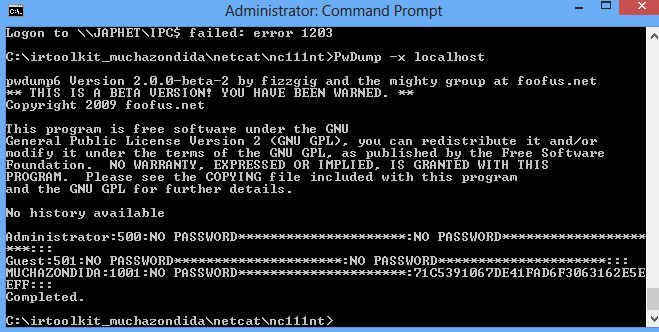
**SCREENSHOT**



COMMAND: PsLogList

**TASK 8: User Accounts**

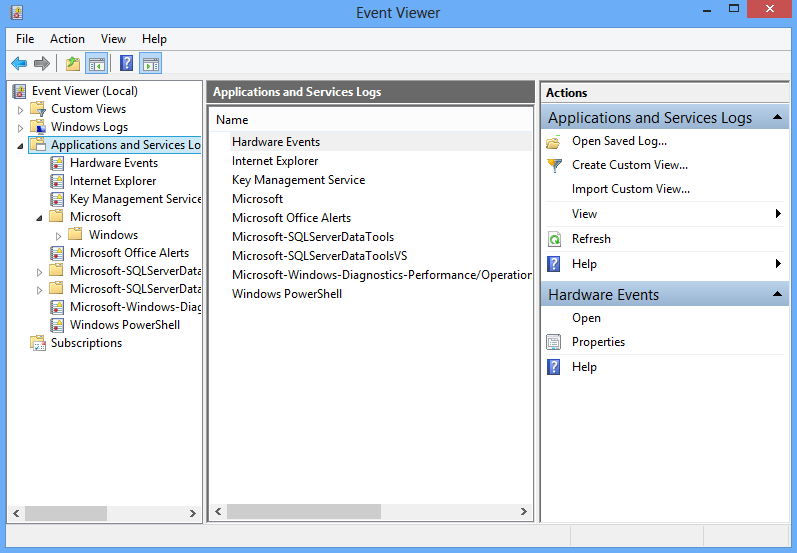
**SCREENSHOT**



COMMAND: PwDump –x localhost

**TASK 9: IIS Logs**

**SCREENSHOT**

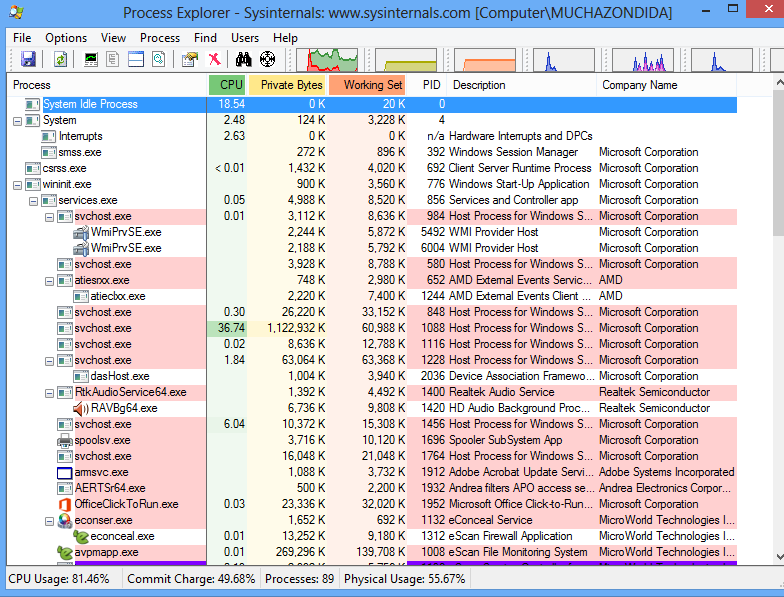


COMMAND: start eventvwr

**TASK 10: Suspicious Files**

TOOLS: procexp.exe

**SCREENSHOT**



COMMAND: procexp.exe

**Doskey /history**

