

**NAME:** **PATIENCE MATARIRO**

**REG NUMBER: H140342H**

**MODULE: COMPUTER FORENSICS LAB2 NON VOLATILE DATA**

**TUTOR: MR MARENGEREKE**

|  |
| --- |
| **TASK 1:**ESTABLISH REMOTE CONNECTION BTWN SERVER AND VICTIM |
| **TOOLS:**NETCAT |

**SCREENSHOT: SERVER MACHINE**

****

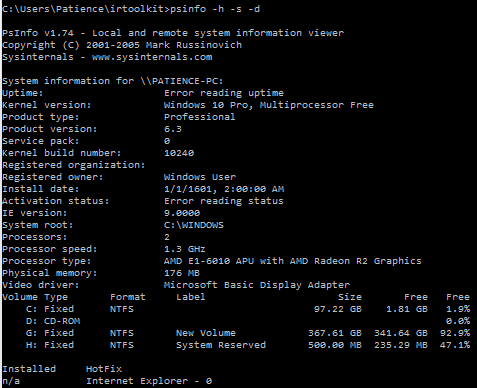
|  |
| --- |
| VICTIM MACHINE |
| **COMMAND:** COMMAND (DATE) |NC FORENSIC \_WORKSTATION\_IP\_ADDRESS 2222. |

**SCREENSHORT: VICTIM MACHINE**

**C:\Users\vimbai\Desktop\slab\lab2\ne2.PNG**

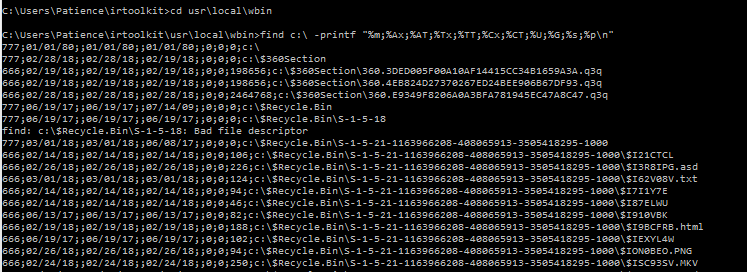
|  |
| --- |
| **TASK2:**SYSTEM VERSION AND PATCH LEVEL |
| **COMMAND** :PSINFO –H –S -D |

**SCREENSHOT:**

****

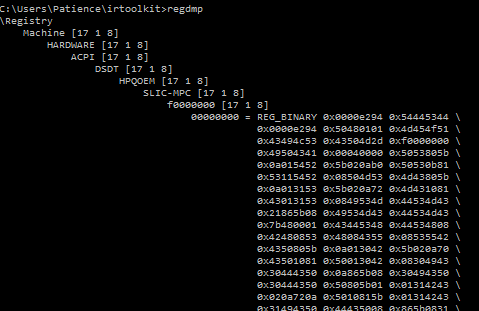
|  |  |
| --- | --- |
| **TASK 3** | FILE SYSTEM TIME AND DATE STAMPS |
| **COMMAND** | find c:\ -printf “%m;%Ax;%AT;%Tx;%TT;%Cx;%CT;%U;%G;%s;%p\n” |

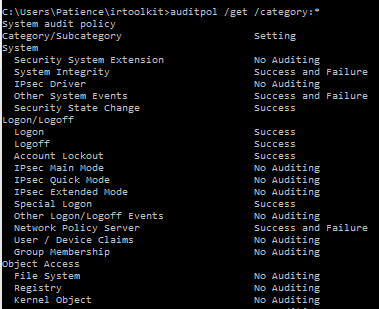
**SCREENSHOT**

****

|  |  |
| --- | --- |
| **TASK 4** | REGISTRY DATA |
| **COMMAND** | REGDMP>>patience\_h140342h.txt |

**SCREENSHOTS:**

****

****

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

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

**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 |

**SCREENSHOTS:**



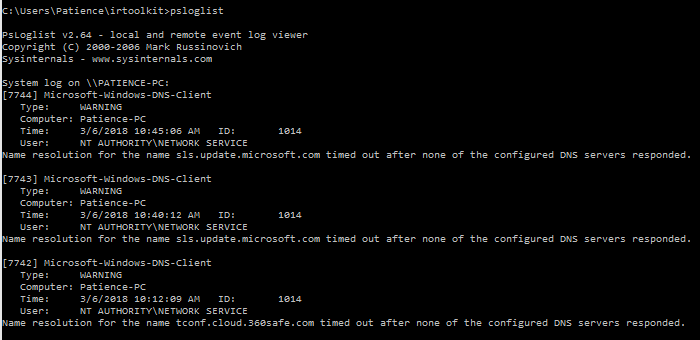


|  |
| --- |
| COMMAND : ntlast.exe |

**TASK 7**: GET SYSTEM EVENT LOGS AND SECURITY

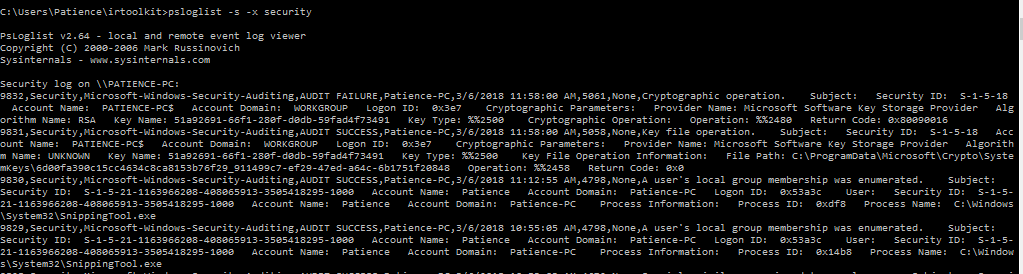
|  |  |
| --- | --- |
| **TOOLS** :PslogList | |
| Arguments that can be passed for **DATE** | |
| el |enum logs | List log names |
| gl | get-log | Gets log configuration information |
| sl|set-log | Modify configuration of a log |
| qe|query-events | Query from an existing log files |
| Epl | export-log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

**SCREENSHOT: SYSTEM LOG**

****

|  |
| --- |
| COMMAND : psloglist  Sows all the list of system logs |

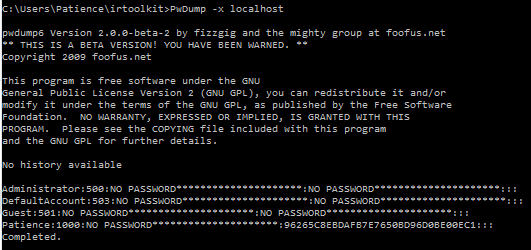
**SCREENSHOT: SECURITY LOG**

****

|  |
| --- |
| COMMAND : psloglist –s –x security  Sows all the list of system security logs |

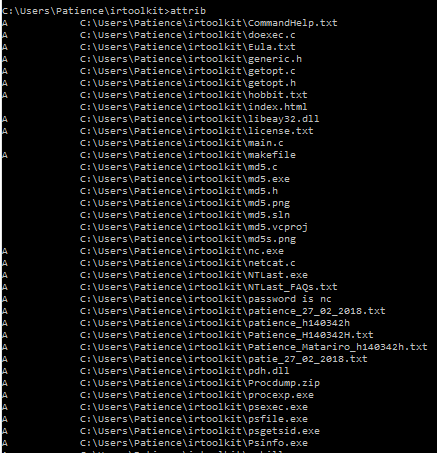
|  |  |
| --- | --- |
| **TASK8** | User Accounts |
| **COMMAND** | PwDump -x localhost |

**SCREENSHOT:**

****

|  |  |
| --- | --- |
| **TASK 9** | SUSPICIOUS FILES |
| **COMMAND** | ATTRIB |

**SCREENSHOT:**

****

|  |  |
| --- | --- |
| **TASK 10** | IIS FILES |
| **TOOLS** | WINDOWS POWERSHELL |

**SCREENSHOT**

