

INFORMATION SECURITY AND ASSURANCE

JABULANI DAVID ZULU

**ISS 421: COMPUTER FORENSICS**

**LAB 2: NON-VOLATILE DATA**

MR T. MARENGEREKE

**Task 1: NetCat**

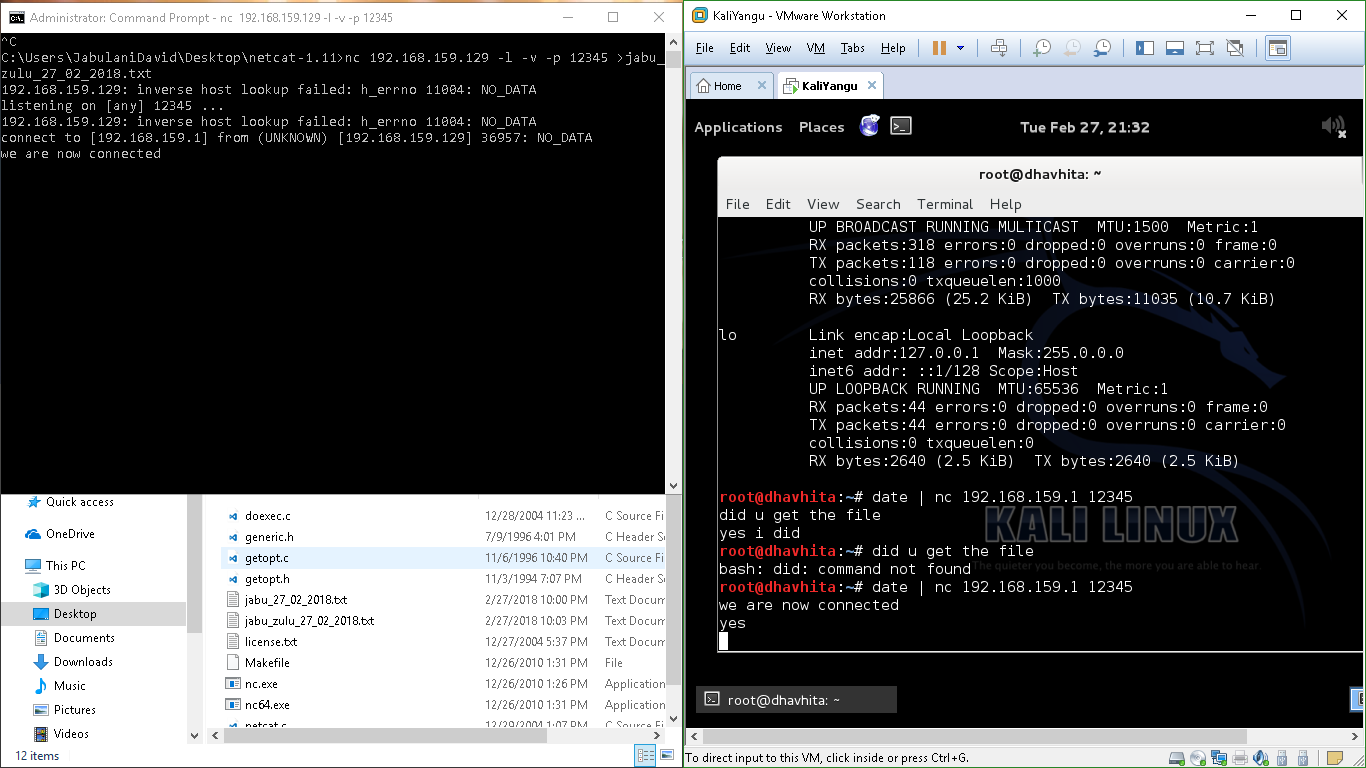
TOOLS: netcat 1.11

1. **Starting NetCat Server**

COMMAND: “*nc 192.168,159.129 –v –l –p 12345 > jabu\_zulu\_27\_02\_2018.txt”*

1. **Send victim machine date**

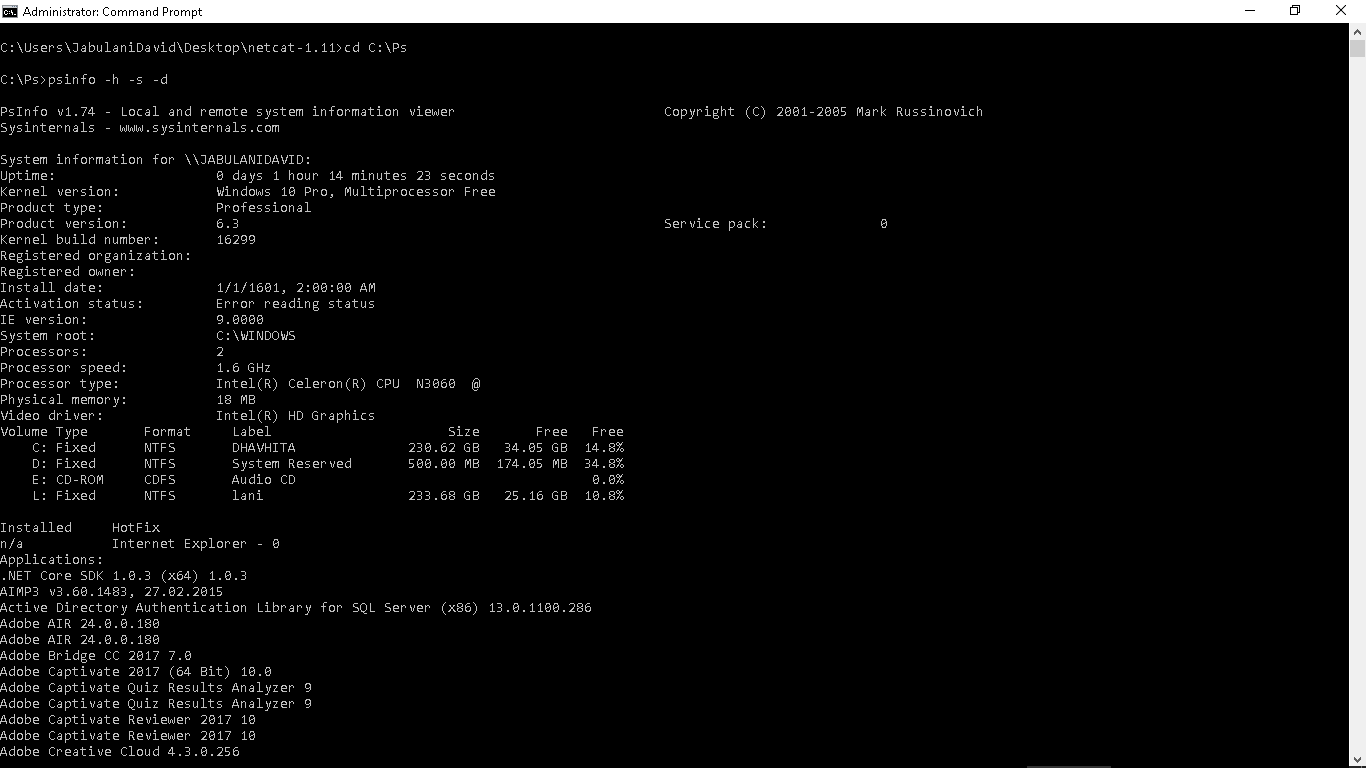
COMMAND: *“date | nc 192.168.159.1 12345”*



**Task 2: Check System Version and Patch Level**

TOOLS: PsTools, cmd.exe

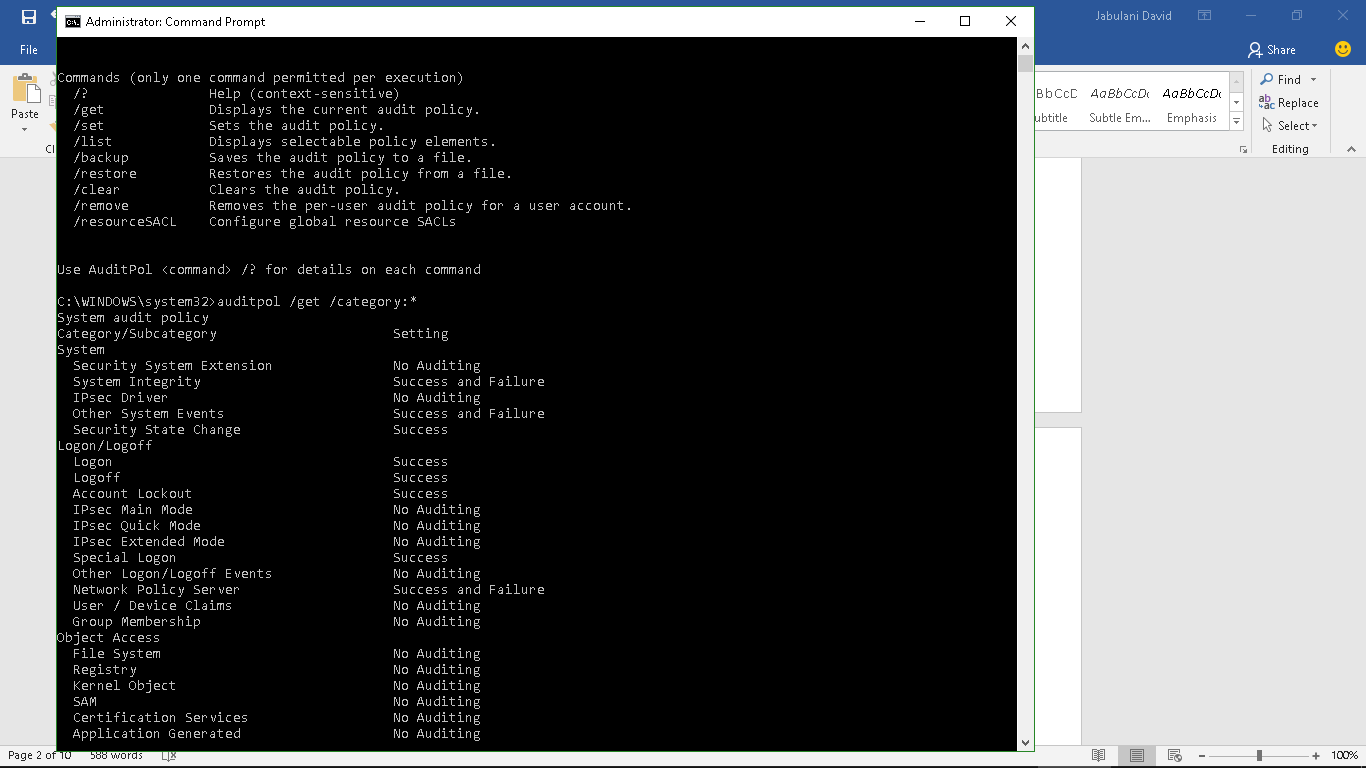
COMMAND: “psinfo -h -s -d*”*



**Task 3: The Auditing Policy**

TOOLS: AUDITPOL

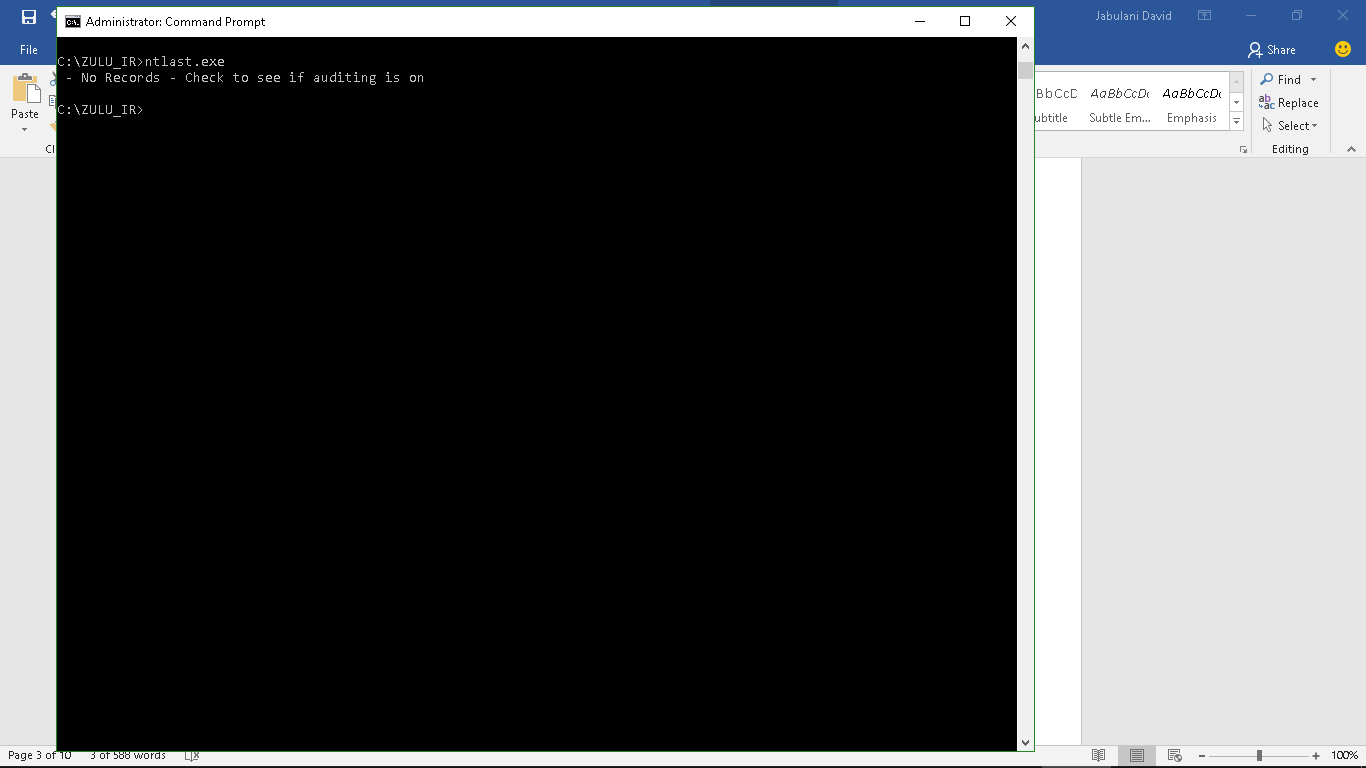
COMMAND: “*auditpol /get /category:\*”*



**Task 4: A History of Logins**

TOOLS: McAfee NTLast Tools

COMMAND: “*ntlast.exe”*



**Task 5: System Event Logs**

TOOLS: PsLoglist

COMMAND: “*psloglist –s –x security*

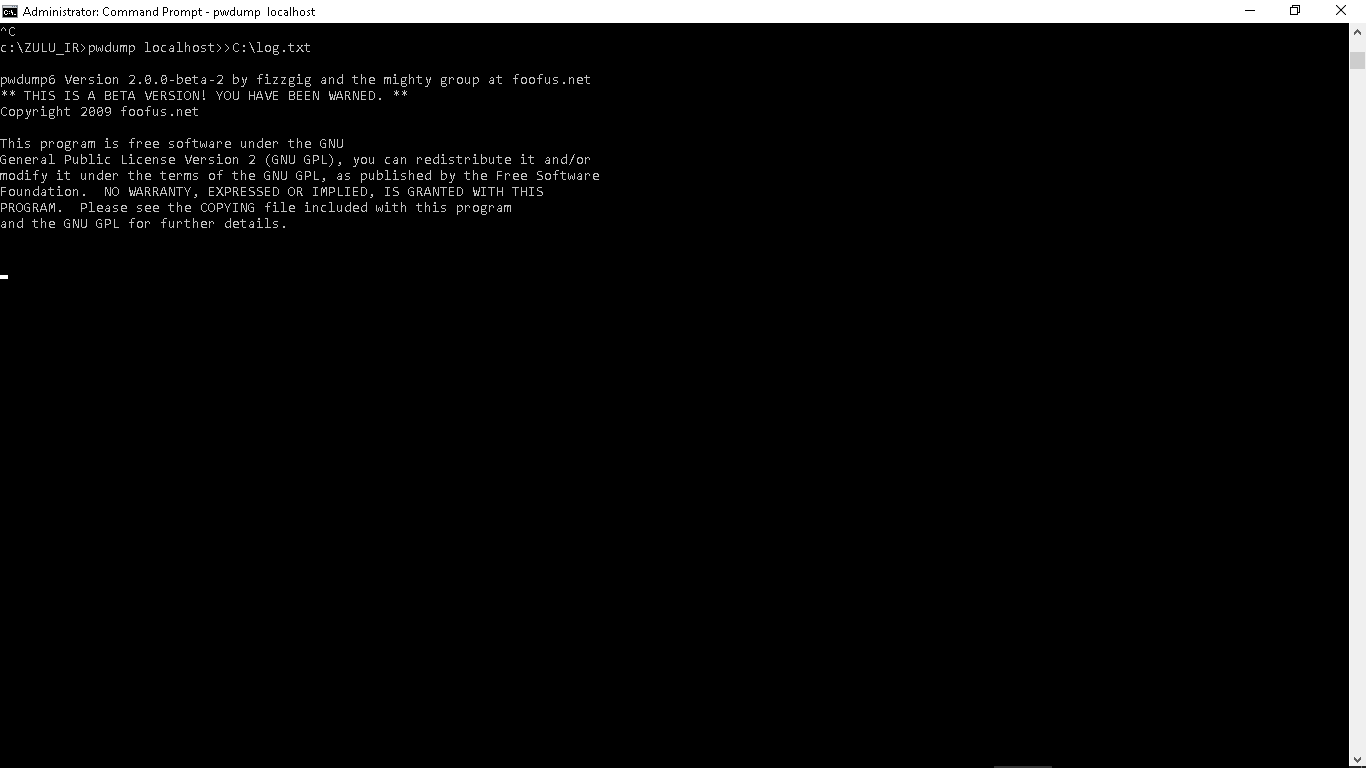
OUTPUT:



**Task 6:** **User Accounts**

TOOLS: pwdump6.exe

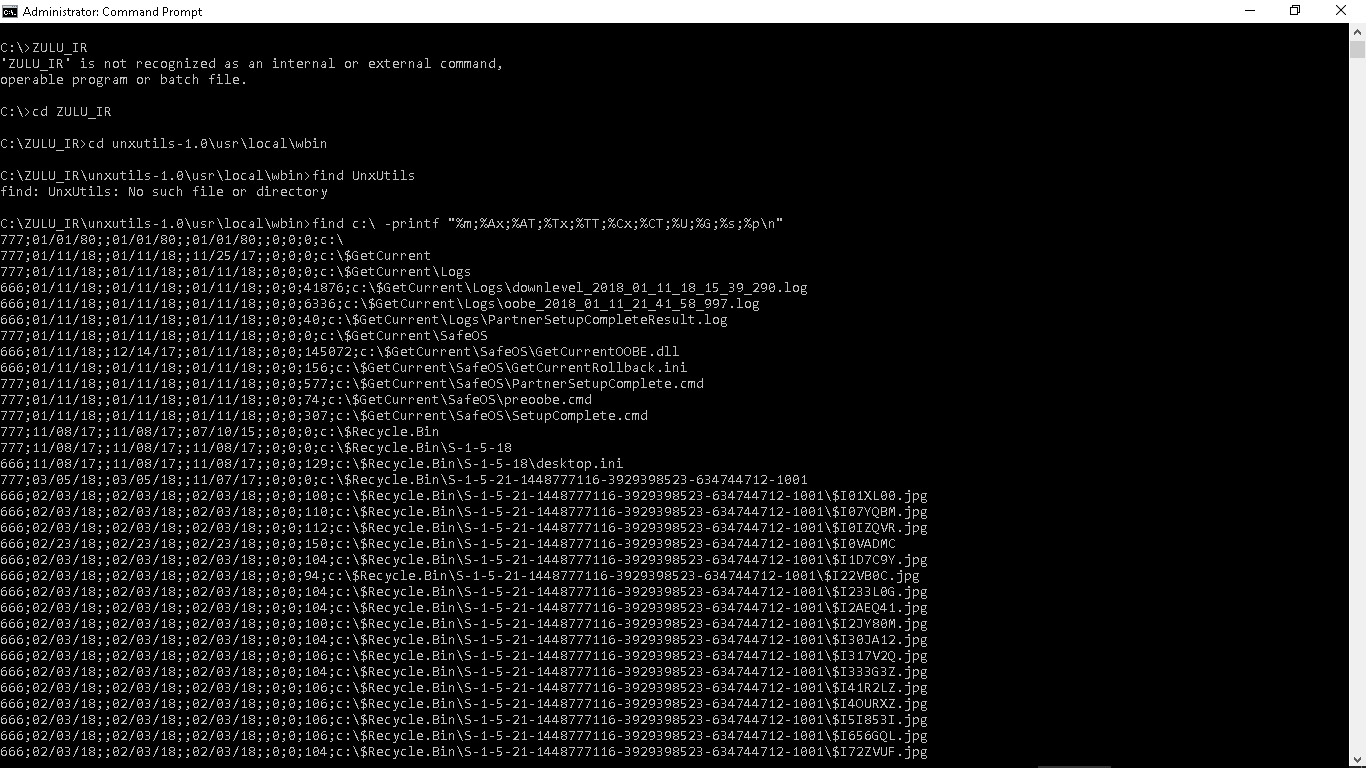
COMMAND: “*pwdump localhost>>C:\log.txt*”



**Task 7: UnxUtils**

TOOLS: Find, UnxUtils

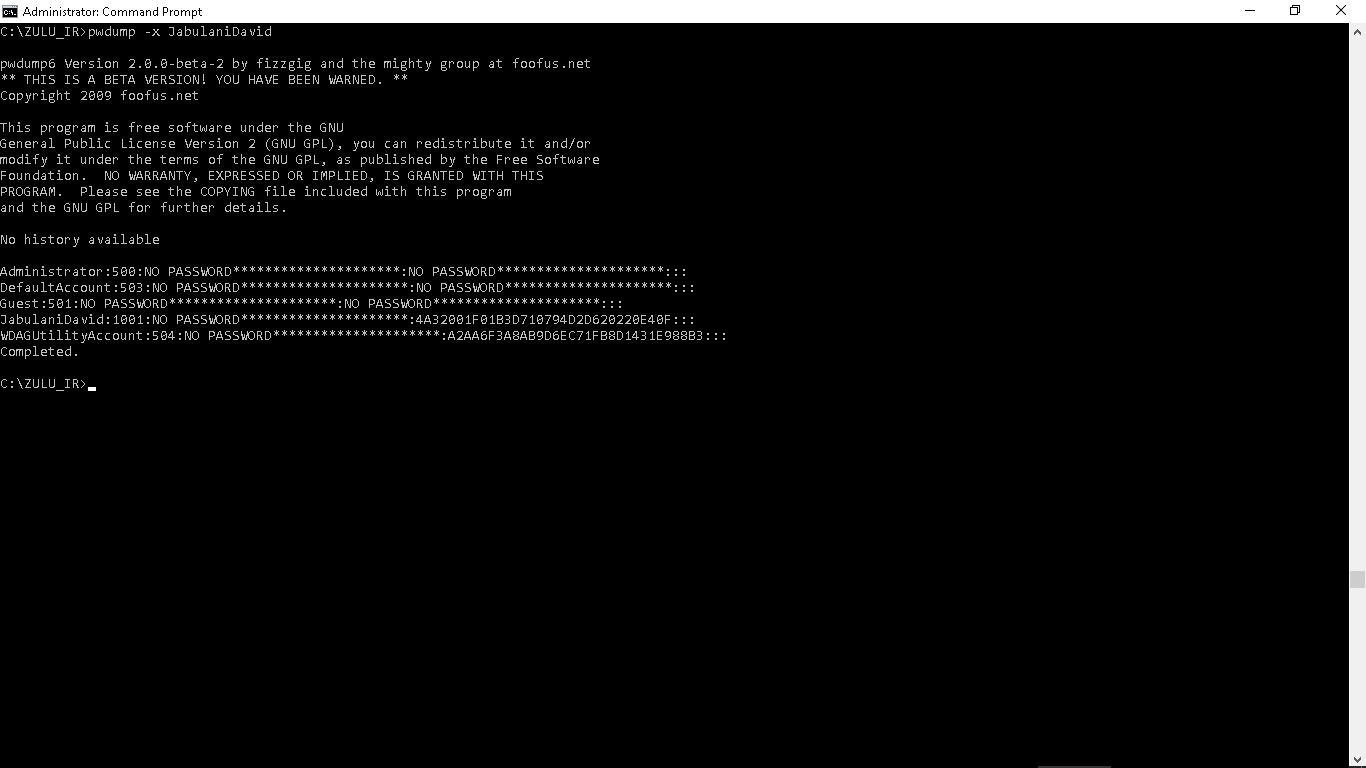
COMMAND: find c:\ -printf “%m;%Ax;%AT;%Tx;%TT;%Cx;%CT;%U;%G;%s;%p\n”



**Task 8: User Accounts**

TOOLS: PwDump6

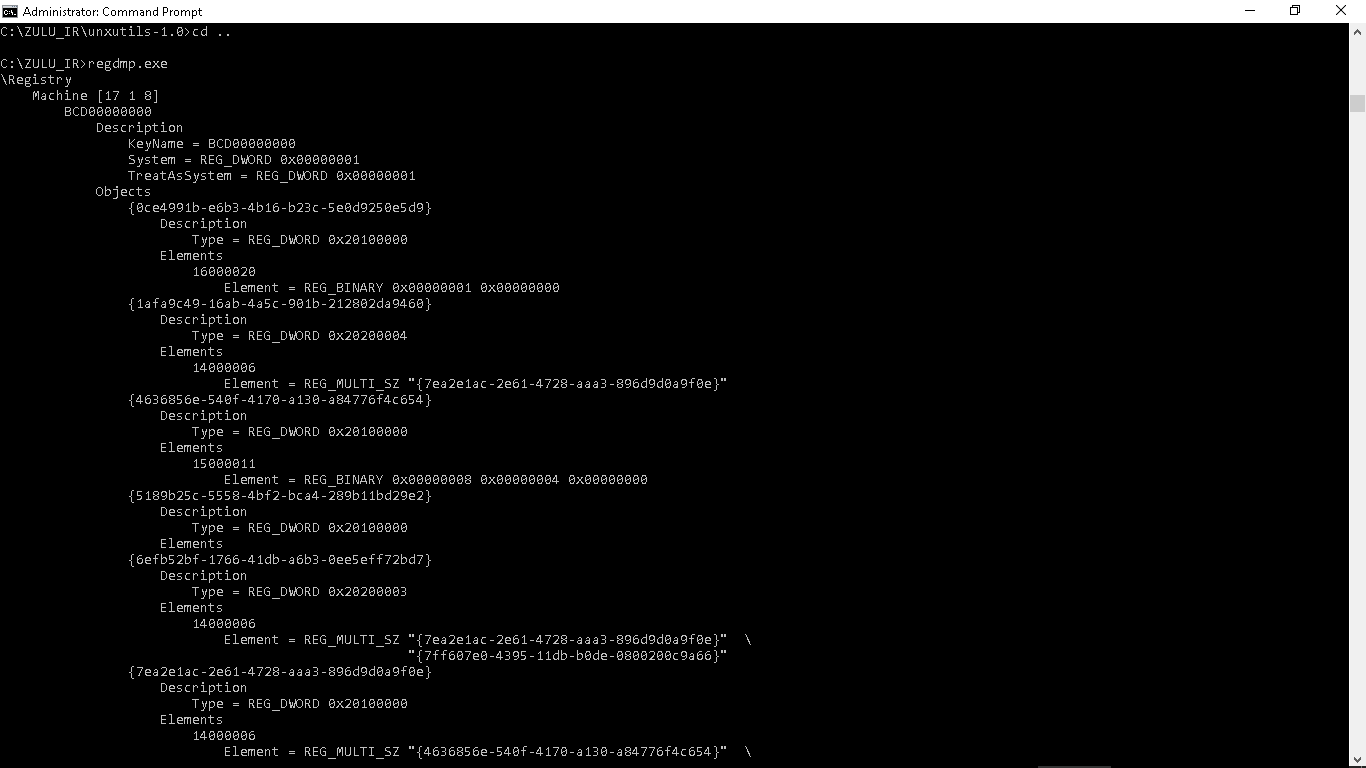
COMMAND: pwdump -x localhhost



**Task 9:** **Registry Data**

TOOLS: regdmp

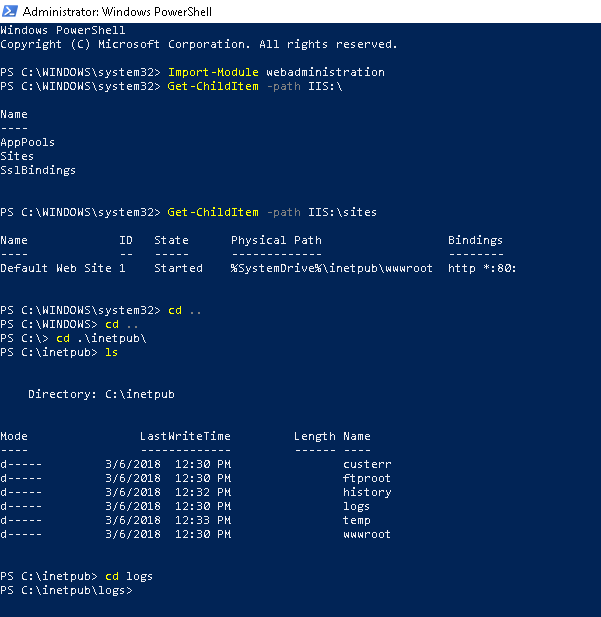
COMMAND: regdmp.exe



**Task 10:IIS**

TOOLS: IIS, PowerShell

COMMAND: Get\_ChildItem -path IIS:\



**Task 11: SUSPICIOUS FILES**

TOOLS: procexp.exe 