INFORMATION SECURITY AND ASSURANCE

ISHEANESU T MAGAYA

ISS 421: COMPUTER FORENSICS

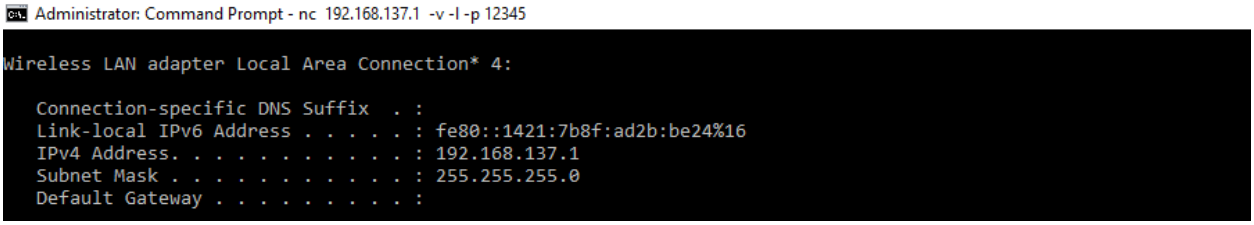
LAB 2: NON-VOLATILE DATA

MR T. MARENGEREKE

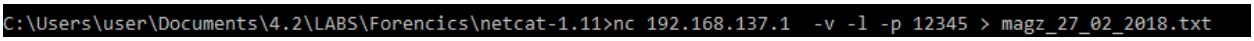
Task	Description	TOOLS
1	**Starting NetCat Server** **Send victim machine date**	NetCat 1.11

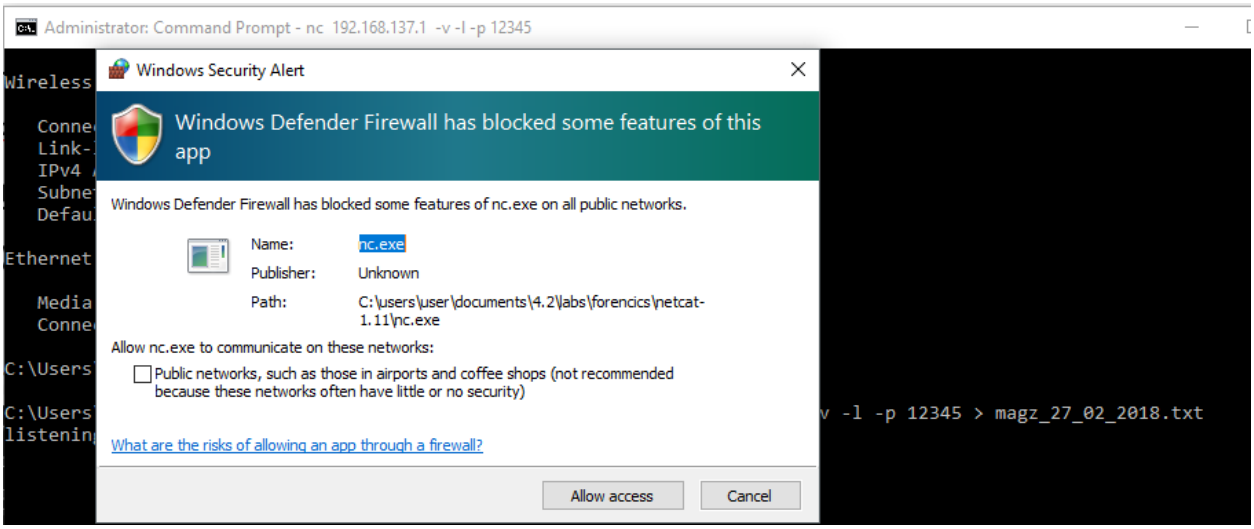
a) Starting NetCat Server

✓ *Command : Ipconfig get the host machine i.e. on windows*

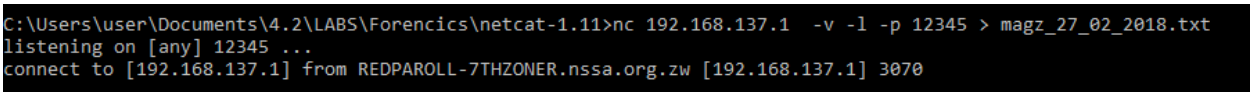


✓ *Command: "nc 192.168.137.1 –v –l –p 12345 > magz_27_02_2018.txt"*



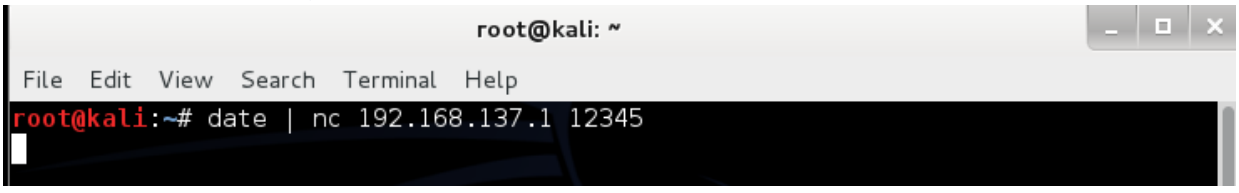


Requires access and permissions



b) Send victim machine date

✓ *Command: "date | nc 192.168.137.1 12345"*



Result

Task	Description	TOOLS
2	Check System Version and Patch Level	PsTools, cmd.exe

✓ *Command: "psinfo -h -s -d"*

```
C:\Users\user\Documents\4.2\LABS\Forencics>psinfo -h -s -d
```

```
C:\Users\user\Documents\4.2\LABS\Forencics>psinfo -h -s -d

PsInfo v1.74 - Local and remote system information viewer
Copyright (C) 2001-2005 Mark Russinovich
Sysinternals - www.sysinternals.com

Querying information for REDPAROLL-7THZO...
```

```
Microsoft Windows [Version 10.0.17093.1000]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\user>CD C:\Users\user\Documents\4.2\LABS\Forencics

C:\Users\user\Documents\4.2\LABS\Forencics>psinfo -h -s -d

PsInfo v1.74 - Local and remote system information viewer
Copyright (C) 2001-2005 Mark Russinovich
Sysinternals - www.sysinternals.com

System information for \\REDPAROLL-7THZO:
Uptime:                    2 days 4 hours 34 minutes 29 seconds
Kernel version:            Windows 10 Enterprise Insider Preview, Multiprocessor Free
Product type:              Professional
Product version:           6.3
Service pack:              0
Kernel build number:       17093
Registered organization:
Registered owner:          user
Install date:              01/01/1601, 2:00:00 AM
Activation status:         Error reading status
IE version:                9.0000
System root:               C:\WINDOWS
Processors:                4
Processor speed:           2.2 GHz
Processor type:            Intel(R) Core(TM) i5-5300U CPU @
Physical memory:           10 MB
Video driver:
Volume Type       Format     Label                    Size       Free   Free
    C: Fixed      NTFS                           464.79 GB   61.70 GB  13.3%
    E: CD-ROM     CDFS       CDROM                14.17 MB              0.0%
```

Task	Description	TOOLS
3	The Auditing Policy	AUDITPOL

✓ *COMMAND: "auditpol /get /category:*"*

```
C:\WINDOWS\system32>cd C:\Users\user\Documents\4.2\LABS\Forencics

C:\Users\user\Documents\4.2\LABS\Forencics>auditpol /get /category:*
System audit policy
Category/Subcategory                      Setting
System
  Security System Extension               No Auditing
  System Integrity                        No Auditing
  IPsec Driver                            No Auditing
  Other System Events                     No Auditing
  Security State Change                   No Auditing
Logon/Logoff
  Logon                                   Success
  Logoff                                  Success
  Account Lockout                         Success
  IPsec Main Mode                         No Auditing
  IPsec Quick Mode                        No Auditing
  IPsec Extended Mode                     No Auditing
  Special Logon                           No Auditing
  Other Logon/Logoff Events               No Auditing
  Network Policy Server                   No Auditing
  User / Device Claims                    No Auditing
  Group Membership                        No Auditing
Object Access
  File System                             No Auditing
  Registry                                No Auditing
  Kernel Object                           No Auditing
  SAM                                     No Auditing
  Certification Services                  No Auditing
  Application Generated                   No Auditing
  Handle Manipulation                     No Auditing
  File Share                              No Auditing
  Filtering Platform Packet Drop          No Auditing
  Filtering Platform Connection           No Auditing
  Other Object Access Events              No Auditing
  Detailed File Share                     No Auditing
  Removable Storage                       No Auditing
  Central Policy Staging                  No Auditing
Privilege Use
  Non Sensitive Privilege Use             No Auditing
  Other Privilege Use Events              No Auditing
  Sensitive Privilege Use                 No Auditing
Detailed Tracking
  Process Creation                        No Auditing
  Process Termination                     No Auditing
  DPAPI Activity                          No Auditing
```

Task	Description	TOOLS
4	A History of Logins	McAfee NTLast Tools

✓ *COMMAND: "ntlast.exe"*

```
C:\Users\user\Documents\4.2\LABS\Forencics>cd C:\Users\user\Documents\4.2\LABS\Forencics\ntlast30

C:\Users\user\Documents\4.2\LABS\Forencics\ntlast30>NTLast.exe
 - No Records - Check to see if auditing is on

C:\Users\user\Documents\4.2\LABS\Forencics\ntlast30>
```

Task	Description	TOOLS
5	System Event Logs	PsLoglist

✓ *COMMAND: "psloglist –s –x security"*

OUTPUT:

Task	Description	TOOLS
6	User Accounts	pwdump6.exe

✓ *COMMAND: "pwdump localhost>>C:\log.txt"*

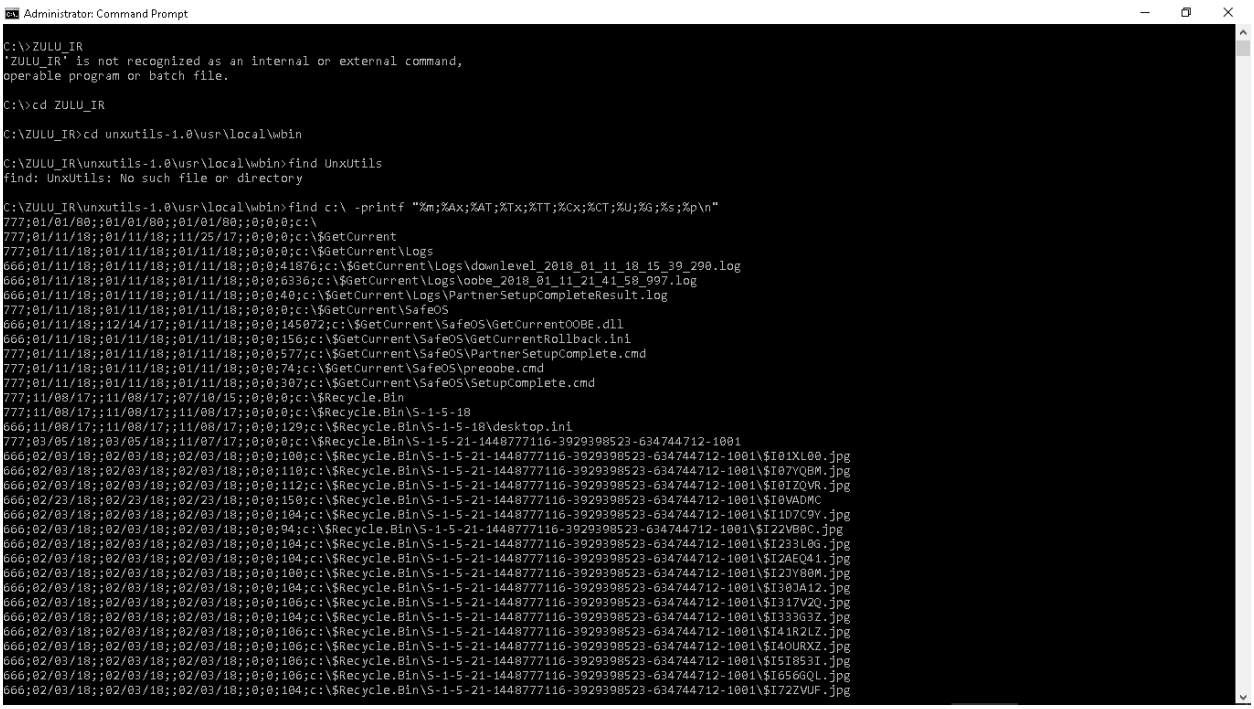
```
C:\Users\user\Documents\4.2\LABS\Forencics>cd C:\Users\user\Documents\4.2\LABS\Forencics\pwdump6-2.0.0-beta-exe-only

C:\Users\user\Documents\4.2\LABS\Forencics\pwdump6-2.0.0-beta-exe-only>pwdump localhost>>C:\log.txt

pwdump6 Version 2.0.0-beta-2 by fizzgig and the mighty group at foofus.net
** THIS IS A BETA VERSION! YOU HAVE BEEN WARNED. **
Copyright 2009 foofus.net

This program is free software under the GNU
General Public License Version 2 (GNU GPL), you can redistribute it and/or
modify it under the terms of the GNU GPL, as published by the Free Software
Foundation.  NO WARRANTY, EXPRESSED OR IMPLIED, IS GRANTED WITH THIS
PROGRAM.  Please see the COPYING file included with this program
and the GNU GPL for further details.
```

Name	Date modified	Type	Size
4dc8a42e778f28f0447df84d59ff	05/02/2018 8:38 PM	File folder	
composer	06/02/2018 4:01 PM	File folder	
Dell	05/02/2018 8:09 PM	File folder	
Intel	08/02/2018 8:28 PM	File folder	
metasploit	07/03/2018 4:30 PM	File folder	
PerfLogs	03/02/2018 9:56 AM	File folder	
PortQryV2	06/03/2018 2:59 PM	File folder	
PostgreSQL	07/02/2018 5:51 PM	File folder	
Program Files	12/03/2018 5:41 PM	File folder	
Program Files (x86)	20/03/2018 11:18	File folder	
Python27	05/02/2018 8:40 PM	File folder	
SQLite3	12/03/2018 5:38 PM	File folder	
Users	22/02/2018 5:55 PM	File folder	
Windows	16/03/2018 7:06 PM	File folder	
Windows10Upgrade	06/02/2018 11:54	File folder	
xampp	05/03/2018 2:42 PM	File folder	
log.txt	21/03/2018 5:23 PM	Text Document	0 KB
sshd.pid	19/03/2018 12:23	PID File	1 KB

log.txt

Task	Description	TOOLS
7	UnxUtils	Find, UnxUtils

✓ *COMMAND: find c:\ -print "%m;%Ax;%AT;%Tx;%TT;%Cx;%CT;%U;%G;%s;%p\n"*



Task	Description	TOOLS
8	User Accounts	pwdump -x localhost

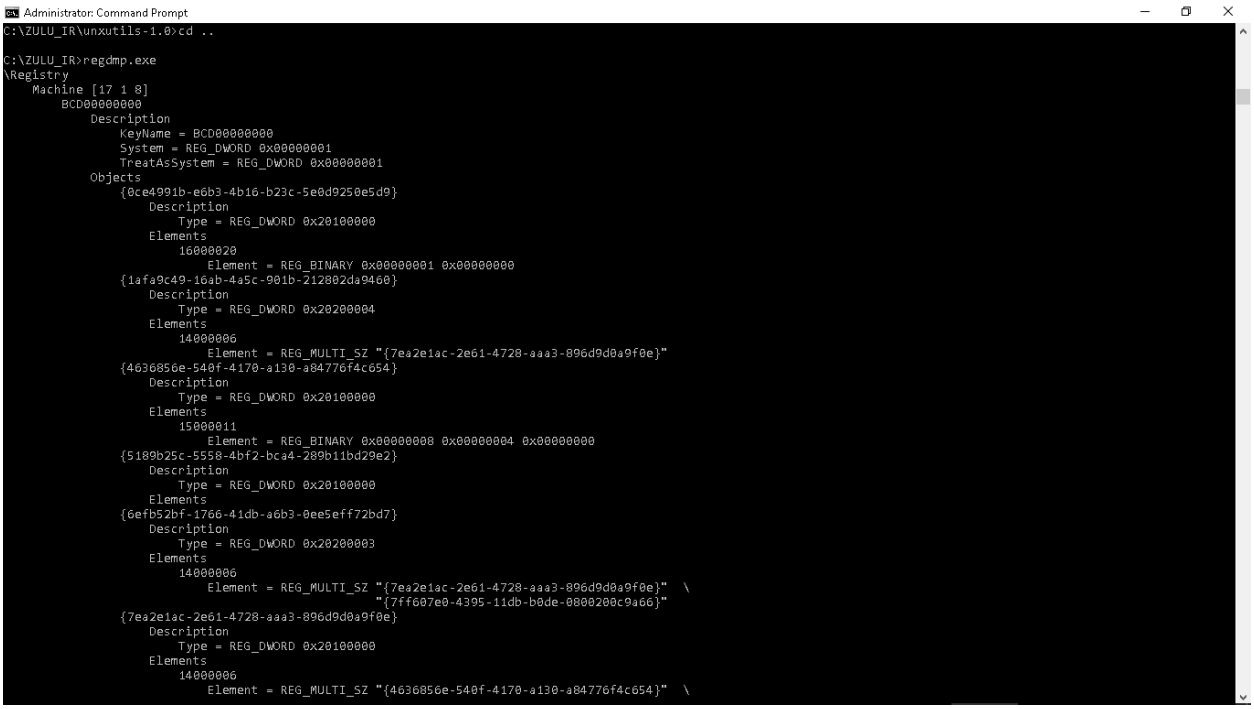
✓ *Command: pwdump -x localhost*

```
C:\Users\user\Documents\4.2\LABS\Forencics\pwdump6-2.0.0-beta-exe-only>pwdump -x localhhost

pwdump6 Version 2.0.0-beta-2 by fizzgig and the mighty group at foofus.net
** THIS IS A BETA VERSION! YOU HAVE BEEN WARNED. **
Copyright 2009 foofus.net

This program is free software under the GNU
General Public License Version 2 (GNU GPL), you can redistribute it and/or
modify it under the terms of the GNU GPL, as published by the Free Software
Foundation.  NO WARRANTY, EXPRESSED OR IMPLIED, IS GRANTED WITH THIS
PROGRAM.  Please see the COPYING file included with this program
and the GNU GPL for further details.

Logon to \\localhhost\IPC$ failed: error 53

C:\Users\user\Documents\4.2\LABS\Forencics\pwdump6-2.0.0-beta-exe-only>
```

```
C:\Users\user\Documents\4.2\LABS\Forencics\pwdump6-2.0.0-beta-exe-only>pwdump -x REDPAROLL-7THZONER

pwdump6 Version 2.0.0-beta-2 by fizzgig and the mighty group at foofus.net
** THIS IS A BETA VERSION! YOU HAVE BEEN WARNED. **
Copyright 2009 foofus.net

This program is free software under the GNU
General Public License Version 2 (GNU GPL), you can redistribute it and/or
modify it under the terms of the GNU GPL, as published by the Free Software
Foundation.  NO WARRANTY, EXPRESSED OR IMPLIED, IS GRANTED WITH THIS
PROGRAM.  Please see the COPYING file included with this program
and the GNU GPL for further details.

No history available

Administrator:500:NO PASSWORD*********************:2206E25E10C931F68AEF5EEE93689B76:::
cyber:1008:NO PASSWORD*********************:7F0B34DA909C8FE56CCB56A25F71A130:::
DefaultAccount:503:NO PASSWORD*********************:NO PASSWORD*********************:::
DevToolsUser:1004:NO PASSWORD*********************:03E8D5E4F609DAC621B4A9E78901AEA1:::
Guest:501:NO PASSWORD*********************:NO PASSWORD*********************:::
iteem:1007:NO PASSWORD*********************:506966598E6D6B3C6D205E43E6159D1C:::
sshd:1003:NO PASSWORD*********************:62DA02F3B22E94BF679852E30978877B:::
user:1001:NO PASSWORD*********************:66FBD27471FA9BC4137C190BFED0F82E:::
WDAGUtilityAccount:504:NO PASSWORD*********************:054CF628185E39527BBB3AEB34EAB501:::
Completed.
```

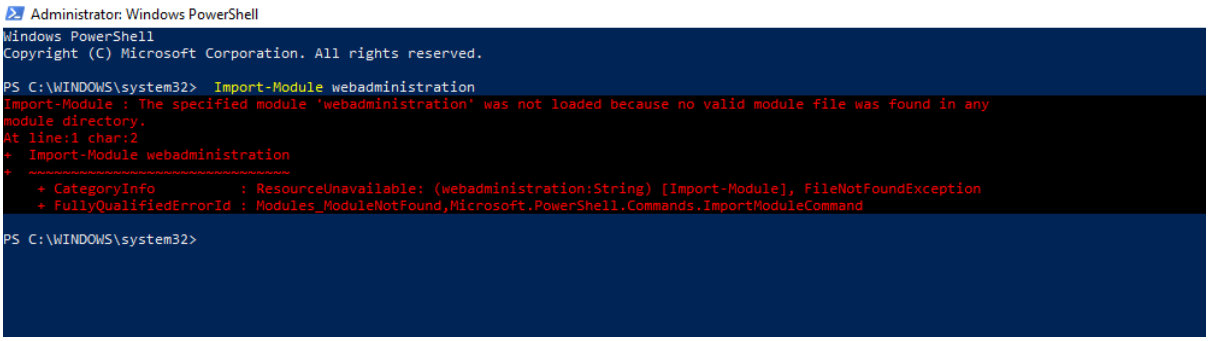
Task	Description	TOOLS
9	Registry Data	regdmp

✓ *COMMAND: regdmp.exe*



Task	Description	TOOLS
10	IIS	IIS, PowerShell

- ✓ *COMMAND: Get_ChildItem -path IIS: *



Task	Description	TOOLS
11	SUSPICIOUS FILES	procexp.exe

✓ *Command: procexp.exe*