



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*

Administrator: Command Prompt - nc 192.168.137.1 -v -l -p 12345

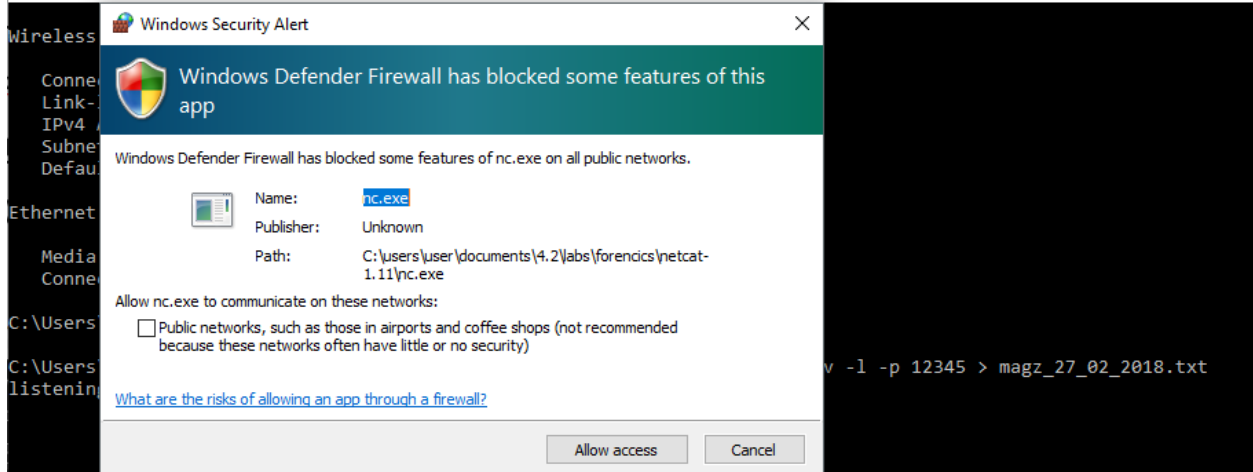
```
Wireless LAN adapter Local Area Connection* 4:

Connection-specific DNS Suffix  . : 
Link-local IPv6 Address . . . . . : fe80::1421:7b8f:ad2b:be24%16
IPv4 Address. . . . . : 192.168.137.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
```

✓ *Command: "nc 192.168.137.1 -v -l -p 12345 > magz\_27\_02\_2018.txt"*

C:\Users\user\Documents\4.2\LAB5\Forencics\netcat-1.11>nc 192.168.137.1 -v -l -p 12345 > magz\_27\_02\_2018.txt

Administrator: Command Prompt - nc 192.168.137.1 -v -l -p 12345

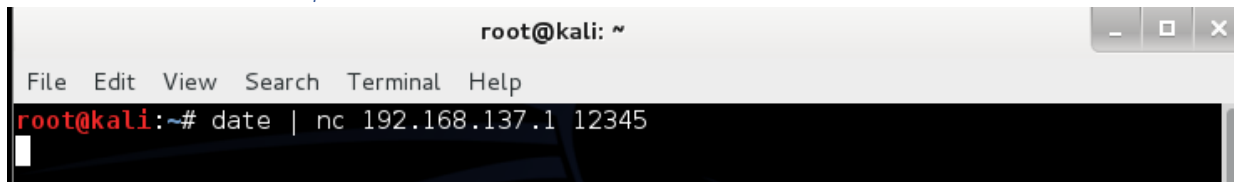


*Requires access and permissions*

```
C:\Users\user\Documents\4.2\LAB5\Forencics\netcat-1.11>nc 192.168.137.1 -v -l -p 12345 > magz_27_02_2018.txt
listening on [any] 12345 ...
connect to [192.168.137.1] from REDPAROLL-7THZONER.nssa.org.zw [192.168.137.1] 3070
```

b) Send victim machine date

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



## Result

magz\_27\_02\_2018.txt - Notepad

File Edit Format View Help

Tue Mar 20 02:58:48 UTC 2018

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	<u>The Auditing Policy</u>	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	<u>A History of Logins</u>	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	<u>System Event Logs</u>	PsLoglist

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

OUTPUT:

```
Administrator Command Prompt - psloglist -s -x security
443 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-t
ype configurations such as scheduled tasks, or when using the RUNAS command.
31595,Security,Microsoft-Windows-Security-Auditing,AUDIT SUCCESS,REDPAROLL-7THZONER.nssa.org.zw,06/03/2018 12:01:23 PM,4648,None,A logon was attempted using explicit cr
edentials. Subject: Security ID: S-1-5-21-2353939616-1809426805-2775209177-1001 Account Name: user Account Domain: REDPAROLL-7THZO Logon ID: 0x16bc7c L
ogon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: magayai@nssa.org.zw Account Domain: ? Logon GUID: {000
00000-0000-0000-0000-000000000000} Target Server: Target Server Name: Ndc-p-exchm-02.nssa.org.zw Additional Information: Ndc-p-exchm-02.nssa.org.zw Process In
formation: Process ID: 0x1490 Process Name: C:\Program Files\Microsoft Office\Office16\OUTLOOK.EXE Network Information: Network Address: 10.10.15.36 Port:
443 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-t
ype configurations such as scheduled tasks, or when using the RUNAS command.
31594,Security,Microsoft-Windows-Security-Auditing,AUDIT SUCCESS,REDPAROLL-7THZONER.nssa.org.zw,06/03/2018 12:01:22 PM,4648,None,A logon was attempted using explicit cr
edentials. Subject: Security ID: S-1-5-21-2353939616-1809426805-2775209177-1001 Account Name: user Account Domain: REDPAROLL-7THZO Logon ID: 0x16bc7c L
ogon GUID: {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: magayai@nssa.org.zw Account Domain: ? Logon GUID: {000
00000-0000-0000-0000-000000000000} Target Server: Target Server Name: Ndc-p-exchm-02.nssa.org.zw Additional Information: Ndc-p-exchm-02.nssa.org.zw Process In
formation: Process ID: 0x1490 Process Name: C:\Program Files\Microsoft Office\Office16\OUTLOOK.EXE Network Information: Network Address: 10.10.15.36 Port:
443 This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-t
ype configurations such as scheduled tasks, or when using the RUNAS command.
31593,Security,Microsoft-Windows-Security-Auditing,AUDIT SUCCESS,REDPAROLL-7THZONER.nssa.org.zw,06/03/2018 12:01:15 PM,4624,None,An account was successfully logged on.
Subject: Security ID: S-1-5-18 Account Name: REDPAROLL-7THZO$ Account Domain: NSSA Logon ID: 0x3e7 Logon Information: Logon Type: 5 Restricted Ad
min Mode: - Virtual Account: %1843 Elevated Token: %1842 Impersonation Level: %1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account
Domain: NT AUTHORITY Logon ID: 0x3e7 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-00000000
0000} Process Information: Process ID: 0x2f0 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: - Source Network Add
ress: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name.
(NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi
cate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or
Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indi
cate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workst
ation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session ca
n impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can b
e used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name i
ndicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was re
quested.
31592,Security,Microsoft-Windows-Security-Auditing,AUDIT SUCCESS,REDPAROLL-7THZONER.nssa.org.zw,06/03/2018 12:01:09 PM,4624,None,An account was successfully logged on.
Subject: Security ID: S-1-5-18 Account Name: REDPAROLL-7THZO$ Account Domain: NSSA Logon ID: 0x3e7 Logon Information: Logon Type: 5 Restricted Ad
min Mode: - Virtual Account: %1843 Elevated Token: %1842 Impersonation Level: %1833 New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account
Domain: NT AUTHORITY Logon ID: 0x3e7 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-00000000
0000} Process Information: Process ID: 0x2f0 Process Name: C:\Windows\System32\services.exe Network Information: Workstation Name: - Source Network Add
ress: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name.
(NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indi
cate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or
Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indi
cate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workst
ation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session ca
n impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can b
e used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name i
ndicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was re
quested.
```

Task	Description	TOOLS
6	<u>User Accounts</u>	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 fizzaig 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	<u>UnxUtils</u>	Find, UnxUtils

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

```

Administrator: Command Prompt

C:\>ZULU_IR
'ZULU_IR' is not recognized as an internal or external command,
operable program or batch file.

C:\>cd ZULU_IR
C:\ZULU_IR>cd unxutils-1.0\usr\local\wbin
C:\ZULU_IR\unxutils-1.0\usr\local\wbin>find UnxUtils
find: UnxUtils: No such file or directory

C:\ZULU_IR\unxutils-1.0\usr\local\wbin>find c:\ -printf "%m;%Ax;%AT;%Tx;%TT;%Cx;%CT;%U;%G;%s;%p\n"
777;01/01/00;;01/01/00;;01/01/00;;0;0;0;c:\
777;01/11/18;;01/11/18;;11/25/17;;0;0;0;c:\$GetCurrent
777;01/11/18;;01/11/18;;01/11/18;;0;0;0;c:\$GetCurrent\Logs
666;01/11/18;;01/11/18;;01/11/18;;0;0;41876;c:\$GetCurrent\Logs\downlevel_2018_01_11_18_15_39_290.log
666;01/11/18;;01/11/18;;01/11/18;;0;0;6336;c:\$GetCurrent\Logs\oobe_2018_01_11_21_41_58_997.log
666;01/11/18;;01/11/18;;01/11/18;;0;0;40;c:\$GetCurrent\Logs\PartnerSetupCompleteResult.log
777;01/11/18;;01/11/18;;01/11/18;;0;0;0;c:\$GetCurrent\SafeOS
666;01/11/18;;12/14/17;;01/11/18;;0;0;145872;c:\$GetCurrent\SafeOS\GetCurrent00BE.dll
666;01/11/18;;01/11/18;;01/11/18;;0;0;156;c:\$GetCurrent\SafeOS\GetCurrentRollback.ini
777;01/11/18;;01/11/18;;01/11/18;;0;0;577;c:\$GetCurrent\SafeOS\PartnerSetupComplete.cmd
777;01/11/18;;01/11/18;;01/11/18;;0;0;74;c:\$GetCurrent\SafeOS\preoobe.cmd
777;01/11/18;;01/11/18;;01/11/18;;0;0;307;c:\$GetCurrent\SafeOS\SetupComplete.cmd
777;11/08/17;;11/08/17;;07/10/15;;0;0;0;c:\$Recycle.Bin
777;11/08/17;;11/08/17;;11/08/17;;0;0;0;c:\$Recycle.Bin\S-1-5-18
666;11/08/17;;11/08/17;;11/08/17;;0;0;129;c:\$Recycle.Bin\S-1-5-18\desktop.ini
777;03/05/18;;03/05/18;;11/07/17;;0;0;0;c:\$Recycle.Bin\S-1-5-21-1448777116-3929398523-634744712-1001
666;02/03/18;;02/03/18;;02/03/18;;0;0;100;c:\$Recycle.Bin\S-1-5-21-1448777116-3929398523-634744712-1001\I01XL00.jpg
666;02/03/18;;02/03/18;;02/03/18;;0;0;110;c:\$Recycle.Bin\S-1-5-21-1448777116-3929398523-634744712-1001\I07YQ0M.jpg
666;02/03/18;;02/03/18;;02/03/18;;0;0;112;c:\$Recycle.Bin\S-1-5-21-1448777116-3929398523-634744712-1001\I01ZQVR.jpg
666;02/23/18;;02/23/18;;02/23/18;;0;0;150;c:\$Recycle.Bin\S-1-5-21-1448777116-3929398523-634744712-1001\I0WADWC.jpg
666;02/03/18;;02/03/18;;02/03/18;;0;0;104;c:\$Recycle.Bin\S-1-5-21-1448777116-3929398523-634744712-1001\I1D709V.jpg
666;02/03/18;;02/03/18;;02/03/18;;0;0;94;c:\$Recycle.Bin\S-1-5-21-1448777116-3929398523-634744712-1001\I122V00C.jpg
666;02/03/18;;02/03/18;;02/03/18;;0;0;104;c:\$Recycle.Bin\S-1-5-21-1448777116-3929398523-634744712-1001\I233L00.jpg
666;02/03/18;;02/03/18;;02/03/18;;0;0;104;c:\$Recycle.Bin\S-1-5-21-1448777116-3929398523-634744712-1001\I2AE041.jpg
666;02/03/18;;02/03/18;;02/03/18;;0;0;100;c:\$Recycle.Bin\S-1-5-21-1448777116-3929398523-634744712-1001\I23Y00M.jpg
666;02/03/18;;02/03/18;;02/03/18;;0;0;104;c:\$Recycle.Bin\S-1-5-21-1448777116-3929398523-634744712-1001\I30JA12.jpg
666;02/03/18;;02/03/18;;02/03/18;;0;0;106;c:\$Recycle.Bin\S-1-5-21-1448777116-3929398523-634744712-1001\I317V2Q.jpg
666;02/03/18;;02/03/18;;02/03/18;;0;0;104;c:\$Recycle.Bin\S-1-5-21-1448777116-3929398523-634744712-1001\I333G3Z.jpg
666;02/03/18;;02/03/18;;02/03/18;;0;0;106;c:\$Recycle.Bin\S-1-5-21-1448777116-3929398523-634744712-1001\I41R2LZ.jpg
666;02/03/18;;02/03/18;;02/03/18;;0;0;106;c:\$Recycle.Bin\S-1-5-21-1448777116-3929398523-634744712-1001\I40URXZ.jpg
666;02/03/18;;02/03/18;;02/03/18;;0;0;106;c:\$Recycle.Bin\S-1-5-21-1448777116-3929398523-634744712-1001\I518531.jpg
666;02/03/18;;02/03/18;;02/03/18;;0;0;106;c:\$Recycle.Bin\S-1-5-21-1448777116-3929398523-634744712-1001\I6566QL.jpg
666;02/03/18;;02/03/18;;02/03/18;;0;0;104;c:\$Recycle.Bin\S-1-5-21-1448777116-3929398523-634744712-1001\I72ZVUF.jpg

```

Task	Description	TOOLS
8	<u>User Accounts</u>	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	<u>Registry Data</u>	regdmp

✓ *COMMAND: regdmp.exe*

```

Administrator: Command Prompt
C:\ZULU_IR\unxutils-1.0>cd ..

C:\ZULU_IR>regdmp.exe
\Registry
Machine [17 1 8]
  BCD00000000
  Description
    KeyName = BCD00000000
    System = REG_DWORD 0x00000001
    TreatAsSystem = REG_DWORD 0x00000001
  Objects
    {0ce4091b-e6b3-4b16-b23c-5e8d9250e5d9}
      Description
      Type = REG_DWORD 0x20100000
      Elements
        16000020
          Element = REG_BINARY 0x00000001 0x00000000
      {1afa9c49-16ab-4a5c-901b-212002da9460}
        Description
        Type = REG_DWORD 0x20200004
        Elements
          14000006
            Element = REG_MULTI_SZ "{7ea2e1ac-2e61-4720-aaa3-896d9d0a9f0e}"
      {4636856e-540f-4170-a130-a04776f4c654}
        Description
        Type = REG_DWORD 0x20100000
        Elements
          15000011
            Element = REG_BINARY 0x00000000 0x00000004 0x00000000
      {5189b25c-5558-4bf2-bca4-289b11bd29e2}
        Description
        Type = REG_DWORD 0x20100000
        Elements
          {6efb52bf-1766-41db-a6b3-0ee5eff72bd7}
            Description
            Type = REG_DWORD 0x20200003
            Elements
              14000006
                Element = REG_MULTI_SZ "{7ea2e1ac-2e61-4720-aaa3-896d9d0a9f0e}" \
                  "{7ff607e0-4395-11db-b8de-000200c9a66}"
      {7ea2e1ac-2e61-4720-aaa3-896d9d0a9f0e}
        Description
        Type = REG_DWORD 0x20100000
        Elements
          14000006
            Element = REG_MULTI_SZ "{4636856e-540f-4170-a130-a04776f4c654}" \

```

Task	Description	TOOLS
10	<u>IIS</u>	IIS, PowerShell

✓ *COMMAND: Get\_ChildItem -path IIS: \*

Administrator: Windows PowerShell

Windows PowerShell

Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\WINDOWS\system32> Import-Module webadministration

Import-Module : The specified module 'webadministration' was not loaded because no valid module file was found in any module directory.

At line:1 char:2

+ Import-Module webadministration

+

+ CategoryInfo : ResourceUnavailable: (webadministration:String) [Import-Module], FileNotFoundException

+ FullyQualifiedErrorId : Modules\_ModuleNotFound,Microsoft.PowerShell.Commands.ImportModuleCommand

PS C:\WINDOWS\system32>

Task	Description	TOOLS
11	<u>SUSPICIOUS FILES</u>	procexp.exe

✓ Command: *procexp.exe*

Process Explorer - Sysinternals: www.sysinternals.com [REDPAROLL-7THZO\user]

File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		1,268 K	21,180 K	96		
System Idle Process	0.50	52 K	9 K	0		
System	17.66	220 K	15,740 K	4		
smss.exe	2.14	0 K	0 K	n/a	Hardware Interrupts and DPCs	
Memory Compression	0.15	3,056 K	983,144 K	2684	428 Windows Session Manager	Microsoft Corporation
csrss.exe	0.01	1,864 K	5,412 K	592	Client Server Runtime Process	Microsoft Corporation
wininit.exe		1,312 K	5,672 K	684	Windows Start-Up Application	Microsoft Corporation
services.exe		8,084 K	15,788 K	760	Services and Controller app	Microsoft Corporation
svchost.exe		1,048 K	3,804 K	900	Host Process for Windows S...	Microsoft Corporation
svchost.exe		23,016 K	40,224 K	924	Host Process for Windows S...	Microsoft Corporation
unsecapp.exe		1,828 K	7,272 K	8264	Sink to receive asynchronou...	Microsoft Corporation
WmiPrvSE.exe	15.69	42,996 K	57,420 K	3040	WMI Provider Host	Microsoft Corporation
WmiPrvSE.exe		5,292 K	12,572 K	7584	WMI Provider Host	Microsoft Corporation
WmiPrvSE.exe		3,416 K	9,344 K	12212	WMI Provider Host	Microsoft Corporation
WmiPrvSE.exe		6,012 K	15,724 K	12932	WMI Provider Host	Microsoft Corporation
WmiPrvSE.exe		19,624 K	32,848 K	5588	WMI Provider Host	Microsoft Corporation
unsecapp.exe		1,448 K	7,004 K	12636	Sink to receive asynchronou...	Microsoft Corporation
ShellExperienceHost.exe	Susp...	121,348 K	92,060 K	5980	Windows Shell Experience H...	Microsoft Corporation
SearchUI.exe	Susp...	144,908 K	114,324 K	14492	Search and Cortana applicat...	Microsoft Corporation
RuntimeBroker.exe		12,512 K	39,168 K	11008	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		13,568 K	43,600 K	14440	Runtime Broker	Microsoft Corporation
SpeechRuntime.exe	< 0.01	16,456 K	22,972 K	13484	Speech Runtime Executable	Microsoft Corporation
ApplicationFrameHost.exe		13,992 K	33,124 K	3020	Application Frame Host	Microsoft Corporation
CastSrv.exe		6,536 K	11,892 K	7944	Castling protocol connection L...	Microsoft Corporation
ilhost.exe		6,120 K	14,400 K	5768	COM Sumogate	Microsoft Corporation
SettingSyncHost.exe		25,024 K	6,360 K	3292	Host Process for Setting Syn...	Microsoft Corporation
SkypeHost.exe	Susp...	40,528 K	22,280 K	7648	Microsoft Skype	Microsoft Corporation
RuntimeBroker.exe		4,820 K	11,480 K	11936	Runtime Broker	Microsoft Corporation
LockApp.exe	Susp...	17,872 K	44,564 K	992	LockApp.exe	Microsoft Corporation
RuntimeBroker.exe		8,884 K	32,832 K	16304	Runtime Broker	Microsoft Corporation
SystemSettingsBroker.exe		13,036 K	37,640 K	18288	System Settings Broker	Microsoft Corporation
RuntimeBroker.exe		2,520 K	11,032 K	13176	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		10,740 K	38,424 K	16332	Runtime Broker	Microsoft Corporation
SystemPropertiesA...		2,872 K	12,396 K	13744	Advanced System Settings	Microsoft Corporation
RemindersServer.exe	Susp...	7,824 K	19,588 K	1668	Reminders WinRT OOP Ser...	Microsoft Corporation
ilhost.exe		1,588 K	6,068 K	16064	COM Sumogate	Microsoft Corporation
ilhost.exe		19,308 K	26,900 K	16316	COM Sumogate	Microsoft Corporation
FileCoAuth.exe		3,688 K	12,360 K	584	Microsoft OneDriveFile Co-A...	Microsoft Corporation
RuntimeBroker.exe		21,068 K	37,956 K	21280	Runtime Broker	Microsoft Corporation