**Volatility:**

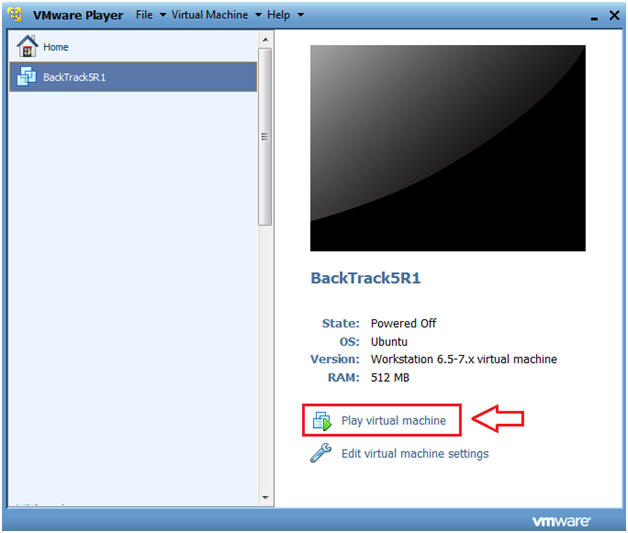
**Analyzing A Metasploit Memory Capture from Windows XP SP2**

**Section 0. Background Information**

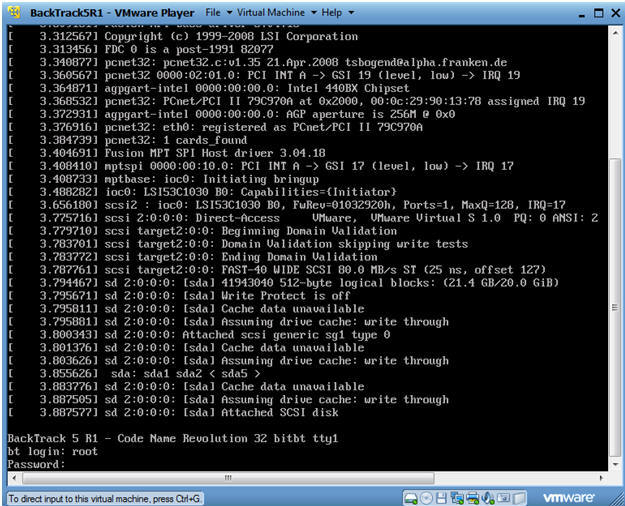
* Volatility Overview
  + <https://www.volatilesystems.com/>
  + The Volatility Framework is a completely open collection of tools, implemented in Python under the GNU General Public License, for the extraction of digital artifacts from volatile memory (RAM) samples. The extraction techniques are performed completely independent of the system being investigated but offer unprecedented visibility into the runtime state of the system. The framework is intended to introduce people to the techniques and complexities associated with extracting digital artifacts from volatile memory samples and provide a platform for further work into this exciting area of research.
* Prerequisite Labs
  + Install Volatility Framework 2.0 on BackTrack5 Lab
  + Window's Physical Memory During Metasploit Session

**Section 1. Login to BackTrack**

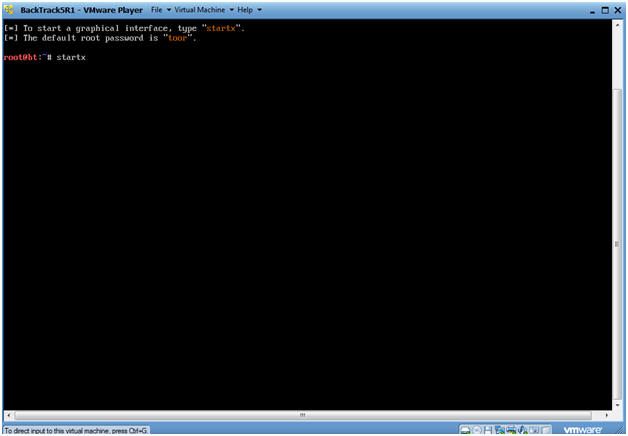
1. Start BackTrack VM Instance
   * **Instructions:**
     1. Start Up VMWare Player
     2. Select BackTrack5R1
     3. Play virtual machine



1. Login to BackTrack
   * **Instructions:**
     1. Login: root
     2. Password: toor or <whatever you changed it to>.

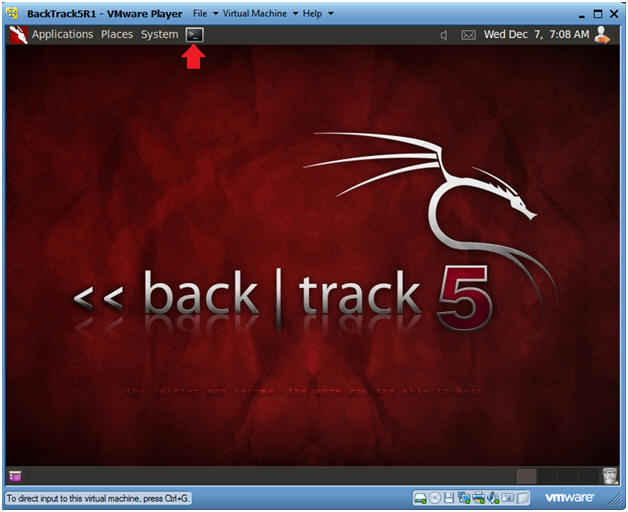


1. Bring up the GNOME
   * Instructions
     1. Type startx



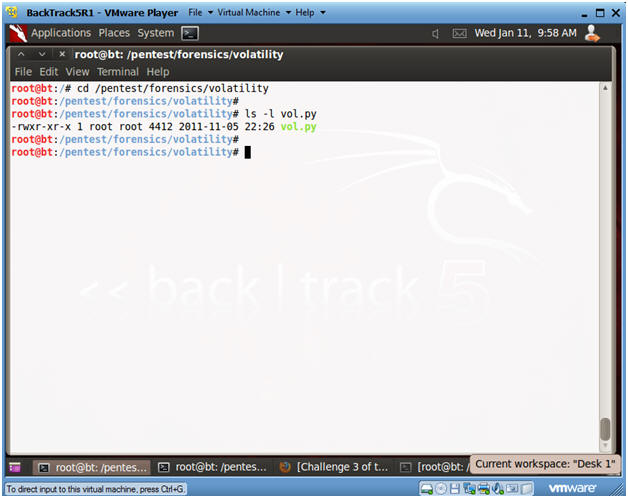
**Section 2. Bring up a console terminal**

1. Bring up a console terminal



**Section 3. Using Volatility**

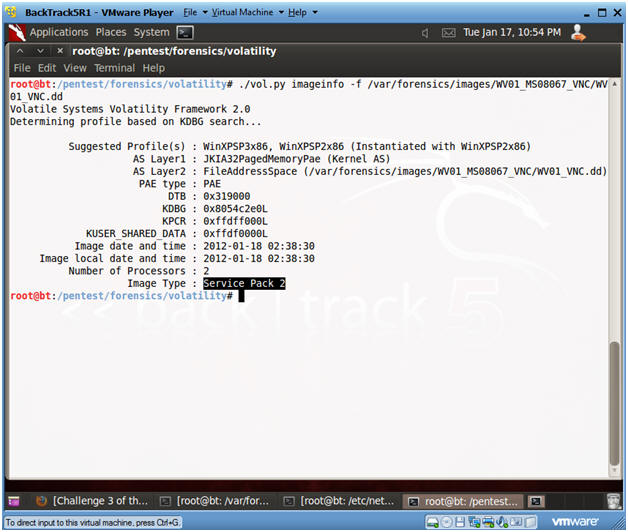
1. Navigate to Volatility
   * **Instructions**
     1. cd /pentest/forensics/volatility
     2. ls -l vol.py



1. Obtain the image profile
   * **Instructions**

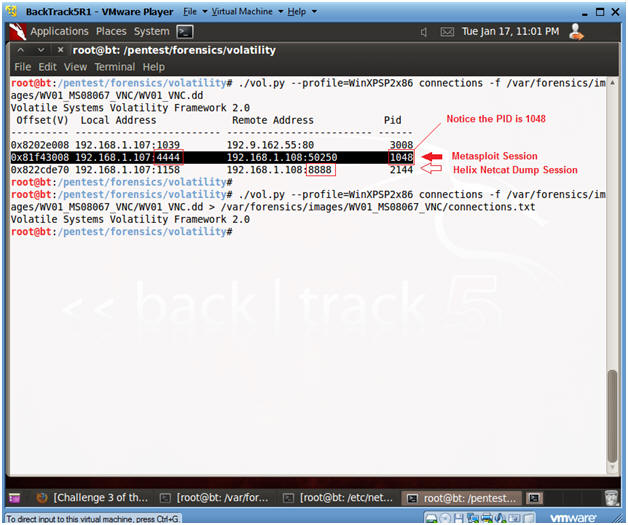
**:**

* + 1. ./vol.py **imageinfo** -f /var/forensics/images/WV01\_MS08067\_VNC/WV01\_VNC.dd
  + **Notes:**
    1. The Volatility Framework tries to guess and tell you what image profile to use.
    2. We know that our Server is Windows XP running SP2.
    3. Volatility suggest that we either use the profile WinXPSP3x86 or WinXPSP2x86.
    4. We will use the **WinXPSP2x86** profile.



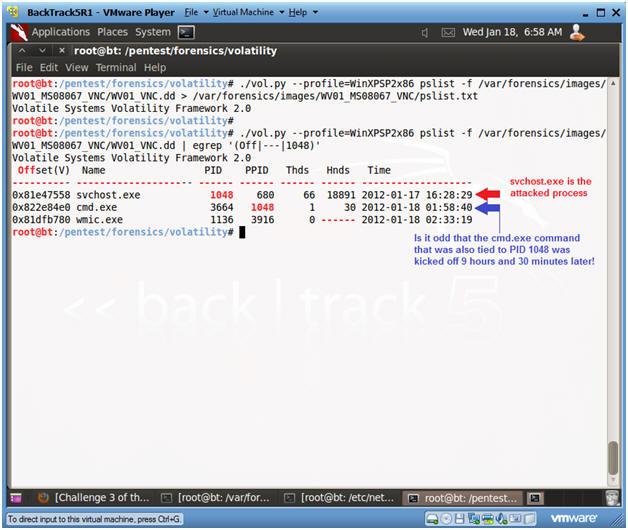
1. View Open Connections
   * **Instructions**
     1. ./vol.py --profile=WinXPSP2x86 **connections** -f /var/forensics/images/WV01\_MS08067\_VNC/WV01\_VNC.dd
        + This command just displays output on the screen.

* + 1. ./vol.py --profile=WinXPSP2x86 **connections** -f /var/forensics/images/WV01\_MS08067\_VNC/WV01\_VNC.dd > /var/forensics/images/WV01\_MS08067\_VNC/connections.txt
       - This command saves the output to a file called connections.txt
  + **Notes:**
    1. The Metasploit Session has a process ID of 1048 and is connected to port 4444 on the Victim's machine.
    2. The last line is the Helix Netcat Dump, which is connected to port 8888 on the BackTrack machine.
    3. **Record the PID of the Metasploit session for the next steps**.  In my case it is 1048.  In your case, it will be different.
    4. This displays all the running process during the time we captured the image in [Helix Lesson 5](http://www.computersecuritystudent.com/FORENSICS/HELIX/lesson5/index.html).



1. Searching for Specific Processes
   * **Instructions:**
     1. ./vol.py --profile=WinXPSP2x86 **pslist** -f /var/forensics/images/WV01\_MS08067\_VNC/WV01\_VNC.dd > /var/forensics/images/WV01\_MS08067\_VNC/pslist.txt
        + This command saves the process list to a file.

* + 1. ./vol.py --profile=WinXPSP2x86 **pslist** -f /var/forensics/images/WV01\_MS08067\_VNC/WV01\_VNC.dd | egrep '(Off|---|**1048**)'
       - This command will show the column header line along with the PID 1048.
       - Remember 1048 was the PID associated with the Metasploit Session attached to port 4444.  It will probably be different in your case.
       - The svchost.exe process was attacked at 16:28 on 1-17-2012.



1. View Socket Connections
   * **Instructions**

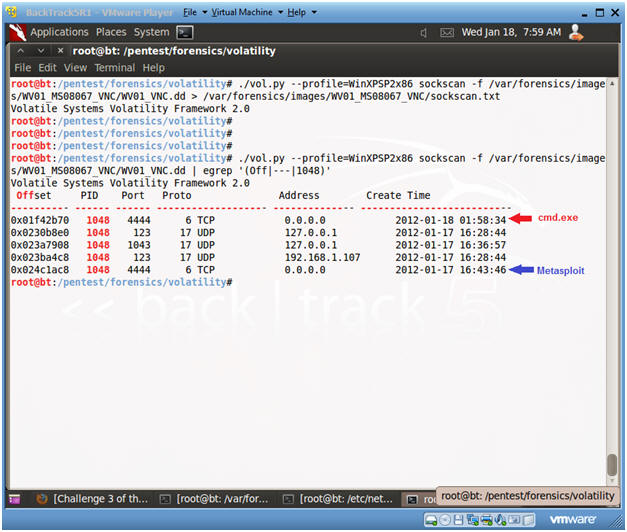
**:**

* + 1. ./vol.py --profile=WinXPSP2x86 **sockscan** -f /var/forensics/images/WV01\_MS08067\_VNC/WV01\_VNC.dd > /var/forensics/images/WV01\_MS08067\_VNC/sockscan.txt
       - This command lets you view **all open** Socket Connections.

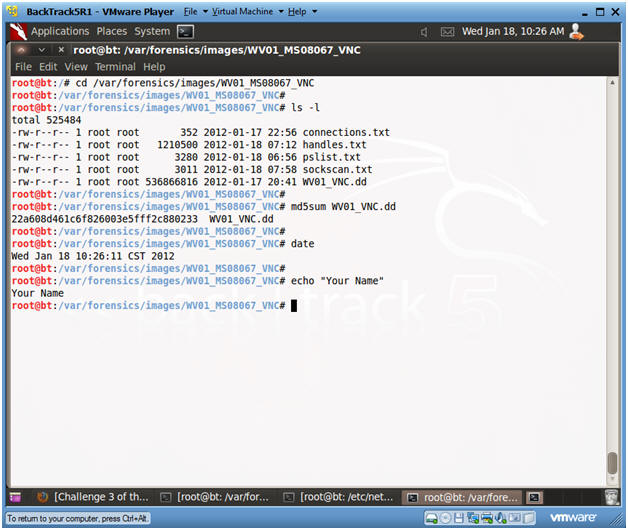
* + 1. ./vol.py --profile=WinXPSP2x86 **sockscan** -f /var/forensics/images/WV01\_MS08067\_VNC/WV01\_VNC.dd | egrep '(Off|---|**1048**)'
       - **Note:** This command lets you search for all processes associated with PID 1048.
  + **Note**

**:**

* + 1. In summary, we can say with confidence that Metasploit exploited PID 1048 (svchost.exe) at 16:43 on 1-17-2012 and connected to the Victim using port 4444.
    2. With less confidence, it is difficult to establish when cmd.exe (Metasploit Courtesy Command Prompt) was executed over port 4444, since the creation time is 9 hours and 30+ minutes after the svchost.exe attack. The vnc payload immediately executes a command prompt, so the creation time should be very close to the svchost.exe time.
    3. The previous point could be a credibility problem in court.  I will work on some deeper forensics to show how this time was modified.



1. **Proof of Lab**
   * **Instructions:**
     1. cd /var/forensics/images/WV01\_MS08067\_VNC
     2. ls -l
     3. md5sum WV01\_VNC.dd
        + As a Forensics investigator, it is always necessary to verify that the image has not changed during the investigation.
     4. date
     5. echo "Your Name"
        + Replace the string "Your Name" with your actual name.
        + E.g., echo "John Gray"



**Section 4. Proof of Lab**

1. Proof of Lab
   * **Proof Of Lab Instructions:**
     1. Do Section 3, Step 6.
     2. Do a PrtScn of the below commands
     3. Paste into a word document
     4. Upload to Moodle