SANS Sift Workstation

Download: https://www.sans.org/tools/sift-workstation/ login/pass: sansforensics/forensics

Mods

VMWare crap

Reinstalling VMware tools to enable sharing was brutal.
→
https://communities.vmware.com/t5/VMware-Fusion-Discussions/Update-VMware-tools-greyed-out-in-Fusion-12/td-p/2809208
copy the linux.iso from the installation software location to a place where you can mount it as cdrom image from the VMWare.
Then copy the content of the VMWare Tools folder to /tmp

```
tar xvzf VMwareTools-10.3.23-16594550.tar.gz
cd vmware-tools-distrib/
./vmware-install.pl
reboot
sudo vmhgfs-fuse .host:/Share /mnt/windows_mount -o allow_other -o uid=1000
```

Share is the name of my shared folder

Yara rules

yara rules can be found on git : https://github.com/Yara-Rules/rules

```
sudo su
cd /opt
mkdir yara
cd yara
git clone https://github.com/Yara-Rules/rules.git
chown -Rh sansforensics /opt/yara
```

Fix volatility-yara

→ https://github.com/teamdfir/sift/issues/389

- edit /usr/local/lib/python2.7/dist-packages/volatility/plugins/malware/malfind.py

```
185     def __init__(self, config, *args, **kwargs):
186         taskmods.DllList.__init__(self, config, *args, **kwargs)
187         config.add_option("ALL", short_option = 'A', default = False,
action = 'store_true',
188                           help = 'Scan both process and kernel memory')
189         config.add_option("CASE", short_option = 'c', default = False,
action = 'store_true',
190                           help = 'Make the search case insensitive')
191         config.add_option("KERNEL", short_option = 'K', default = False,
action = 'store_true',
192                           help = 'Scan kernel modules')
193         config.add_option("WIDE", short_option = 'W', default = False,
action = 'store_true',
194                           help = 'Match wide (unicode) strings')
195         config.add_option('YARA-RULES', short_option = 'U', default =
None,
196                           help = 'Yara rules (as a string)')
```

Change line 189 short_option = 'C' for 'c' and line 195 short_option = 'Y' for 'U'

If you don't do that:

```
$ vol.py -f black_energy.vmem --profile=WinXPSP2x86 yarascan -h
Volatility Foundation Volatility Framework 2.6.1
Traceback (most recent call last):
  File "/usr/local/bin/vol.py", line 192, in <module>
    main()
  File "/usr/local/bin/vol.py", line 174, in main
    command = cmds[module](config)
  File "/usr/local/lib/python2.7/dist-
packages/volatility/plugins/malware/malfind.py", line 190, in __init__
    help = 'Make the search case insensitive')
  File "/usr/local/lib/python2.7/dist-packages/volatility/conf.py", line
363, in add_option
    self.optparser.add_option("-{0}".format(short_option), "--
{0}".format(option), **args)
  File "/usr/lib/python2.7/optparse.py", line 1021, in add_option
    self._check_conflict(option)
  File "/usr/lib/python2.7/optparse.py", line 996, in _check_conflict
    option)
optparse.OptionConflictError: option -C/--case: conflicting option
string(s): -C
```

yara rules fix

Some malware rules are broken

- /opt/yara/rules/malware_index.yar line 104

```
//include "./malware/MALW_AZORULT.yar"
```

From:
https://wiki.fortier-family.com/ - **Warnaud's Wiki**

Permanent link:
https://wiki.fortier-family.com/os/kali/sansdift

Last update: **2021/12/29 21:03**