XenServer_monitor

共包括 7 个文件：

conf.py: 用于配置主机 url, username 和 password.

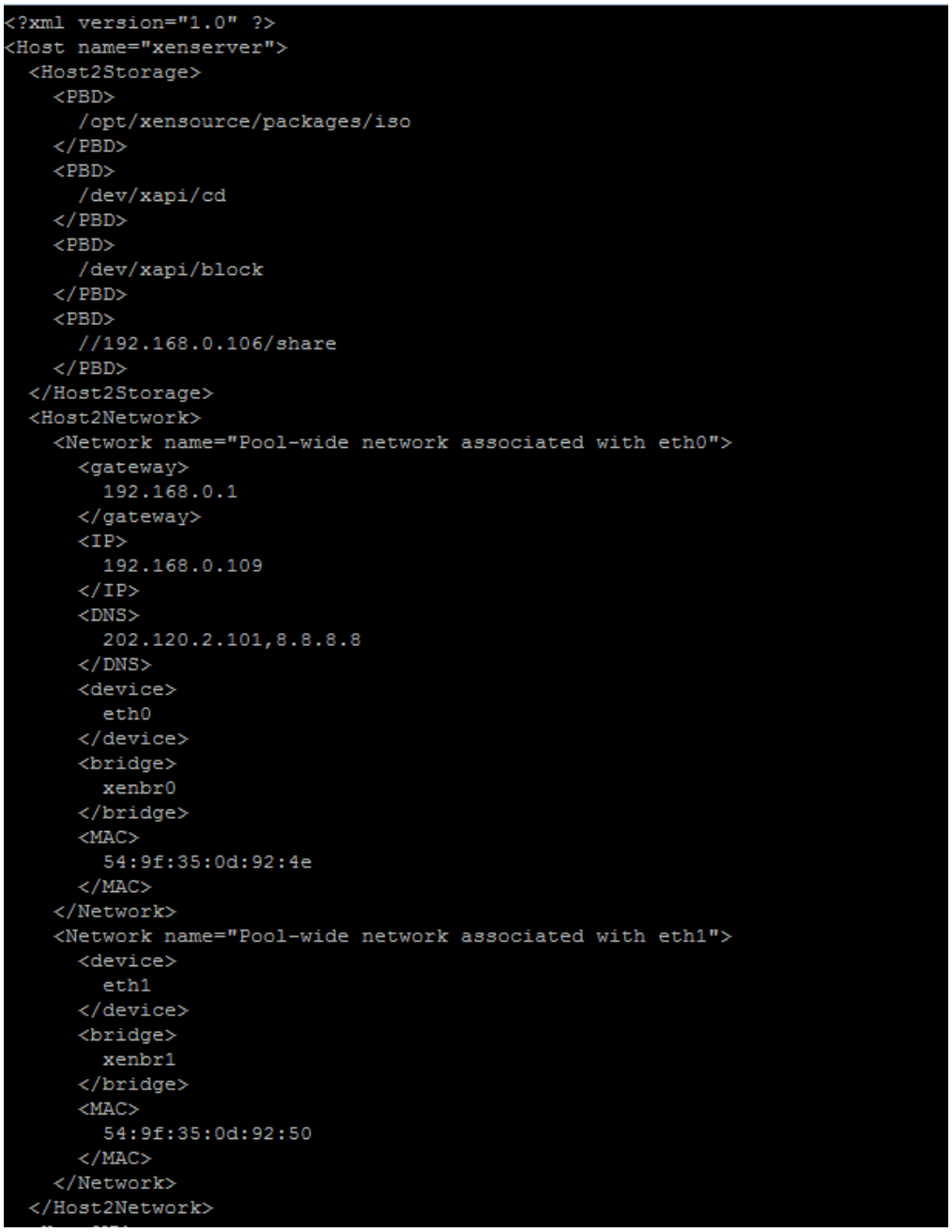
provision.py XenApi.py: XenServer Python SDK.

myutils.py srutils.py : 两个自定义辅助工具

host1.py host2.py : 以 xml 形式输出 host 信息，host1 比 host2 输出更详细。

sr.py : 以 xml 形式输出 sr 信息。

host1(2).py 不支持参数，输出 host 上所有网络、存储和虚拟机信息。



```
<?xml version="1.0" ?>
<Host name="xenserver">
  <Host2Storage>
    <PBD>
      /opt/xensource/packages/iso
    </PBD>
    <PBD>
      /dev/xapi/cd
    </PBD>
    <PBD>
      /dev/xapi/block
    </PBD>
    <PBD>
      //192.168.0.106/share
    </PBD>
  </Host2Storage>
  <Host2Network>
    <Network name="Pool-wide network associated with eth0">
      <gateway>
        192.168.0.1
      </gateway>
      <IP>
        192.168.0.109
      </IP>
      <DNS>
        202.120.2.101,8.8.8.8
      </DNS>
      <device>
        eth0
      </device>
      <bridge>
        xenbr0
      </bridge>
      <MAC>
        54:9f:35:0d:92:4e
      </MAC>
    </Network>
    <Network name="Pool-wide network associated with eth1">
      <device>
        eth1
      </device>
      <bridge>
        xenbr1
      </bridge>
      <MAC>
        54:9f:35:0d:92:50
      </MAC>
    </Network>
  </Host2Network>
```

sr.py 不支持参数，输出 host 上所有 sr。

```
<?xml version="1.0" ?>
<SRs>
  <SR name="Local storage">
    <PBDs>
      <PBD>
        <device_config/>
      </PBD>
    </PBDs>
    <VDIs>
      <VDI name="Ubuntu 0">
        <location>
          75317c70-6360-449c-9431-5941dcb00c27
        </location>
      </VDI>
      <VDI name="Windows7 0">
        <location>
          a05f0372-f1a3-4392-ab6a-8a4d7d0690bf
        </location>
      </VDI>
    </VDIs>
    <physical_size>
      290837233664
    </physical_size>
    <type>
      lvm
    </type>
  </SR>
  <SR name="XenServer Tools">
    <PBDs>
      <PBD>
        <device_config>
          <location>
            /opt/xensource/packages/iso
          </location>
        </device_config>
      </PBD>
    </PBDs>
    <VDIs>
      <VDI name="XenCenter.iso">
        <location>
          XenCenter.iso
        </location>
      </VDI>
      <VDI name="xs-tools.iso">
        <location>
          xs-tools-6.5.0.iso
        </location>
      </VDI>
    </VDIs>
```

Xen_mount

mount.sh domain-img mount-dir: 挂载虚拟机文件系统
umount.sh domain-img mount-dir: 卸载虚拟机文件系统

```
dom@moster:~/xen_config$ sudo ./mount.sh windows.img /mnt
add map loop0p1 (252:2): 0 204800 linear /dev/loop0 2048
add map loop0p2 (252:3): 0 41734144 linear /dev/loop0 206848
dom@moster:~/xen_config$ cd /mnt/2
dom@moster:/mnt/2$ sudo echo "hello from linux " >linux.txt
dom@moster:/mnt/2$ ls
data.txt              hiberfil.sys  pagefile.sys  ProgramData     Program Files (x86)  $Recycle.Bin                Users
Documents and Settings  linux.txt     PerfLogs      Program Files   Recovery             System Volume Information   Windows
dom@moster:/mnt/2$ cd -
/home/dom/xen_config
dom@moster:~/xen_config$ sudo ./umount.sh windows.img /mnt
del devmap : loop0p2
del devmap : loop0p1
loop deleted : /dev/loop0
dom@moster:~/xen_config$
```

Injector

依赖关系：首先安装 Xen、libvmi、rekall 和 drakvuf 等软件。

process-list domain-name: 列出虚拟机上的所有进程。
injector recall-file domain-id process-id command: 在 domain-id 虚拟机中以 process-id 为父进程，以 command 为可执行文件创建一个新进程，以此实现进程注入。

```
dom@moster:~/drakvuf/drakvuf/libvmi/examples$ sudo ./process-list windows
LibVMI Suggestion: set win_ntoskrnl=0x3c00000 in libvmi.conf for faster startup.
LibVMI Suggestion: set win_kdbg=0x1f10a0 in libvmi.conf for faster startup.
LibVMI Suggestion: set win_kdvb=0xfffff80003df10a0 in libvmi.conf for faster sta
rtup.
Process listing for VM windows (id=5)
[    4] System (struct addr:fffffa800236c990)
[  220] smss.exe (struct addr:fffffa8003472b30)
[  296] csrss.exe (struct addr:fffffa8003c32920)
[  344] csrss.exe (struct addr:fffffa80023da060)
[  352] wininit.exe (struct addr:fffffa80023e39e0)
[  384] winlogon.exe (struct addr:fffffa8003d83b30)
[  444] services.exe (struct addr:fffffa8003db2060)
[  456] lsass.exe (struct addr:fffffa8003393b30)
[  464] lsm.exe (struct addr:fffffa8003c9cb30)
[  572] svchost.exe (struct addr:fffffa800338cb30)
[  636] svchost.exe (struct addr:fffffa8003e4cb30)
[  744] svchost.exe (struct addr:fffffa8003eb08a0)
[  792] svchost.exe (struct addr:fffffa8003ed19e0)
[  820] svchost.exe (struct addr:fffffa8003efc530)
[  880] audiodg.exe (struct addr:fffffa8003f16b30)
[ 1004] svchost.exe (struct addr:fffffa8003f75b30)
[  432] svchost.exe (struct addr:fffffa8003fb1b30)
[ 1064] spoolsv.exe (struct addr:fffffa8004015060)
[ 1100] svchost.exe (struct addr:fffffa800404fb30)
[ 1164] taskhost.exe (struct addr:fffffa80034b4060)
[ 1272] dwm.exe (struct addr:fffffa80040e11b0)
[ 1288] explorer.exe (struct addr:fffffa80040e6b30)
[ 1440] svchost.exe (struct addr:fffffa800419c360)
[ 2008] SearchIndexer. (struct addr:fffffa8003f5c260)
[ 1540] SearchProtocol (struct addr:fffffa8004344b30)
[ 1620] SearchFilterHo (struct addr:fffffa8004196b30)
```

```
dom@moster:~/drakvuf/drakvuf/src$ sudo ./injector ~/windows.rekall.json 5 1288 "
cmd.exe"
Init VMI on domID 5 -> windows
Rekall profile: '_KPCR' has no 'PrcbData' member
Failed to find offset for _KPCR:PrcbData
Reservation increased? 0 with new gfn: 0x8040
Xen altp2m view created with idx: 1 idr: 2
Windows kernel base address is 0xfffff80003c00000
libdrakvuf initialized
Injector starting cmd.exe through PID 1288 TID: 0
Target PID 1288 with DTB 0x39897000 to start 'cmd.exe'
```

```
dom@moster:~/drakvuf/drakvuf/libvmi/examples$ sudo ./process-list windows
LibVMI Suggestion: set win_ntoskrnl=0x3c00000 in libvmi.conf for faster startup.
LibVMI Suggestion: set win_kdbg=0x1f10a0 in libvmi.conf for faster startup.
LibVMI Suggestion: set win_kdvb=0xfffff80003df10a0 in libvmi.conf for faster startup.
Process listing for VM windows (id=5)
[    4] System (struct addr:fffffa800236c990)
[  220] smss.exe (struct addr:fffffa8003472b30)
[  296] csrss.exe (struct addr:fffffa8003c32920)
[  344] csrss.exe (struct addr:fffffa80023da060)
[  352] wininit.exe (struct addr:fffffa80023e39e0)
[  384] winlogon.exe (struct addr:fffffa8003d83b30)
[  444] services.exe (struct addr:fffffa8003db2060)
[  456] lsass.exe (struct addr:fffffa8003393b30)
[  464] lsm.exe (struct addr:fffffa8003c9cb30)
[  572] svchost.exe (struct addr:fffffa800338cb30)
[  636] svchost.exe (struct addr:fffffa8003e4cb30)
[  744] svchost.exe (struct addr:fffffa8003eb08a0)
[  792] svchost.exe (struct addr:fffffa8003ed19e0)
[  820] svchost.exe (struct addr:fffffa8003efc530)
[  880] audiodg.exe (struct addr:fffffa8003f16b30)
[ 1004] svchost.exe (struct addr:fffffa8003f75b30)
[  432] svchost.exe (struct addr:fffffa8003fb1b30)
[ 1064] spoolsv.exe (struct addr:fffffa8004015060)
[ 1100] svchost.exe (struct addr:fffffa800404fb30)
[ 1164] taskhost.exe (struct addr:fffffa80034b4060)
[ 1272] dwm.exe (struct addr:fffffa80040e11b0)
[ 1288] explorer.exe (struct addr:fffffa80040e6b30)
[ 1440] svchost.exe (struct addr:fffffa800419c360)
[ 2008] SearchIndexer. (struct addr:fffffa8003f5c260)
[ 1160] cmd.exe (struct addr:fffffa8004344b30)
[ 1208] conhost.exe (struct addr:fffffa80040d5400)
[ 1904] svchost.exe (struct addr:fffffa8004046060)
[  808] explorer.exe (struct addr:fffffa8003d92b30)
```