Forensics in Qubes OS

version-r41, security

taradiddles 1 June 2, 2023, 6:04am

Sometimes it may be necessary to forensically investigate a Qubes OS VM. This guide describes how this can be accomplished. It is intended for advanced users.

For forensics of Qubes OS `dom0` please refer to any standard Linux forensics guide.

Disk Forensics

You can **mount disks of all VMs to another investigation VM** in both r/w and r/o fashion and use your favorite forensic analysis tools.

Users of non-LVM **storage pools** may refer to **this code**.

Memory Forensics

The following guide uses **volatility3** for memory forensics on a previously created memory dump. Other tools may work as well.

The VM under analysis is called `vm`. The VM where the memory dump is analyzed is called `analysis-vm`.

(dom0) Use template VM kernels

Since Qubes OS currently does **not provide kernel debug symbols** for its default kernels, you will have to switch to VM template kernels at least for the VM under analysis *and* the analysis VM. Without this step, the analysis tool (here **volatility3**) will be unable to interpret the memory dump.

Please follow **the official guide on how to use a kernel installed inside a VM**. The required package for `pvh` VMs is called `grub2-xen-pvh`.

(dom0) Pause the VM under analysis

```
qvm-pause vm
```

You can later unpause it via `qvm-unpause vm`. Skipping this step may cause memory smear and render the memory dump useless.

(dom0) Dump the memory

```
virsh -c xen:// dump vm vm.dump --live
sudo chown [user]:[user] vm.dump
```

(dom0) Create the analysis-vm

```
qvm-clone --class StandaloneVM debian-11 analysis-vm
qvm-prefs analysis-vm label red
qvm-prefs analysis-vm netvm sys-firewall
qubes-vm-settings analysis-vm (make sure you have at least 7 GB free system storage
qvm-copy-to-vm analysis-vm vm.dump
```

(analysis-vm) Install volatility3

Follow the install instructions inside the `REAMDE.md`.

As of 2023 the volatility3 support for Xen memory dumps is limited. Your mileage may vary.

(analysis-vm) Create a volatility binary for convenience

```
sudo su
echo '#!/bin/bash'$'\n''python3 "[path to vol.py]/vol.py" "$@"' > /usr/bin/volatili
chmod +x /usr/bin/volatility
exit
```

(analysis-vm) Build and install dwarf2json

You may have to install golang first (debian: `sudo apt install golang`).

```
cd ~
git clone 'https://github.com/volatilityfoundation/dwarf2json'
cd dwarf2json
go build
```

(analysis-vm) Generate the symbol tables for volatility3

On debian use `sudo apt install linux-image-amd64-dbg` to install the version matching the kernel version of the VM under analysis.

Afterwards generate the symbol table lookups for volatility3 via `dwarf2json`:

```
./dwarf2json linux --elf /usr/lib/debug/boot/vmlinux-[kernel version]-amd64 --syste
```

(analysis-vm) Analyze the memory dump

```
cd ~
mv ~/QubesIncoming/dom0/vm.dump ~
volatility isfinfo (should show the symbol file)
volatility -f vm.dump banner
volatility -f vm.dump linux.pslist
```

▼ This document was migrated from the qubes-community project

- Page archive
- First commit: 13 Jan 2023. Last commit: 13 Jan 2023.
- Applicable Qubes OS releases based on commit dates and supported releases: 4.1
- Original author(s) (GitHub usernames): 3hhh
- Original author(s) (forum usernames): N/A
- Document license: CC BY 4.0

1 Like

Kernel with debugging symbols