8
Installing Qubes OS

Qubes OS, a Xen-based operating system, which is also considered extremely secure, will be the focus of this chapter.

Qubes OS operates under the assumption that it has already been breached, so every application is run in its own virtual environment.

In this chapter, we will learn how to install and use Qubes OS for accessing the Deep Web

- What is Qubes OS?
- How to install Qubes OS
- Accessing the Dark Web with Qubes

What is Qubes OS?

Qubes OS is another security, privacy, and anonymity-focused operating system. The developers designed it with the belief that, currently, there's no tool or software that can completely protect us from **zero-day attacks** (attacks that exploit software vulnerabilities, which have, so far, not been discovered by the software vendor, and hence they have no patches or fixes yet, and can be exploited by hackers) and sophisticated hackers, who use tools and attacks that can bypass most, if not all, of an organization's defenses, be it firewall, antivirus, or another tool.

So, they came up with a great idea: compartmentalization, separating what we do on the computer into securely isolated compartments, which the developers named **qubes**.

Applications' hardware and sessions can be separated into their own secure qube, providing strict separation from the other qubes, and, this way, if the user surfs to a compromised website, and the user's browser is infected by malware, no other part of the user's computer or applications will be affected (effectively preventing the attacker from reaching anything *of worth* and allowing the user to deal with the issue).

The same idea works with running an infected application.

Even though almost everything in Qubes OS is isolated, the user experience provides a unified interface, with different colors for window borders, differentiating the various applications and locations, which allows for quick identification of the security level that the user gave the app, location, and so on.

Hardware is also isolated, so the common targets, such as USB controllers, network cards, and firewalls, are also protected.

Qubes also utilizes an interesting *Template* system, which provides locations to install software and to share resources, in a manner that's similar to virtual machines. These TemplateVMs are based on several OSes, such as Fedora (which is the default template), Ubuntu, Whonix, and Archlinux.

Not every app runs in its own qube. Each qube represents what the developers call a **security domain**. By default, all qubes are based on a single, common TemplateVM, (more TemplateVMs can be created if required). Qubes have read-only access to the filesystem of the template on which it's based. If a qube is ever compromised, the TemplateVM on which it's based (including any other qubes based on that specific TemplateVM) remain safe.

Installing Qubes with the default options will provide several default qubes: work, personal, and untrusted. Each qube is also assigned a **label**, which is one of several pre-defined colors. These labels are used to visually differentiate between qubes, and how you interpret them, or use them, is up to you, the user.

In previous chapters, we talked about live CD OSes (OSes that boot from USB or CDs and aren't installed on the computers hardware). They have many security advantages, but, according to Qubes OS developers, live CD OSes are still vulnerable. If these OSes get infected, everything in the OS is at risk, while with Qubes OS, only the specific qube would be infected and the rest of the OS stays safe.

Qubes installs with Xen, a bare-metal hypervisor, by default and is not intended to be installed as a virtual machine (or on a different hypervisor)

Preparing to install Qubes OS

First, download the ISO file from `https://www.qubes-os.org/downloads/`.

Remember, as always, to verify the signature of the downloaded file. There are several ways to get the Qubes Master Signing Key, which allows for the signature verification:

- Fetch it with GPG:

```
$ gpg --fetch-keys
https://keys.qubes-os.org/keys/qubes-master-signing-key.asc
```

- Download it from `https://keys.qubes-os.org/keys/qubes-master-signing-key.asc`, and then import it with GPG:

```
$ gpg --import ./qubes-master-signing-key.asc
```

- Get it from a public `keyserver` (specified on first use with `--keyserver <URI>`, then saved in `~/.gnupg/gpg.conf`), as in the following example:

```
$ gpg --keyserver pool.sks-keyservers.net --recv-keys
0x427F11FD0FAA4B080123F01CDDFA1A3E36879494
```

- Next, obtain the Release Signing Key from the **Downloads** page on the Qubes website, or by fetching it with GPG:

```
$ gpg --fetch-keys
https://keys.qubes-os.org/keys/qubes-release-X-signing-key.asc
```

  If you downloaded the file, you will need to import it with GPG, as seen in the following command:

```
$ gpg --import ./qubes-release-X-signing-key.asc
```

- Fianlly, verify the Qubes OS ISO file by running the following:

```
$ gpg -v --verify Qubes-R4.0-x86_64.iso.asc Qubes-R4.0-x86_64.iso
```

If part of the message you see contains the following, then you're good to go: **Good signature from "Qubes OS Release X Signing Key"**.

Next, you need to transfer the ISO file to the DVD or USB flash drive. If you prefer to use a USB drive, then you just need to copy the ISO on to the USB device, for example, using `dd`:

```
dd if=FILENAME of= target device bs=1048576 && sync
```

According to the Qubes OS website:

> *"On Windows, you can use the Rufus tool. Be sure to select "DD image" mode (you need to do that **after** selecting the Qubes ISO):*
> ***Warning:** If you do that on Windows 10, you can only install Qubes without MediaTest, which isn't recommended."*

You can obtain Rufus from here: `https://rufus.akeo.ie/`.

Universal USB Installer can also be used.

You can also install Qubes on a USB flash drive, as a Live CD/USB, with one specification: leave the option checked to **Automatically configure my Qubes installation to the disk(s) I selected and return me to the main menu**.

Hardware requirements

The minimum installation requirements are as follows:

- 64-bit Intel or AMD processor (AMD64)
- Intel VT-x with EPT or AMD-V with RVI
- Intel VT-d or AMD-Vi (in other words, AMD IOMMU)
- 4 GB RAM
- 32 GB disk space

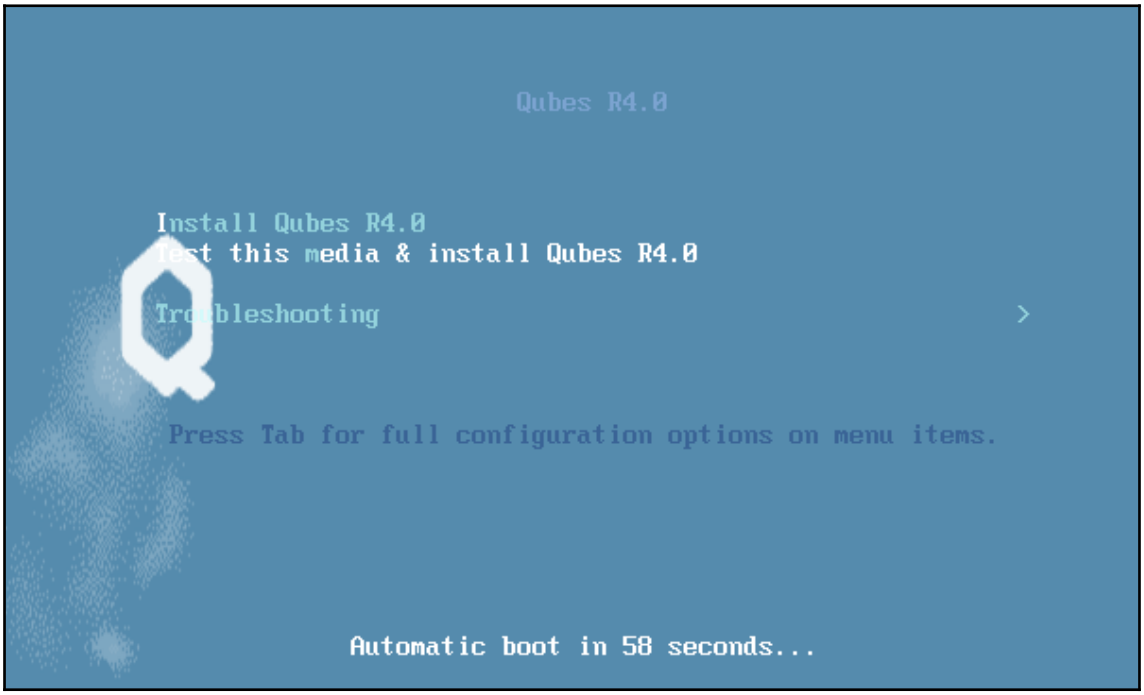
The following are the recommended requirements:

- Fast SSD (strongly recommended)
- Intel IGP (strongly preferred):
    - Nvidia GPUs may require significant troubleshooting
    - ATI GPUs have not been formally tested
- TPM with proper BIOS support (required for **Anti Evil Maid**)
- A non-USB keyboard or multiple USB controllers

The installation process

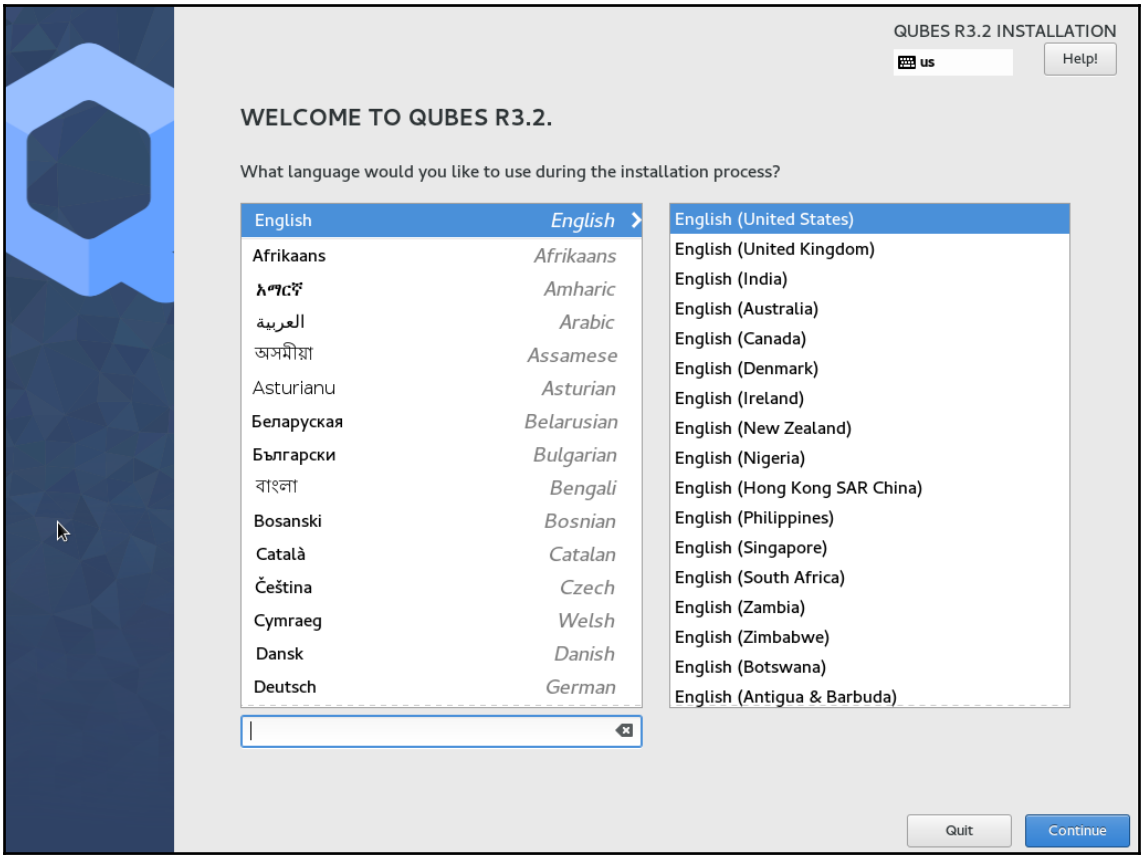
After preparing the installation media (USB/DVD),

1. Boot the computer from it.
2. You'll receive the following screen, where you should choose one of the displayed options (**Test this media & install Qubes** will verify the target installation media for compatibility):



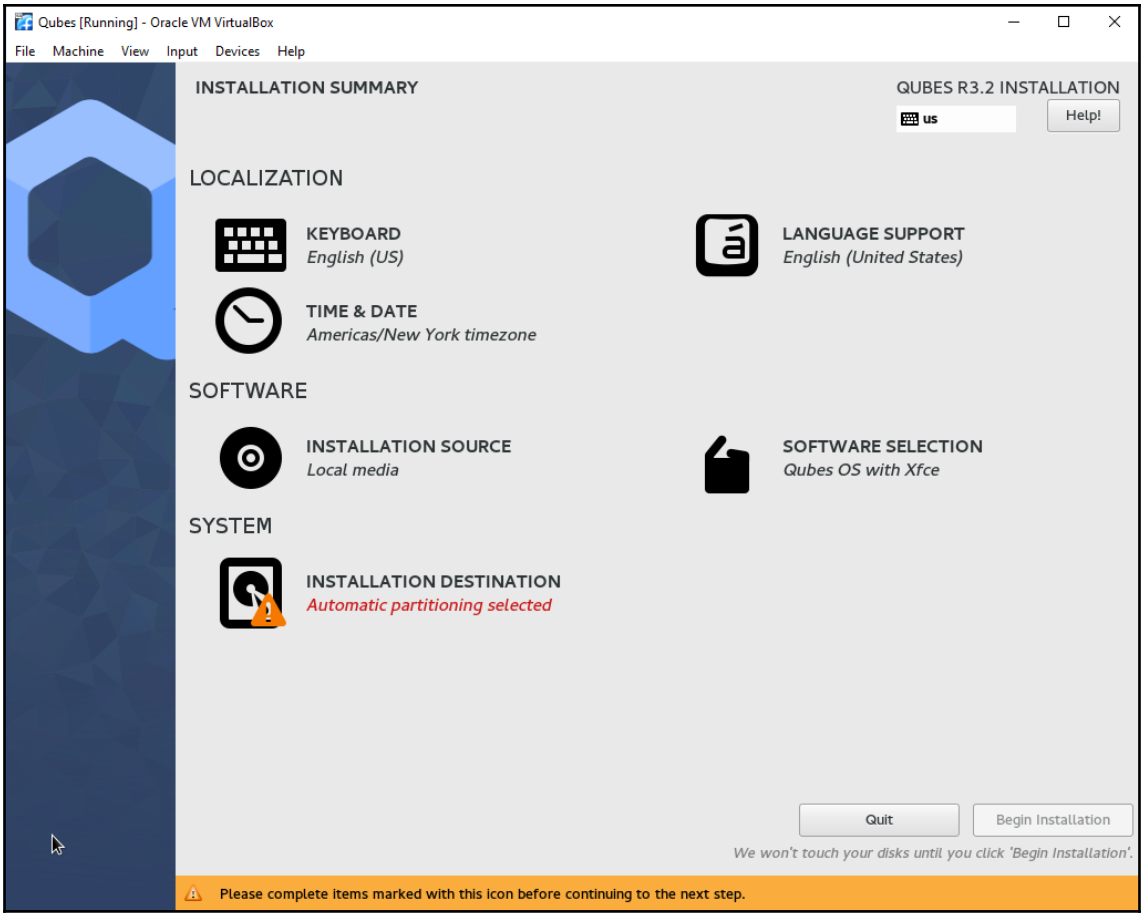
Install Qubes

3. You'll then see the installation process begin, starting with the installation of Xen on the computer. This will be in a **console/shell** view. When that process ends, you'll see the following screen:



Welcome to Qubes

4. Choose the language you want and then press **Continue**:



After a short wait, you'll reach the previously displayed screen, where you'll need to finalize the installation process, by completing the marked options, **Installation Destination**, and then, on the following screen, provide a username and password. The installation process will proceed and, when it ends, you'll be able to log in.

Using Qubes to access the Dark Web with Tor Browser is a little different than other operating systems. In its latest versions, Qubes use Whonix as a secure way to access the Tor network. Whonix replaced TorVM (a VM dedicated to Tor access) as the way to access Tor on Qubes. We'll discuss Whonix in depth in the next chapter, but, for now, let's understand how it helps with Qubes.

Whonix is installed with Whonix-Gateway and Whonix-Workstation TemplateVMs, where the Gateway is the part that accesses the network (or, more specifically, Tor). Whonix was developed and designed to be run inside a VM and paired with Tor. This makes it a perfect fit for Qubes. To install Whonix in Qubes, you need to access dom0 first.

To do so, perform the following steps:

1. Go to the **Start** menu and click **Terminal Emulator**.
2. Press *Alt + F3*, and type the following, and then press *Enter* twice:

```
xfce terminal
```

3. Right-click on the desktop and select **Open Terminal Here**, and then run the following:

```
sudo qubesctl state.sls qvm.anon-whonix
```

This can take some time (up to 30 minutes or more), and there's no progress indicator, so be patient. Stopping the process will result in errors.

According to the Qubes website, if an error message appears stating that `qubesctl` doesn't exist or the command isn't recognized, then it's necessary to enable the testing repository and install `salt`. To do so, run the following:

```
sudo qubes-dom0-update --best --allowerasing --enablerepo=qubes-dom0-
current-testing qubes-mgmt-salt-dom0-virtual-machines
```

If you install Qubes R4 and above, you can choose to set up a DVM Template as a base for **disposable VMs** (a VM that will be disposed of, after use, for more security). To do so, run the following in dom0:

```
sudo qubesctl state.sls qvm.whonix-ws-14-dvm
```

Now, update both the Whonix-Gateway and the Whonix-Workstation Template VMs by running the following:

```
sudo apt-get update
```

Accessing the Dark Web with Qubes

To launch Tor Browser, run the following:

1. Qubes App Launcher (blue/grey "**Q**") | Domain: anon-whonix | Privacy Browser
2. Now you can surf the Dark Web with Tor Browser, anonymously and privately, using Qubes OS (with a little help from Whonix), by entering the URLs of `.onion` sites into the browser address bar, as you would in a *standard* browser.

Always remember, do NOT provide your real details on the Dark Web: not your name, address, emails, and definitely not your credit card details.

Even though we're discussing how to access the Dark Web in a more secure and private manner, remember the cardinal rule: do not trust software! They all have inherent vulnerabilities and can be exploited by attackers. Using security, privacy, and anonymity-focused operating systems helps minimize the risk, but it's never enough.

Be careful.

Summary

In this chapter, we talked about Qubes OS, how to install it, and its basic use. We discussed what makes Qubes unique and how it helps protect the user's privacy and security. We saw how two different systems work together (Qubes and Whonix), to provide an encompassing secure way to access the Dark Web.

In the next chapter, we'll discuss Whonix, another security-focused OS, but with a different approach.

Questions

1. What makes Qubes unique?
2. How can you differentiate between various qubes?
3. What hypervisor platform allows Qubes to create its qubes?

    A. Xen

    B. VMWare

    C. Hyper-V

Further reading

Please refer to the following reference:

- Qubes OS: `https://www.qubes-os.org/`