Using a cloud to manage a cloud

Sysadmin Miniconf at Linux.conf.au

Slides: https://github.com/orionvm/LCA2020
$ whoami

- Alex Sharp, Andrew Reimers, Anuj Dhavalikar
- Using Qubes for Dev/sysadmin work for ~ 3 years
- Working at OrionVM –
  - White-label cloud (IaaS)
Agenda

- Why protect sysadmins?
- What is Qubes?
- Isolations provided by Qubes:
  - Graphics
  - Networks
  - Ssh/GPG keys
  - USB/PCIe
- Recommended hardware
- Q&A
Threat model

- Zero day exploit – 100K USD for Firefox RCE
- Cost per exploited user
- Profit per attack
- Political motivation
- Ransomware
- Password stealing
What is Qubes?

- “A reasonably secure operating System” focusing on security through isolation - “You can’t hit what you can’t see”
- Consists of multiple Qubes and an isolated management VM
  - A Qube is a Xen VM running an OS (Linux/FreeBSD/etc)
  - Has it’s own xserver for graphics
  - “Desktop Cloud”
- Tied together via vchan, virtual networking
- Optional USB devices (proxy), PCIe devices (IOMMU)
- Managed by an internal agent (qrexec) via vchan.
Is it usable?

- Generally yes.
Firefox and a password manager
Firefox and a password manager

Please sign in
Username
Password
Don't Remember Login

Enter master key
Home/user/passwords.kdbx

Password: 00000000000000000000000000000000

Oracle VM

Sysadmin Miniconf @ Linux.conf.au 2020
Firefox and a password manager
Network isolation

cust01-work  cust01-vpn

cust02-work  cust02-vpn

vault

disp1337

sys-firewall

sys-net

WIFI
Vault isolation

```
user@vault:~$ ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
user@vault:~$ lspci
user@vault:~$  
```
Vault isolation

1. RPC via VChan
   qubes.SshAgent

2. Ssh key agent protocol

3. Vault

4. Work
USB isolation

- USB is a lovecraftian nightmare
- A ‘USB key’ can be a
  - Keyboard
  - Mouse
  - Virtual ethernet device
  - Storage device
  - Pizza oven
USB isolation

USB
→ USB HBA
→ PCIe
↓ IOMMU

USB Keyboard
USB HBA
PCIe
IOMMU

sys-usb
VChan
DOM0
VChan
Qube

[SysAdmin Miniconf @ Linux.conf.au 2020]
Hardware isolation
Qubes video call
Qubes video call
Disposable qube
Convert to trusted PDF

- Built on top of disposable qubes
- Did you know that printers update via printable documents? Does your printer have an internet connection?
# Qube Manager

<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
<th>Template</th>
<th>NetVM</th>
<th>Disk usage</th>
<th>Internal</th>
<th>IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>dom0</td>
<td></td>
<td>AdminVM</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>personal-work</td>
<td></td>
<td>fedora-30</td>
<td>default (sys-firewall)</td>
<td>35773.44 MiB</td>
<td>10.137.0.17</td>
<td></td>
</tr>
<tr>
<td>sys-firewall</td>
<td></td>
<td>fedora-30</td>
<td>sys-net</td>
<td>104.24 MiB</td>
<td>10.137.0.6</td>
<td></td>
</tr>
<tr>
<td>sys-net</td>
<td></td>
<td>fedora-30</td>
<td>n/a</td>
<td>137.01 MiB</td>
<td>10.137.0.5</td>
<td></td>
</tr>
<tr>
<td>sys-usb</td>
<td></td>
<td>fedora-30</td>
<td>n/a</td>
<td>172.85 MiB</td>
<td>10.137.0.15</td>
<td></td>
</tr>
<tr>
<td>vault</td>
<td></td>
<td>fedora-30</td>
<td>n/a</td>
<td>105.68 MiB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>anon-whonix</td>
<td></td>
<td>whonix-ws-15</td>
<td>sys-whonix</td>
<td>0.0 MiB</td>
<td>10.137.0.10</td>
<td></td>
</tr>
<tr>
<td>deb-dvm</td>
<td></td>
<td>debian-10</td>
<td>default (sys-firewall)</td>
<td>145.82 MiB</td>
<td>10.137.0.20</td>
<td></td>
</tr>
<tr>
<td>debian-10</td>
<td></td>
<td>TemplateVM</td>
<td>default (n/a)</td>
<td>8019.35 MiB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>default-mgmt-dvm</td>
<td></td>
<td>fedora-30</td>
<td>n/a</td>
<td>0.0 MiB</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
Recommended Hardware

- Intel integrated graphics best
- AMD/Nvidia with good OSS drivers will do
- Intel CPU with ME cleaner best
- Recent AMD cpus - Check kernel support.
- 8gb okay, 16gb good, 32gb overkill for most use cases.
- Coreboot/heads firmware not required but improves security
- Purism Librem 13/15 best, Insurgo PrivacyBeast X230/NitroPad good
- Intel NUC/Dell XPS/Lenovo Thinkpad etc. ok.
- https://www.qubes-os.org/hcl/
Help wanted

- Windows drivers!
- Python/Bash help needed!
- Open source project!
- [https://github.com/QubesOS/qubes-issues](https://github.com/QubesOS/qubes-issues)
- [https://www.qubes-os.org/donate/](https://www.qubes-os.org/donate/)
More info

- BOF on Thursday at Lunch, room 7
- “The future of the desktop is on hypervisor powered containers” talk tomorrow
- https://www.qubes-os.org/
- https://www.qubes-os.org/support/
- https://wiki.qubes.rocks
Thank you for your attention! Do you have any questions?