Security +
Virtualization

Author: Joseph Lee
Email: joseph@ripplesoftware.ca
Mobile: 778-725-3206

Virtualization

- Hosting one or more virtual systems or virtual machines (separate OS's) on a single physical system
- Virtualization provides **good ROI** due to **elasticity**, **flexibility**, and **convenience**
- Virtualization provides **convenience** and **efficiency** because VMs can be created from snapshot images and deployed very quickly to a secure baseline configuration
- Virtualization provides **flexibility** by allowing a single piece of hardware to run multiple versions of an OS or software application concurrently
- Virtualization provides **good enough security** for some use cases such as sandboxed of a computer virus defence because **VM's are sandboxed** and so it's a good testing environment

Host
- The computer running the hypervisor

Guest
- The virtual machine operating system instance that is running on the host

Persistence
- Allows changes to be saved on the VM that will be there after reboot / logout

Non-persistence
- Does now allow saving of changes after reboot / logout

Hypervisor
- Software that controls and runs the VMs such as **Oracle VirtualBox**, **Microsoft Hyper-V**, **VMware**, and **KVM ()**
- **Type 1 / Bare metal**
  - Runs directly on the system hardware as a dedicated appliance
  - Configured and carefully developed to increase availability
  - More efficient and reliable than type 2 hypervisors
- **Type 2**
  - Runs as software within a normal operating system
  - Not as robust / reliable or scalable as a type 1 hypervisor

Host elasticity and scalability

- Ability to dynamically resize computing capacity to each VM based on the load

Application cell / Container virtualization

- Runs applications or services within isolated application cell or container
- All services share the same OS
- Is more **efficient** than using a **type 2 hypervisor**
- **Docker** is one popular example of a **container management system**

Virtual Desktop Environment VDE / Virtual Desktop Infrastructure VDI

- A workstation desktop environment is running as a VM on a server
- Can increase hardware resources of a workstation
- Support persistence or non-persistence

Risks of Virtualization

VM Escape

- Attack that allows a hacker to access the host system

VM Sprawl

- Improperly managed VMs / un-patched VMs present risk to network security
- VMs must be updated regularly and disabled after their use is over

Data loss

- Virtual machines are easy to image and steal as files

Benefits of VM’s

Segregation

- Provides security benefits of being able to sandbox OS, services, and software

Segmentation

- Trust zones of virtual networks (SDNs) can be created with virtualization

Isolation

- Testing of software and observation of the behaviour of malware can be done in a way that protects the other network infrastructure

Lower operating costs

- Through sharing resources