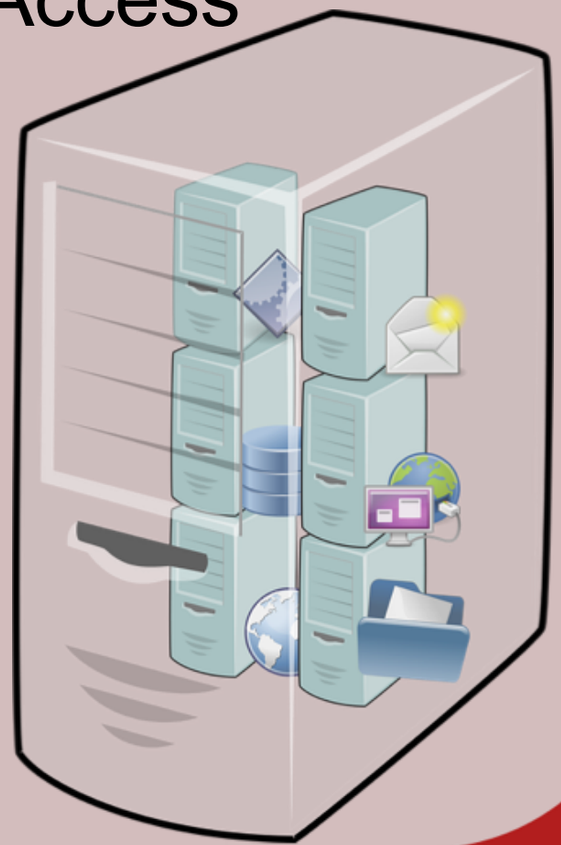
JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Virtualization Vulnerabilities

VULNERABILITY MANAGEMENT

Virtualization Vulnerabilities

- VM Escape
- Management Interface Access
- Virtual Host Patching
- Virtual Guest Issues
- Virtual Network Issues



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

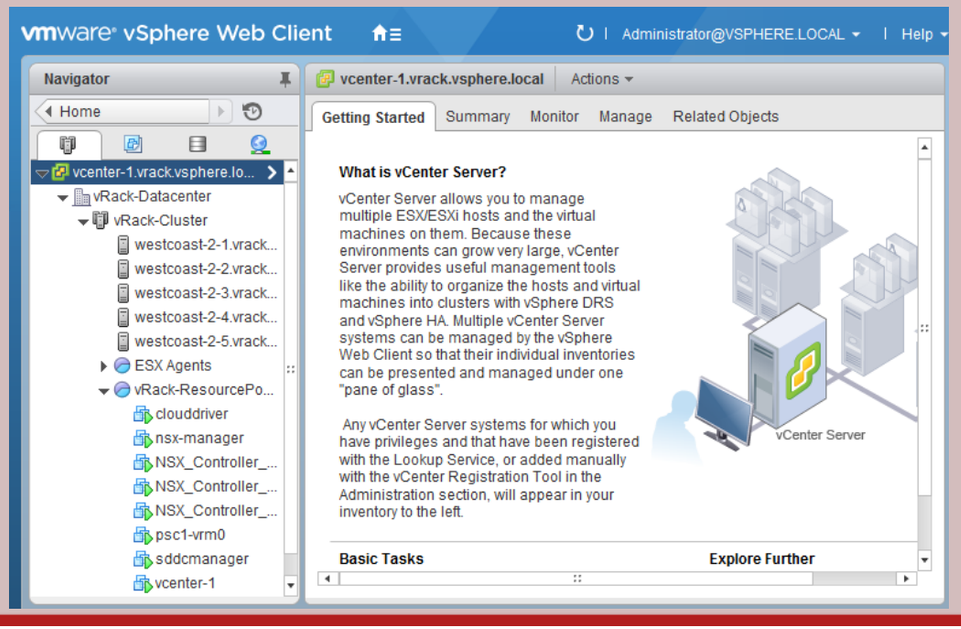
VM Escape

- Most serious of all virtualization issues
- Occurs when an attack can break out of the virtual machine (guest) and reach the host (hypervisor)
- In May 2017, a hacking contestant stitched together 3 different exploits and managed to perform a VM escape

Source:
https://arstechnica.com/information-technology/2017/03/hack-that-escapes-vm-by-exploiting-edge-browser-fetches-105000-at-pwn2own/

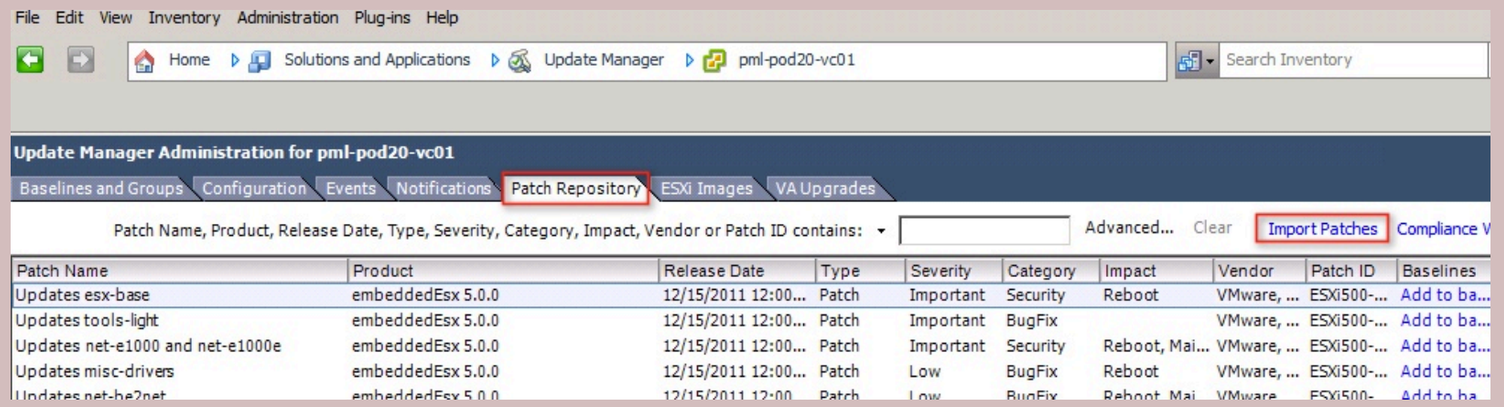
Management Interface Access

- This interface controls access to all the virtual machines and can configure them
- Should be highly secured, including use of two-factor authentication



Virtual Host Patching

- Just like other servers Virtual hosts need patching of their OS and software
- This can help prevent VM Escape



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Virtual Guest Issues

- Each guest represents another server on the network, and they all need patching
- Ensure your remediation and patch management considers all your VMs
- Ensure your vulnerability management program also scans Guest VMs

Virtual Network Issues

- Virtual firewalls, routers, and switches all need to be considered as part of your scanning program

- If embedded as part of your VM solution, ensure appropriate patching is being done to prevent attacks