Beware Of The Rogue VMs!

Published: 2024-11-11 · Archived: 2026-04-05 21:52:34 UTC

At this years VMware Explore 2024 in Barcelona, I did a presentation called “CMTY1321BCN: Beware Of The Rogue VMs!”, a recording of the session is also available on the VMware Explore 2024 Community YouTube channel.

Here is a quick text based recap of it.

What are Rouge VMs?#

First off, we need to define what a *Rougue VM* is. In short, a rougue VM is a VM that runs on an ESXi host, but you don’t really know that it’s running. It is not shown in ESXi Host Client, or in the vSphere Web Client.

Back in January 2024 MITRE’s Networked Experimentation, Research, and Virtualization Environment (NERVE) was compromised through a series of vulnerabilities. They have written a detailed post-mortem of it that highlights all the details, but in short the attackers were able to inject their own VMs into the environment. VMs that don’t show up using the “normal” administration interfaces.

How are Rogue VMs created?#

This is surprisingly easy to do. If someone has SSH and root access to an ESXi host, all that is required is to place a valid VM on an available datastore, edit the .vmx file to connect it to a valid network and run the following command:

```
/bin/vmx -x /vmfs/volumes/volname/vmname/vmname.vmx 2>/dev/null 0>/dev/null &
```

This commands starts the VM, without registering it in the inventory (which is why it doesn’t show up in the ESXi Host Client, og the vCenter Web Client) and sends the output to `/dev/null`. This VM then runs as a normal VM, but hidden.

The `vim-cmd vmsvc/getallvms` (documentation) command will not show this VM, as that command queries the host inventory. `esxcli vm process list` (documentation) however, will show it, as it shows **all** the running VMs on the host, regardless of registration status.

How are Rogue VMs Made Persistent?#

When an ESXi host boots `/etc/rc.local.d/local.sh` is run, so making these VMs persistent once they are placed on an ESXi host is as simple as adding the `vmx` command above to it. Once that is done, the Rogue VM will autostart when the host reboots, still undetectable in the usual admin interfaces.

Identifying Rogue VMs#

There are a couple of available resources that will help identify Rogue VMs in an environment.

- Invoke-HiddenVMQuery by MITRE (PowerCLI)
- VirtualGHOST by Crowdstrike (PowerCLI)
- RVTools In the RVTools vHealth tab, VMs located on a Datastore, that are not registered with the inventory, are identified as “Possibly a Zombie VM!”

Rogue VM Mitigation Strategies#

1. **Always keep vCenter and ESXi hosts patched**
2. **DO NOT enable SSH on your ESXi hosts (or vCenter)**
    - “Everything” can be done through vCenter/Host Client/APIs anyway, there are few real world use cases when SSH needs to be enabled at all
    - Open SSH only when required, and close after use
3. **Monitor ESXi logs for SSH enablement and logins, and look for these events:**
    - `/var/log/shell.log`
        - SSH[ID]: SSH login enabled
        - shell[ID]: Interactive shell session started
    - `var/log/auth.log`
        - sshd[ID]: FIPS mode initialized
4. **Use Secure Boot**

    Secure Boot prohibits `/etc/rc.local.d/local.sh` from running on boot, this preventing perseverance

Of course, if someone has SSH and root access to your ESXi hosts, all bets are off anyway as they can pretty much to whatever they want. Make sure this is limited to only being available when absolutely required and please practice safe ESXi!
