Wireless Security Lab – ESXi Scripts API

Chris Van Oort c@chrisvanoort.com 12/11/13

I enabled VNC support in the firewall on ESXi 5.1 with this script:
https://gist.github.com/jasonberanek/4670943

All scripts are located on the ESXi Server at "/vmfs/volumes/datastore1/wnsl-tools"

Create a new VM for a User

For creating a new VM for a user; the script is smart enough to do a cleanup if it needs to before creating a new clone. Meaning it will mercilessly delete an existing VM.

It will create a new VM for the student based off of the student's username under the "datastore1/student_images/USERNAME/attacker or defender/" folder.

Next it generates a VMX configuration file for the newly created VM, and enables VNC access in that via the specified port number. The VMX files output are based off of the VMX files from the base machines we are cloning from.

Finally it registers the VM with ESXi and then powers it on.

Scripts: clone_attacker.sh, clone_defender.sh

Usage: clone_attacker.sh USERNAME PORTNUMBER

Example: clone_attacker.sh chrisv 5901

Power On/Off & Get Power Status

Power On just turns an existing VM on if it's there.

Power Off will power off a machine AND release any assigned USB devices.

Get Power Status will return the power status of the machine, it should be string processed to get remove information other than "on" / "off".

Scripts: poweroff_attacker.sh, poweroff_defender.sh

poweron_attacker.sh, poweron_defender.sh

powerstatus_attacker.sh, powerstatus_defender.sh

Usage: poweron_attacker.sh USERNAME

Example: poweron_attacker.sh chrisv

Delete a VM for a User

This will power off a VM, unregister it from ESXi, delete the VMDK, and clean up any remaining files.

Scripts: delete_attacker.sh, delete_defender.sh

Usage: delete_attacker.sh USERNAME

Example: delete_attacker.sh chrisv

Assigning USB Hardware

Scripts: assignusb_attacker.sh, assignusb_defender.sh

Usage: assignusb_attacker.sh USERNAME 1-5

Example: assignusb_attacker.sh chrisv 1

> This will assign the first usb device specified in "usbdevices_includes.conf" to the attacker VM for student chrisv.

Common-Path & Configuration Files

attacker_includes.conf

> Includes the paths and file names to the base attacker VM.

defender_includes.conf

> Includes the paths and file names to the base defender VM.

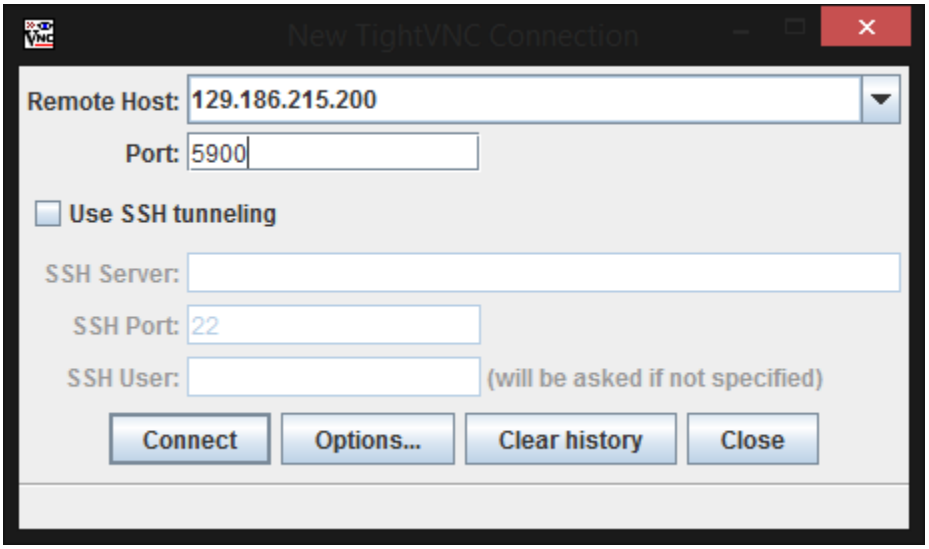
usbdevices_includes.conf

> Currently there are 5 USB WiFi dongles plugged in and visible in ESXi, this contains the hardware address of those for use in the "assignusb_*" scripts.

Connecting to a VM as a Student

Download the TightVNC Java Viewer from here: http://www.tightvnc.com/download.php

Run the jar executable:



Enter the server IP (129.186.215.200)

Enter the port number as specified on the website, in our case it’s 5900.

Click ‘Connect’ and then when prompted for the password, enter your website username.

You’re now connected to the Virtual Machine.