Building a better (pentesting) playground!

Presented by

Maurice Cronin

Background

- Left CIT with a BSc in Analytical Chemistry
- Worked in various labs
- Building work
- Tool hire
- Coring and chasing
- Small engine repair
- Back to CIT for the first year of the H. Dip in Cloud Computing
- Software QE at EMC

ESXi

- A ‘bare-metal’ hypervisor from VMWare
- Lightweight OS
- Allows you to create and control virtual machines (VMs)
- Runs on a wide-range of hardware

Specs for my ESXi server

My ESXi setup is a re-purposed desktop machine, with parts from 2011 (though it now has a whole extra 2 GB of RAM!)

Dear Mr Maurice Cronin,

This email is to acknowledge placement of order number [redacted]
Order date and time: 19 Apr, 11, 12:43 am.

Your order consisted of the following items:

Item	Qty	Price
Gigabyte GA-P55-USB3 Intel P55 (Socket 1156) DDR3 Motherboard	1	£71.66
OCZ Agility Series 30GB 2.5" SATA-II Solid State Hard Drive (OCZSSD2-1AGT30G)	1	£37.99
	Sub Total:	£109.65
DPD Two Day Parcel - Eire & Scottish Islands	Shipping:	£12.15
	Total Vat:	£25.58
	Total inc Vat:	**£147.38**

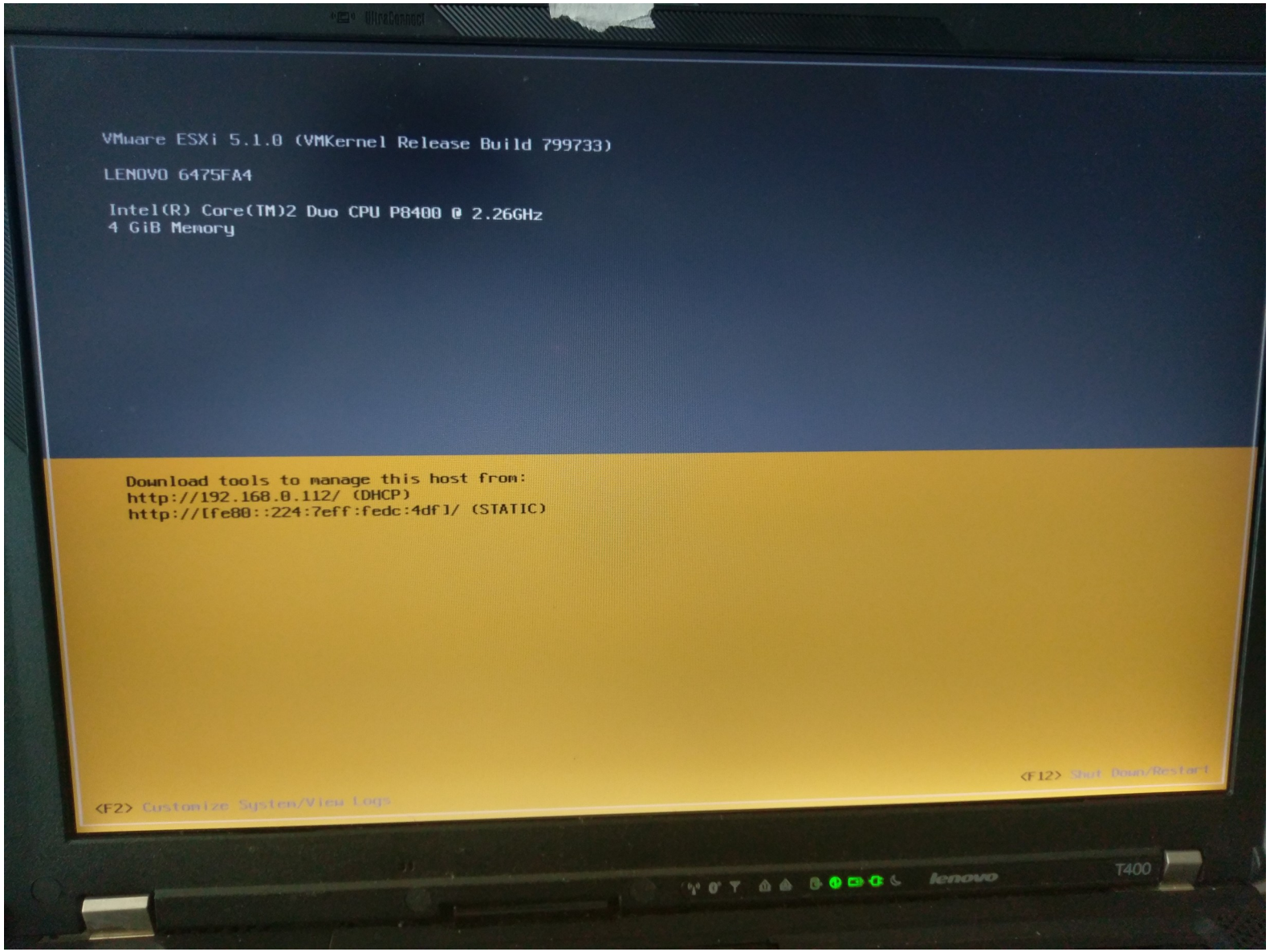
Dear Mr Maurice Cronin,

This email is to acknowledge placement of order number [redacted].
Order date and time: 28 Apr, 11, 9:05 pm.

Your order consisted of the following items:

Item	Qty	Price
Intel Core i3 550 3.20GHz (Clarkdale) (Socket LGA1156) - Retail	1	£74.99
OCZ Gold 4GB (2x2GB) DDR3 PC3-10666C9 1333MHz Low-Voltage Dual Channel Kit (OCZ3G1333LV4GK)	1	£41.66
Western Digital Caviar Blue 500GB SATA 6Gb/s 16MB Cache - OEM (WD5000AAKX)	1	£27.49
	Sub Total:	£144.14
DPD Two Day Parcel - Eire & Scottish Islands	Shipping:	£12.90
	Total Vat:	£32.98
	Total inc Vat:	**£190.02**

Running on an old laptop



- Why ESXi?
  - Fexlible
  - Easy to use
  - Free
  - Easily isolated
  - Lots of documentation and online resources

Why build an isolated lab?

- Provides a safe, secure environment for penetration testing, malware analysis, network studying
- Pentesting can be disruptive, safer to have a seperate environment
- If you’re doing malware analysis something unpleasant could escape
- As your lab is running on a server it can be left running continuously, useful for long tests/scans
- Snapshots/cloning make it easy to roll back VMs

What is needed for an isolated lab?

- ESXi server
- Router
- Ethernet cables
- Client to manage and access the Vms
- Don’t connect it to anything else

The Plan

- Add files to .iso format using genisoimage
- Transfer files to datastore in 2 ways
  - Datastore browser
  - SCP
- Create an internal virtual network
- Create VM for linux and start the OS install
- Create a router VM
  - Attach the router disk to a linux VM
  - Copy the router image to the linux VM via CD
  - Use dd to write the image to the router disk
  - Detach the router disk and then boot the router