Master Thesis - Security Aspects in Virtual Networks

SITREP 11

Laurent De Wilde
Master of Science in the Applied Computer Science
Vrije Universiteit Brussel

March 23, 2015

Work done

This is an overview of the work performed in the past week:

- Installed Snort IDS on an Ubuntu VM running on Hyper-V as shown on the figure below. The switch port of the Snort VM is now the destination, meaning it "sees" all the traffic on the other Hyper-V VM's as well as the traffic that is sent to the Hyper-V host. As will turn out later, Snort is also able to "see" traffic from and to the Xen virtual network.

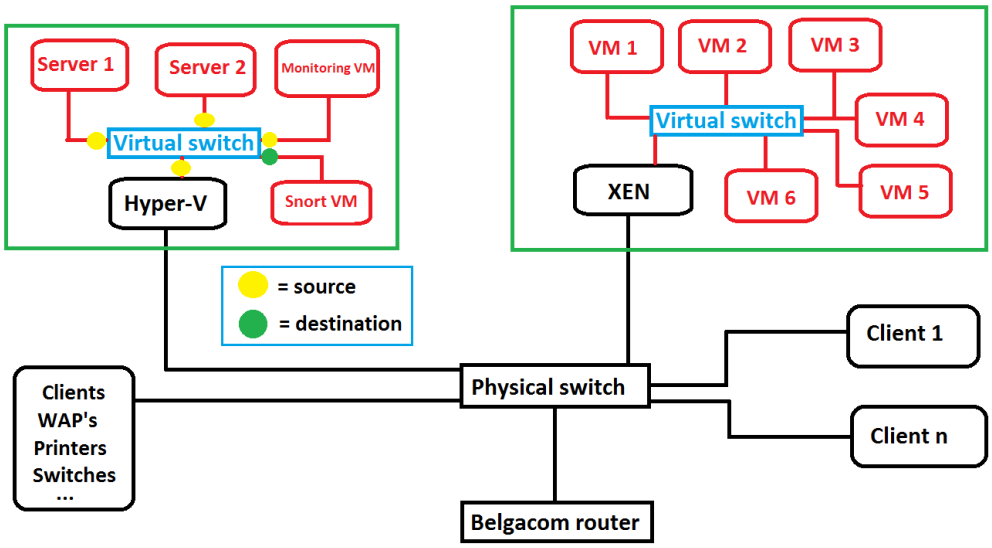


Figure 1: The modified and network setup.

- Tested the VM to see if it is indeed capturing / sniffing network traffic. Therefore, I used "tcpdump". This was indeed the case. So this means that all traffic to and from the virtual Hyper-V network is picked up by the SnortVM and therefore also by Snort itself as it will turn out later.

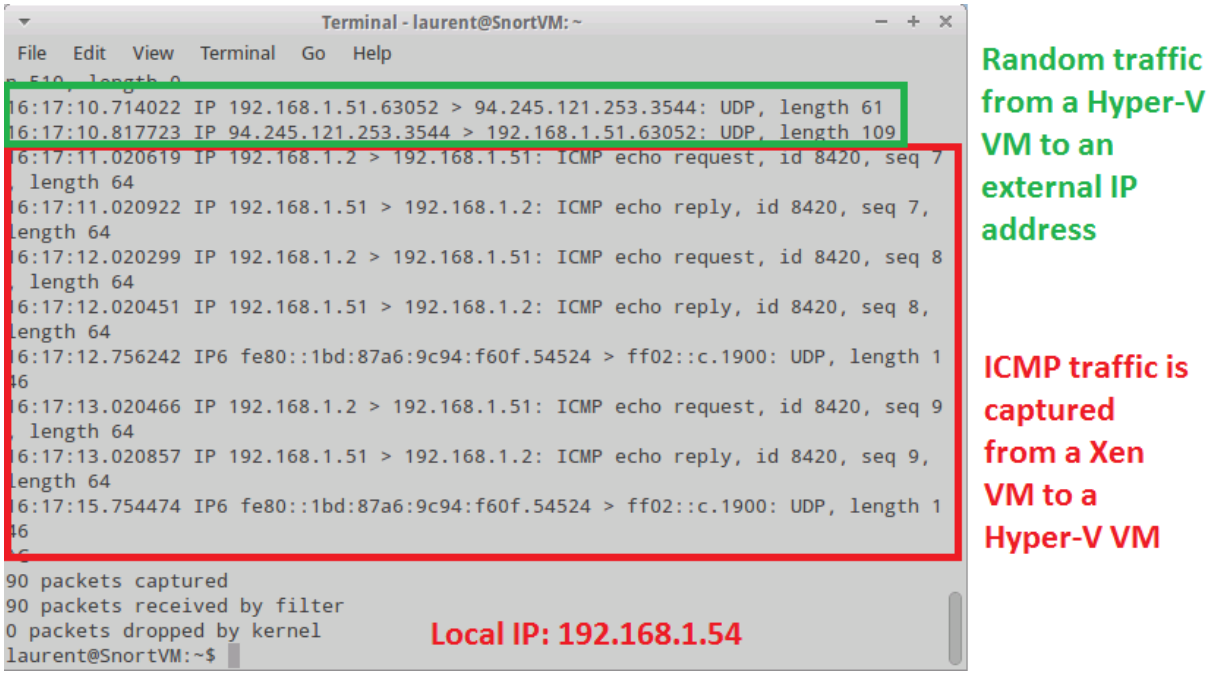


Figure 2: Traffic is captured from a Hyper-V VM to an external IP address and from a Xen VM to a Hyper-V VM by the sniffer (tcpdump).

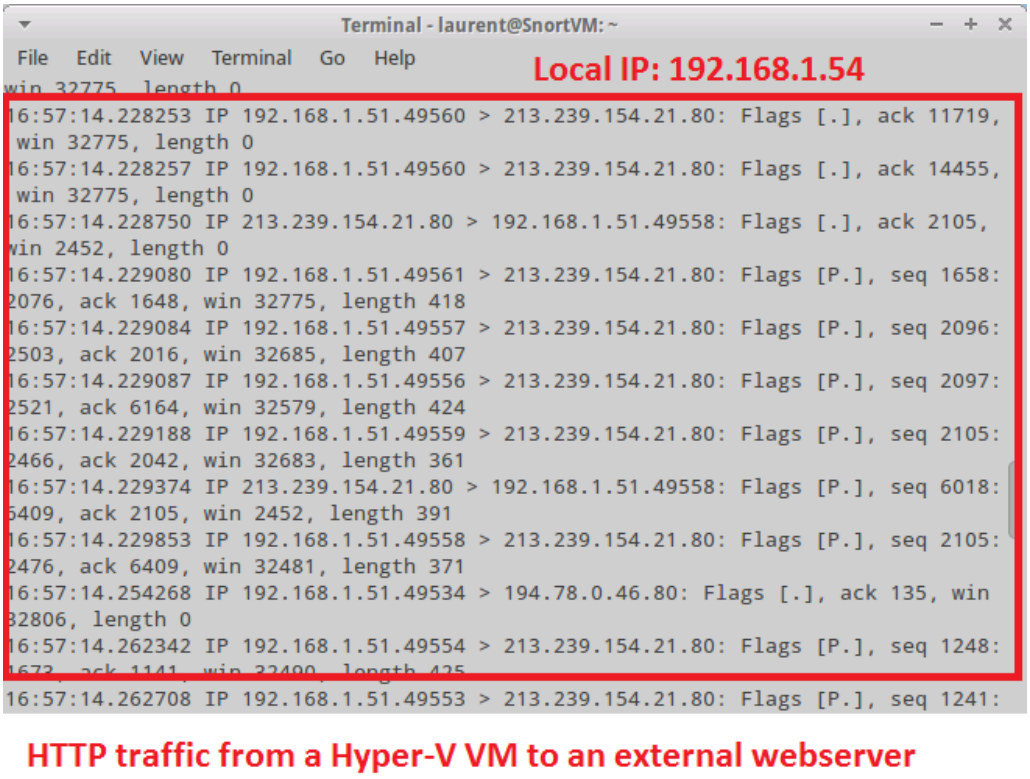
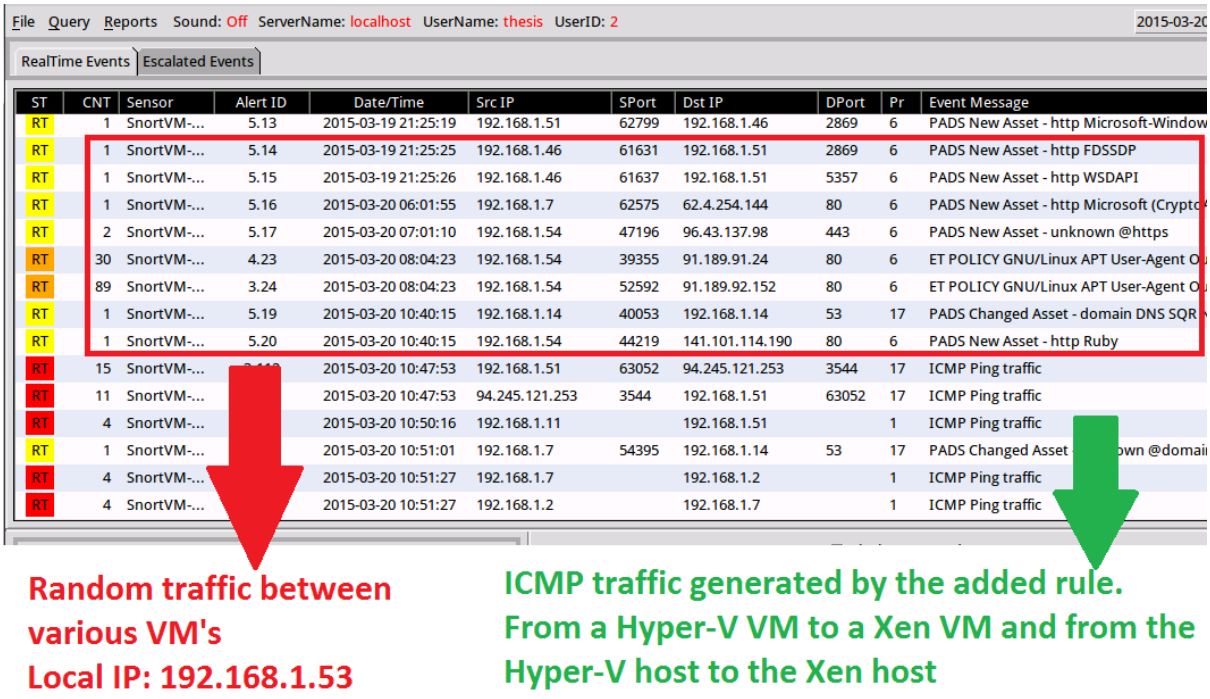


Figure 3: Traffic is captured from a Xen VM to a Hyper-V VM by the sniffer (tcpdump).

- Tested Snort for the correct working (added PING rules) as can be seen in the figure below. It turns out that Snort is indeed capable of detecting intrusions on the Hyper-V virtual network.



ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	SnortVM-...	5.13	2015-03-19 21:25:19	192.168.1.51	62799	192.168.1.46	2869	6	PADS New Asset - http Microsoft-Window
RT	1	SnortVM-...	5.14	2015-03-19 21:25:25	192.168.1.46	61631	192.168.1.51	2869	6	PADS New Asset - http FDSSDP
RT	1	SnortVM-...	5.15	2015-03-19 21:25:26	192.168.1.46	61637	192.168.1.51	5357	6	PADS New Asset - http WSDAPI
RT	1	SnortVM-...	5.16	2015-03-20 06:01:55	192.168.1.7	62575	62.4.254.144	80	6	PADS New Asset - http Microsoft (Crypto
RT	2	SnortVM-...	5.17	2015-03-20 07:01:10	192.168.1.54	47196	96.43.137.98	443	6	PADS New Asset - unknown @https
RT	30	SnortVM-...	4.23	2015-03-20 08:04:23	192.168.1.54	39355	91.189.91.24	80	6	ET POLICY GNU/Linux APT User-Agent O
RT	89	SnortVM-...	3.24	2015-03-20 08:04:23	192.168.1.54	52592	91.189.92.152	80	6	ET POLICY GNU/Linux APT User-Agent O
RT	1	SnortVM-...	5.19	2015-03-20 10:40:15	192.168.1.14	40053	192.168.1.14	53	17	PADS Changed Asset - domain DNS SQR
RT	1	SnortVM-...	5.20	2015-03-20 10:40:15	192.168.1.54	44219	141.101.114.190	80	6	PADS New Asset - http Ruby
RT	15	SnortVM-...		2015-03-20 10:47:53	192.168.1.51	63052	94.245.121.253	3544	17	ICMP Ping traffic
RT	11	SnortVM-...		2015-03-20 10:47:53	94.245.121.253	3544	192.168.1.51	63052	17	ICMP Ping traffic
RT	4	SnortVM-...		2015-03-20 10:50:16	192.168.1.11		192.168.1.51		1	ICMP Ping traffic
RT	1	SnortVM-...		2015-03-20 10:51:01	192.168.1.7	54395	192.168.1.14	53	17	PADS Changed Asset - own @domai
RT	4	SnortVM-...		2015-03-20 10:51:27	192.168.1.7		192.168.1.2		1	ICMP Ping traffic
RT	4	SnortVM-...		2015-03-20 10:51:27	192.168.1.2		192.168.1.7		1	ICMP Ping traffic

Figure 4: Snort is indeed picking up traffic / intrusions on the Hyper-V virtual network and reports so.

- However, Snort is only picking up intrusions on the Hyper-V network including the Hyper-V host. Thus, intrusions on the Xen virtual network are not detected, because those VM's resides on a seperate virtual switch.

  So I wanted a way to also detect malicious activity on the Hyper-V network with the SnortVM running on a seperate virtual network.

  Since I'm using in-kernel bridging for the virtual Xen switch, my initial idea was to snif the bridged interface (since all traffic - also between VM's - passes through this interface) and copy all the packets to another, physical interface set in promiscious mode. From there, I could then forward the packets to the Hyper-V network.

  However, it is not possible to forward packets on an interface that is in promiscious mode. So instead of making a copy of the bridged interface, the only solution was to make a copy of the packets on each virtual interface connected to the vSwitch.

  This solution works fine as illustrated in the following screenshots.

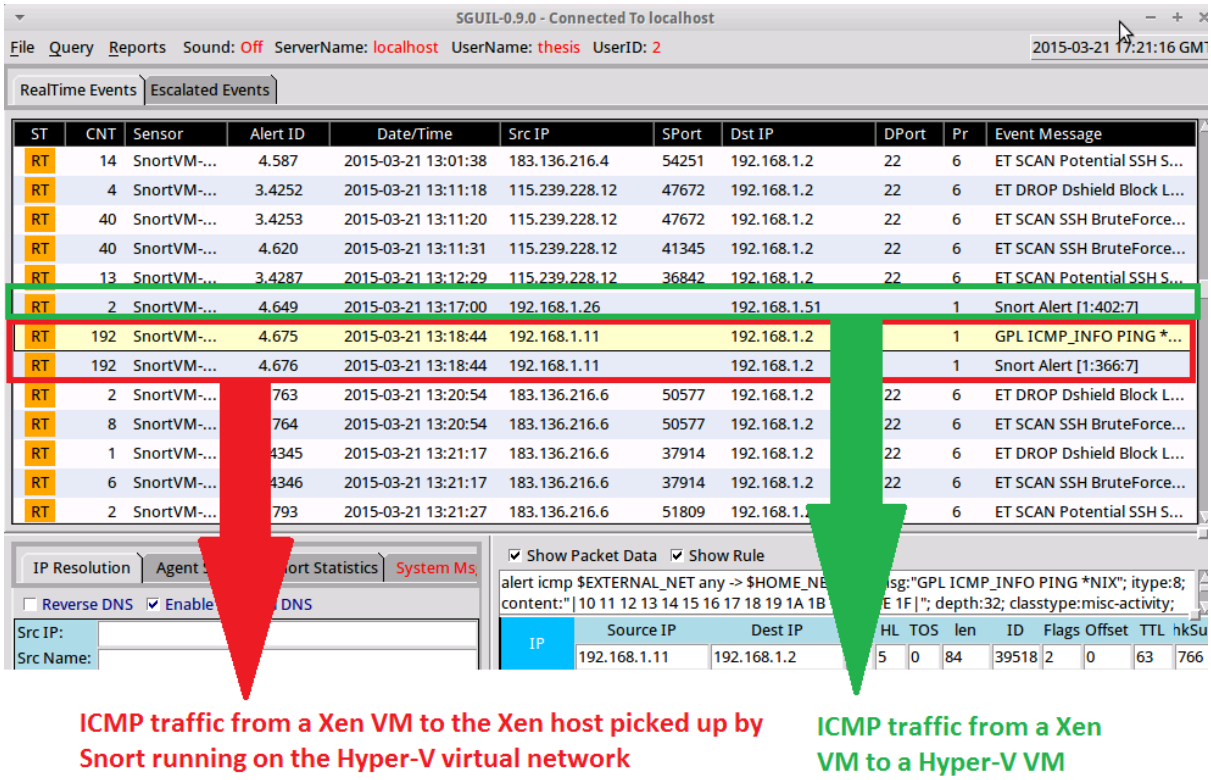


Figure 5: Traffic / intrusions between a Xen VM and a Xen host as well as intrusions between a Xen VM to the Hyper-V host.

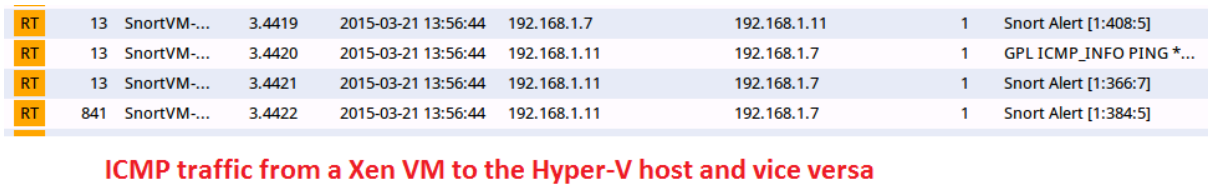


Figure 6: From a Xen VM to the Hyper-V host.

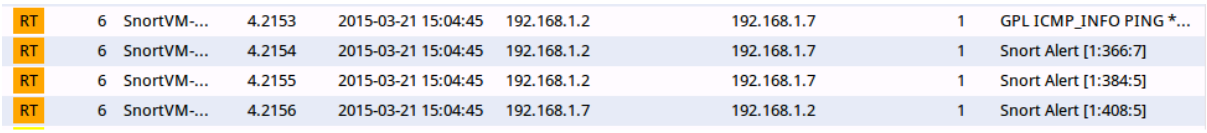


Figure 7: Intrusions between the two hosts of both virtual networks.

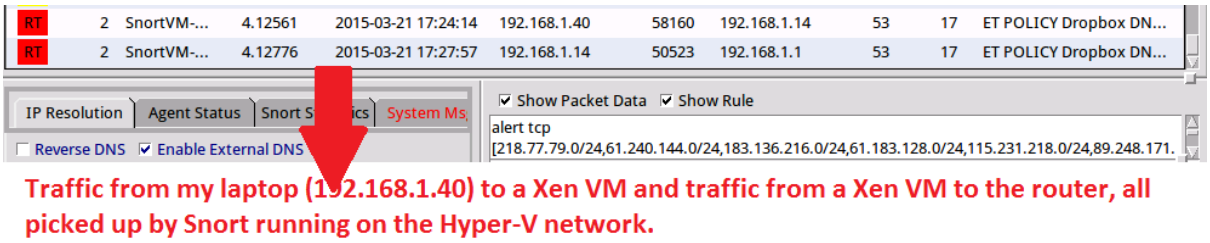


Figure 8: Traffic / intrusions from a client to a Xen VM (Xen virtual network) picked up by Snort running on the Hyper-V network.

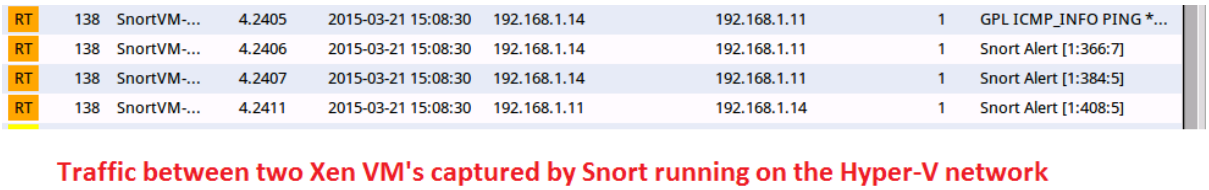


Figure 9: Traffic / intrusions between two Xen VM's (inside the Xen virtual network) picked up by Snort running on the Hyper-V network.

So to summarize, the following is possible / is achieved regarding intrusions:

- Detecting intrusions between two VM's running on the Hyper-V virtual network.
- Detecting intrusions between a VM running on the Hyper-V virtual network and the Xen virtual network and vice versa.
- Detecting intrusions between two VM's running on the Xen virtual network.
- Detecting intrusions between the Xen host and Hyper-V host and vice versa.

Planning

Problems

Issues

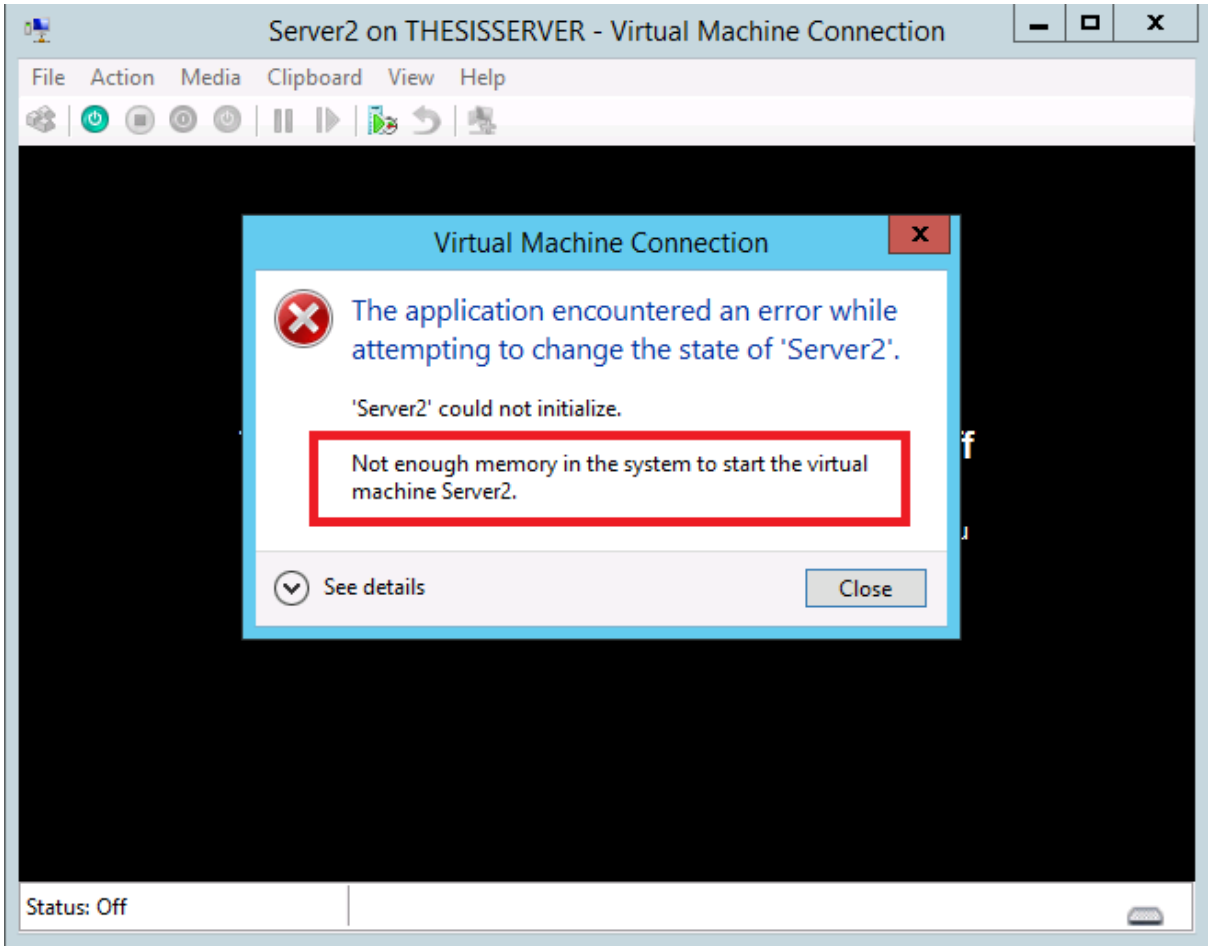


Figure 10: Running two Windows 7 VM's with each 1GB of RAM is not possible with Snort running on the same host with 8GB of RAM. Only one Windows 7 VM is able to run with a Snort VM on the same Hyper-V host with 8GB of RAM.

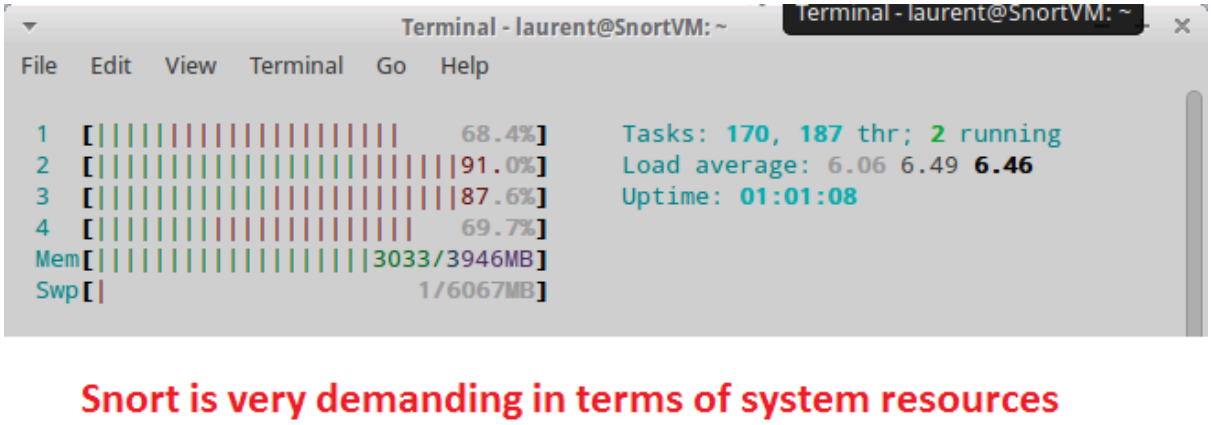


Figure 11: Snort uses a lot of system resources.

Assistance

Is it possible, before the Easter holidays, to reserve another server that I can experiment with for my MA thesis? The current server with Hyper-V installed on is a single boot installation, but for future work, I'll need a dual boot system and I would rather not format the current pizza server.

Any type of server (tower or pizza) is OK.