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.

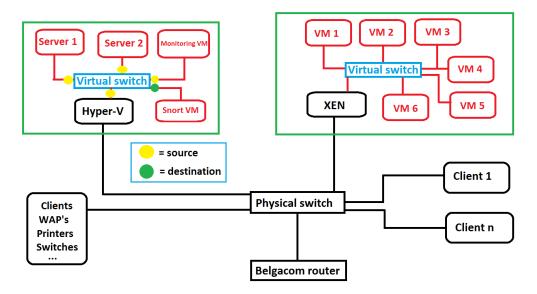
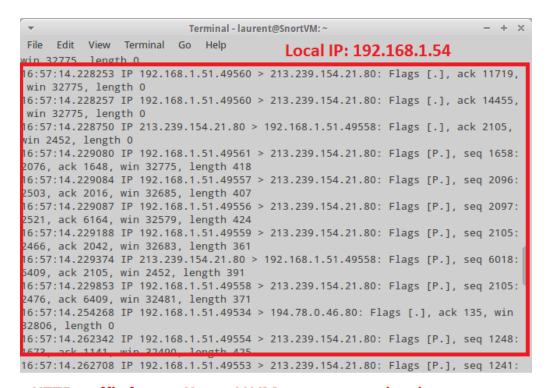


Figure 1: The modified and network setup.

• 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.

```
- + ×
                            Terminal - laurent@SnortVM: ~
File Edit View Terminal Go Help
                                                                                       Random traffic
                                                                                       from a Hyper-V
16:17:10.714022 IP 192.168.1.51.63052 > 94.245.121.253.3544: UDP, length 61
16:17:10.817723 IP 94.245.121.253.3544 > 192.168.1.51.63052: UDP, length 109
6:17:11.020619 IP 192.168.1.2 > 192.168.1.51: ICMP echo request, 1d 8420, seq 7
                                                                                       VM to an
 length 64
                                                                                       external IP
6:17:11.020922 IP 192.168.1.51 > 192.168.1.2: ICMP echo reply, id 8420, seq 7,
                                                                                       address
length 64
6:17:12.020299 IP 192.168.1.2 > 192.168.1.51: ICMP echo request, id 8420, seq 8
 length 64
 6:17:12.020451 IP 192.168.1.51 > 192.168.1.2: ICMP echo reply, id 8420, seq 8,
length 64
6:17:12.756242 IP6 fe80::1bd:87a6:9c94:f60f.54524 > ff02::c.1900: UDP, length 1
                                                                                       ICMP traffic is
6:17:13.020466 IP 192.168.1.2 > 192.168.1.51: ICMP echo request, id 8420, seq 9
                                                                                       captured
 length 64
                                                                                       from a Xen
 6:17:13.020857 IP 192.168.1.51 > 192.168.1.2: ICMP echo reply, id 8420, seq 9,
length 64
                                                                                       VM to a
6:17:15.754474 IP6 fe80::1bd:87a6:9c94:f60f.54524 > ff02::c.1900: UDP, length 1
                                                                                       Hyper-V VM
90 packets captured
90 packets received by filter
O packets dropped by kernel
                                      Local IP: 192.168.1.54
laurent@SnortVM:~$
```

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).



HTTP traffic from a Hyper-V VM to an external webserver

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.

RealTime Events Escalated Events										
ST RT	CNT 1	Sensor SnortVM	Alert ID	Date/Time 2015-03-19 21:25:19	Src IP 192.168.1.51	SPort 62799	Dst IP 192,168,1,46	DPort 2869	Pr 6	Event Message PADS New Asset - http Microsoft-Windo
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 (Crypt
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 (
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 (
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 SQF
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	-2-112	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 @dom
RT	4	SnortVM	7	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

Random traffic between various VM's

Local IP: 192.168.1.53

ICMP traffic generated by the added rule. From a Hyper-V VM to a Xen VM and from the Hyper-V host to the Xen host

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.

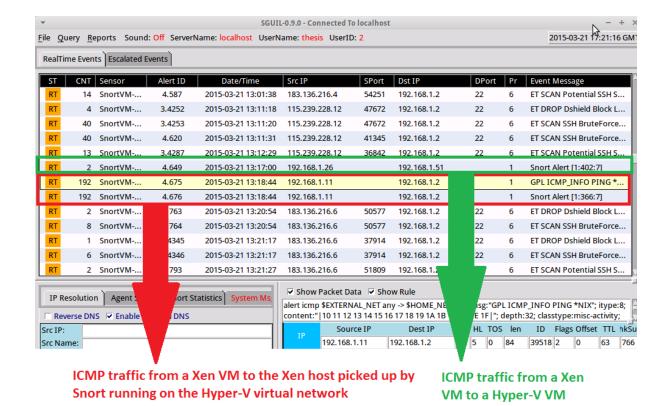


Figure 5: Traffic / intrusions between a Xen VM and a Xen host as well as intrusions between a Xen VM to the Hyper-V host.

RT	13 Sn	nortVM	3.4419	2015-03-21 13:56:44	192.168.1.7	192.168.1.11	1	Snort Alert [1:408:5]
RT	13 Sn	nortVM	3.4420	2015-03-21 13:56:44	192.168.1.11	192.168.1.7	1	GPL ICMP_INFO PING *
RT	13 Sn	nortVM	3.4421	2015-03-21 13:56:44	192.168.1.11	192.168.1.7	1	Snort Alert [1:366:7]
RT	841 Sn	nortVM	3.4422	2015-03-21 13:56:44	192.168.1.11	192.168.1.7	1	Snort Alert [1:384:5]

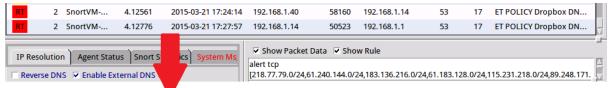
ICMP traffic from a Xen VM to the Hyper-V host and vice versa

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

RT	6 SnortVM	4.2153	2015-03-21 15:04:45	192.168.1.2	192.168.1.7	1	GPL ICMP_INFO PING *
RT	6 SnortVM	4.2154	2015-03-21 15:04:45	192.168.1.2	192.168.1.7	1	Snort Alert [1:366:7]
RT	6 SnortVM	4.2155	2015-03-21 15:04:45	192.168.1.2	192.168.1.7	1	Snort Alert [1:384:5]
RT	6 SnortVM	4.2156	2015-03-21 15:04:45	192.168.1.7	192.168.1.2	1	Snort Alert [1:408:5]

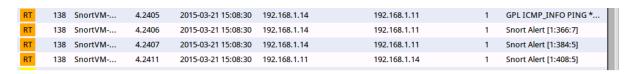
ICMP traffic from the Xen host to the Hyper-V host

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



Traffic from my laptop (1)2.168.1.40) to a Xen VM and traffic from a Xen VM to the router, all picked up by Snort running on the Hyper-V network.

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



Traffic between two Xen VM's captured 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

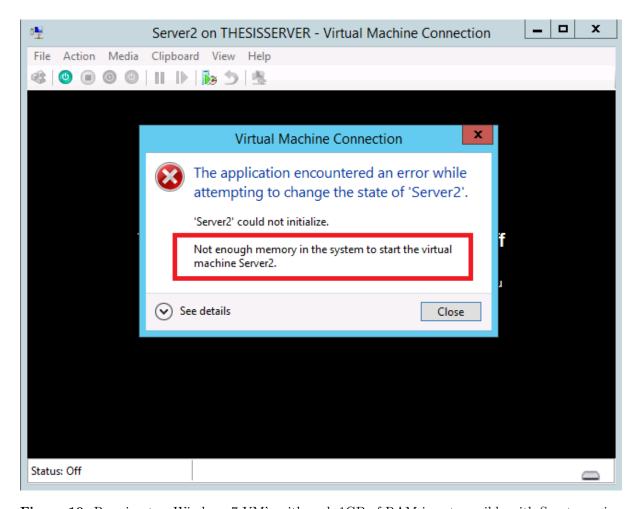


Figure 10: Running two Windows 7 VM's with each 1GB of RAM is not possible with Snort running on the same host with 8GB of RAM. Only one Windows 7 VM is able to run with a Snort VM on the same Hyper-V host with 8GB of RAM.



Snort is very demanding in terms of system resources

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.