Kernel Debugging Using Network on Physical Machine.

By Anand George

Why we need this setup while we have virtual machine?

- Virtual Machine kernel debugging is for sure convenient easy and a game changer.
- But it has many limitations.
- Most of them are para virtualized which means if you go for some very low level investigation things wont work out as you expect.
- I personally wont recommend do any lowest level debugging experiments with VMs.
- Very hardware specific commands like for instance ba (break on access) rarely works right with any VMs.

Via Network

- Fairly new at the time of this presentation.
- Make sure you debugger is latest at least windows 8 or 8.1 SDK/WDK I recommend.
- Make sure your target is Windows 8 or later.
- MS says host should be Win xp or later.
- This can open a great number of production kernel debugging opportunities which use to be a night mare with older ports (USB,serial,1394 etc)
- I will be using this setting a lot in coming presentations.

Steps

1. Make sure you have all the latest debugger and OS as per previous slide.
2. Make sure your target OS' NIC is in the list of "Supported Ethernet NICs for Network Kernel Debugging in Windows 8.1." in msdn.
3. Get the IP of host using ipconfig command.
4. Get select a port number between 49152 to 65535

Steps (cont)

5. Connect host and target via a router or switch.
   - In my set up I have connected “GreenDog” (host) and “violetcat” (target) which is win 8.1 via 2 network cables connected to a TP Link router.
   - Although the router is wireless I have used the wired ports. This wont work on wireless so far.
   - VioletCat’s Nic is Qualcomm Atheros AR8132 PCI-E Fast Ethernet Controller (NDIS 6.30)
   - Nic is sitting on the position - PCI bus 3, device 0, function 0
   - I would recommend remove additional NICs if you have more than one NIC on the target to avoid complications.

Steps (cont)

6. Disable all kind of firewalls on both endpoints.

7. Get on to target and type following command in Elevated prompt,

```
bcdedit /debug on
bcdedit /dbgsettings net hostip:w.x.y.z port:n
```

8. You will get a key which you need to save and transfer it to Host.

9. Reboot target

10. On the host computer, open WinDbg. On the File menu, choose Kernel Debug. In the Kernel Debugging dialog box, open the Net tab. Enter your port number and key (we got at step 8). Click OK.

Demo

TroubleShooting

- Make sure you have following all the step with out any single failure.
- Get wire shark on the Host and look for periodic UDP ping packets from target.
- Demo.

Summary

- KD of physical machine is recommended over VMs.
- Very convenient with new Network cable method.
- Two additional information we have discussed which is not there in msdn.

Thank you