CSCI 4271W : Lab 10 (Wireshark)

Part Two : Software Exploration :

This next part is a sofware exploration, that allows you to familiarize yourselves with the Wireshark tool. In order to make this possible the CSE-IT people were very generous to create remotely accessible linux virtual machines! At this point I should have emailed all of you a virtual machine host name, and password. Let me know ASAP via email (tsche043@umn.edu) if you have yet to receive this email.

These virtual machines are running on a segregated network, and you guys should have full root access to configure the VM's and also install packages. You guys should be able to remotely connect to the virtual machines from the lab or from elsewhere as long as you are connected to the University VPN. Since these machines are on a segregated network, and you will have special access, they will not have access to some university resources such as the shared home directories. However should you need to transfer files, you should be able to do so using something like scp. Bascially the virtual machines allow you to explore a tool like Wireshark in a "safe", and "controlled" environment where you can't actually do any real harm. Each virtual machine is running ubunut by default, and has 2cpu, 4GB ram, and 40GB disk space. The CSE-IT default is 2GB ram, but I negotiated 4GB to make things a little easier. CSE-IT also enabled desktop view for the vms so you can "see" the actual computer. The first step will be connecting to the virtual machines. There are two ways to do this.

Method I (Connecting via SSH) :

This is the easiest method. To connect with SSH simply SSH into the machine using your student account, e.g :

ssh student@csel-xsme-f22-csci4271w-25.cselabs.umn.edu

Where student is literally the word student (i.e., do not replace it with your x500 or things will not work for you). Replace the last part with the vm info I sent you via email. You will also need the password associated with the machine you are attempting to access, I should have included this in the same email.

Method II (Accessing the Machines via GUI) :

This method gives you full desktop view. It will require logging into CSE-IT's vSphere instance. The steps here are as follows,

1. Navigate to https://vsphere.cse.umn.edu/
2. Click the Launch vSphere Client button.
3. Log in with your internet ID and password.
4. When you log in, at the search bar at the top, search for the machine associated with your user id. Once again I emailed you this info on Monday.
5. On the page for your VM, there should be a "Launch Web Console" link which gives you two ways to access the console. I typically open a web console. This should bring you to a log-in splash page where you can log into a Gnome desktop.

Jack's Note : You may might encounter warnings about the site being insecure. This is because the SSL certificate for vsphere.cse.umn.edu is signed by CSE-IT

instead of a “trusted” 3rd party. You'll want to click near the bottom of the message which should say something like "More..." or "Advanced" and it should display additional options, one of which will say something like "Proceed anyway" or "Accept the risk and continue" , clicking that should take you straight to the login page.

Next Steps Using Using MahiMahi and Wireshark

Once you are connected to your virtual machines you will need to install Wireshark and also MahiMahi. MahiMahi is a very light weight network emulator developed by the good folks at M.I.T., I am attaching a link to the official website, and also a conference paper discussing it. Do the installs as follows.

$sudo apt install wireshark

This should work. If for some reason it doesn’t you may need to uodate APT by running these commands.

$SUDO APT UPDATE
$SUDO APT UPGRADE

Since these are virtual machines you all should have full root access, so you can use sudo for the installs. It might request your password, this is your **VM password**, not your normal login password. At some point in the install you want to make sure to enable superuser/root privileges (this is required for Wireshark to operate). Lastly you can simply launch Wireshark using the command.

$wireshark

This only works if you are using the desktop view for GUI. Otherwise there is a command line way to interact with Wireshark, called TShark, but I don't reccomend it.

Jack's Note : Running Wireshark is OS specific, I know how to do it for Mac, Solaris, Open BSD, and (Newer) Windows. If you want to know how to do it on one of these Operating Systems talk to me outside of lab…

Next you will need to install MahiMahi, do this as follows.

$sudo apt install mahimahi

mahimahi is basically a virtual NIC, so now you can run

$ifconfig,

And you should see several interfaces like the loopback, see if you can find the one for mahimahi.

Or if you are feeling more advanced you can try to simulate the wget attack on a virtual server. To do this might require you to run the following command

$sudo apt get apache2

You might need to play around with syntax.

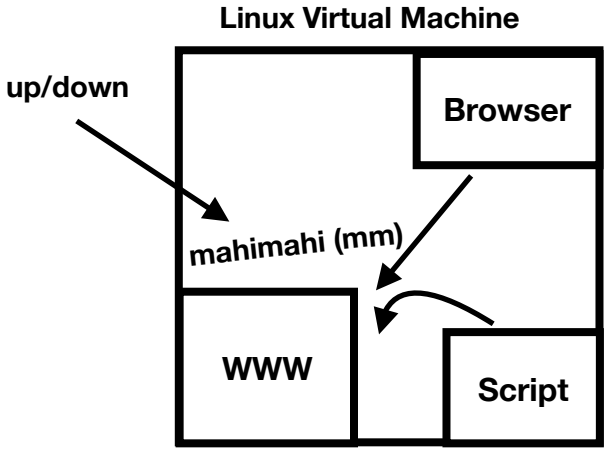

Figure I : Try to simulate the demo attack using mahimahi. You can experiment with writing your own wget script, and also weaken the link (by adding some delay for example).

References and Further Reading:

Official MahiMahi Website :

http://mahimahi.mit.edu/

Official Wireshark Docs :

https://www.wireshark.org/docs/wsug_html_chunked/

A Conference Paper Presenting MahiMahi :

https://cs.nyu.edu/~anirudh/mahimahi-sigcomm2014.pdf

Official Lua Docs (Wireshark is Partially Written in Lua):

https://www.lua.org/docs.html

Books on Lua (All available on Amazon, last I checked) :

G., S. L. F. (2009). *Programando em Ncl 3.0 Desenvolvimento de aplicações Para Middleware Ginga: Tv digital E web*. Elsevier.

* My addition is in Portuguese (Such a beautiful language), you can also find the same edition in English or Chinese, if you are so inclined.

Ierusalimschy, R., de, F. L. H., & Celes, W. (2006). *Lua 5.1 reference manual*. Lua.org.

Whitehead, J., & Roe, R. (2010). *World of warcraft programming a guide and reference for creating Wow addons*. Wiley Pub., Inc.

* Not specifically on Lua, but if anyone plays any World of War, it is a truly spectacular read.