

RichM Takes the Field

del.icio.us

Discuss in Forums {mos_smf_discuss:RichM}

EH-Net Welcomes Newest Columnist and Experiment

RichM is a real person. Everything contained in this column is real. This evolving column will live and breath with RichM's daunting new job. Your feedback helps decide the direction the column will take. It may be a bumpy ride, but it will be educational. Let's call this experiment Reality Web 2.0.

First installment

I wanted to write an article that would be a page turner, something that readers couldn't resist. Sadly, this is an article based in real life and not a Hollywood blockbuster. Try as I might, reality is not that sexy.

This office is a disaster, nothing is even close to secure. Its a miracle that our organization hasn't been featured in a prominent magazine for exposing sensitive information about our clients. I clearly have my work cut out for me, and the following is the first month in the quagmire that is my network.

Cleaning house

When I first arrived, I was greeted by a pile old paperwork, ancient computer parts and misc. crap. This of course was my desk and workspace. This was only the beginning. The filth was endemic of what was wrong and was the perfect representation of the old guard. The first thing I did was go through everything, shredding sensitive (unneeded) documentation and destroying old versions of software.

The next step was to identify all warez and destroy it. Warez should never be trusted for two reasons:

1. Due to their illegal nature they are more often than not un-patchable.
2. Warez often carry a hidden payload which could devastate your entire network.

Basically it's just not worth it, and it is against the CISSP code of ethics.

Mapping the network

Its always a good idea to know who or what is on your network. For those not familiar, the best application for this task is nmap. Nmap is a free port scanner available at <http://insecure.org/nmap/download.html>. If you are not familiar with nmap, I highly encourage you to learn all that you can about it. For the purposes of mapping the network I used the following command:

```
nmap -O 192.168.100.* > nmap.txt
```

This command allowed me to identify every machine on the network (192.168.100.*), the OS they run (-O) with the ports that are open on each machine, and finally dump the output to a text file (>>nmap.txt) that could be printed and used as a reference. Once I established who was supposed to be on the network, I was able to remove machines that were on the LAN that didn't necessarily need to be there. The final step I took was creating a spreadsheet with all the servers and IP addresses to track updates and network activity.

Expect the unexpected

Though not security related, I thought this occurrence would sum up the mountain of obstacles you can hope to read about in the coming months. The CTO had asked me to give him a hand troubleshooting a VPN issue. Apparently after more than two users connected to the VPN, the firewall would reboot and obviously the VPN clients were kicked out. We began to analyze everything and then turned our attention to the ports the fw was connected to. While investigating the switch we noticed something rather detrimental. A switch in which two T1's terminate and where the firewall also terminates was not a switch but a hub! Basically all the traffic generated on the hub was flooding every port and overwhelming the firewall causing a DoS. After ripping out the hub as fast as humanly possible and installing a switch, the problem was gone. Surprise, surprise.

This article (as was this entire month) was a chance to lay a foundation and create a work environment that will be more cohesive to the changes I plan on making. As I continue, the articles will be more technical and less narrative. Please feel free to post ideas or approaches that will help to shape this column.