Andy Graybeal CYBR 1100 Week 1 23, August 2025

Case Project 1-1

The Couriers

I used to work for the University of California – Santa Cruz's central IT Dept back in the late 90s and early aughts. One of the first responsibilities given to me was to run their online classes. There were no complex Learning Management Systems back then. It was a proprietary system called WebCBT. WebCBT was loaded with what we called Computer Based Training modules, or CBTs. The modules had the latest IT certification information, like Cisco and Microsoft and all the other popular certificates back then. WebCBT ran on top IIS 4.x on NT 4.0 Server. In my home lab, I was familiar with running NT4.0 with IIS4 safely behind my NAT'd network. I wasn't aware of the security updates that I should have run… which is honestly ridiculous on my part. At the time, each machine on UCSC's network was given a public IP address, and we weren't behind a firewall. Anyway, I was an idiot and didn't run any updates to IIS.

Either the FTP server that was included with IIS had an open account or could be hacked to have an open account. Someone eventually found it and loaded the latest "WAREZ" or pirated software packaged by notable pirates in the WAREZ scene. UCSC had fat pipes and that hard drive had plenty of space. If I remember correctly it was a Compaq branded server box, with a RAID array. So whomever was sharing the illegal software had bragging rights on having a fast pipe and could move software quick.

I don't remember what lead me to find the issue, maybe it was that the hard drive was full or something like that. Luckily I had the backup client software scheduled and working correctly. I assumed none of the data regarding the CBT had been messed with. I myself was a part of the WAREZ scene. I was known as a courier. And this is what every good courier did. Find places to move WAREZ. The group I was involved in was organized on secret chat channel on EFNET. And having done the same thing, none of us cared what was being legitimately served on the machines we used.

Luckily the CBT server was the least used server the department ran. It's downtime went under the radar and any users that might have been effected were silent. I turned the machine off, wiped the data and reloaded Windows and IIS. This time, making sure that I got a blessing from a senior IT guy regarding properly securing the server.

I loaded the WebCBT app and then brought the CBT Modules and user data over from tape. Our tape system was notably awesome. I forget the specifics right now but each server ran a backup-client software and we had a central backup server with a small warehouse of tapes, on and offsite.

I don't remember any policies regarding breaches and honestly I was too embarrassed to tell anyone, let alone mention it to my supervisors. I will never forget the surge of blood pressure, distraught feelings and absolute embarrassment. I remember a short meeting with upper-management… but it was all a blur and I felt so terrible. Anyway.. I wasn't fired, they still kept me in charge of that server and handed even more responsibility my way.