

Episode Eight: Still Waters

Robert G. Ferrell 2001-07-10

Chasing the Wind, Episode Eight: Still Waters

by Robert G. Ferrell

last updated July 10, 2001

Construction of the new Acme Ailerons facility was over budget and behind schedule. The company chosen to replace the original contractor took over smoothly and efficiently. They seemed competent, organized, and consummately professional. Not only had they agreed to finish the job for the same price as in the original contract, they promised to work around the clock to meet the completion deadline, despite the fact that the project was a good three months in arrears.

Bob was pleased at the sudden change in fortune surrounding the project, but in the corner of his mind where his training and experience as an intelligence officer resided, a little alarm was going off. He could ignore it, but it would not be silenced. He told himself that he was just being paranoid, and that there was nothing to be concerned about.

[Beep, beep, beep]...his brain obviously wasn't buying it.

Whatever the case, the new contractors certainly seemed to have none of the bad luck that had plagued their predecessors. Supplies arrived on schedule, employee sick calls were rare, and each inspection went flawlessly. Acme management, not to mention the GSA and DoD, were overjoyed. Bob was gratified that things were back on track, but he still couldn't shake the seemingly irrational sense of misgiving. Without any tangible evidence of misconduct, however, he knew better than to voice his discontent to anyone in his chain of command.

One morning a larger than usual crew showed up at the site. The general supervisor explained that a number of tasks were due for completion that day, and the need for several interoperative systems to be brought online simultaneously necessitated the large crew. At about three that afternoon, a small fire broke out near the employee cafeteria. The fire was contained by the contractor crew within a couple of minutes with very little damage sustained. However, policy dictated that the fire department be summoned. For about an hour and a half every member of the government overseer and Acme management teams on site were involved in the inspection and debriefing near the cafeteria.

Unbeknownst to any of them, a small but highly efficient crew was taking advantage of the distraction to install some 'undocumented' devices in the fiber optic lines running under the floor into the main computer center. They were small cylindrical inline units, scarcely noticeable when installed, and took less than fifteen minutes to position and hide in the vast collection of cabling that ran in dozens of conduit clusters leading into the computer center complex.

The fire department completed their investigation and declared the fire to have been caused by a short circuit in a paint sprayer compressor. After the inevitable reams of paperwork had been filled out and submitted in quadruplicate to the various agencies and officials, Bob sat in the half-finished cafeteria with a cup of coffee and reviewed the day's events. His intelligence training just wouldn't let go - something was going on here. He didn't believe in coincidence or luck, at least not where matters of national security were concerned. He decided to go for a little walk and think things through.

Ian was tired but happy. He had finally gotten his new LAN configured the way he wanted. He was working part-time for a local computer store now, and his earnings, combined with the employee discount, had enabled him to pick up a nice hub and a small remanufactured router. He installed these in his room and connected all four of his computers to the new LAN so he could test his code under different environments and operating systems. He'd also gotten hold of an external SCSI hot swappable drive housing, which made it possible for him to keep several identical hard drives with different operating systems on them at the ready. All he had to do to go from Red Hat Linux to FreeBSD was swap out the drive and reboot. All in all, he could test three different incarnations of Linux, two commercial and three open flavors of Unix, three Microsoft operating systems, and even BeOS. Life was looking better and better.

Douglas looked up from his computer and noticed the time. He was supposed to meet in the lobby in fifteen minutes for a tour of the new building. It wasn't ready for occupancy yet, but the anticipated move-in date was only two weeks away. The VP for Engineering wanted to make certain that everyone on the Bellatrix project was fully prepared, so that the downtime associated with the move was minimized. Douglas was usually a rather sedate individual, being more interested in engineering physics than smoozing, but he had to admit experiencing a certain sense of excitement at the thought of his new state-of-the-art laboratories. From his

perspective, testing could start as soon as he was moved in. He had run every conceivable simulation so many times he could almost spit out the modeling profile data for each of them by memory.

After the tour, Douglas sat at his non-classified workstation updating his personal Web sites. They weren't personal in that they displayed his favorite music or pictures of his dog, they were personal because they did not directly represent Acme Ailerons, its products, or services. They were, however, closely related to what Douglas did for a living, as they provided a variety of engineering utilities, links to current standards bodies and working groups, and the headquarters site for a local users' group for the principal Computer-Aided Engineering package that Douglas made use of in his job.

He hadn't received specific written approval from his manager to operate the sites, primarily because he had put them up before the company had any formal policy on such things. In fact, Douglas's oldest site predated the Acme Ailerons site by over a year. According to his logs, more two thousand professionals in the international engineering community had his sites bookmarked, and he got around 400 page views a day. Not one of the top hundred Web sites by volume by any means, nevertheless one he was dedicated to maintaining.

It made him feel as though he were doing his part to support the free and open sharing of information among the Web using public. He was careful never to let working on his sites interfere with his job, and usually did his updates and other changes either before or after his official duty hours. Truth be told, no one at Acme seemed even to have noticed Douglas's sites on their servers. All that was about to change, however. The Engineering Department had just hired their own network manager.

Deanna was an attractive woman. That was Jake's first impression of her, at least. After a more complete inspection, he upgraded his opinion to *remarkably* attractive. He had no idea what she thought of him, of course, but hope springs eternal...

Wresting control back from his metencephalon, Jake switched on his professional mien. Deanna noticed the subtle change of direction and was silently impressed. As a consultant in the IT industry, she encountered unattached males of his type on a daily basis. Most didn't have the character or poise to snap out of appraisal mode before she was offended, or at least annoyed. Jake managed to sneak in under the wire on that score.

Over the next few hours, Jake would get a taste of Deanna's formidable intellect and her keen analytical skills, as well. By the time she had gone over every item on her Solaris secure installation checklist with him, he'd more or less forgotten her physical charms, and was instead trying to keep up with her mentally. She was very thorough, and he sensed that she knew exactly what she was doing.

They spent what seemed like hours just going through all the scripts in the `/etc/rcx.d` directories, stopping running scripts, setting them not to start on boot up, and testing the effects. They made sure the boxes weren't being used as routers, edited `/etc/passwd` and `/etc/shadow` to remove unnecessary default accounts, modified the search path and umask for root, and drastically reduced the number of services running under `inetd`. Next they installed TCP Wrappers, OpenSSH, and Tripwire, as well as Iplog and Snort. Deanna gave him her own handout on writing rules for Snort, and spent some time explaining and demonstrating the process. To wrap things up, they set TCP initial sequence numbering to strong, disabled IP forwarding and source routing in `/etc/init.d/ineinit`, set logging to a remote host that Jake had provided for that purpose, and removing unnecessary `suid` and `sgid` bits from system files. By the time they finished, it was almost five.

As Deanna was packing up to leave, Jake tried to organize all the notes he'd taken and materials she'd provided him. He was trying desperately to keep it all from ending up as the seed of yet another deep pile of cellulose debris on one of his already densely populated work surfaces. Deanna watched him with a sort of detached amusement.

"Why don't you get some file folders for all that?" she asked, arching her eyebrows.

Jake looked a little sheepish, "I've got some - over there, in that drawer," he winced and cleared his throat, "I can never find enough time to print out the little labels for them." He trailed off, embarrassed.

She looked at him and laughed. "Well, they say honesty counts for something."

Jake really had no idea why he did what he did next, but something told him the time was right. He suddenly looked Deanna straight in the eyes and asked if she would have dinner with him. He was immediately overcome with shock at being so forward, so much so that it took a few seconds for it to register when she just as suddenly said yes, she'd love to.

Fortunately for Jake, it wasn't necessary for him to be anywhere or do anything for the next few minutes, as this little exchange had left his head spinning. Deanna smiled, shook his hand, and left his office, her own powers of ambulation seemingly unaffected.

Sitting in her car on the way home, Deanna wasn't sure why she'd said yes. She'd never succumbed to temptation with a client before, not that many of them had been courageous enough to ask. It was something to do with Jake's eyes...

Douglas put the phone receiver back in its cradle slowly, without any conscious awareness of the action. He was stunned by the words that had issued from that receiver, namely, that the new engineering network manager had ordered him to take down the Web sites he hosted on company systems. According to the network manager (who's name, Douglas seemed to recall, was something short and vaguely derisive) people hitting those sites were using company bandwidth that could be put to better use. Any site not officially sanctioned by Acme Ailerons and containing material not dedicated solely to the company's interests was henceforward banned from using any Acme resources.

It wasn't that Douglas couldn't see the logic to this argument, or that he disagreed with the sentiment, close-minded though it may have been. It was the abrupt, coldly clinical way a stranger had called him up out of the blue and, without even discussing the situation, ordered him to negate several years' worth of his life.

Two of Douglas' sites had won awards for fostering open sharing of information in the international engineering community. Douglas had received over two hundred e-mail messages of thanks and praise from every corner of the globe. None of these points seemed to matter to the voice on the other end of the line, however. In fact, he seemed to shrug them off the way a dog shakes off a bath. Douglas let the simulation he was running abort on an error and crash the system. He just wasn't able to think clearly at the moment.

Douglas opened his e-mail. The first message he came to was a forward from a friend of his who was a systems administrator for a local community college. As he read, Douglas felt his shock and sense of betrayal gel rapidly into anger. The forwarded message was a post to a city-wide computer administrators' newsgroup. It made a number of uncomplimentary and totally baseless charges against Douglas, accusing him of deliberately circumventing the company's

policy on personal Web sites. It implied that the reason Douglas hadn't asked for permission is that he knew it would be refused. The rant went on to suggest that the poster of the message was going to institute sweeping changes at Acme Ailerons in order to wipe out this "near-criminal misuse of company resources." It was signed:

A. Asworthy
Network Manager
Engineering Technologies Department
Acme Ailerons

Douglas punched the print hotkey on his e-mail program and stood there seething as the libelous document came spitting out of his DeskJet. This was no longer a misunderstanding that could be cleared up by a friendly meeting of the minds. This was war.

To read **Episode Nine: Smoke and Mirrors**, click [here](#).

Robert G. Ferrell, CISSP, is an Information Systems Security Officer in San Antonio, Texas. He is also active as a [Perl Monger](#), an Internet Technologist, and a [literary humorist](#). He has been involved with (primarily Unix) systems programming, administration, and security on and off since 1977.

Relevant Links

[Chasing the Wind Episode One: No Place to Hide](#)

Robert G. Ferrell

[Chasing the Wind Episode Two: Raising the Stakes](#)

Robert G. Ferrell

[Chasing the Wind Episode Three: From Out of the Blue](#)

Robert G. Ferrell

[Chasing the Wind, Episode Four: Through a Glass, Darkly](#)

Robert G. Ferrell

[Chasing the Wind, Episode Five: The Devil in the Details](#)

Robert G. Ferrell

[Chasing the Wind, Episode Six: The Gathering Storm](#)

Robert G. Ferrell

[Chasing the Wind, Episode Seven: An Ill Wind](#)

Robert G. Ferrell



[Privacy Statement](#)

Copyright 2006, SecurityFocus