

Episode Seven: An Ill Wind

Robert G. Ferrell 2001-06-13

Chasing the Wind, Part Seven: An Ill Wind

by *Robert G. Ferrell*

last updated June 13, 2001

Jake wasn't coping too well with life, the universe, and everything.

He had gotten to work on time, and given that it was Monday, this was cause for some small amount of self-congratulation. The week was looking as though it might shape up to be a good one. Scanning his email, he saw a message from one of his friends. He opened it, and it contained only one line: a URL. Jake obediently clicked on the URL (first making sure it contained no odd characters or anything else overtly suspicious) and read midway through the first paragraph. His shoulders slumped and he felt himself droop involuntarily in his chair. He closed his eyes for a moment and then opened them slowly, one at a time, as though if he gave the words a chance, they might rearrange themselves into something less objectionable. It didn't work.

Well, so much for good omens.

It took Jake at least an hour to come to terms with the news that Douglas Adams had died. Adams was only 49. It reminded Jake strongly of when one of his best friends, who was 50 at the time, had passed away suddenly a little over 4 years previously, also of a massive heart attack. Jake thought of many people he knew whose untimely demise would have been less of a psychic blow. Death was not only unfair, it was downright arbitrary.

As if to help take Jake's mind off the tragedy, Michael in Receiving phoned at that moment to tell him that there were four largish crates on the loading dock. It took a few seconds for the message to sink in, but when it finally did Jake came partially out of his philosophical coma. "Uh, great," he said, shaking his head to clear away some of the cobwebs, "Can you have 'em hauled down here?"

Jake sat down heavily. Although he was still in shock from the bad news, a part of his mind was reacting to the incoming equipment. "Must be the new Sun boxes," he muttered, almost but not quite inaudibly. As he sat and planned how he was going to incorporate the Internet Services Cluster, for that was to be the function of the newly arrived servers, into the existing network

architecture, he suddenly had an idea that cheered him, albeit not much. He would name the four new servers in honor of the late Douglas Adams.

Douglas (the live engineer, not the author, whom we have now established is deceased) tapped his fingers on the desk in a kind of thoughtful fidget. He was reviewing the latest test results obtained on one of the modular components of Project Bellatrix, and what he saw made him at once excited and uneasy: excited, because he was beginning to believe that this thing might actually be possible, and uneasy, because he still didn't understand how he could possibly think that. He'd never entirely shaken the feeling that this project was based less on physics than metaphysics. That is not a naturally tenable position for an engineer.

He ran the computer simulation once again, and watched the numbers being displayed in neat little bar graphs in the upper left hand corner of the screen. Simulations were about all he could manage right now, until the new laboratories were finished. He thought about the computers he was using for the exercise: massive parallel processors involving banks of over two thousand 1.5 GHz CPUs. It was a lot of number-crunching power; almost more than his mind could comfortably encompass. Yet, according to top secret Secure Compartmentalized Information reports from the Bellatrix Computational Team, one of the byproducts of the gadget he was building would be quantum computers, computers capable of data processing at several orders of magnitude beyond anything currently available. Several orders of magnitude beyond mind boggling - he didn't like to dwell on it.

Douglas sighed, and switched off the secure computer. He went next door to his "insecure" office and logged into his normal workstation. Maybe a little Web surfing would help to unknot his jumbled cortex.

Ian was sweating. He'd made a careless mistake while defacing a corporate Web page the previous evening, and was now embroiled in a nerve-racking cat and mouse game with someone who seemed to anticipate his every move. He was being gradually backed into a corner, and getting a little scared.

Every time he switched to a different proxy host to try to elude pursuit, his assailant followed

within a few seconds. Ian could see someone at that same IP address log in just after him. How in the devil did he know where Ian was going? He couldn't have time to set up a sniffer at each new box; sometimes Ian stayed there only long enough to type in a new dotted quad. It was almost as though the person chasing him could see over his shoulder. Almost as though his software knew what he was going to... Ian froze. He moved his fingers over to a different keyboard without taking his eyes off the screen. He was using a hacker tool called "nVader" to navigate between open proxies and find or start root shells on them when possible. Still watching the netstat data on the proxy, he typed `# strings /usr/sbin/nVader | egrep`

Ian paused while he cut and pasted the IP address of his pursuer onto the end of the command, then hit enter. It was there. Ian sat up straight in his chair and ran the program through a crude disassembler. He scanned the code until he found the line with the IP address in it. A little more reverse engineering and the answer suddenly hit him. It was like being smacked in the forehead by a large brick with polka dots all over it; it hurt like heck but it was nonetheless vaguely amusing. Maybe it was the subtlety of the joke, maybe it was just from sheer relief, but whichever the case, Ian started chuckling, a chuckle that soon gave way to a full fledged semi-hysterical laughter. There was no pursuer; nVader was generating the spurious login itself. He'd been had, and royally: the exploit tool was itself trojaned.

There is no honor among thieves, nor security among hackers.

Bob and Vijay, from Acme's Assets Protection department, stood in a partially finished hallway with a blueprint and a thermos of coffee each. They had tight, determined sets to their mouths and they glanced around at the dangling fixtures, half-painted sheetrock, and floor tiles stacked against the wallboards with what could only be described as naked frustration.

The new facility was two months behind schedule and suffered from numerous "accounting inconsistencies" that the Defense Department and the General Services Administration, not to mention the Defense Contractor Auditing Agency, were "looking into." There were a lot of people hired to work on Project Bellatrix who sat in hastily rented offices playing solitaire on their newly-purchased state of the art workstations, waiting for this building to be declared ready for occupancy. That seemed to be as likely as the imminent democratization of China.

"Jeez, look at that," growled Bob, pointing to one of several gaping holes in the suspended ceiling, "That Cat-5 isn't even in a cable tray." Vijay followed Bob's finger up into the cavernous

crawlspace above their heads. "Are you even sure," he asked after a moment, "that it *is* Cat-5?"

Bob blinked at Vijay and shook his head: "Don't give me any worse nightmares than I'm already having."

"I'm sorry to hear that you aren't sleeping well, my friend," replied Vijay, softly. He was kneeling next to a row of rectangular holes gouged out of the sheetrock. "Perhaps this would not be a good time to point out that they seem to have gotten the Ethernet and telephone drops reversed. Also, didn't I hear you say at a facilities planning meeting that all the workstations in this wing were supposed to have fiber to the desktop?"

Bob vowed not to go to sleep again until the building was finished, and finished correctly. He knew deep down that it was an unnecessary pledge.

"We have submitted our bid through the pre-established channels. The construction is approx. 52 days behind schedule; by now there should be very little remaining dissension among target management concerning our proposed contract modifications. Plan is proceeding as predicted." Baseball cap rubbed his bald spot and hit the 'send' button on his email program. The triply encrypted message sped off across, or rather, underneath, the Atlantic on its nefarious mission. Here in the good ol' U.S. of A., he decided, it was Miller time. The collection of empty bottles aligned in various odd patterns on every horizontal surface in the room suggested that this was not his first encounter with that thought.

```
# reboot -r
```

Jake sat back to watch the phosphor characters flicker and dance in their electronic ballet. This was the last of the configurations he needed to make; hopefully the high availability array would be fully functional once this machine made it back to multi-user mode. He had assigned the host name `zaphod.acmeaileron.com` to this box, to go along with `trillian`, `arthur`, and `fenchurch`. All were names concocted in the fertile brain of Douglas Adams and adopted by Jake in his honor. Jake was strangely satisfied by this small tribute. It made him feel the emptiness of losing someone whom he had considered a friend, though they had met but once at a book signing and hardly spoken, a little less keenly.

Jake glanced at his watch and suddenly remembered that he had a visitor coming in less than half an hour. Deanna somebody, from that security company, whose name he couldn't remember because it sounded like a law firm, would be here soon to make sure he had implemented her security recommendations. Jake didn't really feel that he needed anyone checking up on him, but anything that kept his machines out of the statistics and his rear end out of a sling couldn't be all bad. Besides, he had no real choice in the matter.

Ian was struggling with offsets. After a lot of false starts, he had managed to feel his way through his first original buffer overflow exploit in C; now he just had to find the right place to insert his shell code into the memory of the target machine. Ian still didn't understand the way memory worked as thoroughly as he would like, but he had a couple of well-written papers on the subject--one he got at the hacker convention and one on the Web. If he read through them enough times, he figured, they would eventually sink in.

His exploit took advantage of weak bounds checking on a user input string in a widely-used remote login utility. If he could figure out the right length of "padding" to put in before the code he wanted to insert, he could overflow the area in memory allocated to that part of the program and trick the computer into executing arbitrary instructions; in this case, starting a shell with root privileges running on a high-numbered port. The problem was that in order for his code to overflow the buffer, he had to know both how big that buffer was, and where it started in memory. To find those magic numbers at his level of expertise was a time-consuming process of trial and error. Still, time isn't really a problem for a 15 year-old boy who spends every free moment at his computer. Besides, he could automate some of the procedure using tools he'd managed to accumulate here and there.

Merv was a facilities engineer with a lot of contacts. He was a large, cheerful sort who seemed to make friends just about anywhere he went. Through his elaborate network of acquaintances, he was often privy to some pretty sweet deals. One of those deals involved getting a very expensive piece of computer-aided design software, and a dedicated computer on which to run it, *gratis* from a friend who was upgrading his business systems and who owed Merv for helping to renovate his kitchen.

Merv brought his new stuff to his office at Acme Ailerons, since he could make best use of it

there. He didn't have a spare Ethernet jack in his work area, so he scrounged a little five-port hub from the spare parts room at the end of the hall and found a cable to plug into it. After getting the system set up as best he could, Merv turned it on. As it booted, it asked him a series of questions about the network environment. He really didn't know the answers, so he accepted the default where this was an option and made something up where it wasn't. Surprisingly, the system came up without a hitch.

Pleased at his technical accomplishment, Merv turned off the monitor to save energy, but left the CPU on. "No harm in leaving it running," he thought, "And I've read somewhere that powering systems up and down too often actually shortens their functional life."

"Heck," he said to himself as he locked his office door for the evening, "this networking stuff isn't as hard as people make out - there's really not much to it at all."

Fate and the bad guys would soon beg to differ.

To read **Episode Eight: Still Waters**, click [here](#).

Robert G. Ferrell, CISSP, is the Information Systems Security Officer for the National Business Center of the U.S. Dept. of the Interior. 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

[Privacy Statement](#)

Copyright 2006, SecurityFocus