

Episode Thirteen: Cabbages and Kings

Robert G. Ferrell 2001-12-27

Chasing the Wind, Episode Thirteen: Cabbages and Kings

by *Robert G. Ferrell*

last updated December 27, 2001

Jake sat at the incarcerated Merv's terminal and scratched his head. The military security people had told him that this box was sending bursts of (presumed) classified data to an undisclosed location in another country. Okay, except that this segment of the network had no physical attachment to the secured net. In fact, the segment into which this box was plugged wasn't even on his network map. That was a little disturbing, but not entirely surprising, since the data telecomm documentation he'd inherited from his predecessor was a little on the skimpy side. Facilities wasn't exactly the center of the Acme Ailerons computing universe, after all. Jake felt he had a pretty decent grasp of the overall topology of the networks under his control, but every now and then something like this popped up to remind him that he was a bit shy of omniscience.

Still, he was puzzled and concerned that someone could be compromising a top secret project right under his nose. He gathered all the relevant data he could about the network interface card and cabling; the hard drive had been removed by the feds for forensic analysis. The IP address being used by the box was one belonging to a DHCP pool and wasn't supposed to be assigned statically. Well, he thought grimly, this wasn't the first time policy and reality had been slightly out of alignment - it was just the most significant.

Baseball cap was running scared. He had no functional computer, no data, and his pipeline back to the organization seemed to have been severed. He was alone in a hostile country, a country which had once cherished him as a native son until he had turned his back on it and plotted against it.

He didn't know what had happened, but somehow his cover had been blown. It seemed almost inconceivable: he had taken every precaution, observed every protocol. Nevertheless, he knew a stakeout when he saw one. They were waiting for him. His only chance was to leave the building unobserved, or at least unrecognized. He arranged for a friend to pick him up two

blocks away, at a preset location that he referred to on the phone by a code name, to confuse the inevitable phone tappers. Now he just had to figure out how to get there.

Bob cradled his sheath of blueprints under his arm and stepped off the parking garage elevator. He was beginning to feel as though he'd never retired from Army Intelligence. He kept having flashbacks of little plywood-paneled hole-in-the-wall offices in which he'd spent months at a time, poring over photographs and intercepted dispatches, looking for code words and hidden meanings. He could smell once again the peculiar combination of dust, photographic developer, dried perspiration, and insect repellent that permeated his working days.

His vivid reminiscences were interrupted by Will's voice. It took Bob a moment to refocus his thoughts on the present. Will had been a part of that past, and the juxtaposition disoriented him briefly.

"Glad you could make it, Bob. Let's step into my office over here and take a look at those diagrams."

Will was congenial, but there was an undercurrent of urgency that served as the final impetus to pull Bob back into the here and now.

"Sorry I'm a little late. It took me a while to find some of these plans," he apologized, "I had them sort of misfiled."

"Not a problem," replied Will. He led Bob into the back of a panel truck, the inside of which was decked out with an impressive collection of electronic gear and soundproofing.

Bob whistled through his teeth. "Nice setup," he said appreciatively. He noticed several small monitors in various locations. "So, you guys get ESPN in here?"

One of the agents smiled and replied, "When it's part of the mission, you bet."

Will chuckled. "We're equipped to monitor just about anything we need to monitor, including broadcast TV, digital satellite, microwave, wireless, IR, Bluetooth, you name it. A little better than in your day."

Bob shook his head. "Boy, that's the truth. I remember trying to read lips with binoculars

through a fogged-up window and straining to hear what was going on below you using a ceramic mike lowered into a ventilation duct from the attic crawl space. Now you sit in a temperature controlled van and watch the World Series." After a slight pause he added, "That's what I call *progress*."

Will laughed and spread out the secure network topology map. He studied it intently for a full minute.

"What is it exactly that you're looking for?" Bob finally asked.

"I have a sneaking suspicion that there's something on your network that you don't know about," replied Will, without looking up from the map, "and I'm trying to figure out where it might be hidden."

Bob's forehead wrinkled. "What do you mean 'something I don't know about?' You and I watched every component of that thing get screwed on, plugged in, and locked down. How could there be anything I don't know about?"

"Your sysadmin -what's his name? - Jake told me that the box that was transmitting the data bursts wasn't on the secured net. If that data was classified, then, it had to be relayed to facilities somehow. I'm betting there's a little wireless device somewhere in these miles of cabling."

Bob considered this. "But the cabling is almost entirelyly optical," he objected, "you can't just waltz in and splice a transmitter into fiber. The network management software would notice it immediately."

Will looked up. "Not if it was installed at the same time as the network itself."

Douglas watched the numbers on the laser power meters count up. He'd realized that not only could he control the test system from his office, he could even get power to the lasers by routing the power supply telemetry feed through his master control board. Since the lasers were hard wired into an ultra high precision power supply unit that was computer controlled, rather than simply plugged into a wall socket, with a little adjustment to the software he could switch the power on and off from here. Douglas chuckled when it occurred to him that he had

just 'hacked' the system. Jake would be so proud...

Once everything was up and running, and he had tested his data relay channels several times to make sure he had enough clean bandwidth for effective data capture, Douglas decided to program a low level test before trying anything fancy. He still wasn't entirely confident with his ability to make reproducible runs, so a simple set of calculations would be a good warm up. He chose a minor problem, like figuring out the first thirty Mersenne primes. He already had the mathematical model representing this problem mapped out, because looking at Mersennes was one of his hobbies. All he had to do was modify it a bit to be compatible with the Bellatrix data input schema.

A few tweaks here and there, and he was ready to rock. Douglas checked all his parameters one final time, then pushed the input button. The answer came spitting back before he even finished taking his hand off the button. Must be a problem somewhere, he thought. He punched up the 'view results' screen and stared open-mouthed at the monitor. There were all thirty of the numbers, correct and in sequence. It had taken Mankind over 500 years from the discovery of the Mersenne prime to calculate the first 30, and this machine had done it in - he checked the run stats - 12.3 milliseconds. He sat back in his chair and exhaled slowly while he pondered the implications of this thing he had helped to create. It was so fast and so powerful, and it operated in the mind-twisting realm of quantum physics, where events happened before they were triggered and could be detected before they happened. Douglas sat up abruptly, stunned by his own sudden fabulous idea. He scooted over to his "non-secure" terminal and surfed to the State Lottery site. He downloaded the database of all the winning numbers that had been drawn in the Lottery's ten-year existence. With this data on a floppy, he rolled back over to the Bellatrix terminal. He cracked his knuckles, flexed his fingers, and started churning out modeling code.

The first inkling Ian had that someone might be looking for him was a posting on one of his hacker groups by a regular known as MsThang, who worked for a large ISP. She said that federal agents had come in and installed a 'black box' on one of their routers that was looking for specific traffic. She had managed to wheedle one of the spooks into telling her that they were trying to track down someone who had sent a message to the feds about a computer that was transmitting classified information to another country. Ian was taken aback when he read this, but decided that he was being a little paranoid assuming it was himself to whom they were

referring. All the same, he felt it prudent to assume a low profile for a while. No sense taking unnecessary risks.

Meanwhile, he was continuing his self-education on firewalls and network architectures. As he delved more deeply, he became increasingly aware of his limited knowledge of TCP/IP, which prompted him to dig up as much information on that critical set of protocols as he could. He cast around the Net for information, and eventually decided to go straight to the horse's mouth; i.e., to the Internet Engineering Task Force, more specifically, to RFC 1180, *A TCP/IP Tutorial*. He was particularly intrigued by the multiplexing/demultiplexing model, which explained the sometimes-confusing IP header construction process more clearly than anything he'd so far encountered. While he knew that each layer in the network added or stripped header information from a frame depending on whether it was coming in or going out, he hadn't fully grasped the reasons for this. The multiplexing model dictates to which transport module in the TCP/IP stack a frame is passed. This in turn allows the same data to be transported by a variety of services, depending on the type field in the protocol header. It was kind of like sending a gift to someone. First you wrap the gift, then you package it in a box for shipping. Once it's in a shipping container, you can choose from a variety of methods for getting it to its destination, without changing anything about the box itself. Nifty.

While reading the part about how Ethernet keeps packet collisions to a minimum, CSMA/CD (Carrier Sense and Multiple Access with Collision Detection), Ian came across these sentences:

```
Everyone in the room has equal capability to talk (Multiple
Access), but none of them give lengthy speeches because
they are polite. If a person is impolite, he is asked to
leave the room (i.e., thrown off the net).
```

Ian chuckled. "Maybe that was true in 1991 when this RFC came out," he said out loud to no one in particular, "but it sure isn't the ways things work these days." If it were, he thought, the Internet would be a vastly different place, not to mention virtually uninhabited.

"I think we've found a match," said the voice on the other end of the phone, "Several misspelled words and odd capitalizations in newsgroup postings strongly resemble those in the suspect message."

The OSI agent sat up with sudden interest.

"Yeah? What's the hacker handle used in the postings?"

"Let's see...that would be i-R-8-d-0-g."

"Okay, let's have a look at the headers and see if we can't figure out where this 'irate dog' holes up."

"Looks like they were posted through one or more proxies. We'll probably need a 2703(d) for each hop."

"Check. Give me the relevant info and I'll get right on it. We ought to have this kid in custody by next week, if all goes well. And you know what?"

"What?"

"I'm really looking forward to it."

To read **Episode Fourteen: A Bird in the Hand**, click [here](#).

Robert G. Ferrell, CISSP, is a Systems Security Specialist 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](#)

[Chasing the Wind Episode Two](#)

[Chasing the Wind Episode Three](#)

[Chasing the Wind Episode Four](#)

[Chasing the Wind Episode Five](#)

[Chasing the Wind Episode Six](#)

[Chasing the Wind Episode Seven](#)

[Chasing the Wind Episode Eight](#)

[Chasing the Wind Episode Nine](#)

[Chasing the Wind Episode Ten](#)

[Chasing the Wind Episode Eleven](#)

[Chasing the Wind Episode Twelve](#)

[Privacy Statement](#)

Copyright 2006, SecurityFocus