

Episode Twelve: The Serpent's Tooth

Robert G. Ferrell 2001-11-14

Chasing the Wind, Episode Twelve: The Serpent's Tooth

by *Robert G. Ferrell*

last updated November 14, 2001

Jake and Deanna sat in a quiet little out-of-the-way Oriental restaurant in the old King William district and gazed into one another's eyes. They held hands across a small antique table equipped with a brightly colored vinyl tablecloth, a small candle in a knobby red glass vase, and a single artificial flower that had seen better days. They weren't so much romancing as simply drawing support from one another. The shock of recent events had begun to wear off, leaving in its wake a dull melange of fear, sadness, and a deep sense of innocence lost. Life was suddenly rather empty and forlorn, as though the laughter of nearby children and the verdant aroma of honeysuckle had been abruptly banished from the world. Though the South Texas air was still quite warm, the city, the planet, the universe, seemed cold and harsh. It was hard to remember the smiles of friends, or celebrations, or joy, or the elations of the past. They clung to one another and hoped that the light would gradually return, although they sensed somehow that it could never be the same illumination they had once known.

As though in response to their shared anguish, both of them had found the same message printed on the little slip of paper in their respective fortune cookies: "This too shall pass."

Baseball cap winced. His data stream had suddenly been cut off, for no apparent reason. He couldn't tell if the problem was with the transmitters, his receiver, or some other component. This was the first real data transmission failure since the project began, and coming as it did at a critical point in the proceedings, it made him very nervous. He walked over to the windows and opened a narrow slit in the blinds. The street looked normal; no unusual vehicles or other suspicious activity were in evidence. He shrugged and sat down at his desk. Perhaps there would be a coded message in his e-mail that would shed some light on the situation.

He had four e-mails to download. That was about the usual number. One of them was quite large; it might be an important communique from the home office. As luck would have it, of course, it was the last message on the list. He waited somewhat impatiently as the first three

slowly slithered their way onto his hard drive. One was a software vendor offering him a demo version of some new and vastly improved knowledge management system; he chuckled at that in spite of himself. The next bit of wisdom was a blunt invitation to a sex site, sent from an obviously spoofed address. He made a mental note to visit the indicated URL later. The third and final obstruction to the information he really needed to see was a message telling him that a new computer virus was going around that would erase his hard drive and sell the contents of his e-mail address file to the highest bidder via an online auction site. Baseball Cap raised his eyebrows as far as they would go and clicked on the attachment, which promised to protect his system from this new menace. After a few seconds a graphic of a large snarling dog sporting a collar studded with nasty metal spikes appeared on his screen, with the words "System Protected" emblazoned in large red letters beneath it. Well, thought Baseball Cap, that's one less thing I have to worry about.

Finally the message he was waiting for began to download. About three quarters of the way through, his system locked up. He gritted his teeth and started pressing keys. Nothing helped. He tried ctrl-alt-del. That elicited no response, either. He waited a couple of minutes, and turned off the CPU. After thirty seconds of concentrated agony, he turned the computer back on. It churned for a moment, then this ominous message appeared:

`Operating System Not Found.`

Ian had gotten into intrusion detection systems. He'd started with some simple packet filtering, progressed to IP Chains, and now was exploring the intricacies of Snort. He set up one of the Linux boxes on his LAN as a hacking target, running Snort, TCP-Wrappers, and IPLog. He particularly favored Snort because it was written in Perl. While he still wasn't nearly as good at C as he'd like, Ian had become quite proficient at Perl. It made sense to him, whereas the pointers and memory allocation/cleanup stuff in C sometimes left him confused, especially when he was tired and trying to finish a complex hack before bed.

Ian's collection of programs designed to break into or gather information on other people's systems was sizeable. While he'd usually tested these exploits on his own boxes before using them against someone else, he'd never really done much with code designed to fend off these attacks, or at least track them. Mostly he just looked for target systems that weren't using any firewalls or other defensive programs. But now it seemed to him that the next logical step in his evolution should be to embrace and fully comprehend the other side of the hacking coin; i.e.,

defending against malicious code. The more he played with Snort, the more he liked it. There were so many rules to tinker with, and so many individual components that could be altered a little bit at a time, to observe the effect. Ian learned much more by experimentation than he did from reading manuals or textbooks. He also had a lot more fun that way.

Ian had largely forgotten about the message he had sent pointing out the suspicious activity at Acme Ailerons. The traffic stopped; whether his message had anything to do with it he had no way of confirming. His interests had begun to shift away from Web page defacements and 0-day exploits to network engineering. Acme's once tantalizingly open network had become increasingly less accessible, and Ian had grown less and less interested in challenging it. He was maturing into a true hacker.

He was also, unknowingly, the subject of a rather impressive manhunt.

Bob sighed as he stared at the mountain of paperwork he needed to wade through before his round of meetings started bright and early the next morning. The new emergency security measures in place meant that not a lot of work was getting done in the secure facility, what with all the searches and random audits and surprise inspections. Not only did he have to address the information security issues, he also had to explain to the board of directors why people were having a harder time accessing data from their workstations. He started daydreaming about retirement and that little llama ranch he'd always wanted...

An unfamiliar phone ringing shook him loose from his reveries. He frowned and looked at his desktop. After a confused moment he saw the secure phone that the DoD had installed the previous day, with a direct link to Colonel Briggs, and identified it as the source of the foreign ring. He picked up the sleek white receiver. "Bob here."

"Bob, this is Will."

Big shock, Bob thought.

"We've had an interesting development. Meet me in the parking garage in 30 minutes, near the South elevator."

"Wilco," Bob replied, "Anything I need to bring?"

"Network cabling diagrams would be nice," said the voice on the other end of the phone.

Bob looked surprised, but simply said, "Check. See you then."

Network cabling diagrams? This was getting weirder by the minute.

Douglas and in fact most of the rest of the civilian Bellatrix team were frustrated. Now that the quantum computing model had proven itself, they were anxious to begin full scale testing. However, the labs were locked down tight, surrounded by armed guards. They weren't allowed anywhere in the facility except for their own offices. Douglas sat at his table full of computer terminals and reflected on how much of his career as an engineer he'd spent waiting for someone else to finish something so he could get on with a project. It was a depressingly large chunk, he decided. It could be days or even weeks before the military felt that security had been sufficiently restored to allow them to get back to work. By then he would have lost most of his 'intellectual momentum,' not to mention having forgotten the million little mental notes he had made during the recent trials.

Douglas wasn't in the habit of committing such things to paper, given the amount of time involved, but maybe he should try writing at least some of the more important stuff down before it got buried too deeply in his long-term memory, or simply cast off.

As he was struggling with putting into words as many of his mental notes as possible, one of them jiggled a neuron that started a chain reaction in his brain, the upshot of which was Douglas suddenly remembered a "back door" he had left in the systems control box in the laser lab. When he was doing the final calibration of the controller, he had created a direct duplexing link from his workstation to the box. This allowed him to tweak and monitor the controller from his office, where the modeling and other salient engineering software resided. It wasn't technically within the rules, since his office was not afforded the same security level designation as the lab, but it saved Douglas a lot of walking back and forth.

He scooted over to the appropriate terminal and typed a few commands. The link was still there, and still fully functional. Now if he could just figure out some way to power up the lasers from here...

Merv the facilities engineer was on the verge of total panic. He was sitting in a tiny cell that seemed to be made completely of steel, with no windows and very heavy bars where the door should be. How he came to be there was the part that made him want to panic.

He'd come to work at his usual time, about 7:15 AM, and found two men in dark suits waiting for him. The building was crawling with military and civilian security types recently; he didn't see anything unusual about two more of them, even though they seemed uncomfortably interested in him specifically. The men followed him into the building and waited until he sat at his desk. They started asking questions about his job, his computer, his recent travels, and other seemingly unrelated things. He answered them the best he could, but when they started asking questions about his computer, he found himself unable to satisfy them. They handcuffed him and told him he was under arrest for 'espionage.' Merv didn't have the slightest idea what they were talking about.

Now he was sitting in a steel cage in some building, still without a clue as to why. He hadn't been allowed to make any phone calls, or in fact been able to talk to anyone at all. He was alone and trapped in a predicament that was, as far as he could tell, totally unrelated to anything he had done to deserve it.

In a high-ceilinged room that smelled faintly of spices, several well-dressed men were engaged in a spirited conversation.

"We have the satellite, we have several gigabytes of data, and we have the tapes. We do not need the American."

"But he has been our contact and ally for years. We cannot simply abandon him!"

"He is an American. Sooner or later he will betray us. It is the way of the corrupt West."

"So you are saying that we should betray him first? Is that honorable?"

"Honor has nothing to do with it. We are fighting for our very existence here!"

"I cannot agree to such an act of treachery. We must allow him time to escape."

"Fortunately for our organization, your agreement is not essential. I have already ordered it be done; further discussion is pointless."

"You have not heard the last of this, I think."

"On the contrary, my friend, I think I have."

To read **Episode Thirteen: Cabbages and Kings**, 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 Thirteen](#)

[Privacy Statement](#)

Copyright 2006, SecurityFocus