

## Episode Six: The Gathering Storm

*Robert G. Ferrell* 2001-05-02

### Chasing the Wind, Episode Six: The Gathering Storm

*by Robert G. Ferrell*

last updated May 2, 2001

---

Deanna Neare slowed the car and swerved to miss a turkey vulture that was on the road, a little too intent on its meal to get completely out of the path of her vehicle in time. She chuckled to herself - the sight of vultures always made her think of her former profession, and to wonder whether she made the right decision in leaving it.

She had majored in computer science in college, and graduated with honors. Her father was a lawyer, as had been her grandfather. As the only child, she was given little choice of vocation - law school was inevitable. Not that she hadn't excelled in that as well. But her father's practice, which she was expected to join and eventually take over, was primarily business-to-business civil litigation and, quite frankly, left her cold. While in law school, she had fantasized largely about two things: defending people wrongly accused of heinous crimes and making a lot of money. It didn't take much time as a practicing attorney to find out that those goals were mostly incompatible.

After a couple of years of suing and countersuing, Deanna was fed up. Over her father's vehement protests, she quit the law firm and went back to school to get her master's degree in Information Technology. While in graduate school she became interested in computer security. After graduation, she attended a couple of study courses and passed two of the more prominent certification exams with relative ease. With her new credentials, she got a job with a well-known contract security firm.

It was in the performance of her duties in this latter occupation that she narrowly avoided hitting the vulture. Her client today was a fairly large engineering firm called Acme Ailerons. Her job was to evaluate the IT security posture of the company and make recommendations for improvement. Today had all the earmarks of being just another day in (or rather, out of) the office...

---

Jake was in a relatively good mood. Shipping and Receiving had just called and there were

several boxes for him on the way up. Jake knew what they were his new firewall and hardware virus scanner. He'd been hitting the online firewall rules documentation pretty hard over the past few days. Now it was time to see if he had learned anything useful.

After all the unpacking and plugging in had been accomplished, Jake set up an xterm session to the firewall and settled in for some serious config action.

First, he needed to retrieve the disk image of the firewall's boot helper program, to be saved on a diskette. To do this, he had to enable TFTP on his Unix box.

```
# cd /etc
# cp inetd.conf inetd.conf.bak
# perl -ne 's/\#tftpd/tftpd/; print' inetd.conf > inetd.conf2
# mv inetd.conf2 inetd.conf
```

Now he had to restart inetd to get the new service up and running.

```
# ps -ef | grep inetd
root  148    1  0   Apr 29 ?           0:01 /usr/sbin/inetd -st
# kill -HUP 148
```

With TFTP functional, the next step was to transfer the boot helper program to the Unix box and make a disk image of it on a diskette.

```
dd bs=18b if=./bh510.bin of=/dev/rdl
```

Once the boot helper diskette was created, Jake used it to transfer the binary image from the TFTP server to the firewall. With that step behind him, Jake started in on the actual firewall configuration process, but not until he had disabled TFTP again. Wouldn't want that mischievous little daemon running around unsupervised...

```
configure terminal
clear arp
ctrl-Z
```

After resetting the default route for the router and all the hosts on the perimeter subnet to point to the firewall, Jake started feeding interface names, global addresses, and local addresses to the firewall. He had drawn up a rough chart of the security structure he wanted to create. He then used it to map out the DMZ proxy hosts that would act as buffers between the

firewall and the computers inside Acme Ailerons. Those computers would have nonrouteable local IP addresses only and would not be communicating with the Internet directly. Only the firewall would have a map of which NAT addresses mapped to which hosts.

For his part, Jake felt safer already.

---

Ian sat transfixed at his terminal. It was late Sunday afternoon, and he hadn't slept since Thursday night. Well, that wasn't entirely true; he'd catnapped a couple of times for 15 minutes or so. His room was a collage of candy bar wrappers, semi-crumpled soda cans, casually strewn CD cases, hacking files printed out from the Web and, of course an ever-growing collection of computer parts. Buried underneath all of this, he mused as he tore his eyes away from the screen for a moment's rest, were some new clothes his mother had bought for him the previous week. Ian suddenly realized that the rather disagreeable odor he'd been catching wind of occasionally over the past few hours was himself. He hadn't bathed in several days, either. Reluctantly, he pried himself away from his Linux entertainment center and stumbled off to take a shower.

When he returned a few minutes later, the fatigue that had been starting to set in was, at least for the moment, dispelled. He was rarin' to go, and dove back into the complex paper from his hacker convention, which he had been on the verging of giving up on before the invigorating application of soap and water. The paper concerned embedding exploit code in the body of a Graphics Information Format, or GIF, file. That concept had quite simply never occurred to Ian, and it seemed positively brilliant.

"A GIF file contains an area reserved for comments," he read, "And those comments can be read as executable Javascript code by certain browsers under the right conditions." This was too good. He had to try it out. He set to work looking for just the right graphics file to use as his "carrier."

---

Colonel William Briggs sat in a smartly appointed leather chair at the end of an impressive walnut table. Immediately in front of him were several stacks of intelligence reports and photographs from the image analysis section of the Pentagon, which is where the table and chair happened to be located. Across the table from Will were three gentlemen with lots of stars

on their shoulders and collars. They had decidedly unflattering pictures of themselves hanging around their necks, constituting part of the official-looking ID cards suspended by little fabric bands with words he couldn't make out woven into them. The lighting in the room was subdued, but there still seemed to be enough photons bouncing around to glint menacingly off their sartorial constellations whenever one of the generals leaned forward to speak.

"Colonel Briggs, you have made a highly unusual request. The President and his Security Advisor will want to know exactly upon what data you have based the assumptions underlying it."

Will stirred uncomfortably in his suddenly and inexplicably slippery leather seat. "I understand, sir. I have brought with me what I hope will be sufficient and just evidence for my request to be granted." He paused to sort through some photographs. "I've had these analyzed by the microphotogrammetry folks, and have indicated in the margins the probable identification and significance of each of the findings." He shoved a stack of photos across the table to the General who had spoken. "With all due respect, I think you gentlemen will agree with me that this is not a matter to be taken lightly. Sirs." He leaned back and tried to relax as the assembled brass looked over his photos and notes.

"That, um," replied one of the generals as he peered at the material through his reading glasses, "That remains to be seen, Colonel."

"Of course, sir."

Outside, a generous late Spring thunderstorm was gathering force for an assault on America's largest office building. Down in the basement, the janitorial crew donned their galoshes and readied their mops and buckets. The Pentagon, it is said, has many leaks. Not all of them are brought about by rain.

---

Bob looked up from his *CIO* magazine and punched the speaker phone button on his telephone. "Yes, Constance?"

"There's a Ms. Neare here to see you, sir."

Bob wrinkled his brow for a moment, then punched up an electronic business card on his palm

top. Digitally-enhanced recognition flooded in.

"Ah, yes, the computer security consultant. Please send her in. Oh, and Constance, would you find Jake and have him report to my office also, please?"

After the usual round of pleasantries and a few pointed questions from Bob to reassure himself that Deanna was as knowledgeable as her company's marketing had claimed, Bob laid out the specifics of what he wanted Deanna to accomplish. His systems administrator, Jake, was essentially the front line for both operational administration and IT security. Jake had some formal training in security now, but not enough to design a comprehensive security plan for the entire company.

Deanna's job was to review the entire company's IT infrastructure and make specific recommendations about which hardware, software, and policy to be put in place to harden the network. It would be a time-consuming task, and one for which the funding had been wrested from the tightly clutched fingers of other department managers. They would be watching the proceedings with keen interest, to put it mildly; Bob knew that his rear end was on the line here.

For a CIO, however, that is a familiar position.

---

A middle-aged man in a blue serge suit sat at a functional but not very attractive desk in a sparsely decorated room, unpacking one of a dozen or so cardboard boxes marked simply "New Office." The contents of the boxes were, in a word, generic. There was a phone, a notepad, some files, some office supplies, a calendar, and some random books to go on the shelves. There was a desktop computer, of course, and most of the other trappings of an office environment.

To the casual observer, this would appear to be just another small business office, housing a small law practice or a manufacturer's sales office. It was neither of the above, however. It was a front for one of the most insidious conspiracies ever perpetrated against the United States Government. It would be the focal point for an operation so secret the conspirators didn't know each other by sight or even precisely for whom they were working. The plan to be put into operation from this deceptively simple office would cause a splash that would ripple to the far

corners of the civilized world.

Across the street was a busy construction site, shielded behind a tall fence that obscured it from ground level view. The view from the 7th floor office was excellent, however. Every movement of the construction crew and every piece of equipment or material brought in or out could be carefully documented through the highly mirrored one-way glass.

The office had been rented by an organization that called itself Global Technical Products, AG, with headquarters in Amsterdam. The building site they had gone to such great lengths to monitor so scrupulously belonged to Acme Ailerons.

To read **Episode Seven: An Ill Wind**, 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 member of the Netwits. 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*

[Privacy Statement](#)

Copyright 2006, SecurityFocus