

## Episode Two: Raising the Stakes

*Robert G. Ferrell* 2000-10-17

### Chasing the Wind

Welcome to the second installment of "Chasing the Wind," a continuing series that chronicles the education of folks on each side of the 'digital curtain.' This is a fictional account, yet just about everything that happens in it is something I've seen take place at one time or another during my sysadmin/computer security career. While the primary purpose of this series is to identify and elucidate various aspects of computer security--after all, that's what Security Focus is all about--it's also intended to be an entertaining piece of literary techno-humor, because that's what I'm all about.

You might think that "Chasing the Wind" is a rather unusual title for a series about computer security. You might even observe that it's not very technical. You'd be right on both counts. If you further believe, however, that it isn't descriptive of any aspect of the computer security field, I'd have to take exception to that opinion. Anyone who has diligently tried to wade through all of the announcements, alerts, warnings, bulletins, patches, patches to patches, speculations, exaggerations, understatements, misinformation, and general ballyhoo generated by the computer security community on a daily basis knows why I call this little melodrama "Chasing the Wind." Truly secure and simultaneously useful systems are as elusive as any given molecule of oxygen on a breezy day.

If computer security is an illusion, as some have suggested, let us all strive to be David Copperfield.

### Episode Two: Raising the Stakes

Douglas sat at a test bench overflowing with wires, probes, and electronic components and stared fixedly at an oscilloscope tracing. He was a model of intense concentration; every nerve fiber dedicated to the task at hand. He swivelled in his chair and reached to his right for a waiting mouse. Moving the mouse slightly and typing with two fingers of his left hand, he brought up a new screen. A couple of clicks later, he watched as the computer painted a complex wire frame image of the flight system he was modeling. He swung around even further to the right and typed a few characters on a second keyboard. There was a pause of perhaps five seconds, at the end of which Douglas winced as though he had stepped on a thumbtack on

the way to the bathroom at night. The screen of the second computer went solid blue. He pounded on the desk in consternation and briefly considered attacking the offending machine with an eight ounce ball peen hammer. Realizing the utter futility of this gesture (eight ounce wasn't the right sized hammer for this job), he sat back and exhaled sharply. Suddenly a phone list posted on the wall near his workstation caught his eye.

"Network Operations, Jake speaking," said Jake mechanically into the receiver. He was involved in reading a book about firewalls and not really paying much attention to anything else.

"Hey dude," came a husky voice from the earpiece, "This is Douglas in Systems Engineering. Dude, my NT machine locked up in the middle of a sim run. Can you scoot up here and give it mouth-to-mouth?"

"Oh, sure. Be there in a minute," Jake replied absently.

"Cool. I'm in 6D34. Thanks."

A little mental termite set up housekeeping in one corner of Jake's brain and began to gnaw at his gray matter, until he gave up trying to ignore it and jerked himself away from IP chains. He suddenly realized that he had promised to go help someone with something. Someone in the SE Group. On the sixth floor somewhere, he seemed to remember. He tried to replay the conversation in his mind, but mostly all he got was static and stuff about packet filtering. Oh well, Jake thought, at least I know what floor he was on. I think...

After a few minutes of popping into random offices and bewildering people with questions about their computer problems (most of them replied with some variant of "Yes, I am having trouble. How did you know?" His stock answer to this question was, "It's my job to know"), Jake finally stumbled into Douglas coming back from the restroom.

"Dude, you made it," said Douglas brightly.

"Uh, yeah, piece o'cake. What's your problem?"

"Blue screen of death," Douglas replied wryly, "Revenge of the nerd."

Jake rolled his eyes, "Yeah, you probably asked it to divide by something that wasn't an integer. I'll take a look."

Bob put down Jake's report on the security incident and sighed. He was visualizing the fight he was going to get from the other area managers when he asked for an increase in the IT budget to cover computer security measures. Ed in Facilities would bring up his tired and basically irrelevant argument that computers were just furniture and should be under his department. Brigid in Engineering Ops would argue that new workstations for her engineers were more important than "network band-aids." Doris in Accounting would no doubt try to cloud the issue with her overdramatized rendition of the recent security *faux pas* and its effect on email integrity (although Bob thought he might be able to engineer a little favorable spin doctoring on that one). He wasn't sure how Vijay in Assets Protection would figure into the picture. Physical security folks tended to be a little too hard-nosed about limiting access to computers, in Bob's experience, but past encounters had hinted that Vijay was fairly enlightened in this respect.

---

Ian slammed the door to his room shut, threw the deadbolt, and tossed his backpack onto the rumpled bed. Today hadn't been a good day, by any standard. Not only had he barely passed an algebra test he thought he was going to ace, but the girl who had seemed interested in him for the past couple of weeks suddenly and mysteriously blew him off for an asinine baseball jock. To top it all off, his acne was now officially worse than ever. He felt rejected and belittled at every turn. Ah, but he was home now. The world played by his rules here in this room. He flipped several switches and watched as his computer system, the electronic scepter and diadem with which he ruled his empire, scrolled and flashed its way into life.

```
TO: ir8_d0g@haxmail.com
FROM: deathdr0id@0fffx.net
SUBJECT: Re: AA Hack
```

```
>Herez the password file to pr0ve I g0t in.
>How ab0ut it? I'd like t0 be a Bbandit cauz I think u
>dudez rul3.
```

```
S0rry, d0g. It takes more than a luser m$ hack to be 31337. The
Bandits
```

rul3 cause we're smarter than the f3dz or the so-called security 3xp3rtz.  
Mayb3 when u gr0w up someday.

dEatHdR0id

Ian sat slack jawed at his computer, stunned and outraged and crushed all at the same instant. Someone was going to pay for this insult, and pay dearly. He was through playing around.

---

Jake wandered around the engineering lab while Douglas ran a few test simulations on the newly resurrected NT box. No point in trotting off too soon and having to come all the way back up here to do it again. He felt pretty confident that the service pack he had downloaded and installed would solve the problem, but better safe than sorry.

In one corner of the lab Jake discovered a large white sealed box with windows and a console with two joysticks and the odd switch or two on the front. Peering through the darkened windows, Jake saw two mechanical arms, each with two fully articulated fingers. He fiddled with one of the joysticks and watched the arm inside move correspondingly. A few minutes later he was completely engrossed in moving the little claws back and forth when suddenly Douglas' voice spoke just behind his right ear.

"Having fun?"

Jake was so startled that he almost broke off one of the joysticks. "Jeez, man, where'd you learn to sneak up on people like that?"

"Dunno. Guess it's my Native American blood. Like my clean box?"

"Is that what this is?" Jake was still breathing a little heavily, but he wasn't shaking quite so much now. "What do you use it for?"

"Here, I'll show you." Douglas flipped a couple of switches; a fan roared to life and bright light flooded the box. He operated the joysticks deftly and opened a little metal container. Inside was a small semiconductor chip embedded in a complex framework of wire supports and miniature tubing that fed down into the base of the container. Directly above the box was a sort of turret with several cylinders of different diameters and lengths protruding from it. It resembled the

objective lens part of a microscope. Douglas reached up and pulled down what looked like the front half of a pair of binoculars that had been nestling unseen in a sheltered alcove above the windows. These were attached to an arm that could pivot freely on several axes. Douglas brought them down in front of his eyes and peered into them while he manipulated the mechanical arms with very fine movements of the joysticks.

"Here," he said after about a minute, "Take a look at this."

Jake raised the eyepieces just a bit (he was slightly taller than Douglas) and brought them to his face. He saw a greatly enlarged image of the chip. A protective covering of some sort was peeled back to reveal what looked like a regularly spaced array of bubbles on the chip's surface. Each of the bubbles seemed to contain a tiny drop of water with things swimming around in it.

"This is wild!" Jake exclaimed, "Looks like little fish ponds or something."

"That's a project I'm working on with NeoBiologica. It's a controller chip with special genetically engineered embedded bacteria."

"Cool. What are these bacteria supposed to do?"

"They act as environmental sensors, in this case. Temperature, salinity, and oxygen content. When those parameters change, the bacteria adjust their microenvironment and that affects the resistivity of the surrounding matrix. Sort of a reactive variable semiconductor."

"Freaky stuff. What good is it?"

"Well, at this point it's just sort of proof-of-concept," said Douglas, "But eventually it's supposed to have lots of applications in medical implants, control systems, and who knows what else."

"Wow," Jake whistled through his teeth, " I didn't even know we did stuff like that."

"It's because of a new research consortium we recently formed with seven or eight other companies," Douglas answered, "Kind of hush-hush, if you know what I mean."

"Gotcha," nodded Jake, "I didn't see a thing."

At 3:28 AM the following morning, Ian made his next move. In his previous intrusion into the Acme Ailerons network, he had made note of a number of other boxes which he decided were running NT, based on the fact that ports 135 and 139 were listening for traffic. A quick revisit using queso confirmed his suspicions. He was more focused this time around. The stakes, at least from his point of view, had increased dramatically. Tonight he was going to prove himself beyond any shadow of a doubt.

At first it seemed that nothing had changed on his target network. Ian chuckled; maybe this wouldn't be as hard as he'd imagined. The initial telnet attempts were refused, but that had happened before. Eventually he'd stumble across a box that would accept his connection. This time, however, the couple of hosts that didn't refuse the connection attempts outright simply timed out. After half an hour he still hadn't gotten in anywhere. He gritted his teeth and settled in for a long, tedious session of enumeration.

By 6:00 AM he hadn't found anything he could really use, and by this time it had become obvious to Ian that some serious firewalling had gone on at his previously wide-open victim's site. Rather than being discouraged, Ian was more determined than ever to crack this nut. His status depended on it. He spent the rest of the day surfing anonymously, looking for suitable backdoor trojans.

---

The senior staff meeting went more or less the way Bob had expected. He felt he had managed to deflect most of the flak directed at his request for a funding increase. He was pleasantly surprised by Vijay, who turned out to be a largely unanticipated ally. Vijay fully supported his request, and went further, suggesting that in addition to the inhouse measures a security consulting firm be hired to do a full risk analysis and provide recommendations for a sound information security architecture. Bob was gratified and impressed. Vijay was a quiet man, whose words were carefully chosen and always to the point. With his assistance, Bob got virtually the entire funding package he had asked for. This didn't endear either of them to some of the other managers, but Bob's philosophy had always been that you have to break a few eggs to make an omelette. Now that he had substantial financial resources at his disposal, breakfast was about to be served.

---

Ian sat back in what he liked to think of as his 'command chair' and smiled a tight little smile. He had sent the email with the trojan to so many people at Acme Ailerons, at least one of them was bound to open it. One was all he would need. He had only to sit back and wait for the trojan to notify him that the network sniffer it carried had been activated. Life was looking up.

It took three levels of his favorite computer game before he got any response, but finally that little mailbox icon popped up. He opened it and was rewarded with a user ID, password, and some other interesting and useful tidbits. Now it was just a matter of waiting for the right moment to strike...

**To be continued...**

To read **Episode Three: From Out of the Blue**, 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

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

*Robert G. Ferrell*

[Privacy Statement](#)

Copyright 2006, SecurityFocus