

Chasing the Wind, Episode One: No Place to Hide

Robert G. Ferrell 2000-09-17

Chasing the Wind

Welcome to the first 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 One: No Place to Hide

After six tedious hours in Human Resources, filling out more forms than it took to draft the Treaty of Versailles, Jake was finally sitting in the computer room at the console of his new Sun Ultra 10 workstation. He was the systems administrator and monarch of all he surveyed. The room thrummed with the activity of packets fluttering to and fro like little digital moths around a digital streetlight. He could feel in this room the very electronic heartbeat of Acme Ailerons, his new employer. Every byte of data generated by the company was stored here, and he was the caretaker. He took a minute just to sit back, close his eyes, and feel the power surging through his veins. Life was good.

Jake was not exactly new to systems administration. He'd been doing similar work for several years at other companies, usually because he was the only person with enough computer aptitude to survive sysadmin training. But this time things were different: he was officially the Systems Administrator, with an office and everything. He was legit.

He had several flavors of *nix, an NT server farm, and a fair collection of networking and remote access equipment. It was all his to rule. To top it all off, they actually paid him to rule it. How much happier could he get?

Halfway across the country, Ian sat and stared at the keyboard of his recently cobbled-together Linux machine. He'd built it of parts scavenged, scrounged, and begged from friends. The monitor was an old 14 inch that had an annoying tendency to quiver around the edges until it got good and warmed up. Sometimes, just for variety, it would get out of sync with itself and flash like a strobe, only without any discernible sense of rhythm. This made Ian a little surly.

He had recently turned 15, and he felt it was high time he established himself as a hacker. Most of his friends spent their free hours defacing each other's Web sites and playing Quake over the Internet; Ian had higher aspirations. He longed to be a member of the elite hacker club "The BroadBandits." The trouble was, the Bandits wouldn't give him the time of day until he proved himself worthy. Armed with several root kits and a port scanner his best friend had hacked from nmap, bolstered by a six pack of heavily caffeinated sodas and a dozen gooey candy bars, Ian set out to find an unlocked door.

The first thing I need to do, thought Jake, is to figure out just what I've got here and how I can best monitor it all from a central console. He was primarily a Unix kind of guy, so he dug around and found a copy of some software that would let him connect to and monitor the NT boxen from his Sun station. After a couple of hours of mapping IP addresses and hostnames, setting permissions, and banging around on the interface, he finally succeeded in coming up with a display he could live with. He hummed a happy little sysadmin tune.

Next he decided to do an audit of the applications and services running on each box, as well as establish what sort of file sharing architecture was in place. "Looks like NFS and some Novell," Jake mumbled as he crawled through the directory services trees. A few leaves fluttered to the floor as he did; he pushed them under his desk with one foot.

By the time he was relatively confident that he understood the directory services on his systems, it was after 5 PM. Jake decided not to overdo it on his first day, so he threw some policy manuals in his briefcase, gave his loyal cybersubjects one final adoring, yet nobly commanding, glance, and headed out the door. There was a new first person action game he couldn't wait to dig into on his PC at

home.

It was about 4:30 PM by the cheap digital alarm clock that glowed redly in Ian's darkened bedroom. He had just come back from eating something that probably would have seemed to an outside observer to be lunch, although Ian himself considered it breakfast. During the summer his internal clock went on its own schedule, rendering references to traditional mealtimes (and, it must be said, menus) approximations at best.

He sat at his Linux terminal and stared fixedly at the monitor. He was feeling a little sleepy, despite the fact that he had only been up for 45 minutes, and a nap was surely in the offing. But first, time to pick a new subnet and let sniff the dogs of war.

He glanced over an alphabetical list of possible targets. Discarding several of the "A's" as being either too boring or too potentially problematic, he settled on "Acme Ailerons."

"Sounds like a wiener," he mumbled as he typed in the IP range. "Let's see what they've got under the hood." Ian stayed long enough to watch the initial connection being made, then trudged across the room and flopped down bonelessly on his mind-bogglingly disarrayed bed.

As Ian snored softly, back in CPU-land the scanner was churning away like a madman.

```
# Found clueless box!
# Starting nmap_hack script...
# nmap_hack sS flaps.acmeaileron.com o scan_txt m scan_delim D ./decoys1,ME,./
decoys2
```

```
# Interesting ports on flaps.acmeaileron.com
```

Port	State	Protocol	Service
21	open	tcp	ftp
23	open	tcp	telnet
25	open	tcp	smtp
110	open	tcp	pop3
135	open	tcp	locsrv

139

open

tcp

netbiossn

Awake from his nap but still a little groggy, Ian ambled back over to da box and popped up the scanner log file. He whistled hoarsely through his teeth as he glanced over the data, then stopped short, with a sharp intake of breath. "Houston, we've got a possible luser here," he chuckled.

A few minutes later he started a null session with the remote NT box, and a few minutes after that he had a nice list of user IDs to play with. He plugged this intelligence into his favorite brute force password cracker and was rewarded in less than half an hour with the admin account.

"Mmmmmm," he purred, "Just like candy from a baby."

Ian bopped around in the directory tree of the owned NT box for a while. He didn't have any real objectives, other than to document his victory for the sake of the Bandits. He suddenly had an urge to scope some mail.

After a couple of hours of reading employee gossip, messages to stock brokers, and even a few technical communications about ailerons that he didn't really understand, Ian had a mischievous thought. He took an email sent by one of the auditing assistants to a friend which spelled out in the clearest possible terms the secret crush she had on a metallurgist and put it in the inbox of the object of her clandestine affections. It then occurred to Ian to slap a "blind cc" in the header of the message, so that it would look as though the author had sent the message herself, by accident. Giggling with evil joy at the mental image of the brouhaha that would undoubtedly ensue the next morning, Ian grabbed a few system files to prove he'd been there, left a hidden but not *too* hidden calling card (U w3r3 0wN3d by iR8 d0g), and cleaned up after himself. It was, after all, time for "Doctor Who."

The next morning dawned bright and clear. By 7:00 AM Jake was comfortably ensconced in his 'command chair' in the computer room. He scanned logs and diagnostics from the previous night, but saw nothing particularly noteworthy. Yes, the /var partition on one of the Unix boxes was almost full from a messages log that hadn't been trimmed, as far as he could tell, during the last two presidential administrations.

There was also a rather substantial error log on one of the NT boxes generated by an unruly piece of code that slipped out of a development environment and flopped around for a while loose on the

intranet, but otherwise things looked fairly peachy.

It wasn't until early afternoon that the first hint that something wasn't right reared its ravenous beak. By this time the fallout from the previous evening's musical emails had begun to spread hoary little tendrils of chaos throughout the highly organized Gossip Distribution System (GDS) in place at A.A. Half of the Materials Engineering group wasn't speaking to the other half, Accounting & Auditing had barricaded themselves in their offices and were lobbing cream cheese danishes at anyone who came too close, and the Vice President for Human Resources had developed a noticeable nervous tic just below her left eye. It was only a matter of time before the IT department became involved.

It happened at 2:17 PM. Bob, the CIO, got a terse phone call from the Accounting Department Manager (with whom he had never really clicked), who stated rather flatly that she thought that someone in IT had been deliberately tampering with the internal email system. Bob took a deep breath and leaned as far back in his chair as he could without actually falling over.

"Now, why would anyone want to mess around with your email, Doris?" he asked, in his most innocent voice.

"Don't you patronize me, you overpaid geek," Doris shot back, "It wasn't my email, it was one of my people's. A person who shouldn't have gotten a personal email she sent to someone else got it anyway and read it, and now both of them have gone home sick."

Bob thought about this for a moment.

"Maybe they're just sick of being at work," he started, but Doris cut him off, "Can the comedy and fix the problem."

"All right, all right," answered Bob, in a hurt tone, "How do you know she didn't send this email out herself, accidentally?"

There was a palpably exasperated pause at the other end of the line. "Honey, you don't make mistakes with the kind of email *I'm* talking about."

Bob made a little smacking noise with his lips. "I see. I suppose raising the issue of whether or not sending that sort of email is a proper use of company resources in the first place would be futile at this point."

"I'll worry about that. You worry about which one of your geeky little robots has been playing with

the mail."

"I'll look into it."

"Damn right you will. I've already called Mr. Averson." The phone went silent. Bob sighed. Averson was the Executive Vice President for Operations. "Goodbye, Doris," he said to the handset, "Hope your AC shuts down."

His other line lit up as he was putting down the receiver. The LCD panel read "Averson, Nathaniel." Bob sighed again and picked up the phone.

"Hello, Mr. Averson," he said brightly. "What can I do for you?"

Lunch had gone surprisingly well. Jake didn't make a habit of leaving the building for lunch; in fact, he usually never even left his computer. Today, however, some of the IT folks had decided to go check out a new restaurant and had invited him along. He felt that he should mingle at least enough to get to know his new co-workers, so he pried himself away from the console and went with them. The food was good, the company cordial, and all in all he was feeling pretty mellow as he logged back into his console. He noticed a few messages in his inbox with some rather disturbing subject lines, but before he could open one, he felt someone looking at him. Jake swivelled around in his chair to see Bob standing there.

"Hi Jake," said Bob, "We need to talk."

The postmortem wasn't pretty. It didn't take Jake too long to find Ian's 'calling card' once he had reason to suspect a breakin. The damage done to files and data was minimal; a quick reload of some things from tape and a little testing and Jake felt fairly confident that the status quo had been restored, systems-wise. No, the real complications stemmed from the social aspects of the assault. People were, for the first time, doubting the security of their mail and, by extension, their data. Once congenial pairs of eyes now squinted and frowned at one another in passing. Someone in the company was a spy, a voyeur with sadistic tendencies. It could be anyone. No one could be trusted.

All because some snot-nosed kid had broken into their mail server and pulled a childish prank. It was obvious that some serious securing of servers was needed here, and this was one area where Jake quite frankly didn't have a lot of experience. He sat down heavily at his desk and stared dully at the pile of books with words like "Security" and "Firewall" in their titles he had brought back from the local Computer Bookstore. He chose one at random and opened it.

"A fundamental tenet of information security is controlling access to the critical resources that require protection from unauthorized modifications or disclosure."

It was going to be a long night.

To be continued...

To read **Episode Two: Raising the Stakes**, 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.

[Privacy Statement](#)

Copyright 2006, SecurityFocus