

Episode Ten: The Road Less Travelled

Robert G. Ferrell 2001-09-04

Chasing the Wind, Episode Ten: The Road Less Travelled

by *Robert G. Ferrell*

last updated September 4, 2001

It was almost noon, and no one had managed to have much effect on the target Web server in Jake's "hands on" hacking class. There had been a couple of minor interruptions, but nothing that could really be classified as a denial of service. The instructor had warned them at the beginning that this was not meant to be a pushover exercise; it was becoming apparent to the students that he wasn't kidding. Jake had tried most of the tricks he knew, with no success: smurf, ping of death, echo-chargen, and teardrop, among others. He leaned back in his chair and closed his eyes. It was time to think outside the box.

He mentally ran over all he had learned in the lecture portion of the class, taking it point by point. No insights there. He thought about the hundreds of messages pertaining to denial of service attacks he'd read on various security-related mailing lists and news sites. Nothing leapt out at him. He reached forward and idly scrolled back through his command history. Something made him stop at 'arp -a' and hit enter. As the arp table printed out he scanned the hardware addresses, and suddenly the reason his subconscious had urged him to replay this command hit him. The first six hex characters in the hardware address were called the OUI, or Organizationally Unique Identifier. They were assigned to specific manufacturers of network-enabled devices by the Institute of Electrical and Electronics Engineers as a means of identifying the device on a network. The OUI was combined with a serial number to label each network device uniquely, like a fingerprint. One of the computers on this network had an OUI that Jake recognized: it was a network interface card with which he'd had extensive dealings in a previous job. At first glance there wouldn't seem to be any useful information in this discovery, but after a few seconds of concentrated thought Jake realized that here was a potential exploit staring him in the face.

A bit anticlimactic, thought Douglas. He had been watching the Bellatrix display panel for ten seconds now, and nothing much had happened. Admittedly, this was just an early operational test of a system he'd never really expected to work, but somehow the lack of any visible result at all was a little disappointing. The apparatus was obviously on, and the lasers were pulsing. No numbers were appearing on the screen, however. Everyone in the room let out a collective exhale when it became apparent that the first trial run wasn't going to produce anything spectacular. Most of the witnesses were officials with tight schedules, so the development manager stood up and hastily reminded

everyone that this was merely an initial trial to work out some of the kinks, and that the absence of spectacular results didn't have any bearing on the ultimate success of the project. He put up a brave front, but it was apparent to anyone paying close attention that he was just as disappointed as the rest of the crowd.

Douglas was puzzled. All of the components passed their function checks, and the system seemed to be performing as designed, except for the minor glitch of not producing any actual result. He checked and rechecked all the test parameters, looking for some anomaly that might explain the failure. By the time he had finished his first diagnostic run-through, it was early evening and everyone else in the Bellatrix SCIF had gone home. Douglas was on the verge of joining them when something caught his eye as he was scanning a row of binary numbers representing the settings of software flags.

He carefully compared the numbers fed into the test program with the ones he'd prepared from countless simulation runs. The lists were identical except for one number. Tracing back the position of that number and matching it to the parameter database, Douglas suddenly realized what had happened. They had asked the system to perform all calculations using only virtual quantum channels—those which reentered the "real" world before the experiment started. While it was possible to gather information thus calculated by analyzing the states of photons entangled with those in the virtual channels, it couldn't be done unless a real channel had been reserved for each entangled pair so the results could be displayed. The errant "0" had made all those numbers be generated before the apparatus had been able to register them.

A simple change to one number, a reload of the parameters, and a few seconds to reenergize the lasers. Douglas pressed the enter key with no fanfare at all this time. Three seconds later screenful after screenful of numbers began spewing out, almost faster than the processors and data bus on the heavily beefed up workstation could handle. The system was programmed to run for ten seconds. At the end of that time, which seemed like an eternity to Douglas as he sat, fascinated, watching the blur of mathematics, the machine shut down. It took about fifteen more seconds for the supercomputer buried deep in the bowels of the facility to read the generated data and spit out a statistical analysis of it.

For a long moment Douglas didn't completely comprehend what the analysis was telling him. It seemed somehow unreal, like a signpost half remembered from a dream. He printed it out and sat staring at it for quite a while, trying to wrap his brain around the number. As he stared at it, it became meaningless, the way any word or symbol can do when pondered too long without any context. Finally he decided simply to walk away and worry about it in the morning. He left the printout there on the console, switched off the power and the lights, and headed for less mind-numbing climes.

The printout read:

Effective Processing Speed Achieved: 145,783,219,423,655 flops per second.

Estimated Percentage of Total Operational Capacity: 0.034

Ian had been lurking on his favorite IRC channel for about half an hour, while playing a computer game on another system. He wasn't paying close attention to who was conversing, or what they were saying. He just had the words scrolling by as a sort of background noise while he blew away mobsters in an Orwellian New York City. In between gunfights, however, he glanced at the IRC screen and happened to see something that snatched his attention away from crime-fighting altogether. It was an IP address someone had posted as being open to a newly released exploit. The address was in a range that looked very familiar to Ian...

The dotted quad did, in fact, point to Acme Ailerons, but it wasn't one Ian had ever seen before. He felt himself oddly angered that anyone else would dare to be probing around in 'his' territory. He shut down the game he was playing and headed straight to the indicated address to see what sort of vulnerabilities it indicated. The thought that other people were probably doing the same made him all the more determined to get there first and head them off.

The answers Ian got back from his port mapping and OS fingerprinting were surprisingly inconclusive. He wasn't sure just what sort of box this was; he wondered what made the lamers on IRC think it was exploitable. It did seem to be wide open and outside the firewall, though. Maybe they knew something he didn't. He went back and read the entire IRC transcript to find out what had made the AA box a topic of conversation in the first place.

Apparently a few guys had noticed an odd traffic pattern associated with the Acme box and concluded, rather baselessly, that it was being generated by a new exploit of some kind. Ian didn't have any idea what was causing the traffic, but he felt relatively sure that it wasn't a run-of-the-mill hack. It almost looked as though the box were being used as some sort of relay. The disturbing thing was that the data being relayed were encrypted and seemingly headed for an IP address not routable by properly configured routers. While it was possible that the data were simply going from one internal machine to another, the latency suggested otherwise. Unless something was seriously wrong with the campus network at Acme, this system was transmitting bursts of encoded data to an address a long way off.

While Ian was far from being an expert at all aspects of Acme's business dealings, he was quite familiar with their network traffic patterns. He ought to be ? he'd mapped them extensively for over a year now. At first he was just trying to impress the BroadBandits and be accepted. As time went on, though, that goal became less and less important. What really mattered to him was the sheer adrenalin rush of learning new things about computers and networks. He was obsessed with each little grain of information and addicted to the hunt for more. As he watched the curious network activity emanating from that one mysterious Acme node, he was a bit surprised to realize that he was worried about something illicit going on. Ian had come to regard Acme as his personal stomping grounds, and the idea that someone else might be exploiting them irritated him. He decided to investigate further and put a stop to it if he could.

Will Briggs sat at his desk with an envelope in front of him. It had just been delivered by special courier, and was sealed about half a dozen ways. It had a variety of official warnings emblazoned on it about the dire consequences of opening it if you weren't Col. William Briggs. He took a few seconds to make sure he was the right Col. William Briggs, just to be absolutely clear on the point. No sense taking chances.

Once he had managed to convince himself of his identity, Will began breaking the seals on the envelope. Inside was a single sheet of paper, embossed with the seal of the Joint Chiefs of Staff, U.S. Department of Defense. It had "For Eyes Only" stamped across it in bright red ink. Will chuckled. He'd always found this particular phrase amusing. "I'm sure as heck not gonna read it with my feet," he muttered.

The contents of the letter were curt and to the point. In fact, they consisted of only two lines:

Request for suspension of Project Bellatrix pending security review denied. Reason: insufficient cause.

And that was that. Will sighed and shrugged. He'd given it his best shot. The high muckity-mucks weren't impressed. All he could do now is hope that he and Bob had been wrong. He wasn't very optimistic about the odds surrounding that assertion, however. When two veteran intelligence officers have the same gut feeling, it usually turns out to be justified.

Only time would tell.

Deanna glanced at her watch. She had one more client visit to make, then at five o'clock she was going to pick Jake up at his training class. She and Jake were seeing more and more of one another these past few weeks. She wondered just how far things would get. So far Jake hadn't done anything but make her happy. In her experience, though, it was only a matter of time until he started to slip up. Every one of her relationships up to now had followed that old familiar pattern. Still, one could hope...

On a high plateau in Anatolia, a lizard scampered madly across a sandstone outcropping as the peaceful rhythms of the desert were shattered by the roar of a rocket booster coming to life. It lifted off flawlessly, carrying into orbit a smallish tuna can-shaped satellite about six feet in diameter. While it was tracked by multiple governments across the planet, it was registered to a private company that was reportedly establishing a telecommunications network to support its commercial activities, and so was not regarded as any sort of military threat. The owner of record of the newly launched satellite was a Dutch-based company called Global Technical Products, AG. The tracking stations relaxed once orbit had been achieved. There was nothing to worry about, now that the satellite was safely in its planned trajectory.

The lizard watched the fiery demon scream towards the sky with a deep sense of foreboding. Nothing like this had ever before disturbed his peaceful existence. Though he could not grasp the mechanism of or purpose for the launch, he knew instinctively that it was not a natural event in his desert, and therefore must be a bad thing. There was something intrinsically evil about it.

Score: lizard 1, world governments 0.

To read **Episode 11: Fire and Brimstone**, 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: 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

[Chasing the Wind, Episode Six: The Gathering Storm](#)

Robert G. Ferrell

[Chasing the Wind, Episode Seven: An Ill Wind](#)

Robert G. Ferrell

[Chasing the Wind, Episode Eight: Still Waters](#)

Robert G. Ferrell

[Chasing the Wind, Episode Nine: Smoke and Mirrors](#)

Robert G. Ferrell

[Privacy Statement](#)

Copyright 2006, SecurityFocus