

Episode Four: Through a Glass, Darkly

Robert G. Ferrell 2001-01-31

Chasing the Wind, Episode Four: Through a Glass, Darkly

by *Robert G. Ferrell*

last updated Jan. 31, 2001

After several days of filtering through the data he'd downloaded from the Acme Ailerons facilities workstation, working an hour or two at a time as he had the opportunity while studying for semester exams, Ian came across an interesting item. It was a CAD file that contained blueprints for a new building scheduled for construction the following spring. Ian didn't know much about architecture, but he was insatiably curious. So he took to the Net to look up some of the information he saw listed on the blueprint. Two of the references that caught his eye were "NSA-65-6" and "NSA-73-2A." After a fair bit of data mining on the Web, Ian managed to track down these numbers. They were U. S. government specifications.

NSA 65-6, NACSIM 5204, R.F. Shielded Enclosures for Communications Equipment: General Specification, National Security Agency.

NSA 73-2A, NACSIM 5204, National Security Agency Specification for Foil RF Shielded Enclosure, National Security Agency.

Ian was no expert on the intelligence community - all he really knew about the NSA was based on the uninformed and derogatory comments made about the agency by his online brethren. However, he saw no immediate reason why blueprints for a new facility would refer to an NSA standard for electronic shielding. Acme Ailerons seemed to make most of their money in the avionics field, crafting custom instruments for specialized applications in the aerospace industry. Ian concluded that the new building was going to house a laboratory for developing some sort of instruments for the Department of Defense. He didn't know enough about aircraft instrumentation to even hazard a guess at what they might be planning to produce there. "Probably some new bomb sight or something," he mumbled. Most of his knowledge in this area came from old movies and watching archived footage of Desert Storm (he was too young to remember the actual events very clearly). He would monitor the progress of this project with interest. It just might prove to be the 'scoop' he needed to get in with the Bandits.

Jake finally finished his examination of the compromised machine. The attacker had done a good job of covering his tracks. If it hadn't been for the Tripwire warning, in fact, Jake realized he might never have discovered the intrusion at all. One last time, he ran every virus and trojan locating utility he had managed to acquire on the box, just to make sure that nothing was lurking in the shadows of the

operating system, waiting to jump out and say "boo" at him somewhere down the line. Everything looked to be clean. He sighed and wiped his brow in a ritual gesture of finality. Nothing to do now but make sure the patches stayed updated. It was time to go home and get a little sleep after his 17 hour day.

Bob slowed the car and rolled down the window as he approached the security post. Even though he had a sticker on his front bumper that granted him access to most military posts as a retired officer, this one was different. No one got in or out without positive identification and a metal detector sweep. He showed his ID card to the guard, who made a tick mark on his clipboard. "Please step out of the vehicle and through the metal detector, Colonel." The guard was polite but completely businesslike. Bob did as he was told and passed through the detector without incident. "Right thumb on the pad, please, Sir," said another guard, motioning to a small box on the counter of the guard shack. The monitor screen lit up in green with the words "Briley, Robert P. O-6 R SCIF Active"

"Thank you, Colonel," said the first guard, handing him an orange key card. "This is your facility key for the Orange Labs. The inner doors are all biometric to your thumbprint. Colonel Briggs will meet you in the Officer's Lounge in Building 27. Have a nice visit, Sir." The guard saluted sharply. Bob returned the salute a little stiffly - it had been a while.

The base had changed somewhat, but not to the extent that Bob had any difficulty navigating. The buildings were color coded with stripes according to the security level necessary for entry. Blue was the lowest, followed by green, yellow, white, and the highest, orange. He noted several new orange buildings on the little map the guard had given him, one of which seemed to be mostly underground. It was interesting to speculate on the cause for the new construction, since the base itself had been targeted for closure in less than a year. This part of the facility had always been a universe unto itself, though. Even the telephone prefix was unique among the rest of the base.

He found Building 27 without any trouble. It was a Command, Control, Communications, Computers, and Intelligence (C4I) center, with a properly impressive neo-classical facade and the red tile roof that was standard issue for the base. He parked in the visitors' area, which positively bristled with pan, tilt, and zoom surveillance cameras. He swiped the orange card through the reader at the door and was concerned when nothing happened. He realized after a few seconds of puzzling that he had swiped it with the magnetic stripe on the wrong side. It was getting harder and harder to stay smarter than technology; even opening a door these days required an engineering degree and three references. Bob chuckled grimly at his own little joke, since there wasn't anyone else around to do it for him.

Colonel Briggs was waiting for him in the lounge, as advertised. Neither had seen the other for a couple

of years, since a retirement party for a mutual friend.

"How are you, Will?" Bob asked the officer, shaking his hand.

"Never better. How's civilian life treating you, Bob?" Will Briggs was a large, vital man, balding with brown hair and a round face that seemed too accustomed to laughter for a man in his stressful position, which was so classified even he wasn't allowed to know what it was all the time.

"Can't complain," Bob replied, then added, "except for present circumstances, of course." He smiled as he said it, but Will could feel the sharp undercurrent in his tone of voice. He nodded his head sympathetically.

"Let's get a cup of coffee and head over to my office."

"Sounds like a plan."

Douglas sat at his desk and read through the thick sheaf of documents that had been delivered to him by an armed Air Force Senior Master Sergeant. The whole thing was a little spooky at first, but the project outlined in those pages was sufficiently interesting that he gradually allowed the cloak and dagger culture-shock to recede into relative quiescence, where it merely taunted him from a distance.

The engineering feat he and the others on his team were being asked to perform was far from trivial. In fact, it was closer to science fiction than any project with which Douglas had previously been engaged. It seemed to involve some physics that must have escaped his notice in school. Maybe he'd been sick that day.

After a couple of hours of reading, it became obvious to Douglas that he wasn't 'getting it.' He hoped that he could just build the thing without worrying about how, exactly, it was supposed to work. He wasn't even sure how to tell if it *was* working.

Ian sat at his keyboard, skimming through some port scan data he'd collected the night before. He was in a mood to do a little defacing today, so he was looking for port 80 traffic to identify potential Web servers. He grepped the text file for '80' and got back a nice list of candidates. Some of them were identified by IP address only, meaning that no canonical name mapping existed for them in the Domain Name System. One of these numeric addresses looked strangely familiar to Ian. So he pulled up a little Perl script, which he had found on the Internet, that automated 'whois' lookups and fed the dotted quad

into it.

It was assigned to the Acme Ailerons address space.

Ian's eyes lit up like a child's on Christmas morning. He grepped the scan file for the address and found the telltale signs of an NT box. Things were definitely looking up. Time to dig out the RDS exploit and see if the fish would bite. First, though, he decided to do a little 'recon'. He went to an anonymous Web-surfing site and entered the address of his target. After a few seconds, a generic IIS 4 welcome screen popped up. This bonzo either hadn't bothered to install an index page, or, better yet, didn't even know he was running a Web server. How much luckier could Ian get? He twirled around in his computer chair in a little geekish pirouette of triumph.

This looked like a job for msadc.pl. It had been coded by a well-known hacker (rain.forest.puppy) and used by legions of script kiddies who didn't understand how it worked (which was, in simple terms, to take advantage of the fact that NT system commands could be embedded in remote data services queries made to a server running the default configuration of IIS 4 with the option pack installed.) Ian understood the basic premise of the script, if not every little nuance. He had realized that the only way to evolve out of the script kiddy tadpole stage was to tear apart exploits and understand their mechanics, one line at a time.

Late that night, Ian slipped on the old "Buckaroo Banzai" head band he habitually wore while engaging in cybercombat and fired off the msadc script at his newly discovered victim.

Step 1: Trying raw driver to btcustmr.mdb

Ian watched directories print out as the script tried to brute force a connection to a little-known inactive database installed by default on the system.

Success!

This meant that the very first attempt to create an exploitable connection had succeeded. This was, in all probability, a totally default and, most likely, totally unattended Web server installation. Ian almost wet his pants.

He flew through the rest of the script execution in a state of unbridled joy. When the time came, he uploaded a small HTML file he'd created just for this occasion. It contained a rather rude graphic and a few lines of text.

```
U have been h4x0r3d by ir8_d0g. Ph33r my 5ki115!!!  
Gr33tz to Br04dB4ndits (they rule), #underdawgz, & Beverly (shes so fine!!!)
```

Remember: !ADM!ROX!YOUR!WORLD!

Ian sat back and surveyed his handiwork, content and happy. He surfed over to the newly hacked index page via the anonymizer and was almost moved to tears by the sight of his defacement on the Acme Ailerons computer. He sat up suddenly and dashed off a note to hacked@attrition.org. Not much point in defacing a page and not getting credit for it, was there? He also sent a little announcement to one of Beverly's friends (Beverly was his latest heartthrob) with whom he was on good terms, since he was afraid to tell Bev directly that he'd declared his affections to the whole planet on a defaced Web page. You'd think that would rock, but you never knew how girls were going to react to stuff.

Ian didn't entertain any delusions that this kiddie defacement would impress the Bandits, but he decided to plug into his favorite IRC channel (#underdawgz) and see if any lesser mortals noticed. Word fame is, after all, word fame.

Will raised his eyebrows and sat back heavily in his executive chair with the U.S. Air Force logo emblazoned on the head cushion. He was sucking on a jaw breaker and seemed for a moment to be choking on it. He dislodged it from his throat after a brief struggle, however, and spat it out - it's hard to sound serious with a marble in your mouth.

"That has to be some sort of hoax," he said to Bob, "you haven't even built the facility yet."

"That's what I thought at first, too, but what if it isn't?"

"All we can do at this stage is keep our eyes open and follow the security protocol to the letter," Will replied after a moment of consideration, "and hope for the best." Bob nodded in agreement and stood up.

"Oh, just leave that tape here with us, if you would," Will added, "and I'll ship it off to Ft. Meade to see if they can make anything of it." He cleared his throat. "One last thing, Bob. I'd appreciate it if you didn't involve anyone in this who wasn't absolutely necessary. It's going to be tough enough dealing with this glitch as it is, without raising any red flags in the Pentagon or Langley."

Bob tossed him the cassette and gave Will a little half-smile: "I think I can handle that."

To Be Continued...

To read **Episode Five: The Devil in the Details**, 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

[Privacy Statement](#)

Copyright 2006, SecurityFocus