

Security audit

By Joel Shore

Professional auditor Shawn Bernard of Networks Unlimited exposes risks overlooked by IT staff of a New England medical center.

Only a security audit can expose the truth about a network's vulnerability. To see how well-prepared a typical enterprise network is, we found a business willing to let us tag along while a professional auditing company poked and probed 28 of its servers, and then delivered its findings in a face-to-face meeting.

The results were frightening — and should sound the alarm for IT directors everywhere.

The company, a major New England medical center (we agreed to conceal the name), has thousands of network devices, but had never been audited. It relies instead on a "high level of confidence in our senior engineers and technicians," says the company's technical services director. The idea of an audit, he concedes, had "come to mind time and again."

Finally, the time had come.

Let the audit begin

Networks Unlimited operates from a 19th-century hilltop Victorian mansion framed by giant sycamore trees. The Hudson, Mass., company audits a diverse mix of businesses - banks, retailers, law firms and government agencies - and provides security solutions. Business is booming.

The purpose of a security audit, says company President Harry Segal, is not to access or corrupt sensitive data. Rather, it is a controlled demonstration that these acts could be carried out. Documenting the breaches and identifying files at risk makes you a security auditor. Access those files and you've crossed the line into hackerdom.

In what was once the dining room, under an ornate gas-lit chandelier, Segal and security engineer Shawn Bernard huddle over a PC, eager to begin a complete security audit of 28 servers, hand-picked from hundreds by the hospital's IT staff. Sitting under a wall adorned with security and vendor certifications, they'll pass this night probing the network, searching for weaknesses, exposing the potential for digital dastardliness. Two weeks later they'll present their findings - and advice - to managers in the hospital's technical services group.

Bernard is gregarious, quick to talk about his family and just as quick to note that he maintains close ties to the hacker community - to better learn about their latest exploits, techniques and tools. Segal spent years at NEC Information Systems and erstwhile modem maker Microcom.

"We will always find issues that must be addressed quickly," Segal says. The top reason for security breakdowns, he says, is almost laughable: company policies that limit server maintenance to just a few weekend hours. "If you discover a security breach - fix it! Now!" he says. "Wait for the weekend maintenance window, and by Monday there might be no business to come back to."

Bernard's PC is loaded with a software smorgasbord any hacker would envy; his tool of choice is Internet Scanner from Internet Security Systems. Internet Scanner provides automated network-vulnerability assessment across servers, desktops and infrastructure devices. It also probes network services, operating systems, routers, switches, servers and firewalls.



"We'll be testing for 1,211 different types of vulnerabilities," says Shawn Bernard of Networks Unlimited.

"We'll be testing for 1,211 different types of vulnerabilities," Bernard says. One mouse click, and the audit is underway.

Segal adds that this audit is testing only for vulnerabilities from the outside world. A complete audit would also look for - and inevitably would find - internal vulnerabilities.

This audit is somewhat different than most because the IT staff was warned. Usually, the rank-and-file IT staff receives no advance notice. It's not until the final report is presented at a department meeting that the secret is revealed. "We don't want people running around in a frenzy plugging holes," Segal says. "An audit should be a snapshot of business as usual."

Easy access - too easy

As Segal is talking, Bernard suddenly perks up. He's discovered what seems, at first, merely odd, then surprising, then unimaginable. "We've found servers running Compaq's Insight Web management software," he says. "This is not a good thing."

By using one server as a proxy, the other servers let Bernard bypass the perimeter security of the network firewall. In just moments, he gains access to a BayStack hub, residing between two Nokia firewall devices. The hub's factory default password was still in place, easy pickings for an attacker who quickly could disable the device, plunging an entire network segment into digital darkness.

"This is pretty serious," Bernard says, noting that it might be possible to reach any of the hospital's hundreds of servers, not just the 28 in this audit. Bernard takes a few notes and moves on.

Probing further, Bernard stumbles across a Compaq server running the hospital's HP Jetadmin printer-management software. Why this application or the Insight Web management software would be Internet facing, that is, visible to anyone who would bother to look, is anyone's guess. Although possibly no more than a configuration error, it is akin to a flashing neon sign, extending an engraved invitation to the malicious mind bent on amusement or criminal mischief. Except that neither Bernard nor an attacker would know the password.

Not a problem. He visits a favorite Web site, one that, for better or worse, publishes common logon ID and password combinations for thousands of products.

It takes one try. One try! We're in. We see the name, model, network address and physical location of each printer. We can check toner levels, firmware version numbers, page counts. Could we actually intercept a print job? Anything is possible. Not easy, but possible.

"I can go in and change the control-panel language on hundreds of printers," Bernard says. "I can swap queues. I can send print jobs to every printer saying 'you've been hacked.' I can take them offline. I am in total command."

But wait, there's more.

- Bernard finds a server running an outdated copy of Microsoft Internet Information Services that's badly in need of an updated security patch.
- A mail server is running the Simple Mail Transfer Protocol verify command, which an attacker could use to validate the existence of specific e-mail accounts.
- A proxy service, vulnerable to a denial-of-service attack, is several patches out of date.
- A server running the pcAnywhere remote-access program is discovered.
- A server is running Network News Transfer Protocol, a service that could let users post to and read from newsgroups without authorization.
- Ports galore are open, for no apparent reason.

With the sun rising, Segal and Bernard call it quits. Confident that the breaches they've unearthed is enough to mortify IT director, they save their mountains of data, log off and head home.

Tomorrow, the pair will start compiling the results from thousands of port scans, vulnerability checks and surveys of software versions, resulting in a report nearly an inch thick. Then it's off to the client with the bad news.

Don't shoot the messenger

Two weeks later, we pile into Segal's minivan. It's report-card day, when the hospital's IT staff learns if its network is healthy or needs immediate surgery. As we enter an IT conference room, the technical services director and about 15 staffers shuffle in, coffee mugs in one hand, notepads in the other. Expressions range from "I think we're OK" to downright fear.

Moving quickly to defuse a potentially adversarial meeting, a diplomatic Segal says, "We're here to help you do your jobs better." No one nods to agree. "Security here is already very good, but we've found a few things you can improve," he says. Later, Segal acknowledges he would have used harsher language if the presentation had been a one-on-one with the technical services director. On this day, IT has safety in numbers.

Bernard takes over, handing out his inch-thick report, explaining it page by page.

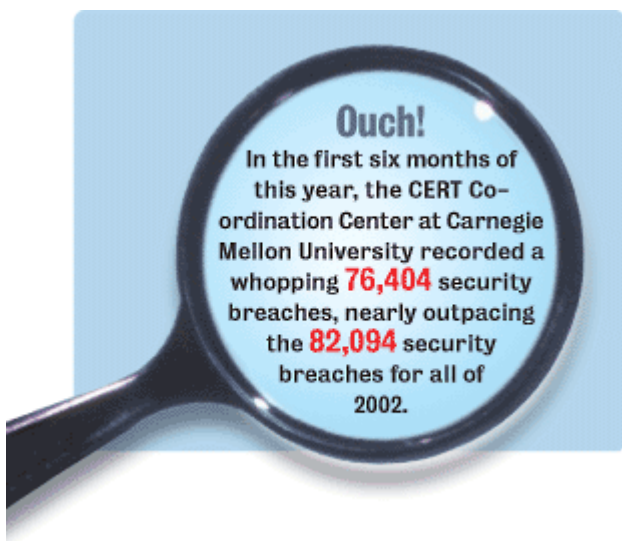
All 28 audited servers are listed, led by the most vulnerable. First place goes to the server running the Compaq management software. It should never have been visible outside the firewall, because anything it talks to, a hacker can, too.

It's all there: IP address, domain name, operating system and version. The problem with Compaq Web-based Management Software Version 4.7, installed on Port 2301 - the default, open to anyone - is described in detail. Bernard describes how a hacker, sending a username containing exactly 460 bytes could cause a buffer overflow, allowing the execution of arbitrary code with administrator privileges.

Fixing this potentially deadly breach is easy: download and apply the appropriate patch as listed in Compaq Security Advisory SSRT0705. Skip it and risk everything.

And on it goes. Bernard describes each vulnerability in detail and suggests a remedy. Sometimes it's a patch, stopping an unneeded process or closing a port that's open.

Tempers never flared. The discussion was surprisingly placid. "Yeah, we already knew about that one and planned to fix it" eventually gave way to relief that most breaches were someone else's problem.



"Some things we don't control," one staffer said.

"They had to subvert another group to get to my group," another said.

"The executives here are focused on the hospital's clinical mission," yet another said.

Not at all a good reaction, according to Segal and Bernard. "If this was a bank," heads would be rolling. "This is a hospital. Security is no less critical. It's everybody's problem," Segal says.

As for the technical services director, the IT manager who agreed to the audit, his calm reaction to the litany of potentially catastrophic security breaches was an enigma to Segal.

"I was pleased to see that the majority of the findings were relatively benign," he said in a follow-up interview. "We had fully addressed all but one of them by the next day."

Not nearly good enough, Segal says. "This is a business that should be extremely security-conscious," he says. "In certain areas, I could see a determined effort by the IT staff to have strong security, but they failed miserably in others."

Harsh words from a man who just played the diplomat. Bernard says: "Their senior engineers and technicians deserve praise, but having 'good people' is not the same as having proper security. Good people make honest mistakes."

Lessons for all

The Networks Unlimited audit could have been much worse. This audit was unusually narrow in scope, but a more sweeping audit undoubtedly would have uncovered additional failures.


"This was a limited external audit," Bernard says. "We didn't look at internal security, but you can be certain they haven't implemented adequate internal security to protect critical data and operations from unauthorized access."

On the ride home, Segal gets philosophical. "Every business is vulnerable," he says. "This one is no different. Hire an auditor and fix the problems before it's too late."

Was it too late for our patient, the regional medical center? "Darn lucky," he says. "Darn lucky."

Reducing the risk

Networks Unlimited President Harry Segal, recommends these low-cost steps you can take to make your network a safer place:

	Reducing the risk Networks Unlimited President Harry Segal, recommends these low-cost steps you can take to make your network a safer place:
Do	Don't
<ul style="list-style-type: none">• Estimate the cost of a break-in to guide your security decisions.• Configure firewalls to deny all traffic, then open needed ports.• Change default passwords before	<ul style="list-style-type: none">• Don't connect unpatched machines directly to the Internet.• Don't ignore old servers whose purpose and ownership are uncertain.

deploying software or hardware.

- Delete unnecessary user accounts (guests, anonymous).
- Establish and adhere to a process for obtaining and applying patches.
- Use only VPNs for remote access.
- Implement intrusion prevention to stop attacks that can pass unimpeded through the firewalls.
- Beware of internal attacks that might be initiated not by a user, but by the user's machine.

- Don't assume anti-virus programs protect against all malicious activity: Many hacker tools use legitimate software not detected by anti-virus programs.

- Don't trust your staff — or yourself: Have an experienced third-party review security regularly.

- Don't believe that firewalls protect all: Many attacks appear as legitimate traffic.

- Don't ignore the security threat from internally connected laptops or VPN-connected remote systems.

- Don't let external PCs connect via remote-control software.

- Don't provide unlimited network access to business partners.