Jack the Hacker Tells All:

Insights into Security Do's and Don'ts

Legal Notice

NetIQ Corporation provides this document “as is” without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. Some states do not allow disclaimers of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

This document and the software described in this document are furnished under a license agreement or a non-disclosure agreement and may be used only in accordance with the terms of the agreement. This document may not be lent, sold, or given away without the written permission of NetIQ Corporation. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Companies, names, and data used in this document are fictitious unless otherwise noted.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of the document. NetIQ Corporation may make improvements in and/or changes to the products described in this document at any time.

U.S. Government Restricted Rights: Use, duplication, or disclosure by the Government is subject to the restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of the DFARs 252.227-7013 and FAR 52.227-29(c) and any successor rules or regulations.

Jack the Hacker Tells All:
Insights into Security Dos and Don'ts

Want to keep the bad guys out? This handy guide, *Jack the Hacker Tells All: Insights into Security Dos and Don'ts* relays the ins and outs of security implementation, as told by Jack the Hacker. In this guide, the reformed hacker cracks away at myths surrounding the implementation of a sound IT security plan and offers tips for your best bets for network security. Get a glimpse into the mind of the very people who break into your computer systems and intrude on your company's privacy.

Taken from two chats sponsored by NetIQ–"Inside the Hacker's Mind"–Jack the Hacker Tells All will show you how to develop and implement a successful security strategy to protect your corporate network infrastructure. Learn about the security defenses, how to protect your organization and ways to respond to security threats before they become major incidents.

Architecture

We are about to start hosting our own Web server. Are the securities built into Windows NT 4 enough or should we use a firewall?

Jack_the_Hacker: If at all possible, always invest in a good firewall, as well as sound architecture for the Web server. If you are able to invest in an appliance firewall, buy one with three interfaces. If you can only invest in the software, then you should be able to fit a server with three NICs to create a buffer zone in which to put your Web server. One interface is for the Internet, with a second NIC for the internal private network and the third for a DMZ (Demilitarized Zone). The security built into Windows NT 4 and Windows 2000 hosts is good. But when subjected to numerous scans and cracking attempts, some default installs will be cracked within only a few minutes to an hour. That is why you should keep current security patches for the OS and applications that run on the server.

Are there any known security issues with Windows 2000 Server running remote routing functioning as a VPN?

Jack: To date, I have not yet worked on this ability of Windows 2000. I would recommend a more specialized VPN solution over the Windows 2000 solution. I am currently looking at the ISA product, and will be able to give you a better answer after some more testing with it.

What are the basic areas I need to secure on a Web site?

Jack: How many sites on attrition.org were defaced by the RDS script? Quite a few. The basic areas that I look to hardening are the OS by checking for current security patches and implementing them on a test machine before even throwing my site up. That is just for the Web server. For the perimeter defense, you should throw a firewall up and create the Web server into the DMZ.

We have a connection that is monitored by our sister company. Very early in the morning, our bandwidth usage goes through the roof. We are not aware of anything running at that time. What would you recommend we use to determine what is occurring? Could someone be taking advantage of a security hole?

Jack: The ever-present sniffer is your best friend. Put a sniffer on the link between you and the sister company. The problem may be a kit looking for other servers in a massive blast, a mis-configured server or a security hole, but the sniffer logs will let you know where to start.

As far as NAT routing is concerned, can vulnerabilities be exploited even in this type of hidden internal network? Beyond just Trojan's getting in?

Jack: NAT (Network Address Translation) routing is another security measure that more companies are using. Taking over a router is still a mainstay in the cracking community. Just because someone can't get to your internal network due to private addressing doesn't mean that they will take another route to your systems. Your routers are still there for the taking.

What is your idea of good security implementation?

Jack: One in which policies had been set in place before the actual implementation. Set aside the test environment. Verify the patches that are installed on the machines don't make them quit functioning. Make sure that policies are strictly adhered to, but the policies must be workable as well. Creating each and every one of your servers in C2 compliance will not work if you want them to talk to one another. You must make trade-offs to have the systems work coherently. A good process consists of a month or two of testing desired policies to determine what is feasible, followed by the architecture's implementation.

Are there any issues with implementing a NT domain in a DMZ? We want to set a Microsoft Cluster in the DMZ.

Jack: Make sure that no one trusts that domain. You can set the cluster up in the DMZ. But remember what the risk is with the DMZ – the DMZ is going to be hacked.

What are the advantages of using a VPN vs. a modem pool as far as security is concerned?

Jack: A modem pool is usually not secured very well, and a war dialer can find the pool rather easily. The VPN uses encryption by its nature and can withstand most petty attempts at breaking it.

What are the best methods to secure the internal network from disaffected users?

Jack: Proper adherence to a security policy that involves Human Resources should minimize the risk. However, as empirical data shows that this may not be enough. Depending on how large the corporation is, this task grows exponentially. If the user had minimal access, then the security admin won't have much to do. Close communications between HR and Security teams should lead to swift and effective severance of access. Again, it rolls back to a security policy than a technology issue.

What do you think of using protocol control, such as frame relay connectivity for internal communications, within an enterprise and then have firewall and proxy control to limit/control access in and out of the enterprise through the Internet at large?

Jack: This is a very good idea, but can be a very difficult and extremely costly implementation. The more complex your solution, the greater the likelihood is that you'll have vulnerabilities in your infrastructure.

Is there a definitive, or nearly definitive, way to secure an enterprise against hacking?

Jack: Disconnect from the Internet, pull the modem banks and do no business. You also have to make sure that your initial implementation of your architecture is sound. Make sure that security policies are in place and employees adhere to them. No rogue servers should be allowed onto the network. Development networks should have firewalls on them to segment them away from other departments, as well as maybe the accounting and finance areas. At the same time, try not to make the architecture too complex. You have to find a happy medium, one that is secure but also allows communications to occur.

We are currently using dual firewalls configured for high availability, security routers and a packet shaper that is doing some filtering. Do you think that we also need to use IDS (Intrusion Detection Systems) on top of this to secure our environment?

Jack: From what it sounds like, your current architecture is quite sound. I think the IDS would help you find out some internal activity, but it sounds like you aren't letting a lot get through. That is a pretty secure environment.

How do you suggest better protecting servers in a DMZ?

Jack: DMZ servers are your "sacrificial lambs." These are the servers that you hope don't get hacked, but will eventually find their way to the ATTRITION mirror. Here are some steps you can take. First, patch the systems very quickly after advisories come out and you test them for your environment. You must make sure the servers in the private network never get hacked. Next, use encrypted channels as often as you can. And finally, harden the OS to disallow easy hacks and tighten the ACL (Access Control Lists) on the routers to allow only trusted traffic.

Can you talk about what defenses we should establish in order to prevent an attack (i.e. SP's, hot fixes, additional software)?

Jack: Those defenses deal with the OS, the root of all evils. An application cannot run without its OS. Now, keeping up with Service Packs and hot fixes is a main staple to all IT and Security personnel. This helps you keep track of most of the new hacks coming out for which script kiddies have tools. But remember – test them first to see if they develop other problems with your applications. Some additional software that could be looked into is quality control for your home-brewed applications. Make sure your developers adhere to strict coding guidelines that don't introduce buffer overflows.

Would you say that using an IP address from the 10.0.0.0 range on your internal networks is a good idea?

Jack: If you are trying to get the most addresses, then yes, that makes sense. Try picking something a little less obvious than 10.0.0.0, but that is my preference.

Honey Pots

What is your opinion of honey pots? Have they become an effective deterrent?

Jack: As a security person, I like to see a honey pot implemented. However, these systems usually allow too much time on their system that normally raises a flag for me. They are effective in learning new techniques of hackers, but a security team must know when to step in and pull the plug.

Are honey pots having an impact in the cracker community?

Jack: The more skilled hackers don't even deal with less-than-secure systems. Those hacks are the ones about whom you will never read. The less-than-skilled kiddies normally have no idea they are on a honey pot until the plug is pulled or they hear a battering ram on the door. The use of honey pots is having an impact on crackers because they are more leery, but the white hats are gaining a lot of information right now. Maybe in the future, these systems may not have the impact that they do now. But they seem to be keeping the white hats in step with the other side.

How do you feel about the deployment of honey pots and IDS systems? Are they too obvious?

Jack: Honey pots and nets are a good thing if you are really interested in the research value and want to update your own IDS systems. But they do not offer enough protection to warrant investment as a means of protection. The IDS is definitely necessary and is more obvious than a honey pot.

What is your take on creating a honey pot on your network? Does that attract more attention or is having only a firewall better?

Jack: I like Honey Pots only for research purposes. If I notice a large increase in traffic to a specific port or range of ports, I will throw up a couple of honey pots to capture the data and analyze it. If I am not aware of a new exploit, then that research is invaluable.

What is the best installation or application for a honey pot?

Jack: Read the new white paper by Lance Spitzner at http://project.honeynet.org/papers/honeynet/. If you are looking at a commercial honey pot, then the Sting server from PGP is good. Otherwise, a default install of an OS and slapped onto the 'Net is a pretty good start.

VPN

How do I protect the corporate network from hacks affecting my remote/VPN users?

Jack: This is one of the most difficult hurdles to overcome in the security field – remote usage. Multiple tools and programs that are now on the market give security personnel more control over what a remote user can have access to, as well as provide another layer of security for the internal network. Personal firewalls, such as Network Ice's BlackICE Defender, their corporate solution ICEpac Security Suite and ZoneAlarm PRO, give you a better chance of catching certain attacks on your remote users. On another level, you can invest in Check Point's SecureClient if you have a Check Point firewall solution, or in RedCreek Communications Ravlin Soft software solution.

What tool should I use to do port scans to ensure my router and VPN installations are not left open to hackers?

Jack: One of the best-known tools to use is nmap (or the Win32 ported nmapNT). This is a tool-de-jour of most script kiddies and malicious crackers. Using libnet from the Packetfactory gives you the ability to craft your own packets to test your router configuration.

How secure are VPN technologies, such as Check Point's VPN-1 software suite?

Jack: VPN authentications, such as Check Point, are very secure. Check Point especially utilizes Triples DES encryption. So from a mathematics perspective, the VPN knows who you are. In addition, Check Point's secure VPN clients offer a personal firewall with policies that can be controlled via central management. This allows for the VPN to reject a non-secure connection.

Can you share your tricks on accessing VPN?

Jack: This all depends on the VPN itself. I don't have any tricks on getting through to a VPN because that is a realm into which I have not delved. Looking at some of the documentation from @stake, the latest incarnation of MS-CHAP looks like some of the same procedures are used between v1 and v2. The same procedures used to derive a 24-byte response can be sniffed and a dictionary attack can be staged against them.

Have you tested the Lucent LSMS? How do you think the LSMS stacks up as a firewall/VPN device?

Jack: I have not yet tested this product.

Public Key Infrastructure

How secure is PKI?

Jack: The answer is two-fold: What problem are you trying to solve, and what size implementation are you seeking? PKI as it stands is quite secure, and studies on the RSA 512 factoring conclude this. the RSA 512 has been factored, but how many people do you know that have access to more than 300 computers running parallel and then feeding the matrix to a Cray? Not many. If you are trying to solve just a private e-mail issue, than you don't necessarily need a full-blown PKI solution. If you are looking for a complete implementation, than PKI is good for the company. Technology-wise, this is a secure product. As far as implementation, PKI is what you make it, and that is where the problems arise.

Jack, who do you believe has a better security key solution - VeriSign or RSA's Keon solution?
Jack: To me, it depends on who you want running the show, Verisign or yourself. If you don't want to deal with the headaches of setting up a new PKI infrastructure, then go with Verisign. If you want total control of your keys, than choose Keon.

Firewalls

Should a company employ a firewall to prevent internal malicious users from doing damage?

Jack: Internal firewalls are a good thing when you want to segment groups or address ranges. Firewalls make traversing the network without being noticed more difficult for malicious employees.

From your experience, which are the best and worst firewalls?

Jack: This is personal preference issue. If I tell you that I like firewall A and you like firewall B, and you think that B is better than A, and I think the opposite, what has been accomplished? You don't like A and I don't like B. This is much like the Ford v. Chevy – you like one and hate the other. For me, Firewall-1 has done a good job to this point. I like PIX as well, and I have worked with Gauntlet.

Is one OS/platform better than another when it comes to firewall implementation?

Jack: There is no one platform better than another. Harden the OS, remove all of the unnecessary services and make the machine a standalone. Or run an appliance firewall like Nokia, CyberGuard, SonicWALL or Cisco.

In your opinion what are the best hardware firewalls on the market? Which ones are the hardest to crack?

Jack: Nokia Firewalls and CyberGuard appliances seem to be the best right now. The IPSO OS on the Nokia devices are essentially hardened OpenBSD machines, which are pretty difficult to crack. The KnightStar devices are pretty difficult as well, but the main obstacle is implementation/proper configuration.

What vulnerabilities are commonly exploited with MS Proxy and do you think ISA will be better?

Jack: A Proxy Server or firewall is only as good security-wise as the underlying OS - that lends itself to security risk. I won't speak on Proxy Server, but with respect to ISA - too much on one machine. The refining process is going to take some maturing, just like Check Point and some of the other top security products have.

What are your thoughts about firewall appliances and are they more secure than software-based firewalls?

Jack: By far. Vendors have gone to a lot of trouble to harden the OS, and have removed a lot of the probable "red zones" where administrators make implementation mistakes on OS-based firewalls.

Canned firewall or build your own –which is better?

Jack: Canned

What about Cisco PIX Firewalls?

Jack_the_Hacker : Cisco PIX firewalls are Proxy-based firewalls. They do offer reasonable protection but their vulnerability is in management. If you are utilizing multiple PIX firewalls, a high probability exists that vulnerabilities will be introduced through simple mis-configurations.

What software firewalls do you recommend?

Jack: Check Point.

When my firewall gets port scanned, I would like to know what this "offender" is actually doing. Does such software exist that gives me an idea what's outside the firewall?

Jack: Check your border router logs and run a sniffer on the line. You can't see what is going on unless something picks up the data.

Given the choice of a software firewall that you install on a server or a separate hardware device that you place in front of the server, are there any advantages or disadvantages to either one?

Jack: If you are talking about software versus appliance firewalls, I like both. Unless you are comfortable in hardening your server that you are going to install the firewall software on, then I suggest the appliance. If you know exactly what you want in your server, then install the software firewall. Remember, in the end, they are both the same firewall application.

How secure is a network that lives behind a correctly configured Check Point Firewall?
Jack: Correctly configured is a vague statement, but I would say that is safer than before. Do you remember what port you usually open up for you to host your site? 80? It's still an open port. The fewer holes in the firewall, the less with which crackers have to work.

Personal Firewalls

In my opinion, the next security product is going to be the personal firewall. How secure will these be? Are users going to be lulled into a false sense of security?

Jack: I would tend to agree with you on the widespread usage of the personal firewall. A report completed fewer than 3 months ago showed a large hole in the basics of these firewalls. They are basically proxy servers. So if you can get someone to open a Trojanized program (i.e. Explore.exe), you have bypassed the security. Users will get into an automatic mode with these tools as they see the scans register.

What do you think of ZoneAlarm?

Jack: ZoneAlarm is a great personal firewall, but every personal firewall has one main flaw - policy management. We're not going to go into that here, but a recent case study reviewed the overall security of all personal firewalls. You can probably find that case study with a Web search.

Jack, please tell me what you think. How secure are small PC [windows] networks [always on cable or DSL] that run firewall programs like ZoneAlarm or BlackICE?

Jack: Having the personal firewall programs is better than nothing. They do a pretty good job at keeping out the truly amateur individuals, but nothing against some higher-level script kiddies.

What would you recommend for a personal firewall for desktop users with cable or DSL connections?

Jack: Of the three main personal firewalls, I like ZoneAlarm, mainly due to price. I think that BlackICE is darn good as well, and so is Norton's solution.

Hacking/Auditing

How can I test my security from external attacks?

Jack: Penetration testing is the main source of information that tells you whether you have done an adequate job of securing your environment. How would you do the pen. test? Black-box it. Try to have someone in the infosec team run the test without any prior knowledge of the target. Run such tools as firewall tools, port scanners and more.

What are some good footprinting tools? Where can I get them?

Jack: Nmap – get it at www.insecure.org. There are plenty of others, but this is the most used one and the best right now.

Are smaller companies' networks less attractive to a hacker than a larger company? Or maybe more attractive because they could be more vulnerable?

Jack: Attractive nonetheless. I would use that as a waypoint for more ambitious goals. Small companies make for good decoys. Most small companies want their systems to run and are not as interested in security. They will know they need security when IBM calls them and says that their logs reach back to XYZ Company attempting to break in.

What is the industry standard with regard to third-party ethical hacks being accepted by clients? We are getting more clients requiring their own ethical hacks, and they are not allowing third-party hacks to be used for security assessment.

Jack: There is not an industry standard at this time for third-party ethical hacks. This is more along the lines of: Do the ends justify the means? If you are in an industry where security is a paramount issue, then ethical hacks are necessary. If you are in one where security has taken a back seat, then an ethical hack may not be necessary.

How do hackers stay in touch with one another today?

Jack: IRC is my friend and compatriot. If you see that running on your system, you have an issue. Squash it. ICQ, and some message boards are also popular methods.

What tools do you recommend for penetration testing?

Jack: Tools from Foundstone are good, tools from farm9.com seem to be good. But this is more of a services function from consulting firms, such as Ernst &Young and Accenture.

Where would I find a copy of nmap or nmapNT?

Jack: Insecure.org and eeye.com, respectively.

Are most external attacks basically random? Or are they more planned, as in a need to garner a badge of honor for some club of attackers?

Jack: Mostly random and looking for the recognition, or for trying to join a crew. Look at SilverLordz, Hackweiser, and some others that have been on a tear lately. The more planned external attacks lie dormant for extended periods of time, and may or may not be the work or a true hacker, not a skiddie.

If you're a newbie infosec, besides nmap, where would you go for information on penetration testing.

Jack: SANS.org is a good place for information. Get on the Pen-test listserv from Securityfocus.com and Vuln-dev list.

What are your tools of choice when searching for vulnerabilities?

Jack: Security Analyzer from NetIQ does a great job and comes back with a thorough list.

Besides social engineering, what are your other favorite exploits? Where do you see the most problems with a security implementation, besides human error?

Jack: Mis-configuration is one thing, but admins forgetting to implement patches in a timely fashion is another. How long has the NT RedButton vulnerability been out? Yet you can still find this on the Net. How about the wu-ftpd problems? Same thing – still out there. IIS has taken a lot of flak recently because of rain forest puppy's research, but the disclosure of these holes is important to companies that want to do business on the Net. Make sure your admins keep current.

Would a hacker be more inclined to go after a target because they have a broadband connection versus analog dial-up? Or are both equally at risk?

Jack: Both are at risk, but having a broadband connection as a pipeline is very enticing to a cracker. If I take over a machine running 98 with a 1.5MB line attached to it, I have a great place to start most of my attacks. "Always-on" connections are easier to find than dynamically assigned addresses when dialing up to an ISP.

What was site interested you when you were hacking?

Jack: That depended on my mood of the day. If I wanted a challenge, hacking into a larger corporation would take a few days to a week, while just wanting to be playful prompted me to access small businesses that did secure their sites.

What are some of the "clues" left behind (and during) a hack?

Jack: Depending on where they got in, your router logs might be able to see the IP address showing where the traffic originated. Depending on which OS they are getting into, the tracks could be in the System logs, or the sys partition.

What is Ping O' Death?

Jack: This attack causes a buffer to overflow on the target host by sending an echo request packet that is larger than the maximum IP packet size of 65535 bytes. As the target machine reconstructs the packets, the final packet is larger than the 65535 limit and causes the DoS attack. This was an old style tactic from a few years ago. Most OS's have been patched to withstand this attack. Get more information here: http://www.insecure.org/sploits/ping-o-death.html

What are the legal implications with hacking your company's systems to prove they are vulnerable and raise security on the to-do list?

Jack: I have never hacked my company's site unless I got prior written approval. This included legal counsel from the company. Some of the qualifications that I would ask for include: exposure of confidential information would not lead to suspension or termination (such as passwords, e-mail and instant messages) and complete shutdown of a production server due to an attack could not lead to suspension or termination.

Admins receive phone calls often and are asked questions concerning the physical network, etc. of their worksites. What questions should you never answer and why?

Jack: Answer as vaguely as possible. Never answer, "Who is in charge?" or "Where are you located?" Those answers just lead to narrowing down attacks. I am always paranoid about people that ask me about my network, I just answer, "It is working."

What is a teardrop attack?

Jack: A teardrop attack is one in which the fragmentation of the packets is overlapping. This causes the targeted, mostly Linux, machine to incorrectly attempt to re-assemble the packets and crash. The target machine looks at the offset of the packets and re-assembles them according to the offset, but packet B's offset states that it starts inside of A:

> 13:23:13 hostile.com.32157 > friendly.com.53: udp 28 (frag 242:36@0+)
> 13:23:13 hostile.com > friendly.com: (frag 242:4@24)

Should I really interpret port scans as a prelude to attack?

Jack: Not necessarily an attack, but definite door rattling. Once they start to pick the lock, consider it an attack. What I mean by this is once you notice that the scans burst at you for a few days in a row and then you see intermittent attempts, be ready for the attack.

Are there any "Robin Hoods" in the hackers or crackers community?

Jack: It depends on your definition of a "Robin Hood." Some of the things I did before now could be considered a Robin Hood act. I helped the poor sys admins who did not quite understand security and prodded them into action.

Information Sites

What are your favorite sources of online information?

Jack: Bugtraq, Max Vision's Whitehats.com, SANS and GIAC. Astalavista.com also has some very good links to the underground.

Are there any publications (online or otherwise) that list NT Server 4 security loopholes and fixes that you would recommend?

Jack: Bugtraq archives and Windows IT Security (formerly NTSecurity.net). More monetary damage comes from inside, and most systems internally are NT/Windows.

Do you recommend any sites on the Web?

Jack: www.whitehats.com, Windows IT Security (formerly NTSecurity.net), www.securityfocus.com and packetstormsecurity.org are good starting sites.

What books or learning materials do you consider viable to learning about taking advantage of certain weaknesses found in systems? Or are any worth investing in?

Jack: Since I have been in the security field, I have had more respect for some people in particular. Stephen Northcutt is a good analyst. Bruce Schneier is a leading expert. And of course the guys over at @Stake are great. *Hacking Exposed: Second Edition* is pretty good. And the older *Maximum Security* by Anonymous is good. But the best learning materials are your peers. The security field is really a small world. The more communication you have with one another, the better you stand a chance of turning away kiddies and resisting even skilled hack attempts. SANS has become a leader in gathering some very bright minds together for analysis, and the papers that they release are good learning materials as well.

What do you think of Foundstone's Hacking Class? Have you ever seen this before and what is your take?

Jack: I met the Foundstone people a few months back, even if they don't remember me, and they strike me as knowing what they are doing. I would be interested in actually attending one of their Extreme Hacking classes if only to see what they do know. Their research is headed up by JD Glaser. He is very talented, as evidenced by his previous tools under NTObjectives.

Jack, what is the best book on the market today that would be a study guide on how to be a hacker and at the same time teach you how to protect your servers from being hacked?

Jack: There is no definitive guide on how to hack. There ARE guides on how to protect your system, one of which is *Hacking Exposed: 2nd Edition* by the guys from Foundstone. However, it's also best to subscribe to lists such as SANS, CERT and other vulnerability resources. By the time it's in a book, you're already extremely far behind.

Jack, I had questions about training – how to convince a small- to mid-sized company that their network admins need security training even though they do not have as large a Web presence as companies like Microsoft.

Jack: One mid-size ($50M+) company I recently worked with refused to upgrade or even consider security options. What they can't grasp is that the information they keep under lock and key (their sales contact list) could be extracted by simple social engineering, and their company could be severely damaged financially by a competitor receiving that contact list. According to recent studies, more than 3 percent of unplanned outages are related to security breaches and issues. So for no other reason, you'd do this to improve availability. How much is your intellectual property actually worth?

With the exception of reading the numerous e-mails and information I receive from SANS, CERT, etc., how can I keep abreast of all the new information?

Jack: Limiting yourself to a couple specific sources helps. If you've overflowed yourself with information, you probably need to cut back and remove whichever source is your "weakest link."

You mentioned above that when it's in a book, you're far behind. But what about UNIX OS and some computer languages, among other things? They're still the basics, aren't they? I mean with that knowledge, you can become a hacker?

Jack: That is definitely a place to start. Most individuals I know started in UNIX and learned to program from there. What we mentioned above is more along the lines that by the time the book is checked for errors and edited, the exploits have been in the wild for too long. You're playing catch-up by then.

Are you familiar with Steve Gibson's shields up site? If so, how effective an indicator of one's security is it?

Jack: I am familiar with this site. This is a good site for the normal consumer to have a look at when they have an "always-on" connection to the Internet.

What are the best sources of information for securing an NT/2000 network, particularly IIS?

Jack: I have read parts of the *Mastering Windows 2000 Server* by Mark Minasi and found it to be quite good. *Hacking Exposed: Second Edition* has some very good points on what to secure within your environment. Checking out SecurityFocus.com always helps as well. The Microsoft team put together a very nice checklist for IIS. at http://www.microsoft.com/technet/security/iis5chk.asp.

What are the best avenues one should follow to find the best bang for the buck, if you will, in security training? I am familiar with self-learning. But there are so many exploits out there that learning them all on your own without proper guidance is difficult.

Jack: I took a track from the SANS team a while back, and I really enjoyed my time there. There is a lot of good information from the courses. The least -expensive security training is getting on message boards and asking a lot of questions. There are thousands of people out there that want to pass on their knowledge on security. Some of the self-learning that you can do is put up a honey pot and watch it get taken over. Make sure that you are able to see what happens on it before you deploy it, and learn from those actions.

What would be a good book to read that shows an administrator more understanding of how to secure Linux?

Jack: Try the *Real World Linux Security : Intrusion Prevention, Detection and Recovery* by Bob Toxen.

How does one subscribe to CERT and the other good subscription lists to stay up to date on security?

Jack: SecurityFocus has instructions on its site (SecurityFocus.com) as to how to subscribe to their multiple mailing lists. CERT is the same way. Check out the sites from which you want to receive mail, and they should have instructions on how to subscribe.

What is a good "Security 101" book for the complete novice?

Jack: The *Hacking Exposed* books are pretty good. But to be honest, there are no "Security 101" books. Security is such an all-encompassing problem that no single book could tell you everything you need to know, even for the complete novice.

How do you feel about Lance Spitzners' white papers?

Jack: Lance's papers definitely hold a lot a value from which individuals can learn. The motives paper shows actual logs of what the script kiddies do once they have access. Lance and the Honeynet (Project) crew know their stuff.

Lack of security knowledge by admins: What are some tips you can give to lock down each of these OS's?

Jack: The quickest way would be to go to SecurityFocus and check out each section of their site (SecurityFocus.com). The Microsoft section has checklists on securing IIS, NT 4.0, 2000. The Linux section has the same layout and information.

Do you have any suggestions for security training?

Jack: Try the GIAC courses offered by SANS, as well as looking into the studies for CISSP certification.

Tools

Are DoS and DDoS attacks going to (continue to) be a threat?

Jack: These attacks are definitely going to be a threat. DoS attacks are easy enough to initiate upon a vulnerable system, but almost every system is vulnerable to DDoS attacks. It is the same adage that shows if they have a larger pipeline to use than you do, the DDoS will more than likely work. However, if you are able to subscribe to some online tracking listservs, such as Bugtraq, you should be able to keep up with some of the openings and how other security individuals are trying to combat them. The security field is like a large fraternity or sorority, everyone knows the same names, and everyone looks for help when a disaster strikes.

Are any tools available that don't require two full-time people to monitor the alerts and track them down?

Jack: This is dependent on both the size of your environment, as well as your initial assessment on what is going to be monitored. Most organizations should have at least two individuals on staff that track and/or monitor the alerts that come in. Should they be full time? Not necessarily. Most current tools may be distributed among numerous monitoring stations. At least one individual should look at these alerts almost full time. The reason it should not be full time is the human element. If one were to look at the same logs for 8 hours a day, 5 days a week, it becomes "noise" to them. That is where the backup comes into play. When the saturated person becomes overwhelmed, the backup person should be able to take a fresh look at the information. Even when talking to other Intrusion Detection analysts, they will tell you the same thing. That is why a community of these analysts help you through your detects.

Are there any tools/utilities that you would say are essential?

Jack: There are multiple tools that are essential in order to have a well-rounded security solution. First would be log consolidation tools. One of the key sources for forensic analysis are the logs. If they are not secured, any information gleaned is suspect at best. Next is an IDS tool. VA tools and automated response actions are also required. A firewall is very essential.

How do you see integration between auditing activity (audit logs consolidation), monitoring activity (Host network-based IDS) and vulnerability assessment activity (host-network)?

Jack: This would be considered the complete package as far as security. Security cannot be looked upon as a one-size-fits-all type of solution. You cannot rely only on your firewalls, your network-based intrusion

systems and your auditing capabilities separately. Security has to encompass all viable points of entry, and even some you don't see. These are the reasons why you need to look into implementing a security policy using those host- and network-based scanning tools before an attacker or internal employee does attacks your system. You must be able to look through logs from your firewalls, your border and internal routers and your network-based intrusion tools and host-based tools. Lastly, you would have to look through your host audit logs, whether they be *NIX of Windows.

Have you seen any conversations regarding the value (or lack) of biometrics solutions?

Jack: Biometrics was a necessary security tool on one of my previous contracts, but that lays within the physical security aspect of things. The controller for the biometrics is the target at that point. Again, it depends on what you are trying to secure – physical access to your most critical servers or your users' access to the network.

How important is it to stay on top of vulnerability fixes on my publicly accessible servers?

Jack: IT is VERY IMPORTANT to keep up to date with these fixes. Countless examples are Attrition.org that show how admins who don't keep up with patches ride into the sunset in infamy.

What is the most exciting security technology that you see today?

Jack: I am interested in seeing if the Rabin crypto stands up to the analysis of Mr. Schneier and others in the crypto field. Another lets you implement a single point of log consolidation from numerous points – audit logs, firewall logs, IDS logs and host-based logs. Now, if you can come up with something like that, the development would be exciting because it takes many of the unseen problems and makes them visible.

What is your opinion on the effectiveness of IDS?

Jack: Network or host-based? Network has problems when used in switched networks. Network IDS is possible, but much harder to implement. Host-based, when used alone, is only one facet of the overall security of your environment. IDS alone will not save you. But an overall security scheme of, say, restricted border router, firewall A, load balancer, NIDS sensor in DMZ, firewall B, internal switched network, internal NIDS sensors and then host-based IDS is great. If you can make that work in your environment, you would be about 90-percent complete. Vulnerability testing and adherence to security policy will make up most of the rest.

Should hackers who release proggies like VBS Worm Generator be held responsible, like the person who goes and gets the proggie and releases the worm to the Net?

Jack: IMHO yes.

We've been looking into some intrusion detection tools, but most don't seem to be worth the time or money. Have you had any success with these types of tools?

Jack: Traditional IDS is like reading in the newspaper that you've died in a car accident the day after it happened. You want to establish a security solution that takes data from IDS tools, but can then be adaptive and automatically respond. Remember that exposure time equals detection time plus reaction time. If your IDS does not provide immediately reaction time, then you are still behind the hacker.

What do you think of the latest program from Rain Forest Puppy that renders IDS essentially useless?

Jack: I am trying to find the program you are talking about, but the one that does come to mind is from K2 called ADMutate. That API is dangerous. We knew that this would come along someday, and that is why most IDS systems fail – the system is based on recognizing signatures, not out of band processes. RFP released RFProxy, which is something that we are currently evaluating.

What about SAINT?

Jack: SAINT is a good tool that has been around for a while. It definitely does a good job.

Would a Web server running VMS on an Alpha be less vulnerable to hacking?

Jack: I don't know since I have never come across that combination. That would almost lead into the "defense-by-obscurity" realm.

How do you perceive the use of polymorphic code such as ADMutate? Good or evil?

Jack: Both. Good, so that one can try and duplicate the morphing of a new exploit before it happens, and bad because of the intentions behind it.

Do you recommend a Unix-based OS for an intrusion detection box? Or is NT/2000 sufficient?

Jack: NT is sufficient, but anything straight out of the box is not secure. Look at the skill set of your team: Do you have more *NIX people than NT? Vice versa? Go with what works for your team. *NIX can be highly tuned, and so can NT.

What are your thoughts on the newest wireless network problems?

Jack: This was bound to happen sooner or later. More people want the really interesting equipment in their offices. The problems with WEP are basic implementation, which in turn, shows the problems with the algorithms used for WEP. As is documented at http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html, current implementations use a single key that is shared between all mobile stations and access points. Sharing a single key, along with the low strength of the initialization vector, makes cracking an encrypted transmission possible. I believe that more vendors will be looking to strengthen this technology.

What happened with PitBull in Europe?

Jack: What happened is that they went up against a true set of hackers, ones that know an OS and don't use blatant DoS attacks. The fact that the hack was known in the underground for some time also shows that securing the OS is one of the most important steps in securing your infrastructure. What LSD did was hack Solaris for x86, but the PitBull software was not hacked. But who cares? They won because they knew what they were doing. Period. End of story.

**NIX*

In your opinion, is an open source OS, such as Linux, as secure as a proprietary flavor of Unix (for instance, AIX or Solaris)?

Jack: No version is secure out of the box. Read the reports that show that old patches that were not implemented on an OpenBSD box were exploited by a hacker, or put any *NIX flavor in the place of OpenBSD. Most Proprietary *NIX flavors improve performance, not necessarily security.

How secure is Linux?

Jack: I think that a Linux box is as secure as you make it. Every default install is not good, whether it be NT or Linux. The open source community does a very good job of keeping everyone informed of new patches and holes that are found.

What would you consider the easiest targets for attack – NT/2K or Linux?

Jack: Linux by far. The majority of the people administrating Linux systems have almost no clue of how to secure or even MINIMIZE risk. Second would be NT4, and then 2000. All three are considered easy to implement OS's, but fall victim to bad practices. Again, I can't stress how important good implementation is.

NT / 2000

Jack, do you have some tips on securing NT?

Jack: SANS top 10 list for securing NT is a good starting ground. I saw a script yesterday that looked really good as well, but I don't have the reference right now. There is one thing that I would like to say on that issue though – what do want that server or workstation to do? That is what determines the level to which you harden a box.

For you, Win2K is more secure than NT? How much?

Jack: I think over the past year, with security measures that were put into 2000 show, that a true 2000 implementation is a pretty sound solution. There is that backwards compatibility issue with NT, but I think that Microsoft has done a good job with 2000. You can't put an index on the amount security has improved in 2000, but Microsoft learned some lessons from 4.0 and tried to improve them in 2000.

Is NTLMv2 much more secure than NTLM? What is the difference between the two?

Jack: While initially it was believed that NTLM v2 was more secure, conversations with Microsoft by an individual who recently submitted his findings to NTBugtraq may suggest otherwise.

What is the best way to secure a Win2K Server?

Jack: There are checklists that the Win2K team has put together. If I had the URL handy I would post it - this is one of those subjects that could spawn a chat in and of itself.

What is the best way to lock down a Win2000 Domain?

Jack: Remove your network cable. There is no "one thing" that I can cover in the context of this chat. I highly recommend getting a Windows 2000 book, such as Mark Minasi's *Mastering Windows 2000 Server* book. Microsoft press also has several books that cover this.

You are stating that Windows NT is easier to hack than 2000? Why?

Jack: NT has been around longer and more people know about the vulnerabilities in the system. Windows 2000 has not been around long enough to have a massive explosion of vulnerabilities, even though it has its fair share of them. If you have a completely 2000 infrastructure, getting into that system is harder than using old tried and true tricks for an NT system. The usage of AD and Kerberos help quite a bit.

What are your thoughts about securing Windows 2000 Active Directory?

Jack: If you are asking me on ways to secure Active Directory, I know some ways to help it out. First thing, make sure that only one or two individuals get the Enterprise Administrator's role, and no one gets Schema Admin. Second, think about how you are going to setup the AD well ahead of implementation. Understand Active Directory as well as you can.

If Linux machines are easier to hack, why are so many NT servers broken into?

Jack: Most of the Linux machines that are used in the consumer area do not get security updates as frequently as Windows machines. Businesses that use Linux must stay on top of package updates, especially security-related updates, and they can't always do so. That is why it may be easier to hack than an NT machine. However, most businesses run NT servers.

How secure is terminal server in a Win2K native domain?

Jack_the_Hacker : It is pretty good. We are still doing some research on this topic as it has become more prevalent for us to deal with. If you do a search on Securityfocus.com, you will notice that there are not a lot of issues with Terminal Server for Win2K.

What is your opinion on Windows 2000, specifically IPsec, Kerberos and NAT?

Jack: Always have liked IPsec, and I especially like how Win2K has implemented it. The Kerberos is definitely a step above using NTLM hashes, and NAT has been around and is quite common.

What do you see as being some of the biggest problems with Windows 2000?

Jack: The three I's - Implementation, Implementation and Implementation. In the OS itself, the worst problem now is reverse-compatibility with insecure network protocols. For example, NT4 SMB.

Misc.

We all know that network security is a vital role in all major organizations. Why then is the world waking up so late to it and why is the IT industry not creating hype to promote a "security-conscious" world?

Jack: There is no real need for the IT industry to hype security than it has to this point. Companies that do not understand what security is do not invest their resources into anything more than performance over security. These companies will not understand their risks until they have a wake-up call from (hopefully) an internal source rather than an external attack. The IT industry hyped e-commerce during its explosion because getting hard-working individuals to submit their credit card information to a Web page, rather than a person who they would see slide it through a reader, was difficult. They wanted to show peace of mind with security for B2C and P2P businesses. As that boom has started a small downturn, more individuals have started to take that information and try to translate it to security within the workplace. Most individuals have misconceptions of hackers, crackers, phreakers and script kiddies or their stereotypical ideas of based on media persona. The FBI will tell you that crackers do not fall into a stereotypical person. The attack could be from a 12-year-old girl to a 53-year-old system admin.

What is your opinion on full disclosure of vulnerabilities?

Jack: This is a question that is loaded and ready to go off. For me, I like to let the system vendor know what I found, give them a few days, then let Bugtraq know. I believe in full disclosure for certain problems. Others, I leave with the vendor. If it is a large hole like the BIND bug, full disclosure was good and bad. Disclosure of a small vulnerability in Netscape's browser that allows them to take over a non-secure session, I leave with Netscape.

How long have you been doing security?

Jack: Security on the good side, five years. On the other side, around seven years.

Aren't you concerned that speaking in an open event like this could also bolster any crackers looking to get resources for tools and information?

Jack: I opened myself up for this event. More than likely, some outside entities will look for the information for which IT managers are looking. I wouldn't say being scared, I say wanting to inform outside individuals.

What is your programming language background and platforms?

Jack: Some old-school Assembly, C & C++, some VBScript and Perl. My main platforms are OpenBSD, Windows and Solaris.

How do you feel about security certification? (CISSP, SANS certs, etc)

Jack: I like the CISSP certification because of the broad range it covers. The GIAC cert is pretty good because of the level of testing that they use. Certifications in previous products and years were considered "paper certs" because you didn't need a lot of real world experience. I think that SANS and ISC² figured that out and wanted their certifications to mean something. I would much rather trust a CISSP with designing and implementing a security policy for my company than a strict auditor.

What is your background? Did you start in networking and work into security, or was your start in programming? Which do you see as being more beneficial?

Jack: I first started out as a bona-fide user. My first real start was in networking and some BASIC programming at the same time. I stuck with the networking aspect and kept up with the programming side. With security, you can't have one without the other. If you do, you are just an admin resetting passwords.

Haven't the recent prosecution of hackers discouraged would be hackers?

Jack: I don't think they have been discouraged. They seem to be more determined in certain cases. Hackweiser is on a rampage right now. And until he/she is prosecuted, the defacements will continue. Back a few years ago, you had a few good crews put together. Nowadays, you have a lot of average to good crews who are looking for props from their peers and then they want recognition from the security field as well. After the first few successive hacks, it is a power game. And everyone thinks they are invincible.

Is it easy to crack a computer running Gnutella, Napster and other similar file-sharing apps?

Jack: I have not delved into the realm as of yet. I cannot give you an educated answer to this question. I can do some more research to let you know in the future.

Do you see a career model from the underground into the enterprise employment or consulting as current options that would create more interest in hostile security "cracking?"

Jack: It is evident in some of the defacements out there, but those are kiddies that want to break into the security field and get paid for what they know about their scripts.

What reformed Jack?

Jack: Realizing that there was more to life than having to watch my back for badges every day. Plus, when I had FBI agents show up at door one morning for something completely different. Those badges look scary.

What would be the best method to discourage would be hackers from starting in the first place?

Jack: I don't know. The media glorifies the attention these hackers like.

Who/what influenced you to change sides AND how did you sell yourself as trustworthy/employable, given extents of background checks, etc.?

Jack: There was this one network admin that I met at one of my first real jobs that showed me the ropes on how to work in the real world. I don't remember his name, but I figured that I didn't have to stare at a CRT in my room the rest of my life. Actually, some of the companies did not do background checks on me. And I don't have a rap sheet. I was forthcoming with them when asked about my experience with the "other side." But those actions were done when I was young and naïve. Now, I am just young.

What keys should one look for in a log to spot an intrusion?

Jack: When your audit logs are gone. It depends on the method. Slow-and-low is hard to see. A straight hack-attack is pretty blatant. Take a look at the Honeynet Project's logs, as well as some of the papers from SANS.

In your opinion what needs to be done to prevent people from hacking (i.e. tougher laws, better prosecution, etc.)?

Jack: All of the above. The old adage that the world is a small place rings even more true with the Internet. You can't tell if the hack was from your neighbor across the street or in some other foreign country. I think more crackdowns are going to happen across the globe, and that might stop a few of the hacks. But this will never stop. Tougher extradition laws would be a start, but I am not going into law here.

What do you get out of hacking?

Jack: Different people get different things from hacking. Those driven by money often find a very lucrative source of income (ask those stung by the FBI). Others do it for the game, sort of like rich kleptomaniacs. They don't need to steal but enjoy the rush. Some try to believe the "noble ends justifies barbaric means," so they are doing sys admins a favor. I tend to lean toward the thrill of the game – can I do it?

What is your definition of a hacker and how do you know when he/she has been reformed?

Jack: Hackers work on the foundational premise of freedom of information. Crackers work on the foundational premise of infliction of harm. Determining whether or not someone is reformed is very difficult. Who's to say an alcoholic doesn't sneak a drink now and then?

How can one be reformed? Do you ever get the itch?

Jack: Check out the efforts of the 2600 crew. The itch is always there for curiosity, but I no longer get the urge to crack systems without proper approval (or funding).

What happened with the Microsoft Premier Support hiccup?

Jack: This is a prime example of what everyone in the security field should know: A computer is administered by a human and configured by a human - it's bound to go wrong somehow. The processes were not completely followed and a mis-configuration occurred, opening up a hole. This is the No. 1 problem with all infrastructures – the technology is good, but the implementation may not be right.

Has the perceived economic slowdown affected the security market? If so, how?

Jack: In some ways, the slowdown has. Most of the high-tech marketplace is feeling the pinch of the slowdown. But so-called "old" money firms, such as the oil and gas industry, are booming. There are more laid-off employees who may have damaging information, and some know how to get back into their ex-employers systems. If there is a time for more security, now is that time.

What is the HIPAA initiative looking like?

Jack: With a 2003 deadline, more providers are finding out that this is larger than once thought. As evidenced last year when someone accessed a Washington State hospital's patient information, hacking the system wasn't too difficult. This is a very large undertaking, and those providers who have not yet started on the path to compliance are going to have a problem to finish before the deadline. The main problem is the ever-changing face of security. Several years ago, it was physical, then it turned to anti-viral, now it's PKI and intrusion-detection systems. Are those providers ready for it? Probably not.

Is network security compromised with the use of IM's?

Jack: This has not been widely studied, but initial studies indicate that yes, this is the case.

With all the talk of Chinese hackers these days, how susceptible is our nation's infrastructure to cyber-terrorism?

Jack: Various areas and companies are obviously going to be better-protected than others. A better source of information might be the NSA or other government agencies.

What do you consider the hardest OS to hack into?

Jack: IPSO - the OS that runs on the Nokia Firewall Appliances. OpenBSD is a close second. However, this doesn't take into consideration poor systems administration. Bad implementation will open big holes in your network regardless of how strong your NOS is.

How do you recommend that admins react to Web site penetration attempts? Offensively or defensively? Any specific offensive tools that you recommend?

Jack: I would recommend acting defensively. Reacting with an offensive state of mind is much easier when your territory is being invaded. Collect all of the data you can from the attack, seal it away and call your law enforcement officials. Make sure that they are able to do forensic analysis on the data, and have them prosecute the crew or individual. Taking matters into your own hands could be bad. What happens if the IP address that you are killing is actually another company that has been hacked? Do you want to add to that sysadmin's headache already?

What is your best advice for someone who has been fired from a network admin job for allegedly "hacking"? Do any good law firms support "the hacker"?

Jack: I can't answer that question very well because I have not gone to that extent with my activities. The Stanford Law School is attempting to defend the 2600 crew in the DeCSS trial.

How do VMS/OpenVMS rate in terms of 'hardness'?

Jack: I haven't used VMS in a while. But do a search on packetstormsecurity.org for VMS. See how many vulnerabilities exist.

How do you convince a company that security needs to be a prime concern and to take action?

Jack: Convincing the company's upper management that they need security is still difficult because they see the bottom line and ask why they are spending so much on security when they haven't had an attack. My response is, "You haven't had an attack that you can see because of your current architecture." I will then hand them their passwords, selected e-mails that they have sent out among one another, their current driver's license information and Social Security Number that was sniffed off a Web site. That usually gets their attention. This is the normal scare tactic that security analysts are left with. This is not the best way, just the easiest.

As a professional hacker, would you want, or think it beneficial, to be a dedicated security specialist or be a jack of all trades? (No pun intended)

Jack: To become a dedicated security specialist, you have to be a jack-of-all-trades. Look at the CISSP requirements. Security does not have just one facet. It is quite multi-faceted.

Do you find that firms, in particular industries, are attacked more frequently than others? If so, which do you find are mainly targeted? (e.g. real estate, political, etc)

Jack: "Hacktivism" targets mostly government sites to spread literature on human rights that the cracker feels are being violated. From my experience, just about anyone is a target, not just the high-profile hacks.

Would you enter your own personal credit card number online with today's current security practices?

Jack: Yes, but only after I have done some research on them.

What are your thoughts on computer forensics, in terms of the job market?

Jack: I think that the demand is much greater than the supply of qualified forensic analysts. With as many hacks that occur on a daily basis, an analyst could have four months of data to sift through.

Do you think the whole e-commerce will eventually melt down? Anything can be hacked into eventually? Will businesses just stop doing business on the open 'Net?

Jack: In my opinion, the e-commerce world will not melt down. It has become too entrenched in today's marketplace that consumers and businesses cringe at the thought of no e-tailers and e-business.

How old were you when you started learning to Hack?

Jack: I started around the age of 15.

I understand that ICQ is one of the biggest security risk. Is this true?

Jack: I don't think that it is the biggest threat, but it certainly does open up holes that are not necessary. There are multiple ways to have a person open up a Trojan (horse) received through ICQ, and the overall security of ICQ is not that great.

What are some of the things that a small company should avoid doing, so they don't become "interesting" to the crackers?

Jack: Understand that everyone is a target, but for varying reasons. Hardening your Web servers will keep your site from being defaced. But make sure that your databases are more secure. Following that mantra will thwart most of the attacks that your site will come up against. Don't keep casual contact information on the Web site. That casual contact information makes figuring out your naming convention easier for me. As much as you would like your investors to see who is in charge of running the business, it makes my life easier.

What did you find to be the hardest obstacle to overcome?

Jack: Old school mentality. How can a person of my age be able to do the things that I say I can? Plus, human nature shows that if you don't understand something or someone, you tend to disregard them or try to keep away.

With the Feds starting to come down hard on hackers and crackers, do groups still recruit new memberships to train and compete against other groups? Or has the entire scene gone underground?

Jack: There has never been a large movement to go out and recruit people to create a crew to squash another crew. Crews get together because they want to. There are no fliers out there saying, "Come join us!" But there are lots of solicitations by people wanting to join a crew.

Is there a common mistake most people tend to make when it comes to securing from an outside vulnerability?

Jack: Believing that they have secured everything. The worst thing that you can do with security is become relaxed.

Is it me, or is Microsoft heavily under fire? Or shouldn't I trust Microsoft's platform as a secure environment?

Jack: The market leader is always going to be under fire because we trust them to produce the best products. I think that they have always tried to keep up with security issues, but the consumer wants everything. That consumer can be the home user or the corporate user - it doesn't matter. You want to be able to browse graphic sites and not have a problem with it. Remember when it was a text-only BBS? That was before we the consumer who wanted his/her e-mail to work directly with their word processor or spreadsheet program. That was before HTML pages knew what 1.0 looked like. I like Microsoft's platforms, but I don't personally trust any operating system out of the box.

Let's say a company you work for has NO security policy. Should you feel it is your responsibility to implement security measures of your own? Or should you insist that the directive comes from higher management?

Jack: I would like to be able to do this myself but the directive must come from upper management.

How do you think crackers today are responding to all the media around their activities?

Jack: Pumping up their already inflated egos

For more information on NetIQ's Security Management Solution, visit
www.netiq.com/solutions/security/