Hackers keep the heat on Windows NT security

By Larry Lange

BOSTON -- A group of sophisticated hackers has stepped up the assault on the security of Microsoft's Windows NT operating system. The group, called the L0pht (pronounced 'loft'), has posted on the Internet a hack--called LOphtcrack--they claim can be used to retrieve NT network-domain user names and passwords and display them in plaintext.

"If you have an NT network, and you have that network connected to the Internet, you're in deep trouble," said "Mudge," L0phtcrack's co-author and an encryption expert.

L0phtcrack follows in the wake of two separate NT hacks--PWDump and NTCrack--posted in the past two weeks by security experts in California.

Reports on *EE Times* Online about PWDump and NTCrack brought sharp responses from Microsoft on its Web site.

Microsoft officials contacted last week said they were not familiar enough with LOphtcrack to comment specifically about it.

The LOphtcrack hack is a graphical user interface (GUI)-executable that adds a spreadsheet-like interface atop PWDump. "It [LOphtcrack] sets up columns of the user lists, what their passwords are--such as the MD4s and the LANMANs [passwords that are fairly easy to crack]--and when you click 'Run,' it just starts screaming down [decrypting] all the passwords. And then you can save that file out to a disk or print it," said Mudge.

According to L0pht, L0phtcrack is the tip of an iceberg of software that's being generated by hackers poised to slam what the group calls Microsoft's complacency on the subject of NT security. The hackers who have taken on NT in recent weeks are members a worldwide network of code breakers who communicate over the Internet via electronic-security mailing lists, Usenet groups, FTPs and Web sites. In recent months, the community appears to have shifted its attention from Unix- and encryption-cracking techniques to take aim at Windows NT, which has begun to find favor among corporate users.

"We're doing this because Microsoft is shoving stuff down people's throats, and you don't have the ability to look and see how good it is," said Mudge. "They're saying, 'Trust us; it's secure.' "

For its part, Microsoft officials insist that if network administrators and users pay adequate attention to security issues, cracking encrypted passwords on any NT network remains inherently difficult. Microsoft also noted that most, if not all, operating systems have been subject to similar types of attack.

While these hacks--L0phtcrack, included--require that the user have network-administrator privileges to access a password-encryption file, hackers note that common workarounds already exist if you know where to find them.

Mudge said Microsoft has to change the way it undertakes product development. "They should post their specifications, so people can pick it apart before [the product] comes to market," he said. "Then when you do come to market, it'll be a great product, because 3,000 hackers and crypto experts will have ripped it apart and Microsoft will have had a chance to fix it all" before the final release.

But Mike Nash, Microsoft director of marketing for Windows NT Server, countered that NT was more than adequately tested. "NT has one of the

most extensive beta programs in the industry," he said. "Over 100,000 people beta tested 4.0, and I expect even more will beta test [the upcoming] 5.0." Even the U.S, Department of Defense subjected NT to rigorous testing, Nash said.

Coming a mere two weeks after the breakthrough program that began the acceleration of NT hacking, L0phtcrack is a direct result of that first program, PWDump, written by Jeremy Allison, a programmer at Cygnus Solutions (Sunnyvale, Calif.). PWDump is the heart of the L0phtcrack GUI program and is included in L0phtcrack's "tool kit." Also included is an additional "dictionary attack" program that uses a "brute force" method. That program goes far beyond the capabilities of the previously reported NTCrack dictionary program.

Password, please

The L0phtcrack program does require a user to be an NT administrator and to have an administrator's password in order to access the file that contains the encrypted passwords. But hackers maintain that by using several common methodologies, a person could access those "admin" privileges directly over the Internet, and then gain access to the file (or registry) of passwords via the GUI and its extensions.

According to Microsoft's Nash: "Unauthorized access to an administrator account can only happen in three major ways. One is that the administrator is a "bad guy"--a non-trusted person who has the administrator account and compromises the system with intent. Second, the administrator could inadvertently do something he didn't mean to do. And the third is where the administrator is in the account but is doing things beyond just administrating the system . . . [That is where] a Trojan horse gets involved in that system and compromises it."

Nash added that NT is not alone: "All three of these cases are possible on any operating system."

But far more serious problems may lie ahead for Microsoft, according to L0pht. The group has warned publicly that a second version of L0phtcrack, due to be available within a few weeks, promises even easier access to the NT-password file from remote locations, including over the Internet. Further, with the new version, a user would not need to be an administrator or have an administrator's password.

"They [L0pht] make a claim here," said Nash, "but the claim that you can basically get [admin privileges] without knowing the admin password is a pretty significant claim that's unsubstantiated."

"The next version [of L0phtcrack] is going to blow Microsoft out of the water," said Mudge. He said L0pht hopes to supply Microsoft with at least a week's "lead time" to react via a "fix" or a "patch." However, Mudge noted that only one day after the first L0phtcrack version was posted, he had received three messages from other hackers who were interested in getting the password registry without the admin.

"It's going to happen," he added. "We've got our program working within a test environment; it's just a matter of fleshing it out."

Philip Eskelin, a principal NT technologist for Fortune 100 companies at technology recruiting firm Pencom Inc. (New York), thinks the L0pht may be on to something. Eskelin has followed the advances of such hacker groups to uncover possible dangers to the NT networks he recommends for top corporate accounts. "Guys like those at the L0pht are feverish hackers who want to crack all these systems; that's where they get their high," said Eskelin. "And something like that is very good, because these guys get their high and make us all aware of all these issues.

"With the L0pht's next version of this, [they claim] you won't have to be admin; but even now [with the GUI program], if you're on the NT network on the client side as a user, such as a consultant, there's an icon on your Windows desktop that dials in to the network. You establish the

connection, and you simply put a floppy in to run the program and just have it happen.

"You just have to be part of the NT domain to get these passwords. Remote access is obviously an easy way to become a part of the network, rather than having to physically go to the site and plug yourself into the network via a machine."

Eskelin is less than impressed with Microsoft's reaction to the assault by hackers. "The immediate response that Microsoft gave was, 'Oh you need to be logged in as an administrator,' but that isn't the point," he said. "The point is that there are all kinds of alternative ways that you can actually [do] what needs to be done to get these passwords without having to be logged in as admin, such as the Trojan horse method or using Internet Explorer bugs."

Eskelin criticized Microsoft for "blowing off the [the earlier reports] the way they did," since "this is a very serious problem for the company."

He warned of the dangers of corporate espionage, noting: "It's not so much the hacker at home who will be using these kinds of programs for malicious intent; it's more of the corporations with multiple master domains across Europe and America, with thousands of machines, with all kinds of proprietary and confidential corporate data at stake. Look at what American Express has on its NT network--thousands and thousands of credit-card accounts. This could all be pretty nasty."

Microsoft's Nash said that using any of these techniques would be difficult if the NT admin has taken the proper steps to protect against them. "First, using PWDump requires the administrator password. And second, even if you are an administrator, you have to attack this with a dictionary attack--an attack that is very, very easy to avoid by using 'strong' [hard to guess] passwords. We also have a utility for NT to force 'strong' passwords; it's used inside at Microsoft for our 22,000

employees."

The L0pht's Mudge acknowledged that "the brute-force method in the program needs computing power" but, he added, "We ran it on a Pentium 133 [MHz], and it took three days, which is nothing. A [similar] Unix Crack program could take four or five days. If you're brute forcing, and if you have a list of users that you're trying to break that's 10 users long, it could take you three days with a 133, but if the list is 500 users long, it can take the same three days by adding more power.

"People have the time; after all, the computer does all the work. On a Pentium Pro 200 [MHz], we can do it in under a day. If it's a multiple-processor box, we can do it under a half a day."

The L0pht's Web-site NT advisory notes that "L0phtcrack will recover passwords from Windows NT registries by feeding in the output from PWDump and a dictionary file for both the LANMAN and MD4 plaintext passwords. L0phtcrack gives you the capability to brute force the entire keyspace and recover all user passwords up to 14 characters in length . . . by going through the entire keyspace available, this program will return all of the plain-text passwords up to and including 14 characters in length."

The advisory does note that the User Login Dialog box on NT machines limits the amount of characters that can be typed to 14, though technically NT allows for up to 128 characters.

Still, Mudge is confident that NT passwords can be cracked in most cases. "Microsoft's line has been that you need to use strong passwords--not use 'cat' or 'dog'--to prevent against dictionary attacks," he said. "But our response this time is that now you can't even choose passwords such as 's753@6yz'--up to and including 14 characters."

Many hackers claim that PWDump is actually a useful utility tool for administrators who want to migrate users from Unix to NT systems, for

example. But a big problem for NT is that users can access admin privileges fairly easily, right over the Internet, and then go back through an NT network and glean the password file list from the Security Accounts Manager (SAM).

Take a sniff

A program with the seemingly innocuous name "sniffer" is the most common methodology used by hackers for gaining access to admin privileges on Unix and, more recently, NT systems. Mudge explained that a sniffer is "like the old party-line telephone system, but unlike the nice neighbor who picks up the line, realizes that somebody is talking and puts it back down, [the sniffer] picks up the line and keeps listening."

Sniffer programs are readily available commercially and are primarily used for network analysis. "Net Xray is one," said Mudge. "TCP Watch and LANWatch from FTP Software are others, and there are free ones for Windows, such as Gobbler. Anybody can grab [that one] off the Net."

He explained that to glean an administrator's password, "you run the sniffer, and then you watch somebody logging in from one NT machine to another, or using a share, or using a printer or anything [else] over the network. Then you take the output from that and put it into our program. You then can say, 'Give me the LANMAN or MD4 passwords information,' and it will dictionary-attack against that."

Mudge agreed that a common "Trojan horse" form of attack, as reported by *EE Times* Online, would work as well. "Most of the Trojans are done in the form of DLLs in Windows. It says 'Hey, I've got an administrator here; great. What do I want from him, what do I want him to execute for me?' The admin ends up running a program without even realizing it. The Trojan [can also be written to] say, 'Hey, I've got administrator here. Guess what I'm going to do: I'm going to dump the password file and then mail it to myself.'"

Microsoft's Nash repeated that a Trojan horse is a problem for all operating systems and added that, "certainly, protecting against Trojan horses is an important part of the policy that administrators want to have for their systems." He noted that steps to protect against Trojan horses and other attacks are explained at the company's security Web site.

But Pencom's Eskelin warned that there might not be an easy answer for Microsoft. "To fix or patch NT 4.0 would be problematic for Microsoft, due to the way the architecture is set up. It would definitely be a big hit to them to actually have to go in and redo it. Even if Microsoft went in and put in some kind of weird hack, PWDump would still work. If you are logged in as admin and their hack said, 'You can't look at the password information in the registry'--well, [NT] can't do that, because being able to look at the security information is part of being an administrator."

Mudge and Eskelin also agree that the coming release of NT 5.0 may not prove to be the perfect solution that Microsoft hopes for. "With all the upgrades comes more functionality," said Eskelin, "but also more shortcomings and bugs for hackers to get at. Whether it is NT 5.0 or NT 20.0, it's still going to be the same juggling contest. It's not going away."

And patches, he said, are not the answer for the long haul. "It would be like patching holes in a dam--like the guy who puts his finger in one hole, but then another one pops open."

Eskelin believes Microsoft should begin a process of collaboration with the hackers. "It is important for Microsoft to start working with the hackers rather than against them, since those are really the people who are testing [NT] to make sure that it's a secure operating system."

But Nash said that the ongoing dialogue on Microsoft's security Web site has been quite helpful for the company's NT customers."Security is a technical issue, but it's also a policy issue," he said. "Therefore, it's Microsoft's job to make sure that everyone's aware of the steps necessary

to ensure a secure site." Provided certain steps are taken by the network administrators, he said, NT is as secure as any operating system available.

What are those steps? Said Nash: "Secure your administrator password, make sure you don't use your administrator account for anything other than administrative work, and make sure that a policy of strong passwords is implemented in your corporate site."

Eskelin acknowledged that Microsoft is correct in observing that NT is far from the only hacking target. "I wouldn't say just blow off NT because of these type of things; there are lots of different holes in Unix too." The lesson to be learned from the recent rash of hacks, he said, is that all "companies need to be aware of ways to mold their security policies in order to protect themselves."

Go To Previous Story
Go To Next Story
Back to *This Week's News*