**Hacking NT – A Wee Story – David Litchfield, 2nd February 1998**

**Johnny Hacker has a Windows NT Server at home. Why? Because he knows if he's going to hack NT he's best using the same type of computer...it gives him all the necessary tools. He has installed RAS and has a dial-up connection to the Internet. One morn ing, around 2:00am he dials into the Internet...his IP address is dynamically assigned to him. He opens up a Command Prompt window and gets down to work. He knows www.company.com's web server is running IIS. How? Because he once did a search on "batch fil es as CGI" using Excites search engine. That phrase is in Chapter 8 of Internet Information Server's on-line help....and unfortunately it's been indexed by Excite's spider...now Johnny has a list of around 600 web servers running IIS.**

**He ftps to www.company.com. He isn't even sure yet if the server is running the ftp service. He knows if he gets a connection refused message it wont be...he's in luck though...the following appears on the screen :**

**C:\ftp www.company.com**

**Connected to www.company.com.**

**220 saturn Microsoft FTP Service (Version 3.0).**

**User (www.comapny.com:(none)):**

**This connection message tells him something extremely important : The NetBIOS name of the server : SATURN. From this he can deduce the name of the anonymous internet account that is used by NT to allow people to anonymously u se the WWW, FTP and Gopher services on the machine. If the default account hasn't been changed, and he knows that it is very rare if it has been changed, the anonymous internet account will be called IUSR_SATURN. This information will be needed later if h e's to gain Administrator access to the machine. He enters "anonymous" as the user and the following appears :**

**331 Anonymous access allowed, send identity (e-mail name) as password.**

**Password:**

**Johnny often tries the "guest" account before using "anonymous" as the user. A fresh install of NT has the "guest" account disabled but some admins enable this account....and the funny thing is they usually put a weak password on it such as 'guest' or no password at all. If he manages to gain access to the ftp service with this account he has a valid NT user account....everything that the "guest" account has access to...so does Johnny, and sometimes that can be almost everything. He knows he can acces s their site now...but there is still a**

**long way to go yet....even at this point he still might not get access. At this point he doesn't even supply a password...he just presses enter and gets a message stating that the Anonymous user is logged in. First off he types "cd /c" because some admins will make the the root of the drive a virtual ftp directory and leave the default alias name : "/c". Next he sees whether he can actually "put" any files onto the site ie. is the write permission enabled for this f tp site. He's in luck. Next he types "dir" to see what he has access to. He chuckles to himself when he sees a directory called "CGI-BIN". Obviously the Webmaster of the NT machine has put this here with the rest of the WWW site so he can remotely make ch anges to it. Johnny knows that the CGI-BIN has the "Execute" permission so if he can manage to put any program in here he can run it from his web browser. He hopes that the Webmaster hasn't, using NTFS file-level security, cut off write access to the anon ymous internet account to this directory...even though he knows there are sometimes ways round this. He changes to the CGI-BIN directory and then changes the type to I by using the command "binary". Then he types "put cmd.exe". He's in luck..he gets the f ollowing response :**

**200 PORT command successful.**

**150 Opening BINARY mode data connection for CMD.EXE.**

**226 Transfer complete.**

**208144 bytes sent in 0.06 seconds (3469.07 Kbytes/sec)**

**Next he puts getadmin.exe and gasys.dll into the same directory. With these three files in place he doesn't even gracefully "close" the ftp session; he just closes the Command Prompt window. With a smile on his face he leans back and lights a smoke, savouring the moment...he knows he has them.... After crunching the cigarette out in an overflowing ashtray he connects to AOL. He does this because if logging is enabled on the NT machine the IP addres s of AOL's proxy server will be left and not his own...not that it really matters because soon he'll edit the logfile and wipe all traces of his presence. Opening up the web browser he enters the following URL :**

**http://www.company.com/cgi-bin/getadmin.exe?IUSR_SATURN**

**After about a fifteen second wait the following appears on his web browser:**

# CGI Error

**The specified CGI application misbehaved by not returning a complete set of HTTP headers. The headers it did return are:**

**Congratulations , now account IUSR_SATURN have administrator rights!**

**He has just made the anonymous internet account a local administrator and consequently using this account he can do pretty much what he wants to. Firstly though, he has to create an account for himself that he can use to connect to the NT server using NT Explorer and most of the Administrative tools. He can't use the IUSR_SATURN account because he doesn't know the randomly generated password. To create an account he enters the following URL:**

**http://www.company.com/cgi-bin/cmd.exe?/c%20c:\winnt\system32\net.exe%20user%20cnn%20news%20/add**

**He has just created an account called "cnn" with the password "news". To make the account a local administrator he enters the following URL:**

**http://www.company.com/cgi-bin/getadmin.exe?cnn**

**It has taken him less than ten minutes to do all of this. He disconnects from AOL and clicks on start, goes upto find and does a search for the computer www.company.com. After about a minute the computer is found :**

**Next he right clicks on the "computer" and then clicks on Explore. NT Explorer opens and after a little wait Johnny is prompted for a user-name and password. He enters "cnn" and "news". Moments later he is connected. Admin rights for the computer www. company.com are appended to his own security access token...now he can do anything. Using User Manager for Domains he can retrieve all the account information; he can connect to the Internet Service Manager; he can view Server Manager...first though, usin g NT Explorer he maps a drive to the hidden system share C$. He changes to the Winnt\system32\logfiles directory and opens up the logfile for that day. He deletes all of the log entries pertaining to his "visit" and saves it. If he gets any message about sharing violations all he has to do is change the date on the computer with the following URL:**

**http://www.company.com/cgi-bin/cmd.exe?/c%20date%2002/02/98**

**Next, using the Registry Editor he connects to the registry on the remote computer. Then using L0phtcrack he dumps the SAM (the Security Accounts Manager - holds account info) on the NT server and begins cracking all the passwords on the machine. Using the Task Manager he sets the priority to Low because L0phtcrack is fairly processor intensive (NB L0phtcrack ver 2.0 sets the priority to Low anyway) and there is still a few thing he must do to hide the fact that that some-one has gained entry. He deletes cmd.exe,**

**getadmin.exe and gasys.dll from the cgi-bin, then he checks the security event log for the remote NT server using Event Viewer to see if he's left any traces there. Finally using User Manager for Domains he removes admin rights from the IUSR_SATURN account and deletes the cnn account he created a few moments earlier. He doesn't need this account anymore....L0phtcrack will be able to brute force all the accounts. Next time he connects to this machine it will be using the Administrator account. He breaks his connection to the Internet and sets 10phtcrack's priority to High, leaves it running and heads to bed...Looking at his alarm clock : it's just passed 2:30am....Sighing to himself, he mumbles, "Sheesh, I'm getting slow!" and falls asleep with a grin on his face.**