dem0nseed of The DMF Crew, presents:

I'm just going to throw this white paper out here, because I want to know if this application has a future, who all wants it, wants to help test it, and whatever else. This application will be freeware, I've been in the game for a while, but I'm not going to sell out like l0pht did ☺

If you would like to test the current capabilities of crax0r or would like to set up a test system for me, contact me. My contact information can be found at the end of the document

- dem0nseeed
The DMF Crew (est. 1996)

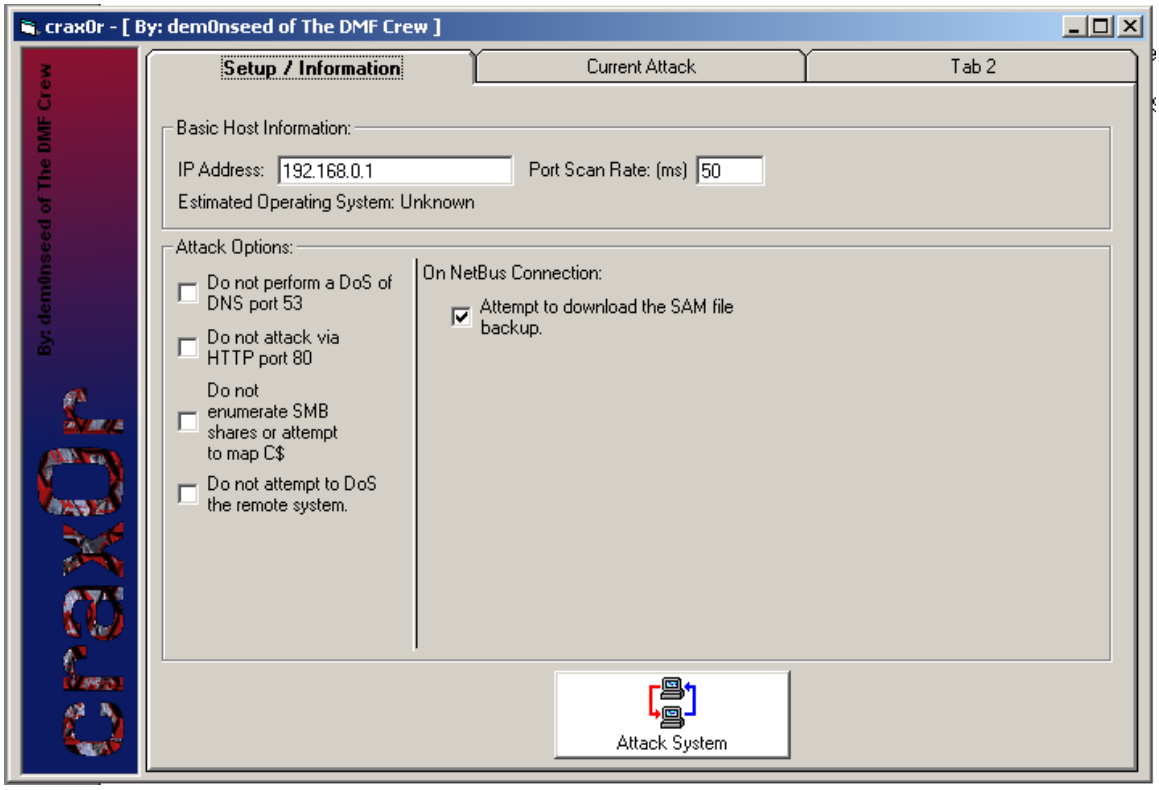
What is Crax0r?

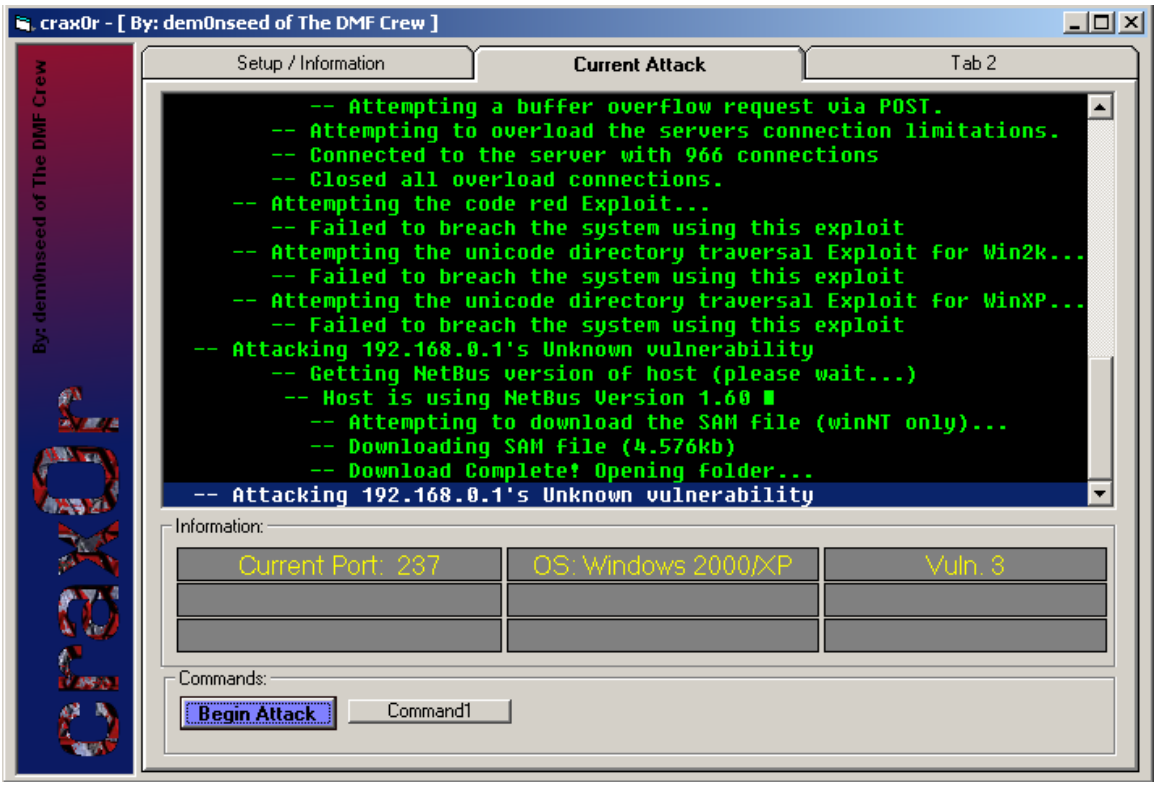
Crax0r is a security tool used to exploit numerous known computer vulnerabilities, allowing you to gain access of the system. Crax0r works in a way that conventional hacker applications do not. Below is the process that crax0r goes through every time an attack is specified.

1. Port Scan the system:
    - During this time, crax0r scans the ports on the remote systems machine looking for exploitations and vulnerabilities.
2. Build A Plan of Attack:
    - Based on your choice of optimization, whether it be for speed or just merely to get in, crax0r will create a "plan of attack", an order in which it will follow to attempt exploitation of the system
3. Attack
    - Crax0r will attempt to break into the system through any means possible, if the system could not be exploited, crax0r will then try to DoS the machine and knock it offline, as a sort of revenge. Crax0r looks for the following exploits:
        i. FTP – Crax0r will go through a dictionary word list of usernames and common passwords in attempt to gain ftp access.

ii. Telnet – Crax0r will go through a dictionary word list of usernames and common passwords to attempt to gain telnet access, once inside, if the system is UNIX, crax0r will attempt to 'su root'.
iii. HTTP – Crax0r will attempt numerous tactics to compromise the system, including
    1. Malformed URL requests (DoS)
    2. Code red requests
    3. Unicode Directory Traversal
    4. Standard Directory Traversal
    5. Nimda requests
    6. Server load DoS, attempts up to 3,000 'GET /' requests to a webserver. This DoS was discovered by me, and currently affects ALL Linux/UNIX systems running Apache webserver. My Linux box running RedHat 8.2 was knocked offline for two hours and eventually core-dumped due to this. It may also affect non-IIS webservers as well. Eventually, the system will overload and for some reason begins to connect to itself issuing, and sending requests, creating a network loop.
    7. DNS DoS – Crax0r attempts to buffer-overflow systems running DNS servers.
    8. SAMBA (SMB) – Crax0r automatically enumerates the shares and usernames of a remote system using ENUM.EXE. Crax0r also attempts to download the SAM file through samba.
    9. NetBus – Crax0r connects to the NetBus host, gets the remote system information (including username) and attempts to download the backup of the Windows NT SAM file (SAM file contains ALL usernames and system passwords).

This is an early screenshot, of pre-1.0 crax0r (before compile):





My Windows box is running a port forwarder that forwards connections to my Linux box, so, by the end of this document, the Linux boxes hard drive had been swapping for already 15 minutes, I was booted from telnet and while trying to visit the hosted web pages, I was unable to due to server load limitations and the box dying.

Contact Information:

AIM: OzzPIMP
Yahoo: Korncalendar2001
E-Mail / MSN: OzzPIMP@hotmail.com
IRC: irc.prison.net – nick: dem0nseed – channels: #og, #cellular
PLA Voice Bridge: between 9pm and 2:30am Monday-Sunday I may be on the voice bridge, between those times, go www.phonelosers.org and get the number from the site, you will see it in big letters during those times.

Our website is www.TheDMFCrew.tk, we are undergoing server issues currently, so keep checking there, the site should be up again shortly.

Contact me if you want to know more, would like to get a copy of my book, other software, to beta-test crax0r, or whatever else… or even if your bored. If you don't see me on AIM, I have buddy list only turned on, so e-mail me and ill add you to the list…

Thanks,
Dem0nseed