

how do hackers do it?

1. gather info on the target host

whois

Organization: Fiji ABCDEFG Inc.
Admin-Name: Josese Bula
Admin-Mailbox: jbula@abcdef.com.fj
Tech-Name: Maciu Vinaka
Tech-Mailbox: mvinaka@abcdef.com.fj
NS1-Hostname: dns1.somenetwork.com.fj
NS1-Netaddress: 202.151.23.2

Google

Find vulnerabilities, revealing error messages, usernames and sometimes even **passwords** on your target host, all without ever connecting to it

see <http://johnny.ihackstuff.com/>

2. scan/sniff to find a way in

nmap

superscan

tcpdump

wireshark (formerly ethereal)

dsniff

nessus

3. exploit vulnerabilities

metasploit framework

john the ripper

cain and abel

thc-hydra

4. cover your tracks

```
nc -L -d -t -p 23 -e cmd.exe
```

```
rootkits
```

edit logs

help! what can i do?

- . remove all unnecessary services*
- . firewall services that do not need remote access*
- . actively patch vulnerabilities*
- . use strong passwords*

most importantly:

- . educate your users again and again and again*

*chris hammond-thrasher, cissp
hammondthrasher_c@usp.ac.fj*