Appendix A

Useful Free Stuff

> Only those defenses are good, certain and durable, which depend on yourself alone and your own ability.
>
> *The Prince*
> —NICCOLÒ MACHIAVELLI

For those contemplating securing their own networks, a lot of useful—and free—code is available on the Internet. Here we list a number of packages, along with their locations as of mid-1994. The list is necessarily incomplete; new code is being written all the time.

Bear in mind that you must accept all responsibility for running any of this code on your machine. We do not use all of the packages listed here. Even though we believe that none of the authors have planted any Trojan horses, we cannot guarantee that any of the code is bug-free. Nor can we guarantee the security of the archive sites—there have been at least two incidents of sabotaged network utilities. It is quite within the realm of possibility that some or all of these packages have been tampered with. Besides, we could be wrong about the authors. . .

On a more mundane but equally serious level, some of the software we mention is subject to various usage and/or distribution requirements. Read all such notices carefully.

In addition to the places we have listed, many tools are archived on FTP.UU.NET in the USENET archives, or on FTP.CERT.ORG. A number of other useful security tools may be found on the latter as well.

To retrieve a file from an archive site via FTP, use the dialog shown in Figure A.1 if you are on a UNIX system. Material that you should type is shown in a font *`like this`*. Fill in the appropriate values for `archive.site`, *`package`*, etc. There are numerous other useful subcommands to FTP, such as *ls* and *cd*; consult your local manual for details.

If you do not have FTP access, you can retrieve many packages by electronic mail. Send a message saying `help` to *ftpmail*@DECWRL.DEC.COM.

```
$ ftp archive.site
Connected to archive.site.
220 archive FTP server ready.
Name (archive.site:yourname):  anonymous
331 Guest login ok, send ident as password.
Password:  # Give your email address
230 Guest login ok, access restrictions apply.
ftp> binary
200 Type set to I.
ftp> get pkg myfilename
200 PORT command successful.
150 Binary data conn. for pkg (1.2.3.4,1738) (xx bytes).
226 Binary Transfer complete.
local:  myfilename remote:  pkg
xx bytes received in yyy seconds (zzz Kbytes/s)
ftp> quit
221 Goodbye.
$
```

Figure A.1: Retrieving files via anonymous FTP.

A.1 Building Firewalls

A.1.1 TCP Wrapper and Potmapper

The *tcpwrapper*, by Wietse Venema, is the best known mechanism for adding logging and filtering to most standard services. It is restricted to services that are invoked through *inetd*. A companion program, *potmapper*, provides similar services for RPC-based servers invoked via the standard *portmapper*.

Host: FTP.WIN.TUE.NL
Path: `/pub/security/tcp_wrapper*`
Host: FTP.WIN.TUE.NL
Path: `/pub/security/portmap.shar*`

A.1.2 Securelib

As noted, the *tcpwrapper* only works for servers run via *inetd*. The *securelib* [LeFebvre, 1992] package is a replacement shared library for SunOS that provides filtering for servers that are not invoked by *inetd*.

Host: EECS.NWU.EDU
Path: `/pub/securelib.tar`

A.1.3 Socks

The *socks* [Koblas and Koblas, 1992] package can be used to build circuit relays and firewall machines. The subroutines used by the applications have calling sequences that are almost identical to the standard networking system calls, which makes installation fairly easy.

Host: FTP.INOC.DL.NEC.COM
Path: `/pub/security/socks.cstc`

A.1.4 TIS Firewall Kit

The TIS firewall toolkit [Avolio and Ranum, 1994] is a set of software components and system configuration practices intended to provide the basic building blocks for Internet firewalls. Included with the tookit are application proxies for *telnet*, *rlogin*, and FTP, as well as tools for securing SMTP-based mail, and providing strong user authentication.

Host: FTP.TIS.COM
Path: `/pub/firewalls/toolkit`

A.1.5 Proxy X11

As noted in Chapter 3, use of X11 through a firewall is best mediated via an application gateway. The *xforward* [Treese and Wolman, 1993] package provides this service. Note the copyright restrictions before deciding to use it.

Host: CRL.DEC.COM
Path: `/pub/DEC/xforward.tar.Z`

A.1.6 Bellcore S/Key

S/Key is a one-time password scheme based on [Lamport, 1981]. Its big advantage is that it requires no extra hardware; you can print off a list of passwords for use when traveling. Support for *S/Key* is included in the TIS firewall kit.

Host: THUMPER.BELLCORE.COM
Path: `/pub/nmh/skey`

A.1.7 The *Ident* Daemon

There are two almost-compatible versions of the Identification Daemon protocol, *ident* and *tap*. Both may be built from the same source code.

Host: FTP.LYSATOR.LIU.SE
Path: `/pub/ident`
Host: FTP.UU.NET
Path: `/networking/ident`

A.1.8 The *Swatch* Logfile Monitor

Swatch is a tool that lets you associate actions with logfile entries. You can arrange for mail to be sent, *finger* commands executed, etc.
Host: SIERRA.STANFORD.EDU
Path: `/pub/sources/swatch.tar.Z`

A.1.9 Network Daemon Source Code

The source code for recent versions of many network daemons is freely available, though often protected to some extent by copyright. We list just one set on one archive machine; many variants are scattered around the Internet.

Most of these tools will not compile unchanged on your version of UNIX. On the other hand, they won't require much work, in most cases, and if you spend the time to find or build a compatibility library early on, you'll have a much easier time with the next one.

The `Linux` versions present an interesting question: they are not for any vendor's standard version of the UNIX system, but they're often the latest and greatest. Of course, too often that means that they have the latest and greatest bugs, or that they're Feature Creatures.
Host: FTP.UU.NET
Path: `/systems/unix/bsd-sources/usr.sbin/{inetd,portmap,syslogd}`
Host: FTP.UU.NET
Path: `/systems/unix/bsd-sources/libexec/*`
Host: FTP.UU.NET
Path: `/systems/unix/linux/packages/net/net-2/sources/*`

The latest version of *telnet* runs on most platforms. It does not include support for encryption, because of U.S. export regulations; the version with encryption is supposed to be part of the domestic release of 4.4 BSD.
Host: FTP.CRAY.COM
Path: `/src/telnet/telnet.94.02.07.NE.tar.Z`

A.1.10 *Screend*

Screend [Mogul, 1989] is a package that lets you convert a UNIX system into a packet filter. However, you need kernel source code to install it.
Host: GATEKEEPER.DEC.COM
Path: `/pub/DEC/screend/screend.tar.Z`

A.1.11 NFS

Linux has a user-level NFS server. It would be a good starting point for a proxy version similar to ours.
Host: TSX-11.MIT.EDU
Path: `/pub/linux/BETA/NFS`

A.1.12 Karlbridge

Karlbridge is a package that converts a PC or equivalent into a bridge. Filtering can be done on the basis of IP address, port numbers, and the like. *Karlbridge* is also available as a commercial product; this is the free one.
Host: NISCA.ACS.OHIO-STATE.EDU
Path: `/pub/kbridge`

A.2 Network Management and Monitoring Tools

A.2.1 Tcpdump

Tcpdump is the best tool available for UNIX systems for monitoring traffic on a network.
Host: FTP.EE.LBL.GOV
Path: `tcpdump2.2.1.tar.Z`

A.2.2 Traceroute

Traceroute lets you determine the path to a given destination.
Host: FTP.EE.LBL.GOV
Path: `traceroute.tar.Z`

A.2.3 dig

Dig is a better tool for querying the DNS than the standard *nslookup* program.
Host: FTP.ISI.EDU
Path: `dig.2.0.tar.Z`

A.2.4 host

The *host* program is even better for building DNS shell scripts, though still rather complex.
Host: NIKHEFH.NIKHEF.NL
Path: `pub/network/host.tar.Z`

A.2.5 bind 4.9

The latest of *bind*, the UNIX system name server, has a lot of bug fixes and security patches. For example, it can be used to block zone transfers. Besides, you have the source, so you can make other necessary changes (although the code is quite complex).

Dig and *host* are bundled with *bind* 4.9.
Host: GATEKEEPER.DEC.COM
Path: `/pub/BSD/bind/4.9`

A.2.6 SNMP

A variety of useful information can be obtained via SNMP, especially from routers. There are many commercial packages available. A free one can be obtained from CMU.
Host: LANCASTER.ANDREW.CMU.EDU
Path: `pub/snmp-dist`

A.2.7 The *Fremont* Network Mapper

Fremont is a network topology discovery program. The copyright notice contains the following usage restriction:

> This software may not be used for purposes inconsistent with network appropriate use policies. Inappropriate use includes, but is not limited to, collecting information for the purposes of attempted illegal entry into a computing system.

Host: FTP.CS.COLORADO.EDU
Path: `pub/cs/distribs/fremont`

A.3 Auditing Packages

Even though the strongest gateways contemplate a successful invasion of their bastion host, life is simpler if that never occurs. A number of auditing packages are available that can help spot configuration errors. The auditing function is exceedingly important even if you choose not to evaluate your own machines. You may rest assured that volunteers on the Internet will do it for you, but they may not report their results to you.

A.3.1 TAMU

The *TAMU* system [Safford *et al.*, 1993b] is a collection of very useful tools. Some can be used to build your own firewall, others can detect attack signatures. The Tiger scripts can be used to assess the security of your own machines.
Host: NET.TAMU.EDU
Path: `/pub/security/TAMU`

A.3.2 COPS

COPS [Farmer and Spafford, 1990] is another popular auditing package along the lines of the Tiger scripts.
Host: FTP.CERT.ORG
Path: `/pub/tools/cops`

A.3.3 Tripwire

Tripwire [Kim and Spafford, 1993, 1994a, 1994b] that is a package that evaluates a system and checks for altered files and the like.
Host: FTP.CS.PURDUE.EDU
Path: `/pub/spaf/COAST/Tripwire`

A.3.4 ISS

The *ISS* package is a network vulnerability auditing package, along the lines of *TAMU* and our network sweep programs. It can be used to probe entire networks for vulnerabilities. Again, even if you choose not to run this package, others with less-than-pure hearts will. Closing the holes it checks for is vitally important.

ISS has been recently published for the first time. It covers a number of fairly old holes. We expect that the public will add modules to this package, until it becomes a very thorough test. If we are right, we encourage you to keep up with these tools and run them. The Bad Guys will.

The author of ISS has indicated that his future enhancements will be to a commercial version; the free one remains available.
Host: FTP.UU.NET
Path: `/usenet/comp.sources.misc/volume39/iss`
Host: AQL.GATECH.EDU
Path: `/pub/security/iss`

A.3.5 SATAN

SATAN is another network vulnerability auditing package. As of the latest press time it was not yet finished. Availability of the final version will be announced on various newsgroups and mailing lists.
Host: FTP.WIN.TUE.NL
Path: `/pub/security/satan.tar.Z`

A.3.6 Crack

The best way to beat password crackers is to get out of the game. Authentication devices are the best defense. Shadow password files help, but are no defense against the eavesdropper.

If you are stuck with passwords, the best defense against bad passwords is a smart version of the *passwd* program like *passwd +*. The *cracklib* library provides routines to check the safety of a proposed password.

If none of these are used, crack your own password files and weed out the weak ones. *Crack* is a well known and widely distributed password cracking program by Alec Muffett.
Host: FTP.CERT.ORG
Path: `/pub/tools/crack`
Host: FTP.CERT.ORG
Path: `/pub/tools/cracklib`

Crack permits you to add your own dictionaries. You can find a large collection in
Host: BLACK.OX.AC.UK
Path: `/wordlists`

A.3.7 SPI

SPI, the *Security Profile Inspector*, combines the functionality of programs such as *COPS* and *tripwire*. It also attempts to track important security patches on a per-platform basis. *SPI* is available only to certain U.S. federal and state government agencies; see the `README` file for details.
Host: IRBIS.LLNL.GOV
Path: `/pub/spi`

A.4 Cryptographic Software

Most of the packages listed in this section are described in detail in Chapter 13; no further description is given here. As noted there, much cryptographic software is subject to a variety of import, export, usage, and patent restrictions. Check carefully with a competent lawyer before proceeding.

A.4.1 RIPEM

Host: RIPEM.MSU.EDU
Path: `/pub/crypt/ripem`

A.4.2 RSAREF

Host: RSA.COM
Path: `/rsaref`

A.4.3 PEM

Host: FTP.TIS.COM
Path: `/pub/PEM`

A.4.4 PGP

PGP is available from a variety of non-U.S. sites; some are listed below. A more current list can be found via WWW from `http://www.mantis.co.uk/pgp/pgp.html`. The M.I.T. repository is for U.S. or Canadian residents only.
Host: NET-DIST.MIT.EDU
Path: `/pub/PGP`

Host: FTP.DSI.UNIMI.IT
Path: `/pub/security/crypt/PGP`
Host: FTP.DEMON.CO.UK
Path: `/pub/pgp/*`
Host: /FTP/FUNET.FI
Path: `/pub/crypt/pgp*`

A.4.5 Kerberos

Host: ATHENA-DIST.MIT.EDU
Path: `/pub/kerberos`

A.4.6 MD2 and MD5

Source code for the MD2 and MD5 hash functions can be found in the RFCs defining them: [Kaliski, 1992] and [Rivest, 1992].

A.4.7 SNEFRU

The *snefru* hash algorithm was developed by Ralph Merkle.
Host: PARCFTP.XEROX.COM
Path: `/pub/hash`

A.5 Information Sources

A.5.1 CERT Tools and Advisories

CERT—the Computer Emergency Response Team—provides an archive site. Among other things, they store tools contributed by the community, as well as their own security advisories. The file `tech_tips/packet_filtering` contains guidance on what ports should be blocked.
Host: FTP.CERT.ORG
Path: `pub/cert_advisories`
Host: FTP.CERT.ORG
Path: `pub/tools`
Host: FTP.CERT.ORG
Path: `pub/tech_tips`

A.5.2 The *Firewalls* Mailing List

A mailing list dedicated to firewalls is hosted at GREATCIRCLE.COM. To join the list, send mail to *majordomo*@GREATCIRCLE.COM with a body consisting of a single line:

```
subscribe firewalls
```

or

`subscribe firewalls` *your_email_address*

There is also a digest form, if you prefer to receive fewer messages per day; subscribe to `firewalls-digest` instead.

A.5.3 The *Bugtraq* Mailing List

Bugtraq is a security mailing list whose differentiating principle is that it's proper to disclose details of security holes, so that you can assess your own exposure and—perhaps—see how you can fix them yourself. Send subscription requests to *bugtraq-request*@FC.NET.

A.5.4 RISKS Forum

The *Risks Forum* is a moderated list for discussing the dangers to the public from poorly built computer systems. Although not a bug list *per se*, most significant security holes are reported there.

RISKS is available as a mailing list (send subscription requests to *risks-request*@CSL.SRI.COM) and as the *comp.risks* newsgroup on USENET. Excerpts from RISKS appear in *Software Engineering Notes*.

A.5.5 USENET Newsgroups

A number of USENET newsgroups are dedicated to various aspects of security. These include *comp.security.announce*, *comp.security.misc*, *comp.security.unix*, *alt.security*, and *sci.crypt*. Security-related discussions sometimes pop up in other newsgroups as well, such as *comp.sys.**, *comp.windows.x*, *misc.legal.computing*, etc. Naturally, the list changes constantly.

A.5.6 COAST Security Archive

The COAST Security Archive is intended to be a comprehensive repository for all sorts of papers, tools, etc. It will, as necessary, act as a mirror for other sites.
Host: COAST.CS.PURDUE.EDU
Path: `pub`