PRESIDENT'S
COMMISSION *on*
CRITICAL
INFRASTRUCTURE
PROTECTION

A HACKER PRIMER

Matt Devost

April 5, 1997

PREFACE

The President's Commission on Critical Infrastructure Protection (PCCIP) was formed to bring together the combined forces of government and industry to develop a strategy for protecting US critical infrastructures and assuring their continued operation. In order to fulfill the challenge of their mission, the PCCIP determined a need to categorize the range of potential threats including aggressor states, terrorists, criminals, insiders, computer hackers and natural disasters.

The purpose of this document is to provide information on one of the infrastructure threat categories: computer hackers. While much has been written about the hacker community, this document goes further to provide actual Internet reference points for hacker tools and hacker groups. It also provides a descriptive listing of hacker communication mechanisms and discussion of potential hacker targets, motivations and trends.

The document is organized as follows:

An introduction to the document is followed by an examination of hacker organizational and social considerations to include a detailed listing of hacker communication mechanisms and listings of high profile hacker groups. Subsequent sections identify hacker targets and off-line techniques hackers use to supplement their intrusion capabilities, provide a descriptive listing of common hacker tools with Internet reference points, and furnish a listing of hacker references to include WWW sites, related books, magazines and movies.

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

TABLE OF CONTENTS (Continued)

HACKER PRIMER

1.0 INTRODUCTION

Critical infrastructure protection requires an adequate understanding of the threat and capabilities of potential adversaries. This document provides insights into one of the infrastructure threat categories: hackers. This document was compiled from open sources to provide educational background material and points of reference only. It was not an investigation, nor does inclusion in this document imply criminal or other illegal activity. If you decide to visit any of the online resources included in this document, please do so at your own risk. Remember, your activity will be tracked when you are browsing some of these sites, so do so from behind an adequate firewall or through a dynamic Internet Service Provider account.

2.0 ORGANIZATIONAL AND SOCIAL CONSIDERATIONS

A comprehensive study[1] of the hacker community was conducted by Nicholas Chantler over a period of 12 years. Mr. Chantler's Ph.D thesis provides the first comprehensive description of hackers and their environment based on formal research. He interviewed over two hundred hackers and examined hacker "artifacts" such as files, email, and other communications to derive statistics about the hacker community's social structure and its knowledge base. Among the 500 pages of data, we find that:

- Most hackers start hacking at age 14 - 15.
- Only 22 percent select specific targets to hack.
- 48 percent admit to working alone instead of as a team or hacker group.
- Only 1 percent admitted that the threat of detection and prosecution inhibit their activity.
- Reasons for hacking:

Addiction	Freedom
Knowledge	Recognition
Self-gratification	Pleasure
Challenge	Friendship
Excitement	Profit
Sabotage	Espionage
Theft	Vengeance

(Challenge, Knowledge and Pleasure combined, total nearly half of the reasons why hackers hack.)

The hacker community lacks any significant organizational structure, but does tend to aggregate based on capabilities and knowledge. The most knowledgeable and skilled of the hacker community are the "elite" and the unskilled are often referred to as "newbies" or "lamers."

---

[1] Chantler, Alan Nicholas, "Risk: The Profile of the Computer Hacker," School of Information Systems, Curtin Business School, Australia, 24 November 1995.

Lamers seek knowledge from the elite in hopes of conducting hacks that will allow them to garner elite status within the community. Because knowledge is a form of power or currency online, communication mechanisms are established to facilitate information sharing. These mechanisms are described in detail in Section 2.2.

2.1 Terminology

While the term hacker is used indiscriminately throughout this document to describe a larger subset of individuals and activities, the online community does differentiate itself based on ethical and functional considerations. The following provides a brief overview of hacker terminology.

2.1.1 Hackers

The use of the term "hacker" has been subject to controversy over the past several years. Historically, the term hacker was used to describe a computer enthusiast who enjoys learning everything about a computer system and, through clever programming, pushing the system to its highest possible level of performance. Today, the term has taken on a duality to describe not only the traditional type hackers, but anyone involved in criminal activity conducted via a computer or network technology.

Steven Levy, in his book, *Hackers: Heroes of the Computer Revolution* identified what he described as a hacker ethic. Today's hackers often cite the hacker ethic as the difference between good hackers and bad hackers:

- Always yield to the hands-on imperative! Access to computers - and anything else which might teach you about the way the world works - should be unlimited and total.
- All information should be free.
- Mistrust authority - promote decentralization.
- Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.
- You can create art and beauty on a computer.
- Computers can change your life for the better

2.1.2 Crackers

The term cracker is often used to signify the criminal element of the hacker community. Crackers break into systems, not for the excitement or knowledge, but for disruption, destruction or personal gain. In 1994, when Emmanuel Goldstein, editor and publisher of 2600 Magazine, was asked to convene a panel of Hackers v. Crackers for the Conference on Computers Freedom and Privacy, the hacker side of the panel filled five seats, while the crackers were represented by a box of saltines. The distinction Goldstein was trying to make, however unclear, was that crackers are the criminals, and while many known hackers were happy to participate in the panel, he could not identify one human cracker willing to round out the debate.

2.1.3 Warez Dudez

Warez dudes or software pirates are engaged in the illegal copying, cracking and sharing of commercial software via the Internet or other electronic medium.

2.1.4 Phreaks

Phreaks or phreakers focus their attention on exploiting, manipulating or exploring public and private phone networks. The online hacker publication Phrack is a combination of the words Phreak and Hack signifying its target audience - most hackers are often phreaks as well in order to circumvent the high phone bills they would otherwise incur from being online.

2.2 Communication Mechanisms

The hacker realm of choice is the networked environment. In order to share information, the hacker subculture utilizes several forms of interaction mechanisms. These range from real-time electronic data exchange, such as Internet Relay Chat and telephone conferencing, to face to face social gatherings, affectionately referred to as "cons." This section describes and details these various interaction mechanisms.

2.2.1 Bulletin Board Systems (BBS)

Bulletin board systems were the first major interaction mechanism utilized by the hacker community. A bulletin board system would be established on someone's home computer and opened for access based on certain criteria. Most were private and individuals were given access if they knew the right person or could demonstrate a particular skill. Many of the boards tended to be regional, which resulted in the formation of many regional hacker groups. However, the most skilled hackers could circumvent phone systems to the degree where they called bulletin board systems world-wide at no cost.

Bulletin board systems allow for the exchange of information, email and binary files (hacking tools, illegal copies of commercial software, viruses) limited only by the storage capability of the host machine. In today's technological environment, the potential storage space on any given system is practically unlimited.

With increased access to the Internet and numerous law enforcement operations targeting hacker bulletin board systems[2], usage of this mechanism has become less common. However, many hacker groups still utilize private bulletin board systems to exchange information. The following table presents an unconfirmed listing of current hacker BBS:

[2] The biggest of these being Operation Sundevil.

Bulletin Board System	Phone Number
Rune Stone	(203)832-8441
The Truth Sayer's Domain	(210)493-9975
Hacker's Haven	(303)343-4053
Independent Nation	(413)573-1809
Ut0PiA	(315)656-5135
underworld_1994.com	(514)683-1894
Alliance Communications	(612)251-8596
Apocalypse 2000	(708)676-9855
K0dE Ab0dE	(713)579-2276
fARM R0Ad 666	(713)855-0261
kn0wledge Phreak BBS	(719)578-8288
The Edge of Reality	(805)496-7460
Static Line	(806)747-0802
Area 51	(908)526-4384

2.2.2 Newsgroups

Usenet newsgroups are distributed mechanism for sharing discussion, information and correspondence based on subject areas. There are over 20,000 newsgroups currently in operation on any number of subjects. Postings to newsgroups are distributed to all newsgroup servers allowing for discussions to take place at a global level. Posting can also be anonymous, which allows hackers to post sensitive or illegal information without fear of compromising their identity. However, due to the global distributed nature of Usenet, it is easily and actively monitored by corporations and law enforcement. The following table designates some of the newsgroups that attract or facilitate hacker participation in the discussion:

Newsgroup	Description
alt.2600 alt.2600hz alt.2600.codez alt.2600.debate alt.2600.moderated	The 2600 hierarchy of newsgroups are used for the discussion of hacking and phreaking. The most popular and active, by far, is the alt.2600 newsgroup.
alt.cellular alt.cellular-phone-tech	Newsgroups dedicated to the discussion of cellular technology are often inhabited by hackers looking to harvest information regarding the operation of cellular phones and networks.
alt.comp.virus	Dedicated to the discussion of viruses.
alt.comp.virus.source.code	More technical discussion of viruses to include the distribution and analysis of source code which if compiled becomes a live or active virus.
alt.cracks	Discussion and distribution of cracks or hacks for commercial software.

alt.cyberpunk	A hacker oriented newsgroup that focuses on the social instead of the technical issues of hacking as well as cyberpunk science fiction works by authors such as William Gibson, Bruce Sterling, and Neal Stephenson
alt.fan.kevin-mitnick	A newsgroup that follows the activities and trials of famed hacker Kevin Mitnick
alt.fan.lewiz	Lewis De Payne fan club
alt.hackers	Historical hacker newsgroup focused on the technical discussion of technology with very little focus on intrusion techniques.
alt.hackintosh	Newsgroup discussion Macintosh hacking.
alt.hackers.malicious	Discussion of destructive hacking.
alt.ph.uk	United Kingdom version of alt.2600
alt.radio.pirate	Pirate radio discussions. Most hackers also have an interest in radio and many run pirate radio stations. A hacker vehicle caravan from California to the annual Defcon conference in Las Vegas features a traveling pirate radio station for the listening pleasure of hackers in the caravan.
alt.radio.scanner	Scanners are also a favorite toy of hackers for signals interception and law enforcement monitoring.
alt.security	Newsgroup for discussion of computer security issues.
comp.dcom.telecom	Telecommunications digest (Moderated)
comp.os.netware.security	Discussion of Novell Netware security.
comp.protocols.tcp-ip	Discussion of TCP and IP network protocols, which are the protocols utilized on the Internet and other networks.
comp.risks	Discussion of the risks to the public from computers and systems. Moderated by the Association of Computing Machinery (ACM).
comp.security.announce	Announcements from CERT about security
comp.security.firewalls	Discussion of firewall security.
comp.security.misc	Another security oriented group.
comp.security.unix	Discussion of Unix security
comp.virus	Computer viruses & security (Moderated)
de.org.ccc	Newsgroup for the Chaos Computer Clube
rec.radio.scanner	Another newsgroup dedicated to scanner discussion.

2.2.3 Mailing Lists

Mailing lists are a popular Internet interaction mechanism and have been utilized by the hacker community in a limited manner. Many members of the hacker community participate in professional computer/network security mailing lists, but there are mailing lists reserved for hacking related discussion. Due to their open nature, these mailing lists tend to focus on personal interaction and on requests for information. Very limited discussion of illegal activities

takes place for fear of law enforcement monitoring the list traffic. The table below provides a sampling of mailing lists of interest to hackers:

Mailing List	Subscription Directions
8lgm (Eight Little Green Men)	majordomo@8lgm.org subscribe 8lgm-list
Group of hackers that periodically post exploit scripts for various Unix bugs.	
Bugtraq	LISTSERV@NETSPACE.ORG SUBSCRIBE BUGTRAQ
This list is for detailed discussion of UNIX security holes: what they are, how to exploit, and what to do to fix them.	
Computer Underground Digest	cu-digest-request@weber.ucsd.edu SUB CUDIGEST
Covers issues and news concerning the computer underground.	
Windows NT Security	request-ntsecurity@iss.net subscribe ntsecurity
This is an unmoderated mailing list discussing Windows NT security as well as the Windows 95 and Windows For Work Group security issues.	
Sneakers	majordomo@cs.yale.edu subscribe Sneakers
The Sneakers mailing list is for discussion of LEGAL evaluations and experiments in testing various Internet "firewalls" and other TCP/IP network security products.	
DefCon Stuff	majordomo@dis.org subscribe dc-stuff
Hacker mailing list for the annual DefCon hacker conference that is used for hacking discussions and information requests.	

2.2.4 Internet Relay Chat

Internet Relay Chat is a real-time text-base interaction mechanism. Hackers flock to designated hacker “channels” for discussion, information exchange and to trade files. There are many public channels designated as hacker areas based on subject groupings (hacking, phreaking, warez trading), but often hackers move to private or invite-only channels based on pre-established groupings of “who knows who?” The following table lists hacker IRC channels.

Channel	Description
#hack #hackers #hackerz	Miscellaneous hacker IRC channels. Discussion of hacker events, files exchange, etc. Actual channel name varies from server to server and all three may be present at one time. Depending on who is running the channel, it may be invite only.
#2600 #2600hz #2600(XXX) XXX = Area Code	IRC channel focused on the hacker magazine 2600. Various hacking, phreaking and social discussion. Occasionally used for 2600 sponsored IRC meetings. Groups often segment off into separate channels based on area codes or other regional distinctions.
#wares #warez	Channels dedicated to software piracy.
#phreak	Channel focused on telephone network intrusion and manipulation.
#root	Another hacking oriented channel. To obtain "root" on a system is to have system administrator privileges.
#unix	Channel dedicated to discussion of hacker operating system of choice.
#cellular	Channel dedicated to the discussion of cellular technology.

2.2.5 Conferences and Meetings

The hacker community gathers several times annually to meet face-to-face and exchange information and demonstrate hacking prowess. Hackers have been gathering at these conferences for at least ten years. Initially, most conferences were invite-only but in most cases that trend has been discontinued in favor of a more open and accessible format. Some hacker conferences openly invite law enforcement and security professionals to join them for discussion and some of these professionals are even featured speakers at the events. Most notably, the annual DefCon conference in Las Vegas has had speakers from the FBI and private industry and features a Hacker Jeopardy-like contest that once resulted in a final round between military representatives and a hacker group.

Typically, these conferences have network connectivity and hacking contests on volunteered machines. The average hotel room has several computers and radio receivers/transmitters. In fact, a tactical communications channel is usually established for the conference organizers and attendees to keep up with any conference activities that might be occurring. Police and security frequencies are also monitored for indications that rooms might be searched or to determine other law enforcement/security actions. The following table provides a listing of hacker conferences and meetings:

Conference	Location	Date	More Information
DefCon	Las Vegas	July	[http://www.defcon.org]
Perhaps the most popular of the hacker conferences. Attendance levels have risen over the years such that over 1,000 people are expected to attend the 1997 conference. Conference organizers welcome law enforcement, computer security specialists and other interested parties.			
SummerCon	Washington, D.C.	Summer	email scon@2600.com
Annual conference alternates between Washington DC and Atlanta and focuses on security issues. Historically a social conference, speakers are usually drawn from the audience. Traditionally invitation only, it is now open to any interested in attending. The 1996 conference featured an a group tour of the FBI headquarters.			
PumpCon	Philadelphia	October/November	
Invitation only conference is usually publicized on the Internet in advance. Activities usually lead to the arrest of one or more of the conference members every year.			
HoHoCon (CuervoCon)	Texas	December/January	[http://www.cuervocon.org]
Annual Christmas hacker gathering. Recently renamed CuervoCon when the conference was held on the Mexican border in Texas in 1996.			
HOPE	New York City	August	[http://www.2600.com]
Hackers on Planet Earth (HOPE) was originally held to celebrate the 10th anniversary of the hacker magazine 2600. Due to the popularity of the conference, it will recur at undetermined intervals in years to come. The second HOPE conference (Beyond HOPE) will be held in New York City on August 8-10, 1997. It will coincide and have direct Internet links established with the European hacker conference Hacking in Progress (HIP).			
2600 Meetings	Various locations worldwide	First Friday of the Month	[http://www.2600.com/magazine/meetings.html]
Hackers gather the first Friday of each month at various locations worldwide to meet face to face and exchange information. Meeting are open to all and are held at public locations like malls.			
HIP	Netherlands	August	[http://www.hip97.nl]
Hacking in Progress (HIP) is the annual European hacker conference. Site location is usually a campsite with tents and other temporary structures used as the conference center. This year the HIP conference coincides and will have direct Internet links to the U.S. based HOPE conference.			

2.3 Hacker Groups

There are hundreds of hacker groups around the world. Some are loosely organized social affiliations used to find people of similar interests. Many are based on geography such as state or even a telephone area code. A handful are used to combine skill sets to create a resource pool for hacking activities and focus on producing hacking tools, concepts and sometimes protection mechanisms. There are also criminal hacker groups, maintaining a lower profile and using the anonymity of the Internet to conduct their illegal activities. This section highlights some of the more visible and stable hacking groups on the Internet. Their sites provide valuable staring points for a very dynamic community that changes web addresses or resource locations often. It is not implied that these groups are engaged in illegal activity, but rather provide useful insights regarding the nature of the hacker community.

2.3.1 The Internet Liberation Front

Group responsible for a series of Internet attacks in 1994 - 95. Hacker Christopher Schanot was arrested for these attacks. It is not known whether he was operating alone at the time, but the name "ILF" is often attributed to current hacks.

2.3.2 johnny [xchaotic]

Responsible for the series of email bombings in 1996 that targeted government, journalists and other selected targets. Though their "Open Letter" to the Internet speaks in the plural, it is not known whether this a hacker group or one individual, commonly referred to as the Unamailer.

2.3.3 Cult of the Dead Cow (CDC) [http://www.l0pht.com/cdc.html]

Hacker group that operates out of the l0pht in Boston, MA. They help sponsor many of the hacker conferences and sell hacking CDROMS as well numerous hardware inventions.

2.3.4 The Dismembered Youth Corps [http://www.tdyc.com/]

Hacker group that advocates "annoying" behavior on the Internet.

2.3.5 The Guild [http://www.slip.net/~daemon9/guild.html]

Hacker group that claims among its members the editor of the electronic hacker magazine Phrack. Source code and white papers for some of the most sophisticated Internet attacks come from this group including the Phrack version of the SYN Flooding program. Their homepage suggests "Corporate persuasion through Internet terrorism."

2.3.6 The New Order (TNO) [http://38.250.25.1/tno/index.html

Hacking group from Colorado loosely associated with the Guild.

2.3.7 TACD [http://www.tacd.com/main.htm]

Techno Anarchists Creating Disorder (TACD) provides one of the more sophisticated hacker group web sites on the Internet.

2.3.8 The Infected [http://www.infected.com]

Hacker group focused on virus creation and distribution.

2.3.9 Global kOS [http://globalkos.org]

Hacker group that wrote and distributed the mail-bombing/denial of service program called "UpYours!"

2.3.10 X-trem [http://www.nyct.net/~nyangel/x-treme/]

Hacker group that describes themselves as the "future of hacking."

2.3.11 The Legion of Doom [http://www.lod.com]

Famous hacking group from the late 1980s to early 1990s. Fought a hacker war across corporate, educational and government networks against the Masters of Deception. Various members of both groups were convicted for their crimes. Their website offers legitimate ISP services, but hacker files are still available in some directories.

2.3.12 The Masters of Deception

Famous hacking group from the late 1980s to early 1990s. Involved in hacker war with the Legion of Doom. Group member Mark Abene (Phiber Optik) was convicted in a very high profile hacker case.

2.3.13 The Inner Circle (New and old)

The original Inner Circle was an early 80s hacking group that disbanded after the arrest of several of its members. Recently, the name Inner Circle has reemerged in conjunction with a popular and very exclusive software piracy group that posts thousands of dollars worth of illegal software to publicly accessible Internet sites every day.

2.3.14 Chaos Computer Club [http://www.ccc.de/]

European hacker group profiled in the computer espionage book *The Cuckoo's Egg* by Cliff Stoll. This group is still active and recently grabbed media headlines when it demonstrated a flaw in Microsoft's Internet Explorer that allowed the group to transfer funds from the accounts of people who hit a specific web page on their server.

2.3.15 Dutch Hackers

Hackers from the Netherlands that probed and intruded on American military systems during the Gulf War. Though lacking any organizational structure, the Dutch hacker group is still active in the hacker community sponsoring and organizing one of Europe's largest hacker conferences. Hac-Tic, a Dutch hacking magazine similar to the US-based 2600 recently went out of business, but the Hac -Tic owned Internet Service Provider is thriving and offers safe haven to materials that might be or have been censored in other European countries.

2.3.16 R00T [http://www.r00t.org]

Hacker group with a strong presence at many hacker conferences. Information on the website varies and is sometimes completely blank.

2.3.17 SIN [http://www.sinnerz.com]

Self Induced Negativity (SIN) is a gothic styled hacker group that writes hacker software and makes it available online. It also produces hacker literature and has been known to interview other hackers for publication online.

2.4 Social Issues (Hot Buttons)

The hacker community tends to be rebellious in nature. This may be due to the fact that a majority of hackers are most active between the ages of 14 and 22. However, there are several issues that serve as catalysts for hacker activity. Perhaps the most significant issue is government or corporate involvement in the Internet. Many sites have been hacked in the past two years in which messages where left signifying that the attack was conducted because of corporate involvement in the Internet. The government is also a target because of recent efforts to regulate content on the Internet. The recent attack on the Department of Justice website protested the Communications Decency Act, which is currently under Constitutional review by the Supreme Court.

Another social issue of great concern to hackers is privacy and protecting privacy through encryption. Most hacker sites contain encryption programs, information and links. Some hacker communications are encrypted and it is common to find hacker storage drives encrypted to prevent law enforcement forensic teams from gathering incriminating data. Government key escrow and encryption initiatives such as the Clipper chip are protested in the hacker community.

3.0 HACKER TARGETS AND OFFLINE TECHNIQUES

3.1 Targets

Hackers are fairly non-discriminate in choosing their targets, as was noted in the Chantler thesis. Universities and Internet Service Providers usually offer practice ground for new hackers or new methods, while corporations and government sites are "prize" kills. Depending on the motives

of the hacker, the target site might be chosen to maximize public exposure to the hacking "feat." Recent WWW hacks might be viewed as ego or exposure type hacks, since they were initiated not to gain data or deny service but to demonstrate capability or to protest against the target site.

The following table outlines some of the attacks that have occurred in the past year:

Target System	Type of Attack
Department of Defense	Croatian teenage hacker used openly available hacker tools to hack into the computers at Anderson Air Force Base.
CIA	WWW attack replaced the CIA homepage with a protest page containing hacker links and pornography.
Department of Justice	WWW attack replaced the DoJ homepage with a protest page featuring a picture of Hitler, hacker links and pornography. Potentially spurned by the DoJ Supreme Court case over the Communications Decency Act.
U.S. Air Force	WWW attack replaced an Air Force homepage with alternative content.
NASA	WWW attack replaced a NASA page with alternative content.
PANIX	Denial of Service SYN attack disrupted business operations for several days.
WebCom	Denial of Service SYN attack disrupted business operations for several days.
NCAA website	WWW attack replaced NCAA homepage with racist content. This attack was coordinated to coincide with the announcement of the NCAA tournament selection committee results, thus maximizing the potential exposure of the hack.
British Labour Party website	WWW attack replaced Labour Party homepage with alternative content.
Kriegsman Furs	WWW attack replaced corporate page with a protest page.

With the exception of the telecommunications and financial services infrastructures, there is very little openly available information on the Internet regarding infrastructure targets. The material available on the telecommunications infrastructure is oriented towards fraud and not destruction.

Determining the level of hacker activity in these infrastructures requires adequate reporting from the infrastructure owners, an unlikely possibility given the reluctance of the private sector (which owns, operates and maintains most infrastructure assets) to expose itself to liability or public distrust.

3.2 Off-line Techniques

Hackers supplement their online capability with the off-line techniques such as social engineering or trashing (discussed below). These techniques are used to gain additional information to supplement on ongoing or forthcoming attack.

3.2.1 Social Engineering

Social engineering is a deception technique utilized by hackers to derive information or data about a particular system or operation. A hacker, for example, will call a company claiming to be an internal technician and trick a user into revealing information such as an account password or dial-in line number.

Because social engineering is a form of acting, the hacker might play one of several roles: a new computer illiterate employee calling technical support for log on instructions; a technician trying to troubleshoot a network problem; hysterical employee trying to access data for a deadline project; or secretary or assistant to senior management trying to track down information in a crisis situation or with a very demanding "your job is on the line" tone. Each of these social engineering techniques have been successfully demonstrated numerous times and are often practiced before live audiences at hacker conferences.

3.2.2 Trashing (Dumpster Diving)

Trashing involves physically entering the trash containers at a target site in hopes of finding valuable information such as passwords, system documentation, or employee personal information to be used for social engineering attacks.

3.2.3 Physical Penetration

Hackers may also attempt to physically penetrate the target site in order to collect manuals, software and other valuable information. Some physical penetrations involve actually disguising as an employee. Others simply involve looking for open access points at the physical target. Physical penetration was especially popular at telecommunications sites such as switching centers. A hacker may also get a job within the target building in order to gain physical access.

3.2.4 Frequency Monitoring

Hackers are also very active in the area of signal interception in various forms. Scanners are bought with a capability for, or modified to, intercept cellular phone calls. These scanners are also used to track law enforcement communications, utility communications, and other radio

communications of interest. When the notorious hacker Kevin Mitnick was arrested, he was actively monitoring police frequencies for activity that might lead him to believe his identity and location had been compromised. However, law enforcement was aware of this capability and refrained from radio communications when raiding his location.

Scanners also easily intercept cordless phone communications and other radio frequency devices such as baby monitors, cordless speakers and intercoms.

At least one hacker group also sells devices that when plugged into a scanner and interfaced with a computer allow for the interception of alphanumeric and numeric pager transmissions. These devices are used to monitor nation-wide paging and local paging services. The software has the capability to log all message traffic and also allows for tracking of specific pager traffic. A hacker could obtain your pager number from a business card or correspondence, send you a trigger page such as "9999999999" to obtain your pagers unique RIC code, and then set the software to log and alert him/her of every page that you receive.

4.0 COMMON HACKING TOOLS

There is a trend, both within the security industry and the hacker community, to automate and design graphical user interfaces for hacking tools and site assessment utilities. These easier-to-use tools allow individuals with limited technical expertise to test or penetrate the security of a given network or host.

4.1 Vulnerability Assessment Tools

4.1.1 **COPS** [ftp://coast.cs.purdue.edu/pub/tools/unix/cops/]

Computer Oracle and Password System (COPS) is a UNIX security toolkit that analyzes your system security. Created by Dan Farmer while he was a graduate student, this program is the predecessor to the now famous SATAN security analysis tool developed and distributed by Farmer.

4.1.2 **SATAN** [ftp://coast.cs.purdue.edu/pub/tools/unix/satan/]

Security Administrator Tool for Analyzing Networks (SATAN) is another UNIX security toolkit that analyzes system security. This program generated a lot of concern when it was released, because it allowed for the analysis of external sites and provided an analysis tool with a graphical user interface.

4.1.3 **ISS** [http://www.iss.net]

Internet Security Scanner (ISS) is a commercial product that provides vulnerability assessments from a graphical user interface on a variety of platforms. The demo version of this program is freely distributed on the Internet, but only allows for the analysis of the local host or computer it is being run on.

4.2 Exploit Scripts and Hacking Toolkits [http://www.tacd.com/exploit/expmain.htm]

These scripts are written to exploit known vulnerabilities in certain classes of systems, operating systems or hardware configurations. New exploit scripts are produced weekly and are often distributed within the hacker community prior to a formal announcement by the vendor of the product or a third party such as CERT. This allows a window of vulnerability in which systems can be exploited before a patch is implemented. For a comprehensive list of exploits, see the above Internet site run by the hacker group TACD.

4.2.1 Sendmail Exploits [http://www.tacd.com/exploit/mail.htm]

Sendmail is one of the most utilized Unix utilities used on the Internet for the exchange of electronic mail. There are numerous sendmail exploits and it is identified as one of the top vulnerabilities exploited on the Internet. New vulnerabilities are identified on almost a monthly basis. The 1996 CERT Annual Report acknowledges that:

> "Intruders continued to attack the sendmail program. Unfortunately, some of these attacks were successful because sites were running old versions of sendmail and/or were not restricting the sendmail program mailer facility. The most current version of sendmail contains many security fixes. Sendmail's program mailer facility can be restricted by using the sendmail restricted shell program (smrsh) or a program called mail.local. This year, the CERT/CC published three advisories relating to sendmail vulnerabilities."[3]

It is anticipated that Sendmail will continue to be a hacker target of opportunity and additional vulnerabilities and potential exploits will be found allowing hackers to compromise the target system.

4.2.2 Other Common Exploits [http://www.iss.net/vd/vd.html]

Exploits have also been written for most common Unix utilities, especially for those for which a known vulnerability exists, such as ftp, login, fingerd, snmp, and httpd. Internet Security Systems maintains on online database of common vulnerabilities which may be exploited by a potential intruder.

4.2.3 ROOTKIT [http://www.ilf.net/Toast/files/unix/rootkit.zip]

RootKit is a common hacker tool used to obtain and maintain system administrator privileges on a target system. RootKit includes a network sniffer, a backdoor login which disables the computer auditing function, Trojan horse system utilities, and an installation tool to match checksums to originals so system administrators do not notice changes.[4]

---

[3] CERT 1996 Annual Report, Feb 23, 1997, Available online: [http://www.cert.org/cert.report.96.html

[4] Denning, Dorothy. "Protection and Defense of Intrusion," March 5, 1996. Available online: [http://guru.cosc.georgetown.edu/~denning/infosec/USAFA.html]

4.3 Attack Scripts and Programs

Attack scripts are intended to disrupt, degrade or disable a target system. They are often used for revenge or denial of service attacks. There has been a significant increase in these type of attacks over the past few years.

4.3.1 SYN Flooding

[ftp://ftp.infonexus.com/pub/Source/Guild/Route/Projects/Neptune/neptune.tgz]

SYN Flooding denial of service (DOS) attacks (explained below) have caused considerable concern on the Internet in the past 12 months. While this vulnerability has been known for over ten years, the technical expertise required to implement the attack acted as a protective membrane. However, within two weeks of each other, two hacker magazines, Phrack and 2600 published source code that exploited the SYN flooding vulnerability, making it an viable attack method to a large number of hackers with little technical expertise.

Security expert Dale Drew from MCI describes the vulnerability:

"When a normal TCP connection starts, a destination host receives a SYN (synchronize/start) packet from a source host and sends back a SYN ACK (synchronize acknowledge). The destination host must hear an ACK of the SYN ACK, and then the connection is established. This is referred to as the "TCP three-way handshake."

While waiting for the ACK to the SYN ACK, a connection queue of finite size on the destination host keeps track of connections waiting to be completed. This queue typically empties quickly since the ACK usually arrives a few milliseconds after the SYN ACK.

The TCP SYN attack exploits this design by having an attacking source host generate TCP SYN packets with random source addresses at a victim host. The victim destination host sends a SYN ACK back to the random source address and adds an entry to the connection queue. Since the SYN ACK is destined for an incorrect or non-existent host, the last part of the "three-way handshake" is never completed and the entry remains in the connection queue until a timer expires, typically for about one minute. By generating phony TCP SYN packets from random IP addresses at a rapid rate, it is possible to fill up the connection queue and deny TCP services to legitimate users.

There is no easy way to trace the originator of the attack because the IP address of the source is phony.

The external manifestations of the problem include inability to get mail, inability to attach to WWW services, or a large number of TCP connections on your host in the state SYN_RCVD."[5]

[5] Drew, Dale. "Potential Denial of Service Attacks at Internet Service Providers (ISPs)", Available online: [http://www.security.mci.net], September 1996.

4.3.2 Port Flooding [http://www.ilf.net/Toast/files/cool/owdport.zip]

Port flooding is another denial of service attack that floods open ports on a target system with connection requests significantly slowing the system down and preventing legitimate users from accessing the target system.

4.3.2.1 Pnewq

Port bombing tool for Windows 95/NT. Floods the target machine with requests for connections through a graphical user interface. As described by the author "This is, by far, the most elite port-bombing tool currently available to Windows 95/NT users. It is, arguably better than currently available Linux/Unix programs of its type. After simply entering the server and port, it attempts to connect with as many local sockets as you wish (from 1 to 1000), flooding the other side with connections. It only works on listening ports (what is the point otherwise?) and you can use PortPro to investigate what ports are available for 'PNewqing'."

4.3.3 Mail Bombers [http://www.ilf.net/wilter/ehack/email/email/mail.html][6]

Mail bombers are used for harassment and denial of service attacks. In their simplest form the sent a large quantity of email messages to a particular address. Some of the more complex programs make this process harder to trace and correct by inserting random headers and using multiple source addresses and even subscribe the target address to mailing lists in order to create a continuos stream of email that is very labor intensive to correct. All mail bombers listed in section 4.3.3 are available at the above website.

4.3.3.1 UpYours

Mail bomb program for the Windows 95 operating system. Floods target mail server with thousands of email messages that are untraceable. Also creates random subject lines and return addresses to prevent defensive filtering mechanisms. Also has the capability to subscribe target addresses to Internet mailing lists, similar to the attack method used against the White House and other Internet users (Time Warner, Rush Limbaugh, etc.) in the Unamailer attacks of 1995-96.

4.3.3.2 Avalanche

Another Windows 95 based email bomber similar to UpYours.

4.3.3.3 Kaboom

Windows 3.X/95 based email bomber. Very difficult to obtain copies since the author does not want it distributed to the Internet masses.

---

[6] Note: this site is very dynamic with regards to which directory the programs are in.

4.3.3.4 Other Mail Bombers

Homicide (Win 95), Unabomber (Win 3.X/95), Extreme Mail (Win 95), Shocker (Win 95), AOLSD (Win 3X/95 and AOL account), BomdTrack (Mac), FlameThrower (Mac), Vodoo (Unix).

4.4 Network Monitoring Utilities [http://www.morehouse.org/hin/filez.htm#SNIFF]

Network monitoring utilities are used to gather information such as passwords that are transmitted during remote access sessions. Non-network monitoring utilities might capture keystrokes at the target computer or offer "false" log on screens to capture data.

Security expert Dorothy Denning describes the sniffer concept: "Sniffer programs, installed on network nodes, intercept packets traversing the network and ferret out login IDs and passwords, credit card numbers, or messages containing certain keywords. This information is stored in a file, where it can be read by or transmitted back to the owner of the program."[7]

4.5 IP Spoofing or Deception Utilities

[ftp://ftp.infonexus.com/pub/Philes/NetTech/TCP-IP/IPspoof-route.txt.gz][8]
[http://www.tacd.com/papers/seqnumsrc.c]

As described by computer security expert Dorothy Denning, "this involves forging the Internet Protocol (IP) address of a trusted host in order to establish a connection with a victim machine. One method floods the trusted host with connection requests and then, while the host is recovering, sends packets that forge the node's IP address. The forged packets may contain data that allow the attacker to gain privileged access on the victim machine."[9]

A process requiring significant technical expertise, very few utilities exist on the Internet for these sorts of attacks, however, they are available as evident by the above WWW link which provides source code demonstrating this sort of attack.

4.6 Supplemental Utilities

Hackers also utilize several supplemental utilities. These include programs that map out network connections, crack password files or generate credit card numbers. A brief outline of the sorts of tools available is provided below.

---

[7] Denning, Dorothy. "Protection and Defense of Intrusion", March 5, 1996. Available online: [http://guru.cosc.georgetown.edu/~denning/infosec/USAFA.html]

[8] This link is to a white paper on IP spoofing written by a hacker called Daemon9.

[9] Denning, Dorothy. "Protection and Defense of Intrusion", March 5, 1996. Available online: [http://guru.cosc.georgetown.edu/~denning/infosec/USAFA.html]

4.6.1 **Toneloc** [http://www.morehouse.org/hin/dialers/tl110.zip]

A wardialing program used by hackers to seek out numbers in a certain exchange or area code that answer with a computer. This program dials a range of numbers and records which lines have a computer attached for later exploration by a hacker. A map of a whole exchange can be created identifying which numbers respond with a voice, data line, fax line or are currently disconnected. This program is completely automated and can be started and left to run until the entire sweep area has been covered. As a footnote, the author of this program is currently in jail.

4.6.2 **CRACK** [ftp://coast.cs.purdue.edu/pub/tools/unix/crack/]

Crack is a password guessing program that is designed to quickly locate insecurities in Unix (or other) password files by scanning the contents of a password file, looking for users who have misguidedly chosen a weak login password.

4.6.3 **IP Scanner** [http://www.morehouse.org/hin/zip/ip_scan.zip]

Scans networks for valid IP addresses to map out the network connections or active machines on a specific network or subnetwork.

4.6.4 **AOHELL** [http://www.ilf.net/Toast/files/AOL/aoh96b3.zip]

AOHELL is a hacking program designed for disruption and fraud on the commercial Internet service provider America Online.

4.6.5 **Log Cleaners** [http://www.tacd.com/exploit/log/]

Log cleaners are used to remove system log entries that may indicate a hacker's activity on a particular system.

4.6.6 **Credit Master** [http://www.ilf.net/Toast/files/CC/cmaster2.zip]

Used to generate credit card numbers based on bank codes and number generation algorithms to ensure the production of a valid card number that either has been or could be issued. Similar programs exist for calling card number generation.

5.0 HACKING TRENDS

In the past, hacker tools and discussions were focused on two areas: access and fraud. The main objective of many hacker efforts was to gain access to a forbidden network or system. To obtain this objective, fraudulent activities such as gaining free access to the phone network were also initiated by the hacker community. Recent events, pointed out in Section 3.1 above, however, indicate a disturbing trend towards destruction, disruption and protest.

6.0 REFERENCE

6.1 Selected WWW Sites

The World Wide Web has become the fastest growing Internet communications protocol on the Internet. Therefore, it is not surprising that hackers have utilized this medium for the sharing of information. The following are selected starting points for exploring hackers on the WWW.

6.1.1 **2600 Magazine** [http://www.2600.com]

Having existed for over 12 years, this quarterly hacker magazine is one of the most visible hacker organizations. Hackers meet under the 2600 flag in over 30 cities worldwide the first Friday of the month to exchange information and share ideas. Emmanuel Goldstein, the editor and publisher of 2600, also maintains a media profile by appearing in many hacker documentaries and news items, hosting a radio show in New York city, and vocally protesting the incarceration of hackers across the US. The website offers information about the magazine, meeting locations, archives of hacked www sites (CIA, DoJ, etc.), and also maintains an extensive Secret Service file to protest the Secret Services involvement in hacker investigations.

6.1.2 **Phrack Magazine** [http://www.fc.net:80/phrack/]

Hacker magazine electronically distributed at random intervals. Often contains technical hacking guides including source code for exploit scripts. The magazine gained notoriety in the 1980s when charges were brought against the publisher for distributing documentation about the 911 system. The case was dismissed when evidence regarding the public availability of the 911 document was introduced by the defense.

6.1.3 **The L0pht** [http://www.L0pht.com]

The L0pht is a physical hacker hangout housed in a Boston-area rented studio. Local hackers meet there to hangout and explore technology. The L0pht crew and their associated hacker group the Cult of the Dead Cow often sponsor hacker conferences. The site offers information about hacking as well as hardware for sale (for $80 they will sell you a pager decoder that you plug into a PC and a scanner to intercept nationwide and local pages) and a listing of current projects.

6.1.4 **The Hacker Defense Fund** [http://www.hackerz.org]

The Hacker Defense Fund coordinates legal representation for hacker cases. The premise being that new lawyers may take a high profile hacker case for free of reduced fees just to get the exposure and experience.

6.1.5 **The Underground** [http://underground.org]

Extensive site that compiles computer security related information from the hacker community and the corporate world.

6.1.6 Chaos Computer Club [http://www.ccc.de/]

Website for the German-based Chaos Computer Club.

6.1.7 Hacker Information Network [http://morehouse.org/hin/hindex.htm]

Comprehensive site with an extensive online archive of hacking programs, tools and utilities.

6.1.8 Information Liberation Front [http://www.ilf.net/]

The name of the site is a play on the "Internet Liberation Front" hacking group responsible for computer attacks on various corporations and individuals. This site provides extensive links to the hacker community and houses the home pages of several hacking groups. The site claims to be dedicated to the following two notions: "1. Security through Obscurity is not effective and; 2. Information needs to be liberated."

6.1.9 CyberToast's Underground [http://www.ilf.net/Toast/]

Extensive hacking related site housed on the Information Liberation Front server.

6.1.10 The Ping O' Death Page [http://www.sophist.demon.co.uk/ping/]

Page dedicated to identifying vulnerabilities that allow for the remote disruption of various computer platforms using the Internet Ping command. Detailed descriptions of this vulnerability categorized by operating systems with available fixes or patches listed.

6.1.11 Daemon9 Project Page [http://www.slip.net/~daemon9/project.html]

This page outlines the current and past hacking projects of Daemon9 and his friends. Since, Daemon9 is also an editor of Phrack magazine, this page provides a good indication of future Internet hacking trends.

6.1.12 The New Hacker's Dictionary [http://www.ccil.org/jargon/jargon_toc.html]

Comprehensive listing of hacker terms, slang, and writing style with historical and current examples.

6.1.13 Infowar.com [http://www.infowar.com]

Information warfare and information security site contains hacker discussion and file areas and also features hacker IRC meetings once per week. These meetings are well attended by the hacker community.

6.1.14 X Underground [http://www.cdc.net/~x/main.html]

Contains and extensive exploit library and a photo gallery from hacker cons as well as links to other sites.

6.1.15 The Hacker/2600 FAQ [http://www-personal.engin.umich.edu/~jgotts/hack-faq/]

The frequently asked questions (FAQ) provides a comprehensive overview of hacking. The FAQs are compiled to allow new users to look for answers without disrupting the communications mechanism (mailing list, Usenet news, etc.) with previously discussed questions or topics.

6.1.16 Web Rings

The online world of hacking is very dynamic and following current activities requires much effort. It is not uncommon for site locations to change monthly, weekly or even daily. New technology on the web allows for the creation of webrings in which sites are linked together to form a continuous subject-matter or interest-area loop. Hackers have used this technology to establish hacking rings that allow a surfer to move smoothly from one site to the next. Some rings are tightly controlled and restrict membership, but some are open to all. A few of the more popular and well established hacker webrings are listed below.

6.1.16.1 Fringe of the Web [http://main.succeed.net/~bbuster/webring/]

One of the most popular hacker webrings. As described in the ring introduction: "Welcome to the Fringe of the Web.....The Fringe is a "ring" of pages all over the net, if you were to follow this "ring", and jump from site to site, you would eventually come back to this site. The Fringe of the Web was made in June of 1996, in an effort to join pages that are on the Fringe, pages that deal with topics that the Government and other people would just like to sweep under the carpet. This ring gives it members quick access to other resources on the ring plus the safety of knowing that they are in the largest hacking group on the web today; after all there is safety in numbers. All the pages on the ring deal "Directly" with Hacking, Phreaking, Virus [sic] production and use, Warez, Privacy, Encryption, alternate E-mail uses/resources and IRC hacks."

6.1.16.2 The Inner Ring [http://www.ilf.net/warez/join.html]

Boasts being the largest hacker webring on the Internet with over 350 active pages linked together to form a non-exclusive ring.

6.1.16.3 The Ruiner's Webring [http://members.tripod.com/~Ruiners/index.html]

Another active hacker webring.

6.1.16.4 Digital Anarchy [http://rampages.onramp.net/~piranha/digital.html]

Another active hacker webring.

6.2 Related Books

The following books are on or about the hacker community.

BloomBecker, Buck. *Spectacular Computer Crimes: What They Are and How They Cost American Business Half a Billion Dollars a Year*. Illinois: Dow Jones- Irwin, 1990.

Clough, Bryan & Mungo, Paul. *Approaching Zero: The Extra-ordinary Underworld of Hackers, Phreakers, Virus Writers & Keyboard Criminals*. New York: Random House, 1992.

Denning, Peter J. *Computers Under Attack: Intruders, Worms and Viruses*. New York: ACM Press, 1991.

Forester, Tom & Morrison, Perry. *Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing*. Cambridge: The MIT Press, 1994.

Hafner, Katie & Markoff, John. *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. New York: Simon & Schuster, 1991.

Kroker, Arthur & Weinstein Michael A. *Data Trash: The Theory of the Virtual Class*. New York: St. Martin's Press, 1994.

Landreth, Bill. *Out of the Inner Circle*. Microsoft Press. Bellevue, WA. 1985.

Levy, Steven. *Hackers: Heroes of the Computer Revolution*. New York: Dell Publishing, 1984.

Littman, Jonathan. *The Watchman: The Twisted Life and Crimes of Serial Hacker Kevin Poulsen*, Little, Brown and Company, 1997.

Littman, Jonathon. *The Fugitive Game: Online with Kevin Mitnick.* Little, Brown and Company, 1996.

Ludwig, Marc. *The Little Black Book of Computer Viruses*. American Eagle Publications, 1990.

Parker, Donn B. *Crime by Computer*. New York: Charles Scribner's Sons, 1976.

Quittner, Joshua & Slatalla, Michelle. *Masters of Deception: The Gang That Ruled Cyberspace*. New York: HarperCollins, 1995.

Rheingold, Howard. *The Virtual Community: Homesteading on the Electronic Frontier*. New York: Addison-Wesley Publishing Company, 1993.

Rushkoff, Douglas. *Cyberia: Life in the Trenches of Hyperspace*. New York: HarperCollins, 1994.

Schwartau, Winn. *Information Warfare: Chaos on the Electronic Superhighway*. New York: Thunder's Mouth Press, 1994.

Sterling, Bruce. *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. New York: Bantam Books, 1992.

Stoll, Clifford. *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*. New York: Doubleday, 1989.

The Knightmare. *Secrets of a Super Hacker*. Washington, Loompanics Unlimited, 1994.

Van Duyn, J. *The Human Factor in Computer Crime*. Princeton: Petrocelli Books, 1985.

6.3 Magazines

There are several print magazines, either produced by hackers, or of interest to them. A sampling of these magazines is provided below.

6.3.1 2600: The Hacker Quarterly [http://www.2600.com]

One of the most popular hacker magazines in print, 2600 has a distribution of 40,000. Also sponsors monthly hacker meetings worldwide and various conferences.

6.3.2 Blacklisted 411

Newly created hacker magazine similar to 2600.

6.3.3 Gray Areas [http://w3.gti.net/grayarea/]

Magazine focused on societal "gray areas" often covers hacker events and stories. This magazine "scooped" the Internet Liberation Front story by obtaining the first and only interview with a member of the group. It was later discovered that the member of the group was living with the editor of the magazine.

6.3.4 Mondo 2000

Glossy cyberpunk culture magazine with a hacker following.

6.3.5 Wired Magazine [http://www.wired.com]

Has written many articles on hackers, crackers and warez dudes in the past four years. Often dispatches correspondents to hacker conferences.

6.3.6 Internet Underground [http://www.underground-online.com]

Limited coverage of the hacker community can be found in this magazine.

6.4 Videos/Movies

6.4.1 Unauthorized Access [http://chat.bianca.com/bump/ua/]

A film by Annaliza Savage. As described by the producer: "Unauthorized Access" is an insiders view of the computer cracker underground. The filming took place all across the United States, Holland and Germany. "Unauthorized Access" looks at the personalities behind the computers screens and aims to separate the media hype of the 'outlaw hacker' from the reality."

6.4.2 Hackers 95 [http://www.rockpile.com/security/hacker.htm]

Another hacker documentary filmed from the hacker perspective. Covers several hacker conferences and features interviews with elite hackers.

6.4.3 Dutch Hacker Video

Home video depicting a successful Dutch hacker attack on a random military system. This video was used for some hacking exposes in the US media and is available for sale through 2600 Magazine.

6.4.4 Hacker Culture Movies

The following movies are often identified by the hacker community as cultural films. Some are even identified as inspiration for hacking aspirations.

Wargames
Blade Runner
Hackers
Sneakers
The Net

7.0 CONCLUSION

This document provides no formal conclusions regarding the hacker community or its potential threat to US critical infrastructures. It provides background information and potential points of exploration to learn more about this unique and diverse subculture and to provide insights regarding their capabilities and knowledge.