



TECHNOBABBLE

The DCIS Cyber Crime Newsletter



TECHNOBABBLE
Volume 2, Issue 1

January, 2001

This issues suggested computer crime bookmarks:

Geek.com Online Technology Resource:

<http://www.geek.com>

Security Focus Internet Security Site :

<http://www.securityfocus.com>

The Screen Saver's Technical Assistance Page:

<http://www.thescreensavers.com>

Inside this issue:

Boston Man Sentenced for Hacking. 1

Federal Court Rules on Port Scans. 1

Suggested SysAdmin Response to Computer Intrusion. 2

Suggested Reading: "TCP/IP Clearly Explained." 3

This Issue's Useful Definition - RAID. 4

Juvenile Sentenced for Compromising Web Sites. 5

23 Year Old Pleads Guilty to Stock Scheme. 5

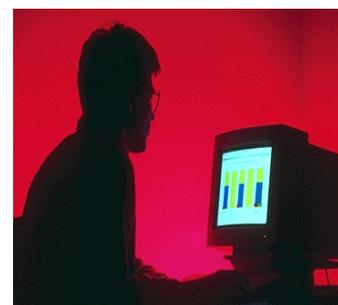
Boston Man Sentenced for Hacking

On November 17, 2000, Ikenna Iffih of Boston, MA appeared before U.S. District Court Judge Robert E. Keeton, District of Massachusetts, and was sentenced to 2 years probation, with the first six months of his probation being house detention. Iffih was also ordered to pay \$5,000 in restitution to Zebra Marketing Online Services and to forfeit all computer equipment used to obtain unauthorized access to United States Government computers, which included NASA and U.S. Department of Defense systems. The judge further banned Iffih from using computers for any other purpose than work or school.

The sentencing arose from a previous plea of guilty by Iffih to a three-count criminal information charging him with the illegal interception and possession of electronic communications transmitted to and through a United States Government computer; the illegal and intentional access and damage of a computer used in interstate and foreign commerce; and the willful and malicious interference of a working communications system operated and controlled by the United States Government.

The investigation was conducted by special agents of the Defense Criminal Investi-

gative Service; NASA's Office of Inspector General, Computer Crime Division; the Federal Bureau of Investigation; the U.S. Department of the Interior's Office of Inspector General; and the Immigration and Naturalization Service.



Federal Court Rules on Port Scans

A recent U.S. district court ruling in Georgia concluded that port scanning a network does not damage it, and dismissed an IT contractor's attempt to sue a competitor for damages resulting from a need to assess the potential impact of scans.

In his opinion, Judge Thomas Thrash stated that the value of time spent investigating a port scan can not be considered damage. "The statute clearly states that the damage must be an impairment to the integrity and availability of the net-

work," wrote the judge, who found that a port scan impaired neither.

"It says you can't create your own damages by investigating something that would not otherwise be a crime," says hacker defense attorney Jennifer Granick. "It's a good decision for computer security researchers."

A port scan is a remote probe of the services a computer is running. While it can be a precursor to an intrusion attempt, it does not in itself

allow access to a remote system. Port-scanning programs are found in the virtual tool chests of both Internet outlaws and cyber security professionals.

Some industry officials feel that the decision may, in actuality, be beneficial to law enforcement in that it could help define statutes' civil boundaries at a time when more companies are eyeing lawsuits against computer intruders as an alternative to relying on government prosecution.

Suggested System Administrator Response to Computer Intrusions

Systems Administrators (Sysadmins) have overall responsibility for the functioning of computer networks, including assuring day to day network operations run smoothly and efficiently. While some organizations employ a separate Systems Security Administrator, many sysadmins are responsible for addressing misuse of their networks, including acting as a first responder to potential system compromises. Unfortunately, many sysadmins receive little if any training in appropriate responses to suspected computer intrusions. The following are some suggestions as to how to properly respond when a potential compromise is discovered.

1) Notify law enforcement, and the appropriate Computer Emergency Response Team (CERT) as soon as possible (i.e. CERT coordination center at Carnegie Melon, Department of Defense CERT, etc). CERT teams conduct detailed analysis of attack patterns, and may have valuable information relative to methods utilized in attacking your system. Likewise, law enforcement officers specifically trained in computer crime response will be able to provide invaluable assistance, including instructions relative to preserving potential evidence of an attack.

2) In some cases, law enforcement may request that you do not turn the system off. In other cases, officers may suggest you unplug the system from the network and prepare to make a full

system backup. A third approach may involve law enforcement officers responding to your location in order to create a duplicate image of the system for purposes of evidence preservation. Work closely with these individuals in order to increase the probability of prosecution once an offender is identified.

3) Locate and secure removable media containing the most recent complete back-up of the impacted system's hard drive, made before the intrusion (this also contains valuable evidence).

4) Start taking notes -

- What did the attacker do? (gained root access, denial of services, theft of services, theft of data, established unauthorized account, changed passwords, installed sniffer, removed password file, etc.)
- When was the attack discovered?
- How was the attack discovered?
- When did the attack occur?
- What actions were taken in response to the attack?
- Is the system off-line?
- Did any suspicious activities precede the attack (scan, system failure, etc)?
- Has the system been attacked before?

- Was any data copied or removed from the system?
- Were any files placed on the system? (If so, what are the file names and location on the server?)
- Are there system files/logs documenting the activities of the attacker? (If so, law enforcement may request that you copy the files to removable media, and secure the media for collection as evidence.)
- Any known suspects?

5) Keep detailed information relative to financial damages incurred as a result of the attack. This is crucial to prosecutors who will have to make a determination as to how to proceed once the offender has been identified. Don't forget to include the amount of productivity time lost due to attack, and the amount of time required to patch and re-establish the system.

6) Law enforcement officers will undoubtedly have many questions relative to the incident. Expect to be asked:

- Brand name, model number, serial number, physical location, domain name, and IP address of the impacted computer(s).
- User IDs and accounts exploited by attacker.
- MAC addresses of network cards.



“Unfortunately, many sysadmins receive little if any training in appropriate responses to suspected computer intrusions.”

- Operating system name and version on the server. Most recent updates?
- Is there a warning banner on the system?
- What is the purpose of the system (DNS server, web server, data processor, etc.)?
- How many clients and other servers are networked to the server?
- Who has root/administrator access (authorized) to the server?
- When were the passwords last changed?



In dealing with potential system compromises, remember... **its all about teamwork!** System Administrators are trained computer networking experts that know their systems better than anyone. Likewise, computer crime investigators are trained in specific methods, laws, and policies which relate to computer crime and preservation of computer evidence that could be crucial to successful prosecution of a system compromise. When sysadmins and computer crime investigators work together in a cooperative atmosphere, the chances of successfully pursuing a perpetrator, and holding them accountable for their actions increases dramatically!

Useful contact Information

Carnegie Mellon
Institute's
CERT Coordination
Center

www.cert.org
E-mail: cert@cert.org

Hotline: 412-268-7090
Fax: 412-268-6989

U.S. Department Of Defense CERT

www.cert.mil
E-mail: cert@cert.mil

Phone: 800-357-4231
Fax: 703-607-4009

This Issues Suggested Reading

TCP/IP Clearly Explained

This issues suggested reading is "TCP/IP Clearly Explained," by Pete Loshin.

In order to enable computers of varying types to communicate, the Internet utilizes a suite of protocols known collectively as Transmission Control Protocol / Internet Protocol, or "TCP/IP." Without TCP/IP the Internet would cease to exist, since different operating systems such as Unix, Windows, and Mac OS would be unable to "speak each others' language."

Once a computer crime investigator learns the basics of Internet based investigations, he or

she will undoubtedly develop a desire to dig deeper into the inner workings of the net. TCP/IP Clearly Explained provides the means to do so. The book starts out with basic networking concepts, and progresses into more complex topics, such as Internet Commerce, and Internetwork Implementation and Management.

A recent customer review from Amazon.com sums the book up nicely when it states that, "there are lots of books available about TCP/IP. Some are filled with great technical information, but are difficult to follow, because of the realm of information. Others are easier to read, but lack some important details. This book strikes a happy me-

dium: full of excellent information, but still written in a style that's easy to follow and understand."

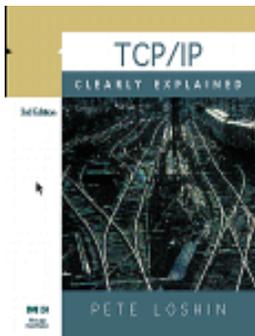
Whether a newcomer to the world of Internet investigations, or an accomplished veteran, TCP/IP Clearly Explained is sure to prove a valuable tool in the war on cybercrime.

Title:
TCP/IP Clearly Explained

Authors:
Pete Loshin

Cost: **\$44.95**

ISBN: **0-12-455826-7**



This Issue's Useful Definition

RAID (Redundant Array of Independent Disks)

RAID (Redundant Array of Independent Disks) is an acronym first used in a 1988 paper by Berkeley researchers Patterson, Gibson, and Katz. It described array configuration and applications for multiple inexpensive hard disks, providing fault tolerance (redundancy) and improved access rates.

The most vulnerable part of a computer system is the hard disk, since it's the only mechanical, moving part in an otherwise electronic assembly. Data written to a single drive is only as reliable as that disk, and the question is not whether a drive will fail, but rather when it will fail.

RAID provides a method of accessing multiple individual disks as if the array were one larger disk (SLED, or single large expensive disk), spreading data access out over these multiple disks, thereby reducing the risk of losing all data if one drive fails, and improving access time.

Why is RAID Important to Investigators?

Historically, RAID was only used by major corporations utilizing extremely large file servers, transaction or application servers where data accessibility was absolutely critical, or in situations where fault tolerance was required. Today, RAID is also being used in desktop systems for CAD, multimedia editing and playback, or any application where higher transfer rates and increased storage capacity are desirable. With the recent decrease in hard disk

drive cost (at time of publication, a 30 gigabyte hard disk can be purchased for under \$130), investigators are sure to encounter RAID setups when conducting investigations of systems ranging from a corporate network, to a single desktop stand-alone.

What are the standard RAID types and what are their advantages and disadvantages?

RAID 0: Also known as 'striping', this is technically not a RAID level since it provides no fault tolerance. Data is written in blocks across multiple drives, so one drive can be writing (or reading) a block while the next is seeking the next block. The system will view a type 0 array as a single, super capacity hard disk. The advantages of striping are the higher access rate, and full utilization of the array capacity. The disadvantage is there is no fault tolerance - if one drive fails, the entire contents of the array become inaccessible.

RAID 1: Mirroring provides redundancy by writing twice - once to each drive. If one drive fails, the other contains an exact duplicate of the data and the controller can switch to using the mirror drive with no lapse in user accessibility. The disadvantages of mirroring are no improvement in data access speed, and higher cost, since twice the number of drives is required (50% capacity utilization).

RAID 3: RAID level 3 stripes data across multiple drives, with an additional drive dedicated to parity, for error correction/

recovery. RAID 3 is not found on all controllers.

RAID 5: RAID level 5 is the most popular configuration, providing striping as well as parity for error recovery. In RAID 5, the parity block is distributed among the drives of the array, giving a more balanced access load across the drives. The parity information is used to recover the data if one drive fails, and is the main reason this method is the most popular. The disadvantage is a relatively slow write cycle (2 reads and 2 writes are required for each block written). The array capacity is N-1, with a minimum of 3 drives required.

RAID 0+1: This is striping and mirroring combined, without parity. The advantages are faster data access (like RAID 0), and single-drive fault tolerance (like RAID 1). RAID 0+1 still requires twice the number of disks (like RAID 1).

JBOD: JBOD stands for "Just a Bunch of Disks". Each drive is accessed as if it were on a standard SCSI host bus adapter. This is useful when a single drive configuration is needed, but offers no speed improvement or fault tolerance.

To learn more about RAID setups, check out the following links:

http://www.computerworld.com/cwi/story/0,1199,NAV47-81_STO45211,00.html

<http://www.ecs.umass.edu/ece/koren/architecture/Raid/basicRAID.html>

"RAID provides a method of accessing multiple individual disks as if the array were one larger disk, spreading data access out over these multiple disks, thereby reducing the risk of losing all data if one drive fails, and improving access time."

Standard RAID Types	
0	Striping - data written in blocks across drives.
1	Mirroring - Data written twice—once to each drive.
3	Striping, with an additional drive for parity.
5	Striping, with a parity block distributed among drives.
0+1	Striping & Mirroring (no parity)
JBOD	Each drive accessed separately

Juvenile Sentenced for Compromising Web Sites

On November 20, 2000, a 17 year old juvenile residing in Colorado Springs, Colorado, pled guilty to one count of a state computer crime statute (Colorado Title 18, Article 5.5, Section 102), and was sentenced to 2 years probation. The judge also ordered the juvenile to pay restitution to his victims in the amount of \$24,000.

In his plea, the 17 year old admitted to compromising and

defacing numerous Internet web sites, including U.S. Department of Defense web sites, and NASA sites at the Johnson Space Center, Houston, TX, and the Goddard Space Flight Center, Greenbelt, MD.

Over 40 web sites were defaced, including web servers maintained by the U.S. Department of the Interior, U.S. Department of Transportation and several state, local, commercial, and

educational sites.

The investigation was conducted by the Defense Criminal Investigative Service, NASA's Office of Inspector General, Computer Crime Division; the Federal Bureau of Investigation; the Colorado Springs Police Department; and the Texas Department of Public Safety. The El Paso County Office of the District Attorney, handled the prosecution.



23 Year Old Pleads Guilty to Stock Scheme

A 23-year-old college student, pleaded guilty to manipulating the stock of Emulex. The charges carry a potential sentence of up to four years in prison.

Mark Simeon Jakob admitted to orchestrating a scheme in an attempt to stave off \$97,000 in losses from selling Emulex stock short.

Jakob sent a false press release designed to topple Emulex's share price--netted him more than \$241,000 in profits while costing investors \$110 million.

His actions caused the stock price of Emulex to fall by 62 percent- about \$2.5 billion-from \$110 per share to \$42. Jakob faces 46 months in prison when he is sentenced by U.S. District Judge Dickran Tevrizian in March and could be ordered to pay huge fines as well as restitution.

As part of his guilty plea, Jakob surrendered \$54,000 to the FBI in cash from his bank account

that represented part of his profits.

Prosecutors said that the case should serve as a lesson about the ease of stock manipulation in the Internet age.

Jakob engineered his scheme by sending a false press release about Costa Mesa, Calif.-based Emulex, a data networking equipment company, to news dissemination service Internet Wire Inc., where he worked at the time. The release alleged that Emulex was under investigation by the Securities and Exchange Commission and would have to restate its earnings.

Internet Wire filed the release, and it was picked up by several major financial news services, including Bloomberg and Dow Jones.

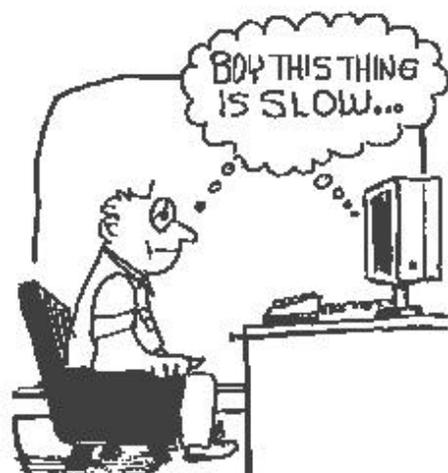
"We hope this will be a lesson to everyone who distributes the news," Assistant U.S. Attorney Carl Moor said outside court. "This is the first crime where someone really took advantage

of the legitimate news media and in that sense it was a spectacular case."

Until recently Jakob was a student at El Camino College near Los Angeles, where the computer used to send the bogus press release was located.

After discovering that the Emulex press release was false, Nasdaq officials halted trading in the stock. Trading was reopened later in the day after Emulex was able to publicize the fact that it was the victim of a bogus press release.

"This is the first crime where someone really took advantage of the legitimate news media and in that sense it was a spectacular case."



*A publication of the DCIS
Northeast Field Office*

Defense Criminal Investigative Service
Northeast Field Office
10 Industrial Highway, Bldg. G, Mail Stop 75
Lester, PA 19113

Phone: (610) 595-1900
Fax: (610) 595-1934

Send comments to: lives@dodig.osd.mil

We're on the Web!

www.dodig.osd.mil/dcis/dcismain.html



The Defense Criminal Investigative Service

"Protecting America's War Fighters"

The Defense Criminal Investigative Service is the investigative arm of the U.S. Department of Defense, Office of the Inspector General. As such, DCIS investigates criminal, civil, and administrative violations impacting the Defense Department. Typically, DCIS investigations focus upon computer crime involving U.S. military and civilian DoD systems, contract procurement fraud, bribery and corruption, health care fraud, anti-trust investigations, export enforcement violations, environmental violations, and other issues that impact the integrity and effectiveness of the U.S. Department of Defense.

If you encounter issues that impact the U.S. Department of Defense, please call the DCIS office within your region.

DCIS Northeast Field Office.

10 Industrial Hwy., Bldg. G
Lester, PA 19113
Phone: (610) 595-1900
Fax: (610) 595-1934

DCIS Boston Resident Agency

Rm. 327, 495 Summer Street
Boston, MA 02210
Phone: (617) 753-3044
Fax: (617) 753-4284

DCIS Hartford Resident Agency

525 Brook Street, Suite 205
Rocky Hill, CT 06067
Phone: (860) 721-7751
Fax: (860) 721-6327

DCIS New Jersey Resident Agency

Wick Plaza 1, 100 Dey Pl., Ste. 102
Edison, NJ 08817
Phone: (732) 819-8455
Fax: (732) 819-9430

DCIS New York Resident Agency

One Huntington Quad, Suite 2C01
Melville, NY 11747
Phone: (516) 420-4302
Fax: (516) 420-4316

DCIS Pittsburgh Post of Duty

1000 Liberty Ave., Ste. 1310
Pittsburgh, PA 15222
Phone: (412) 395-6931
Fax: (412) 395-4557

DCIS Syracuse Resident Agency

441 S. Selina St., Ste. 304
Syracuse, NY 13202
Phone: (315) 423-5019
Fax: (315) 423-5099