Global Information Assurance Certification Paper

Good News, Bad News: The Infosec Issues of Usenet

Bob Long

May 22, 2001

Submitted for GSEC Practical Assignment version 1.2d

Introduction

To the majority of today's users, the Internet mostly means Web browsing and searching, E-mail, online transactions, games, and various flavors of chat. Only seasoned Internet veterans, or the more curious, stubborn and/or technically inclined newer users, will likely bother with Usenet, AKA Network News (or sometimes just News). Compared to its brethren, the face of Usenet isn't very pretty or user-friendly: no graphics, no flash, and no streaming media. Usenet demands some effort to figure out what it's for and how to use it: more than just an intuitive point and a click. Members of the academic community have been utilizing Usenet for many years (even before the invention of the Internet), and are likely well aware of its benefits and risks. For them, much of the information here will be "old News". For those of us from the private sector, and others who are relative newcomers, some introductory information on Usenet may be helpful. (1)

First, a brief history review: Usenet was developed in 1979 by Tom Truscott and Jim Ellis, and based on the UNIX UUCP protocol. (2) Its original purpose was to allow messages to be shared among groups of UNIX system users. Over time these discussion groups, now more commonly

referred to as newsgroups, became increasingly wider in audience and subject material. In these early years of Usenet software development by a number of talented people resulted in three major releases of Usenet server software, referred to as News A, News B, and News C. During this period, Usenet was largely confined to University and ARPANET use.

As the Internet developed and Usenet usage grew, the UUCP protocol was found to have some shortcomings for supporting the Usenet service. UUCP was subsequently augmented by, and eventually mostly displaced by, the NNTP service of the TCP protocol. NNTP was defined in RFC 977 in 1986, and is assigned to TCP port 119. (3) The first version of today's de facto standard for News server software, called InterNetNews or INN, was written by Rich Salz and released in 1992. INN is Open Source software, and is maintained by the Internet Software Consortium. (4) To put some historical perspective on all of this, the World Wide Web service was not introduced until 1991, twelve years after Usenet and five years after NNTP. (5)

The Good News

Usenet continues to be a significant presence on the Internet. Estimates place the total number of Internet newsgroups somewhere over 50,000. (6, 7) A typical Internet News server carries thousands of active newsgroups. Of two commercial Internet provider news servers I recently sampled, one provided nearly 33,000 and the other over 36,000 groups.

The "good News" is that this service continues to provide a large number of useful forums for information and problem sharing on a variety of academic, computing-related, and other

constructive topics. Some active examples in the Infosec (Information Security) subject area are comp.security.firewalls, comp.os.linux.security, comp.security.unix, and microsoft.public.win2000.security. Although web-based alternatives have recently proliferated, newsgroup forums are still often the best, and sometimes the only, way to find help with some of the personal and professional challenges people face.

Even though Usenet is not as popular as E-mail or the Web, support for Usenet technology is ubiquitous. The newsreader software required to access Usenet is bundled with popular E-mail packages and/or Web browsers, for example Microsoft Outlook Express/Internet Explorer, and Netscape Communicator. There are also a large number of commercial and freeware dedicated newsreader packages available for every computer platform. Virtually every significant Internet provider has one or more News servers. Apparently, there must be more than just a handful of academics and technical types using this service to justify all this, and that is where some of the "bad News" comes in.

The Bad News

If Usenet were a text-only service, it probably would have been relegated to obscurity some time ago. However, Usenet messages (AKA articles) also support large binary attachments. Coupled with a libertarian Usenet culture regarding what constitutes an acceptable newsgroup, availability of "anonymous" access (termed "lurking"), and lack of a built-in mechanism to facilitate monetary exchange, this has resulted in the free sharing of virtually every kind of electronic

content imaginable. As a result, a significant number of new Usenet users have been attracted to this (in some cases illicit) windfall.

To examine this in more detail, a word about how newsgroups are organized is needed. Newsgroups are organized in a "dotted" hierarchical structure somewhat like DNS, except the notation is "top-down" rather than "bottom-up" reading from left to right. Some of the most notable top newsgroup subject hierarchies are: comp: computing; misc: miscellaneous; news: commercial news feeds; humanities: classics and philosophy; rec: recreation; sci: science; soc: society, culture and genealogy; talk: philosophical, social and political discussions; alt: "alternate" discussions. There are dozens of other top-level subject areas, including designations for various countries. (8) The sub-divisions under the main hierarchies are largely arbitrary, named by those who started the group, however there are some conventions. (9) One lower-level name of particular interest is the label "binaries", which typically denotes that binary attachments are permitted by a particular newsgroup's charter. (10)

Some of the newsgroups under the "alt" (alternate) main subject hierarchy, and also many of the "binaries" groups, give cause for concern. The alt hierarchy is probably the single largest top-level topic. On one server that I sampled, alt newsgroups accounted for over 38% of the total number of groups. Sampling the names of newsgroups available under "alt" on a typical public News server provides a hint of some of the available content. [Table 1]

Please note that I have not reviewed the actual content within these newsgroups in the table. It is possible that some of the groups listed have very legitimate and constructive purposes. For

example, the term "hacker" has an honorable connotation in some programming circles. I apologize to the members of any such newsgroups that are included. However, the names of most of these groups suggest that their content is questionable at best, and may include cracker tools and information, pornography, warez (pirated software), or digitized versions of copyrighted music, movies, or other copyrighted material.

Search on: warez OR crack	Search on: music OR movies AND binaries
alt.2600.warez	alt.binaries.mpeg.video.music
fido7.r46.warez.new	alt.binaries.music.heavy-metal
fido7.xgamwarez.info	alt.binaries.music.jungle
alt.2600.crack	alt.binaries.music.mp3
alt.2600.cracks	alt.binaries.music.oasis
alt.2600.crackz	alt.binaries.music.springsteen
alt.binaries.cracked	alt.binaries.music.steve-vai
alt.binaries.cracks	alt.binaries.music.the-doors
alt.binaries.dominion.cracks	alt.binaries.sounds.music
alt.crackerjack	alt.binaries.sounds.music.rock.metal
alt.crackers	alt.binaries.monster-movies
alt.cracks	alt.binaries.movies
alt.cracks.nl	alt.binaries.movies.divx
alt.new.cracks	alt.binaries.movies.erotica
fido7.crack	alt.binaries.movies.mirage-mrg
fido7.crack.talks	alt.binaries.movies.shadowrealm
fido7.ua.os2.crack	alt.binaries.movies.zeromovies
viwa.crack.and.hack	alt.binaries.sounds.movies
Search on: hack	**Search on: sex AND binaries**
alt.2600.hackers	alt.binaries.erotica.groupsex
alt.2600.hackers.programming	alt.binaries.erotica.sex
alt.2600.hackerz	alt.binaries.sex.erotica.
alt.binaries.hacking.beginner	alt.binaries.multimedia.erotica.strap-on-sex
alt.binaries.hacking.computers	alt.binaries.pictures.bisexuals
alt.binaries.hacking.utilities	alt.binaries.pictures.erotic.groupsex
alt.binaries.hacking.websites	alt.binaries.pictures.erotica.alt.sex
alt.bio.hackers	alt.binaries.pictures.erotica.alt.sex.pictures
alt.hack	alt.binaries.pictures.erotica.groupsex
alt.hacker	alt.binaries.pictures.erotica.sex
alt.hacker.malicious	alt.binaries.pictures.erotica.transexual
alt.hackers	alt.binaries.pictures.erotica.transexual.action
alt.hackers.aol	alt.binaries.pictures.groupsex
alt.hackers.aol.sucks	alt.binaries.pictures.sex
alt.hackers.discuss	alt.binaries.pictures.sex.fetish
alt.hackers.groups	alt.binaries.pictures.sex.fetish.fish
alt.hackers.malicious	alt.binaries.sex
alt.hacking	alt.binaries.sex.pictures.female

Table 1: A sampling of newsgroups in the alt hierarchy, found using various search terms.

Content, Liability, and Policy

The availability of questionable content in newsgroups raises questions of liability and acceptable use for organizations that provide Internet access to their personnel. Details of the legal and financial liabilities will depend on jurisdiction and circumstances, and discussion of them is beyond the scope of this article. Consult your local legal counsel for advice. There are however some policy issues that should be considered.

Many organizations have developed usage policies for Internet Web and E-mail use, and/or monitor or filter access to inappropriate content. However, if these policies are too narrow and concentrate only on Web and E-mail they may fail to address newsgroup access, resulting in a loophole or blind spot. To compound the problem, commercial monitoring, filtering, reporting, and even logging tools are geared primarily toward Web and E-mail content rather than newsgroups. As a result, Usenet can become a covert channel for moving all kinds of information and files in or out of an organization. Inappropriate newsgroup traffic can easily slip through the cracks, if access is unrestricted.

Another risk is that Usenet abuse by users within your organization could result in revocation of either your organization's Usenet privileges, or in extreme cases of your Internet connection. In 1998, and again in early 2000, the @Home network was threatened with "UDP" (Usenet Death Penalty) by the Usenet community, because of excessive spamming activity by @Home users. (11) An additional issue is that excessive use even of acceptable newsgroups may present a productivity problem for your organization's management.

Viruses, Trojans, and Worms

Users of any newsgroup, not just the “alt”, or “binaries” ones, are potential targets for most of the varieties of malicious software, such as viruses, worms and Trojan horse programs, that otherwise are often propagated by E-mail. The first reported instances of several significant viruses have been in newsgroups. The Melissa virus and, more recently, the Anna Kournikova virus, are examples. (12, 13) In these cases, the virus was likely deliberately posted by an individual. However, some malware postings may be the result of an infected system automatically replicating a newsgroup-enabled worm without the system owner’s knowledge. Several viruses and worms propagate in the manner, for example the Happy99 Trojan, the Kak worm, and more recently the Godzilla worm. (14, 15, 16) Although “non-binaries” newsgroups typically do not by charter permit binary attachments, some news servers may not discriminate between groups, and process attachments destined for “non-binaries” groups.

Newsgroups have also been utilized as self-update resources by malware. The Hybris virus plugin, for example, checks a specific newsgroup for upgrades to itself. (17) Another way that crackers employ Usenet to support hacking activity is by posting executables for various backdoor Trojans, such as the SubSeven Trojan, on newsgroups. These are usually disguised as a tempting attachment, for example "SexxxyMovie.mpeg.exe", to trick the unwary into opening them. (18)

The bottom line is that Usenet is a malware transmission vector nearly as effective as E-mail, even if not quite as widely used. Even if a person only uses E-mail, and does not access Usenet, they may still be vulnerable since the newsreader software is often bundled and installed with E-mail or Web browsers. More important, as in the case of content control, centralized virus scanning tools have concentrated on E-mail and web, but not News traffic. As a result, newsgroup access can provide a vulnerable malware entry point in an otherwise well-protected environment.

Privacy and Confidentiality Issues

Earlier in this article I mentioned that newsgroups offered the capability for "anonymous" access, which is referred to as "lurking". The reason for the quotes around "anonymous" is that the anonymity of lurking really only extends to other users of the newsgroup, provided that you do not post (send a message) to the group. Lurker activity, including newsgroups accessed, message downloads, network addresses, and other information, can be logged by the operator of the news server. (19)

If a user posts to a newsgroup, they have just made themselves very public. This can be the case even if they have taken steps to hide their identity, such as a false E-mail address, or even forging message headers. Usenet message headers can be analyzed not only by News server administrators, but also by clever users, and often tracked back to the original poster. (20)

Network News is by nature a very public medium, with largely unrestricted worldwide exposure. Avoid posting confidential information in an Internet newsgroup: you never know who might be "lurking". Also, bear in mind that in posting you are creating a document that may be publicly available for a long time. This is even more the case with News than with E-mail. Google (previously DejaNews) maintains a database of over 650 million newsgroup messages dating back through 1995, and serves them up in searchable web format. (21) As a result, an ill-considered remark could come back to haunt you, or your organization, at some time in the future. Various government agencies have expressed interest in monitoring newsgroups (22), and rumors periodically circulate that some agencies have done so for years. (23)

Usenet Server and Client Vulnerabilities

News servers have had vulnerabilities from time to time, though perhaps less frequently than other, more rapidly evolving Internet services. The most recent CERT advisory related to Usenet dates back to 1997. (24) However, other vulnerabilities, including root exploits, have been posted for various News server packages more recently. One of the more recent vulnerability reports is of a potential buffer overflow in the Debian OS distribution of inn2. (25) Non-UNIX News servers have also reported vulnerabilities, for example buffer overflows in the News server incorporated with Microsoft Exchange 5.0 and 5.5. (26, 27)

Client software vulnerabilities are also a concern. This is partly because newsreaders are integrated with the most popular E-mail and/or browser applications. As a result, they often share, or contribute to, the vulnerabilities of their bundled applications. An example is the well-

publicized susceptibility of Microsoft Outlook (which incorporates a newsreader) to various macro viruses and scripting exploits. Vulnerabilities in Outlook and/or Outlook Express continue to crop up. (28) Microsoft does not have a monopoly on vulnerabilities and other newsreaders have also experienced them, including the Netscape newsreader (29), and most recently the Debian slrn newsreader. (30)

Mitigating the Risks

For many organizations and individuals, Usenet access is not essential. If this is the case, the most effective means of minimizing the associated risk is to eliminate or restrict access. This can be accomplished on a personal or corporate firewall with reasonable effectiveness by blocking TCP port 119, or by turning off any Usenet or Network News proxies. While it is possible to run the Network News service on other ports, it would be unusual for a normal Internet News server to do so. Whether or not blocking NNTP is suitable depends on your organization's policies, or management discretion. Restricting access by controlling the installation of newsreader software can only be effective if workstations are solidly 'locked-down', since various newsreaders are so freely available and easily installed.

If your organization does permit newsgroup access, usage policies should be reviewed to ensure that Usenet access is covered. In order to control and/or monitor access, consider channeling an Internet Usenet newsfeed to end users through a news server operated by your organization, rather than allowing direct access to Internet servers. This can provide the capability to exclude unwanted content, log usage, and possibly to scan incoming content, if required by your policies.

At home, as well as at work, you should ensure that personal computers are kept up-to-date on patches, virus scanning software, and virus signature files. You should of course be doing this anyway, as part your general computer security plan. Users need to be made aware that the same risks apply to news attachments as do to E-mail ones.

On the privacy front, whether at home or at work, exercise discretion in what you post to a newsgroup. Remember that the audience to your words can potentially be the entire world, and that a record of what you say could persist a long time. Also remember that the anonymity of 'lurking' is somewhat of an illusion.

Conclusion

Usenet, AKA Network News, still provides value in some areas, but there are also a number of associated risks. These include inappropriate content, malware and privacy issues, and to a lesser extent occasional server and client vulnerabilities. Availability of commercial monitoring and scanning tools for News access is limited. For many organizations, restricting access may be the most practical way to minimize the risks. If News access is necessary, channeling access through an internal server, and a "Defense in Depth" strategy can be helpful in preventing content and virus problems. As with other information security risks, incorporating Usenet information into user awareness training can also reduce exposure.

References:

1) The Landfield Group. "Lost in Usenet - Usenet References". 1996.

URL: http://www.faqs.org/usenet/index.html

2) Gene Spafford and Mark Moraes. "Usenet Software: History and Sources". updated December 1999. URL: http://www.faqs.org/faqs/usenet/software/part1

3) Brian Kantor and Phil Lapsley. "RFC0977: Network News Transfer Protocol: A Proposed Standard for the Stream-Based Transmission of News". February 1986.

URL: http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc0977.html

4) Internet Software Consortium. "INN: InterNetNews". 2000.

URL: http://www.isc.org/products/INN/

5) Robert H Zakon. "Hobbes' Internet Timeline v5.3". updated April 2001.

URL: http://www.zakon.org/robert/internet/timeline/

6) Ntrnet Systems. "How many newsgroups does Ntrnet carry?". July 19,1999.

URL: http://www.ntrnet.net/tech-support/faq/faq4a.html

7) Lookoff.com. "An Overview of the Internet: Ch. 2.3: Service Types: Internet Services: News". Last Modified: October 24, 2000.

URL: http://www.lookoff.com/tactics/intro_services.php3#news

8) Internet FAQ Consortium. "Internet FAQ Archives". Not dated, accessed May 2001.

URL: http://www.faqs.org/

9) David W. Wright. "Guidelines on Usenet Newsgroup Names". December 1999.

URL: http://www.landfield.com/faqs/usenet/creating-newsgroups/naming/part1/

10) Bill Hazelrig. "Why "alt.binaries"?". Not dated, accessed May 2001.

URL: http://www.landfield.com/usenet/alt/notes/alt-binaries.html

11) Jennifer Mack, ZDNet News. "@Home-Usenet scuffle could be settled". January 14, 2000.

URL: http://www.zdnet.com/zdnn/stories/news/0,4586,2422695,00.html

12) Robert Lemos, ZDNet News. "Melissa creator may be uncovered". March 29, 1999.

URL: http://www.zdnet.com/zdnn/stories/news/0,4586,2233931,00.html

13) Robert Lemos, ZDNet News. "Dutch treat? Netherlander takes credit for 'Anna' virus".

February 13, 2001. URL: http://www.zdnet.com/zdnn/stories/news/0,4586,2685314,00.html

14) Symantec Virus Encyclopedia. "Happy99.Worm". Updated, December 7, 2000

URL: http://www.symantec.com/avcenter/venc/data/happy99.worm.html

15) Eric Chien, Symantec Virus Encyclopedia. “Wscript.KakWorm”. December 30, 1999.

URL: http://www.symantec.com/avcenter/venc/data/wscript.kakworm.html

16) Brian Ewell, Symantec Virus Encyclopedia. “VBS.Godzilla.A@m”. Last Updated November 6, 2000. URL: http://www.symantec.com/avcenter/venc/data/vbs.godzilla.a.html

17) Richard Cave, Symantec Virus Encyclopedia. “W95.Hybris.Plugin”. Updated May 11, 2001

URL: http://www.symantec.com/avcenter/venc/data/w95.hybris.plugin.html

18) Jason Meserve. "New backdoor for DDOS attacks?". October 8, 2000.

URL: http://www.nwfusion.com/newsletters/bug/2000/1016bug1.html

19) Forrest J. Cavalier III. “Is Usenet safe?”. 1997.

URL: http://www.mibsoftware.com/userkt/0005.htm

20) Carolyn P. Meinel. "GUIDE TO (mostly) HARMLESS HACKING, Vol. 1 Number 4". 1996. URL: http://www.l-u-c-y.co.uk/Security/usenet/gtmhh1-4.txt

21) Stefanie Olsen. "Google brings back Deja's memory". April 27, 2001

URL: http://www.zdnet.com/zdnn/stories/news/0,4586,5081969,00.html

22) John Geralds. “Internet spying plans cause uproar “. Mar 30, 2000.

URL: http://www.pcw.co.uk/News/601489

23) Jason Meserve, Network World Fusion. “Espionage on Usenet?”. April 21, 2000.
URL: http://www.cnn.com/2000/TECH/computing/04/21/net.spies.idg/index.html

24) CERT®. “Advisory CA-1997-08 Vulnerabilities in INND”. Revised September 26, 1997.
URL: http://www.cert.org/advisories/CA-1997-08.html

25) Debian Security Advisories. "DSA-023-1 inn2: local tempfile vulnerabilities" January 26, 2001. URL: http://www.debian.org/security/2001/dsa-023

26) Microsoft Knowledge Base. “Article ID Q177217: XADM: Store Stops with NNTP XHDR on Large Number of Articles”. Reviewed March 17, 1999.
URL: http://support.microsoft.com/support/kb/articles/Q177/2/17.ASP

27) Microsoft Knowledge Base “Article ID Q184437: XADM: Information Store Stops with Large Number of NNTP Users”. Reviewed: April 8, 1999
URL: http://support.microsoft.com/support/kb/articles/Q184/4/37.ASP

28) Neohapsis Archives "Re: Unchecked buffer in Outlook Newsreader, Re: Local Buffer overflow in OutlookExpress". March 21, 2001.
URL: http://archives.neohapsis.com/archives/vuln-dev/2001-q1/0762.html

29) John David Galt. “Netscape 4.7 Danger: ‘Active’ Newsgroup Messages”. December 1, 1999.

URL: http://catless.ncl.ac.uk/Risks/20.66.html#subj11.1

30) Debian Security Advisories. "DSA-040-1 slrn: buffer overflow". March 9, 2001.

URL: http://www.debian.org/security/2001/dsa-040

Note: All links were checked and are current as of May 22, 2001.

Last Updated: June 26th, 2017

Upcoming Training

SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Community SANS San Diego SEC401	San Diego, CA	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS