GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Thomas L. Roberts
GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4b

Information Security in Higher Education: Threats & Response

Introduction

The catastrophic events of 9/11/2001 initiated many organizations to review and audit their existing information security practices. A very important, if not overdue audit is the review of information access at colleges and universities. The traditional practice of open information access and collaboration can be ideologically opposite to strong information security and assurance goals.

This paper discusses the information security threats many colleges and universities are facing. It explains why the design of higher education is ripe for threat activity along with examples of threats discovered in college computing environments. The final section of this paper lists recent responses to information security threats in higher education.

Setting the Stage for Threats

The Open Exchange of Ideas

The traditional culture of higher education promotes the free exchange of ideas. Not surprisingly, this culture has transferred to academia's dependence on information systems and the Internet. As an educational tool, instant information access benefits the academic mission and goals of universities. Often, the priority of keeping educational information secure is not one of those goals. Mary Grush, the editor of Syllabus, a popular higher educational technology publication writes:

> ***One of the hardest things about security is recognizing the need for it…In higher education, the traditional need for openness, academic freedom, and the sharing of information helped to spawn the early Internet. And we want these values to continue to support teaching and research at colleges and universities… The fact is that most of us —happily—aren't tuned into the abuses of our computer systems*** *(Grush, p.4).*

The previous statement illustrates a common perception of information openness at many higher educational institutions. The initial need for security is often overlooked and many academic users are not "***tuned into the abuses***." The culture and tradition of openness has created networking environments of very lax security and information security awareness programs are in great need (Goral, Higher). Vigilance and review of information security practices at

© 2013 The SANS Institute Author retains full rights.

universities is so important that it needs to be included as a responsibility goal for all technology users.

Security Can Be a Tough Sell at Universities

According to Jeffrey Schiller, MIT's network manager, information security at a university setting is a "***negative deliverable***". This means that when strong security polices are in place, security remains generally unnoticed, but when it is absent, it is very noticeable. For these reasons, higher education has difficulty earmarking resources for information security (Security, p.12).

He also mentions that many university users do not understand very basic information security threats. For example, how a compromised system can be used to attack another system on the Internet or why password protection can lead to identity theft. (Security, p.12). Not surprisingly, the implementation of a successful information security awareness program can be a difficult and monumental task.

Although layers of information security products are available for installation at universities, many do not get the needed attention. For example, the implementation of egress filtering can help prevent "spoofed" attacks on other Internet systems by examining the source address of out-going data information. Although these devices are very helpful for preventing attacks, they are not widely used. Universities tend to focus on current information attacks and not ways to prevent future attacks from occurring (Lesniak, pg.23).

The paybacks for security are not usually immediate and many universities to not face this issue until absolutely necessary. Many favor devices that will protect incoming threats, such as firewalls and intrusion detection devices. These items also tend to have more visibility to help justify the security costs (Goral, Network).

Reluctance to Balance Information Safety & Convenience

An optimum information security process tries to balance safety and convenience. If an information device was completely safe and locked down, it would be unusable by anyone and not very practical. Conversely, a very convenient information device not only constantly accessible, but open to any local or remote exploitation via the worldwide Internet. (Norton, p.9). Based on these criteria, it would seem logical that universities would value a balanced security stance to protect their information infrastructures, but many are unwilling to do so. Many choose to keep the traditional open access atmosphere (Goral, Network).

Vulnerabilities and Broad-based Computing

Universities also use a variety of information technology equipment, both new and old. Along with hardware, the use of various flavors of Unix, Linux, Solaris, Windows and Mac operating systems are deployed campus wide. This broad-

© 2013 The SANS Institute Author retains full rights.

based computing mixture along with various levels of configurations can create holes or vulnerabilities that can be easily exploited (Goral, Higher).

Some systems can be configured with default settings and not properly administered or updated with security patches. Often, the administration tasks can be informally delegated to a faculty or student member of very limited technical expertise (Lesiak, p.22).

If these systems are the responsibility of professional university technical staff, the assigned workload may be too large to provide the proper attention needed for security updates and basic administration tasks (Lesiak, p.22).

One common exploit that has been discovered in many operating systems is the ***buffer overflow*** attack. Many programs were designed to store data at a fixed size in a buffer. If an attacker sends larger amounts of data to these buffers, unexpected results occur. Some of these results can be the discovery of passwords, the ability to install backdoor programs, or gain access to another unintended system area (Armstrong, p.30).

Threats inside and outside of Campus

According to the Computer Emergency Response Team (CERT) at Carnegie Mellon, the number of network incidents reported in 2001 was 52,658, which jumped from 21,756 the previous year. In addition, the reports of system vulnerabilities reports also rose to 2437 in 2001. In 2000, 1090 vulnerabilities were reported. (Goral, Network) Many cyber crime experts expect that number to greatly increase in 2002. On Nov. 7, 2002, the CERT website reported the vulnerability count for 2002 is currently 3,222, (CERT/CC).

Every day universities are scanned for vulnerabilities by anonymous hackers worldwide. Along with information loss, these systems can be compromised as holding areas for digital movies and music, or be used to attack other systems on the Internet (Lemos, University). One of these attacks, a ***denial of service*** attack will be discussed later in this paper.

Not all attacks and threats originate from outside of campus. In July of 2002, a university student was charged with breaking into the school grade system and changed her failing grades to A's. Reportedly, she used techniques to compromise instructor passwords to gain access to the grading system (Police).

In addition, not all university members can be trusted to use their computing systems responsibly. In July of 2002, a university admissions official broke into a competing university via the Internet and accessed private student application information. (Princeton).

Types of Threats in Accessible Computing Areas

<u>Keyloggers</u>

Many universities place information technology equipment in open access areas for collaboration purposes. This allows easy access to email, web courses and Internet information. Many of these kiosks also provide access without

© 2013 The SANS Institute Author retains full rights.

verifying user information or implementing tracking mechanisms for security control.

Unfortunately, this ease of access can introduce security threats into the university computing environment. The installations of ***keyloggers***, which are software and/or hardware devices that record all typing activity, have been discovered at many universities. A primary goal of these devices is to capture access passwords and credit card numbers. Some of these keyloggers have the ability to send the captured information remotely, which helps protect the identity of the information stealers that have installed these devices. Some keylogger technology is very difficult to discover. One such device is disguised as a name brand keyboard to avoid detection.

In the summer of 2002, the U.S. Secret Service reported multiple installations of keyloggers at universities in four states. They contacted and alerted many other higher education institutions to watch for this activity (Lemos, Secret).

Viruses, Worms and Trojans

Other software that can be installed in these open computing areas are viruses, worms and trojans. Although many are familiar with the data-destroying effects of viruses and worms, trojan software may not be as familiar. This software installs “backdoors” or access to the computers from a remote location. Not only does this allow information to be stolen as with keyloggers, it allows the computers to be remote-controlled. This can set the stage for increased hacking activity and network attacks.

Denial of Service Attacks

This type of attack can be very damaging to other computers locally or via the Internet. When a network computer has been compromised by a trojan, it is referred to a ***zombie***. These zombies can be remote-controlled one or many at a time, which is a precursor to a ***denial-of-service*** or (**DoS**) attack. This means the zombie computer can be instructed to send massive amounts of data traffic to a victim computer. By doing so, a victim computer may feverishly attempt to process the data which can tie up processing cycles of the computer. When many zombies are summoned to attack a single victim computer (known as a distributed denial-of-service attack or **DDoS**) the computer may crash or be taken temporarily out of service throughout the duration of the attack.

Although DoS attacks may sound like science fiction story, many of these attacks have taken place and traced to compromised university systems. Some of the victims of these attacks have been notable ecommerce and web portals such as CNN, Yahoo and Ebay (Goral, Higher).

These infected systems can also multiple compromises that can propagate much faster. These “blended threats” can cause multiple attacks and more difficult to isolate and remove (Lesniak).

© 2013 The SANS Institute Author retains full rights.

Sniffers

Other information stealing devices that have been reported in open university computing areas are “sniffers.” Sniffers are normally software (and sometimes incorporate hardware) devices that capture digital data information passing over the wire. By monitoring this information, passwords, credit card, financial and personal information can be intercepted and used for culvert purposes, such as identity theft. Many software versions of sniffers are freely downloaded via the Internet (Security).

Wireless Sniffing

The installation of wireless computing has greatly increased in higher education environments. Because of wiring cost savings and the advantages of mobility computing, many universities have heavily deployed wireless in open campus areas. Unfortunately, this mobility and ease of access can create a host of security risks.

One of these is the ability to use sniffer technlogy to intercept information over the air. If default wireless configurations are used and controls are not implemented, sniffing personal information can be much easier to obtain.

Although there are ways to improve wireless security, many are too expensive and difficult to deploy in a university computing environment. In addition, some protections such as Wired Equivalent Privacy protocol (WEP) that adds security by encryption can be cracked by downloading free software over the Internet (Gnagni).

File Sharing Threats

The permissive use of ***peer-to-peer*** (**P2P**) file sharing at many universities is also a dangerous security threat. These programs are easily downloaded from the Internet and contain the ability to serve or search for files on the Internet. The most popular files that are traded and shared are digital music and movie files. Many of these files are copyrighted, which can expose universities to potential lawsuits and legal action. Some examples of popular P2P applications are KaAaA, Gnutella and BearShare.

Viruses, worms, trojans and keyloggers can also spread via file sharing technology. Sometimes files can be disguised to appear as sound or video files but actually contain harmful payloads. Infected or compromised systems can also leak personal information to other Internet users. By doing so, private information can unwilling become public.

© 2013 The SANS Institute Author retains full rights.

Instant Messaging Technologies

Although this popular technology was primarily used for text based chatting, it has evolved into a suite of Internet applications. Three of the most popular examples of instant messaging products are America Online's Instant Messenger (AIM) and ICQ, Microsoft .NET Messenger and Yahoo! Messenger.

These applications also incorporate file sharing technologies, which present similar infection and copyright infringement threats of permissive campus file sharing activities.

In a survey of instant messenger users by Central Command, almost half use the file-sharing capabilities. In addition, 15% of those users surveyed accept file downloads from unknown users. This greatly increases the risk of future infections via messenger technologies. (Woods).

In addition, these programs have adaptive capabilities that can be resistant to network protection devices such as firewalls and port filters. For example a common port used by some instant messaging products is port 5190. If this port is blocked for use on a university network, a simple reconfiguration of the messaging application to use another common open port (such as port 80 for web traffic) can easily circumvent the blocked port (Dalton, Instant).

Recent reports have documented pop-up windows users have received pop-up window messages with web address URL's that when clicked by the victim, infects them with a virus or worm (Woods).

Abundance of Bandwidth

Many universities have increased bandwidth by upgrading their network infrastructures to improve information reliability and speed. These improvements help draw talented faculty, staff and students to these institutions and set the stage for cutting edge research, collaboration and distance education programs. Unfortunately, they also draw unwanted threats and attention to universities.

According to an October article in The Chronicle of Higher Education, one university reported that 75% of their bandwidth was consumed by students sharing files with other students on campus along users located all over the world (Mangan). In addition, universities have also reported that improved bandwidth has increased reports of pirated software and digital movies on university systems. Many are Internet chat bots (automated programs) that are holding areas for pirated digital information. Sometimes they are controlled from remote users not affiliated with the university (Lemos, University). This extra bandwidth consumption can cause major traffic problems with the intended academic uses of the network, such as web searches, portals, research, email and distance education.

© 2013 The SANS Institute Author retains full rights.

Response to the Threats

Bandwidth Management Technology

Many universities have resorted to bandwidth shaping technologies to control the exhaustible resource of bandwidth. The technology is similar to a valve that controls water flow. Although it can be configured many ways, it generally allows the academic network applications to have a consistent share of the bandwidth and controls other uses such as peer to peer file sharing to not consume a large portion of the bandwidth. One commercial example of this technology is called Packet Shaper by Packteer, Inc. and it has been installed at 600 higher education locations (Students').

This technological solution can be expensive and has created a lot of controversy among students. Many technical experts feel that it is only a matter of time before someone figures out a way to circumvent the technology and return to open and unrestrictive downloads to the student community (Students').

The White House: National Strategy to Secure Cyberspace

On September 18, 2002, The President's Critical Infrastructure Protection Board released a draft document addressing information security issues at a national level and suggestions for improvement. Some of these key points affecting higher education are:

- Historically, university computer systems have often been targets of hackers and therefore used to attack other systems on the Internet.
- Open access and the high capability of computing available at universities are reasons hackers choose universities for exploitation targets.
- Information security needs to be a much higher priority at these institutions.
- Universities need to update their security policies and improve the way they use information security tool technology.
- Higher education needs to collaborate with industry and government, along with teaming efforts with these groups to help secure the national infrastructure.
- Universities need to address security issues relating to the personal and private information they store about students, faculty and staff.
- Higher education needs to address, find and fix the ten most common security holes published by the Sans Institute. It also strongly suggest that universities continue to follow safety practices outlined by Sans.

© 2013 SANS Institute, Author retains full rights.

- Universities need to examine and address security issues relating to Internet2 and methodologies related to security research information technology devices.

- Point of contacts need to be established involving technical and law enforcement officials at universities to address cyber attack issues.

Although higher education groups have discussed some of these issues previously, many disagree with the government's suggestion that in the future, grant funding at universities may be linked with compliance of the proposed standards. (Carlson).

Notification to Universities about Copyright Infringement

In October of 2002, representatives of movie and music organization sent a letter to over 2000 university presidents to address issues related to university students sharing protected copyrighted materials at higher educational institutions. Following are some excerpts:

"We are concerned that an increasing and significant number of students were using university networks to engage in online piracy of copyrighted creative works….We believe there must be a substantial effort, both discipline and continuous, to bring this piracy under control…Students must know that if they pirate copyrighted works they are subject to legal liability. It is not different from walking into the campus bookstore and in a clandestine manner walking out with a textbook without paying for it." (Mangan, p.1).

This recent effort follows efforts by these organizations to contact colleges and universities for individual copyright infringements, many detected from dorms and campus housing computing areas. The general notification cites the recent Digital Millennium Copyright Act and makes strong suggestions to avoid future legal litigation against the university; the sharing of copyrighted material must be removed. It is possible that this sensitive issue will become a landmark legal case and decide how universities will set policies regarding copyrighted material.

University Bans Windows 2000 on Residential Network

In early Novermber of 2002, The University of California at Santa Barbara decided to ban Windows 2000 and Windows NT 4.0 from all of the residential areas on campus. This was decided after numerous security threats of viruses, worms and denial-of-service attacks were reported and caused many outages of the university network. Although Windows 2000 is supported on the academic portion of the universities network, support staff claimed that it was very difficulty

© 2013 The SANS Institute Author retains full rights.

to keep student's computers configured in a secure fashion. To help alleviate this issue, the university asked student's to upgrade their systems to Windows XP. The university support felt that XP was easier to configure securely for student residential computing usage (Read).

List of References

Armstrong, Illena. "Hacks and Attacks: A Complex Infestation?" SC: Info Security News Volume 13 No. 9 (2002): pg. 26 – 32.

Borland, John. "Hollywood cracks down campus pirates." ZDNet:Ebusiness_ URL: http://zdnet.com.com/2100-1106-961637.html (27 Oct. 2002).

Carlson, Caron. "Bush to U.S. Colleges: Send in the CIO's." eWEEK URL: http://www.eweek.com/article2/0,3959,508676,00.asp (27 Oct.2002).

"CERT/CC Statistics 1988-2002" website URL: http://www.cert.org/stats/cert_stats.html#vulnerabilities (7 Nov. 2002).

Dalton, Curtis E and Kannengeisser, William. "Instant Headache." Information Security August 2002. URL: URL: http://www.infosecuritymag.com/2002/aug/cover.shtml (31 Oct. 2002).

Gnagni, Steven. "Technology: Wireless Insecurity?" University Business. URL: URL:http://www.universitybusiness.com/issues/story.asp?txtFilename=d:\webs\matrix\archives\dec01jan02\insecurity.htm (27 Oct. 2002).

Goral, Tim. "Higher Ed Cybervigilance: Now More Than Ever." April 2002. URL:http://www.universitybusiness.com/issues/story.asp?txtFilename=d:\webs\matrix\archives\apr2002\morethanever.htm (27 Oct. 2002).

Goral, Tim. "Network Security: Unwelcome Visitors." April 2002. University Business URL:http://www.universitybusiness.com/issues/story.asp?txtFilename=d:\webs\matrix\archives\apr2002\hackers.htm (27 Oct. 2002).

Grush, Mary. "Editor's Note." Syllabus: Technology for Higher Education. Volume 16, No. 1. (2002):pg 4.

Lemos, Robert. "University systems a haven for hackers." News.Com May 2, 2002 URL:http://news.com.com/2100-1001-898084.html (27 Oct. 2002).

Lemos, Robert. "Secret Service probes school hackings." News.Com June 20, 2002. URL:http://news.com.com/2100-1001-938126.html (27 Oct. 2002).

© 2013 The SANS Institute Author retains full rights.

Lesniak, Rick. “Blended Threats: A New Risk to Academic Freedom.” Technology For Higher Education Volume 16, No. 1. (2002):pg 22-23.

Mangan, Katherine. “Colleges Could Face Lawsuits Over Illegal File-Sharing.” The Chronicle of Higher Education October 14, 2002.
URL: http://chronicle.com/free/2002/10/2002101401t.htm (27 Oct. 2002).

“The National Strategy to Secure Cyberspace: For Comment – DRAFT”
URL: http://www.whitehouse.gov/pcipb/cyberstrategy-draft.pdf (27 Oct. 2002).

Norton, Peter and Stockman, Mike. Peter Norton’s Network Security Fundamentals. Indianapolis: Sams Publishing, 2000. Pg. 9

“Police: Student hacker gave herself A’s.” July 17, 2002.
URL:http://fyi.cnn.com/2002/fyi/teachers.ednews/07/17/university.hacker.ap/index.html (27 Oct. 2002).

“Princeton accused of Ivy League hacking.” CNN.com July 25, 2002. URL: http://www.cnn.com/2002/US/07/25/yale.princeton/index.html (27 Oct. 2002).

Read, Brock. “Citing Security Risks, U. of California at Santa Barbara Bans Windows 2000 on Residential Network.” The Chronicle of Higher Education (4 Nov. 2002). URL:http://chronicle.com/free/2002/11/2002110402t.htm (6 Nov. 2002).

“Security on Campus: An Interview with Jeffrey I. Schiller, MIT.” Technology for Higher Education Volume 16, No. 1. (2002):pg 12-14.

“Students’ file sharing overloads college networks.” CNN.com (10 Oct. 2002).
URL:http://www.cnn.com/2002/EDUCATION/10/10/college.computers.ap/ (27 Oct. 2002).

Woods, Bod. “Half of IM Users Accept Downloads.” Instant Messaging Planet :Security
URL:http://www.instantmessagingplanet.com/security/article/0,,10818_1470691,00.html (26 Sept. 2002).

© 2013 The SANS Institute Author retains full rights.

Last Updated: September 19th, 2017

Upcoming Training

Click Here to {Get CERTIFIED!}

Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS New York SEC401*	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Oct 03, 2017 - Nov 14, 2017	Mentor
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
Community SANS Omaha SEC401	Omaha, NE	Oct 23, 2017 - Oct 28, 2017	Community SANS
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Colorado Springs SEC401**	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401*	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event