Global Information Assurance Certification Paper

Are the Open Network Standards at the Universities Coming To a Close?

GSEC Version 1.4b Option 1

Seth Scavette
February 27, 2003

Abstract

With the ever painful and frustrating need to strengthen internet security the open-door policies of universities that once helped create the internet are beginning to look like the weakest links in the aspect of security on the internet. My document will begin by giving a look at some of the brief history in the making of the internet and how the universities became key players in the internet we know today. With this paper I will take a look at how and why universities are being used as tools for attacks, information theft, copy write infringement, and other unlawful activity. I will elaborate on and demonstrate on the fact that open network universities are a problem to them selves as well as the entire internet community. I will touch on some studies with brief findings of compromised university networks. I will give some break down on the chain of events of the compromise and take a brief look at some of the security policies in place at the time. In the closing of the paper I will address what I believe to be the future of these so called open-door networks. I will apply some of my recommendations based on existing trends, research and history thus far. I will begin to outline steps that I believe should be taken towards a better security infrastructure in the university network systems. The avoidance of network, system compromise, and the theft of information at the university level must be addressed in today's world to ensure tomorrows future.

As I touch on the above stated in my document I have attempted to keep details short in order to provide more of an over view on the subject of universities and their security. My goal for the reader is to catch the attention of a person that was not aware of what is happening in more than some of the university network infrastructures. Most of my findings are based on articles from what I believe to be reliable sources. I my self am also and employee in a central IT department for a university. Some of my views and experiences are expressed in this document. My writing does not reflect the views, opinions, ideals, or any other policies of my employer.

Research

From ARPANET(Advanced Research Projects Agency Network) to the Internet, it started to begin with one of the first small simple networks that linked MIT in Massachusetts to Berkeley University in California. The ARPANET was a small but significant network design in 1966/1967 by Lawrence G. Roberts and Thomas Merrill. This network design had begun to show us some of the way on the path to the internet. Their network provided a slow but mostly effective means of transmitting a digital message to and from hosts using what was referred to as IMPs (interface message processors). IMP's would be considered hosts in today's world. Roberts and Merrill proved that time based computers regardless of geographic location were capable of the sharing information and possibly even centralizing applications using this new ARPANET.

Shortly after in 1968 UCLA and Stanford University used a login system on the ARPANET to access a database on a remote host, once again proving the concept of data sharing. At this point in 1968 ARPANET consisted of 4 host's total. More universities and a handful of research centers soon joined on brining the count up to 23 hosts in 1971.

By 1972 the ARPANET started to show up more in the public spotlight. Soon after 1974 came an evolution of the ARPANET with research underway to begin a possible deployment of a TCP (transmission control protocol) which could and soon would provide a standard way of communication among the growing host community of the ARPANET. In 1983 the replacement of the NCP protocol running on the ARPANET was officially moved to the TCP protocol creating more solid standards for users to build around with better addressing ability that was not as platform dependent. In the years to follow TCP now known as TCP/IP (transmission control protocol/internet protocol) became a standard among many network infrastructures, private and public. TCP/IP is a standard today for the internet as we know it now.

In my research I found one of the original design ideas that also helped lead on to the Internet today came from a Bob Kahn in 1972. He was basing some of his research and ideas on that of an open network infrastructure. Bob Kahn referred to this as "Internetting". In the open network infrastructure individuals could utilize the network to fit the needs of their own environment. Users could design applications and tools with little to no constraints on the network integrated part since it would be an open standard. Documents and information could be polled freely and shared freely among other network enabled entities to fill a pool of knowledge sharing, and learning.

The open network structure idea was in fact one of the major contributors to what has provided us all with the rapid growth of the internet in place today. In 1984 ARPANET had reached 1000 hosts that were emailing and sharing applications and data freely to anyone connected. By this period in time the Internet was truly born and so were hackers and the viruses, worms, etc. written by them. National governments pushed to have the internet adopted by all higher education organizations, regardless of the type of educational medium. Any higher academic organization was urged and even funded to join the internet.

From early ideas evolving into a reality of a network connected space to share information and knowledge spawned traditions in the academic communities and their internet enabled networks. The ability to exist in and on an open access network without constraints became an accepted sort of standards among public and even some private academic communities and their organizations.

Now that we have hundreds and maybe thousands of universities on the internet we can start to look at why the open network infrastructure of many universities is being targeted for vulnerabilities, information theft, etc...

Many security experts believe that the university networks are a natural target for hackers and script kiddies. To simply look at most university politics you will find a lack of focus on the subject of security, online piracy, and information theft.

Some universities have begun to put more solid security plans into place with some funding recently but it has been a slow process that can be difficult to architect. The vast majority of universities is still very much behind the times and are simply not funded to gear up security on the network. University networks seem to imply a reputation for extremely relaxed security policies and vulnerable hosts. Taking a look at whom and what populates the university networks and what tends to make them vulnerable to the hackers it can start to become more clear why they are successfully attacked so often.

Most of the university organizations are usually made up of large distributed high speed infrastructures. The network infrastructure can consist of gigabit fiber back planes or faster and possible 10 base Ethernet connections or faster to all of the network devices and hosts attached. The network infrastructure in turn is usually piped into a large internet enabled connection. The internet connection can have an abundant amount of available bandwidth in many cases. Just the above stated ground shows as a perfect spot to try and launch flood attacks, scans, spamming platforms, Code attacks, and so on. The kind of activity that would thrive in a speed enabled connection is what the hackers will try out. Other wrongful uses may be the distribution of software, movies, music, etc. usually copy written material. Since most of these files would be of a large nature the bandwidth would be ideal for a hacker to get the data in and out fast. The bottom line here is plenty of bandwidth that can be used for all sorts of hacker like activity.

Inside some of this bandwidth enabled university infrastructures there can be a very wide range of hosts and network enabled devices running all types of operating systems and hardware specifications. In most cases universities have large publicly addressable IP address scheme for all of their connected devices. In many cases delegation and control of these devices and hosts are left to the owners of these machines. The owners of the devices can usually be broken down into a few individual groups.

The first group may be some sort of centralized IT (information technology) department that maintains the core infrastructure for the entire campus or campuses. Generally the core infrastructure group would be the maintaining body of the basic network policies, basic usage guidelines, core systems, and core networks. The core systems may be the university wide email server, the web server(s), university DNS (dynamic names server) servers, directory services, DHCP (dynamic host configuration protocol) , etc. IT traditionally will control the connection basically up to the data port in the lab, the classroom, or the administrative office and so on. In practice the central IT department usually does dictate and set guidelines for network usage on the campus.

The IT group however are not always aware or in coordination with the users of the distributed network and their systems online. I will elaborate more on this in the following paragraphs as we talk more about the users and their networks past the data port on the wall.

Because of the traditional nature of collaboration and access to information on campus it's rare to find devices such as firewalls and access control blocking devices in a place. Such perimeter devices if any usually are not found on the gateway from the University campus to the internet. The main campus IT group usually finds they can only lock things down to a minimum degree so as not to disrupt the free flow of information in the end users environments. The dynamic range of ports and protocols in use on campus makes it extremely difficult to manage a perimeter firewall. Occasionally you will find a firewall securing a section of the network such as a machine room.

If we look at the point that a user or group of users connect to the data port supplied by university IT you may find that the system administration and security management usually fall into a second group of individuals out side of campus IT. This group may be known as department technical people or LAN (local area network) administrators of a college or department. When you get down to the department level (also may be called a college level) the LAN administrators typically run the show. The administrators have also tended to develop an almost private network environment of their own to suite the needs of the department. The rest of the department LAN network may include switches, hubs, wireless access points, etc. all part of the departments own network architecture. Some departments set up mail servers, web servers, VPN (virtual private network) servers, DNS servers, and so on.

In many universities the main IT group is starting to clamp down much more on security with network device hardware policies, especially with affordable high speed wireless on the map now. The days of "IT will supply the network but past the data port it's the departments network." are going away fast. I am still finding however that much more security and centralized control is needed. The types of "lock down on the network" policies are an up hill battle for many large university distributed networks. Even after a policy is in place what still gets plugged in may be difficult to track and police, especially on a large distributed network with mixed environments and visually decentralized IT. Here lies a big problem of responsibility for security, and the integrity of all of the university systems that is not easily managed due to its de-centralized and vastly distributed common structure make up.

If we look at what the departments or colleges can develop system wise we will see a varied range of hosts on the network to accommodate services they may offer locally. Some of the host's hardware may be SUN, PC, Alpha, etc... Operating systems can be Solaris (all versions), BSD (all flavors), Linux (all flavors), Windows (All Versions), VAX, etc...

Some of these systems can be very old and dated. Patches and security updates may no longer be supported for these older systems. These older boxes tend to be the result of lack of funding and the general attitude of "If it's not broken don't fix it." Hardware and software is usually chosen by the department technical person and security is usually not the main concern when making purchase decisions; from what I have found in my research. Usually the LAN administrator is faced with ideas, or directives that he or she must follow to meet the needs of the college or department. This type of action has spawned from the core IT group of the university not implementing centralized common thread services in many cases. The sorts of systems and applications departments take on sometimes require a great depth of training and knowledge to properly deploy securely and effectively.

The vast majority of the time we see the department or college is under funded. The administrative person doesn't get the required training or tools to properly supply a secure and productive environment. In many cases the rollout turns into a quick approach with out of the box applications and little to no security planning.

For a quick example of a technical system rollout problem which I found very common on campuses we will look at a system proposal and a brief detail of what can happen to make things go wrong. Let us say we have a department that has a part time technical person or even a student worker with some basic network and systems knowledge; this is very common. The technical person would be asked to build an interactive login environment for the users with collaboration tools in place such as a shared calendar, tasks, etc... The tech person decides for simplicity and general familiarity to go with a local email system running a Microsoft Exchange 2000 server. To build the Exchange 2000 server a Microsoft Active Directory server is also required. The director of the department would also like the systems to have web based access for email and calendar tools.

Looking at just some of the beginning steps we can see how things start to go wrong commonly. First we have a technical person that is not entirely educated with the packages; this can cause some serious issues obviously. He or she may be part time or splitting the work load with other tasks as well. The department may also be under funded in the technical areas but they have needs and would like them met cheap and of course fast. To deploy this type of environment properly it would require some good planning and quite a bit of on going security management. All of the systems in this environment will be on the internet like most universities systems are. The tech person most likely will choose what seems to be the simple route of using defaults for installs and out of the box un-patched software initially. A very common mistake takes us to the domain controller build. The machine is hooked up plugged into the live network and Windows 2000 server is loaded onto it with all the default installed applications and settings. Here comes problem number one. Within minutes or less of that

machine being loaded it gets scanned and perhaps infected with an IIS worm or worse. A experience or properly trained person knows that the default install of Windows 2000 Server includes IIS unpatched. Statistics show an unpatched IIS server has a survival rate of 20 seconds on a public network at the right time of the month. The box was unpatched and on a live IP addressable unprotected data port. The tech person may have had good intentions to go online and patch the box but it was too late. Chances are the box stays online compromises until someone notices because they get scanned by the box or notice the high traffic. This example can go on and on, I probably could write a few pages of the security issues that could be born from this environment. This person has to build it and they will but at the cost of security, time, and possible liability. To a properly trained or experienced tech person this may seem like common knowledge but I can assure you that this happens all the time on these networks and others.

Typically the security problems fall on lack of knowledge or understanding of security and policy. In some cases departments do not have time or funds to manage systems in place so the systems simply fall behind on patches and updates. The constantly changing software and the software's vulnerabilities can require a lot of time and research to keep on top of. The push of the "traditional open network" also plays into the actions of the departments to follow the mission statement of academic freedom. Sometimes a hosted server becomes everyone's server for the shared information but no ones responsibility to maintain securely.

The other groups I will talk about on campus are the students. The different groups of students with computers or access to them can supply an almost un-manageable amount of security issues. Students themselves can actually be broken into some categories. For the sake of simplicity we will look at two major categories of students.

One group of students are the technically inclined students that are studying in a computer related, technical field, or just have good working knowledge. These students are what I will call the more computer savy students. The students can have a very wide variety of applications, operating systems, and network enabled devices that they will commonly use. These students will build systems for classes, personal study, or just personal use. The technically inclined groups of students that build systems for classes tend to be a little better educated about security and have a better idea about perhaps how to patch and help secure a box for its purpose on the network.

In today's classrooms education is starting to bring application and system vulnerabilities more into the schooling. The other side of this I have found in research is that sometimes its not enough. If a student has an application he or she is building for a class project they sometimes only focus on one layer of the system.

An example would be a student that has a class that he or she is studying Oracle the database application. The Oracle class may teach the proper security and patching of the Oracle application itself but not the proper lock down of the operating systems. Now we may have a fully secure implementation of Oracle on an unpatched Windows 2000, or perhaps SUN Solaris server.

Some students just simply don't care to take the time to patch and secure since they may consider the host a test box or project box and it would be scraped if compromised so they choose the quick and dirty route. In this scenario the quick and dirty test box is a prime candidate for attack on the open internet enabled network.

The other group of students is the ones that have no technical computer knowledge. They are simply users in the most plane vanilla sense of a PC user. They use there machine to surf the net for information, to write papers, and generally to do study related work. Some of these students may have brought in there own PC's and loaded there own software. Most PC software out of the box is sold with security functions turned off and a lack of the latest patches. These non-technical students tend to be the hardest hit on campus by virii, worms, and backdoor software applications. The students just simply don't understand or even care to understand the reality of plugging into a piece of the internet in there dorm room or on campus. Some of them are infected from peer-to-peer applications. The student may have downloaded some software that had a backdoor or a virus. A lot of Universities now are providing students with anti-virus software and updates for there operating systems and their standard applications along with guidelines for better network protection. What has been happing however is that many students do not stay up to date with virus definitions and the patches so they are still not fully protected and seem to get compromised again by hackers.

It is also not uncommon with any of the students to find web servers, email servers, DNS servers, wireless and private networks, peer-to-peer networks, and many other types of systems the students have built on the campus networks. The high availability of internet bandwidth is a temping environment for the exchange of copy written material such as MP3, DivX, MPG, etc. via the commonly used P2P applications such as Kazaa and Morpheus. The RIAA (Recording Industry Association of America) has been encouraging universities to step up and do something about the massive amount of illegal content being shared by students on many university networks. RIAA has begun taking steps to actually prosecute offenders in court that violate copy writes. It's possible that in the future RIAA and organizations like it may hold the university itself responsible for the content of the university network enabled hosts.

Students also manage to get involved in the more technical levels of being hackers or script writers them selves. Students have been going beyond just the simple sharing of copy written files.

Student hackers have been found to be quite common on campus these days. The network environment as I have been outlining is just right for student hackers. To elaborate more the computer systems that some colleges have available for the students to use can be state of the art technology. Students can have access to some of the fastest networks in the world. Students also have access to public computer labs. From any lab it could be easy to conceal a real identity; they could hide within the network for a period of time and then move on before being tracked down.

Its would be difficult and even more drawn out to describe the many scenarios there could be in the student and departmental environment. To wrap up on these groups the ingredients for open vulnerable and exploitable machines are well mixed. The bottom line I am finding in research is that too many university networks today are rich fertile grounds for hacker activity because of lack of policy and policing. There is a lack of vulnerability assessment and resolution along with little to no accurate monitoring tools in place. Hackers can hone there skills in a virtually anonymous environment in many cases. There are large servers with big disk drives just begging for data on fast internet enable connections. The university networks can essentially become a perfect staging ground for large hack attempts and also a perfect place for new hackers to learn the ropes easily.

To elaborate on or demonstrate some of the problems of the open university networks and their security I am going to look at some actual cases of hacker activity and how Universities were affected or involved.

In February of 2000 there were a huge amount of DOS (denial of service) attacks directed at ebay.com, cnn.com, and a few select others. It is believed that the tools used for these attacks were created and tested on university networks. Some of the key machines used in the actual attacks were within university networks. The machines in the attacks were used to direct large amounts of messages and requests to the commercial web servers. The servers were overwhelmed causing web pages to be unavailable or extremely delayed loading and processing times. This case involved the use of the anonymous factor, ease of finding exploitable machines, high bandwidth availability, lack of monitoring, no firewalls or improperly configured ones, and many university networks.

A hacker gained access to a Linux system inside a university hospital. The Linux system allowed him to get to a VNC (a remote desktop program) application that was exploitable. In turn the hacker exploited the application to gain access to a Windows NT box that had weak passwords and also operating system vulnerabilities. Once he was in the NT box the hacker used various tools to expand his reaches into the core of the network. Many backdoor programs were installed along with some trojan horse programs to help expand the hackers reach.

In the end the hacker was able to steal the private medical records of over 4500 patients. The hacker exploited a university network with no firewalls, weak passwords, vulnerable applications, and lack of monitoring in short.

Hackers penetrated a University web server through means of weak security and lack of monitoring by the university. The group was able to gain the information of students and there records. The list contained informational decisions on acceptance of the students to the university. The university may be charged with criminal charges along with funding being withheld because they breached a student confidentiality act. Basically the hackers were able to get the information simply because the web sever was not properly secured and monitored.

A campus computer lab was exploited and used to send spam email and serve illegal files via an ftp server. The boxes were loaded with the hacker's applications via the floppy disk drives that the machines had in the open lab. The computers were not properly locked down to stop this sort of activity. The computers were also not monitored for the addition of software or hacking tools. The lab administrators noticed a sharp increase in the amount of traffic on the network and discovered the seized machines.

Universities machines were broken into and used to steal credit card numbers and personal student information by a hacker. The hacker claimed to have been able to break into hundreds and even thousands of computers on university networks. He would use the machines to steal user names, passwords, emails, credit cards, and any sort of material he could capture from a users session. Some of the tools used were key logging software that would record each keystroke a user entered. The logged key strokes could then be stored or sent to a specific location for the hacker to process. A lot of the programs the hacker placed on compromised machines could be controlled from IRC (internet relay chat) rooms or channels. Basically the hacker could log on to a IRC channel and send a command to hundreds of machines. This hacker exploited and used all the weaknesses of the universities and other networks he could find. The universities in the end were the easiest and the safest for him to use he stated.

A large group of educational institutions were used in an elaborate DOS (denial of service) attack on IRC servers all around the globe. The compromised machines were all Microsoft windows machines 95, 98, and 2000 versions. The exploits used were mainly known bugs in the IIS (internet information server) web server. IIS is a package built into several versions of Windows that has had a rough history of extremely large security holes. Most of the machines had application running on them that could send has much as 5 mbits/sec from each compromised machines. This hack was a huge problem for about 36-48 hours until traffic was able to be blocked or filtered. All of the infected hosts had to be rebuilt and properly patched in order to prevent the attack again. This entire case spawned from machines that were not properly patched and locked down.

The machines were also not monitored enough to be able to react quickly to the high amounts of traffic the hosts were producing.

As I researched on the internet for cases of compromised universities I found the results to be quite surprising of just how many documented cases there are so far. Most universities were claiming between 2-20 successful hacks per day on their campus. Numbers ranging from 20,000-200,000 hacking attempts made per day. Attempts were things like scans, probes, and searches for specific applications or vulnerabilities. Many of the tools that hackers can use today can successfully compromise an improperly managed host in less then a minute after the host is found. The amount of compromised machines on campuses has more then doubled in the last few years.

So with what I have stated above in consideration I am going to look at some possible ways of improving the methods of dealing with security issues on campus.

- Network analysis and real-time monitoring
    - Document and track all known infrastructure devices
    - Document versions of software and patch levels of network infrastructure devices
    - Store all device configuration files in a centralized location
    - Compare live configurations to stored ones to track un-tracked changes
    - Employ a change management procedure for all managed network devices
    - Analyze configuration for signs of problems
    - Create a system to poll the network devices on a regular schedule and use SNMP where applicable to check for the proper response from a device and report back failures
    - Create a syslog database to accept error or message traps from the network devices
    - Written and enforced network policies to dictate what gets plugged in to the network
    - Specific networks secured and designated for wireless devices should require proper encryption and login key methods
    - Monitoring tools to shape packets and track traffic trends
        - Checks for peer-to-peer heavy traffic and possible copy written file sharing
    - Intrusion detection systems on the network at various key points of the network that has visibility of core infrastructures
        - IDS would detect unacceptable use of network
        - IDS would report actively of any violations on the network that are defined as such in the rules of the IDS

- Centralized source for user authentication and secure key systems
    - Provide a centralized directory service that students and departments can rely on for authentication methods
    - Require identity proof for servers on the campus network as well as students, staff, and faculty
    - Provide key management systems for encryption methods that can be centralized and used by departments and students
    - Password policies should be put into place to create an environment with strong passwords

- University wide computing standards, and network and computing required written and acceptable use policies
    - Develop a standards and policies committee within the core IT infrastructure to work with representatives of departments
        - Develop standards for technology replacements of the future
    - Coordinate technology upgrades with a group of representatives from departments
        - Define the direction of technology to meet the defined needs across the organization
        - Create strategies to break down road blocks amongst the departments and work to better integrate existing services, systems, and tools into a more centralized environment
        - Develop projects to address common technology issues among majorities of departments that has flexibility and can be centralized
    - Deploy centralized and managed antivirus software and also make it mandatory on all campus networked hosts applicable
    - Offer a committee to research university funded programs to get grants for equipment, training, and technology that can be centralized and offered as a services on campus
    - Build focus groups with students and faculty to address campus network security
    - Develop university wide standards for the training of technical and management staff members to include computer security as a requirement
    - Develop security analysis and audit standards that must be met by the systems and environments within the university campus network
        - Scanning for vulnerabilities with scanning tools
        - Weak password checks
        - Open vulnerable file shares
        - Patch management
    - Encourage security training sessions on campus by qualified security staff
    - Provide affordable technical assistance from a qualified support staff to the departments and students

    - Post campus wide security bulletins to promote more secure environments and get the attention of the public
    - Provide a single point of solution for network security and related campus issues
    - Develop authentication and standards for open labs and walk up data ports
    - Develop disaster recovery strategies for centralized systems and networks

- Physical device and perimeter security
    - Firewalls should be put in place on the perimeter of the networks
        - Firewalls could alternatively be placed on sections of the university network such as a machine room subnet
    - Door locks, key cards, coded doors into physical network device areas should be restricted

I believe the future of the university network has a lot of change coming in the next 20 years. We have seen quite a bit of change already towards secure and better locked down environments at the univeristys. As hacking and the successful compromise of university networks is continuing to rise action will be taken to counter the attacks. Accountability for stolen information, distribution of copy written materials, and general hacker activity is starting to fall on the owners of the network as well as the owners of the machines. More firewall like devices will most likely be installed and more monitoring of these networks will be applied. Although I think that the universities will always have an open learning environment on the network it will be met with strict security requirements. The requirements will be that of a much more secure and robust systems. Strong authentication for hosts and well as users will become more apparent and required to help reduce the amount of unknown users on a network. Servers will most likely have to be approved and properly secured before they can be connected to the network so that they can resist hacker attacks. The deployment and development of new monitoring tools for the networks will not only help monitor activity but also police it for weak systems, devices, and individuals not conforming to university network policies. Security technologies will get better and better over time to help fight off the hackers. I think closing doors on the open university networks is going to happen more and more. The tradition of an open learning environment structure will still thrive but inside of a controlled secure environment.

Resources

The Associated Press. “Russian mob may have hacked university PCs.” 6/20/2002. URL:http://www.usatoday.com/tech/news/2002/06/20/russian-mob.htm (2/10/03)

The Associated Press. “Man who hacked NASA computers gets 21 months.” 2/05/2002. URL:http://www.usatoday.com/tech/news/2002/02/05/hacker-sentenced.htm (2/10/03)

Hillig, Kurt. University of Michigan. “Systems Security, Hacked Machines, and DoS Attacks.” 7/13/2001. URL:http://www-nettools.ns.itd.umich.edu/htmlarchive/msg00031.html (2/10/03)

Mrozek, Thom, PAO. U.S. Department of Justice. “Orange County, California Computer Hacker Pleads Guilty to Hacking University Computers, Defrauding Western Union.” 8/01/2001. URL:http://www.usdoj.gov/criminal/cybercrime/diekman4.htm (2/10/03)

Greenspan, Jesse. Arizona Daily Wildcat. “UA computers hacked daily.” 12/02/2002. URL:http://wildcat.arizona.edu/papers/96/67/01_1.html (2/11/03)

University Of Michigan News. “Sites PC Environment Hacked Into; Users Urged to Change Passwords.” 1/22/2003. URL:http://www.itd.umich.edu/news/2003winter/01222003a.html (2/10/03)

Lubow, Eric. The Register. “Princeton ‘hacks’ Yale admissions site.” 7/26/2002. URL:http://www.linuxsecurity.com/articles/hackscracks_article-5401.html (2/11/03)

The Thompson Corporation and Health Data Management. “University Confirms Medical Records Were Hacked.” 12/08/2000. URL:http://www.healthdatamanagement.com/html/ExpertStory.cfm?DID=2746 (2/10/03)

Poulsen, Kevin. SecurityFocus. “Hospital Records Hacked.” 12/06/2000. URL:http://www.securityfocus.com/news/122 (2/11/03)

ISN. SecurityFocus. “University computers are prime targets for hackers.” 6/01/2001. URL:http://cert.uni-stuttgart.de/archive/isn/2001/06/msg00009.html (2/11/03)

Security Wire Digest. “Alert Issued for Academic Institutions.” 6/27/2002. URL:http://www.infosecuritymag.com/2002/jun/digest27.shtml (2/11/03)

McWilliams, Brian. Internetnews.com. “Net Still Wide Open to Smurfing.” 8/11/2000. URL:http://www.internetnews.com/bus-news/article.php/3_436031 (2/11/03)

Belous, Yegor. PRAVDA.Ru. “Russian Mafia Penetrates US College Campuses.” 6/26/2002. URL:http://english.pravda.ru/main/2002/06/26/31223.html (2/11/03)

Wired News. “Public-Computer Users Beware.” 2/06/2003. URL:http://www.wired.com/news/infostructure/0,1377,57587,00.html (2/11/03)

Delio, Michelle. Wired News. “Hoosier Favorite Hack Victim?” 6/13/2001. URL:http://www.wired.com/news/culture/0,1284,44501,00.html (2/11/03)

Lemos, Robert. CNET News.com. “University systems a haven for hackers.” 5/02/2002. URL:http://news.com.com/2100-1001-898084.html. (2/11/03)

Network-1. Security Solutions, Inc. “Universities Deploy CyberwallPLUS Host Intrusion Prevention.” 5/21/2001. URL:http://www.network-1.com/website/news/press_rel/old/05_21_01.asp (2/11/03)

Roberts, Michael. Educom Review. “Shared Infrastructure and the Future of University Networking.” 12/1997. URL:http://www.educause.edu/pub/er/review/reviewArticles/32660.html (2/11/03)

Delio, Michelle. Wired News. “College: A Cracker’s Best Friend.” 2/28/2001. URL:http://www.wired.com/news/culture/0,1284,42063,00.html (2/11/03)

Griffiths, Richard T. Leiden University. “The History of the Internet.” 10/11/2002. URL:http://www.let.leidenuniv.nl/history/ivh/chap2.htm (2/11/03)

Leiner, Barry M. Cerf, Vinton G. Clark, David D. Kahn, Robert E. Kleinrock, Leonard. Lynch, Daniel C. Postel, Jon. Roberts, Lawrence G. Wolff, Steven. Internet Society. “A Brief History of the Internet.” 8/4/2000. URL:http://www.isoc.org/internet/history/brief.shtml (2/11/03)

Cox, Beth. Internetnews.com. “RIAA Trains Anti-Piracy Guns on Universities.” 1/30/2003. URL:http://www.internetnews.com/bus-news/article.php/1577101 (2/11/03)

SCS News. “Criminal Hacking Today, Terrorism Tomorrow? Unsecured Campus Networks Make Alluring Targets.” Fall/2002. URL:http://www.scs.nevada.edu/about/news/f2002/security.html (2/11/03)

Vamosi, Robert. CNET Software. “Pirated movies now playing on a server near you.” 5/08/02. URL:http://www.cnet.com/software/0-8888-8-9864702-1.html (2/11/03)

Olsen, Florence. Chronicle of Higher Education. “The Growing Vulnerability of Campus Networks.” 3/15/2002. URL:http://www.chronicle.com/free/v48/i27/27a03501.htm (2/11/03)

Radcliff, Deborah. Computerworld. “Clarke warns educators about need for better security.” 6/05/2002. URL: http://www.idg.net/ic_873565_1794_9-10000.html (2/11/03)

Nebeker, Annie. University of Utah. “Addressing The Behavior of Student Hackers.” 7/10/2002. URL:http://www.naspa.org/netresults/article.cfm?ID=688 (2/11/03)

Tuckwiller, Tara. Sunday Gazette-Mail. “College Unplugged.” 11/03/2002. URL: http://sundaygazettemail.com/news/Valley+&+State/2002110220/ (2/11/03)

Sans Institute. “SANS/FBI The Twenty Most Critical Internet Security Vulnerabilities.” 10/17/2002. URL:http://www.sans.org/top20/ (2/11/03)

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Community SANS Trenton SEC401	Trenton, NJ	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 Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	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
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
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
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS