Global Information Assurance Certification Paper

Information and Network Resource Administration and Security in an Education Network Environment

Ryan W. Davis

August 12, 2001

Introduction

The goal of this document is to discuss and apply knowledge of Information Security to common security problems and concerns in an educational environment. My motivation for researching and discussing issues in an educational environment stems from my experience in such networks. With the explosion of the Internet and connectivity around the world and especially in the United States educational networks have become heavily reliant on connectivity within the institution and to the Internet. This connectivity facilitates the main goal of education as well as is a requirement for doing daily business related to that institution. At the same time this connectivity in which students, faculty, and staff participate has created a breading ground for vulnerabilities, threats, and compromises within these networks. Since educational networks must remain generally open in order to aid in the exchange of information these networks inherently pose great difficulty in securing and curbing the amount of intrusions since security compromises cannot be eliminated in its entirety. So what is an information security person to do in such a widely open environment? The main goal would be to layer security measures ("defense in-depth") in order to minimize security risks. These security measures cannot be so direct as to eliminating all un-solicited traffic into the network. In this paper I will cover various topics that will aid in concealing and securing information and network resources within an open network, specifically a higher education network such as a University or College.

Background

A multitude of resources can exist on an educational network at any given time. I say any given time because educational networks are very dynamic. Educational networks by definition are on the "cutting-edge" of technology. Client and server software are constantly being updated and changed to facilitate the many needs, which a higher-learning institution requires. Also educational networks are a central location for test environments on different computing technologies, which may contain vulnerabilities, as it is not ready for public release, as well as research in various fields that may contain intellectual property that must be kept confidential lest others use that information for commercial purposes before its public release. Steps must also be taken to prohibit sensitive information from falling into the hands of the wrong individuals inside that network as well. As many can imagine not all students can be trusted to keep university information confidential as well as not using that information for personal gain. To trust everyone on that network to "play nice" would be tempting fate. So not only must

security measures be in place to prohibit malicious access from the outside world, but also measures must be taken to ensure that the policies set forth by that institution are adhered to. Again care must be taken not to become so strict with security measures as they may become a double-edged sword and restrict the free-flow of information and ideas between individuals in that educational network.

Connectivity

Of the utmost importance is connectivity. Care must be taken in order to ensure that connections within the network must be kept on and flowing as quickly as possible. That means that administrators and network security officers must take care that hardware that maintains the inter-connectivity is online and operational as well as being hardened so that attacks made against that hardware are unsuccessful. Suggestions for doing this range widely. A good practice is to take care in choosing IP addresses for hardware that maintains connections for that network. How an individual can accomplish this is by semi-randomizing the IP addresses. Having all networking hardware such as routers, switches, and name servers maintaining the same last byte of an IP address would make little work for someone wishing to launch an attack such as a Distributed Denial of Service attack against that network. An example would be to randomly choose IP addresses of different hardware on different subnets to a certain range such as them being between *.*.*.150 and *.*.*.200. It should be a requirement that documentation be kept on network resources anyway so putting IP's within a certain range poses little difficulty in documenting. Granted network resources must maintain static IP's for convenience but using DHCP to lease IP's for workstations is a must for educational environments. Also care should be taken not to make information about network resources readily available to the public as possible because it can make the job of an attacker all that much easier. At my educational institution we use a network monitoring service called BigBrother. While this system does an excellent job of making information on server and resource status available to the individuals responsible for maintaining that network from a security stand-point this can be a risk due to the fact that it makes information viewable to anyone that is able to find and use the system via the web. A good idea would be to password protect such systems that display network information via the web and have them authenticate through any authentication methods currently in place on the network, such as Kerberos. As many security experts have noted though, it is almost impossible to stop a serious DDoS from occurring. A case in point would be the Denial of Service documents by the Gibson Research Corporation that chronicle the denial of service attacks against the author (see http://grc.com/dos/grcdos.htm). In this case procedures must be in place to curb the damage caused if a DDoS were to occur. Completely severing the connection is not always a viable option in a network that relies on intercommunication. Designing procedures to approach an incident such as this is imperative. A good start may be to list ways to thwart such an attack. Such as custom filtering packets at the router into your organization by analyzing information logged from the attack. Your ISP as well as technical support for your networking equipment (i.e. Cisco or Nortel) should be kept close at hand. Certainly though these incidents may not be completely avoidable, but they can be thwarted or lessened by creating procedures that make it more difficult for

attackers to target key points of network infrastructure.

Network Resources

One of the most key areas to protect besides general network connectivity would be file and information servers. I would venture to say that a good majority of the traffic on a higher-education institutions network would be traffic between client and server machines. That is most likely because many faculty, staff, and students rely on servers for the vital information that drives learning in the modern day. All members of a modern University rely on email to conduct personal and business conversations that are quick and to the point. As it is become evident with the rest of the online world email is key. Web-servers account for a lot of information exchange on an educational network as well. Today's educational web-servers not only provide access to email, and information about the university to prospective students but also provide information to current students about due dates, meeting-times, and exams. Its true, I have rarely heard of a class today that does not have a website in some form or another. Web-servers provide a wealth of information to students, faculty, and staff that pertain to their daily activities. An educational network may contain a multitude of other servers such as Novell servers that contain network shares or information pertaining to authentication on the network and printer direction and queuing for high traffic environments. Many universities may have Unix or Linux shell systems that are needed for development for other systems or classes. Plus I'm sure many more systems needed to meet that institutions needs. All of these systems are vulnerable in one way or another to attacks while on a network. Since educational institutions usually draw a lot of traffic from external sources this could be dangerous. A good idea would be to install some type of local firewall or Intrusion Detections System on said systems in order to protect these systems from attacks that can occur. These are important to setup even if your institution already has a firewall set up at its connection to the Internet. Quite often attacks come from inside the DMZ on compromised machines. Local machine protection is key because it adds another layer to your defenses against these attacks. Good ways to protect servers are to use secondary software created by other companies designed for this sole purpose. For Unix and Linux servers I recommend portsentery this is a very good program and is free. Also IPChains and IPTables are also available in most Linux distributions to aid in securing those machines. For windows machines I advise Zone Labs Zone Alarm or Network Ice's Black Ice Defender. While I am partial to Zone alarm, Black Ice Defender can be a valuable tool for securing servers since it is in essence an IDS/Firewall Hybrid. It can also be customized for servers to allow incoming traffic needed access. Zone alarms personal version is free, but corporate or large organization use requires registration or purchase, there is also a professional version that can be purchased. Black Ice Defender can be downloaded for a thirty-day trial, but must be purchase after that. Network Ice also has other versions of their IDS/Firewall software specifically designed for servers and other security software that can be purchased as well. Logging should also be a key priority in securing a network such as this. Logging helps administrators of servers on the network to detect suspicious activity and alert them of errors on the system. There is also other software that exists to help manage the extensive data that can come from log files

associated with monitoring network activity. There is also software out there that is able to hide data on the network. While scanning can be considered a hostile activity there is no way to completely eliminate the possibility of port probes on a system. If an attacker probes a system that shares files via netbios or samba then these ports will obviously come through as "listening". When these scans occur the attacker can then use information that the system responds with in order to evaluate its OS and any vulnerabilities it may have. Software exists such as fingerprint fucker by The s0ft project that changes the systems TCP appearance to confuse anyone not acquainted with a system of its true purpose. These things are critical in securing the vital data that may exist on the network.

Policy and Enforcement

Policy in an educational network is definitely an area to be examined. If the correct policy is not in place individuals that administrate that network may not have the flexibility they need in order to ensure its health as well as giving anyone else not responsible for its health the ability to conduct activity that is counter-productive to its purpose. Most institutions recognize this possibility and work to create an extensive policy to "Cover the bases" but do nothing to aid readability and thoroughness. As many large educational networks are seeing many individuals, such as students, faculty, and staff are participating in (sometimes illegal) file sharing that is not necessary for daily completion of work. This consumes a large amount of bandwidth as well as can cause the institution to come under legal fire in copyright infringement cases. In order to make sure that the network is living up to its full functionality it may be necessary to create policies in order to discourage this type of activity as well as enforce it. Systems such as MRTG can be used to monitor traffic in order to give administrators a visual representation of traffic on their network. This way traffic can be examined for bandwidth consumption as well as patterns in transfers at certain times. This system can also be used to note anomalies in network activity. To enforce this policy my institution has deployed software by Palisade Systems called PacketHound. This software allows network administrators to monitor, manage, or block protocols based on their characteristics as well as by port number. Now administrators could always filter such ports on the router or firewall but unfortunately many file-sharing applications have the ability to change the port on which they function. That is where PacketHounds characteristic identifiers may prove useful, but if a low-cost method is needed then manual filtering may be your choice. In most educational institutions it is not a priority to attack file sharing due to legal concerns, because many users on the network cannot be policed easily, the concern lies in the consumption of bandwidth and resources that limit productivity.

End-user Machines

Another concern in computing in an educational institution may be public computing sites that may need flexibility, but security in place to limit any malicious activity both remotely and locally. Care should be taken to secure any image or installation on a machine owned by the institution guarding against external attack as well as user error or

abuse. Many guides exist that can be purchased or downloaded detailing steps in securing your software. Some of these can be purchased or downloaded for free. SANS.org currently publishes step-by-step guides that detail securing workstation and server machines that operate on the Linux, Windows NT/200, and Solaris platforms. Other specific operating system software or application security documents exist that can usually be downloaded from vendor websites. I will not go into the detail of securing specific environments in this document for brevity but will say again that many resources exist. Most of these guides detail installing patches, but that may not always meet your security needs. In an educational resource environment flexibility is needed in order to ensure ease of service. Since there is no "across the board" security measures that can be implemented for all machines on the network a case-by-case or group-by-group security implementation scheme might be a good approach. As always time is a limited resource. A strategy of limiting user-privileges and rights to machines and resources is the best possible route to take. Users should never be given access to resources they don't need. When granting access and file rights this is key. This prohibits abuse and misuse of any resources that need to be secured. Printers and file-shares should always be authenticated, through a system such as Kerberos. If that is not an option care must be taken to observe and delimit the extent of those resources.

After the task of protecting and securing your institutions resources has been accomplished the task of enforcing local machine security in machines on the network but not owned by the institution becomes apparent. At my institution not a semester goes by that a student user in a Residence Halls machine becomes compromised. Obviously this can be a very nasty situation in which all parties involved can reap the consequences. This compromise usually results from a careless user who either cares not to patch his operating system and software or lacks the computing knowledge to accomplish such a task. How do we protect against this? Your institution may wish to employ vulnerability scanning mechanisms to alert you to any vulnerable or compromised machines on the network. A good tool that no security officer should be unaware of is Nessus. The Nessus.org website has the following to say about their project:

> "The "Nessus" Project aims to provide to the Internet community a free, powerful, up-to-date and easy to use remote security scanner.
>
> A security scanner is a software which will audit remotely a given network and determine whether bad guys (aka 'crackers') may break into it, or misuse it in some way.
>
> Unlike many other security scanners, **Nessus does not take anything for granted**. That is, it will *not* consider that a given service is running on a fixed port - that is, if you run your web server on port 1234, Nessus will detect it and test its security. It will not make its security tests regarding the version number of the remote services, but will really attempt to exploit the vulnerability.

> Nessus is very fast, reliable and has a modular architecture that allows you to fit it to your needs. “

As the above text notes a security scanner is a program that will remotely examine machines on a given network to check for known vulnerabilities and alert you to their presence. Once a security scanner is in place in can check the network and log all vulnerabilities and their originating machines. Some can even notify the system administrator to the vulnerability directly upon detection. If this may not be an efficient option security personnel may just be able to make note of vulnerable machines and notify administrators or users seperately. If these users are not available for contact or refuse to respond or take necessary measures the security officer can then use in-place policy to turn off network access to the vulnerable machine. This action, although extreme, usually results in the user contacting personnel to determine the problem and take the necessary measures to secure their machine.

The Gibson Research Corporation also has many resources, but more importantly small programs that can be downloaded for free and run locally or run remotely from their website that check for many computer vulnerabilities, firewall integrity, and spy-ware that may exist on your local machine. Fortunately and unfortunately they are too numerous to completely list in this document. Some of the GRC’s software contributions are PatchWork, LeakTest, and Shields Up!. Many Institutional IT divisions have websites to list information. A good idea would be to publish periodical articles detailing safe information security practices and links to many of the topics listed in this document. All these steps can aid in securing end-user machines so that functionality and safety of the network is kept at best.

Conclusion

Today’s Internet can be a wonderfully and massively educational experience. No doubt numerous resources on almost any topic imaginable exist. Many of these resources are located on educational institutions around the world. At the same time the Internet can be a dangerous place for the ignorant or careless user. Too often the freedom needed in aiding education on a large scale is confused with careless computer and network security practices. It is the job of the security officer and end-user alike to keep that environment safe for education and enjoyment. Hopefully many of the pieces of information and steps I have outlined, when implemented properly, can help to keep that institution functioning at its best.

Resources

General Security:

1. The SANS Institute Online
   http://www.sans.org/

2. CERT Coordination Center
   http://www.cert.org/

3. Security Focus (Computer Security Info, Software and Bugtraq mailing list)
   http://securityfocus.com/

4. NIST Computer Security Resources Center
   http://csrc.nist.gov/

5. Gibson Research Corporation
   http://grc.com/

Listed Software

1. Zone Labs ZoneAlarm
   http://www.zonelabs.com/

2. Network Ice's BlackIce Defender
   http://networkice.com/

3. Snort
   http://www.snort.org/

4. Psionic Software's PortSentery
   http://www.psionic.com/abacus/portsentry

5. Tripwire Security's Tripwire
   http://www.tripwiresecurity.com/

6. MIT's Kerberos Information Website
   http://web.mit.edu/kerberos/www/

7. BigBrother
   http://bb4.com/

8. Nessus.org
   http://nessus.org/

9. Palisade Systems PacketHound
   http://www.palisadesys.com/products/packethound/

Misc.

1. SANS Institute Online Bookstore
   http://sansstore.org/

2. NSA/CSS Information Security Website (Contains literature on various topics)
   http://nsa.gov/isso/index.html

3. CERT Listing of Computer Security Newsgroups and Electronic Mailing Lists
   http://www.cert.org/other_sources/usenet.html

4. SecurityFocus Listing of Computer Security Electronic Mailing Lists
   http://securityfocus.com/