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 (Security 401)"
at http://www.giac.org/registration/gsec

Full Name: Paul Claxton

Course/Certification: Security Essentials Courses (expanded/six day course).

This is an original submission.

Descriptive title: "*Violations of basic computer security principles within the television broadcast community and some suggested solutions.*"

I participated in the SANS Security Boot Camp in San Diego in October.

© SANS Institute 2000 - 2002, Author retains full rights.

Violations of basic computer security principles within the television broadcast community and some suggested solutions.

By Paul Claxton

Abstract.

Both the television industry and their equipment vendors must take a more active roll in securing computer equipment in the broadcast television industry.

Introduction.

The television broadcast industry has embraced computer technology as a way to reduce human errors though automation and lower labor costs at a time when computer hacker activity is at an all time high.

Network security can be a daunting task with ever-changing physical and logical topology advancements. Those in charge of television facilities tend to be broadcast engineers with little to no computer security administration experience or training. A factor that compounds this issue is that vendors of equipment tend to hold tight control of equipment configurations blaming system failures on configuration changes made by equipment owners.

In the television industry time is money and corporate image is of paramount importance. Each minute of television programming lost can mean hundreds of thousands of dollars of lost revenue to a hacked television network. A hacked web site can destroy the efforts of a television facility to establish itself as a trusted and secure provider of information.

The ability to hack into computers use to require advanced knowledge, expensive equipment, and plenty of time. Recently hacking has entered a new era with slick interfaces and easy to use tools readily available on the internet for free that will allow anyone with even with a small amount of experience gain access to un-protected or weakly secured networks.

Common broadcast television computer network security vulnerabilities.

I. Shared and weak passwords are used by groups of engineers and operators. Combine that with the failure to log or audit computer use means that the principle of least privilege is often violated without documentation.

Passwords are the first line of defense for computer systems; logging and auditing user access validates that line of defense. “One of the most common problems on networks is simply accounts with weak passwords, or no password at all”[1]. Just because a network server is kept behind locked doors doesn’t mean a strong password isn’t needed. Often these servers are connected to the Internet via high speed T-1 or better lines allowing easy access by outside sources.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The use of common passwords used for various job functions sets a television station up for failure both by prohibiting the auditing of logs and preventing the trace of a stolen password. If separate log-on names and passwords are used an audit trail exists which can allow a particular problem to be traced back to an individual for additional training or corrective action. Additionally using common a log-on often gives privileges to those without a need for them or knowledge of how to properly use them. Senior engineers will share the same powerful log-on and privileges with junior technicians.

Complete and through logging should be used where computer network operating systems allow. The industry logs its television shows and commercials very completely and should do the same with the use of those computer programs that schedule these products for airing. Logs should be used to record system log-on and log-offs, both successful and unsuccessful attempts, and need to be reviewed on a weekly if not daily basis for unusual activity that might indicate an attempt to gain illegal access.

Users often choose weak or easy to remember passwords. A password assessment program can be used to crack users passwords to ensure that they are following policy. A good policy will state the complexity of the password to include length and character sets required, how often the password is required to be changed, how many old passwords are prohibited from being recycled, and a minimum password use length to prohibit users from cycling rapidly though new passwords back to their old one.

Biometrics, card readers, and security tokens have gained acceptance as their cost has dropped and their reliability has risen. These devices add to the security equation two addition factors: who you are and what you have to the what you know, the password. According to Maggie Biggs of InfoWorld, "For high-impact applications, you'll want to use a multi-layered approach that leverages ID and password constructs along with one or more authentication techniques. The authentication marketplace will meld together during the next couple of years and many of these authentication technologies will begin to be more interwoven into single solutions"[2]. Television video servers are certainly high-impact machines within the modern television plant and should be prime candidates for such dual authentication techniques.

Both secure cards and tokens are relatively easy to manage and control and pay for themselves in a number of months worth of use though reducing helpdesk calls to re-set expired or forgotten passwords. These devices can act as a very secure method of authentication and provide encryption too for field reporters and affiliates keeping important corporate business private across the public Internet. Most of these authentication applications support Windows 2000, ME, NT 4.0, and 95 and other operating systems like Novell's NDS, Solaris 2.6 and above and Linux providing a secure logon and automatic logoff procedure. They can be rolled out a little at a time securing one portion of the network at a time as funding becomes available.

II. Security though obscurity is rampant in the industry. Television broadcast equipment is connected to the plants information technology LAN, to the Internet, or via modem to the public telephone network without firewalls.

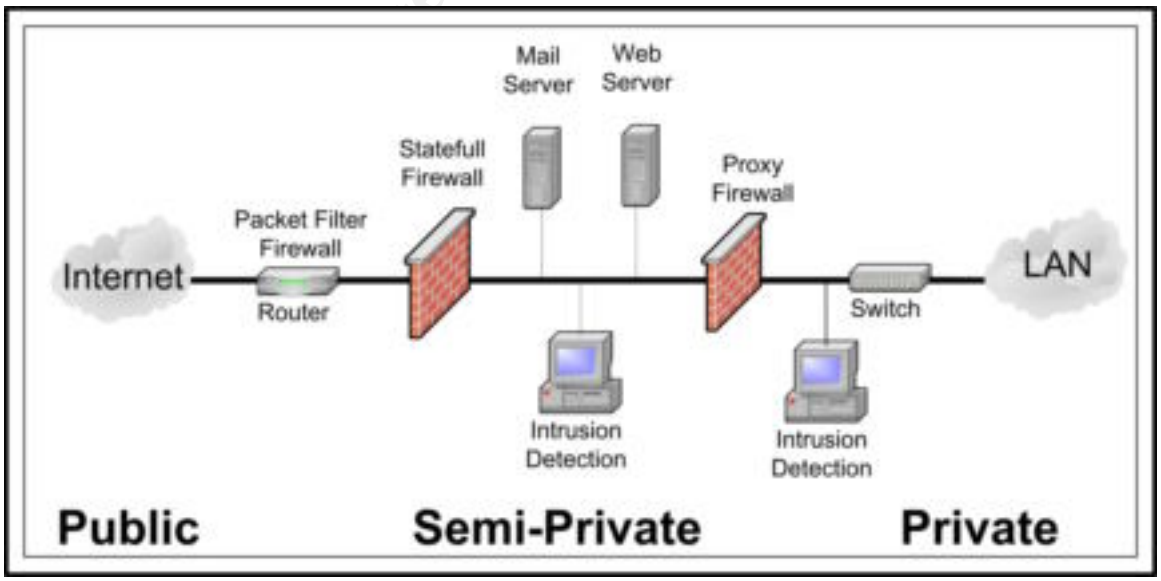
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Even a system that uses strong passwords can be broken into without much effort in a given length of time. The television industry typically has high-speed computers with huge storage space and fast T-1 and better connections to the Internet. These represent targets of prime interest to computer hackers. Computer espionage is also on the increase and corporate knowledge stored on Internet exposed computers is a tempting treat for a competitor or a hacker willing to sell that information to one. A firewall placed between a television facilities network and the Internet can enforce a security policy and at the same time obscure internal computers from outside electronic eyes.

Firewalls come in three primary types: packet filter firewalls, stateful packet inspection firewalls and finally application-level proxy firewalls. There are firewall applications that combine these functions into one or more machines.

Even a simple router that is used to connect the facilities internal network to the Internet can be programmed with some simple and effective rule sets that will prevent some common hacking methods. It makes sense to set up a set of packet filter firewall rules set that screen out anyone but trusted IP addresses from entry into the DMZ unless public access is required to a web or mail server. A list of affiliates IP addresses can be manually entered into the rule set screening out all others. It is possible to spoof IP addresses so the packet filter firewall isn't the only defense needed.

Stateful packet firewalls are typically computers with additional software programming that screens each packet coming and leaving a network for programmed characteristics. They are third generation devices designed to be aware of and inspect not only the packet being received but also the context of the connection. These firewalls build tables recording the current state of each connection though the firewall. There are various attacks that can by-pass stateful firewalls so yet another layer of defense is recommended.



Suggested firewall and intrusion detection system block level diagram
(Developed from notes on a presentation by Eric Cole)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

A proxy firewall acts as a go between taking internal computers requests and acting on them seeking the information from the Internet, which is then returned to the internal computer. This proxy hides or shields the IP and media access control addresses from external eyes. The advantage is without the IP address the outside hacker has a greater difficulty in exploiting and internal computer. An additional administrative advantage of using a proxy firewall is the ability to use network address translation to use free non-routable internal Internet addresses inside the firewall and present a routable Internet address to external networks. This can greatly save on the cost of leasing and managing routable legal Internet addresses.

Firewalls are only as effective as their rule set or programming. Often times inexperienced technicians set up a firewall with weaknesses that create exploitable holes though it. After a new firewall is installed it makes sense to have it tested by one or more third parties who will attempt to penetrate though it from the outside accessing its strengths and weaknesses. The technicians or vendor who installed the system should then be required to address and correct any found weaknesses. As Philip Brown states, "When it comes to firewalls, and security in general, paranoia isn't just a state of mind; It's a way of life! To sum it up: Trust no one. Trust nothing to work, unless you personally have seen it work.[3]"

To monitor the effectiveness of the firewalls additional computers with special software called intrusion detection systems (IDS) are employed within the protective boundaries of the DMZ, which is the area between the stateful packet inspection and proxy firewalls, and then again inside the internal network. See the figure on the previous page. An IDS system monitors the network looking for the signatures of a hacker's attack actions much like a virus scanner looks for virus signatures. The benefit of an IDS is that it will alert an administrator as an attack is in progress so that action can be taken often before damage can be done. They can be programmed to sound audio alarms and send emails and pager alerts when they detect an intruder on the network.

"Firewalls are extremely effective, they will keep the hacking masses at bay, but there are so many different ways to exploit network connections that no method is entirely secure. Many administrators mistakenly assume that once their firewall is online and shown to be effective, their security problem is gone. That's simply not true"[5]. Protecting the network from the Internet may require additional means of protection as modems represent yet another possible avenue of entry into what would otherwise be a secure network. Where needed modems should be disconnected between uses and never set to auto-answer an incoming call. Vendors will often need to call-in to a piece of broadcast equipment to make adjustments or install patches. If a modem line is disconnected between uses this requires the vendor to telephone an engineer to connect the modem. This not only protects the equipment but also serves to notify the engineer that the vendor is modifying or adjusting his equipment.

Finally an often-used method around the firewall is social engineering where people from within the network are exploited to assist a hacker into entering the network. IT people are often targeted and should be trained to handle attempts to obtain information about the LAN configuration and its security. All network users should receive training and continual updates on the latest virus, worm and hacker threats.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

III. Un-patched default installations. Television vendors are installing their software on default installations of operating systems and failing to install security patches.

Un-patched systems running Windows NT server or Windows 2000 server have a number of software bugs, which can allow for local promotion allowing a normal user to gain administrative access to a system. All operating systems are a living set of code and require periodic updates and security patches. According the SANS/FBI Top Twenty Internet Security Vulnerabilities:

> **"For operating systems, default installations nearly always include extraneous services and corresponding open ports. Attackers break into systems via these ports. In most cases the fewer ports you have open, the fewer avenues an attacker can use to compromise your network. For applications, default installations usually include unneeded sample programs or scripts.[5]"**

Television vendors are notorious for using un-patched default operating system installations often times leaving well known and published exploits uncorrected and leaving services and their ports running when not required.

Additionally when a television facility expresses security concerns to a vendor they more often than not fall upon deaf ears. To fix these delivered problems facilities must "[R]emove unnecessary software, turn off unneeded services, and close extraneous ports. This can be a tedious and time-consuming task.[6]" which is a job best done by the vendor's programmers or technicians. Vendors should be able to justify each and every software application left on a machine and have requirements for every protocol port left open and listening.

Fortunately there are many resources available giving guidance and step-by-step procedures for securing various operating systems. The Center for Internet Security has developed a consensus benchmark for the minimum-security configuration for the Solaris and Windows 2000 operating systems available at http://www.cisecurity.org. The SANS Institute publishes guides for Windows NT and 2000, Solaris, and Linux operating systems that can be purchased from http://www.sansstore.org/. The National Security Agency (NSA) has an unclassified guide called *"The 60 Minute Network Security Guide (First Steps Towards a Secure Network Environment)"* which was developed with Microsoft and the SANS institute and is available for free on the Internet at http://nsa1.www.conxion.com/ that covers general guidelines for Microsoft and Unix applications as well as providing some Cisco router rules for a filter packet firewall.

IV. Not using security policies. The use of a well thought out security policy would prevent initial damage and serve as a tool to mitigate ongoing damage.

A well-written security policy can serve to organize the efforts of a television networks affiliates and far reaching business units into a single secure network. Often it takes but one small overlooked exploit to gain control over a larger network of powerful and expensive computers.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

A security policy "Is a central document that describes in detail acceptable network activity and penalties for misuse. A security policy also provides a forum for identifying and clarifying security goals and objectives to the organization as a whole. A good security policy shows each employee how she is responsible for helping to maintain a secure environment.[7]" The security policy can serve as a guideline on how to carry-on day-to-day operations like virus scanning, intrusion detection, remote access, software patching, passwords and perform backup. It can also include a policy on how to deal with a security incident during and after an attack. The policy should be the result of a careful thought process that defines the acceptable methods of interacting with the network at all levels.

It is important to include all users of a network in the policy as the use of a virtual private network (VPN) spreads trust from one network to another. An intruder gaining entrance into one system at a trusted television network affiliate's location can use the VPN to gain trusted access into another network. The administrator must know how his network is configured and where potential points of access are.

Policies can be general enough to allow future ones to fill in the missing parts and the required detail that will allow them to become useful documents rather than just disregarded strategy statements. A good policy document must allow for a balance between security and accessibility to the tools that let people get their work done.

A corporate policy can also be a guideline for a project's design engineers as they solicit bids on a particular piece of equipment and for equipment vendors when the install equipment. Boilerplate language can be developed so that there is a uniform requirement set used across the entire system.

V. Un-tested backups represent a large hazard as often when a television facility does do backups of critical data or video projects they never test their restoration plan.

The television industry, like many others, relies heavily on computers to manage their business with databases and spreadsheets. In addition the creative products of television represent hundreds of man-hours of original work and are valuable, often irreplaceable assets. These products tend to be huge files that require lengthy back-up times that in too many cases aren't periodically tested for function as they require valuable production machines to be off-line for too long a period.

Many back-up systems include the ability to do a file-by-file comparison between the back-up media and the original source to verify the integrity of the back up. When available this feature should be used. Multimedia files tend to be several gigabytes in size and due to the slow nature of back-ups will often prohibit the ability to verify writes even with very fast tape media. In this case a facility needs to have a policy that routinely has a backup administration restore a project to manually verify that the system is functional. Written procedures need to be in place to guide even inexperienced administrators thought the restoration process as a missing backup administrator can represent a single point of failure.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The use of RAID disk drives is almost a given in video editors and multimedia storage. Whenever possible television facilities should use RAID 5, which provides striping and parity rather than just RAID 0, which is a striped disk array without fault tolerance. Some video editors come set as RAID 0 to gain the speed advantage of striping without the loss of hard drive capacity of the RAID 5 parity disk. The Advanced Computer and Networking Corporation has an excellent primer on RAID array types and their advantages and disadvantages that starts at http://www.acnc.com/04_01_00.html.

Conclusion

Securely managing an ever-changing broadcast television facility can be difficult at best but without unique logins with strong passwords, a well-built firewall set, patched operating system installations, a proper computer network security policy and functional backup the job becomes nearly impossible. The network manager needs to become fully aware of his computer network and its weaknesses and prepare defense in depth to counter the ever-growing threat against it. Television equipment vendors also need to become proactive and provide secure computer systems to television facilities and include security updates in their maintenance.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Notes

1. Scott Blake and Chris Wilburn, white paper *"Top 10 Security Threats for Windows 2000 and Active Directory"*.

2. Maggie Biggs, **"***Fraud, Negative ROI to lead businesses to embrace emerging biometric techniques"* http://www.infoworld.com/articles/op/xml/00/08/07/000807opbiggs.xml

3. Philip Brown *"Free Firewall Configuration Guide"* http://www.bolthole.com/solaris/firewall.html#firewalltypes

4. Mathew Strebe and Charles Perkins, *"Firewalls 24Seven"* (Alameda CA : Sybex), 17.

5. SANS Institute and the National Infrastructure Protection Center (NIPC), *"The Twenty Most Critical Internet Security Vulnerabilities (Updated) The Experts' Consensus"*: Version 2.501 November 15, 2001. http://www.sans.org/top20.htm

6. Ibid.

7. Chris Brown with Cameron Hunt, "*Active Defense. A Comprehensive Guide to Network Security"* (Alameda CA: Sybex), 27.

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.