GIAC Security Essentials Certification (GSEC)
Practical Assignment
Version 1.4 (amended April 8, 2002)

Title: It looks pretty, but is it secure?
Tim Tinnel
July 28, 2002

Introduction

I was recently hired as the IT Director for a mid-sized company with several remote locations located across the United States. I was quite impressed with the variety of technologies deployed within the organization and the apparent depth of redundancy, physical and logical security, backup strategies, and overall system integrity. Most of this initial "honeymoon" period dissolved during my first security audit.

This paper is an attempt to describe the reality under the façade without specifically damaging any vendors or individuals whose good intentions created many of the internal and external vulnerabilities. During our search for good defense in depth, any weakness found and reinforced could prevent a potential exploit within a given threat vector. This paper is not to be used as a checklist for securing your company's network, but is an attempt to share my success and failure as an IT professional attempting to improve each layer of defense within our organization.

Before

Our corporation needed to be able to provide certain services to internal and external customers. The services were being provided, but were done so in a manner that created many security concerns. Our headquarters was moved just prior to my employment. A few of the key servers remained at the previous headquarters. This physical distance between facilities containing production servers made it interesting to perform sufficient auditing.

Functional separation of servers

A single server at our previous headquarters held mail, proxy, and print services. A single attack or failure on this machine could have prevented corporate Internet access, internal and external corporate e-mail, and the ability to print within that facility. The server was configured for both remote and local management via a popular remote control software package. The version and defaults of the software used did not use encryption, leaving usernames and passwords to be transmitted in clear text. This would make it trivial for anyone capable of running a sniffer to grab account information from any user providing remote support to this server.

Separation of duties and least privilege access

Many key IT personnel within the organization had privileges well beyond what was required for them to perform their duties. This was a disaster waiting to happen. Knowledge of a cycling administrative password list alone caused me to cringe, but so many people had so much access it was no wonder that password anonymity was not held sacred. Too many people thought they had the need to unlock accounts or create users, change passwords, etc. As I mentioned in the introduction, my honeymoon was now over.

Social engineering

Having facilities distributed across the United States, but support centrally located at our headquarters opened up opportunity for potential social engineering. Our company, like most, experiences a fairly high degree of turnover. This turnover presented situations where users would call in and request accounts to be unlocked, or even created! Upon request, a user could get an account with user privileges with a simple phone call and the name of a center's manager to use to push through the request.

Virus Protection

There are over 350 computers within our organization and although we had purchased sufficient licenses of a commercial virus-scanning product, it was poorly deployed and rarely updated. Out of the 350 computers, approximately seventy five percent of them had the virus-scanning product installed. Of those with the virus-scanning product installed, less than a quarter of them were receiving updated virus definitions on at least a weekly basis.

Not a single server was set up with a virus-scanning product nor were any data directories being routinely scanned. No e-mail entering the company was scanned for infection or screened for potentially dangerous executables. Employees were openly mailing "joke" executables to each other and hence training our entire workforce to click on anything without any regard for whom it might be from or what it might contain.

Modems

Many users had to be able to connect to their computers remotely in order to track performance, check e-mail, etc. The general practice was to install modems in their computers and allow access through a separate modem extension within our PBX. Often, these modems would directly be set to auto answer and auto connect to the remote access software without any access controls. At least the normal war dialer would not detect the modems, since they were hidden behind a central access number, but if the access number were known, then it was simply a matter of attempting all four-digit permutations that made up our extensions.

No Firewall (or DMZ)

We had deployed our FTP, proxy, e-mail, and web services on a single server. This server was multihomed, both a part of our network with its private IP address and directly attached to the Internet with its public IP address. Although this hid the identity of internal Internet users behind the proxy, it allowed direct access to our network upon breach of the proxy server, ftp server, mail server, or web server. Successfully attacking any vulnerability on any of these services could allow a complete breach of our network.

Open network shares

Five production file servers had sensitive data shared out. The shares were wide open allowing anyone with a valid network login to map the drives and access the data. Successful external attacks that might have breached our network would have allowed a

During

It was quite a challenge to demonstrate that all of the security risks previously described were worthy of expending time and money to address. I had some help to this end in that many of our customers were becoming more sophisticated in addressing privacy and security issues with their vendors. Many of our customers began auditing our infrastructure and although no single audit encompassed all of the issues we had discovered, cumulatively, they were able to uncover many of our deficiencies. Every customer had their own standards and our goal was to find the greatest, not least, common denominator among all of the requirements. The following represents a portion of those requirements.

Functional separation of servers

Several decisions were made that affected the location and function of our company's production servers. All production servers were relocated to our headquarters. Our network utilized dedicated point-to-point network topology to connect all of our call centers to our central headquarters, so this change was fairly simple to implement. We orchestrated the purchase of a new mail server, proxy server, FTP server and two web servers to correspond with the move. This allowed the services to run on individual, separate servers that were each hardened and tuned for their specific purpose. The FTP and web servers were placed within a newly created DMZ. The following section on "No firewall or DMZ" addresses the specific changes made.

Separation of duties and least privilege access

Meetings were held with each department in order to determine what resources were required by each group. It was predetermined that many groups would want much more access than they may have needed, so it was decided that the ultimate decision would be negotiated between the IT Director and each department head. Each group had their own requirements as well as requirements that overlapped other group's requirements. At this point, many access groups were developed so that every employee fit within one or more groups. Each group had its associated file and resource permissions mapped out and we were pleased with our efforts. We soon discovered this was the easiest part of the process.

Now came a daunting task. We needed to take all of the gathered information and make the proper resource and file permission changes described by our newly formed groups. Each production server's file structure was mapped out allowing all file directories to be fully described by group and access right allowed to group. The implementation did not come without its problems. Although we felt we had sufficiently projected all permissions properly, we found file directories that were too restrictive and had to change them to reflect the proper level of access and others that were granted too much control and they had to have privileges reduced or eliminated all together. I guess that happens when it is left up to the IT Director and department heads to formulate your access policies!

Social Engineering

This change was the most difficult one to get our arms around. When dealing with people and their desire to help others or at least show others that they have the "power" to affect change, things can get messy. We have an environment and customer base that requires that all changes be done swiftly. This had created the reactionary environment that so easily allowed social engineering to be used. Our first order of business was to determine procedures that had to be followed in order to change passwords, create accounts, unlock accounts, etc. These changes then had to be enforced and audited. Although I cannot say that we are following all of the procedures all of the time, we have placed seed calls to determine if the procedures would be followed, and have educated our administrators in the process.

Virus Protection

Since we had already selected and purchased licensing for an enterprise wide virus-scanning solution, it now became a matter of how we were to implement that solution in a way that allowed it to be verified. We knew that there were several options ranging from the very manual process of having technicians or administrators travel onsite to each facility and set up the software and its policies all the way up to the built in policy management software which had the capability to monitor engine version and virus definition files. We finally decided upon a hybrid solution. I had hired a regional system administrator for the facilities located furthest from our headquarters. His first order of business was to install the virus-scanning product with the agreed upon configuration on each of the workstations at the remote facilities and setting administrator only rights for any changes or for stopping the scanning engine. Each installation was set up to check for updates on an internal file server once a day. The file server was updated with all definition file updates and engine upgrades automatically as they became available. The remaining facilities and our headquarters were similarly verified, updated where necessary and pointed to the internal file server for updates and upgrades.

While the workstations were being configured for virus protection, my attention turned to our servers. Each server was configured with the server installation of the virus-scanning program. Our mail server was the most challenging as we also set it up to warn us of all mail it encountered which possessed an infected file. Every e-mail that contained a virus would generate an internal mail message to the administration group. Although this might be used against us by someone to flood us with infected e-mail designed to keep us busy while performing some other attack, it has allowed us to quickly respond to large scale virus attacks as they are happening and warn users and in some cases the unwitting persons used to send the infected mail.

Modems

All modems were determined to be unnecessary with the exception of an emergency backup modem to be used in the event we lose T1 access or our ISP failed. It was determined that anyone who had the need for remote access would have to work through our newly integrated VPN. The VPN was a part of the firewall package that will be discussed in the next section. The backup modem was located on a data processing machine housed in a limited access area. This would allow the modem to only be activated in emergencies and even then it would only serve to send data files to our partners. It was placed on an analog line independent of our PBX, but placed on a switched port that allows it to be turned on only when necessary.

Knowing that removing a modem but leaving the extension intact was not going to keep people from adding their own modem, we physically removed all analog phone lines at the terminating blocks of our PBX. This added another layer of defense against unauthorized modems being added to computers connected to our network. Even if someone were to add the modem hardware to their computer, they would have no easy way to connect to an analog line.

No firewall (or DMZ)

Firewalls are not a panacea that will cure all the security ailments of a network. Not having a properly configured firewall, however, is a disaster waiting to happen. We compiled a list of firewall requirements that we used to determine which firewall product or suite would be appropriate for our business.

Firewall appliance – We reviewed white papers on several firewall products and suites and it was decided to go with a firewall appliance. A firewall appliance is a hardware-based firewall. We had very little in-house security expertise so it made sense for us to choose a firewall product that was aimed at lowered administration overhead. It was determined that a firewall appliance gave us a low-cost solution where all hardening was performed by the firewall vendor. A firewall appliance usually has a single WAN port. This port allows the appliance to connect an entire network to the Internet through the use of a single public IP address. The appliance will normally also have a LAN port for connecting the internal network and another port designated as the DMZ allowing the creation of a DMZ for public services. I'll address the DMZ and LAN requirements shortly.

Patching and updating – We understood that it was very difficult for a network administrator to split their time between local administrative tasks and keeping our network secure through the researching of available patches and necessary hardware reconfiguration. We liked how virus-scanning software provided automated updates and looked for a firewall appliance that had similar features.

URL filtering – Our corporate philosophy was not to eliminate the ability of our employees to gain Internet access for web surfing. Our philosophy was to use some common sense in what web surfing we were allowing through a decent content filtering device. Content filtering allows an administrator to enforce web surfing policies by eliminating access to web sites based upon the type of content they provide. For example, if a site is a known pornography or gambling site, it is either already listed in or can be added to a database of blocked sites based upon its known content. We wanted the flexibility to block content by assigning content filtering rules to either specific groups or even specific users.

Virtual Private Networking (VPN) – As mentioned earlier in the paper, it was our desire to remove all modem access. Removing all modem access, however, created a new problem that had to be solved. Our employees still needed a way to access network resources remotely. Our solution was to purchase a firewall appliance that included VPN functionality. The VPN had to provide sufficient authentication and acceptable encryption/decryption schemes. Minimally, we wanted to use triple-DES encryption and digital certificate authentication through a trusted CA. The details behind the authentication and encryption algorithms are beyond the scope of this paper but had to be examined when determining a solution that provided secure communication. As my GIAC training has shown me, what we were looking for was the ability to maintain confidentiality, integrity, authentication, and non-repudiation in the presence of adversaries.

Another requirement for the VPN was to allow grouping of access rights for VPN users so that we could support our least privilege access policy for remote users. We wanted to do this separately from our network rights, so that we could refuse certain individuals the right to access certain network resources once establishing a VPN connection. The biggest challenge was determining who needed what remote access and why it was a good idea to give it to them. This was a point of contention between our newly security sensitized network administrators and the user community. Business rules had to be examined and in some cases redefined in order to provide the right access to the right people while limiting access to people who did not have a business need to remotely access the network.

Open network share

This was an embarrassment and posed tremendous risk. We could not validate the integrity of our client data if every network user has access to modify or delete the data. The information gathered during our discussions on separation of duties and least privilege access allowed us to determine who needed access to what file directories. Armed with this information, we worked to lock down the shares. We chose to apply the least privilege access rules to our file directories. This was quite a cultural change for our users and was second only to our removal of modems in creating negative feedback. Although limiting access and privilege proved itself out over time, I was called into many meetings to defend the action.

Network Intrusion Detection

Probably the single most important tool in the arsenal for information security is one that provides the ability to detect what people are doing on or to your network. We were flying blind. We had loose logging of network related events on our servers, but these were to track the success or failure of logon attempts, application errors, etc. The network traffic itself was not in our line of site.

There were a variety of network intrusion detection architectures from which we could choose. We examined managed intrusion detection services that allowed, at a considerable expense, a third party service provider to act as the watchdog for network intrusion. They would provide hardware and software based detection that checked traffic against known exploit patterns and report any alarms to a contact list with fixed escalation procedures. Although this sounded like a great way to achieve the desired monitoring without the need for internal expertise, it was cost prohibitive and even somewhat frightening. Since they were supplying a service to us and many other clients, it seemed logical that a single, well directed attack on the management provider would have allowed the attacker access to every client they were managing. Although this might seem like a case of paranoia, I was starting to feel that part of an IT professional's job was to hold a healthy case of paranoia toward their systems and networks.

We decided against a managed solution, but did not give up entirely on network based intrusion detection. Although it lacked the ability to sufficiently track insiders, it would allow us to at least begin to acquire information on what traffic was getting to our firewall. As learned in my GIAC training, most attacks come form the Internet. Even though insider attacks could cause us more damage because of the unique knowledge possessed by the insider, we felt that our biggest threat would probably come from outside of our network.

The decision was then made to create two network intrusion detection systems. One intrusion detection system (IDS) was placed in our DMZ to watch network traffic heading for our web and ftp servers. The other IDS was placed just inside our firewall to watch for traffic coming in and out of our network. Standard rules files were set up and modified for our specific network needs. The systems were placed on hardened operating systems with only the services necessary to allow the IDS to function and log traffic.

After

Functional separation of servers

We are not completely satisfied with our efforts to use separate servers for providing separate services. Although we have our web and FTP servers on separate hardware platforms in our DMZ, we still have a single e-mail server on our LAN. We are now looking at how we can push the external mail services into the DMZ and distribute the mail services between two servers. Internally, our domain controllers still provide functionality beyond the role of a domain controller and print servers provide functionality beyond the role of print servers.

Separation of duties and least privilege access

Much was learned through the creation of policies to address these issues. The added benefit of separating duties was that it allowed the management team the opportunity to look at the boundaries that made up our positions themselves. Rethinking why we had people doing certain things allowed us to further redefine positions and their respective duties. It was decided that a quarterly review of whom we had doing what would benefit us all.

Least privilege access had already demonstrated its worth. A certain unnamed user decided that they would clean out "their" files and reported to our help desk that they were unable to delete certain files. Upon further inspection, they were attempting to delete a mapped drive containing client reports. In our old environment, we would have been scrambling to pull up our most recent backups!

Social Engineering

We continue to educate our users and administrators on social engineering ploys to gain privileged information or access. Our seed calls continue to provide opportunities for education and occasional reprimand.

Virus Protection

Although there is no protection against every possible infection, just as there is no silver bullet for securing your network, our users are better protected against themselves and others. We have used available tools to maintain a database of all engine and virus definition file on all of our hosts. We now have 100% of our hosts and servers being scanned for virus signatures. All systems are checking for updates to the virus definitions on a daily basis against the updated copy on our file server. But the biggest difference has been the education of our users. Where we used to have executables past among workers, we now have blocked executables within our mail system and have educated users to not click on everything they receive. We continue to protect, but the education will help prevent future, yet unknown virus threat vectors.

Modems

Our users have become accustomed to their new “modemless” workplace. We began reimbursing for home, high-speed networks that allow users to remotely access network resources at home. We have also provided hardware and software based firewall products for home users to help defend against attackers exploiting the trust relationship.

No Firewall (or DMZ)

We had begun our rule set creation by determining what ports and services we wanted to block. This method was a complete failure. We were ill equipped to identify all potentially dangerous services and their respective ports. Once again, we fell back to the tried and true principle of least privilege access. We denied everything and only opened up services and ports that were necessary for our daily business operations.

Network Intrusion Detection

I have become both amazed and frightened by the data gathered by our IDS. Part of our decision to change our firewall policy was the results found through our IDS. Logging information from the firewall and comparing it to the IDS logs has become a full time job for one of our network administrators. His new job is to do all of my worrying. He and I are both going to attend the SANS Intrusion Detection in Depth training. We are beginning to believe that a hybrid network and host based IDS is a better way of gathering information about our network traffic.

Summary

If I have learned anything, it is that securing my network is a multiple layered problem whose layers seem to get more and more complex every day. Every day, new exploits are found for my network. Every day, a new virus is created to harm or allow harm to my network. Every day, the rules of the security game change. I am just glad that there are others in the battle with us whose career it is to educate us to better address the threat vectors at various depths within our networks.

Bibliography

"PcAnywhere weak password encryption"
URL: http://www.securiteam.com/windowsntfocus/5YQ0H000DY.html

"Securing the Corporate Network: An Enterprise Approach to User Authentication"
URL:
http://www.csu.edu.au/special/auugwww96/proceedings/mcquilken/network.html

Alberts, Christopher J.; Dorofee, Audrey J.:"OCTAVE Criteria, Version 2.0"
URL: http://www.cert.org/archive/pdf/01tr016.pdf

Avolio, Frederick M.: "Best Practices in Network Security"
URL: http://www.networkcomputing.com/1105/1105f2.html

Granger, Sarah: "Social Engineering Fundamentals, Part I: Hacker Tactics"
URL: http://online.securityfocus.com/infocus/1527

Granger, Sarah: "Social Engineering Fundamentals, Part II: Combat Strategies"
URL: http://online.securityfocus.com/infocus/1533

Wreski, Dave & Pallack, Christopher: "Network Intrusion Detection Using Snort"
URL: http://www.linuxsecurity.com/feature_stories/feature_story-49.html