Global Information Assurance Certification Paper

Where Did All My Bandwidth Go? -

A lesson learned in Windows NT 4.0 Security based upon the exploit of an incorrectly configured FTP server

Todd Thompson
June 18, 2001

Introduction

In our society today, where hackers seem to have nothing better to do than find weaknesses in computer systems and exploit those weaknesses, proper cyber security is a must. It is amazing how fast the priority of cyber security will rise when a security event happens in your company. As I read news articles and reports from the security industry, it seems to me that cyber security, which once took a back seat to just about everything else in a corporation, is on its way up the priority ladder. With every email virus that spreads across the Internet and/or the corporate network, with every hacker exploit of a major computer system, business CEOs are becoming more and more aware of the risks involved with putting cyber security at the bottom of the agenda.

This paper will deal with the challenge of cyber security on an FTP server running Microsoft Windows NT 4.0 and Microsoft Internet Information Server (IIS) with regard to proper permissions on User Accounts and Folders. I will explain an exploit that occurred on an FTP Server at my company, the effect it had on our system, the weaknesses that were identified, and the solution that was implemented. I will then explain how the entire exploit could have been avoided in the first place by applying the following philosophy:

1. **Know Your System** – The need to have detailed information about your network to define a baseline so that you are able to identify events that are not "normal" for your system when those events occur.
2. **Principal of Least Privilege** – Only give users the access privileges they need to perform their job function.
3. **Defense In Depth** – The need to have multiple layers of security measures in place to slow down, and hopefully stop, would-be-hackers from penetrating your system.
4. **Prevention is Ideal, but Detection is a Must** – The need to focus on cyber security in terms of prevention and implementing Defense in Depth, but realizing that the detection of a hacker or intruder is imperative to the safety of your system.

A positive outcome from this exploit was that a position was created in the company to directly handle all cyber security matters. This is the position that I hold. Admitting that your company was not only vulnerable to an attack, but suffered because of an attack, is a bitter pill to swallow. I do this in the hopes that others in our field might take this information, apply it to their systems and learn from my company's mistakes.

The Exploit

It all started with a heavy load being experienced on our T-1 connection for more than a week. This was causing a problem with the daily workings of our mainline systems directly affecting our customers. Our support desk operators were fielding continuous calls from upset customers. The first assumption was that our staff was using the bandwidth for non-business related activities such as audio and/or video streams from the Internet. Notification was sent to all employees directing them to immediately cease all non-business streaming processes and usage on their computers. After this directive to our employees we noticed a reduction in bandwidth usage, but the utilization rate was still very, very high and the detrimental effect on our system continued. The question was raised, "Where did all of our bandwidth go?"

At this point in the crisis, we decided to capture packets to try and determine the cause. We quickly found that nearly all of the traffic was of an FTP nature. We then looked at the FTP server and found that there were a few Folders that did not belong on that system. These Folders contained files that did not belong on our system. Along with the added directories we noticed that 75% of the traffic to the FTP server was coming from two IP addresses from a foreign source. We quickly entered into an information-gathering mode and saved all of the data and logs.

We were now pretty sure that we had been hacked and that the hacker(s) were using our bandwidth and FTP server to perform some function. Upon further inspection of our packet-capturing tool log, we quickly realized that the hacker(s) were copying game files to the FTP server. We decided to watch and gather data for a period of time, about 16 hours. During this time the hacker(s) succeeded in copying 2.75GB worth of interactive game files to the Folders they had created on the FTP server. We logged IP addresses from all over the world that were connecting to our FTP server and interacting with the game data files. At this point we unplugged the ethernet cable from the server and removed the Folders and files that did not belong on the system. We noticed that the "Anonymous" user account had sufficient rights to create Folders and upload files in one particular Folder. We had thought that Folder permissions on the system had been set so that only an administrator could add Folders. The permissions for the Folder in question were changed and the system was brought back online after a 12-hour downtime.

A report was filed with the National Infrastructure Protection Center (NIPC). The NIPC's role is to assist with law enforcement investigation into cyber attacks and perform other functions that deal with notification of cyber security threats and vulnerabilities. The hacker(s) quickly ascertained that we were on to them and did not resume their unauthorized use of the system. After examining the log files for the FTP server and our Firewall, we found that the FTP server was not compromised in any way except for the addition and further use of the Folders and game files. The first thing we quickly realized from this experience was that we were extremely lucky to have only

suffered a loss of bandwidth and disk space. Because of this incident a new focus was put on cyber security and the importance of protecting our data assets.

The Effect

My company has real-time processes running that our customers use to make time critical decisions. These processes travel over the Internet via our T-1 circuit. A major loss of capital can be realized if these processes are interrupted. When this exploit occurred, these real-time processes were adversely affected and caused problems with our processes. Data could not flow in a timely fashion causing a massive amount of phone calls to our Operations' Center to have our system operator's manually supply this data to our members. Along with the real-time data problem was the fact that Email was working sporadically due to the T-1 circuit congestion.

The Weakness

During this event many weaknesses were identified. Some we already knew about, but others took us by surprise. To name a few:

- FTP server directly exposed to the Internet with little security protection.
- User Account "Anonymous" with inappropriate permissions.
- Folders with inappropriate permissions.

We already knew that the FTP server was at risk, but the data stored on the server was not of a sensitive nature, therefore stringent security was not considered a high priority.

The Solution

At the time of this exploit the solution was to:

- Capture as much data as possible in a short period of time to use later, if need be, in litigation.
- Remove the system from the Internet by severing the network connection.
- Evaluate and correct Folder permissions on server.
- Remove additional Folders and files created by the hacker(s).
- Leave the system offline for twelve hours.
- Submit formal report to NIPC.
- Notify all employees of the correct procedure to add directories and set permissions on the FTP server.

This was all that was done to fix the problem.

Avoiding the Whole Problem

As you can see from the explanation of this exploit, there is so much that could have been done to prevent this attack from happening in the first place. I am going to focus on the philosophy of "Know Your System", "Principal of Least Privilege", "Defense in Depth", and "Prevention is Ideal, but Detection is a Must", because I believe that there is something to be learned from these four corner posts of the security thought process, especially when it comes to this particular exploit.

1. Know Your System

We must know everything about the systems we administrate in order to recognize if something is not within normal system operation. If we do not know our system's normal mode of operation, then we leave ourselves open to malicious behavior by external, and sometimes internal, forces without even knowing that anything is going on. In the example of this exploit, we should have recognized that something was going on much sooner than we did.

To know our system we should have created a detailed network diagram containing information such as Computer Name, IP Address, Location, Operating System (version and patch level), Software (version and patch level), and other important system details. Knowing that our system changes frequently, this diagram should have been updated as soon as any change took place. This diagram should have been in existence before this attack occurred, but it did not.

We should have created a baseline of the computer system health using log files and other pieces of information in order to have something to compare any suspicious behavior against in order to determine validity.

We should have been examining the log files our various systems create to gain insight as to the health of the system. If we had been looking at the FTP server log files on a regular basis, we would have noticed something was not right rather than finding out after a loss of service.

Before we leave this section I would like to add something that I think fits right in with the topic: Security patches are not an option, but a necessity! Vendors make security patches for a reason: To fix vulnerabilities that are found with their products. These patches are freely available and we should be downloading and applying them soon after they become available. Apparently the implementation of security patch(es) seems to be a huge problem with system administrators. Too many vulnerabilities exploited by hackers could easily be avoided if system administrators will apply the

existing security patche(s) for the given vulnerability. We also must not forget to update our network diagram when we apply a security patch.

These are just a few steps that should aid you in Knowing Your System. The more information you can gather and store regarding your system and how it works, the more prepared you will be in the event of malicious activity on your system.

2. Principal of Least Privilege

We cannot have users on our systems that have more access rights and permissions than what is needed to do their jobs. As you can see from this exploit, a user had the incorrect rights to add a directory to the FTP server and the "Anonymous" account had rights to create directories and upload files. By not applying this portion of the philosophy, we left ourselves open for this attack.

Not all users are created equal in the eyes of the system administrator. Not everyone needs rights to everything on the network. This is why we create groups and have the options to select the appropriate permissions for a given user, regardless of the operating system.

We should have spent more time documenting the users on the FTP server and what their access rights and permissions were. We should have tested the "Anonymous" login to see just what you could do on the system from this account. I could even make the argument for not even having the "Anonymous" account enabled and supplying all of our members a login and password. This would have lessened the chance of an exploit occurring.

Just remember that users only need to have permissions necessary to perform their job function. This may require more time to accomplish, but it will be time well spent.

3. Defense in Depth

Multiple layers of network security defenses are critical in today's cyber world. Simple login and password protection is no longer sufficient to protect our systems from potential hackers and malicious users. In this area of the security philosophy we seemed to do a semi-decent job when this exploit occurred. The hacker(s) did not make it through our firewall and our internal systems were not compromised. The question that comes to my mind though is "Did the hacker(s) even try?". It appears that all he/she wanted to do was copy games to a repository for friends to play over the Internet. Another question that causes even more concern than the first is "Would we have even known that the system had been compromised?".

Multiple layers of security defenses include Firewalls, Intruder Detection Systems (IDS), Virtual Private Networks (VPN), Log Analyzers, Policies, Strong Login and Password

Scheme, Logon Warning Message, etc. The first layer of defense should be the perimeter of the network; this is where we apply Firewalls and IDS systems for protection. Applying these tools in combination with one another provides good Defense in Depth. An example of Defense in Depth would be to have multiple fences around your home.

Having our FTP server directly connected to the Internet was just not a wise decision. We had a firewall for perimeter security, why not put the FTP server on a Demilitarized Zone (DMZ) or Service Network connected to the firewall? The reason I found for this decision was that the data on the server was not of a critical nature, therefore it really did not matter if the server was compromised. As we see from the exploit, this proved to be a very wrong assumption.

Remember that one level of cyber security defense is no longer enough to protect your network. Implementing multiple layers of defense is required to provide stumbling blocks for potential hackers and malicious users to, hopefully, ward off an attack.

4. Prevention is Ideal, but Detection is a Must

Putting measures in place to prevent an attack is ideal, but detecting when a hacker or malicious user has compromised our systems is definitely a must. The damage that a hacker can accomplish in a reasonably short period of time is amazing. Our exploit was not recognized right away and caused some major problems for my company. If we had an Intruder Detection System in place and on the correct network segment at the time of the attack, we might have noticed the attack when it first started and headed it off before it became such a big issue.

We can implement a strong perimeter on our networks, but nothing is totally impenetrable. If and when a hacker makes his/her way into our system, we need to have measures in place to notify us immediately to take action. A well-designed system may take action automatically. We do not want to let a hacker roam free in our network to do as he/she wishes. The attack must be identified and stopped as soon as possible.

Not only are IDS systems necessary tools, but examination of the log files that are supplied by our systems is also a must. There are tools available to help in log file analysis and these tools can be easily obtained from the Internet.

Incident Handling

One thing that is not covered in this philosophy is the issue of Incident Handling. It is vital for security administrators to know how to react in the event of an attack. When this exploit occurred and was finally made known, the network administrators at the company responded quickly and with due diligence to find the problem and correct it. Was the problem handled correctly? Probably not, but there had been no training in

Incident Handling. The task was performed as well as to be expected without the proper training.

Are there predetermined ways to handle an attack? Are there certain steps to follow during an attack? The answer to these questions is "yes". The SANS Institute has a course of study on the topic of Incident Handling and a useful document, "Computer Security Incident Handling: Step-by-Step", that talks about handling an incident when it occurs. It also explains the ten emergency steps to follow in the heat of an attack.

The ten steps are as follows:

1) Remain Calm
2) Take Good Notes
3) Notify the Right People and Get Help
4) Enforce a "Need to Know" Policy
5) Use Out of Band Communications
6) Contain the Problem
7) Make a Backup of the Affected System as Soon as Practical
8) Get Rid of the Problem
9) Get Back in Business
10) Learn From This Experience

As you can see from this list, our exploit was handled reasonably well, but could have been handled better with the correct knowledge and training.

Closing Remarks

As I have previously stated, giving this level of detail about an actual exploit at one's place of business is not an easy thing to do. I came to the realization that in order for security administrators to learn and become better at the job of protecting their networks, we need to be open about these events. These issues are called "lessons learned". We learned a lesson from our exploit, and I hope that by reading this paper you will have too.

References:

National Infrastructure Protection Center (NIPC)
URL: http://www.nipc.gov

Mark Joseph Edwards, "Patching Security Holes: Don't Put It Off" (January 31,2001)
URL: http://www.windowsitsecurity.com/Articles/Index.cfm?ArticleID=19816

The SANS Institute, "Windows NT Security Step by Step" (2000 - 2001)
Many Authors

Brian McKenney, "Defense in Depth" (February 2001)
URL: http://www.mitre.org/pubs/edge/february_01/mckenney.htm

The SANS Institute, "Computer System Incident Handling: Step-by-Step" (1999 - 2001)
Many Authors