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

I Think Our Internet Connection is down

Raymond Hillen III
SANS GIAC
Practical Version 1.2e

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

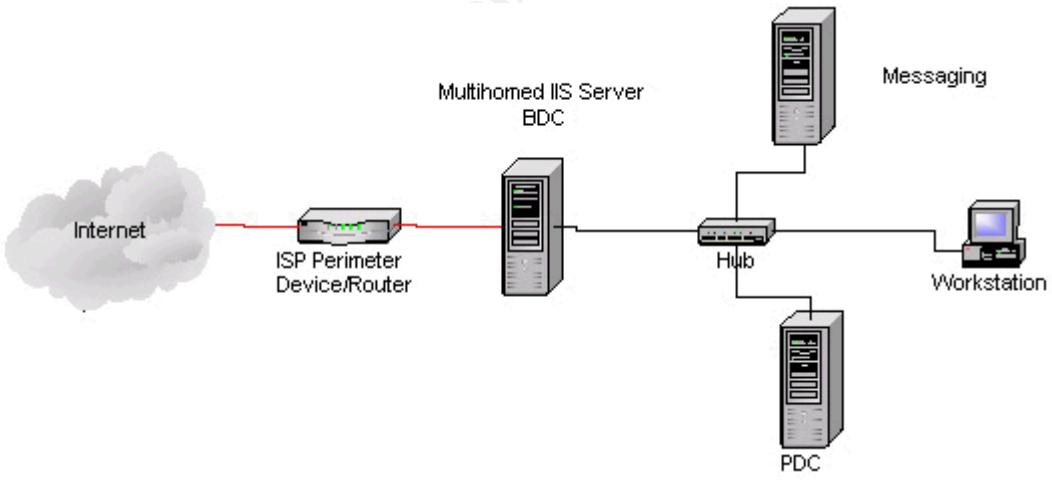
Introduction

Too often, managerial staff of small sized businesses does not take security seriously. Common statements range from "We don't have data of any value", "We're too small for anyone to bother with", "Our competitors wouldn't do something like that", to "We don't have any proprietary information to protect".

The problem seems to stem from a misunderstanding of how their resources could be violated and used. A common misconception is that hackers only go after the "big fish". Not much thought is given to the idea that their resources may be used for things other than launching a nuclear missile.

The following is a "case analysis" of a real incident that was uncovered while trying to assist a small company with a supposed "down" Internet connection. The particular organization published a few specialized magazines and did not have a full time trained technical staff.

The environment consisted of 3 servers, one of which was a multi-homed system running MS Proxy Server (This requires Internet Information Server) that was also configured as a Backup Domain Controller (BDC). The connection to the Internet was provided by a small ILEC that utilized a device that had routing capabilities to provide the connection to the Public Network.



Situation

Day 1: Received a call from the main point of contact stating that their Internet connection seemed to be down. It had been slowing down over the last week, but now e-mail and web browsing were not functioning properly. Had the contact try a few troubleshooting procedures to include pings, dns queries and rebooting the Proxy server. Erratic behavior was observed on all traffic to Internet. I was able to receive a response

© SANS Institute 2000 - 2005 Author retains full rights.

from their mail server when telneting to port 25, but there appeared to be a high degree of latency. Eventually all communications with public network ceased.

Day 2: On site to troubleshoot Internet connection and learned that the provider was experiencing issues in local geographic area with all of it's customers. I attributed this to a "provider issue" and cycled the power on their perimeter device as directed by the providers technical support staff. Internet connection appeared to be functioning properly. All communications to public network reestablished. Sent and received several test e-mails to verify messaging system was working properly. Web browsing resumed at optimal performance.

As this issue was coming to an end and I was packing my things to move on to another client, complaints started again as to the web browsing performance. I immediately called the provider to inquire and was informed that all systems were working fine on their end. Something wasn't right.

Looking at the perimeter device, a multi-homed workgroup server that was running MS Proxy in what appeared to be a "default" configuration, I noticed a significant amount of ftp connections. Upon learning that this client had no ftp server needs and only used the proxy and web publishing features of Internet Information Server and MS Proxy, an alarm was triggered.

I immediately started viewing configuration information of the system. The partition that housed the web services seemed to be utilizing a significantly large amount disk space compared to the average implementation. The directory that housed the default web site was 2 gig in size. Upon expanding the subdirectories a labyrinth of folders, alphanumeric in nature, was discovered. This was beginning to get interesting. It took the better part of 30 minutes to discover the exact root of the ftp site. What was discovered at the root was quite interesting. Sub folders containing book titles, games, an unauthorized release of an Operating System, and a few utilities. This looked like a WAREZ site. I unplugged the connection to the Internet.

After inquiring with the main point of contact it was easy to see that they had no idea what was going on nor did they even know what a WAREZ type site was. I explained that warez was slang for pirated software and that there could be possible legal ramifications for being part of a distributions site. The fact that this company was unaware of its role would not necessarily be grounds for a defense. They had not taken the appropriate measures to restrict access to their resources.

Utilizing a small workgroup hub I connected my laptop on the outside in parallel with the perimeter system. Launching Ethereal, a free network protocol analyzer, I reconnected the proxy to the Internet and watched as a flood of traffic, ftp based connections, consumed the segment. The IP addresses were resolving to places in the United States, Canada, and many European countries. The amount of connection attempts increased at an exponential rate. Even though I had shut down the ftp services the connection

© SANS Institute 2000 - 2005 Author retains full rights.

attempts were still being made. I disconnected the Internet connection once again.

Placing a call to the provider, I asked that all ftp connections be blocked to this specific subnet. Once that was in place I reconnected the Proxy Server. Service appeared to be restored, but quickly fell back to its sluggish state. Another call to the provider revealed that some sort of "brute force" attempt was made to access the provider's perimeter device and they could no longer gain administrative access to it. I was instructed to cycle the power on their device in order to allow them access. They quickly placed an access list allowing only their network direct access to the perimeter device. Once these tasks had been accomplished, normal Internet access was restored. Continued monitoring via Ethereal showed no more ftp based connection attempts.

Briefing the main point of contact and a high level manager of the company was surprising. They were only concerned with the service aspect of the issue and any possible legal liabilities. Impressing upon him the need for implementing standard practices from a security standpoint they still were uninterested in utilizing any more time or money in this area.

I quickly documented what had taken place and removed all remnants of this site. Applied the latest fixes and went through a checklist intended to strengthen the posture of Internet Information Server.

Analysis

Issues that allowed this to take place:

Design:

The placement of the resources wasn't done in a manner that "buffered" the internal network from the public network. While using a multi-homed system for MS Proxy is standard practice, making that system a BDC isn't. This further decreased the ability to protect the environment from unwanted access. Even had the intruder/s compromised the system running IIS they wouldn't necessarily have immediate access to the internal resources. Given the increase in reported incidents in which "script kiddies" exploited the vulnerabilities easily, it only makes sense to keep all access to any system that houses the mechanisms for NT domain authentication, buffered from the public network.

A better design for this environment, using the current resources, would have been to install the Proxy/IIS server as a "stand alone" system. This would have decreased the risk of someone gaining access to the NT domain accounts and having the "keys to the kingdom". Other items could be placed at the perimeter, but given the lack of technical knowledge at this particular company it is doubtful that anyone would periodically review settings and log files. In fact, it could be argued that placing so named security devices and applications within an organization could promote a false sense of security. If company management and support staff aren't properly familiarized with the risks and

© SANS Institute 2000 - 2005 Author retains full rights.

issues not much good is attained by placing products and solutions that aren't going to be properly used and maintained.

Configuration:

Probably the main issue that allowed this company's system to be used for illegal activity was that the Internet Information Server implementation looked to have been installed in a "default" manner without any consideration given to what was actually needed or what steps could be taken to prevent unauthorized access from outside/inside individuals. By simply not electing to install unneeded services, i.e. ftp during the installation process, this issue may have been avoided. Of course there are many ways to gain access to a system running Internet Information Server, and just because one disables ftp doesn't mean that an unwanted user could implement another ftp type of service for the purpose of distributing illegal copies of software or other intellectual property.

IIS configuration should have been thoroughly thought out prior to implementation. There are several good resources for steps you should take to secure a Windows NT 4.0 Server running Microsoft Internet Information Server 4.0 on the Internet.
A few of the top things to consider would be

- Allow network-only lockout for the Administrator account.
- The use of "strong" passwords for the Administrator account.
- Disabling unneeded services.
- Disabling Remote Data Services to prevent the RDS security hole (CVE-1999-1011).

Patches/fixes:

Another point of almost equal importance was the fact that no fixes/updates had been applied since NT4.0 sp3. Since the release of that service pack, many security fixes had been released, some significant in nature. Constant monitoring for new releases or updates of operating systems and services is one of the best ways to lower the risk of being open to common vulnerabilities and exploits. While this particular company didn't have the personnel on hand to do this, placing a call to a vendor of integration consulting firm may have given them a "push" in the right direction.

Password usage:

Password policy was nonexistent. The password for the "administrator" was null, another bad and lazy way to administer an NT environment. With the volatile combination of unneeded services and lack of hot fixes applied, an unwanted intruder could quickly have compromised the system, grabbed a copy of the backup sam database

© SANS Institute 2000 - 2005, Author retains full rights.

and run l0pht crack against it to reveal the password. The current situation was inviting trouble.

Firewall:

While a firewall isn't the answer to everyone's prayers, if properly configured it can provide a certain level of protection and possibly detection. Had a firewall been implemented and ftp services not allowed, this misuse, and ultimately "availability attack" may not have happened. Obviously an ftp service can be configured to advertise and communicate on a port other than 21, but by limiting what traffic is allowed in and out, the risk can be lessened. Additionally, by reviewing a log file, possible communication attempts originating from the "inside" may have been revealed. There are many opinions on the proper implementation of a firewall and a system running web services. It would be impossible to explore all or many of these given the scope of this analysis.

Access Controls:

During the implementation of the Internet connection it would have been prudent to have the provider put access control lists in place that would limit inbound connections to only those services required. While this isn't the catch all, it does limit opportunities for outside connections to improperly configured systems. If an administrator were to unknowingly put services into place on the "outside", the use of acl's on the perimeter device could hide this mishap. Most devices that provide the routing and Internet connection allow for some sort of "access control", not utilizing this feature is a common mistake. Not all providers of "managed" services will enable this capability, but many can and do if asked.

Conclusion

It is easy to see how one can misdiagnose a particular problem. In this busy world of trying to support networks and applications, one can often look for the "quick fix" in order to move on to the next item on the list. Sometimes it pays to step back and dig a little deeper for things aren't always as they appear.

A little time spent up front in network design and resource placement can save a company much time and effort if and when the time comes for a potentially embarrassing issue. Not everyone can possibly keep current with all of the "best practices" and vulnerabilities out there. There are many resources available, at no charge, to anyone who is willing to spend a little time reading. The Internet is probably the most valuable of these. Newsgroups, mailing lists, and vendor websites are some of the fastest ways to be alerted of new vulnerabilities and also a good resource when attempting to implement a specific product or service. The information to implement a solid network design, password

© SANS Institute 2000 - 2005 Author retains full rights.

policy, and maintain currency on platforms is out there. One just needs the time and desire to find it.

Maintaining or implementing a network that provides resources to external users can seem easy, but is typically resource intensive. There are many reasons to try and keep all perimeter systems protected from unwanted access. Some individuals are concerned only with access to and from the Internet and do not consider the possible ramifications of being exploited. These range from "availability attacks" to having resources tied up in the civil courts. The degree to which efforts are made in this area would have to be based on the assets being protected. One thing is certain; few companies can withstand embarrassing publicity.

The time spent on the basics and applying the foundations of "information assurance" can be invaluable in preventing confidentiality, integrity, and availability attacks.

Resources

1. Business Software Alliance- Myth FAQ
http://new.bsa.org/usa/freetools/myth.phtml

2. Ethereal
http://www.ethereal.com

3. A Discussion of Usenet Liability Issues & Proposed Operating Policy
http://www.stiennon.com/ISP/liability/vprecedence.html

4. Software and Information Industry Association-Internet Anti-Piracy Policies
http://www.siia.net/piracy/policy/int_7_abuses.asp

5. SANS Institute- Top Ten
http://www.sans.org/topten.htm

6. Carnegie Mellon Software Engineering Institute- Improving Security
http://www.cert.org/nav/index_green.html

7. Microsoft Internet Information Server 4.0 Security Checklist
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/iischk.asp

8. Microsoft-Security

© SANS Institute 2000 - 2005, Author retains full rights.

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/default.asp

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.