Global Information Assurance Certification Paper

Mike Woods
GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4b
November 7, 2003

KNOW WHAT'S ON YOUR NETWORK AND WHAT'S NOT

Summary

The purpose of this paper is to describe vulnerabilities that may exist on corporate networks that the average network security person may not realize. These vulnerabilities are often overlooked when an IT department performs audits of their equipment. Being able to identify these types of security issues will help network security personnel begin to think "outside of the box" when performing network audits and help them determine what they need to secure.

Understanding how a host that is not on your corporate network could possibly take down your data center is just one example of the vulnerabilities described in this paper. The risks associated with these vulnerabilities and the types of policies that could help mitigate those risks are outlined in this paper.

Introduction

In response to the recent Blaster and Welchia worm outbreaks of August 2003[1] I was attempting to compile a list of all hosts on our corporate network that did not have the latest RPC/DCOM patch from Microsoft (MS03-026/MS03-039). I was using a free scanning tool called *Retina DCOM Scanner* from eEye Digital Security[2]. It is a single audit scanner that can scan up to 256 IP addresses and does not require administrative privileges on the target hosts. The scanning tool was easy to use and did not require advanced network security training to interpret the results. I sent copies of the tool to all of our IT administrators instructing them to scan their local network segments and patch their vulnerable systems.

It was with this tool that I discovered that there were several Win NT 4.0 and Win 2K servers on our network that we did not own or manage (see example #1). What began as a network audit in response to a Blaster/Welchia worm outbreak on our network was quickly turning into a large project to identify all non-corporate equipment on our network. What I found may surprise you; I know it certainly surprised me. And it also surprised the CIO.

The importance of knowing what is on your network will become evident to all administrators after an incident has taken place. The key obviously is to be pro-active. If you know what's on your network, you can protect and secure it. Conversely, you cannot secure a host if you don't know its there.

The following examples describe what I found when I attempted to identify all of the non-corporate equipment on our network. In each example, I discuss how I was able to identify the equipment, what the potential risks were to the corporate network and services, and how best to protect against similar vulnerabilities and prevent them in the future.

Example #1

IKON Print servers. All organizations utilize printers every day. There are many benefits to having networked printers. The bottom line is network printers are not going away. They have become a business critical piece of equipment that no organization can do without.

Identify:

The problem is who is responsible for maintaining the attached print server. Within our organization, we recently discovered *IKON* print servers in multiple locations. These were large, expensive, color printer/copiers utilized by several groups. Initially we assumed they were stand-alone networked printers based on the naming convention. While performing a scan of our network with the RPC-DCOM scanning tool, we noticed what we thought to be printers being discovered as vulnerable to the RPC-DCOM issue[3]. Upon further investigation, we learned that they were in fact servers running Windows NT 4.0 and Windows 2000 operating systems without any locally installed anti-virus software.

Risk:

All hosts on a network share the vulnerabilities of these print servers. A host that is properly secured may not be vulnerable to the Blaster worm, but degradation in network performance caused by excessive scanning could have adverse effects on multiple hosts. The speed with which self-propagating worms can spread makes it imperative to identify and secure vulnerable hosts as soon as possible (see figure 1). Although it's difficult to maintain security patches on Windows based servers, it's almost impossible to secure them without installing security patches. The problem; these servers were leased to our organization from *IKON*. We did not own them. And due to the contractual obligations, we were prohibited from performing any maintenance on these servers. Maintenance includes installing security patches and anti virus software. How do we secure these servers? Removing them from the network is not an option. After several discussions with *IKON,* we learned that the Win 2K servers could be patched with the latest and greatest MS critical updates, patches and hotfixes. Great news? Now all we had to do is get *IKON* to patch the Win NT print servers. Unfortunately, the manufacturer had not yet authorized any patches, updates or hotfixes after Service Pack 6a. With NT scheduled for end of life in the near future[4]. I was not confident that the manufacturer of the printer was in any hurry to test all the post SP 6a patches. We determined that to allow vulnerable

servers to remain on the corporate network posed a significant risk. If these print servers were to get infected with a worm, we would have to remove them from the network. Once they were removed from the network, users would be unable to print to them.

Protect/Prevent:

After several meetings with the vendor we decided the best approach to mitigate the risk was to require the vendor to patch the Win 2K print servers and install anti-virus software on them. We also required the vendor to replace their Win NT 4.0 print servers with the newer, patchable, Win 2K print servers. This would allow us to continue to protect all of our networked hosts from these non-corporate servers and to ensure the availability of the printer services provided by this equipment.

In order to better protect against a repeat of this type of issue, corporate security policies were updated. Stating that all non-corporate equipment that required network access was prohibited from being connected to the network without first being reviewed by the network security group. Corporate security standards for all non-corporate equipment that required network access were also revised to include specific minimum standards for Microsoft based operating systems. Specifically, all Microsoft based operating systems are required to have anti-virus software installed locally and security updates hotfixes and patches must be maintained by the system owner. Implementing policy's after an incident is difficult at best. Once security administrators begin to understand the types of threats that may exist, they will be better able to develop policy's to address these types of issues prior to authorizing vulnerable systems access to their network.

Example #2

A great way to identify hosts that are infected with the Blaster or Welchia worm is to review the perimeter firewall logs for excessive traffic on tcp port 135 or ICMP. Both of these will give a clear indication of an infected host's constant attempts to connect to other hosts sequentially. *The Blaster / Welchia worms spread algorithm was random-start, sequential-search*[5] which makes infected hosts easily identifiable.

Identify:

While reviewing firewall logs I was able to identify a host that appeared to be infected with the Welchia worm. Attempting to determine the location of the host based on the IP address segment proved unsuccessful. I was unable to find this network segment in any of our current documentation. No one in the Network Engineering group was familiar with this segment. Tracing back the IP I was able

to determine the country it was originating from on our corporate WAN. After a phone call to one of our International IT managers I was informed that the segment in question was the "old" *Shiva* dial-in device that was never deactivated. The manager explained that the local IT admins felt it was important to keep it available as a backup to the existing secure remote access systems.

Risk:

Obsolete remote access systems can be used to gain access to a network without any restrictions as to the destination or port. More alarming is the lack of control a security administrator would have to be able to quickly audit, block or restrict access to an unauthorized user. Remote access systems implemented in our environment prior to1996 were not required to be terminated outside the perimeter firewall. And authentication was performed on the dial-in system only. In 1996 the dial-in systems were redesigned in our environment so that all users were required to utilize a *Secure ID* token and authenticate against a firewall. In this way, we can control the destination and ports that users require access to.

Protect/Prevent:

This issue is very simple and straightforward. It is an old, unsecure, outdated system located in a remote office. It was replaced with a new, secure remote access system. Once the new system was tested and brought online into production, the old system was to be de-activated and removed from the network. Security administrators will need to verify that the work has been completed at some point. It's best to verify deactivation of old systems as a final step in a project, as opposed to discovering that they are now a vulnerability. The risk of having these old systems remain on the network far outweigh the convenience of having a backup remote access system that could be used in the event the primary remote access system failed. Contact the senior person in the remote office and have them remove the system. Ensure all personnel in that remote office who require remote access are aware of the current corporate policy. According to CERT Coordination Center *"Security policies and procedures that are documented, well known, and visibly enforced establish expected user behavior and serve to inform users of their obligations for protecting computing assets".*[6] Lastly let the administrators know that if the primary remote access system does fail, their backup system is their vehicle. They will have to drive into work to respond.

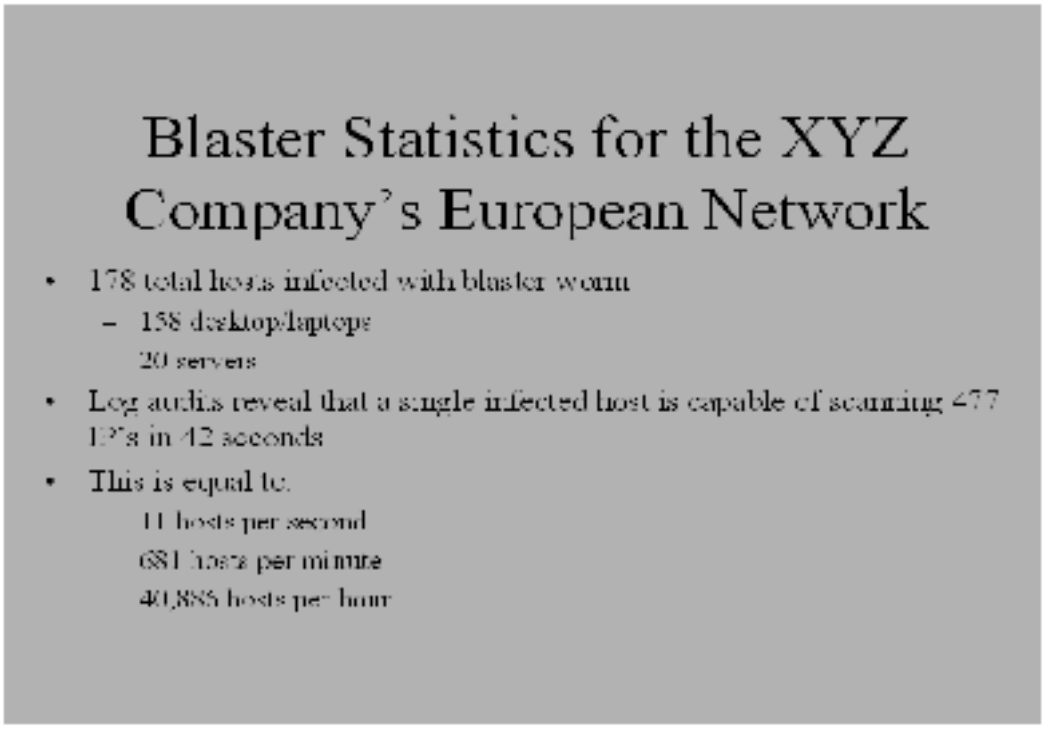

Figure 1

Example # 3

According to a recent PricewaterhouseCoopers Barometer Survey of 170 executives as quoted in Computerworld Magazine [7]*."U.S.-based multinational companies plan to increase their merger and acquisition activity over the next two years, with 70% expecting to be involved in such deals in that period".*

The topic of mergers and acquisitions and the security concerns that stem from them could fill an entire paper all by itself. In this example, the merger had already taken place. Network engineering groups had already exchanged information and completed a project to install a dedicated frame relay link between the corporate headquarters of both organizations. The network security group was tasked with replacing the new organization's firewall with a corporate standard firewall that the corporate security group would fully manage.

Identify:

After completing the installation of a new firewall at the main facility of the newly acquired organization, a comprehensive review of the firewall logs was performed. This would allow the security administrators to ensure all required services were functioning properly. Internet access was tested from all LAN segments. Test emails were sent and received and all appeared to be functioning

properly. The following day several calls were received at the help desk complaining that internet access was no longer working at the Las Vegas office. The only problem was we didn't have a Las Vegas office. Review of the firewall logs confirmed that multiple hosts were being blocked while attempting to access the public internet on ports 80, 443, 25, and 21. As it turned out, the Senior IT director had allowed a frame relay connection to remain in place that should have been disconnected due to the recent merger (see figure 2). The merger did not include the Las Vegas office, but the director thought it would be no problem to allow the connection to remain in place until they implemented a new internet connection on their own.

Risk:

Knowing all of the entry points to your network is a must. You cannot lock down holes that you do not know exist. The risks associated with this type of data connection are numerous. Unrestricted access into your corporate network, and siphoning of network bandwidth and resources are examples of these risks. The liability of malicious activity that originates from your network is reason enough to convince any senior manager that the risk associated with this type of connection far outweigh the benefits of maintaining a cordial relationship with a former business partner.

Protect/Prevent:

When faced with a merger or acquisition do not only rely only on the information provided by your new co-workers. They may not be aware of everything that is on their network. Seek out and determine what is on your new network. Reviewing old diagrams may give you insight into what used to be there, or may still be there, or was never disconnected. Router logs and routing tables offer valuable information that will help an administrator quickly determine what hosts and IP segments exist on a given network. Firewall logs offer one of the best sources of identifying hosts on a network.

Lastly, develop clear policy's concerning mergers and the requirements to fully disclose all information that pertains to data connectivity and network access.

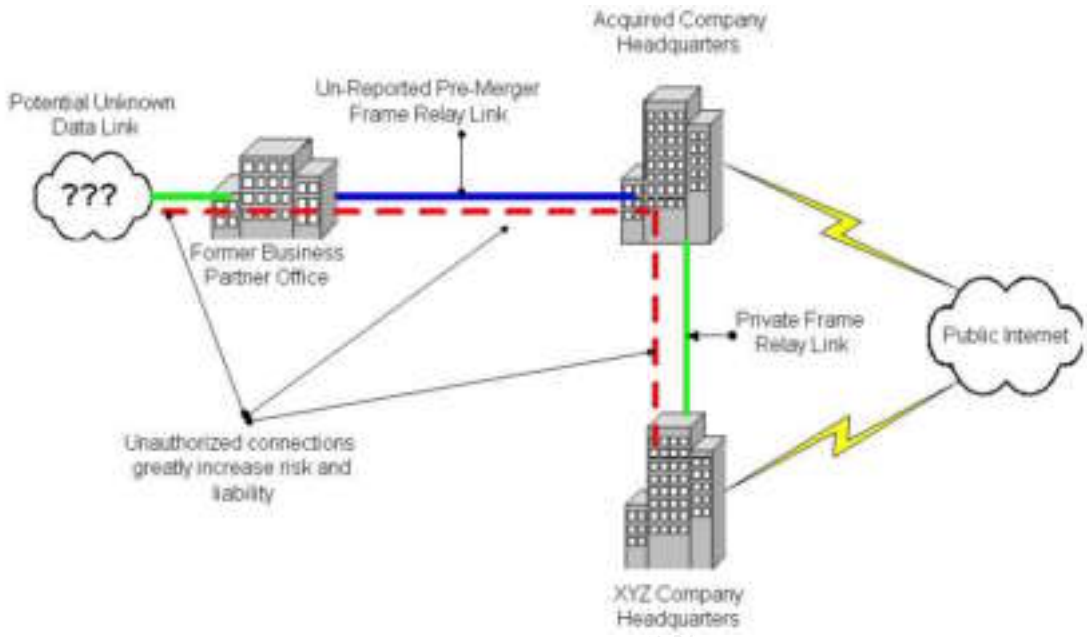

Figure 2

Example # 4

How can a host that is not on your network take down a data center? Data center services are often described as “ping, power, and pipe”. But other services are necessary to maintain data centers. Take away one of the 3 p’s and you will no doubt be unable to provide data services to your organization. What security administrators may not realize is there is another critical piece required in all data centers that will force a shut down of your equipment; air.

HVAC, an acronym for heating, ventilation, air conditioning needs to be considered when discussing critical data center requirements. Data centers have been forced to perform orderly shutdowns when faced with rapidly rising internal temperatures due to air conditioning failures. Most modern data centers are designed with redundant power supplies. When primary power fails, backup generators are automatically activated. Uninterruptible power supplies (UPS) ensure equipment remains functioning.

The following scenario actually occurred resulting in a 4 hour data center shut down. Violent thunderstorms knock out primary power. Backup power systems automatically came on line as designed to ensure no disruption to data services. Several minutes after the primary power failure, a direct lightning strike on the backup generator that powers the HVAC system disabled the system. Temperatures began to rise almost immediately in the data center. As temperatures in the data center began to approach 100 degrees Fahrenheit, decisions needed to be made. Some of the questions facing the data center manager whether to perform an orderly shutdown of all computer equipment? Or risk overheating and permanently damaging systems?

Preventing lightning strikes and inclement weather is beyond the scope of any security administrator. But, ensuring vulnerable systems are properly identified is not.

Identify:

Organizations may have several computer systems that are not managed and operated by the IT group. Different non-IT groups within a company utilize these systems. The responsibilities for the facility services usually do not fall under the standard IT structure. HVAC, lighting, water are all examples of non-IT areas of responsibility.

The areas that do fall under IT are data connections. Data takes 2 basic forms; analog and digital. All security administrators agree that data security is their responsibility. Confidentiality, integrity and availability are the cornerstones of data security. IT personnel who lack security training often fail to realize that availability is a large part of data security.

Determining what is on your network can be accomplished by performing regular audits using tools like *Nmap*[8]. Even a simple freeware port scanner configured to do a discovery utilizing ICMP can provide a detailed list of what hosts are connected to your network. Determining what hosts may be connected to your network and also have a modem and analog phone line connected is accomplished by war-dialing. What is often overlooked is the system that is accessible via a modem that is not on your network.

War dialing is a standard process of any attack and penetration audit. According to Rob Shimonski, *"A war dialing attack is malicious in intent and is a form of penetration into an organization's network designed to elude firewalls and intrusion detection systems (IDS)".* [9] Primarily, the targets of these war-dialing sessions are computer systems that are connected to the corporate network and are also connected to an analog phone line via a modem. Knowing that disabling a data center's HVAC system, one could create a denial of service against an organization. It becomes critical to understand how environmental systems are controlled. Questions to ask include, who controls the HVAC system control computer and what it is connected to? How is the security of the HVAC system now the responsibility of the data security administrator? The security of HVAC systems have a direct effect on the availability of the data center. If it's connected to either the network or an analog phone line, it should fall under the responsibility of the data security administrator.

Risk:

While performing a war-dialing audit against corporate headquarters, a computer was discovered that was configured to answer when dialed into. After establishing a connection to this computer it was quickly determined that it had PC Anywhere running on it with no password set. Full, unrestricted administrative access to the system was obtained in less than 2 minutes. The host was identified as the *Security Command Center* and was utilized for controlling the HVAC, electrical, and lighting systems for the corporate headquarters facility.

Disabling or turning off the lights, although certainly a nuisance, would have little effect on a data centers ability to provide computing services to a corporation. The electrical and HVAC systems could have a direct effect on a data center. Determining the cause of intermittent power outages or fluctuations in the HVAC settings could require extensive time to troubleshoot. Especially if these issues only arise in the middle of the night. The potential risk to the data center in this type of situation is very high.

Protect/Prevent:

Regular audits that include war dialing will help ensure unknown or unauthorized modems are not an easy entry point for a hacker or cyber vandal. Any system that is accessible via *Pcanywhere*, or any other remote control software should be audited for proper configurations. Users who require the use of remote control software must be educated on the risks associated with this type of software, the corporate policy's and standards that address this type of software and the consequences of not adhering to policy.

Conclusion:

The above examples are just a sample of the types of vulnerability's that could exist on corporate networks today. Other types of non-corporate equipment commonly found on networks are shipping company computers, out of band maintenance equipment like modems and terminals, test or development equipment, vendor or temporary consultant equipment.

The key again is to be able to identify this type of networked equipment and in the case of non-networked equipment, determining what systems have a direct effect on your network and data center. One method that may help facilitate identifying these unknowns is to begin to identify the different groups that make up a corporation. Examples of these groups (as mentioned earlier in this paper), facilities groups who are responsible for building services like electricity, water and HVAC. Kitchen staffs, who are commonly outsourced through another company, may require access to the Internet for ordering supplies. Physical security groups also require computer equipment for access control as well as closed circuit monitoring. As technology advances, systems are being designed to utilize TCP/IP for communications to take advantage of the ubiquitousness of the Internet. And as people learn of the ease of connecting into their work computers via a modem or Internet connection they begin to develop in their minds a requirement that they attempt to fulfill without any idea of the effect it may have on the corporation's network and data services.

Once a security administrator begins to "think out of the box" and look at their network and data center from different perspectives, they will be better able to identify potential problems long before they are discovered as part of a post incident review.

References:

[1] Ullrich, Johannes. "*Blaster, Power Outage, Sobig. Two weeks in August and the Internet Storm Center*"
http://isc.sans.org/presentations/sansne2003.pdf

[2] http://www.eeye.com/html/Research/Tools/RPCDCOM.html

[3] http://www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/MS03-039.asp

[4] http://www.microsoft.com/ntserver/ProductInfo/Availability/Retiring.asp

[5] http://www.networm.org/faq/#rs

[6] http://www.cert.org/security-improvement/practices/p090.html

[7] Violino, Bob. "*Strengthen Security During Mergers".* ComputerWorld. 14 July, 2003
http://www.computerworld.com/securitytopics/security/story/0,10801,82937,00.html

[8] http://www.insecure.org/nmap/

[9] Shimonski, Rob. *"Hacking Techniques, war dialing"* 1 August, 2002
http://www-106.ibm.com/developerworks/security/library/s-dial/