Global Information Assurance Certification Paper

James N Silva
GIAC Security Essentials Certification Practical Version 1.4
Option 2 – Case Study in Information Security

Internet and Remote Access Project

Abstract

This paper will discuss a security policy and performance issues many small businesses encounter when their business models encounter growth. This paper follows a project, dicussing Network and Security issues from a Security Essential student with previous experience as a Network Technician. General security policies that existed were compromised in the near term, in order to provide continued functionality. My real world issue, in this case, is to provide at least the previous security policies, and functionality.

Security topics include the Internet Access Policy, and enhancements to the Remote Access Policy. Program functionality and performance as always needs to be considered and will be discussed in the Before Snapshot along with the current and previous security policy.

The conclusion is that following best use practices / policies still provide the most effective results. In this case after evaluating the security posture in the after snapshot, the policy as implemented for access to the local LAN from the Internet accounts for the larger amount of vulnerabilities and should prove to be implemented with a lower risk after accounting for the threat to the vulnerabilities. The comparison in the conclusion is between the Internet Access from the LAN to the Internet and Internet Access (Remote Access) from the Internet to the LAN. The project is a culmination of a Network Technician's attempt to incorporate the beginnings of a proactive approach to the security requirements for a resistant (to the expense) small business community.

Prologue

The nature of a small business is the necessity to include a valuable resource, the small business consultant, in its model. Generally this field service technician's skills may range from apprentice administrator types to experienced network technical types. Seldom does this technician carry security credentials. The small business relationships with these resources are often long term. The familiarity of the known quanitities of the hourly costs and billing practices, as well as the time involved in fostering the personal relationships (with their consultants) tend to equate these relationships with the physics axiom, (Newton's First Law, Appendix B). "An object at rest tends to stay at rest and an object in motion tends to stay in motion with the same speed and in the same direction unless acted upon by an unbalanced force." The unbalanced force in this case, generally, is an extreme circumstance. Of course there are no more extreme cases than a security incident, although perceived incompetence also qualifies as the gravity necessary, to provide the impetus, to schedule the time required, for this decision making process, i.e., changing consultants. Still, knowing which consultant provides which advice, can be a daunting task for any

business person, charged with making those decisions.

A company, perceiving only nominal growth, leases a secondary site. It is not clear whether the increases in personnell will be permanent or temporary. A primary department moves into the new space. Under advice from their telcom consultants, implemented is the new technology of combined voice and data over a T-1 line between the 2 sites. All wiring, connections, and voice have basic functionality. The 384K DSL line remains the connection to the Internet.

The Before Snapshot

I received a call from the technical contact asking for consultation with the telecom consultant. I divulge the technical and IP specifications for the network. I have been waiting for the chance to change the 80.0.0.0 network since I first audited the network a fews years earlier when I began consulting with this business. I later discovered how the numbering scheme was implemented. It was taken directly from a series of help documents included with a POP mail gateway product. The 80.0.0.0 network is a valid Internet address space and was owned by another entity. However, I didn't have the time available to be immediately on site on the morning in question.

When I visited the site all the network and telephone communications had basic functionality. The technical contact informed me of the status. Some voice issues needed to be enhanced. Network communications for the primary accounting and informational programs was very slow. I looked at the IP configuration and discovered the routers were in bridge mode. I learned TCP/IP a number of years ago with the SAMS Publishing book, TCP/IP in 14 days.

I wasn't involved in the recent changes to the primary accounting program the business uses. Previously, a Unix based program was utilized with a terminal emulation program being used at the workstations for connection. Centralized processing, or client server based programs are two types of communications a business can expect to use effectively across a WAN connection. Similar to the difference between a Remote Control based programs, (effective), compared to Remote Access based programs, (ineffective), when trying to extend a LAN, a distributed processing program, like the one the company implemented, replacing the Unix based program, will not effectively run across a WAN connection of a T-1, even for a single user. Doing the math, the performance degredation in this case was 667%. (The calculation is included in Appendix A.)

Prior to the expansion, Internet Access from LAN to the Internet was controlled with Microsoft Proxy Server. Many issues contributed to its removal. The immediate one was that during the connection of the two sites, proxy was non-functional. Proxy's functions are to be replaced with a hardware firewall. There are a number of inexpensive devices. Two features not available with the most low cost hardware solutions are caching of web pages, and stateful inspection, although configuring and using any of the stateful features with Microsoft Proxy Server was beyond my ability. Proxy always stopped functioning whenever I tried to configure any function besides basic access. If a service pack reapplication did not solve the access problems, a new installation could be at least 4 hours. The Internet Access policy was enforced by witholding the proxy client installation from workstations. Although there

was initial sucess with this policy, with the advent of the automatic proxy server discovery option for Internet Browsers, this policy shows that is is outdated by a number of years and should be recreated to a more modern model.

Remote Access to the LAN from the Internet does not exist. There exists a need for the current remote access policy of modem based RAS to broaden. External access to E-Mail for executives and management is desirable with better options and performance. The servers are also in need of more vigilante maintenence than in their initial years of service.

Based on the situation, the project, necessitated by the expansion, entails the formation and implementation of a policy surrounding a new firewall, and the configuring of Internet Access controls from the LAN to the Internet and from the Internet to the LAN. Internet Access is a 384 KB DSL connection and needs to have the resources protected from unauthorized use which could affect the neccessary Network resource functions of E-Mail, web based research and business, internet forms access, and statistical information retrieval, to mention a few. The WAN extension and its performance is the primary reason the expenses will be approved and the factor necessitating remote access policies review.

During Phase

The project starts after contacting the telecom consultant, I make the necessary IP addressing scheme changes to the DHCP scope, and all the other devices using static addresses, including the printers with the help of the HP JetAdmin utilities, while he made the changes to his router's configuration, changing them from bridge mode and into route mode. Voice improved. Network still had issues with the primary accounting program. The mail system and document management programs are both client server based applications. The accounting system is a DOS based distributed application.[1]

By changing the IP addressing scheme from the routeable number to the non-routeable one, NAT implementation can be provided with the small hardware based firewall, a Linksys BEFSR41 Cable / DSL modem router. There are a number of competitors comparable to this device. The company I worked for had been recommending and implementing this device for its customers for a number of years. The relationship with technical support is above average. It will provide the means to filter Internal Internet Access through IP addresses.

The performance solution for the WAN is a Windows 2000 Terminal Server. It offers security with the use of encryption and offers remote performance adequate for a WAN environment. Installed from CDRom, patched from Windows Update Site, [2] and crosschecked at the Microsoft Downloads section for Terminal Server specific patches, baselined, using the techniques in Exercise 6: Auditing your sytem in the GSEC Security Essentials Toolkit and optimized according to document provided by Microsoft[3]. The Terminal Server is brought into service after a baseline backup was performed and stored off-site. The Terminal Server will provide the basis for the

[1] A brief description of Centralized and Distributed Processing can be viewed at http://www.darwinmag.com/learn/curve/column.html?ArticleID=9

[2] .http://windowsupdate.microsoft.com

[3] .http://www.microsoft.com/windows2000//planning/terminal/tsappdev.asp

extended services for the Network Administrator and the general services for the WAN and other offsite users. Being included with a Windows 2000 server license makes it a cost effective solution. Using dumpel, a utility from the Resource Kit which exports the Event Log to a field delimited file, netsvc, another utility from the Resource Kit which can list the currently installed services, fport,[4] a utiltity which can display open ports and associated executables by name or PID, and fc, a file compare utility, is a low cost method for basic host based intrusion detection logging with simple baselining (Note: An ethernet connection is necessary before using fport under W2K or WXP. Viewing potentially harmful results is not possible without remaining at risk.)

Another issue surrounding terminal services on Windows 2000 is licensing. Windows 2000 and above workstations include a terminal server CAL (client access license). [5] Upgrading the Windows NT 4 workstations to W2K Pro and XP Professional was completed. These workstations were patched to current critical and security update levels. Anti-Virus functionality was verified. Remote desktop connections for my ID was enabled on the XP machines.

Before Security Essentials Fault Tolerance and Security offerings to my clients had three levels. I was introduced to a more industry friendly term, Defense in Depth. As the term implies, one's network should not depend on a single point of failure whether trying to protect data from loss or compromise. My Defense in Depth for Internet Access was always based on 3 criteria:

1. Passwords,
2. Firewalls with NAT (Network Address Translation) enabled, and
3. Non default port assignment for remote access services.

Along with Defense in Depth (DID) is the concept of countermeasures. For the above described level of DID, all measures are static. Availability of information is the primary measure for the DID. If the cracker can figure the remote access service allowed, he must then find the service port. Once he has the port, he must find a valid user name and password combination. The NAT concept of using one routeable IP address to provide Internet access for a larger number of hosts with non-routeable (on the Internet) IP addresses, assures that communications to the individual servers and workstations need to be provided with a valid TCP service that has been enabled on the server and access allowed to the service with a rule set on the firewall. In my previous service as a Network Technician this was the suggested implementation. During the After Snapshot, I will provide additional information for this DID along with the countermeasures I can now use for the small business. Logging was alway reviewed on a reactive versus a proactive basis and solely based on the particular product's logging options.

Altering Terminal Services for Windows 2000 server and Windows XP communications service ports are configured in the registry. [6] The above referenced document does not reference Windows XP as an applicable Operating system, but the registry key used to alter the service port, "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" is the same.

[4] http://www.foundstone.com/knowledge/proddesc/fport.html
[5] http://www.microsoft.com/windows2000/server/howtobuy/pricing/terminal.asp
[6] http://support.microsoft.com/default.aspx?scid=kb;en-us;187623.

PCAnywhere's default ports can now be changed inside the program on a per host definition basis in versions 10 and above. This is a very fine feature. Implementing port based security for pcAnywhere on multiple hosts requires less time to configure before communication can start. Previous versions need to be configured in the registry. I used to create a registry file to alter the port settings when I wanted to connect to hosts listening on a different port. Only one session could be initiated. The basic Symantec port document includes a link for configuring version 10 and can be found by going to the Symantec Knowledgebase and select "pcAnywhere IP port usage" from the hot topics list. [7] I have also use Carbon Copy (owned by Compaq / HP last I checked). The default port is 1680. Port usage is configured in the INI file of Carbon Copy's installation folder. I have used many alternate remote access programs to get to less critical hosts. Once inside the firewall I use these other programs. The services for these alternate remote access programs are enabled by one of the available Services Managers, Server Manager on NT4 or Computer Management on W2K. The services are either disabled or unstarted when not in use. The utilities are available to the Domain Admins group and available from a protected area on the Network. This provides an additional layer of security to the Remote Access activity and extends the time it would take for an intruder to get from one host to another.

Documents are created for new workstations and users setup. The justification document based on the network performance, referenced above, was also done at this time. The Terminal Servers service port remains at the default, based on issues surrounding the user's first exposure to the Remote Desktop Connection Utility.

Some mention should be made on small businesses and budgets. Addtional labor costs for any project seems to be expected and authorized. Additional purchases of hardware, software, or security solutions, require new justifications. This is not always cost effective. I think Michael Johnston's comments are well suited to support this statement, and he may have stated it better in his article's second paragraph. [8]

The proposal for the primary performance issue was accepted and implemented as described above. With this one implementation, I had a new job with this company and had a Remote Internet Access policy. Still to be completed was the Firewall configuration for filtering the internal IP addresses and creating the rules for Remote Internet Access. This left only the security issues, but being able to quantify the quality of security and network protection is why I started with the GIAC education series. Having general information about the security offerings and technology, and being able to apply them to a wide range of small businesses, will be an invaluable talent for the 21st Century. (See Appendix C for a personal perspective) I would soon discover a shortfall to the firewall that was implemented. It was a non-stateful device. This will be discussed during the After Section. Now I definitly desired a full-featured firewall with stateful inspection, either hardware or software. I prefer a hardware based

[7] http://service1.symantec.com/SUPPORT/pca.nsf/docid/1998122810210812?OpenDocument&src=hot&prod=pcAnywhere&ver=10.0%20for%20Windows%2095/98/Me/NT/2000&stg=2&base=http://www.symantec.com/techsupp/pca/&next=pca_10_search_other.html&sone=pca_10_tasks.html&tpre

[8] http://www.giac.org/practical/Michael_Johnston_GSEC.doc

firewall for the initial one at the company's perimeter. Yes, you can use more than one. That is DID. I have used Netscreens in the past.The last one I implemented required a device at each site in order to create an IPSEC tunnel because the data crossing the wire would be sensitive, proprietary, client files, and this information provided the basis for the business (Civil Engineering). For the current company, I was told there may be a future need for more remote access without a dedicated T-1 line to provide the initial security. The Internet may be used.

The feature the Linksys has, and I knew I could use to enhance the Internet Access Security Policy for the company was the Filter by IP Address option. The alternatives for a small site are limited. The topology is a switched LAN. No other router based solution is better or worse. HTTP is required for uses on the LAN. The access restriction by IP address or IP address ranges can be entered into the 5 available Filtered Private IP Address Range fields on the Linksys Filters tab in the Advanced Sections. Using previous lease information to obtain MAC addresses. (If you don't know how the MAC address is used in the TCP/IP suite of protocols, do an Internet search for ARP-Address Resolution Protocol.) One can also view MAC address to IP address entries of the ARP cache using the ping and the arp –a (to display the contents of the arp cache) commands. I configured a series of reservations for those workstations authorized for Internet Access in the DHCP Management Console. The remaining IP addresses were added to the filtered address ranges in the Linksys's Advanced Filters configuration page. On this page you configure the IP addresses you don't want to have access to the Internet. DHCP configuration also includes the excluded numbers that had been reserved for printers and servers. Printers are also denied access to the internet. I left one number with Internet access for patching workstations without access, (although this is unnecessary, since changes to the Linksys take place immediately). A small vulnerability to the security policy, but the threat is low since access to the value of the number is limited by physical and password security. (And of course, my memory.)

This fullfilled the Intenet Access policy requirements for the main site, but the recently added 2nd subnet was uncontrollable with this method. The subnets are connected with Cisco 2620 IOS v 12.2 at the main site and Cisco 1601 IOS ver 12.0 at the sattelite office. With the help of Cisco help pages, [9] and past experience, I was able to restrict the user from internet access, using the host to host ACL restriction on the remote router (1601). Remember, once a rule is set on the router another rule needs to be set to return access to the restricted host to those to which you do not want the rule to apply. First create the extended rule and then apply the ACL to the rule. Next give the unfiltered hosts access to the resources.

In enable mode, enter terminal configuration – config terminal

(config) # access-list 101 deny ip host 1.2.3.4 host 1.2.3.5

Note: (1.2.3.4 would be the restricted host and 1.2.3.5 would be the firewall which provides access to the Internet.)

[9] http://www.cisco.com/warp/public/707/confaccesslists.html#extended,

Next:

(config)# access-list 101 permit ip any host 1.2.3.5

Note: Replace the extended ACL number with the ACL number in question. For all users not defined in extended ACL 101, any IP protocol is permitted to the firewall and thus access to the Internet. To undo an ACL entry use the "no access-list 101" command from the terminal.

In this case the router could be configured to restrict the HTTP protocol, (done in much the same way as restricting by host), but the users's needs include HTTP services for the reports generator documents. They are Crystal Reports in HTTP format. Nearly everyone uses these documents. Although not directly serviced by a Web Server or an Intranet, it is one of the main reasons the Unix program is no longer a production application. The Unix application provides only limited reporting.

I would have preferred to have all the rules in one location. With a full featured firewall a technician could define subnets and restrict access by IP address, (both for internal as well as external addresses), user names, or MAC addresses. Where the Linksys only understands a single subnet in Gateway Mode, higher end firewalls are not as limited.

Having discussed the performance and remote access implementation, one can see that security need not impact performance. The same can be said of the relationship between the internet access policy, the firewall, dhcp server and DSL connection. Performance need not be compromised to add a small layer of DID. The topic left undiscussed here in the during phase is passwords. I will discuss this in more detail in the After Project Analysis Section, since most of the disussion centers around the analysis of the password choice, and which database protects it.

After Project Analysis

Stateful inspection of packets becomes a very important feature. Within four months of the change to the Linksys, the NetBios, port 137, name service, Denial of Service, packets began to appear in the logs. [10] This attack remains near the apex of all unwanted activity. This activity is probably a contributor to the October 2002 incident with the DNS root servers. I first read about the incident in the October 24, 2002 issue of the San Jose Mercury News, Business Section and later on the Internet. [11] A stateful device will not only use the rule set on the device, (firewall, router, etc.), it will also look at source and destination ports, addresses, and sequence numbers to determine the validity of the communication. [12]

I captured packets on a Windows XP Professional, using Windump and Ethereal, after halting all possible services, including Server, Workstation, and Browser. Packets continued to traverse the firewall and were broadcast onto the wire. The

[10] http://isc.incidents.org/port_details.html?port=137

[11] http://www.caida.org/projects/dns-analysis/oct02dos.xml

[12] http://www.firewall-software.com/firewall_tech/stateful_packet_inspection.html

workstation then requested a NetBios initiated name resolution from the DNS servers for the offending source IP address. Appendix D contains additional information on how I discovered my networks were / are being attacked. A stateful device is in the future for the business.

As a countermeasure to this vulnerability, I monitor the attacks against the Linksys with the addon products WallWatcher / Wall Reviewer and GetLog. [13] Wall Reviewer provides a front end viewer for the Wall Watcher logging program. One need only configure the "log to" address on the Linksys with the workstation's address that runs the Wall Watcher program. GetLog is a utility that will read the Linksys log files directly, compare the entries with the Wall Watcher log entries and highlight missing entries. Options, to save all current Linksys entries to a new log file or only the missing ones, are available. The GetLog utility can account for missed entries the Linksys broadcasts to Wall Watcher because it queries the device directly not depending on the connectionless broadcast. I initially used the WW2Dshield, a utility to help you submit Wallwatcher log reports to Dshield. Since I first discovered this attack at home, I changed my home firewall to a stateful device, the Netscreen 5XP. [14] All Netbios activity appears to have ceased. A check with the Gibson Research Website, using the Shields Up utility, shows the Netscreen providing expected protection.

In my office we are currently getting an average 6-8 netbios-ns packets per hour. It peaked at 12-17 per hour during October 2002. At home from September 2002 to October 2002 this attack peaked at more than 1 per minute. I tried contacting the company's ISP to request help with the situation. Best use practices suggested checking whether the router at the ISP was stateful. If so, ask if our IP address could get a filter configured to reject such improper communication packets. (My home ISP changed my static IP address which temporarily resolved the issue. I subsequently replace the Linksys.) The ISP for our business responded with a statement regarding our low monthly fee and the provisions for no help, either in changing our static IP address or verifying the stateful nature of their router. I may try to escalate this to Texas, where I recently found a technical support escalation resource. This lack of cooperation is a vulnerability currently outside my control. The vulnerability exists. The threat should remain low with due diligence on my part. Risk is monitored with the logs. I made the change from Field Service Technical consultant to on site long term temporary employee and novice Information Security Technician.

Locating this weakness after making the firewall recommendation and completing the implementation of the Internet Access Security Policy, put those recommendations in question. For now, this will have been the last non-stateful device I will recommend. This recommendation occurred 60 days before starting the Security Essentials Program and discovering the Netbios-ns attack as well as the importance of using a stateful device. (See Appendix D) I contacted my previous employer and provided them with this information. Together we installed a few dozen of the Linksys routers between 1998 and 2002, utilizing the NAT and Forwarding features.

Evaluating the DHCP and IP filtering portion of the Internet Access Policy implementation (always a good idea not only after a set period of time, but immediately

[13] http://www.wallwatcher.com

[14] http://www.netscreen.com/products/index.html

following any policy implementation or network incident) really shows additional vulnerabilities, but the risks remain low. Initially the knowledge of all users with Internet Access is limited to 3 people (< 3%) and one document. Each department manager has the information for their individual department. Further, an employee without access needs to know the computer that can access the Internet, and find the time to get at it, unobserved. Since all workstations are NT 4 or above, administrative rights are necessary to change the IP address. Knowing the one available address, a user would still need to get administrative access to the workstation in order to apply it. Although not always possible with the varying programs businesses need to run on NT systems, there exists no initial need for the primary user of any workstation on this network to be assigned the administrative privilege. This administrative privilege would also be needed for most network analysis tools. Unless a user can bring in his own system, (difficult), to which he has root / administrative access, extract the various correct IP settings, (easy), the risk is very low. Each cubicle has only 1 ethernet network access port so a hub/switch would probably be necessary. WINS, DNS, and DHCP databases are regularly checked for registrations. Naming convention is such that non complying names are easily noticeable. Windows 9x machines could be configured to gain access without showing up and without leaving traces in either of the 3 DBs with a little preperation. The policy is based against administratively gaining access in order to compromise the internal network.

A cracker with even a modicum of skill would be able to gain access to the Internet if he was already on site. However if he is was already on site, compromise to local systems would seem to be a more feasible action. Gaining Internet Access in order to bring compromising code onto the LAN is another possiblity. I expect most attempts to do this will originate from the Internet not from inside the firewall. This external attack is more difficult to protect against. Higher end Intrusion Detection Systems (IDS) are needed on any system running a critical service as well as workstations fitting the same criteria, in order to help provide an audit trail. Employees computer skills can be evaluated by information from HR and IT. In this case all computers are behind two access card enabled, locked doors. A third entry is past the reception area and a buzz locked door. Reception is enclosed behind walls and glass, both bullet proof. Elevator use requires a password be entered on a keypad.

Adminstrative access by guessing or cracking passwords in this event is the vulnerabilty. From information I learned in the Password section of the GSEC Security Essentials Day 2 Chapter 3, Password Assessment and Management, I decided to check the NTLM settings, figuring to enable the somewhat more recent NTLM v2. [15] Other information concerning NTLM functionality across Microsoft Operating systems can be found by seaching on keywords “ntlm v2” at the new Microsoft Knowledge Base. [16] Password cracking utilities were reviewed to help with assessing the password vulnerability. Password cracking requires Admin priviledges so remember to make the admin password strong! This, as well as other advances in common security tools, helps to advance the white hat side of security a little more. LC4 is a good tool that can be used to judge your network's general password strength. Knowing the amount of

[15] http://support.microsoft.com/default.aspx?scid=kb;en-us;239869

[16] http://support.microsoft.com/default.aspx?scid=fh;[ln];kbhowto

time a specific vulnerablity will take to compromise, helps to develop the policies, including time increments for log checking. If you can increase the time it takes a cracker to find and exploit the vulnerability, you may be able to discover the crack in progress which will yield more flexibility in the countermeasures.

LC4 can recover NT passwords much easier with NTLM enabled since the technology goes back to the 80's when security was very much less a necessity for a business. Standard NTLM authentication, required by some legacy applications, if enabled (See Appendix E) does not use salts - a method for randomly generating the hash used to keep same password hashes unique. (Nor do any current Microsoft password databases.) NTLM parses the password to all uppercase, and they are broken into a two piece, seven character limit for storage. Even though the hash is encrypted with the technology, syskey, available with NT4 sp3 and above, (Type syskey on the run command field to view your settings or to make permanent changes), LC3 and above, as well as pwdump2, circumvents this technology using the technique, dll injection. A description of this technique which uses the LSASS (Local Security Authority Subsystem) service's privileges, extracts the hashes, passes the hashes to the password cracking utility being used for the test, can be found in the pwdump2 readme file [17] as well as the Study materials from the GSEC Security Essentials course as referenced above. The fact that dll injection works on other parts of Microsoft's Operating Systems is almost a given. The availability for its use on the primary security mechanism provided me with the understanding of how NDS for NT works. Substituting calls to the SAM (Security Access Manager) file with calls to its own interface, is also how the password assessment utilities can circumvent the added encryption of the syskey utility. This is a primary reason why the Microsoft Security model is and remains flawed.

Having a password of 7 or 14 characters is the best choice in this case since the odd characters above a 7 character password can be broken more quickly and used to help guess / crack the remaining 7 characters. A single or a couple of characters are less time consuming to crack and their discovery can often indicate what other characters might be. While on the topic of passwords, many technicians, while trying to implement and enforce a strong password policy, recommend what is coined as a "hybrid policy" for a user's password. As I recently heard a policy described at a local user group meeting, the admin gets his users to replace common letters with numbers and vice versa, substituting them into a common password, or better yet using the first characters in a phrase or sentence, and substituting using the hybrid approach. For example, replace l with 1, o with 0, e with 3, etc. This is not enough to create a strong password although as a learning tool for your users I can see the value if you progress toward the real strong password. Hybrid passwords are maybe 50 or 60 times more difficult to crack than alpha characters only. Compared to using letters, numbers, and special characters hybrids are only medium strength. In fact, while trying LC4 on my notebook's password database, I noticed the default Brute Force crack does not include numbers or special characters.

So if the potential cracker is a beginner with LC4, you may have even more time to discover the event before it becomes an incident, using strong passwords. Since

[17] http://razor.bindview.com/tools/desc/pwdump2_readme.html

the crack will fail, the cracker will need to change the default settings and try again. Microsoft has provided example articles for enabling strong password enforcement policies. [18]

I generally start the strong password education process with a secret sentence. I ask the user to develop a sentence based on something in their lives, whether it be a favorite car, color, movie hobby, etc. Next I ask them to use the first, second, last, etc character in each word to create the password. Capitalization, punctuation, and some spaces should be included. If there are no numbers, I advise using the hybrid substitution to get that strong password. When the password expires they can increment the letter extraction so the same sentence can be used numerous times. In this case there is a unique strong password of many characters and no need to write the password where others may be able to get it. Social engineering is a risk, but in order to engineer the compromise, the user would have to divulge the complete sentence.

Do not depend on this alone though. There still needs to be physical security for the computers themselves. Physical removal of the devices that store the data circumvents all protections implemented at the site. Physical Security should be able to detect and eradicate the risk before it becomes the threat. In this case the cubicle and offices are checked nightly, alarms are enabled after hours, and access during business hours is as previously described.

If you need to test older Unix systems, Crack is one possible tool to use. Alec Muffett, the author, has a web site. [19] These systems use DES to encrypt passwords. For newer Unix systems, or systems using MD5 or Blowfish, John the Ripper is currently considered quicker based on the algorithm it uses. [20] John the Ripper also can be used to test NTLM, AFS and Kerberos passwords. Not having heard of AFS, I found out it is an IBM filesystem product with its own security system. [21] Newest versions of Crack can also be used to test for systems using MD5 or DES. Demo versions of the above referenced utilities are available for download.

I expanded on the topic of passwords because, in my opinion, in a small business environment, it is still the number one means of security; NAT second; and port redirection for remote access third. Although most large organizations would reference Acceptable Use as the number 1 policy, I have worked exclusively with small companies where litigation is not generally high on the business vulnerabilities list. These are my top three for Defense in Depth.

On day 2 chapter 1 started the road to security policy analysis. To continue beyond the password topic, the idea of the Defense in Depth concept is necessary in assessing the three key dimensions of protection and attack 1.) confidentiality 2.) integrity, and 3.) availability. The risk of a compromise is determined by the vulnerability and the possibility of threats. Now was the time to review the Internet Access solution. The first vulnerability, the most obvious, is that the policy is based on

[18] See 161990 and 225230 in the Microsoft KnowledgeBase

[19] http://www.crypticide.org/users/alecm/

[20] http://www.usenix.org/events/usenix99/provos/provos_html/node13.html

[21] http://www.transarc.ibm.com/Library/documentation/afs_doc.html.

the workstation's MAC addresses which is the address of the network card, a pivotal communication aspect. The MAC address reservation and IP address filtering policy provides restrictions to all users who do not have a computer configured for access. However, users are not restricted from logons to other workstations, without some sort of physical security. The list of computers with access was created by the managers for each department. Initial knowledge is somewhat restricted. Some of the computers are locked when not in use. Users are generally busy processing the entire work day. So the vulnerability is there, the threat is almost high, yet the risk of compromise remains acceptable since an unauthorized user will have to change locations and will generally leave an audit trail. This audit trail is provided by profiles, entries in the Event Viewer, and the Recent Documents and Temporary Inernet Files Folders. More detailed Windows auditing is enabled through User Manager, but I find this unnecessary for the Internet Access Policy review. Besides gaining physical access to an authorized workstation, the vulnerability exists at the firewall level where the restricted IP address information resides and in the DHCP configuration where the authorized IP addresses resides. One other vulnerability exists in the storage of the documentation. The firewall is password protected with a strong password (as previously discussed). DHCP configuration is a server based utility. All servers have logon restrictions, strong passwords, short logon timeouts requiring admin password to unlock, and are behind closed doors. The doors are locked, generally, only after hours. The documents are in a directory with access restricted to the my logon account. No one alone from me is specifically aware of where the documents reside. References to some of the specifics of the policies are being reviewed for secured storage in written form. All previously printed material with the information used in implementing the policy is shredded. In each of these 3 vulnerabilities, the business goals are met. Basic guidelines and restrictions help keep the available 384K DSL line available for E-Mail communications and the required Internet visits for research and data exchange, including security and anti virus updates.

The Internet Access Policy is sound. The threats remain within the business goal, therefore, the risk of the vulnerablity being exploited remains low. There is an audit trail whereby the data can be validated. The method in use is a well know technical solution. The internal network availability for business remains high. Confidentiality is moderate. The individual pieces of knowlege are limited and diverse, yet not complicated. Integrity is also moderate since gathering the necessary confidential pieces of information could allow an unauthorized workstation access to the Internet, thereby using valuable resources as well as possibly starting another known or inadvertant compromise.

Other shortfalls of the policy:

These are functional ssues. Security Updates for workstations without internet access need manual configuration. Either I can remove the restrictions at the firewall during an update blitz, or I can use a single IP address that has been excluded from the exclusion list. This is 1 of the more than 150 unused addresses. The risk is still within the business guidelines. Access to the firewall configuration or manually testing

addresses for access requires password cracking.

Anti Virus

The Anti Virus technology for the network was changed to a centrally located and administered system. Previously, weekly zip files were downloaded and stored at a network location. The workstations were configured to update the pattern files from that location. Two issues occurred. First, workstations without internet access whose configurations had not been altered to get their updates from the local network location were not being updated. Second, the user, charged with downloading the pattern updates, occasionally missed weekly updates or did not put the file in the correct location. E-Mail protection was consistently updated, the network was protected, but all the workstations have CD and floppy drives which could provide the conduit for infection. Currrently the Symantec Security Console provides a centralized means to view current versions of application, pattern files, and scan engine versions as well as the ability to roll out the application to workstations and provide a central quarantine location. Events, virus, and scan history are easily viewed. Centralized and granular configurations are possible. The previous solution lacked this centralized approach, thereby proving itself outdated, based on efficiency and functionality.

Now that inside to outside access was complete, I needed to provide some additional functionality for remote access to internal resources and external access to the internal E-Mail and scheduling systems. I needed to test the implementation against the Remote Access Policy, to provide remote access services for network administrative purposes, remote locations, and the WAN extension.

Web Base Mail

An example of incident handling for this small business follows. Once identified, the countermeasures of Web Server security were added although in a reactive manner. In configuring Web Services for E-Mail, the opening of the http service port at the firewall was done, only to immediately discover spurious attempts of determinable unauthorized access attempts. Checking today, here is an example of the entries similar to what I originally saw. The Server's Netbios Name and non routable IP address have been sanitized, to remind others not to arbitrarily send log files to unkown sources. The offending IP address is included and is deemed to represent limited risk. By the way the IIS log is time stamped with GMT.

Begin Log Entry

#Software: Microsoft Internet Information Server 4.0
#Version: 1.0
#Date: 2003-02-08 07:28:17
#Fields: date time c-ip cs-username s-sitename s-computername s-ip cs-method cs-uri-stem cs-uri-query sc-status sc-win32-status sc-bytes cs-bytes time-taken s-port cs-version cs(User-Agent) cs(Cookie) cs(Referer)
2003-02-08 07:28:17 63.140.31.146 - W3SVC1 {Sanitized Server Name and IP Address} GET /scripts/..%5c%5c../winnt/system32/cmd.exe /c+dir 401 5 744 59 250 80 - - - -

2003-02-08 21:12:46 205.180.247.35 - W3SVC1 {Sanitized Server Name and IP Address} HEAD / - 400 87 157 17 0 80 HTTP/1.1 - - -
2003-02-08 22:44:59 210.201.167.177 - W3SVC1 {Sanitized Server Name and IP Address} GET /default.ida NN%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a 401 5 744 470 562 80 HTTP/1.0 - - -

Yesterday's

2003-02-06 11:13:21 63.25.192.164 - W3SVC1 {Sanitized Server Name and IP Address} GET /scripts/root.exe /c+dir 401 5 744 72 485 80 HTTP/1.0 - - -
2003-02-06 11:13:26 63.25.192.164 - W3SVC1 {Sanitized Server Name and IP Address} GET /MSADC/root.exe /c+dir 401 5 744 70 78 80 HTTP/1.0 - - -

End Log Entries

The first entry shows an attempt to return a directory listing of the C drive. The server returns a "401.2 Unauthorized: Logon Failed due to server configuration" error page.

The second entry I haven't seen or researched before today. It appears that HEAD is a java program that may attempt to get the source for my page. My page is an index page that allows connection to the web based mail server, but is still unviewable.

The third entry is an attempt to propogate the Code Red Worm. I originally did a search on Google in order to determine this the first time I saw the entry in the log.

From the previous day, a couple more examples of attempts to return the directory structure trying to utilize other weaknesses when left unpatched. VB Scripting and the Microsoft Data Access Component are the basis for the attempted exploits. It appears that the attempted cracking is sometimes in the format of a script that the "script kiddies" use to try to find a vulnerable system and then attempt to exploit The Honeynet Project states:

> "The script kiddie is someone looking for the easy kill. They are not out for specific information or targeting a specific company. Their goal is to gain root the easiest way possible. They do this by focusing on a small number of exploits, and then searching the entire Internet for that exploit. Sooner or later they find someone vulnerable. Some of them are advanced users who develop their own tools and leave behind sophisticated backdoors. Others have no idea what they are doing and only know how to type "go" at the command prompt. Regardless of their skill level, they all share a common strategy, randomly search for a specific weakness, then exploit that weakness."

I see the same 2 or 3 dozen attempts to return the C or Winnt directories. I don't discriminate between the two basic types of script kiddies, but then I think it equally important to report the more elusive script kiddie who will only allow 1 failed attempt and then move on, trying to leave minimal evidence as well as the abusive script kiddie. I have monitored the logs showing the same IP address pound away with the same

attack for 5 days before I could get the ISP to recognize the behavior. Don't know exactly how I'll handle the real thing, a cracker with a high level of skills, but the ultimate countermeasure of unplugging the Internet is always an available option (for us) until the vulnerability is altered. This will not affect our functionality since there are alternate means for remote access with similar policies.

Coupled with the log file evidence and best use practices, I followed the guidelines to harden the web server in Day 5, Chapter 7, IIS Security. Although the chapter is based on IIS 5 with the recommendation (loosely stated)

"if you use IIS, use IIS 5"

there are many references to IIS 4 in the document. I adapted the information to my installation. Important changes I made were, to disable the MSDAC (Microsoft Data Access Components) services, to remove the default, sample, and admin web pages, to remove access to the help directory, to verify the everyone group did not exist, to disable some of the recommended services, to enable the W3C format for the log file, to remove unnecessary application mappings, and to disable the anonymous user accounts. The IUSR and IWAM accounts are not necessary for my implementation. They exist to provide the means for anonymous access and COM+ application access. More information can be found in searching the Microsoft KnowledgeBase for IWAM or IUSR, including how to recover and synchronize their passwords. [22] I highly recommend this Security Essentials chapter for anyone charged with an IIS web server's security. Use it. It works (or the configurations that are recommended seem to be working!).

I spend part of my security time reviewing my logs and e-mailing abuse resources at various ISP's. Usually when I send an infomational message pertaining to Code Red or the more recently, the SQL slammer worm, the techs actually thank me. In another instance the abuse techs at an ISP appeared to attempt unathorized access. When I reported it, they replied that is was their procedure to verify the reporting abuse senders were valid. However, I thought attempting to check my web page to be different than verifying that an E-Mail address is coming from a valid domain. In my case the network numbers are actually different between our web domain and our mail domain. I have basically found a 100% lack of offending addresses, returning to my log files so far (6 months) for the reports I have made to US recognizable ISPs. I have less luck with the overseas ISP's, but I continue to send the most abusive exploit attempts to their attention and they seem to disappear from the logs, at least for now. The possibilities are that either the hardening is working, or a cracker is sanitizing the log files. I don't see any evidence of the latter. We intend to implement a better log accounting of Internet Access both remote and internal when the stateful firewall goes online.

Microsoft provides a Web Server hardening wizard for IIS which is version 1. [23] The URL referenced is different than the one in the Security Essentials Toolkit workbook, since Microsoft changed the location. IIS 5 has an included hardening wizard. There is an exercise on how to use the wizard in the the Toolkit workbook.

I found that removing everything that isn't needed to provide the functionality the web services uses, is a best use practice.

[22] http://support.microsoft.com/default.aspx?scid=kb;en-us;297989

[23] http://www.microsoft.com/downloads/details.aspx?FamilyID=dde9efc0-bb30-47eb-9a61-fd755d23cdec&DisplayLang=en

Thanks to Eric Cole, Matthew Newfield, and John M. Millican for the GSEC Security Essentials Toolkit.

Thanks also to the contributors to the GSEC Security Essential Course Ware, including again Eric Cole (May 2001) and Ms. Wendt for her audio (January 2002).

Remote Access Service

Last in my discussion of topics from this project is remote access services. I want to describe what I found when I finally got the chance to investigate some of the packets of the encrypted communications of Terminal Server configured for high encryption, pcAnywhere, configured with pcAnywhere encryption, and VNC over Zebedee, a couple of freely available utilities. Nathan Rinsema provides a good informational paper on the relationship between these two utilities in describing the combination of Zebedee over VNC, written June 26, 2001. [24] One difference, I use batch files to preload the Zebedee encrypting utility before loading VNC and connecting to the appropriate server. I only use these products inside the firewall so the packet capture of the VNC communication showed the same data encryption offered by each of the other two remote access packages I use. Again I leave the services either disabled or unstarted. For administrative access, this accounts to only a few more minutes when access is required. For the policy, this adds additional DID in that the cracker needs to identify hosts and gain administrative access in order to start the service. An example of the batch file is below.

"C:\Program Files\Zebedee\zebedee.exe" -f "C:\Program Files\Zebedee\{[server]viewer}.zbd" [server]:5800

Inside the *.zbd files is the command

command '"C:\Program Files\Plus!\Microsoft Internet\iexplore.exe" http://[server]:5800'

for java based web access or

command '"c:\Program Files\ORL\VNC\vncviewer.exe" localhost:%d'

for the defaut VNC viewer.
The word command is part of the command expression. I label the *.zbd files with the server name or moniker for the batch files that will call the java based viewer. Only 1 zbd file is necessary if the built in VNC viewer is used.

Switches are used for both subnets. To provide the necessary connection for a sniffer, I connected a logging workstation to a hub between the LAN and the firewall. Using Ethereal, the network analysis tool available for various Operating Systems, [25] I captured packets during the logon process and simple data transfers to

[24] http://www.sans.org/rr/encryption/zebedee.php.
[25] http://www.ethereal.com/download.html

the network and onto the Internet for both the W2K Terminal Server and pcAnywhere. Data transfer is indeed encrypted for both applications. There is no indication of clear text in the packets. The logon process, however, with its 2 or 3 vital pieces of information (logon name, password, Logon Domain) was less than perfect. In high encryption mode and with the available patches, Terminal Server no longer shows the user name and logon domain in clear text as it does without high encryption and security patches. After the logon process, Terminal Server and workstation communicates session state with a cookie whose file name is user's logon name. That's one half of the information necessary to gain access. With pcAnywhere and my local policy, which is to have the system consoles locked, the user name and server name are sent back in clear text as soon as the connecting workstation brings up the unlock / logon dialog box with a CTRL+ALT+Del. If the server were already logged on, then the process would be entirely encrypted since that dialog box would not show up in the communcations process. I find leaving the console unlocked does not conform to the physical security policy. The stronger policy remains at the password level and encryption, requiring sniffing and decryption rather than using an adminstratively logged on Server as a basis for a portion of the security policy. See Appendix F for packet captures.

I am looking forward to using encrypted IPSEC tunnel enabled devices. I have tested the Netscreen Remote client's ability to create a tunnel and encrypt communications. Watching the logs as the connections are made and the tunnel it creates, brings up a lot of the terms I have studied in the recent past and in Security Essentials.These logs makes for greater understanding.

Additionally, remote access is provided for 2 other satellite offices, which dial a modem into a host with PCAnywhere installed and running.

Microsoft's RAS services are provided through a modem for the 1 traveling executive to check E-Mail and make other service requests while out of the office. This is used as an alternative to the web based e-mail only services and provided with a toll free number.

Risk remains at a low level and stays within the business guidelines. The vulnerability for RAS is that the phone number may be found through a war dialer program. These programs dial telephone numbers continuously searching for that modem tone and logging the applicable numbers. Then, if a user name and password can be determined that has Dial In priveleges (6 users, 1 at the administrative level), the threat increases the risk of compromise. The same is true of the pcAnywhere dial-in users. For Terminal Services access, the vulnerability exists at a more technical level. There is a DNS entry for the server, but the entry is not published for commercial services. Domain queries that would return zone information are not allowed. If the IP address could be learned, the threat comes from either guessing a user name and password or sniffing the user's name and trying to break the encrypted password. Terminal Service Access privileges are configured through a special sub applet in the NT4 Domain's User Manager. Access is restricted to 14 users. Console access is restricted by the physical security policy as previously stated. The threat is that a user's password can be sniffed from the Internet and decrypted. For this scenario the risk remain relatively low.

Conclusion

In conclusion, the policy for internal access from a remote internet location is stronger than the policy for internal access to the Internet. This was the expectation when I wrote the policy. After reviewing the policy using the Security Essentials Guidelines the network is protected by Defense in Depth. Using one's experience and resources to help clarify existing or non existant security policies may become more a part of the small business consultant's technology.

I am currently gathering more information on the impact of the NetBios flood, to provide the supporting evidence for the additional firewall purchase in the next fiscal year.

With the information and technical resources mentioned, I hope the evolution of a similar Field Service, Network, Technician (that I was) can progress to include the beginning skills of an InfoSec Tech. The small business arena needs low cost solutions for intruder detection to help provide an overall improved Internet experience. With only a small increase to the overall needs for IT at a small company, monitoring may not approach the proactive state, remaining basically reactive, but experience and knowledge in the security field can provide a great benefit in protecting the company's resources.

Improving availability, ensuring confidentiality, and providing the means for integrity, as the basis for a Defense in Depth strategy, provide a strong basis around which to expand one's knowledge. Understanding the relationship between the threat and the vulnerability and the exposure to risk, will provide a strong foundation with which to evaluate pre existing policies, as well as, to help in the future creation, implementation, and monitoring of the small business network's security policies and improved countermeasures for the inevitable attacks against availability, confidentiality and integrity.

Appendix A

A Description for Justifications of Implementing Terminal Services

Use the XP utility Remote Desktop or available Terminal Services Client for Windows 2000 to connect to the Terminal Server for improved performance in running all distributed applications.

The network link (computer to computer to Server) between the main building and the satellite office is a T-1 line.
This is 1.544 Megabits/second of shared bandwidth.
The network link between computers at each site (to each other) is LAN speed
This is 100 Megabits/second of dedicated bandwidth.
The network link to the Internet from/for all locations is DSL.
This is 384 Kbits/second out of shared bandwidth

Shared bandwidth follows the first come first served rule (with negotiated circumstances) with data packet collisions possible, which mandates new service requests.
Dedicated bandwidth is first come first served under dedicated negotiated circumstances.
Once service request starts the buffer is yours.

So the speed of Network divided by speed of T-1 yields the quotient signifying the difference in bandwidth for the network connection, but since the T-1 is shared we must account for the 10 possible connections that will be using the T-1 connection.
100/1.544=64.77 x10=647.7 (The main office communicates at as much as 647 time greater speeds) Alternately 100/(1.544/10).
If the T-1 were switched (dedicated), which is not currently possible, a user at the satellite office would have .015 (1.5%) the bandwidth of the same user at the Main Building. This is ~67 times more bandwidth for main office computers to servers than from the satellite office computers to main office servers.
Since the T-1 connection is shared and not switched, the difference can actually be as much as 10x or 667 times the performance / performance degradation.
Throw in a little Internet Activity which flows on the same T-1 between the Main Building and the Annex, and you can see the performance issues. 1 computer will usually never get more than 150Kbits / second from Internet, but that is still 10% of the T-1

So in order for applications to perform adequately we need a client-server based relationship for our distributed applications…
Therefore, we needed another Client Server based solution.
Windows 2000 Server provides this functionality with Terminal Services.
The Terminal Server will solicit actions of the accounting system on the behalf of the satellite client. The client sends only keystrokes (at 1 byte or 8 bits / keystroke) and the server sends back screen refreshes utilizing bitmap caching. The performance boost

should eliminate the 10 X sharing penalty as well as at least half of the 66 time difference.
With a baseline (Same process run from Terminal Server at Main Building, same speed workstations at Main Building, same speed workstation at satellite office) we should be able to determine the actual performance numbers the Terminal Server gives to the satellite office users.

Some basic speed descriptions can be found at:
http://whatis.techtarget.com/definition/0,,sid9_gci214198,00.html

Appendix B

Newtons First Law

http://www.physicsclassroom.com/Class/newtlaws/U2L1a.html

Many Physics lessons have been completed, but I would venture a guess to say most managers don't equate the decision making process of an individual or self with the laws of nature.

http://www.batesville.k12.in.us/physics/PhyNet/Mechanics/Newton1/HowManyWays.html See number 8 and 15

Appendix C

Historical Perspective from the Past to the Future

If we can get technologies like Alexander SPK (http://www.alexander.com) to combine with a Centralized patterning protection software like Symantec's Norton Anti-Virus Corporate Editions or Internet Security Systems Real Secure product line, we may have a single product that can provide a great security solution for the small business (eventually). Open Source products like **snort** (www.snort.org) use the same patterning technology. This seems like just the kind of technology that could be combined with heuristics, in order to discover malicious or compromising activity and halt the progress without letting the aberant behavior complete. At this point functioning services for the affected Server remain (for the most part) unaffected. Starting with Security Essentials, I had all sorts of hopes and thoughts for a basic security system for small business clients. For the past 5 years I have used a basic system for getting small businesses a presence on the Internet, including E-mail and remote access technologies. Now that Y2K and the Internet (business) Startup bubble is in the past, it seems to be the time to find a proactive solution for intruder detection. Information Technology for all businesses is merging the with Security Information Technlolgy to provide more complete protection of the services the technology is attempting to provide.

Appendix D

Discovering an Attack

I attended the first mentor led discussion group in early September 2002. I hadn't received my credentials to get the study material yet, but when the discussion turned to sniffers, packet monitoring technologies, TCPdump and Windump were mentioned. My goals for the course were to get some sniffing experience and feel more comfortable about log options and interpretation.

My interest over the previous 3 years centered around discovering what a sniffed TCP/IP packet looked like and if NetWare, Linux, Sun, and Microsoft packets looked the same. Figuring that out I then wanted to prove to myself that PCAnywhere and other Remote Access Software solutions actually did encrypt communications. I have found this information now because I have been armed with the information from the Securtiy Essential Course.

I recieved my credentials that 1st Friday after the first discussion. I downloaded the materials. Day 1 Chapter 3 introduces the Windump utility. I downloaded it. I started it. I looked at it. What was I seeing? I had a little idea, since in the same chapter, the discussion of TCP code bits of SYN, ACK, Urgent, PUSH, Reset, FIN were discussed. I could see my IP address, source sometimes, destination sometimes, the code bit, the service port, (I have known TCP uses service ports for a number of years now) and time stamp. I captured a couple of moments in time to review, since this was somewhat interesting. First I found the SSDP service broadcasting. I disabled SSDP, but I still saw IP activity when I was inactive. A week later I was seeing a log of activity even when a browser or e-mail application was not open. I was also browsing in the SANS reading room. I downloaded fport based on what I read in Douglas T. Orey's practical from 2001. (http://www.sans.org/rr/toppapers/free_tools.php) I then tried to shut down all my netbios ports, since I didn't necessarily need the services. I downloaded, installed, and enabled Black ICE. I turned off all services. I reviewed documents in the Microsoft KnowledgeBase. I brought it up at the weekly discusstion. I looked on Incidents.org and found out this was widespread. I had heard about this exploit as being similar to one of the first ever developed. I couldn't believe current technology, either my firewall (Linksys) or Microsoft Windows XP could not be configured to stop and drop these packets. As a test I removed the Linksys firewall and with all services turned off, I connected my XP station directly to the Internet's DSL Modem, monitoring the activity with both Windump and Ethereal. Between the 2 utilities I clearly saw the activity. Incoming packet with an ACK bit set, XP looking at it and doing a reverse lookup on the IP address, DNS returning no information, XP retrying DNS over and over, then trying any one on the network. The XP would ask the Default Gateway for name resolution, then XP would request the name of the computer with IP address incremented by 1 on my network. I was using 192.168.1.2 and the request would ask for 192.168.1.3. I disabled Netbios over TCP/IP. The packets seem to disappear, but it wasn't the case. They came back even stronger. The packets continued, but with Netbios over TCP disabled my workstation wasn't making DNS queries because of the packet, but the Linksys (my default gateway) continued to look for the non existant IP address

incremented by 1. I actually change my address to see if the request would change. It did.

I called Linksys to see if they knew about the flaw and could do anything to help resolve it. Tech support gave me a few configurations to try. Knowing what I did about their product, I soon realized it was not a stateful device, and they had no intention of addressing the issue. There is no option to block incoming ports.

I then contacted my ISP. They were unable to offer any router filter configurations, (their routers must not have been stateful either), but they did change my IP address, of course without notifying me first. With the new IP address I did not see any more Netbios-ns packets, before I replaced the Linksys with a Netscreen. Nothing stopped the packets except a stateful device knowledgeable enough to realize a valid TCP communications always starts with a SYN returned with a SYN-ACK and handshake completed with an ACK as shown on page 5 of the same Day 1, Chapter 3 document. Topical Information and the explanation given early in the lesson, gave me the means to discover and understand what is behind it.

Seemed like a built in topic for my practical, but my understanding of the evidence didn't exactly match what I was reading from the Internet Storm Center, (http://www.incidents.org), or the Cert Coordination Center, (http://www.cert.org), vulnerability notes, or Microsofts MS-00-047, (Q269239), patch which was rolled into the NT4 Security Roll UP and into W2K's Service Pack 2. I am resolved this is my limited understanding of the various exploits that the NetBios UDP communications empowers.

A decription of CERT from their home page.

"The CERT® Coordination Center (CERT/CC) is a center of Internet security expertise, located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University."

Appendix E

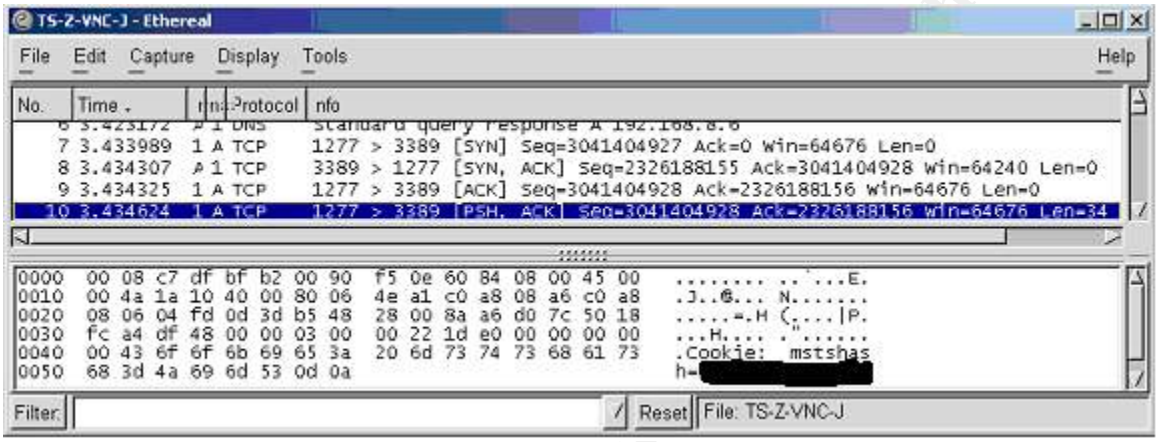
NTLM, a Real World Issue

One application I became aware of that used the NTLM for authentication of the privileges needed to start the service, even when the service was configured to run interactively. Many a system before the P3 processor would have startup difficulties because the NTLM authentication system would not (and should not) be given priority over the SAM authentication for the logon user, and the service would temporarily fail to start. The failed service start was simple a CPU cycle issue. This company had a workaround which I was unable to implement. Unfortunately this company's online support is fee based so I am unable to provide the supporting evidence for the above statement. I provide this footnote only to give an example of the secondary authentication system in Windows and to illustrate possible performance issues in addition to the security issues. Hopefully, the applications your businesses requires, avoid the NTLM authentication and you can disable the service or at least implement version 2 with syskey encryption.

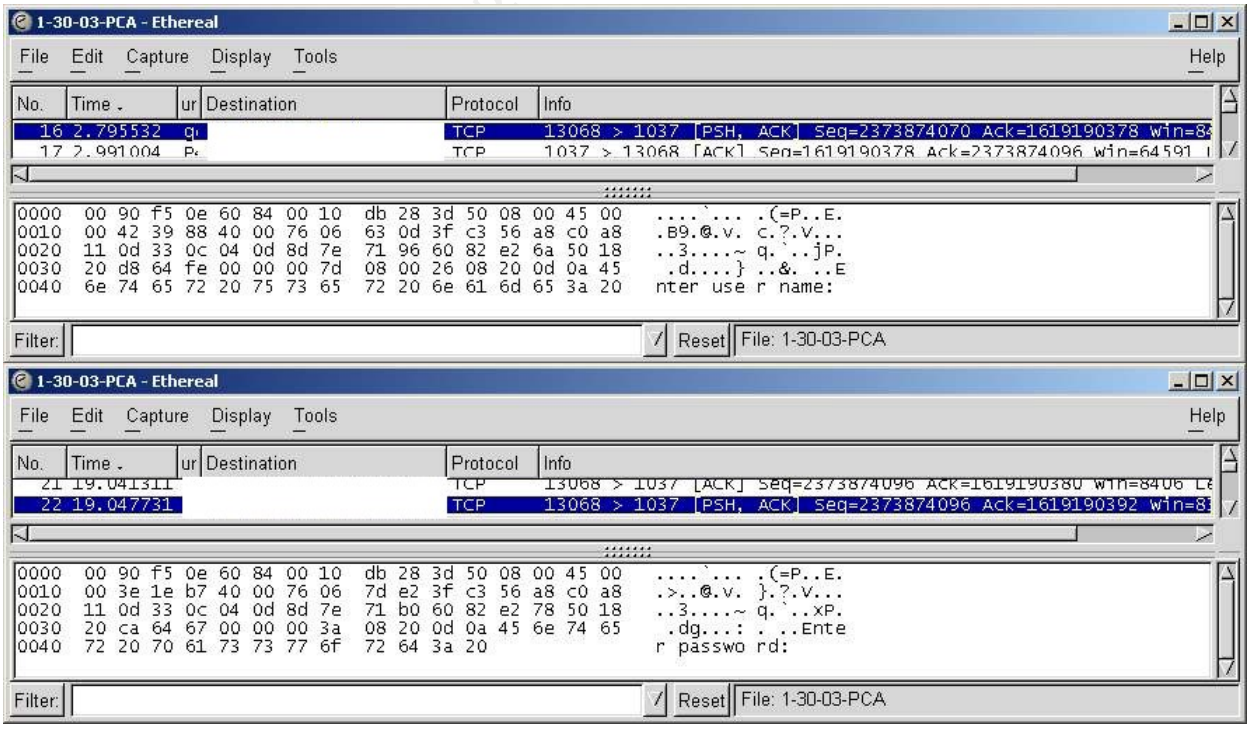
Appendix F

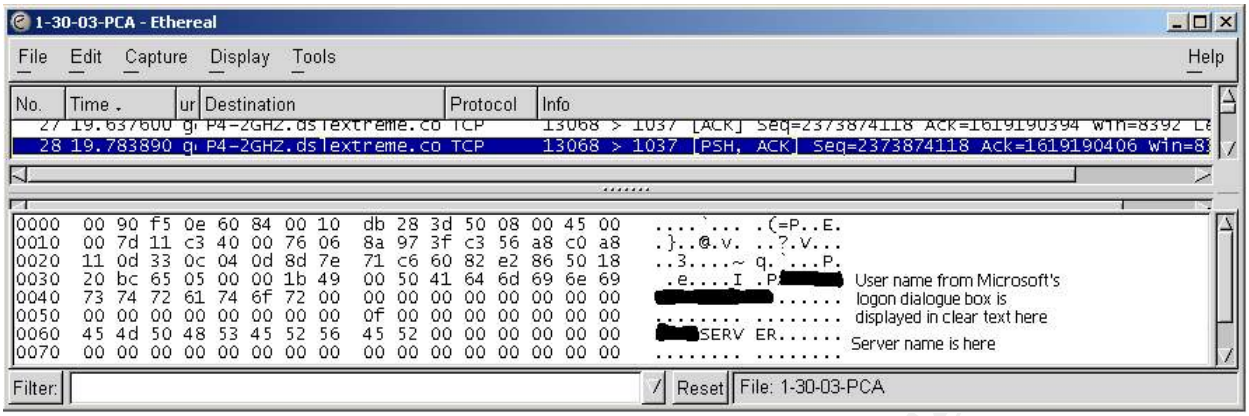
Packet Captures with Ethereal

This image shows the TCP communication initialization starting at packet No. 7 with the SYN -, SYN,ACK-, ACK and then a Push ACK. Logon credentials are sent as a piggyback ACK as described in Day 1, Chapter 3, page 6. Packet 10 with the Push flag (data to be delivered) displays in clear text the name of the cookie being received or acknowledged from the connecting workstation to the server. I have overwritten the valid logon name. Port 3389 is the default Terminal Services service port.



With the pcAnywhere, you can see the clear text from the pcAnywhere's logon dialog box. Similarly a couple packets later you see the Logon name and for some reason the server's name.





List of References

Cole, Eric., Newfield, Mathew., Millican John M. GSEC Security Essentials Toolkit. Indianapolis, Indiana: Que Publishing, March 2002. 83-88, 89-93, 308-314, 322-325.

Causey, James F., Wille, Christoph., Glenn, Walter J., Adamson, Jay.

Sams' Teach Yourself MCSE TCP/IP in 14 Days. Sams Publishing. 1998.

Cole, E., Kolde, J., Wendt, Carla. "Password Assessment and Management." Security Essentials, The SANS Institute, Information Assurance Foundations, 2001:

Northcutt, S., Kolde, J., Kerby, F., Wendt, Carla., "Threat and the Need for Defense in Depth." Security Essentials Day 2, Information Assurance Foundations, 2001:

Cole, E., Wendt, Carla. "Internet Information Server (IIS) Security." Security Essentials, The SANS Institute, Windows Security, 2001:

Cole, E., Northcutt, S., Kolde, J., Wendt, C. Hoelzer, D., Lam, J., Tuttle, D., Brinker, C. "IP Concepts II." Security Essentials, The SANS Institute, 2000-2002:

Slater, Derek. "What is Architecture?" Learning Curve Technology Made Simple. November 15, 2000. URL: http://www.darwinmag.com/learn/curve/column.html?ArticleID=9 (February 03, 2003)

Microsoft Windows Update. 2002 URL: http://windowsupdate.microsoft.com (February 03, 2003)

"Optimizing Applications for Windows 2000 Terminal Services and Windows NT Server 4.0, Terminal Server Edition." September 24, 1999. URL: http://www.microsoft.com/windows2000//planning/terminal/tsappdev.asp (February 06, 2003)

"fport - Identify unknown open ports and their associated applications." 2002. URL: http://www.foundstone.com/knowledge/proddesc/fport.html (February 9, 2003)

"Licensing for Terminal Services in Windows 2000." December 15, 1999. URL: http://www.microsoft.com/windows2000/server/howtobuy/pricing/terminal.asp (February 9, 2003)

"Microsoft Knowledge Base Article – 187623." How to Change Terminal Server's Listening Port. November 14, 2002. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;187623 (February 9, 2003)

"pcAnywhere IP Port Usage." May 5, 2002. URL: http://service1.symantec.com/SUPPORT/pca.nsf/docid/19981228102108l2?OpenDocument&src=hot&prod=pcAnywhere&ver=10.0%20for%20Windows%2095/98/Me/NT/2000&stg=2&base=http://www.symantec.com/techsupp/pca/&next=pca_10_search_other.html&sone=pca_10_tasks.html&tpre (February 9, 2003)

Michael Johnston. " Making the Case for Security at a Nonprofit Institution" March 2002. URL: http://www.giac.org/practical/Michael_Johnston_GSEC.doc (February 9, 2003)

"Vulnerabilities for this Port (from CVE)." URL: http://isc.incidents.org/port_details.html?port=137 (February 9, 2003)

"Nameserver DoS Attack October 2002." Jan 23, 2003. URL: http://www.caida.org/projects/dns-analysis/oct02dos.xml (February 9, 2003)

"WALLWATCHER a free Log Viewer for the Linksys(R) BEF Series of Etherfast Routers." February 4, 2003. URL: http://www.wallwatcher.com (February 9, 2003)

"Netscreen Products." URL: http://www.netscreen.com/products/index.html (February 9, 2003)

Vicomsoft, LTD. "What is Stateful Inspection" Technical Firewall FAQ. 2003. URL: http://www.firewall-software.com/firewall_tech/stateful_packet_inspection.html (February 9, 2003)

"Extended ACLs." Configuring IP Access Lists. October 30, 2002. URL: http://www.cisco.com/warp/public/707/confaccesslists.html#extended (February 9, 2003)

"Microsoft Knowledge Base Article – 239869." How to Enable NTLM 2 Authentication for Windows 95/98/2000/NT. October 8, 2002. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;239869 (February 9, 2003)

"Search the Knowledge Base." November 11, 2002. URL: http://support.microsoft.com/default.aspx?scid=fh;[ln];kbhowto (February 9, 2003)

"PWDUMP2." April 6, 2000. URL: http://razor.bindview.com/tools/desc/pwdump2_readme.html (February 9, 2003)

"Alec Muffett." 2003. URL: http://www.crypticide.org/users/alecm/ (February 9, 2003)

"Impact of Algorithm Optimization and Advance in Processors." Precomputing Dictionaries. April 28, 1999. URL: http://www.usenix.org/events/usenix99/provos/provos_html/node13.html (February 9, 2003)

"AFS." IBM Pittsburgh Lab. URL: http://www.transarc.ibm.com/Library/documentation/afs_doc.html (February 9, 2003)

"Microsoft Knowledge Base – Article 297989." PRB: Configured Identity Is Incorrect for IWAM Account. October 9, 2002. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;297989

"IIS Lockdown Tool 2.1." October 20, 2002. URL: http://www.microsoft.com/downloads/details.aspx?FamilyID=dde9efc0-bb30-47eb-9a61-fd755d23cdec&DisplayLang=en (February 9, 2003)

Risema, Nathan. "Secure (and free) IP Tunneling using Zebedee." June 26, 2001. URL: http://www.sans.org/rr/encryption/zebedee.php (February 9, 2003)

"Ethereal." February 9, 2003. URL: http://www.ethereal.com/download.html (February 9, 2003)

"The Speed of...." 2002. URL: http://whatis.techtarget.com/definition/0,,sid9_gci214198,00.html (February 09, 2003)

"Lesson 1: Newton's First Law of Motion." A High School Physics Tutorial. 2003. URL: http://www.physicsclassroom.com/Class/newtlaws/U2L1a.html (February 9, 2003)

"Physics 1 Dynamics Notes How Many Ways Can You Think of to State Newton's First Law (the Law of Inertia)?" November 27, 2002. URL: http://www.batesville.k12.in.us/physics/PhyNet/Mechanics/Newton1/HowManyWays.html

"Protect Your Network From the High Cost of Downtime." URL: http://www.alexander.com (February 9, 2003)

"Snort The Open Source Network Intrusion Detection System." February 10, 2003. URL: www.snort.org (February 9, 2003)

Orey, Douglas T. "Free NT Security Tools." August 6, 2001. URL: http://www.sans.org/rr/toppapers/free_tools.php (February 9, 2003)

"Internet Storm Center." February 10, 2003. URL: http://www.incidents.org (February 9, 2003)

"Welcome." February 7, 2003. URL: http://www.cert.org (February 9, 2003)

Gibson, Steve. "Shields UP!! NanoProbe Technology Internet Security Testing for Windows Users." URL: https://grc.com/x/ne.dll?bh0bkyd2 (February 10, 2003)

"Know Your Enemy The Tools and Methodologies of the Script Kiddie." Honeynet Project. July 21, 2000. URL: http://project.honeynet.org/papers/enemy/ (February 10, 2002)