Global Information Assurance Certification Paper

Case Study In Information Security

Diagnostic out of band modem security on a WAN router network

GIAC Practical assignment version 1.4b: Option 2

Christopher E DeSain

April 2003

Contents

Abstract

This paper outlines the steps taken to secure a prior implementation of diagnostic modem equipment in a large public organization's network infrastructure. This study will cover an investigation of the organization's vulnerabilities to exploits of the modem technology and the associated risk level. The proposed procedures and policies to reduce such risk will be identified. The paper will conclude with a final evaluation of the procedures and policies that were and were not implemented and the results each had on the final perceived level of risk.

Introduction

This study will focus on the security vulnerabilities of a large Wide Area Network (WAN) for a local company. The WAN that will be analyzed is comprised of over 800 remote locations, which are serviced by one on-site router. The WAN is a twenty-four hour, seven day a week operation with a maximum acceptable down time of four hours for services provided to it's remote users. In addition, it is important to note that the data contained on this WAN is considered highly confidential and the integrity of the data is critical to the mission of this organizations.

Due to the WAN's large geographical coverage, a third party vendor was contracted for maintenance of the remote router equipment. However, despite the implementation of the third party vendor, it was discovered that central site management was essential to fulfill the four-hour maximum down time requirement of the network. The out of band analog diagnostic modems were installed to accomplish the central site management requirement. However, equipment was installed for functionality with little consideration for the security vulnerabilities they imposed on the network. Unfortunately, as with many implementations of technology, no fore thought was given to possible security risks and it was only later recognized as a potential security hazard. Once the risk was identified, the next task will be to pinpoint the vulnerabilities related to the diagnostic modem equipment and define the consequences of that exposure.

In the assessment of vulnerabilities to the equipment we will analyze the state of the customer's current implementation. First, we will examine at the physical security of the hardware at the remote sites. Next, we will study the broader public presence encountered by connection of the network equipment to the public analog telephony community. We will then look at vulnerabilities that might occur prior to a breach of security, along with the vulnerabilities presented after an attacker has breached the security of the perimeter device. We will also look at tools an attacker could use to exploit those vulnerabilities and the availability of obtaining such tools. Following that assessment, we will be able to propose recommendations to correct and/or prevent the noted security hazards. It is important to note that the implementation of security after the fact usually involves increased complexity and possibly higher costs.

The customer's environment is in constant production; therefore, integration of security features while necessary must not hinder fulfillment of the operational goals. In proposing each solution we will include the costs to our customer's organization in dollars, human resources, along with the approximate amount of inconvenience that will

be experienced by the end user. In a perfect world, an organization would not need to weigh these factors and would simply implement every measure of security they could to safeguard their network environment. Unfortunately, in this scenario, limited resources force this organization to manage resources more carefully by striving to obtain maximum results at the lowest possible costs.

Finally, this case study will explore the various solutions given to this organization in an effort to reduce the perceived risk to the network. Each solution was presented with the corresponding costs of implementation and maintenance. The organization was also asked to evaluate its perceived costs in terms of possible losses resulting from a breach of security. Based on these factors the organization weighed the cost versus risk to select and implement security measures that greatly reduced the level of vulnerability to produce an acceptable level of risk. This course of action will ensure compliance with the organization's security policy, while at the same time will keep costs within budget.

Before Snapshot

The study commenced by exploring a representative sample of locations to assess the physical security surrounding the customer's equipment. The buildings and/or offices the customer occupied were considered secured environments. It was found that proper identification was required and thoroughly checked and logged to obtain access to the site. In addition, a specific reason for entry and/or an appointment was required to obtain access, which restricted access to only a limited number of people and provided logging for backward accountability. Once in the site very limited freedom would also be granted to an outside individual.

The next area explored was the installation locations of the network equipment in which very high percentages were found to be in shared vendor closets. Samples ranged from a shared telephone room, to a shared Heating Ventilation Air Conditioning (HVAC) room, to a janitors closet. A few installations were in locations adjacent to public view even when public access was restricted, which raised the question of physical access related to using analog modems. The answer being, they all connect to the telephone vendor and they all have a phone number associated with that connection. Almost every phone jack that the routers where plugged into were clearly marked with the dial access phone number. This opens the door to any vendor with access to the shared router locations and some public access as well. In the case of an attacker specifically targeting the customer's location whom did make the effort to circumvent physical security, he/she would not have to spend time at the physical location jeopardizing detection. Instead, he/she would then have a valuable key needed to engage in a remote compromise of the system.

Next, we will look at the phone number for any additional vulnerabilities. In researching the orders, we found the numbers were contracted as standard Plain Old Telephone Service lines (POTS), which meant they were part of the local exchange and had no restrictions placed on them such as incoming call blocks. Thus making them reachable by any public dialer in the local or long distance calling areas. In itself these factors do not create an exploitable vulnerability. However, the possibility of exploit arises when you combine the public media access with the hardware as installed by the

organization. The diagnostic modems were configured and installed to auto-answer. In auto-answer mode the modem will accept all incoming calls and present the caller with a terminal emulation. A standard tool such as HyperTerminal communications software distributed with the Windows operating systems could be used in conjunction with a PC's modem to make a the remote connection. The auto answer vulnerability also brings in our next class of attacker, the promiscuous attacker, who would not be directly targeting our customer but through the use of tools such as a war dialer could easily discover one of our many remote sites.

A war dialer is an easy to obtain tool ranging from numerous freeware programs such as ToneLoc and THC-Scan to more robust commercial programs such as PhoneSweep[1]. With the use of a war dialer, an attacker could set up to automatically call all numbers in an exchange or possibly a full area code. He would then be presented with a list of numbers through use of this software that had a modem set to auto-answer. In fact, the commercial war dialers are getting so sophisticated that they provide the user with the ability to sort on all kinds of variables including the type of device detected[2]. In researching Sandstorm Enterprises web site[3], a distributor of PhoneSweep for a list of detectable devices, I easily found the organizations router equipment in the list of detectable devices. At this point, a promiscuous attacker finding a moderate to high-end router in his list of detected devices after a sweep would surely mark such a device as an item of interest. At this point, it is clear that an exploitable vulnerability to the diagnostic modems is present as currently implemented. We have also demonstrated that attackers specifically targeting our customer, as well as promiscuous attackers discovering our systems, can exploit the vulnerability.

The threat is now at the front door, assuming that our attacker by whatever means found our number and made a connection to our equipment. The dialer is first presented with a password secured login screen. The screen banner clearly defines the hardware manufacturer and it prompts for a user name and a password. It is important to note that knowing the hardware manufacturer of the device in many cases can help an attacker in several ways. Such knowledge of the hardware manufacturer allows an attacker to look for a list of known exploits related to particular equipment[4]. Exploits that can take advantage of bugs in code as well as purposefully placed back doors into a system. Now we'll look at an example for illustrative purposes. The manufacturer in their effort to support the customer anticipates a typical support call might be, "We lost our password and are locked out of the box". In anticipation, they designed a clever multi key command to reset the password back to default settings. It was a great concept until the customer told his friend, whom then told their friend, and the next day it's posted on a web page as common knowledge. The vendor fixes the back door in their code by releasing a patch or subsequent revision of code. However, until the customer updates all his hardware with their new code the system is vulnerable to the exploit.

---

[1] http://www.sans.org/rr/tools/phonesweep.php
[2] http://www.systemexperts.com/tutors/wardial0299.pdf
[3] http://www.sandstorm.net/products/phonesweep//sysids.shtml
[4] http://www.phenoelit.de/dpl/dpl.html

In case of the organization in this study, it's hardware vendor was contacted on this issue and it established a password-reset feature was part of the code but could not be executed with a diagnostic modem connection. This was tested and was proven to be true. The more common use of manufacturer information is that often times many organizations use the default user names and or passwords supplied with the equipment for authentication. It is a frequent mistake made by many organizations especially when security in the implementation was not a consideration. In our customers case, the hardware vendor uses not only a default user name but it is not changeable by the customer. Therefore, the attacker with a little simple background knowledge or research on the device has one half of what he needs to authenticate. The attacker may now try and use another readily available tool, such as a brute force password hack, to find the password to authenticate.

Brute force password attacks are simply an automated repeated attempt to guess a password. The program will try all possible character combinations until it succeeds. Most brute force tools will start with or can be configured to start with dictionary attacks, common names, and other common alphanumeric passwords[5]. We found the authentication interface by default was set up with the three strikes your out form of protection – meaning, after three failed attempts the connection was cut. This is a deterrent but, unfortunately, the interface was not locked out with any number of failed attempts nor was the authentication account ever frozen to prevent continued password guessing. This scenario would create the perfect environment for the use of a brute force password hacking tool. One liability that must be noted of brute force password guessing tools is the considerable time frame needed to complete the process[5]. It will be shown in this paper that failed authentication attempts associated with password guessing can reveal an attackers presence. It was found in our organization's case, that this time frame would be considerably reduced due to the implementation of a password that contained only six characters. It was also found to be a proper name in all lower case. This at best would be considered a weak password and result in easy prey for a brute force attack.

In the attackers attempt to gain access through password guessing we recognized every failed authentication attempt would reveal the attack was in progress. The detection would take the form of log entries, which would be recorded in the routers local log as evidence. The organization, to date, has not implemented central logging nor is there a log evaluation policy in place; therefore, the failed attempts at password guessing would not be detected until after the fact if ever.

In an attempt to improve security of the network, the organization did purchase, but never put into production, a simple network management protocol (SNMP) event correlation tool. The routers were configured to send SNMP traps to a central server hosting the event correlation software and each trap would be logged based on criteria set by the administrator. With this tool, events such as the failed authentication attempts sent from the router, could be configured in the central event correlation software to create an alert with real time results. For example, if the event correlation software received a failed authentication event nine times within a two-hour time frame it would then alert

---

[5] http://www.itsecurity.com/asktecs/jul101.htm

the network staff. The alarm to staff could be configured as a pop up window on the central site screen, an automatic page to a beeper, or even a text message to a cell phone. While the customer had the foresight to configure the information to be sent to the central server, unfortunately, no such trigger system was implemented with the correlation software so all it does is log the incoming events. So absent of any alarm system, a breach of security could not be proactively prevented or easily corrected because the company would not have a real time alert of where or when the attack was made.

Further Analysis

In this study, we also discovered that the organization's network was vulnerable to attackers who targeting the network purposely, along with prospective attackers promiscuously looking for a target. We have exposed the readily available tools at the attackers disposal and the vulnerabilities that can be exploited by each tool. It is safe to say there is a clear vector of compromise to the network equipment as it pertains to the diagnostic console modems in their current implementation.

With this in mind, we then took a look at the customer's next layers of defense. You may ask why look further, when in this case study we are looking at securing the diagnostic modem. However, the answer is quite relevant to this case study because we may not be able to reduce the risk of a breach through the diagnostic modems to zero. In essence, the customer needs to know the consequences that would result if a breach should it occur. In fact, the knowledge of vulnerabilities in the next layers of defense in the network will directly influence how the customer perceives the risk associated with the diagnostic modems. If the attacker gains access but is highly restricted and can do little, the risk may be looked at as low. On the contrary, if the attacker gains the type of access that will infringe on confidentiality and/or impact the reliability and availability of the network, then in most cases the risk would be deemed substantially greater. Therefore, clear understanding of the risks will lead to a more suitable cost versus risk analysis, ultimately resulting in better decision making related to the selection and implementation of new security measures.

At this point we are now authenticated and logged on to the organization's router. Upon the successful log on attempt, we were first presented with a welcome banner. Next, we discovered that the help function was enabled on the command line, which provides a list of executable commands to the user. Although this may be a time saving tool for the typical user, the downside is that it provides potential attackers with a quick reference guide of the manufacturers proprietary commands associated with the Operating System. With the knowledge of a few quick commands, the attacker can remove the router from the network. An example with a personal computer would be to run a format command followed by a boot. In that scenario, if you format the hard drive and do a boot the hardware looks for boot files to load an operating system. If the files are gone the hardware is rendered useless until the files are restored.

Another technique the attacker may try is to create bogus configurations and leave it as a booby trap for the next hardware boot. If the router was reduced to a non-functional state this would results in a denial of service. Fortunately, in this organization's network architecture this would only affect the users at the individual site

because the routers are remote access routers pointing back at the central site. No applications of any importance are hosted from the remote locations so the resulting costs due to the denial of service intrusion would be minimal. However, it would be unlikely for an attacker to take the time to breach security and only cause a denial of service attack to the first device encountered for fear his presence would be revealed. Instead, it is more likely the attacker first would try to hide the breach thus providing more time for exploration.

A router should be looked at as a gateway device because it points users to other networks and (in almost all infrastructures) to the core of the network or several host networks. One look at the routing table would give an attacker a starting point to map out the network and through the use of commands such as telnet, ping, and trace route, the attacker could explore and create a map of the network. Prior to commencing this study, we had knowledge of the network topology so we went directly for the next device on a path to the central site known as an area border router.

The telnet protocol was used to establish a connection with an area border router, as it was a feature supported by the router operating system. It was found the same log in screen was presented as was presented in our initial connection with the diagnostic modem in the remote router. Once the connection was made, the same user name and password was used for authentication on this area border router and all other area border routers. Next, a telnet connection to the core router was made and once again the same log in screen, user name, password, and welcome message was used to gain authentication. At this point a denial of service attack on the core routers would literally shut down the customer's wide area network. With all applications hosted at the core and no way to reach them all remote users would be out of service. So we have shown access to the core of the routing network but the wide area has to have a point of contact with the host network. Typical infrastructures include a DMZ network separating the wide area network from the host network. In addition, a firewall, usually combined with a router or layer three switch, is typically used to pre filter traffic to alleviate unneeded load on the firewall are also typical. Through this study, we discovered that connections to the firewall's public wan side interface were attempted; however, the appropriate protocols were correctly filtered so no connection could be successfully achieved.

Unfortunately, there is always the possibility of an exploit and also of user error. For example, a firewall administrator doing testing may open a port and forget to close it -- without proper procedures and enforcement of those procedures the open port may not be discovered until it is too late. The change control policy in place at the time of the study made no reference to the firewall and the administrator was free to make changes at any time with no notifications or documentation required. Although the public ports of the firewall were closed, it was found the telnet protocol was allowed through the firewall so a telnet to a device on the private network was completed. Then a connection to the private open telnet port on the firewall was completed. Another flaw identified by this study was that the firewall user name and password were found to be the same as the routers. Needless to say, an attacker on the command line of your firewall ranks very high in terms of security breaches. What makes the security situation even more dire is the fact that our customer had no policy in place for event logging and log evaluation. With the absence of logging and log file evaluation, the intruder who gains access could make configuration changes without detection. Furthermore, the lack of central logging

to protect the log files from tampering would also give the attacker greater opportunity to cover his tracks and go undetected.

One last critical factor in the cost risk evaluation would be that the customer had no disaster recovery plan in place. Employees had been given no specific duties or direction on what to do in case of an emergency. More specifically, written documentation of procedures for recovery of major systems were non-existent. In addition, there was no evidence of any back up procedures for core equipment configurations. The consequences of not having an established disaster recovery plan in place, to deal with a system outage of the core systems, would result in down time well beyond the established four hour maximum limit that is specified in the service level agreement.

We started our study looking at the diagnostic modem technology and vulnerabilities of that technology. We then looked at exploits of this vulnerability and the closely associated security measures in place down stream right to the core of our customer's network. We can clearly see how the state of security in one technology affects the risk level of other technologies. Security as a whole for the organization should be comprised of a very tightly woven architecture of technologies and the security measures of each. We may now present solutions to secure the diagnostic modem technology. The organization's management can now more accurately evaluate the cost of implementation based on the perceived risk not only to the isolated system but also to the security environment as a whole.

During Snapshot

The first proposal would be the removal of the diagnostic modems. This would eliminate all associated vulnerabilities resulting in a zero risk solution. The resource costs of removal would by fairly low and could be implemented as a stand-alone solution for this technology. It would also result in a decreased risk for all other associated technologies. The one unacceptable cost of removal of the modem equipment would be the resulting inability for the organization to meet its business goals so the proposal was rejected. However, rejecting the idea of removing the diagnostic modems means that a risk free solution would not be possible leaving us no option but to explore and recommend risk reduction solutions.

The first risk reduction implemented proposal would be to improve the physical security of the equipment. As noted previously, the physical equipment did have a few vulnerabilities related to public presence, along with being stored in shared vendor closets. The physical security risks for the diagnostic modems were presented in the form of the visible number labeling of the telephone jacks. It was recommended all numbered phone jacks were to be replaced with blank jacks at all locations and clear instructions were attached to the phone line stating the policy to avoid further labeling by third party vendors. Also, a security policy was created and communicated to prevent disclosure of the phone numbers by members of the organization.

We next looked at the restriction of service available from the telco vendor and modem hardware manufacturers. The analog lines as stated previously were "POTS" lines. After researching with the telco vendor, it was found that no restrictions could be imposed on the line to filter incoming access. Unfortunately, the local telco provider was

unable to offer any other line solution with extended features compatible with our modem so no changes to the connection medium could be made. The hardware currently in service was set for auto answer and did not provide any incoming connection authentication or filtering. To remedy that situation, replacement hardware was proposed that could provide incoming ID filtering and or authentication as well as a slightly cheaper second hardware option of a modem that had a feature called dial back. On a cost versus risk basis, the implementation of the new hardware was rejected. However, this decision was not based on the current level of risk. The level of risk would need to be greatly diminished by reducing or eliminating vulnerabilities down stream of the diagnostic modems.

Upon a connection to the diagnostic modem, we noted the terminal screen banner contained the router device's brand name and a user name password authentication entry fields. We also noted that after completion of a login the user was presented with a welcome banner, which was consistent throughout the network from remote routers to the core routers. After working with the hardware vendor, a script was written to remove the Manufacturers name presented in the authentication screen banner; therefore, preventing the disclosure of the hardware manufacturer. In turn, common exploits of that vendor's product, although still present, would be far less evident to an attacker. The default user name was still not configurable in the current level of code. In response, we recommended that the organization put in a change request with the vendor that would permit using a new user name when the hardware vendor released the software code. The default user name or in this case the only available user name would then not be a known starting point for an attacker. The relatively simple implementation of these changes will significantly decrease an attackers ability to breach the routers authentication. Although the risk has not been reduced to zero, the difficulty has been increased to a level that should dissuade many promiscuous attackers looking for an easy target.

Although the security measures mentioned above might deter the attacker who is specifically targeting our system, the network would still be vulnerable without further measures. As noted earlier, the attacker might have been on site at one time, which would have given him the opportunity to get the equipment's manufacturer information. Although the phone numbers were removed from plain sight, this would not prevent alternative methods of breaching security. Our policy of non-disclosure is just that a policy and not an absolute. A notable example of a method to breach that policy could be through the use of social engineering. Social engineering is generally a hacker's clever manipulation of the natural human tendency to trust[6]. To test this I called one of the organizations sites posing as the upper level network staff and used the pretext that we lost the documentation for that site and had a mission critical repair that had to be done immediately. As anticipated, the workers on site were so willing to help that they had the phone company do a tag and locate to get the number at the organizations expense – all in the name of human trust.

---

[6] http://www.securityfocus.com/infocus/1527

Our attackers with or without the hardware information would still need to guess at the password or test exploits. However, no authentication lockouts were in place on the interface. Although logging was done internal to the router, no centralized logging on the server already purchased was in production nor was a log file evaluation policy in place. As evidenced by the router vendor, no authentication lock out was available and although a change request was made it was not accepted by the vendor. The central site logging server was recommended and put into production and configured to record log updates from all remote routers and firewalls. The central server also was configured to send a copy of all logs to a second server on a secure subnet of the network. This was done to increase the integrity value of the data. Data from the central server could be cross-referenced with the date of the secure server. Discrepancies found would quickly point out tampering of the log files. A policy, with the human resources to enforce it, was created to ensure daily log file evaluation. To further enhance the logging policy, the SNMP event correlation tool was utilized to create alerts from the collected SNMP events sent from the remote routers.

Notifications in the form of pop up windows and text paging were configured to warn the network staff in real time of possible security issues. For example, the receipt of five authentication failures from a single host would result in a pop up window notification on the network monitor's screen. Another example would be a repeat of authentication failures from the same host for more than thirty minutes, which would result in the event triggering the tool to send a text page to a senior network staff member. This would quickly identify a possible attempted attack so actions could be taken to prevent the breach. In the event of continued false positives, the administrator could quickly readjust the threshold for alarms as appropriate. Log file analysis would provide a means to identify and possibly catch an attacker that has gained access to the network or possibly identify an internal threat to the network. The log file analysis would also be a strong means to enforce a change control policy. Changes to hardware and software devices, such as firewall rules, would be captured in the logs. By comparing the changes made it could be interpreted if the change followed the current policy.

We will now look at three policies that were implemented in the network layers. The policies were originally proposed specifically to increased security on the diagnostic modem equipped remote routers. However the discoveries of the study found the same vulnerabilities present in hardware in mid and central layers of the network as well as core infrastructure. The policies were then adapted for system wide utilization.

The first policy to be implemented was a password policy. The password policy allowed the use of only "strong passwords". In researching the criteria for creating a strong password several sources were referenced. Each reference had a slightly different opinion on the exact criteria but several common factors were evident in all constructions and a consensus of the opinions was utilized. The passwords would be comprised of at least one upper case letter, one lower case letter, a numeral, a special keyboard character and contain a total of ten characters [7]. Password rotation on a semi annually basis was

[7] http://www.fin.ucar.edu/it/dsn/userdocs/pswdguide.htm

adopted. In consideration of the human resource costs of maintenance the semi annual standard was chosen. Individual unique passwords for all network equipment was initially proposed but later rejected due to the size of the network and cost associated. However, the defense in depth concept of layering was incorporated in the password policy implementation[8] by using the networks already existing layered structure. Logical concentric security layered zones were created in the network to increase the overall security, but more specifically to increase the difficulty to compromise the networks core. The remote routers would use one password. In the event of an exploit of that password layer the attacker would then be faced with the task of breaking other passwords to breach each concentric layer on a path to the central site. The policy also covered disclosure of the passwords to authorized personnel only and storage of passwords for recovery in a secure off sight facility.

The next suggested implementation was to the welcome screen banner presented upon authentication. Working with the hardware vendor the Welcome message was removed and replaced with a Warning banner. The warning banner while a possible deterrent was put in place more for the purpose of litigation if an attacker were caught. It would be in the best interest of the company that we did not present the intruder with a welcome banner. Instead a warning that his unauthorized access was prohibited and that all rights to materials collected would become property of the host organization[9, 10]. Final banner approval was made with consultation of the organizations legal department. The following is the final implemented banner.

Warning Notice!

This is a XXX XXXX XXXXX computer system, which may be accessed and used only for authorized Government business by authorized personnel. Unauthorized access or use of this computer system may subject violators to criminal, civil, and/or administrative action.

All information on this computer system may be intercepted, recorded, read, copied, and disclosed by and to authorized personnel for official purposes, including criminal investigations. Such information includes sensitive data encrypted to comply with confidentiality and privacy requirements. Access or use of this computer system by any person, whether authorized or unauthorized, constitutes consent to these terms. There is no right of privacy in this system.

---

[8] http://nsa1.www.conxion.com/support/guides/sd-1.pdf
[9] http://wwwoirm.nih.gov/policy/warnbanners.html

[10] **http://www.itsc.state.md.us/info/InternetSecurity/BestPractices/WarnBanner.htm - format4**

The last proposed implementation was to turn unneeded protocols off on router interfaces. An important example was the removal of the telnet protocol from the area border routers outward facing interface where there was no need for a remote router client to telnet back in the direction of the core. Other removed protocols included HTTP, TFTP, and ICMP. Many were removed to eliminate possible present or future exploits of the protocols. If protocols are not needed, best practice would suggest to turn them off. For instance, ICMP although highly recognized as a trouble shooting tool, was specifically removed where possible to prohibit trace routing and ping functions to prevent exploratory network mapping.

One final outcome of the study was the introduction and implementation of a disaster recovery policy. The policy included documented procedures for recovery of systems, including job responsibilities, along with a clearly defined backup procedure for recovery process were also documented separately. With the implementation of the disaster recovery policy the customer reduced the perceived costs as they pertain to losses if a disaster were to occur due to a security breach.

After Snapshot

The organization has clearly taken great steps in securing its network. More importantly, it has retained the ability to use the diagnostic modems as an essential tool in providing the mission critical support for its remote network sites. Throughout the implementation of these security measures we can see the customer made no real change to the actual diagnostic modem equipment. The recommended hardware change to a more secure modem was ruled out on a cost versus risk analysis basis. The cost and risk would now be based on the newly perceived risk after putting other closely related security policies into production. Those costs would be based on the actual resource cost of implementation and the new lower perceived cost of losses resulting from a breach of security.

The reduction in the perceived cost can be correlated with the newly created disaster recovery policy. Although, it is clear that risk still exist, this study pinpointed many of the vulnerabilities and we have hardened and/or removed many of the vectors of exploit to these vulnerabilities. The end result is a level of risk the organization can deem acceptable. With the removal of system identification on the log in screen and implementation of a strong password policy we have greatly strengthened the required

authentication. Before the implementation of these recommendations, the attacker was literally given one half of the authentication process and the other half was secured with a very soft password. Upon authenticated the user was originally presented with a greeting welcoming him to the interface. In its place a more purposeful warning banner. Imposing possible deterrent value, but more importantly could be used for future accountability and potential prosecution.

The status of network before the study was a flat security domain with a single system wide authentication password and tools to easily map out and traverse the network. With the implementation of a password policy incorporating the defense in depth layering model authentication layers within the network infrastructure were created. Removal of protocols such as telnet and ICMP disabled tools that could be used to map and traverse the network layers. Thus further reinforcing isolation of the network into separate security layers. Prior to the study, the organization had no in- production logging or SNMP event correlation and authentication to network devices was not monitored giving attackers unlimited ability to attempt to authenticate. In addition, the lack of logging configuration changes resulted in minimal detection by reducing the effectiveness of the existing change control policy as well as allowing changes made by intruders to go unnoticed. The implementation of a central logging server and SNMP event correlation gave the customer real time warnings of failed authentication and an audit trail to identify unauthorized activities. With proper action the real time warnings can thwart repeated authentication attempts and possible breach of securities. Vulnerabilities created due to a human error miss-configurations leading to possible exploit can be detected and corrected before the error can be exploited. Another important feature of logging would be the creation of a baseline. Comparing the baseline to daily logs could isolate anomalies in the network that would be otherwise undetectable by looking at single line items.

Conclusion

My participation in this project was as a third party consultant. What started out as an inquiry into the security of the diagnostic modems lead to several security implementations within the network section. The implementation of servers for logging and the creation of a new section within the organization for log evaluation were proposed and implemented. While I was directly involved with generating solutions for the security vulnerabilities facing this network, I was also charged with assessing the cost versus risk reduction related to each proposal. Although every proposal was not implemented, the organization was able to make an informed decision on what to implement based on factual information presented in this study; ultimately, achieving their goal of heightened security at a reasonable cost

References

1. Hodes, Greg. “PhoneSweep: The Corporate War dialer.” Sans InfoSec Reading Room. 10 September 2001. http://www.sans.org/rr/tools/phonesweep.php

2. Tang, Cheng & Gossels, Jonathan. “Wardialing: Practical advice to understanding your exposure.” February 1999. http://www.systemexperts.com/tutors/wardial0299.pdf

3. PhoneSweep Identified Systems. 26 August 2002. http://www.sandstorm.net/products/phonesweep//sysids.shtml

4. Default Password List. http://www.phenoelit.de/dpl/dpl.html

5. Lockhart, Harold. Nicholls, Weston. Nauado, John. Jugdar, Rauin. Hale, Ron. IT Security.com: Security Clinic. http://www.itsecurity.com/asktecs/jul101.htm

6. Granger, Sarah. “Social Engineering Fundamentals Part I:Hacker Tactics.” 18 December 2001. http://www.securityfocus.com/infocus/1527

7. Desktop Systems & Networking. “Guidelines to strong passwords.” http://www.fin.ucar.edu/it/dsn/userdocs/pswdguide.htm

8. National Security Agency. “Defense in Depth: A practical strategy for achieving information assurance in today’s highly networked environments”. http://nsa1.www.conxion.com/support/guides/sd-1.pdf

9. Center For Information Technology. “NIH Policy on warning banners.” http://wwwoirm.nih.gov/policy/warnbanners.html

10. Information Technology Support Center. **http://www.itsc.state.md.us/info/InternetSecurity/BestPractices/WarnBanner.htm - format4**

Last Updated: May 26th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event