Global Information Assurance Certification Paper

Case Study:

A Path of Least Resistance Approach to Securing Residence Hall Networks

GIAC Practical V1.4b – Option2
Author: Allen Brokken
Submitted: 6/18/2004

Abstract

One of the greatest threats to university campus networks is the large population of student owned and managed computers. These computers tend to be poorly maintained and configured with regard to information security. This Case Study analyzes a university's successful attempt to mitigate the risks associated with these computers without changes to the infrastructure or the implementation of forced controls on these computers.

Introduction

Typical University (TU) is a medium sized state university. The campus network is similar in design to many college and university networks. It is broken up into various security zones, with firewalls between each zone. The infrastructure for the campus is handled by the Central Networking Group (CNG), a sub-division of the Central Information Technology division (CIT) which is responsible for all information and telecommunication functions at TU.

This study focuses on a single network security zone that includes connectivity for all of the student residential halls and the Fraternity/Sorority houses. This network zone is referred to as the Residence Hall Network (RHN). RHN is composed almost entirely of student managed personal computers. A very small number of TU owned and managed computers are connected to RHN, but they are a very insignificant percentage of the whole and will not be considered in this study. The majority of the approximately 3000 computers in RHN are using the Windows 2000 or Windows XP operating systems.

The main purpose for RHN is to provide commodity internet access for students living in the Residence halls. While some administrative functions and maintenance occurs over this network, it was not designed to host TU production services such as email or registration systems. RHN exists to offer students connectivity to educational resources from their residence hall, and to provide TU a competitive advantage in recruitment.

The educational resources include on-line homework assignments, tests, message boards, research, course add/drop, and many other collaborative tools. TU also provides each student a TU hosted email account. Student access to TU email accounts is primarily done through web based email clients. The services are not actually hosted in the RHN security zone, but the quality of the connectivity within RHN has a direct impact on the students' ability to access these resources.

The competitive advantage RHN provides to TU is internet connectivity for students comparable to the best commercial broadband internet services. In the late 1990's it was determined that a reliable high-speed network service offering for the TU residence halls would have a great influence on the decision of a prospective student to come to TU. This service includes student use of peer to peer file sharing, network based games, instant messaging, and general internet browsing at the least.

The one major thing RHN does not allow for is dedicated server access from outside RHN. All subscribers are issued addresses via DHCP and the RHN firewall prevents connections from being established with hosts inside the firewall from hosts outside the firewall. This additional measure was a relatively new addition to the RHN infra-structure in the fall of 2003. Blocking access into the

network was not a part of the original RHN design; however the legal implications associated with file sharing networks[1] forced TU to implement these filters.

Use of RHN is governed by the TU Acceptable Use Policy (AUP). The AUP uses very broad language that does not address particular network or computer technologies explicitly. The AUP grants CIT the right to inspect computers attached to RHN for network vulnerabilities, and disable network access to computers that are; disrupting network functions, engaging in illegal activity, violating other university policy or have been deemed too insecure to be allowed to connect to the network.

CIT most often disables network access for violations of the Digital Millennium Copyright Act[2], and to computers shown to have weak or no administrator password. Both of these AUP violations have well documented procedures and consequences. These incidents represent less than 20 disconnects in a typical week, and are handled in a very programmatic manner. Occasionally there are other incidents involving violations of the AUP; however these are handled on a case by case basis.

Problem Statement

In the fall of 2003 the internet worms associated with the RPC-DCOM vulnerability in the Windows operating system[3] caused a major disruption to RHN. This incident began almost immediately after students moved into the Residence Halls in mid-August. The volume of infected computers forced CNG to disable service globally to RHN in order to keep the rest of the campus network functioning.

This proved to be a tremendous issue for the students living in the Residence Halls. Many of the applications needed to actually participate in class, as well as email and other administrative tools are entirely network-based. Loss of access to the Residence Halls meant students had to go to a computer lab connected to another network zone, or use a traditional dial-up connection to get to the resources they needed.

Many students became disillusioned with the whole idea of in-room internet access. The built-in high-speed connectivity was supposed to allow them

[1] Carlson, In 2003 the major producers of audio and video based entertainment began suing students at various Universities for illegally distributing their intellectual property. Prior to this CIT blocked the traffic of specific applications based on signatures during peak times of day to conserve bandwidth, but did not have an explicit block into the RHN network.

[2] U.S. Copyright Office, The DMCA is the legislation that allows intellectual property owners to prosecute individuals who distribute that property without proper authorization or compensation to the owner.

[3] The RPC-DCOM vulnerability is known by many names but the most complete reference can be found at Microsoft's Security site http://www.microsoft.com/security/incident/blast.mspx

connectivity to everything they needed. Instead, the act of connecting to the network allowed an internet worm to infect their machine, and make it continuously reboot. Even students who didn't need internet access to do their school work were inconvenienced while they sought a remedy for the constant reboots.

Over the next 6 weeks, service was restored to the network incrementally. The first access CIT was able to allow was basic HTTP/HTTPS access to specific campus resources. This happened in the first week of the outbreak, and allowed many of the functions needed for class to become available. As the number of infected machines declined and other measures could be enacted the number of services allowed was increased.

One of the biggest inconveniences even after CIT began to restore basic web access was the loss of connectivity for instant messaging applications. The variety of instant messaging applications in use, meant that restoring service for these was far too complex to re-enable quickly. In many cases the loss of instant messaging was a greater inconvenience to the user than loss of all other access combined.

Approximately 2000 incident tickets were generated in response to this outbreak, representing an equivalent number of student computers. With a typical load of less than 20 AUP or other violations a week, the generation of 2000 tickets in slightly over a week was far beyond the scope of what could be managed by the staff assigned to deal with security incidents. Ultimately all other work associated with the CIT division was impaired or delayed for the first 3 weeks after the onset of the exploit, and staff could not fully re-engage in normal activity until the entire network functionality was restored.

After the incident, the Central Security Group (CSG) of CIT was tasked with estimating the risk of a future outbreak of this magnitude. CSG used data gained from the RPC-DCOM experience to assess the vulnerabilities inherent in the system, and then was given the mandate to proceed with measures to mitigate that risk. The outcome of that mandate has generated a number of simultaneous initiatives that are still in progress. The focus of this study is a single piece of the global defense strategy. This measure was aimed specifically at the students responsible for maintaining their personal computers. The author continues to be personally involved in the design, implementation and maintenance of this particular solution, including acting as the primary author for much of the code and documentation.

Vulnerabilities Revealed by RPC-DCOM Exploits

Support Staff Availability

There ratio of full time personal computer support staff to individual computers connected to RHN is approximately 1 to 500. In the initial triage of the incident, CIT management mobilized all staff that were capable of remedying the issue regardless of job function. This effectively reduced the ratio to 1 staff per 100 computers. Reassigning staff for this purpose, resulted in a massive decrease in productivity for CIT, and ultimately proved to be a futile gesture as remediation on average took over 90 minutes. For the computers represented by the 2000 incident tickets it would have taken approximately 3000 staff hours to finally eradicate the problem. The inability to devote sufficient staff time to the issue was a significant liability.

Network Infra-Structure Capacity

There are more computers in the network zone than can be effectively filtered by the RHN edge devices if multiple computers are exploited simultaneously. As will be seen later in this document, the filtering capacity necessary to deal with a worm is highly dependent on its propagation algorithm. The network devices, including firewalls are designed to deal with a maximum level of traffic based on normal needs. A worm throws that completely out of balance and ultimately it is not cost effective to build the network to withstand the most extreme case.

An additional complicating factor is the design of the network firewalls. A typical firewall is designed to drop or redirect traffic coming from an outward facing interface, not to block traffic from the inside going out. Due to the nature of the RPC-DCOM exploits the massive number of connections going from inside the firewall out to the rest of the network was far beyond their capacity.

Perimeter Defense Limitations

Perimeter based devices cannot protect personal computers from other computers inside the same network zone. The student computers coming to campus arrived from locations world wide. In their previous home, these computers were attached via dial-up, dsl, cable modem or even corporate LANs with varying levels of management and control in place. By their nature, perimeter defenses do not protect computers inside the perimeter from one another.

End User Awareness

The students are responsible for their own computers. Many of them were unaware of the maintenance requirements necessary to secure their computer. As already stated, these computer come from all over the world. Each user had a different level of awareness as to the procedures and reasons for proper computer maintenance.

Personal Computer Vulnerabilities

Lack of awareness means that computers in RHN lack service packs, hot-fixes or other patches recommended by the vendor. Many industry experts believe that for a vendor to require a service pack or hot-fix to be applied is unacceptable for of an end user.[4] However, the current state of the industry requires every computer owner to be aware of, and maintain security patches. Unfortunately, even the automated methods of patch management currently available to Windows users require at least some user interaction to complete.

Lack of Other Mitigating Technologies
Other countermeasures like personal firewalls or anti-virus software have not been installed, or are improperly configured. If an end user is unaware of the necessity of something as basic as patch maintenance, then the need for defense-in-depth in the form of personal firewalls or anti-virus, is an unrealistic expectation.

Risk to the Organization

The Risk to CIT and ultimately TU is the loss of network functionality due to an overload of network devices by a large number of worm infected computers. The severity of this risk is dependent on 3 major factors:

Percentage of Vulnerable Computers:
This factor helps establish the probability of a computer being infected in a given security zone. For a given zone with a 50% rate of vulnerability a random scan to find a host to infect has a 50% chance of finding a host to exploit. This makes the initial probability calculation for a particular zone simple.

Number of vulnerable computers in the security zone:
This factor affects the severity of the exploit. In a zone with 100% vulnerable computers the exploit of that vulnerability is basically assured. If that zone only contains a single computer the damage to the network as a whole from such an exploit is trivial. However, if within the zone there are 1000 computers, that poses a severe risk to the security of that zone.

Propagation Methodology of a given exploit:
The final major factor that has to be considered is the actual algorithm the exploit uses to propagate. Different algorithms have different effects on the health of RHN as a whole. The RPC-DCOM incident highlights the difference the propagation algorithm can make in the overall impact of the exploit. In August 2003 two different exploits of the RPC-DCOM

[4] A very complete discussion of this started with an opinion piece by L. Willis can be found at http://www.csoonline.com/opinion/comments/548.html

vulnerability, W32.Blaster[5] and W32.Welchia[6] both attacked the TU campus. However, they each had very different effects.

W32.Blaster

> … uses a 'choose random IP, then scan sequentially from there' algorithm"[7]

in an attempt to find hosts vulnerable to the exploit payload. Given the size of the whole IP address space, it is highly improbable one computer inside RHN will be able to infect another computer also inside that security zone. Therefore determining the probability of exploit is primarily determined by the percentage of computers in that zone that are vulnerable.

The W32.Welchia worm by contrast,

> discovers the IP address of the host, then uses the Class-B boundary of that IP address and commences an ICMP scan from A.B.0.0 through A.B.255.255. If a host responds to the ICMP echo request, the worm commences an RPC DCOM attack against that host.[8]

Therefore a single exploit inside RHN almost ensures that all vulnerable computers in RHN will become infected. The effectiveness of exploiting computers within the same security zone is a key difference between the W32.Blaster and W32.Welchia algorithms.

Another key difference between the W32.Welchia and the W32.Blaster algorithms is the protocol(s) used. W32.Welchia did not use the same protocol to attempt to find a host as the protocol used to actually exploit the host. This is a key element because many computers needed to have

---

[5] W32.Blaster is the name given to the worm by Symantec as detailed in their Security Response article by Knowles, Perriot, and Szor. This name varies depending on the source of the security information. This paper used the Symantec name for all exploits for consistency sake.

[6] W32.Welchia is the name given to the worm by Symantec as detailed in their Security Response article by Knowles, and Perriot. This name varies depending on the source of the security information.

[7] Vogt.

[8] Bransfield, p.26.

the RPC ports available for proper functionality but could have had ICMP scanning blocked to them from the other network zones[9].

In a practical sense the TU network did not see a damaging volume of network traffic from W32.Blaster. Traffic was elevated beyond normal levels, but traffic shaping at the perimeter effectively limited the impact. However, the massive amount of internal traffic generated by W32.Wechia traversing the internal firewalls was far too much to deal with. This was a practical example of how the propagation algorithm had an impact on the severity of the exploit.

In order to reduce both the probability and severity of the risk of a total network outage, the number of vulnerable computers must be reduced or network access to those computers must be limited. Throughout the industry the best practice of automated patch management in addition to installation of a host-based firewall has become the response to both of these issues. The most obvious validation of these measures can be found in Microsoft's massive consumer oriented "3-Step Get Secure/Stay Secure" campaign.[10] We took great confidence in our conclusion that the primary focus should be addressing these two major mitigating factors.

Lessons Learned from RPC-DCOM

One of the major outcomes of the RPC-DCOM exploit was a tool created by CIT known as TU-RPC. After attempting to patch or remediate infected computers by sending staff room to room CIT, management determined that such an individual effort was not cost or time effective. It was determined at that time that an "all-in-one" highly automated tool should be created to be distributed to the student population via CD. This tool was designed to bring a computer to a currently supported service pack, install MS03-026[11] hot-fix, turn on the Windows Automatic Update feature, and if available, enable the Internet Connection Firewall. Because, the TU-RPC tool was written over the course of 48 hours by a team of 4 people working almost non-stop much of the code logic was poorly conceived, completely undocumented, and ultimately not maintainable. It took over an hour just to update the code to find and replace all of the references to

[9] Mullins. offers a solid explanation of the benefits and risks associated with blocking ICMP traffic at http://techrepublic.com.com/5100-6264-5087087.html

[10] Microsoft Corporation. is currently engaged in a personal computer security initiative called "Get Secure/Stay Secure" Their 3 steps to security are Automatic Updates, Personal Firewall, and Anti-Virus. Due to difficulties listed later in the document we dropped the Anti-Virus as a requirement in the final product.

[11] Microsoft Corporation. this is the original hot-fix associated with the RPC-DCOM exploits.

the MS03-026 when the replacement MS03-039[12] hot-fix became available. However, TU-RPC did exactly what it was designed to do.

The experience of attempting to remediate student computers by hand as well as developing TU-RPC brought on the following lessons:

Anti-Virus complexity
The majority of student workstations come to the TU with anti-virus software installed. Unfortunately this is typically a default installation that has not been properly configured or licensed. Additionally, there are dozens of hardware vendors represented each with their own preferences regarding the choice and installation of anti-virus software. Despite the TU campus license for anti-virus, there has not been a feasible means to automate the removal of the existing anti-virus software to ensure a proper installation of the TU licensed software.

Service Packs
Every hot-fix produced by Microsoft has a minimum service pack requirement. It became clear in the early stages of the development of TU-RPC that we would have to address the issue of brining service packs up to date. Unfortunately the size of the current service pack for Windows XP and Windows 2000 multiplied the size of the package by two orders of magnitude. Depending on the circumstances this added a considerable amount of time to the overall installation process.

Re-applying existing hot-fixes
TU-RPC automatically forced the install of the MS03-026 patch initially and then MS03-039 instead when it became available. The code automatically forced the install without checking for it's existence. This was necessary because some worm variants were designed to make the computer appear to be properly patched when they were not. However, in a number of computers we found that re-installing the patch over itself actually caused issues with the operating system, especially with the automatic update service.

Exploit Specific Detection and Removal Tools
The TU-RPC tool used as many as four different exploit specific detection and removal tools. Unfortunately, they were all slow and often unnecessary for computers that were merely being patched as opposed to computers that had already been exploited. Multi-Purpose detection tools available at that time often reported false negatives. Therefore TU-RPC had to force students to wait through all of the exploit specific scanners to complete successfully.

---

[12] Microsoft Corporation. this is the updated hot-fix associated with preventing the RPC-DCOM exploits.

Additional Considerations

The major concern in designing a pre-emptive method to mitigate this risk was that the residence halls are the students' home. While protecting our network stability is important, we would be in error if that solution were too intrusive or time consuming. This philosophy reduced the number of purely network based solutions we were able to employ.

One thing that makes the solution more complex is that students do not live in the Residence Hall all year long. The Residence Hall is their home for much of the year, but they also leave for weeks at a time on a regular basis. Therefore, any solution has to assume that their computers should work without additional intervention when completely isolated from our network. This drastically reduces the number of workable solutions.

Another factor on the TU campus is the lack of a standard for determining the party responsible for a particular computer. We have data that can tie an exploited workstation to a particular wall-plate in a room. However that doesn't which student staying in that room is specifically responsible for the computer. On the wired network the wall-plate information narrows our search to one of two people. However, we are totally unable to identify computer owners in the residence halls that use wireless connectivity. This consideration is being addressed as part of a larger project, and it was included here in support of that initiative.

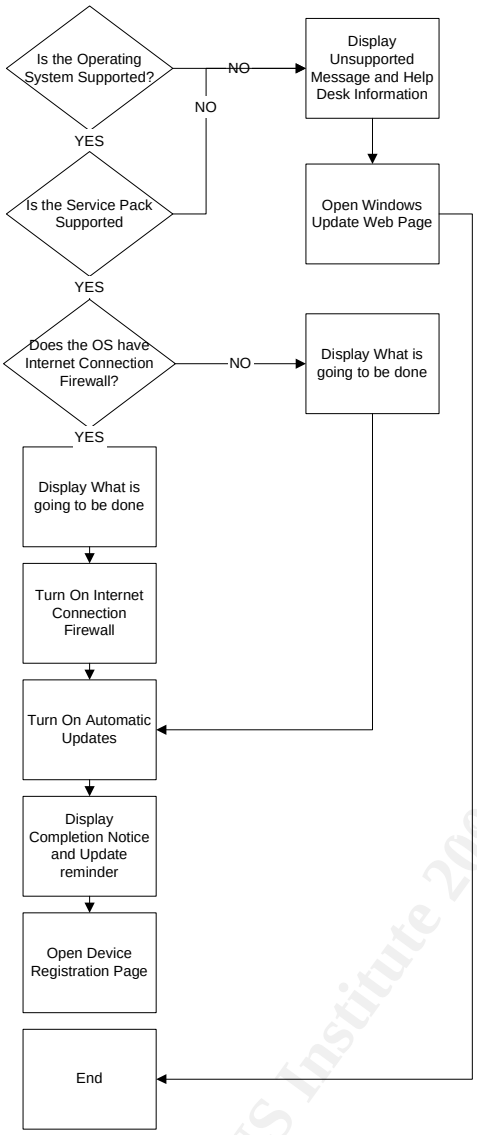
A final insight that changed the way we looked at the issue was Windows Automatic Updates. CSG designed TU-RPC to turn on automatic updates. It set the Automatic Update client to download hot-fixes and prompt the user to install them. However, CSG found that despite the  icon showing in the system tray or the pop-up on the screen the student would not choose to finish the process. It was clear that the students didn't understand the necessity or importance of the update process.

SECURE-IT

In March of 2004 a sudden assault of the W32.Welchia.B[13] worm that forced us to add functionality to TU-RPC. At that time CSG added additional hot-fixes, and changed the issue specific scanners. However, that proved to be an incredibly complex task due to the poor coding standards used in the initial development. After that incident we determined we had to create a lightweight pre-emptive tool to distribute to students whose computers were attached to RNET. The first

[13] W32.Welchia.B is the name given to the worm by Symantec as detailed in their Security Response article by Liu. This name varies depending on the source of the security information.

major decision in that process was to start over from scratch with the code. While some of the functions from the original were copied the majority of TU-RPC was discarded.



The new combination of vbscript was designed to do the following:

Check for a supported operating system version and service pack level.

If both are supported then
Check if Internet Connection Firewall is available
If so turn ICF on
Turn on Automatic Updates
Display Completion Message reminding the user to complete updates when they are prompted
Display the Device Registration Form

If unsupported then
Display the Unsupported Message with HelpDesk information
Direct the user to the Windows Update page.

For this utility we chose to limit support to

- Windows XP Service Pack 1
- Windows 2000 Service Pack 4
- Windows Server 2003 no Service Pack.

The major consideration in limiting the supported Operating System/Service Pack combination was the size of the overall package. To keep the package small and make the install fast we couldn't include the service packs needed to bring anyone running Windows 2000 or Windows XP up to date. Additionally we considered any computer missing the current service pack to be enough of a risk that a full Windows Update was necessary.

One of the oddities in the SECURE-IT implementation is that it is actually two scripts. The logic and most of the work is done by a vbscript. However, in order to enable the firewall on all possible interfaces we had to find code to enumerate

them all. We found code that would do that, however it was in jscript[14] and not vbscript. We used the code from Microsoft with only minor changes to enable the firewall instead of simply enumerating the connections.

When the code was finished we tested it on Windows 2000, Windows XP, Windows Server 2003 with or without the proper service packs using VMWare based virtual machines. The code was then distributed to the desktop support group for further verification. After the code was properly validated we packaged it as a self extracting and executing package using Power Archiver.

At that point the email listed in Appendix 1, was targeted specifically at Residence Hall Students and was sent on April 16, 2004. The timing of this release is important since Microsoft had released the MS04-011 security hot-fix on April 13, 2004 and CIT was concerned about the possibility of an exploit to this vulnerability.

One of the key aspects of the email was showing students exactly what Automatic Updates looks like. Previous communication with the student population had informed students they should update their computers, but did not go into detail about how to accomplish this beyond "run windows update". In this communication we attempted to associate a commonly seen element on their computer, the update icon  , to a real security concern. Additionally, we attempted to communicate to the students that they would see the update globe periodically and should follow through with that operation. If they did not see the icon they should run our tool to enable it.

As the email was being sent, the follow-up documentation in Appendix 2 was created for the help desk. This proved to be a key component in our overall strategy. With TU-RPC there was not sufficient time to document what it did or how the Help-Desk staff could troubleshoot it properly. It was released with only word of mouth information to help users that might call. This created a number of unnecessary trouble ticket escalations and frustrations for the end-users. The help desk information sheet proved to be a very useful tool.

Downloading and running SECURE-IT took most students less than 2 minutes from the first click to the last. For those that may have already waited through the entire hour and a half process for TU-RPC this was a huge improvement.

---

[14] The msdn library offered code to enumerate all the connections. http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ics/ics/retrieving_the_properties_of_a_connection_jscript_.asp . While that is the basis for the code in Appendix 2, it is not the whole of that code. Therefore we reproduce it for completeness.

Outcome

The outcome was quite positive. We had approximately 1300 downloads of SECURE-IT within the next week. On April 27, 2004 a free scanner for the MS04-011[15] vulnerability was produced. A scan of our environment showed that 17% of the computers were vulnerable to the exploit. Previous experience with MS03-043[16] and MS04-007[17] had shown 23% of the computers to be vulnerable after a similar period of elapsed time from vendor release of the hot-fix. SECURE-IT had generated a 26% reduction in poorly managed workstations.

The real proof of the effectiveness of the SECURE-IT initiative was the very minor impact the W32.SASSER[18] worm had on RHN. In previous worm outbreaks CIT had to mobilize a large number of staff over an extended period of time to protect the network. With this outbreak CIT only identified 30 exploited computers in RNET compared to over 300 with W32.Welchia.B and over 2000 W32.Blaster incidents. Some of this reduction was due to the propagation algorithm that W32.SASSER uses[19], however RHN was at the edge of capacity on the RHN firewall with 30 exploited computers. Had RHN had 26% more exploited computers attached to it we would have had actual loss of network service in some areas until we could reduce the damage to a manageable level. With the small number of infections, CNG was able to effectively disable switch ports for these computers and return to essentially normal operations within 4 hours of the initial outbreak.

During the RPC-DCOM exploit in the fall, the worm and the consequences of it were a topic of conversation on the entire campus for weeks. The W32.SASSER outbreak didn't even merit discussion of CIT staff two days later. The students were largely unaware that another major worm outbreak had even occurred. In this case the general lack of student awareness and impact was the best possible result we could have hoped for.

---

[15] Microsoft Corporation. This hot-fix removes the vulnerability that was later exploited by the W32.Sasser worm.

[16] Microsoft Corporation. This hot-fix removes the vulnerability that was known generally as the Messenger vulnerability.

[17] Microsoft Corporation. This vulnerability was more widely known as the ASN.1 vulnerability. It has not been exploited to date.

[18] W32.Welchia is the name given to the worm by Symantec as detailed in their Security Response article by Nakayama and Takayoshi. This name varies depending on the source of the security information.

[19] McAfee Security. Details the propagation algorithm of the exploit at http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=125007#method

The only negative side effect associated with SECURE-IT was that some Peer-to-Peer file sharing applications no longer functioned. This generated a few help desk calls. This is a common problem with the Windows XP Internet Connection Firewall. The help desk is well versed in walking users through the remediation process for this, so it is a very minor issue. Additionally, with Windows XP service pack 2 Microsoft is promising a more robust firewall implementation[20] so CSG expects this issue to be resolved with its release.

The main positive side effect of the tool is an increase in computers in our device registration database. This is a separate project and ultimately registration will be a requirement for network usage. The additional data for identifying who owns a computer saves a significant amount of time when an incident does occur.

Conclusion

SECURE-IT is a low impact tool for helping the typical end user enable basic security functions. It still requires the student to finish the update process, but the communication associated with SECURE-IT appears to do an adequate job of educating them about their responsibility. Additionally, SECURE-IT is not as effective on Windows 2000 computers as it is on Windows XP. CIT is completely relying on the student to follow through with the patch process on Windows 2000. While Windows XP computers have the additional mitigating factor of the Internet Connection Firewall.

This was a voluntary initiative from a compliance perspective. Even after running our tool CIT is at the mercy of the students choosing to finish the update process. The most dramatic example of this is the Greek Houses. While RNET overall experienced a decline in vulnerable computers, the fraternity and sorority subnets within RNET showed an identical vulnerability percentage even after the release of SECURE-IT. CSG clearly needs to implement a different means of awareness education for that subset of RNET subscribers.

CSG did not see SECURE-IT as the ultimate solution to the issue of unmanaged student workstations in our environment. Our primary motivation was to provide a simple tool that would actually be used by the students. The effectiveness of the tool was obvious and measurable from a purely technical perspective.

Despite the clear success of the SECURE-IT intiative, risk to the stability of RHN still exits. The MS04-011 hot-fix was available for three weeks yet RHN still

---

[20] Microsoft Corporation. In support of their “Get Secure/Stay Secure” initiative Microsoft has drastically updated the Internet Connection firewall as well as increasing the functionality within the automatic update client. These changes are detailed http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2chngs.mspx

demonstrated a that 17% of the computers in the security zone were vulnerable. A worm published closer to the release date of the hot-fix will have a much greater impact on the stability of RHN. As many industry experts predict the likelihood of such an exploit increases constantly[21]. Additionally, a more aggressive propagation algorithm could still have a major impact on network stability. CIT has a number of different initiatives in progress to add additional checks and controls to the environment. SECURE-IT is just one of the many tools being used to provide defense-in-depth for our environment.

[21] Wong. Arthur Wong Vice President of Symantec Security Corporation warned Congress that "The time from vulnerability discovery to exploit is rapidly shrinking." in official testimony. This is a key consideration in our ongoing efforts.

Appendix 1: Informational Message to Students

SECURITY ADVISORY: Microsoft Windows users READ!

On Wednesday of this week, Microsoft released four critical security updates that address vulnerabilities in the Microsoft Windows operating system. **Please apply these updates to your computer immediately!**

Viruses that use these vulnerabilities already exist, and it is only a matter of time before they are released. **If you do not take action now your computer could become infected with viruses!**

If your computer gets infected, your network access may be disabled! **Follow the steps below to reduce the risk of losing your computer access during these important final weeks of the semester!**

To apply the updates, follow these steps:

1) Look for the Automatic Updates icon  next to the clock on your screen.

2) If you have this icon, click it and follow the directions. If you do not have it, go to step

3) If you do not see the icon, please download the file from the following link to setup automatic updates.

<<Local URL to files>>

Within an hour after downloading the file, the icon will appear next to the clock on your screen. Click it and follow the directions. If you are running Windows XP, this process will also enable your personal firewall for extra protection.

If you have questions about this alert or need assistance with the Windows Update feature, please contact the CIT Help Desk at 573-882-5000.

Appendix 2: Assistance for Help Desk Staff

The Secure-It script was designed to deal with 3 major issues regarding Windows desktop security; personal fire wall, automatic operating system updates, and device registration. End users get varying results depending on their operating system and patch level based on the following table

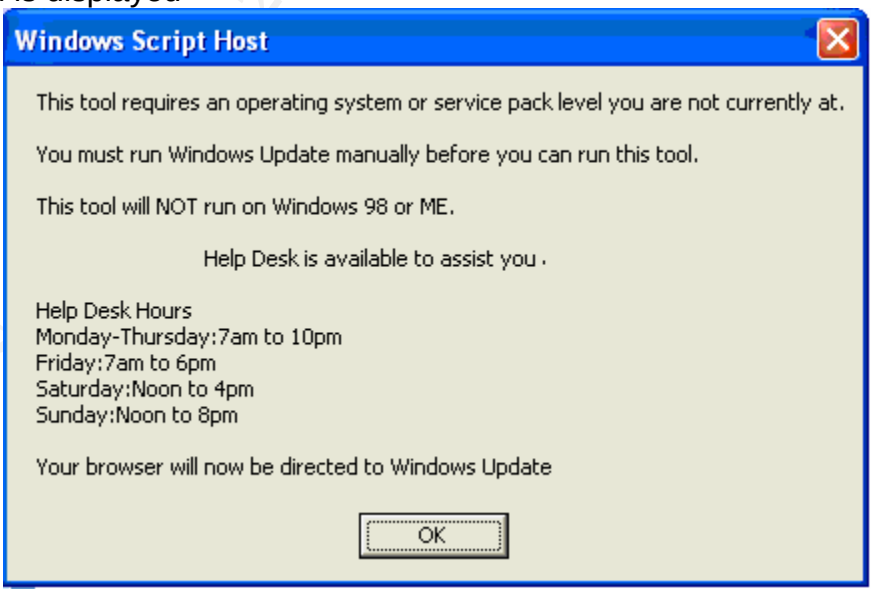
Operating System	Service Pack	Auto-Update	FireWall	Registry	Manual Update*
Windows 9x	Any	NO	NO	NO	YES
Windows ME	Any	NO	NO	NO	YES
Windows NT4	Any	NO	NO	NO	YES
Windows 2000	1-3	NO	NO	NO	YES
Windows 2000	4+	YES	NO	YES	NO
Windows XP	0	NO	NO	NO	YES
Windows XP	1	YES	YES	YES	NO
Server 2003	Any	YES	YES	YES	NO

*The Manual Update is the script automatically opening the page to Windows Update once it recognizes the machine as an OS and SP combination it cannot work with.

When a user downloads the script
It will put a self extracting and executing archive on their machine.
This archive will automatically extract to ***C:\secure-it*** and execute ***C:\secure-it.exe***
Running the script will create a minimal log file that tells what OS the script detected and what steps it attempted to run. The file is ***C:\secure-it\secure-it.log***

OS + Patch Level Not Supported *(Win 9x,ME,NT4,2K SP1-3, or XPSP1)*

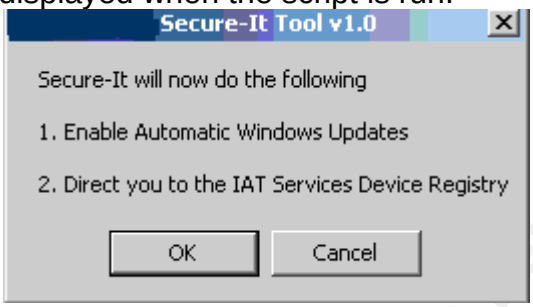
On an Operating System that the script does not support the following screen is displayed



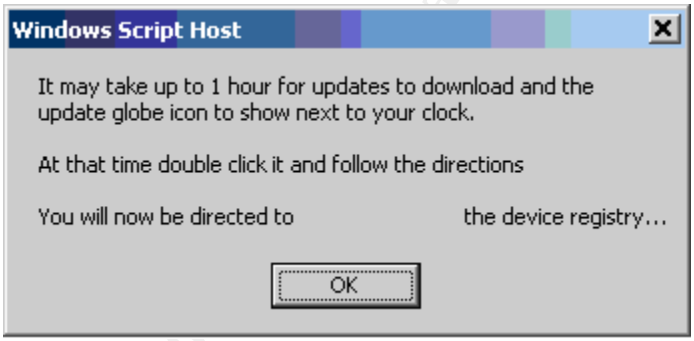
When the user clicks OK a browser windows opens to http://windowsupdate.microsoft.com.

Windows 2000SP4

Since Windows 2000 does not have a Personal Firewall built-in the following dialog is displayed when the script is run.



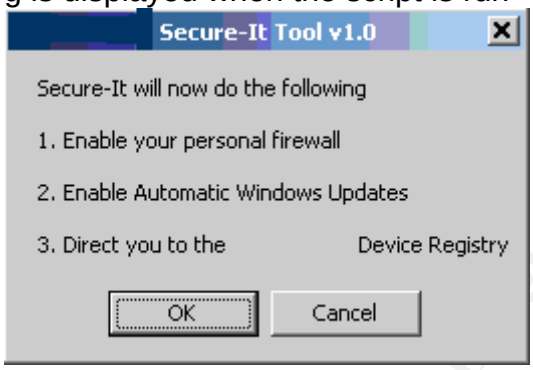
Once the script has finished setting up operating system level security measures it then displays the following



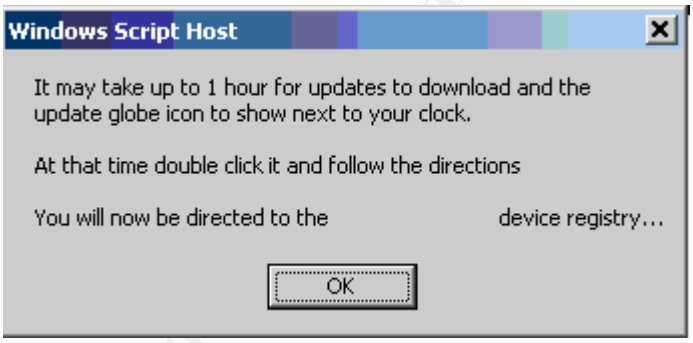
Clicking ok automatically opens
http://iatservices.missouri.edu/security/registry

Windows XP SP1, Windows Server 2003

The following dialog is displayed when the script is run



Once the script has finished setting up operating system level security measures it then displays the following



Clicking ok automatically opens
http://iatservices.missouri.edu/security/registry

Appendix 3: References

Bransfield, Gene. “The Welchia Worm.” GCIH Practical V.3 18. Dec. 2003. URL:http://www.giac.org/practical/GCIH/Gene_Bransfield_GCIH.pdf (3 June 2004). Page 26.

Carlson, Scott. “Record Companies Settle Lawsuits Against 4 Students”. Chronicle of Higher Education. 2 May. 2003. URL: http://chronicle.com/free/2003/05/2003050201t.htm (18 June 2004).

Judy, Brad. **< judy@colorado.edu >** “Higher ed IT environment**.” 10 June 2004. < windows-hied@lists.Stanford.EDU >** (18 June 2004).

Knowles, Douglas; Perriot, Federic. “W32.Welchia.Worm.” Symantec Security Response. 26 Feb. 2004. URL:http://securityresponse.symantec.com/avcenter/venc/data/w32.welchia.worm.html (8 June 2004).

Knowles, Douglas; Perriot, Federic; Szor, Peter. “W32.Blaster.Worm.” Symantec Security Response. 26 Feb. 2004. URL:http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.html (8 June 2004).

Liu, Yana. “W32.Welchia.B.Worm.” Symantec Security Response. 28 April 2004. URL:http://securityresponse.symantec.com/avcenter/venc/data/w32.welchia.b.worm.html (7 June 2004).

McAfee Security. “W32/Sasser.worm.a.” Virus Profile. 7 June 2004. URL:http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=125007#method (8 June 2004).

Microsoft Corporation. “Changes to Functionality in Microsoft Windows XP Service Pack 2.” Microsoft TechNet. 14 May 2004. URL:http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2chngs.mspx (7 June 2004).

Microsoft Corporation. “Microsoft Security Bulletin MS03-026.” Microsoft TechNet. 10 Sept. 2003. URL:http://www.microsoft.com/technet/security/bulletin/MS03-026.mspx (8 June 2004).

Microsoft Corporation. “Microsoft Security Bulletin MS03-039.” Microsoft TechNet. 10 Sept. 2003. URL: http://www.microsoft.com/technet/security/bulletin/MS03-039.mspx (8 June 2004).

Microsoft Corporation. “Microsoft Security Bulletin MS03-043.” Microsoft TechNet. 2 Dec. 2003. URL: http://www.microsoft.com/technet/security/bulletin/MS03-043.mspx (8 June 2004).

Microsoft Corporation. “Microsoft Security Bulletin MS04-007.” Microsoft TechNet. 9 June 2004. URL: http://www.microsoft.com/technet/security/bulletin/MS04-007.mspx (8 June 2004).

Microsoft Corporation. “Microsoft Security Bulletin MS04-011.” Microsoft TechNet. 4 May 2004. URL: http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx (8 June 2004).

Microsoft Corporation. “Protect your PC.” Microsoft Security. 17 Feb 2004. URL:http://www.microsoft.com/security/protect/ (7 June 2004).

Microsoft Corporation. “Retrieving the Properties of a Connection (JScript)”. Platform SDK: Internet Connection Sharing. April 2004. URL:http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ics/ics/retrieving_the_properties_of_a_connection_jscript_.asp (3 June 2004).

Microsoft. “What you should know about the Blaster worm.” Microsoft Security. 22 Jan. 2004. URL: http://www.microsoft.com/security/incident/blast.mspx (7 June 2004).

Mullins, Michael. “Prevent hacker probing: Block bad ICMP messages.” Tech Republic 21 Oct. 2003 URL: http://techrepublic.com.com/5100-6264-5087087.html (10 June 2004).

Nakayama, Takayoshi; Ladley, Fergal "W32.Sasser.Worm." Symantec Security Response 26 May 2004. URL:http://securityresponse.symantec.com/avcenter/venc/data/w32.sasser.worm.html (8 June 2004).

U.S. Copyright Office. "The Digital Millennium Copyright Act of 1998." Dec. 1998. URL: http://www.copyright.gov/legislation/dmca.pdf (18 June 2004)

Vogt, Tom. "Short Blaster Propagation Algorithm Analysis." Full Disclosure Forum. 12 Aug. 2003. URL: http://seclists.org/lists/fulldisclosure/2003/Aug/0560.html (3 June 2004).

Willis, L. "Patch and Pray." CSO Online. Aug. 2003. URL: http://www.csoonline.com/opinion/comments/548.html (7 June 2004).

Wong, Arthur. "Prescription for protection – Trends." Communications News. Jan. 2004. URL:http://www.findarticles.com/cf_0/m0CMN/1_41/112448801/p1/article.jhtml (8 June 2004).

Last Updated: July 27th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event