Global Information Assurance Certification Paper

Minimizing Desktop Security Threats

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4b

Option 2 - Case Study in
Information Security

Submitted by: Carlo M. Merhi
Location: Tyson's Corner
September 30, 2004

Paper Abstract:
Deploying a secured desktop in a campus wide environment and the associated security challenges.

Table of Contents

List of Figures

Introduction

A loud boom, shattering glass and M-16 firing off brought my sleep to a complete halt and jumped me out of my bed. It was around 4am and the bombing had started 3 bombs exploded into the adjacent building while the shrapnel tore through our windows and house. The bombing attacks and machine gun guerilla combat has commenced yet another day. Another restless night full of anxiety, fear and uncertainty. I was 16 years old and a soldier. My heart was racing wondering if I was going to be called to the front lines again. My mother terrified that this will be the last night she sees me alive.

The call comes. My Lieutenant in the Black Maria Tanker yelled for me to get my full gear and rush down. My jump bag ready with my M-16, a 9 millimeter handgun and my bazooka launcher with charges. I had all my survival gear and a few personal items for good luck and faith in my bag. I knew I had trained vigorously and studied as much as I can about the enemy and their tactics. I felt ready and confident that my team and I were fully prepared to take on whatever comes.

Strange excitement and anxiety levels merged into an indescribable high, knowing fully well that this could be the last day being alive.

14 years later…….
A continuous vibrating, rattling sound and a double chirp bring me out of a dead sleep. I reach over to my BlackBerry to see 14 messages from our alert server and from my manager. I start reading the first e-mail, an alert of a suspicious port activity on port ####. I continue to read the next e-mail and realize, we are under attack; a cyber attack. As I am reading my e-mail, my phone rings. I knew it. I was again getting called for duty for another war. My manager informed me that we need to assemble my team for an emergency IRT meeting immediately. This time my jump bag had a slightly different inventory. It had my laptop loaded with all needed forensic software: packet sniffers, KNOPPIX, GFILanguard. Network cables, a small hub, extra hard drive, and remediation software on CDs completed my tools. I was ready.

Abstract/Summary

There is a silent war going on in each and every networked IT environment on. It is an escalating race between the malicious code writer and the Security officer and Information Technology (IT) department. The only time the conflict comes to light is when the enemy wins a battle. Viruses, Worms, Trojan horses and other malevolent codes are constantly being written and revised by hackers in an attempt to further their own agenda. Sometimes the agenda and the codes are benign, sometimes devastating.

Although my first security experience was extreme in comparison to fighting the latest computer security threat, a cyber war is a malicious nasty war that if kept uncontrolled and contained could. I am not sure if anyone can ever stop the cyber wars but we sure can try winning as many as we can.

"Pssstt…hey, you want the new Beyonce album? I have it ripped at 192Kbps MP3 format. I will share it out, hang on. What's your username? Ah, never mind I will just use the Everyone username. That always works."
That is one of the many horrifying things that I quite often hear people say with no regard or understanding as the how dangerous it is was they just did.

In an open and unsecured environment that actually promotes open sharing of information, it becomes evident that the potential for a technology disaster is eminent if security measures are not taken. The challenge becomes having secure communications in a safe and efficient environment. Keeping this user friendly does not hinder the flow of information but merely make it secure.

By keeping an up to date security policy implemented on the desktops, IT professionals can hope to stay ahead of the latest security threats.

The Desktop Atmosphere

The Desktop Configuration (see Appendix A) at the time allowed all domain users to have local administrative rights on their machines. It was the policy. With full control of their systems, users can install anything on their systems, including software like Peer to Peer (P2P) clients that open up a number of ports. Here is just a short list:

Application	Protocol	Port #
eDonkey2000	TCP	4662
eDonkey2000	UDP	4672 (eMule)
Overnet	TCP	4662
Gnutella	TCP & UDP	6346
BitTorrent	TCP	6881
Fasttrack	TCP	1214
OpenNap	TCP	6699
Direct Connect	TCP & UDP	1412
Soulseek	TCP	2234

Associated Risks

After our security risk assessment project was completed, the report showed that at least 1600 out of the 2100 nodes on the network were wide open with full rights to shares. There were also over 100 unauthorized FTP servers and 5 DHCP servers running on the network without proper authorization, restrictions or a secured configuration. The risk assessment also reported that those systems were fully penetrated and had full lists of local usernames and passwords from each system. This ultimately led to the compromise of the PDC and the collection of the Domain SAM. All domain passwords were revealed within days by the security assessors. There were over 65 different open ports on the network. Each system had at least 4 ports opened without the users' knowledge, and their systems included Virus Definitions files (DATs) and security patches were out of date. The report was not only an eye opener, but also a shameful way of realizing that the network security was very weak at best.

Exposure to Unknown Threats

Having freshly completed the security risk assessment, we got our first real bad taste for what it's like to have an unsecured network.

Months previously, we had battled the SQL Slammer that brought all our field technicians and mangers to work on a Saturday. The network came to a complete grinding halt. One thing that we learned is that we really had to implement the type of security that would allow us to at least contain propagation of worms and such code that use open ports. Since The SQL Slammer worm uses only UDP port 1434 (SQL Monitor Port) to spread itself to a new system. To protect the network from the worm's requests this port on the firewall needed to be closed. However, we did not have a firewall in place and no active port blocking for known exploits was implemented either.

We had learned some lessons, but we were about to really learn some new more powerful lessons courtesy of two worms, Blaster and Sasser.

Confirmation of Vulnerabilities

CERT Advisory CA-2003-20 W32/Blaster worm [1]

"…The W32/Blaster worm exploits vulnerability in Microsoft's DCOM RPC interface as described in VU#568148 and CA-2003-16. Upon successful execution, the worm attempts to retrieve a copy of the file msblast.exe from the compromising host. Once this file is retrieved, the compromised system then runs it and begins scanning for other vulnerable systems to compromise in the same manner. In the course of propagation, a TCP session to port 135 is used to execute the attack. However, access to TCP ports 139 and 445 may also provide attack vectors and should be considered when applying mitigation strategies. Microsoft has published information about this vulnerability in Microsoft Security Bulletin MS03-026."

The Blaster worm started harassing networks worldwide in August of 2003, this worm cost between 320 and 500 million worldwide[2] and as many as 16 million machines were infected. Blaster capitalized upon the DCOM vulnerability of the windows code. And used a variety of denial of service (DoS) type of attacks to render the infected computer essential useless. The worm also contained two hidden strings[3]. *I just want to say LOVE YOU SAN!!* and *billy gates why do you make this possible ? Stop making money and fix your software!!* The hidden message a not too subtle affront at Bill Gates former CEO of Microsoft.

Numerous networks were crippled. Un-patched networks were ravaged and regrettably mine was as well. The morning of August 11, 2003 Blaster hit my network. The immediate step to solving the problem was to determine how bad the network was affected. The next was to find a solution, and finally to devise a course of action. Over 90% of our computer's network had been infected. The

[1] http://www.cert.org/advisories/CA-2003-20.html
[2] http://www.acmqueue.com/modules.php?name=Content&pa=showpage&pid=159&page=5
[3] http://encyclopedia.thefreedictionary.com/Blaster%20worm

Help Desk phones were flooded and the blanket orders were disseminated to the clients "remove the network cable from the wall". The most pressing computers - the servers had the patches applied and were operational and stable within the first half of the day. The task of fixing over 2500 computers without the help of remote tools was daunting. Everyone within the IT branch was assembled to address the problem.

Impact of SANS Training on the Situation

"KNOW THY SYSTEM" is the rule. Knowing that the systems on the network have not been aggressively and proactively patched and that SMS was not able to reach all the systems for updating forced us to manually scan system by system and remediate each workstation individually. The ability to scan the systems, collect data, and understand the reports more efficiently was significant. The need was to stabilize the network and regain full control and functionality. Understanding the traffic being generated and having learned best practices, we were able to determine where to close out and contain different networks while still maintaining as much network functionality as possible for deploying patches and remotely remediate systems.

Minimizing Security Threats

CAN-2003-0533 W32/Sasser[4]

"…This worm attempts to exploit a buffer overflow vulnerability in the Windows Local Security Authority Service Server (LSASS). The vulnerability allows a remote attacker to execute arbitrary code with SYSTEM privileges. More information on this vulnerability is available in Vulnerability Note VU#753212 and Microsoft Security Bulletin MS04-011.

The worm has been reported to propagate by scanning random IP addresses on port 445/tcp to identify vulnerable systems. When a vulnerable system is found, the worm will exploit the LSASS vulnerability, create a remote shell on port 9996/tcp, and start an FTP server on port 5554/tcp. The victim system will then connect back to the attacking system on port 5554/tcp to retrieve a copy of the worm. Systems infected by this worm may notice significant performance degradation."

The Sasser worm was another worm that contaminated a multitude of networks; it targeted Windows 2000 and XP machines. The worm circulated by open ports, this obviously compounded the effectiveness of the worm, as user intervention was not needed to propagate the expansion[5]. The worm variants from Sasser A through F compounded the pain that networks and IT professionals faced because each needed focus.

[4] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0533
[5] http://encyclopedia.thefreedictionary.com/Sasser%20worm

The outbreak was preventable by installing the patches available for download from Microsoft. The worm devastated computers around the world by exploiting a vulnerability that Microsoft has identified and reported to its customer base. This was a wake-up call for IT Professionals. In the past, the threat of an outbreak in the documentation of the patches, but as the parable of the boy who cried wolf, no one paid enough attention with a heightened sense of urgency.

When the Sasser worm infiltrated my government institution the beginning of May 2, 2004; the security team was already testing the patches on Servers for eventually remote deployment to workstations. Our network was not nearly as impaired as with the Blaster virus and a full-scale response was not warranted. Within a day all servers had been successfully patched and only about 100 workstations were infected. Patches were distributed remotely and by the end of the day only 6 machines remained contaminated. Sporadic infestations appeared throughout the week, mostly laptops and squatters, these were quickly resolved.

Lessons learned from Blaster made the staff pro-active. Intra-team communication and consolidation of forces addressing the impending crisis helped maximize resources. Anti-Virus signatures were current. Patch testing was under way in a private network and plans for remote deployment had been drafted and were waiting the completion of the testing. The anti-virus software cleaned infected machines thus eliminating any intervention in a majority of cases. Finally no machines had to be removed from the network, which made location of infected systems significantly easier to track down. The minimal infestations did not negatively impact our cliental; network resources were consistently available. All these factors severely impeded the spread and impact of the worm and speeded the remediation of infected machines. Sasser's various strains were addressed via login scripts and the Sasser threat was all but eliminated by weeks end.

Updating Existing Practices

What do we have to combat this unrelenting assault upon our network?

Considerable assets that tend to tip the balance of power in a network's favor the majority of the time. The first being current anti-virus software designed to identify suspicious code and remove it. Absence of anti-virus software is not an option in today's wired world; no anti-viruses software equals a network. Closely following the dearth of anti-virus software is dated DAT files. Having old software definitions only protects against old viruses, it's essential these definitions be as current as possible. An educated staff can be invaluable. By knowing a current outbreak provides no threat, resources are then not wasted. Addressing a threat of a compromised necessitates an acute understanding of what and how the network has been affected. Having this knowledge significantly speeds the

patching process, making the network stable and functional again. When a network is down the company bleeds money, keeping a network productive and healthy should be the goal of any IT department. By having established procedures when an outbreak does occur, and it will occur, it's just a matter of time. Every network has been compromised, Microsoft[6], Cisco[7] even the United States government[8] have been compromised. A solid contingency plan when things go awry can save countless time and money.

Barricades have been established to thwart the battering and probing of nefarious codes. Firewalls should always be the first line of defense in any network. Firewalls as their name implies are designed to provide a barricade between the outside world and the integrity of your network. Firewalls can be software or hardware or a combination of both. The job of the firewall is to simply filter unwanted traffic; they can do this in a couple of ways packet filtering, proxy service, or packet inspection. Packet filtering acts comparable to an access-list on a router. If there is a rule forbidding entry to the network the packets is blocked. Proxy service acts as an intermediary and a DMZ for traffic existing and entering the network. Packet inspection acts similar to the heuristics of anti-virus software examining the packet with data from a database with trusted information. My Government institution currently only uses the packet filtering functionality of the firewall.

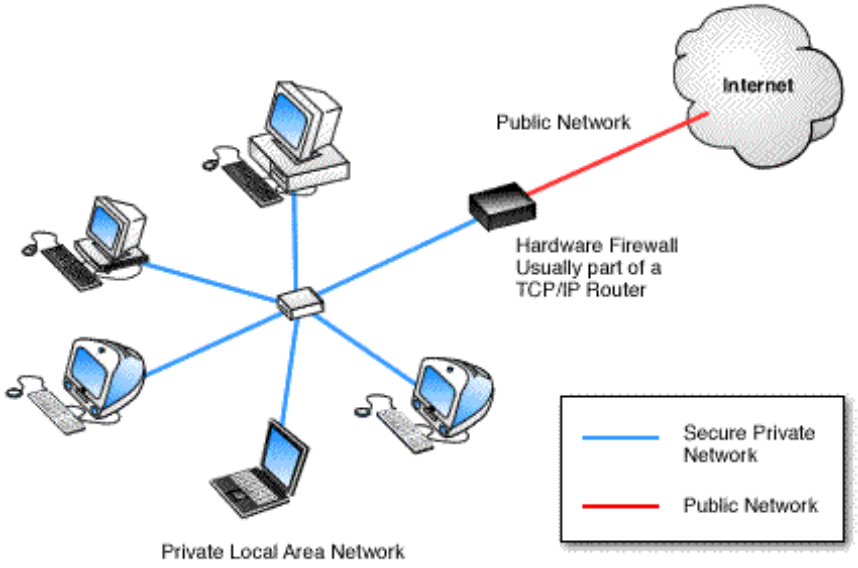

Figure 1 - Hardware Firewall

[6] http://cws.internet.com/article/1204-.htm
[7] http://www.tla.ch/TLA/NEWS/2004sec/20040518CiscoHacked.htm
[8] http://software.silicon.com/security/0,39024655,11029633,00.htm

[9]

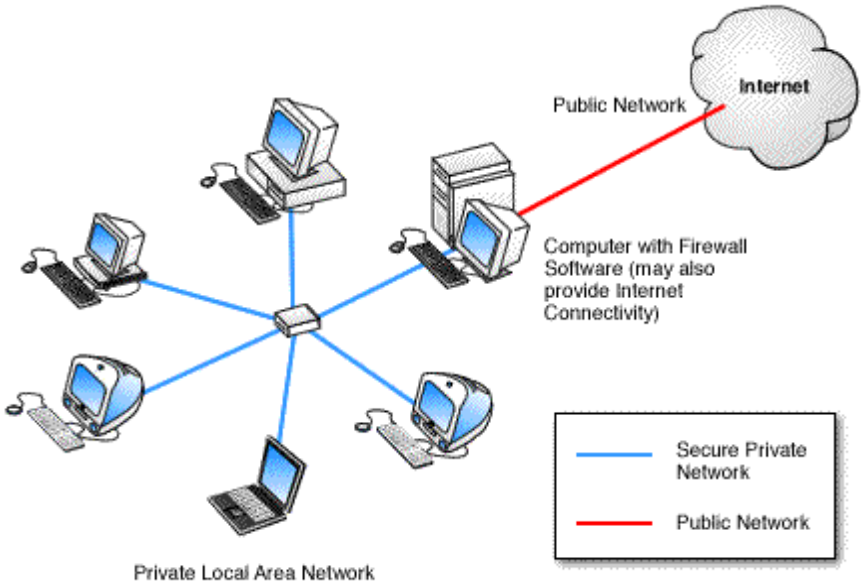

Figure 2 - Software Firewall

[10]

Service packs and patching are the next line of defense. Service packs and patches are software that updates a security breach(s) in the Operating system or particular application. Service packs are comprehensive, well tested fixes they address a multitude of recognized flaws in the software. Patching has its pros and cons.

Every network is inherently different. Changing the files of an operating system or program may affect some service or aspect that a program may require can unwittingly adversely affect the business impact of the user base. Testing is essential especially regarding patches or hot fixes. In a perfect world, testing is done in a private network that emulates the production network. Any potential problems can be resolved without disturbing the production network. Another rule to follow is if it isn't broke don't fix it; understanding what a patch does, empowers the IT professional to make the decision to apply or ignore the patch. If a patch addresses a problem with port 23 but the router has an active access-list denying telnet traffic, applying the patch would serve no purpose. A rolling policy is another way of minimizing potential damage to the network. After testing is complete, have a targeted group within the production environment to apply the patches and no problems arise distribute globally. Nothing is failsafe but this process tends to minimize surprises, and nobody in an IT department likes surprises. Due to the propensity of patches and updates, an attention to

[9] http://support.pcnet.ca/firewalls.htm
[10] http://support.pcnet.ca/firewalls.htm

detail is needed. DAT files update weekly and in times of an outbreak virus definitions and patches can be updated hourly.

Current anti-virus software, patches and firewalls are mighty contributors to limiting infection, however a network is never completely secure unless the network cable is unplugged and the system is turned off. This of course is unrealistic; the goal should be for the network to be as secure as possible, yet consistently available for clients. The network's availability, stability and health should be of supreme importance and every effort should be made for it to be available for clients whenever necessary. The business impact of a downed network should be the driving consideration in how much money is spent on the hardware, software, and man power devoted to its integrity.

Implementing Proposed Solutions

To solve: (ideal)

Local machines:
- Up to date virus software, with current virus definitions
- Current security patches for software, including the O/S

Network side:
- An updated firewall
  - Keeping current settings based on known outbreaks and security warnings
  - Monitoring traffic
- Monitoring software on the network
- Monitoring security policy compliance

IT Desktop Support Staff:
- Educated with information of latest threats
  - Emails sent to group about latest outbreaks
  - File depository available to the staff that is threat specific
    - Information
    - Links and shortcuts to online sources
    - Available removal tools
- Followed security procedures
  - Clear
  - Updated
  - Followed
- Tiers of IT Support
  - Phone support for trouble calls
  - Desktop support to handle issues
  - Ability to escalate for specific or major problems that may need to be handled separately

Customers:
- Keeping their machines on to update at nighttime
- Rebooting when necessary
- Insuring that security updates are user friendly

Additional Needs:
- Creation of emergency scripts
- Connecting systems to the network
- Adding new systems to the domain
- Up to date virus software, with current virus definitions.

Local Machines:

We have deployed and implemented McAfee VirusScan 7.1 as well as ePO agents to all workstation via SMS as main deployment but used GPO and login script as backup to insure successful delivering. Run daily reports and setup alerts for systems that do not have AV software and/or DATs are out of date. Configure ePO (see Appendix E) agent to communicate with the AV server for new configurations or DAT updates every hour.

Create a QCHAIN installer script (see Appendix C) that has all approved patches that deploys on any system that logs on to the domain deployed via either GPO, SMS or login script. Use all methods for insurance.

After evaluating and testing SUS in our environment, we felt that it would benefit us greatly if we were to implement SUS because it allowed us more control over what patches are being used on the systems. We have a very tedious and detailed patch testing process that insures that patches' successful deployment and compatibility on our workstations and network. With SUS, it allowed us to push only tested and approved patches minimizing calls of error messages and broken software due to a patch. It is very important that patches be thoroughly tested and a patch testing and approving procedure be created to insurance quality and delivery. Monitor systems to insure all patches have been installed successfully and investigate failed ones. Subscribe to Microsoft Security Alerts (see Suggested links) to stay up to date and proactive in your patch testing, Make sure to access first if the patch even applies to your environment or not. Do not deploy a patch unless it is needed for your environment.

Maintain an up to date image for standard workstations with all security patches and latest DATs so that when a new system is built and introduced to the network and domain, it can be already patched and ready without causing or creating a vulnerability on the network before whatever method of deployment reaches the system first. With the introduction of Windows XP SP2, IT has gained a little more control over open ports from a desktop perspective because of the built-in firewall within Windows XP SP2. Using carefully selected configurations according to your network, it is quite easy and very efficient to deploy desktop firewall settings blocking certain know exploited ports prevent as well as blocking known applications from launching, rendering a system vulnerable.

Network Side:

It is imperative that you revisit your ACLs often to make sure that all current vulnerabilities are being addressed in the rules.

Subscribe to US Cert alerts[11] or at least regularly visit their site to stay up to date on the latest threat and scan the network for them as well as test your firewall against them.

If possible install real-time network monitoring devices and IDSs to monitor network for known malicious activity or just suspicious activities.

Monitor application use and block access to know exploit software. Block P2P traffic as most work environments do not use such technology or at least clients that are malware that use P2P.

IT Desktop Support Staff:

Keep your Help Desk staff as well all IT groups informed of the latest outbreaks and threats. Be specific in the information that you disseminate. Inundating your audience with e-mails loaded with too much technical info will probably lead to these e-mails being ignored. Inform the groups of what they can do to prevent compromise as well as provide resource information and tools for Virus or Worm removal tools

Make available all security policies and procedures and keep them up to date. They should be clear and easy to follow as well as strongly enforced.

As recommended in "Hackers Beware" [12]book:
"Some ways to close up the biggest holes that make your company vulnerable to attacks against confidentiality are to examine your permissions setup carefully and to educate your employees on good security principles. Making sure that only the people who actually need access have access, and that your employees are aware of and controlling possible weaknesses will go along way toward keeping your company's confidential information just that, confidential"

Customers:

Continuous customer communication and education is a must. Via e-mail or pop-up messages, letting customers know what is going on or what to expect is very important for a successful rollout of any kind. By communicating to the customer

[11] http://www.us-cert.gov/
[12] Cole, Eric. Hackers Beware. New Riders Publishing. 1st edition (August 13, 2001)

base to keep their computers on overnight has significantly increase the success rate of patch deployment.

Keeping workstations' BIOS up to date to support technology like Wake On LAN and Auto Power On ,that enable a system to be booted even if it is turned, has also been instrumental in reaching systems that had been shutdown and needed to be access to have the latest emergency DAT or security update installed. Also, by scheduling non-emergency updates to be installed but delay the reboot process till after business hours has lessened customer frustration and down time.

Additional Needs:

Having the knowledge and capability to create customized scripts as needed has proved to be crucial in our environment. Multiple deployment methods should always part of the plan. In certain cases, SMS and other deployment methods fail to reach systems due to corrupted or incomplete installation of the agent software that delivers that patch. When this occurs, a custom script that delivers that patch via login script or desktop visits become your only method of getting those systems remediated or patched. Different levels of permissions and individual firewalls installed on smaller subnetworks required having different layers of updating. Without such methods, there will be systems on the network that are open to vulnerabilities causing a security hole on the network because standard automated delivery methods failed without a backup plan.

Having a method that insures networked systems are patched and up to date is also imperative. Systems come and leave the network hundreds of times in a day. With contractor machines and vendors having access to internet resources through our network introduces the risk of having unpatched systems on the network. By implementing active real time scanning of systems for patch compliance and auto- blocking non-compliant systems minimizes that risk significantly. Using a GPO that checks every system at login and pushes appropriate missing patches is also another method of patch level assurance.

Insuring that ALL systems on the network whether a contractor, vendor or user machines have the latest patches is as important as making sure that up to date Anti-Virus software with the latest DAT and latest Scan Engine are installed and running properly on all systems on the network.

Conclusion

Lessons learned in a real environment have proven useful in moving forward. Our network being part of a larger domain requires the help of different teams. The desktop seemed to be the overlooked area in which most of the security vulnerabilities were being exploited. An open machine became the gateway into the network. Multiple sets of eyes now view the systems rather than a single point of failure at the server level.

Deploying a secured desktop throughout a large environment is a complicated task to accomplish. It is a job that is never finished, and cannot be done perfectly. By using the resources available from software to mailing lists, and by constantly learning and researching the undertaking becomes a promising outlook on minimizing a shutdown of an entire network from a security threat. From loss of data to downtime, a network of computers cannot afford just one answer to the problem. Utilizing the different groups of professionals that provide the layers of protection can be the best solution.

Communication with the IT staff, updating the procedures, and keeping the systems current with scripts and patches, we can hope to stay one step ahead of the threats looming just over the horizon.

References

ACM. Queue."Blaster Revisited - A second look at the cost of Blaster sheds new light on today's blended threats" URL: http://www.acmqueue.com/modules.php?name=Content&pa=showpage&pid=159&page=5 (August 04, 2004)

The Free Dictionary. "Blaster Worm" URL: http://encyclopedia.thefreedictionary.com/Blaster%20worm (August 06, 2004)

The Free Dictionary. "Sasser Worm" URL: http://encyclopedia.thefreedictionary.com/Sasser%20worm (August 07, 2004)

WinPlanet . "Microsoft Hacked Again?" URL: http://cws.internet.com/article/1204-.htm (July 09, 2004)

TLA News. "Cisco Hacked?" URL: http://www.tla.ch/TLA/NEWS/2004sec/20040518CiscoHacked.htm (July 12, 2004)

Graham Hayday. **"**US government sites hacked by 'Mujihadeen'" URL: http://software.silicon.com/security/0,39024655,11029633,00.htm (January 06, 2003)

PCNET. "Welcome to PCNET's Support & Help Pages" URL: http://support.pcnet.ca/firewalls.htm (August 25, 2004)

Jupitermedia Corporation. "Online Dictionary" URL: http://www.webopedia.com/ (4 June 2004)

"GFI LANguard Network Security Scanner". URL: http://www.gfi.com/lannetscan/ (20 June 2004)

SANS Institute, "The SANS Top 20 Internet Security Vulnerabilities" Version 4.0. 8 October 2003. http://www.sans.org/top20/ (12 June 2004)

Cole, Eric. Hackers Beware
Sams; 1st edition (August 13, 2001) p.60

Suggested Links

CERT: http://www.us-cert.gov/
Mailing list: http://www.us-cert.gov/cas/signup.html

Endpoint http://endpointsecurity.org/

McAfee http://www.mcafee.com/
DAT Update Notification: http://vil.nai.com/vil/join-DAT-list.asp

Patch Management: http://patchmanagement.org/

Microsoft Security: http://www.microsoft.com/security/
Newsgroups: http://www.microsoft.com/technet/community/newsgroups/security/
TechNet Security: http://www.microsoft.com/technet/security/
Security Bulletins: http://www.microsoft.com/technet/security/

Security Pipeline: http://www.securitypipeline.com/
Newsletter: http://www.securitypipeline.com/newsletter.jhtml

Lavasoft http://www.lavasoft.de/

The Eye from Ad-Aware http://www.lavasoftnews.com/archives.shtml

Appendix

Appendix A: Desktop Configuration

Mixed O/S environment
- Windows
  - Windows XP SP1
  - Windows 2000 SP4
- Mac
  - OS 9
  - OS X

Different user groups with different levels of permissions
- Each Domain user has full Admin rights on their box.
- All IT staff has Admin rights on all systems on the Domain within the organization

Large network covering a large campus of buildings
- With many of the newer threats shutting systems down, remote access is not be available

SMS only on 80% of systems on the Domain
No GPO implemented
No software restrictions of workstations

Appendix B: Terms

Viruses according to Webopedia[13] are a piece of code loaded onto a computer without the user's knowledge and runs against the user's wishes. Viruses have been around since the mid 1980's and the codes have evolved accordingly becoming more involved and more damaging. A virus main purpose is to replicate itself and then deliver its payload or the intent of the code. A virus in the 1980's would not have the opportunity of today's networked environment in which millions of people today access the largest WAN on earth the Internet. Thus a virus can spread through territories that seemed unfathomable just a few years ago.

A **Worms** according to Webopedia[14] is a program or algorithm that replicates itself over a computer network; it is self-contained entity and does not need to be part of another code or program to reproduce itself. Worms can be written to do a variety of usually malicious things such as delete files, change system files, deliver a payload or simply burden the system or network with reproduction of itself. Worms have also been around since the middle 1980's and remain a constant threat to networks today.

A **Trojan horse** according to Webopedia[15] is a destructive program that masquerades as a benign application. Trojan horses do not replicate themselves but they can be just extremely destructive. Once again Trojan horses were born in the 1980's and became wide spread with the mass production of the personal computer. Trojan horses usually invoked the end user to download a program, file, or the like and then the true purpose of the code is revealed most time unbeknownst to the user. Free games and Bulletin boards were rampant with applications that contained Trojan Horses. A secure network should limit or deny access to areas that could potential threaten a network.

Abbreviations:

IDS: Intrusion Detection System
IRT: Incident Response Team
LAN: Local Area Network
Malware: Generic term used to refer to all types of malicious computer code
OS : Operating System
SUS: Software Update Services Server

Appendix C: Scripts

[13] http://www.webopedia.com/TERM/V/virus.html
[14] http://www.pcwebopedia.com/TERM/w/worm.html
[15] http://www.pcwebopedia.com/TERM/T/Trojan_horse.html

Windows Patches and Security Updates using QCHAIN written in Wise Installation System (Partial Script for Windows 2000 SP4):

```
item: If/While Statement
  Variable=OSTYPE
  Value=WinNT
end
item: If/While Statement
  Variable=WINDOWS VERSION
  Value=5.0
  Flags=00000010
end
item: Execute Program
  Pathname=%INST%\Windows-KB841720-ENU-V4.exe
  Command Line=/Q /C:"sasscln.exe /S"
  Flags=00001010
end
item: Execute Program
  Pathname=%INST%\DoomCln-KB836528-v4-ENU.exe
  Command Line=/Q /C:"Doomcln.exe /S"
  Flags=00001010
end
item: Execute Program
  Pathname=%INST%\IE_Q867801.EXE
  Flags=00001010
end
item: Execute Program
  Pathname=%INST%\ORS_KB832414.EXE
  Flags=00001010
end
item: Execute Program
  Pathname=%INST%\IE_Fix_28591.EXE
  Flags=00001010
end
item: Execute Program
  Pathname=%INST%\SP4forW2K.EXE
  Flags=00001010
end
item: Execute Program
  Pathname=%INST%\IE_Q833989.EXE
  Flags=00001010
end
item: Exit Installation
end
item: End Block
end
item: Remark
  Text=Windows XP workstations
end
item: If/While Statement
  Variable=WINDOWS VERSION
  Value=5.1
  Flags=00000010
end
item: Execute Program
  Pathname=%INST%\Windows-KB841720-ENU-V4.exe
```

```
  Command Line=/Q /C:"sasscln.exe /S"
  Flags=00001010
end
item: Execute Program
  Pathname=%INST%\DoomCln-KB836528-v4-ENU.exe
  Command Line=/Q /C:"Doomcln.exe /S"
  Flags=00001010
end
item: Execute Program
  Pathname=%INST%\IE_Q867801.EXE
  Flags=00001010
end
item: Execute Program
  Pathname=%INST%\ORS_KB832414.EXE
  Flags=00001010
end
item: Execute Program
  Pathname=%INST%\IE_Fix_28591.EXE
  Flags=00001010
end
item: Execute Program
  Pathname=%INST%\SP1wRollup1forWXP.EXE
  Flags=00001010
end
item: Exit Installation
end
item: End Block
end
item: End Block
end
item: Remark
  Text=Windows 2000 servers
end
item: If/While Statement
  Variable=OSTYPE
  Value=WinNT
  Flags=00000001
end
item: If/While Statement
  Variable=WINDOWS VERSION
  Value=5.0
  Flags=00000010
end
item: Execute Program
  Pathname=%INST%\Windows-KB841720-ENU-V4.exe
  Command Line=/Q /C:"sasscln.exe /S"
  Flags=00001010
end
item: Execute Program
  Pathname=%INST%\DoomCln-KB836528-v4-ENU.exe
  Command Line=/Q /C:"Doomcln.exe /S"
  Flags=00001010
end
item: Execute Program
  Pathname=%INST%\IE_Q867801.EXE
  Flags=00001010
```

```
end
item: Execute Program
  Pathname=%INST%\ORS_KB832414.EXE
  Flags=00001010
end
item: Execute Program
  Pathname=%INST%\IE_Fix_28591.EXE
  Flags=00001010
end
item: Execute Program
  Pathname=%INST%\SP4forW2K_SRV.EXE
  Flags=00001010
end
item: Exit Installation
end
item: End Block
end
item: End Block
end
```

Appendix D: Current Desktop Configuration

Standard O/S environment
- Windows
  - Windows XP SP1a
- Mac
  - OS X

Different user groups with different levels of permissions
Each Domain user has only Power User rights on their box unless an exception is requested with proper justification

Only selected IT staff have limited Admin access on all domain workstations for support purposes only.

Large network covering a large campus of buildings
- -SMS, SUS GPO and login scripts combined have a better success rate of reaching more systems than previously

SMS on 95% of systems on the Domain
Strict GPO implemented
Only approved, fully licensed and tested software is allowed on workstations

Appendix E: ePO agent and VirusScan Client Configuration

Emergency updates, in the event of a major virus outbreak, can be pushed through the server on a real-time basis.

The VirusScan console is set to update the DAT files twice daily to help insure that the virus definitions are current on each machine on the network

ePO agent contacts the ePO server every hour for configuration changes and scheduled tasks.

ePO agent configures VirusScan to perform a full system scan of all files as well as other tasks as follows:

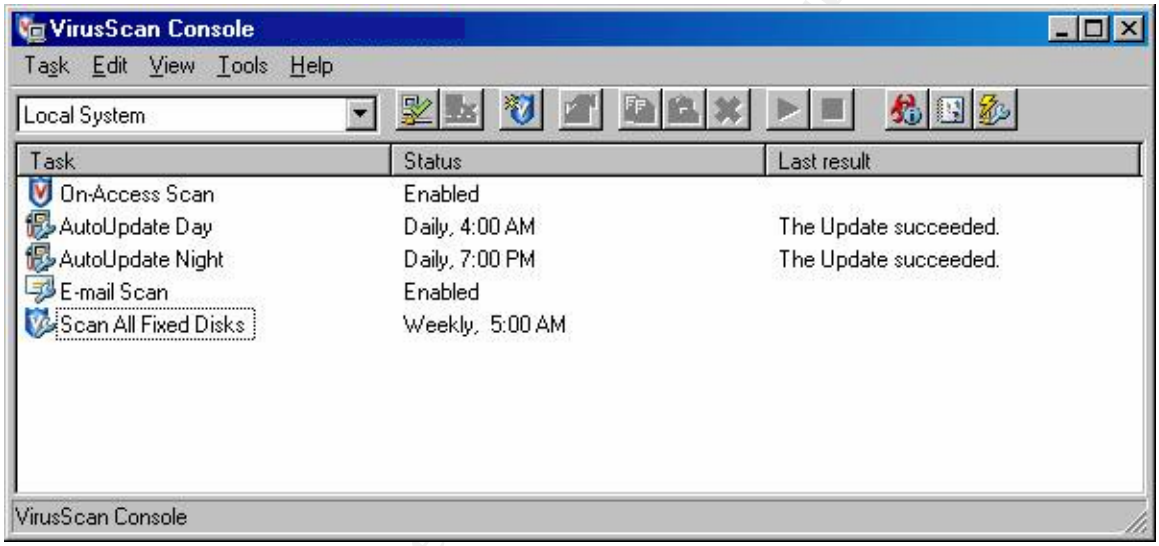

Figure 3 - VirusScan Console Settings