Global Information Assurance Certification Paper

Lessons Learned in Securing Blackboard

Peter Benedict

GSEC Certification Practical Assignment, v 1.4, Option 2

September 2002

Abstract

This paper details the efforts taken to secure Blackboard, a Course Management System (CMS), at an educational institution. Blackboard is currently in use at over 6000 institutions, and CMS use has risen dramatically in recent years. The institution's initial Blackboard implementation was accomplished without any system security policies or safeguards in place. The paper describes the initial process, and then details the variety of system compromises (including a UNICODE compromise and one compromise of unknown origin) and security safeguards that were put in place in the following months. The process of increasing the security of Blackboard proved invaluable for the institution, leading to a number of positive outcomes for Blackboard and for systems across the institution. The paper includes a summary of steps taken to further security, ongoing security concerns and the plans to address them, and some questions for future research.

Introduction

As more institutions seek to provide web-enhanced and distance education through the Internet, Course Management Systems (CMSs) play an increasingly large role in education. The rapid growth in CMS adoption is reflected in the large number of institutions using CMS software. CMSs have added more features in recent years, and as a result have become more critical to educational enterprises. Current CMS features include chat rooms, bulletin boards, grading, and Student Information System (SIS) ties which allow for CMS data to update SIS systems. These features make Blackboard system integrity (and reliability) crucial to the functioning of the university. A two-hour loss of data could mean entire classes of students lose their quizzes or midterm exams, for example, or professors may lose hours of development time.

Blackboard[1] currently holds the largest number of clients among CMS vendors (6000+ as of 2001, see Blackboard's "Blackboard Clients"[2] for examples). Securing Blackboard will be an increasingly important issue for institutions as web-enhanced and web-based delivery of educational content becomes more prevalent.

The challenges of security in an educational enterprise are well documented, including the presence of machines over which network administrators have little or no control[3], lack of coherent and well-understood security policy[4], and the usual challenges of securing any complex environment. This paper is a case study of one university's attempts to secure a CMS environment, detailing initial implementation and concerns, successful system compromises, and the steps taken to lock down the environment. The case study also illustrates how a system administrator can use security compromises as leverage in obtaining security training, adding tools to the security environment, and heightening institutional commitment of administrator time to preventing exploits. The paper will end with a summary of the institution's security improvements, areas which still need improvements, plans to further security, and questions for further research.

Case Study

Description of the University Setting

Institution X (a university of ~12,000 students offering ~6000 courses/year) had previously used an early version of WebCT, a competing CMS. WebCT's early implementation started with one department's efforts, and grew slowly over time until over 25% of the student population used it in some portion of their course work. The only significant outage of WebCT, which lasted three days, was caused by a hack and a subsequent failure of the tape restore process. This was the first high profile compromise of an enterprise system at the institution, and the negative public impact was severe enough to harm the CMS's reputation at the institution.

In early 2001, the institution's management formed a project team to look at CMS

vendors at the enterprise level, with representation from faculty, students, and IT staff. Blackboard was chosen in late 2001. Key project milestones included the arrival of the servers and software (January 2002), testing (Spring 2002), pilot project (Summer 2002) with approximately 30 courses, and full implementation (Fall 2002).

The Blackboard Application Environment

The Institution chose to implement Blackboard in a two-server configuration, with one database server (running MS SQL 2000 on Windows 2000) and one application server (running IIS on Windows 2000). The institution purchased four servers, two for use as production servers, two for use as test servers to test patches, customizations, updates, etc. The institution also elected to have the servers pre-configured by Blackboard (a decision which led to some of the largest hurdles in securing the servers). The server hardware consisted of four identical Dell 6450s, each with four Pentium Xeon processors and 4GB of RAM. The initial implementation used local hard disk storage (no RAID); just before the start of the full project implementation in Fall 2002, the storage was migrated to a Storage Area Network (at RAID 5). Backups were recorded using Veritas's Backup Exec software, using a schedule of one full weekly backup, nightly incremental backups, and off-site storage of monthly backups.

Initial Implementation and Testing

The Blackboard environment was put into testing in February of 2002. Initial concerns and investigations into the software unfortunately did not include security assessments, which highlights 1) the aforementioned lack of security policy in many institutions of higher education, and 2) the common mistake of putting important systems in the hands of administrators without formal training or certification. In hindsight, what the institution implemented was the following: four Windows 2000 servers, all running IIS (two of which needed it, two of which didn't), two with SQL 2000. The OSs were patched to Service Pack 2, IIS was completely unpatched, SQL was patched to Service Pack 2, and no other security settings of any sort were used. At the time, the institution was without a network firewall.

In March 2002 the system administrator attempted to secure IIS by applying the most recent security rollup patches. This was precipitated by a communication from the institution's Network Security Administrator, advising system administrators of a recent vulnerability. The patch was obtained from Microsoft's TechNet[5], and was run in late March on the test and production environments. Within an hour, Blackboard stopped functioning in the test and production environments. The system was still serving web pages, but the pages consisted primarily of SQL error code.

It took approximately one week for the Blackboard servers to be brought back up, a process that required a complete rebuild. The institution at this point discovered

Blackboard's stance regarding OS, IIS, and SQL server patches:

> Blackboard will not support any security updates released by Microsoft, after Blackboard has already been released. Blackboard validates all the Microsoft patches released before the release of Blackboard, so as to ensure the compatibility with Blackboard products.
>
> NOTE: This applies to all Security updates
>
> If you are going to implement updated Microsoft Security patches on your own, please note that you will have permission changes to the file structure of Blackboard and your server. Make sure you do a complete backup of your system before running these patches.
>
> PLEASE NOTE THAT THIS IS NOT SUPPORTED, AS IT HAS NOT BEEN VALIDATED.[6]

The system administrator notified high-level management that Blackboard did not appear to function with IIS patches, and informed them that Blackboard Technical Support stated (by phone) that we could not patch our servers. Management notification included the administrator's assessment that the risk of a security compromise with the existing environment was extremely high. The server administrator at this time began researching security issues, and a SANS Security Essentials training[7] was approved at this time, to take place in June 2002. At this point, however, the concern for Blackboard was still minimal, with little sense of urgency and a sense that the security risks were acceptable.

Blackboard Gets Hacked, Part I

On May 21, 2002, Blackboard test users started receiving messages that there was no storage room on the server. After some investigation, it was discovered that the database server had been filled with a broad variety of "warez" ranging from .mp3 files to a German-language version of "Star Wars: Attack of the Clones." Ironically, only the test database server was hacked, although the production server was identically configured and located just two IP addresses away in the network space.

The institution's network security administrator did some log analysis using Snort[8] and Shadow[9], and determined that the server had been hacked via UNICODE exploit[10], a well-known and well-documented IIS vulnerability. The server was rebuilt at this point, and put back into production in the same state it had been before: unpatched and vulnerable to any attacker, although this time the server was installed without IIS. As a fortunate side effect, a layer of middle management became more concerned, and began to ask questions regarding how we could secure the environment.

Security Training and Leverage

In late June of 2002, the Blackboard system administrator was sent to SANS

Security Essentials training. Upon returning, the system administrator began to define the risks involved in allowing Blackboard to run without being secured in any way. Armed with "Securing Windows 2000: Step by Step[11]," the system administrator advocated for permission to wipe out the test environment and rebuild it using better security practices. In part as a result of concern over the previous hack, this was approved and the system administrator began rebuilding the Blackboard environment (detailed below). The time spent in this endeavor was significant (10-20 hours/week for two months), and required prioritizing security over work on features and flexibility, an adjustment that management initially struggled with but eventually deemed worthwhile.

In July of 2002, the server administrator carried out an ad hoc risk analysis, based on materials covered in the security training. This risk analysis looked at two dimensions: likelihood of compromise and importance of data[12]. Although there are much better risk assessment tools available[13], the risk assessment's results were enough to increase management concern and increase the priority of getting a secured production environment. Given the extremely sensitive data (e.g., social security numbers, grades, etc.) and high risk of compromise, it became an institutional priority to get the production environment secured.

Securing Blackboard

The primary challenge in securing Blackboard was its use in a 24-hour, seven day per week environment. Due to the importance of keeping the system available, the system administrator chose to rebuild the test servers first, secure them, install Blackboard and ensure that it functioned, and then migrate the production system data to the test servers.

The resources used in securing the servers were the aforementioned SANS text; Microsoft's "Window Update" site[14] which contains a variety of unnecessary features and some useful security patches), and the SANS reading room[15]. The most important steps taken in securing Blackboard were the removal of unnecessary services[16] (e.g., IIS on the database server), the patching of IIS on the application server, the patching of Windows 2000 on both servers, and the removal of default code (e.g., the sample files included with IIS during installation).

The installation of Blackboard on the secured test servers was somewhat problematic, as some SQL installation routines failed. They were eventually made to work via some mild hacking of the code. The application itself was not hacked or locked down any further than its default install. Migration of the production system databases and files took place in August of 2002, at the end of the pilot project.

The Importance of Defense in Depth[17]: Blackboard Gets Hacked, Parts II and III

At this point, the system administrator was confident in having a secured environment, and even went so far as to notify the management community of his increased confidence in the integrity of the system. The administrator's optimism, in this case, was short-lived.

Five days later, the system (in this case, the production database server) was again hacked. This was discovered during a routine perusal of the event logs, where messages regarding DameWare NT Utilities[18] were discovered. A perusal of the data drive showed, yet again, a broad variety of "warez" ranging from Peter Pan (French language version) to X-box files. The files were hidden in a sub-folder in the SQL data directory structure, along with an FTP server, which was installed as a service. An examination of open connections to the server showed a user connected through netbios. This connection was severed immediately, and the offending files were deleted.

At this point, the institution's firewall was running in essentially passive mode, allowing all traffic to and from the campus to all machines. It was noted that there was no need for any system other than the application server to connect to the database server, and management allowed the administrators to make Blackboard's database server the first machine to be protected by the firewall. The database server was screened (at the router and firewall) from all connections not originating from the application server.

The application server was hacked one day later. The same files (DameWare, FTP server, etc.) were discovered on the server, with the same bogus user listed as responsible for the hack. This time, however, the hacker added a layer of complexity to the intrusion. A search of the data drive showed that there were 18GB of unexplained used space, that is, there were 3GB of known files on the server, yet the drive showed 21GB in use. A perusal of every folder on the system showed that none of the folders were large enough to account for the extra data… until the recycler folder was examined. This folder is used to store "Recycle Bin" material (deleted files, etc.). There is fairly extensive documentation of recycler vulnerabilities on a number of sites[19], and Microsoft has been aware of recycler vulnerabilities with NTFS since NT 4.0[20]. Apparently, however, the latest Windows 2000 service packs and cumulative security roll-up patches do not close this hole, or perhaps a new exploit has been discovered which is not yet documented. The vulnerability involves a hacker setting up a file in an unused recycle bin that is named after the SID (obtainable if netbios is enabled) of a valid user. The hacker can then manipulate the file as needed.

The server administrator sanitized the servers as best possible by removing DameWare services and files, running comparisons of various directories and file sizes (particularly the system32 directory), visually examining every folder on the system, and deleting the offending recycle bin folder.

After this hack, the Network Security Administrator downloaded and configured Nessus[21], a vulnerability scanner, and used it to probe the Blackboard servers. The resulting information was then used to further harden the server and block connections more effectively. Screening netbios was a particularly high priority, given its vulnerability to exploit[22]. Nessus, for example, was able to print a list of user IDs, shares, etc., through the netbios port. The firewall and router were configured to deny access via netbios, and other known dangerous ports were

blocked. For an excellent write-up of Nessus and how to use it, please refer to the SANS Reading Room[23].

Outcomes, Remaining Issues, and Plans to Address Them

Positive Outcomes

Throughout the course of the Blackboard implementation, hacks, and hardening, the system administrator and institution learned a broad variety of lessons in information security. The institution's experience with Blackboard illustrates the positive outcomes that can follow a security incident:

1. The compromises of the Blackboard servers led to system administrator training (specifically, SANS Security Essentials).
2. The network security administrator gained experience with a variety of security tools, and shared that experience with the Blackboard system administrator. In particular, an upgrade to Snort and the first uses of Nessus were valuable improvements to the institution's security posture.
3. The firewall was put into use more rapidly than called for in its original project implementations date, and its successful use in screening two servers from further attack has given the project some positive community public relations.
4. The Blackboard system administrator has been charged with creating a risk assessment model recommendation that may become policy for the institution's server administrators.
5. Perhaps the most important outcome is the institution's commitment of human resources (i.e., system administrator hours) to security, which has been significant.

Prior to these incidents, the institution was vulnerable across a broad variety of systems: as a result of the fairly minor compromises experienced thus far, the institution has a much higher awareness of security issues, and the implementation of better security practice policy will be much more positively received than if there had never been an incident.

Outstanding Security Issues

Although the Blackboard systems compromises increased security awareness and led to positive changes in security practice, there are still a number of fairly serious security concerns:

1. The institution's firewall is still functioning more like a router than a firewall, as it is protecting only Blackboard at present. All other traffic is allowed to pass through.
2. Netbios connections to the institution's servers are still permitted from off-

campus. This policy has proven extremely resistant to modification thus far, due primarily to faculty members who use netbios connections and consider such functionality critical to their work.

3. Blackboard didn't function when patches were applied after the product was installed, but worked when Blackboard was installed on an already secured system. If this process is required for all future patches and service packs, the human resource investment in keeping Blackboard secure will be quite significant.

4. Blackboard depends on a number of other systems, including a data warehouse, the student information system, an authentication server, DNS, etc. None of these systems have been examined for security features or flaws by a certified or trained administrator.

5. The institution does have some network security policy in place, but there is currently no policy (nor even a best practices document) in place regarding the security of individual systems. As an example, there are policies allowing the security administrator to isolate compromised systems, but no policies or recommendations in place informing administrators of their options (or requirements) for minimum security.

6. The Blackboard application itself may have security holes. Nessus produced a significant number of warnings on ports that Blackboard requires for normal operations.

Addressing Outstanding Security Issues

The list of outstanding security issues is lengthy, and is illustrative of the challenges faced by educational system administrators. Nonetheless, the institution has plans in place to address each of the concerns noted above.

1. The network security administrator will gradually phase in the firewall, initially blocking ports with significant vulnerabilities. There will eventually be a DMZ established, and policy practices for determining whether a server should be in the DMZ or the trusted network. Eventually, unused and unnecessary ports will be blocked by default, and the network will only be opened as required for specific uses.

2. After the netbios connections to Blackboard were explained to director-level management, eliminating netbios moved much higher in the institutional priority structure. Getting buy-in from that level of management means there is a much better chance of eliminating such connections as a matter of policy.

3. Blackboard's refusal to support web server and OS patches and service packs is a matter of concern for a large number of institutions, as evidenced by articles in their Knowledge Base and list serve traffic. Perhaps these concerns will lead to changes, particularly if institutions choose to migrate

from Blackboard to competing vendors. At present, it appears the institution is willing to allot the necessary hours to keeping Blackboard secured.

4. The Blackboard system administrator has created a diagram of system dependencies, and is in the process of developing some best practices documentation so that other institutional resources can be secured (see #5).

5. The Blackboard system administrator has been charged with developing a set of best practices for institutional servers, which will be presented to the Network Systems Architecture team for review, approval, and implementation. The team has not yet decided whether the practices will be required or recommended for institutional server administrators.

6. There are currently no known cases of Blackboard servers being compromised through the ports noted in #6 above. The security of the application is probably the least important priority to the institution at present, as the regular version upgrades and relative obscurity of the application make Blackboard an unlikely target for the majority of crackers.

Questions for Further Research

Questions for Further Research

Some outstanding questions beg further research and/or legal examination:

1. What are the legal ramifications of the decision to use “unsupported” patches and service packs to secure systems?

2. If securing a product causes the application to stop functioning, does a client have the legal grounds to obtain a refund or invalidation of contract?

3. At what point is the vendor responsible for refusal to test new security features after the release of their product?

4. If an institution is told not to apply patches or fixes to a system for the enhancement of security, who is liable if sensitive data is compromised and misused?

5. Would the vendor’s pre-installation of OS, web server, and application limit the liability of the institution?

Unfortunately, these questions will probably get answered over time in the judicial system. There is a growing body of legal privacy requirements[24] regulating protection of sensitive information. At this time, however, there do not appear to be any cases that address the vendor’s responsibility to support security features vs. an institutions’ responsibility to secure their systems or choose a different product. The relative dearth of legal precedence in information security[25] highlights the importance of some of the previously noted questions. Of particular importance for educational institutions is the matter of vendor vs. institutional liability. Clearly, implementing insecure applications which track sensitive data is unethical, but is it

illegal?

In this institution's case, the sensitivity of the data and the critical nature of the software services determined the course of action (securing the servers despite being told not to do so). Fortunately for this institution, securing the servers proved possible in the end, and didn't break anything that was unfixable.

List of References

Blackboard, “Welcome to Blackboard” URL: http://www.blackboard.com, September 2002

Blackboard, “Blackboard Clients: Blackboard Course and Portal Client List” URL: http://company.blackboard.com/clients/index.cgi?cl=cp, September 2002

Vosswinkel, Kerry “Unique Security Challenges in Higher Education - Securely Integrating Student-owned Computers into Your Network” SANS Institute Information Security Reading Room, URL: http://rr.sans.org/casestudies/challenges.php, Sept. 26, 2001

Davis, Ryan “Information and Network Resource Administration and Security in an Education Network Environment” SANS Institute Information Security Reading Room, URL: http://rr.sans.org/casestudies/edu_net.php, August 12, 2001

Microsoft TechNet, “Security: Trustworthy Computing for IT” URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/default.asp, September 2002

Blackboard Knowledge Base Article, Topic ID 181-573, “Microsoft releases different “Security Patches” after the release of Blackboard. Should Blackboard customers run these security patches or updates from Microsoft?” June 13, 2002

SANS Institute, “SANS Institute” URL: http://www.sans.org/newlook/home.php, September 2002

Kipp, James, “Using Snort as an IDS and Network Monitor in Linux” SANS Institute Information Security Reading Room, URL: http://rr.sans.org/intrusion/monitor.php, June 13, 2001

Delvecchio, Anthony “Building Network Intrusion Detection Systems Using Open Source Software” SANS Institute Information Security Reading Room, URL: http://rr.sans.org/intrusion/net_id2.php, June 11, 2001

Miller, Nate “Microsoft IIS Unicode Exploit” Lucent Technologies Worldwide Services, URL: http://www.lucent.com/livelink/0900940380004b2d_White_paper.pdf, September 2002

SANS Institute, “Securing Windows 2000 Step by Step Version 1.5” July 1, 2002

Symantec, “Vulnerability Assessment Guide” URL: http://enterprisesecurity.symantec.com/PDF/167100088_SymVAGuide_WP.pdf, January 2, 2002

Yazar, Zeki, “A Qualitative Risk Analysis and Management Tool – CRAMM” URL: http://rr.sans.org/audit/CRAMM.php, April 11, 2002

Microsoft, “Welcome to Windows Update” URL: http://v4.windowsupdate.microsoft.com/en/default.asp, September 2002

SANS Institute, “Information Security Reading Room” URL: http://rr.sans.org/index.php, September 2002

SANS Institute, “Mistakes People Make that Lead to Security Breaches” URL: http://www.sans.org/mistakes.htm, October 23, 2001

Symantec, “Security Response: Defense in Depth Benefits” URL: http://securityresponse.symantec.com/avcenter/security/Content/security.articles/defense.in.depth.html, September 2002

Dameware Development, “Welcome to Dameware Development” URL: http://www.dameware.com, September 2002

Vidstrom, Arne, “Recycle Bin creation vulnerability in Windows NT / Windows 2000” URL: http://ntsecurity.nu/advisories/a14.shtml, September 2002

Microsoft TechNet, “Microsoft Security Bulletin (MS00-007)“ URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms00-007.asp, February 1, 2000

Deraisson, Renaud, “Introduction: Nessus” URL: http://www.nessus.org/intro.html, September 2002

Slim, Iceberg, “The Visual, Step by Step Netbios Hack” URL: http://www.fromadia.com/newsread.php?newsid=480, May 30, 2002

Mitchell, Jason, “Proactive Vulnerability Assessments with Nessus” URL: http://rr.sans.org/audit/proactive.php, April 26, 2002

Holtz, Gary “System Security and Your Responsibilities: Minimizing your Liability” URL: http://rr.sans.org/legal/liability.php, July 23, 2001

Philip, Amit Raju, “The Legal System and Ethic in Information Security” URL: http://rr.sans.org/legal/system.php, July 15, 2002