Policy Enforcement:
Violation, Detection and Mitigation

GIAC Security Essentials
Certification: GSEC
Practical Assignment
Version 1.4c

Option 2- Case Study in Information Security

Submitted By: William P. Kenney
Location: SANS New England 2004, Boston MA

Date Submitted: February 21, 2005

Abstract

This document describes the tools and techniques employed by a state University to enforce a part of the computer usage policy on the campus which requires all users to maintain patched operating systems, software applications, and employ current antivirus protection while connected to University network resources. Open source and commercial software is used in conjunction with specialized hardware to detect policy violations and offer users appropriate tools to mitigate their threat to the network, the University community, and the Internet.

The name and location of the University have been omitted from this document to protect the integrity of the information systems structure and specific implementation of the tools used to secure the network.

This is a team effort in which my part includes introducing other team members to Unix/Linux operating systems and employing open source software tools to monitor our network and computer resources connected to the network. This entails building Unix/Linux servers and workstations to serve as victims and intruders to enable the team to learn to interpret the results obtained from testing and implement the tools in the production network. This project has been ongoing for several years and continues as new methods of intrusion are propagated and new tools become available. Several commercial tools have been employed in our network as replacements or to augment open source tools.

The University Environment: The University is a member of a state system that consists of a system office and several campuses. The system office provides many centralized services such as ISP, business system clusters and historical archives of business data.

This University can be divided into three major business groups.

1. The administrative group, responsible for financial, HR, and facilities infrastructure,
2. the faculty which maintains and delivers curriculum to students,
3. And the student body, both resident and commuter.

Each group has legitimate needs to access network and computer resources to perform their respective functions. We also provide limited public library access to the general population. Public computer usage is limited to Internet access employing secure kiosks to several research databases at remote locations. Printer access is limited to workgroups.

The requirements of each group differ widely from the student body's very restricted access to University resources that include Internet access and a small file share for assignments to administrative requirements that may include access to financial, health or other sensitive information. Members of the faculty are granted access to student academic information and administrative information required for the conduct of training, evaluate student progress, and perform their administrative functions.

The University is a homogeneous networking and computer environment with desktop collaboration software running Windows and MAC environments and Unix/Linux performing much of the backend business and security processes.

Meeting the Challenge: The University provides a secure and reliable environment for all users by employing many internal and external layers of defense. Malicious code attacks against Internet servers and clients have grown to epidemic proportions in the past several years[1]. As a result we have added many tools to mitigate and correct deficient system controls that allow perimeter and system penetration, DDOS attacks, spam, and more recently, phishing against our users.

Monitoring the Network: Our network defenses appear both layered and like a marble cake. The marble cake view results from the physical location as well as the particular network layer the device or software monitors network activity. Starting at the system office there is firewall and intrusion detection systems that sample both inbound and outbound traffic for anomalies. The bi-directional

[1] Malicious Code Propagation and Antivirus Software Updates http://www.cert.org/incident_notes/IN-2003-01.html

sampling will alert campuses of infected internal traffic and probing by potential intruders. Internally we continue the layering with both commercial and open source products to defend against Trojans, worms and virus attacks, root kits and other forms of system intrusion.

Perimeter Defense: The System Office provides a firewall that limits traffic inbound to shared computer resources at the system office. The configuration is very restrictive, allowing only traffic such as that destined to dns, dhcp, web, and mail services to selected computers in each University's block of IP addresses. Additional services are allowed by request through our network management group for specific IP addresses/ports appropriate for the particular application or service being offered or utilized.

Our local perimeter defense consists of firewall devices to provide additional security should the system office become compromised. Sentinel applications will notify appropriate personnel should this occur. Additional firewalls are employed on our servers to protect against internal attacks.

Network Configuration: Network resources are discreetly apportioned into several Windows domains to address the needs of user accessibility and security. The primary domains will be referred to as Staff and Student in this article. Since the mix of staff, faculty and students in each of the campus locations varies, many Virtual Private Networks[2] are also employed to provide secure access to resources for each group.

The Staff and Student domains are the core domains in which access controls determine what services should be provided to an individual.

A Quarantine Virtual Private Network (VPN) is where much of our policy on virus-free and updated systems is currently enforced. When a computer attempts to join the campus network but does not pass security checks, it is only allowed access to resources to resources in this VPN until it meets the security requirements. This will be described in more detail later in this document.

From Reactive to Proactive:
Lost time, damaged system resources and bad publicity were only a few of the driving factors in moving quickly from a reactive to proactive network security management posture. Education is a business, and like any other business we need to deliver our product on time, within budget to our customers. Without a strong commitment to satisfying the student needs we would lose customers!

Factors Driving Change:

[2] How VPN's work http://computer.howstuffworks.com/vpn.htm

Recent virus attacks on computer systems have challenged the network and operations section of the Information Technology Services (ITS) department. Early attacks, such as the love bug, were propagated via email with a little social engineering to entice the user to open an infected email document. Subsequent attacks have been more subtle, and predominantly aimed at exploiting browser and OS vulnerabilities in the Windows operating environments. Earlier Windows systems were often installed accepting the default options unless there was a specific reason to do a custom installation. This practice left the systems extremely vulnerable to attack through unused and therefore unmonitored ports. System monitoring was usually limited to reviewing the "event logs" when a problem was detected or reported.

Production business servers are predominantly running OpenVMS, Unix, and Linux where default configurations are rarely acceptable. These servers don't have the same issues as the largely windows based user environments. Most production servers have tuned configurations focused on their assigned applications and tasks. A successful attack on a Linux server in 1998 brought the issues around securing our OpenVMS, Unix and Linux based production environment into focus when an application vendor supplied system was security deficient. We remedied this and the lesson provided further motivation toward a proactive security stance for all platforms.

Stages of Improvement: Early responses were primarily reactive. Detection was obvious–systems were infected and non-functional. Mitigation and recovery measures were brute force. Our network was physically disconnected from the Internet and the network segments isolated at key routers and switches. A clean notebook with the appropriate tools was attached to scan and remove the virus from computers in that particular segment. As the systems were cleaned and updated virus scan software and system patches installed, they were allowed back into the network. The cleanup took several days to complete and costs were significant. Several hundred hours of technician, faculty, and outside support were required to repair the damage to the network and, additionally the interrupted training caused many difficult scheduling issues. Faculty, staff and students were made aware of the need to keep their systems updated and response moved into a more proactive posture.

The initial proactive screening of computers during the next semester was an improvement but still led to wide–spread email infection, although recovery time was much better and less labor intensive. The University had upgraded the anti-virus license to a site license and distributed this on CD to all incoming freshmen and returning students. They were requested to run the CD before connecting to our network. Most did and the virus outbreak had a lessened impact.

The following semester was a great improvement for faculty, staff and students. A Microsoft™ System Upgrade Service server was implemented and provided reasonable patching of existing attached systems. A CD was distributed to new and returning students containing additional functionality and software. The additional scripts determined the patch level of the OS, version of the antiviral software and employed the Microsoft™ scanning tool to determine the suitability of the system to allow connection to the University network. A cookie was set if the system passed and the computer was allowed to connect to the network at the next reboot. Those that didn't pass the test got a popup screen directing them to report to the ITS help desk center where assistance in cleaning up the computer was provided. This resulted in several hundred PC's and laptops being delivered to the center. The network was not interrupted but the help desk staff needed to be temporarily augmented to respond to the increased workload. The augmentation came from other sections of the ITS department. Although the additional work was accomplished with in-house staff, overtime costs were significant and other work was postponed. The net cost was much less than the previous incident and, more importantly, to the non-ITS staff everything was "business as usual".

Customized Controls Aid Enforcement: During these semesters the network configuration had undergone a tremendous expansion and modernization due to several major construction projects and infrastructure initiatives. The most significant change that assisted in policy enforcement was the implementation of VLAN's needed to segregate different user groups located in the same building. Users are assigned to a specific VLAN based on the profile contained in the Active Directory for that person logging into our system. This provides the user with access to resources necessary to carry out their tasks regardless of what workstation from which they log on to the network. As an extension to this customization, a "Quarantine" VLAN was established. All new systems attaching to the network were automatically assigned to this VLAN where the system was scanned for missing patches, outdated antivirus signatures and unnecessary open ports. Quarantined systems are identified by MAC address to preclude that system from entering the network from any port on campus until all issues are resolved. Many commercial and open source security tools are employed in this restrictive area to protect the network. Several tools will be discussed later in this document.

Several servers were installed as members of the Quarantine VLAN and the user of the quarantined system had access to them to apply all available fixes for their computer operating system and supported software. Additionally, the user had Internet access in this VLAN to patch and update personal software from the vendor's web site. Once the system was clean and patched it was allowed onto the network in the appropriate domain and VLAN.

Current Environment: Our current environment continues to evolve as result of many changes to our policy, infrastructure, attacks from internal and external sources, and requirements for access as a public educational institution. The University maintains five major groupings with differing levels of access. These help in assuring that the appropriate capabilities and resources to accomplish an individual's proper tasks are available, but sensitive information and control is maintained. All access to information at this University in on a need-to-know basis for everyone. These groupings are the Public, Students, Faculty, Administration and System Management.

Public: As a public educational facility, most buildings are made accessible to everyone during normal working hours and to specialized buildings for public events. The library has computer labs designed to facilitate easy access for everyone. Private Citizens may use the resources in designated areas for research and entertainment during normal hours. The systems designated for use by private citizens are restricted to library resources and the Internet only. Additional physical security measures keep the general public out of restricted areas.

Students: Students may utilize any resource that is not in an area restricted to faculty or staff to login to the system to work or study. Since they login to the student domain they are given appropriate privileges defined in our usage policy and enforced by the Active Directory group policy in effect for students.

Faculty: Faculty may login on any system not in a restricted area. Faculty members have additional system privileges allowing them to add and remove software packages to their office computer to facilitate research as required by their contract with the University. Access to student records is permitted for posting grades and other student/faculty related tasks.

Administration: Administrative members may login on any system not in a restricted area. Administrative members may add or remove software from their office computers, access student and administration information required to carry out their duties, and manage group resources such as printers and other peripheral devices assigned to their work group. Administrative personnel assigned to Academic Support have full access to campus laboratory and classroom computer systems to ensure appropriate software is loaded for faculty and students. Laboratories have assigned monitors when open and classroom equipment is the responsibility of the professor during classes and Campus Security when no class is in session.

System Management: System managers and system administrators are tasked with providing access to shared resources and information in accordance with current University policy. Accounts are created upon receipt of written requests from responsible supervisors. This group is also tasked to monitor system performance, security, and usage trends to recommend changes to existing policy requirements and hardware replacement and upgrade. This group has access to restricted areas such as server rooms, network distribution closets, and business production areas.

This group develops and maintains computer resource images that are consistent with the administrative and teaching needs of the University. Pushing images to laboratory and office computers provides initial configuration in a pristine state and also ensures the number of software licenses deployed in the University do not exceed our site license agreements.

Tool Choices The University employs open source and commercial detection and mitigation tools[3]. Some have been in use for over a decade and still are very useful and other more recent additions have been of tremendous value.

Tools are chosen for several reasons, efficiency, support, ease of use, cost to name a few. A more important issue at a University is that the tool needs to be unobtrusive when employed and can be easily configured by the support staff at their convenience. A University environment is truly 24 X 7 as students require access any time, day or night. Many students do not live on campus or even in the same time zone. This requires us to make sure access to resources is reasonable for the end user 24-hours a day. This is accomplished by scheduling certain security processes on systems when they are least loaded and, in some cases, have added system redundancy to ensure resources are available at all times.

I have briefly described several of the tools that provide consistent value in the following paragraphs. Links to additional information and download sites are included in several of the descriptions.

Detection and Mitigation Tools:

Tripwire: The open source version of Tripwire has been employed on several Unix servers here since 1995. When installed, the software creates a database of system file characteristics for periodic comparison with the current file. Changes in file characteristics cause the program to send an alert to a designated user or email address indicating the file has been altered. False

[3] Network and System Monitoring Tools http://www.alw.nih.gov/Security/prog-full.html

alarms are often caused after system updates which help to confirm the tool is working. The open source version may be obtained by visiting http://sourceforge.net/projects/tripwire/. Additional information on the commercial version and many FAQ can be found at http://www.tripwire.org/.

Crack: This password cracking utility is extremely useful to determine the strength of user and application passwords. Several dictionaries are available from the open source community and system administrators may make their own dictionary to ensure default and weak passwords are not being employed on their systems. Use of this tool supports our strong password requirement. A very informative site can be found at http://www.crypticide.com/users/alecm/ and Crack may be obtained at ftp://ftp.cert.dfn.de/pub/tools/password/Crack/

SNORT: This open source Intrusion Detection System (IDS) has been successfully employed on our network for the past several years. It was instrumental in enabling us to determine which ports were being probed on our network. Unused ports open in default system configurations were closed and systems requiring those ports open to provide services were appropriately patched and monitored. This tool is run after notification of unusually high probing activity and periodically scheduled as a normal precaution. Additional information about SNORT and the platforms it may be run on can be found at http://www.snort.org/about.html

NESSUS: This open source program is a core utility in our detection and mitigation policy. Frequent and random scans of the network will alert administrators to potential vulnerabilities in servers and client workstations. Workstation users are notified of minor problems and given directions to mitigate the problem on their own while more serious problems are handled by our help desk staff. In many cases the workstation is reassigned to our quarantine VPN to preclude negative impact on the rest of the network. Server administrators are notified immediately of all discrepancies noted so they may take appropriate action. It should be noted that many false positives are often generated, but still need to be reviewed to determine if the service in question is still required on that particular system. An excellent knowledgebase is available at http://www.edgeos.com/nessuskb/ and Nessus may be obtained from http://www.nessus.org/download/ .

McAfee Antivirus: Currently, McAfee VirusScan is our primary antivirus software for University Windows workstations and servers. We maintain a site license that allows us to provide this software to all faculty, staff, and students running Windows operating systems on their personal computers. We provide updates to the software and virus database on a local server. Our detection tools also recognize other software vendor antivirus packages that may be installed on individuals' personal computers.

Clam AV: An open source antivirus program. This is installed on new test systems to provide basic antivirus protection and is used to scan other workstations as a backup to the other workstations' installed antivirus software when a new virus is suspected. Documentation is good and the software is simple to maintain. Clam Av may be downloaded from http://www.clamav.net/ . Documentation, FAQ's and installation instructions are also available at this site.

Vexira Antivirus: A commercial antivirus package used on some Linux production servers that have unique software requirements. Key features are available at http://www.centralcommand.com/linux_server.html .
Vexira Antivirus is available for most server platforms and is relatively inexpensive.

Sophos Antivirus: This commercial antivirus package is used on several production Unix servers. This package is exceptionally good at finding infected, corrupt, or password protected files that were created with other operating systems. Additional open source utilities extend the usefulness of the software. The package can be used interactively oy run from a cron job. Sophos does not clean infected files. It will delete or move the files it determines to be infected into a "quarantine" directory to allow the administrator to make the final disposition.

SUS: Microsoft Software Update Services (SUS) is a no-cost add-in component for Windows 2000 and Windows Server 2003 designed to simplify the process of keeping computers up to date. Due to the diverse computer configurations needed to effectively meet the needs of the University population, we employ several servers running this service.

Patches from Vendors: Patches from vendors are applied to the operating systems and software applications as soon as feasible. We normally test the patch on a non-essential system first to ensure it doesn't cause any conflict with the existing configuration. Once we are satisfied the patch will not create an unstable on non-functional system we push the patch into the production area with the tools described above for faculty and staff. Students are notified of vendor patches and directed to the quarantine servers to download and install patches at their convenience. Many sites on the Internet maintain a repository of patches[4] for hardware and software that we don't directly support.

The images maintained by the system management group are updated and lab managers deploy the patched images to the lab computers during scheduled

[4] A patch repository for software and hardware http://www.softwarepatch.com/

lab closures.

Enterasys Dragon: This commercial tool has proven particularly useful in detecting and responding to intrusion against our network. In addition, the excellent graphic displays are easily captured into presentation software that is used for training staff and informing faculty of current threats and methods to mitigate them. Additional information on this product may be obtained by following http://www.enterasys.com/products/ids/.

Campus Manager: Campus Manager is a commercial monitoring product that contains features of several open source tools and has the additional capability of remotely managing network resources. We can turn services on and off from a central location which reduces the out-of-office time for technicians. Remote manipulation of PC's switches, routers and other network devices allows us to quickly isolate problems before they become campus wide. A particularly valuable feature is the ability to block a computer by its MAC address. This precludes an infected machine form being connected anywhere on the network once it has been identified as having or causing a problem. The user is notified of the situation and given instructions to resolve the issue.

Mail Frontier Gateway: Mail Frontier Gateway Server is a recent commercial addition to our perimeter defense. This solution is a collaborative effort between Mail Frontier and PGP Corporation. More information about this effort may be found at http://www.mailfrontier.com/press/press_pgp.html.

The package filters spam and possible phishing before it arrives on our mail servers to preserve system integrity by stopping unwanted junk from inundating our mail servers and client workstations with unwanted mail. It is relatively simple to install and set up. In the short time we have had this product deployed we have been pleased with the reduction of Spam and the ease in which fine-tuning can be accomplished.

A particularly strong point is the fact that the end user is notified when potentially dangerous mail is blocked and the user has the option to accept or reject the mail. This reduces the administrator's involvement and acts as a reminder to the ordinary user that there are still people trying to exploit vulnerabilities in our systems.

Recent initiatives by ISP's are encouraging. Intercepting and disposal of obvious trash at the ISP's servers will greatly improve the usefulness of the Internet for personal and business endeavors, while discouraging many hacker "wanna be's" by increasing the difficulty level of intrusion into the system. This is a great "first step" in providing a secure network but maintaining several levels of defense and employing many tools in different network layers is still required and justified.

Summary and Conclusion: The effort of the past several years is finally paying huge dividends in our systems security and integrity. The end user is rarely bothered with virus infections and when one does arrive, it is quickly dispatched.

The cost of maintaining the network and computer systems in a proactive manner is far less than reacting to an incident after systems are significantly compromised. Time and resources are better utilized in preventing widespread virus infections and unauthorized access to sensitive business information. Securing the system with an array of protective devices and software tools gives one the freedom to take a more deliberate approach to managing the system than having outside influences force you into a hectic crisis management fray. A well planned management system allows user systems to be maintained in an unobtrusive manner by patching when the system is idle and network scans to be done in small increments to keep traffic to a manageable level. Infected systems and systems in need of security patches are removed from the production network and brought into compliance with our policy expeditiously. User inconvenience is kept to an acceptable minimum and our data is better protected.

As part of our ongoing program of network and systems development, we evaluate new releases of currently deployed tools for planned upgrade and patching. We are also evaluating new tools for enhanced capabilities and better labor efficiency. These elements of the ongoing network defense initiative work to provide the best levels of preparedness for future threats and against a reemergence of complacency.

The initial investment in time and personnel resources is high to get a system into a secure and reliable configuration but the alternative is no system at all. Aggressive pursuit of a secure and user friendly system has to be supported by everyone in the organization in order to work.

It can't be overemphasized that network and computer security in any organization must be the result of teamwork by the technical staff, client cooperation, and the adoption of a dynamic policy that is supported and vigorously enforced.

References

1. Russel, Deborah, Gangemi Sr., GT Computer Security Basics.
   Sebastapol; O'Reilly and Associates, 1991

2. Garfinkel, Simson, Spafford, Gene, Practical UNIX & Internet Security.
   Sebastapol, O'Reilly and Associates, 1996

3. Burk, Robin, Horvath, David, UNIX UNLEASHED, System Administrator's Edition.
   Indianapolis, Sams Publishing, 1997

4. Russel, Charlie, Crawford, Sharon, Windows 2000 Server Administrator's Companion. Washington, Microsoft Press, 2000

5. Holbrook, P., Reynold, J., RFC 1244, Site Security Handbook, 1991
   http://www.faqs.org/rfcs/rfc1244.html

6. Pethia, R, Crocker, S, Fraser, B., RFC 1281, Guidelines for the Secure Operation of the Internet, 1991 http://www.faqs.org/rfcs/rfc1281.html

7. Mell, Peter, Tracy, Miles C. Procedures for Handling Security Patches. 2002
   http://csrc.nist.gov/publications/nistpubs/800-40/sp800-40.pdf