Global Information Assurance Certification Paper

Stronghold Hardening: Simple Practices for Securing the Core.
Allen Balasa
GSEC Assignment v1.4b
August, 2002

Abstract.

The existence of checkpoints, perimeters, and secured tunnels within a private network coordinates the groundwork for deterring unauthorized activities stemming from the Internet. The scope of this research will be to creating best core infrastructure practices for locking down the mounting discoveries of exploits and vulnerabilities and concluding with a discussion on security posturing.

Introduction.

The evolution of the Internet has grown in magnitude since its inception in the late 1980's. Expeditious responses of information riding on standardize protocols across great distances have dictated our behavior of conducting global commerce for centuries to come. However, as historical data shows, even the electronic industry breeds the criminal element of the smart, savvy, or inquisitive crowd of underground operatives whose access to the Internet fuels their desires for personal gain. Their intentions may stem from disrupting access or inhibiting services for legitimate purposes or to inflict harm to informational resources. They're commonly labeled as hackers, cyber-attackers, script kiddies, session hijackers, and crackers. Only by creating a hardened security barrier around the protected network is the solution for protecting critical resources from these threats.

Seven Hardening Practices.

First identify what resources present a high risk factor that, if compromised or destroyed, would "break the bank." Is it a single database? Are there folders containing sensitive company data? Is it a server or a server farm that requires 24x7 Internet access? Are there desktops or laptops where critical information is stored on a local drive? By identifying risk factors for the following areas, you'll be able to blueprint a strategic plan to effectively respond to security breaches: [1]

- Local account policies
- Local policies and event logging
- Restricted groups
- Registry security
- File System security
- System services security

[1] Microsoft TechNet, Security Entities Building Block Architecture, p. 4.

1). Hardening the core begins with the file servers. A minimal secured platform for all Microsoft file servers is having a Windows 2000 operating system environment and NTFS as the preferred file system structure. Verify that all production file servers contain the latest security patches, service packs, and hot fixes. Two excellent freeware tools can determine this task, HFNetChkLT.exe from Shavlik Technologies (http://www.shavlik.com/security) and HFNeTChk.exe from (http://www.microsoft.com/downloads/release.asp?releaseid=31154.) Both Shavlik and Microsoft worked in collaboration developing this freeware tool, though Shavlik's version comes with an added convenience to download the latest patches to your servers. Another freeware tool called HFCheck is specifically designed for checking security patches on Microsoft IIS 5.0 web servers (http://www.microsoft.com/downloads/release.asp?releaseid=24168.) Historically, installing patches, service packs or hot fixes always conjures up logistical uncertainties when installed within a production environment. Thus, attentive care necessitates this practice first be installed on non-production equipment to discover any potential disruptions in the network's operating behavior. IIS v5.0 servers are categorized apart from regular file and print servers for they require more assertive attention due to their separate access control list (ACL) settings. For example, the 'Everyone' group contain write and execute privileges by default, giving opportunists an open invitation to browse and navigate the directories and more importantly, the FTP and SMTP directories. A guideline of ACL permissions below is an idea of how you would associate limited permissions to specific file types: [2]

File Type	Access Control Lists
CGI (exe, dll, cmd, pl)	Everyone (execute) Administrators (full control) System (full Control)
Script files (asp)	Everyone (execute) Administrators (full control) System (full control)
Include files (inc, shtm, shtml)	Everyone (execute) Administrators (full control) System (full control)
Static content (txt, gif, jpg, html)	Everyone (read-only) Administrators (full control) System (full control)

2). Another aspect of hardening is sealing off a swell of un-needed services and ports that are inherently open when windows is installed. The only reason for their existence is not to impose any restrictions with all after market applications that are certified to operate under a Microsoft environment.

[2] Microsoft TechNet, Secure Internet Information Services 5 Checklist, p. 4.

3). Validate the operating system environment by verifying which ports and services are essentially required and research third party documentation ensuring the same for proper application functionality. Double verify once again and disable or uninstall those that are non-essential. Some key advise in regards SQL hardening is taken from a checklist compiled by Luis Medina, author of "The Weakest Link Series", a book on network security issues. He suggests:

- Implement security between the front-end servers and the database server and restrict access to those connections that are required.
- Block all TCP & UDP ports and allow only the authorized SQL port.
- Disable unnecessary SQL network libraries, components, and agents.
- Apply IP filtering on the O/S level and only accept the authorized SQL port.
- Validate server role is SQL only do not run IIS on it.

4). Network account passwords are paramount for validating user authentication and authorization to internal resources and they should be managed in strict accordance to the network security policy. The stronger the guidelines for creating passwords, the less of a risk of them becoming compromised. More important key advise for creating a sound password policy are:

- They must contain at least 8 characters.
- No blank passwords are allowed.
- Never loan your passwords out and change it immediately if you did.
- They must have a time limitation for usage. Limited to 30 to 90 days usage.
- You should never write passwords or send them out via e-mail.
- After 3 failed attempts, the account should be locked out for at least 30 minutes or until a system administrator unlocks it.

Other contributing techniques would be to include a mixture of upper/ lower case letters and numeric characters. Don't choose words that are easily discovered within a dictionary and can be susceptible to a dictionary attack used by a password cracker like L0phtCrack (http://www.atstake.com/research/lc)

5). A corporate firewall is a mandatory piece of equipment for segmenting the private network from the Internet. Its role is crucial for establishing your front line defensive border. A firewall can be one of three categories:

- A router configured with access control lists (ACL).
- A file server running a firewall application containing rules within a rule base.
- An appliance that is a self-contained unit, embracing the best of both worlds by integrating leading firewall software with a suite of routing protocols.

6). For router hardening, make some basic configuration adjustments before getting into access control lists. Suffice to say that Cisco routers comprise the backbone of the Internet; therefore adjustments will be specific to their IOS

software. Cisco routers are delivered factory configured with default passwords, you should change it and supply an "enable secret" password for attaining privilege access. Whereas Cisco's "enable secret" encryption algorithm uses a Type 5 MD5 hash, making it difficult to decrypt, their "enable password" encryption algorithm uses a weak Type 7 hash that can be decrypted by any available Cisco password cracker.

Next, disable specific TCP and UDP services that contain inherent vulnerabilities that are susceptible to documented exploits. Cisco refers to these as small services (echo, chargen, and discard) and potentially harmful services like source routing, finger, bootp, and domain lookup. There are documented tables of commands and descriptions of these services and more in their book, "Managing Cisco Network Security by Michael Wenstrom." The information is found under, "Controlling TCP/IP Services" on page 230. For additional references go to (http://www.cisco.com/warp/public/707/21.html,) Improving Security on Cisco Routers.

Remote router management is another area of concern. Cisco's IOS is capable of allowing remote configuration via HTTP protocol. They caution, "The authentication protocol used for HTTP is equivalent to sending a clear text password across the network, and, unfortunately, there is no effective provision in HTTP for challenge-based or one time passwords. This makes HTTP a relatively risky choice for use across the public Internet." With this in mind, disable the HTTP authentication service on the router. There are more secure options for remotely managing a router, for instance, using SNMP v3. It's a better secured version than its predecessors of v1 and v2 because it supports HMAC (Key Hashing for Message, RFC2104) authentication. A secondary option is using the triple 'A' model, a configurable mechanism on Cisco routers with the aid of a triple 'A' server. Triple 'A' (Authentication, Authorization, and Accounting) authenticates with a challenge requiring a user response for validation then authorizing the user with the level of access and permissions to network resources, and accounting for recording and logging transactions that have taken place. Authentication is performed through RADIUS, TACACS+, or Kerberos standards, depending on the features the router can support. A third option is limiting router access to the router's internal interface. An example would be denying a telnet session or disabling port 23 on both external and internal interface from the Internet and allow remote access on the internal interface through a VPN tunnel or through a dial-up session. Apply an extended ACL on the interface that would permit access from hosts that are using the private address space. An ACL (Access Control List) is a list that controls the flow of traffic based on criteria for services, ports, and IP addresses on the interface.

A mandatory security practice is to deny the private address space inbound to the external interface of the router. RFC 1918 specifications define the standard for non-routable addresses that private enterprises utilize due to the finite amount of available IP addresses. The IANA (Internet Assigned Numbers Authority) is an entity that reserves IP address blocks as private address space, the most popular addresses blocks being:

- 10.0.0.0/8
- 127.0.0.0/8
- 172.16.0.0/16
- 192.168.0.0/16
- 224.0.0.0/8

Hackers have the ability to launch spoof attacks by sourcing private address spaces as inbound traffic, undermining the firewall's inspection process by making it believe it's valid internal traffic. Another thing to bear in mind is protecting internal TCP servers from denial-of-service (DdoS) attacks. A SYN flood is a type of a DdoS attack that can be prevented by enabling the TCP Intercept feature on a Cisco router. Used in conjunction with an extended access list, it intercepts client SYN requests and will attempt to complete the "three-way handshake" on behave of the TCP server. If the handshake is established, the router will pass the connection through, otherwise it will be dropped.

7). An excellent and popular application-based firewall is Check Point FW-1 from eAladdin technologies (http://www.checkpoint.com.) The product integrates the inspection engine with the OS kernel and it uses proprietary stateful inspection technology, combining packet filtering and application layer gateway inspection. Initial rule bases should have two foundation rules. The stealth rule, which drops any traffic destined specifically for the firewall, and the implicit deny rule (also known as the "clean up" rule), which drops any traffic not explicitly defined "allowed" traffic. The rule base is a user-friendly GUI interface where you can configure rules to permit explicit IP services, TCP/UDP ports, and user authentication. Checkpoint reigns supreme as another front line network security device but it falls short of being invincible due to its incapability to filter traffic based on the content or the context of data tunneling through it. This is where content filtering or a good anti virus scanner can contribute to layering your defense.

Viruses, Vandals, and Exploits.

With e-mail clients being HTML enabled, your Internet browser and e-mail server are the quintessential gateways for virus, worms, and Trojan attacks. Vandal attacks and exploits can penetrate the network using HTML, scripting languages, ActiveX, Java, or by browser add-ons. A anti virus scanner should be installed on all host based, server based, and Internet border resources. There should also be an automated process to globally keep all virus signature files up-to-date, ensuring they can scan for the latest virus outbreaks. In addition to signature scanning, enable heuristic scanning in case the latest signature files are not at hand, disable booting capability from the A: drive, run the scanner's option to scan all files instead of programs, restrict executable attachments (.exe, .com, .bat) from entering the protected network, centralize scanning logs for reporting on all virus activity, and implement a notification plan on virus activity.

Occasionally you should perform quality assurance tests to test the reliability on all virus scanners. There is a tool called the EICAR anti virus test file (http://www.eicar.org) that will validate a scanner's ability to detect a test scan string from the file. Functional scanners will be able to identify the test string. For HTML enabled content e-mails, Microsoft offers an e-mail security patch for Outlook 98 and 2000 that will confine and control the spread of malicious code but due to its logistical limitations, a better solution is to go with installing a good content management application such as Finjan's SurfinShield (http://www.finjan.com/products/surfinshield.cfm). For now, disable scripting and HTML content, this will keep non-text email features to a minimum. Also, delete all unexpected or suspicious e-mails that have links to the Internet and ensure all client software is up-to-date. Install the latest software, patches, or hot fixes for they contain patches for locking down the latest security vulnerabilities. If you happen to experience the misfortune of a virus outbreak that penetrated the protected network, acquire Microsoft's Exchange Server Mailbox Merge utility (EXMERGE). It's a handy tool for deleting mass amounts of infected e-mails from the public and private information stores. You can download it from their website or from the BackOffice resource kit, second edition for Exchange 5.5 or from the Exchange 2000 Server CD for Exchange 2000. For hardening advise related to the Internet Browser, configure the browser's default security setting not to allow un-trusted content to execute. Secondly, remove or disable unnecessary plug-ins, Java applets, and ActiveX objects. All these settings can be found within the browser itself. And lastly, configure that all file downloads require a user confirmation by prompting an acknowledgment of the action.

Security Posturing.

Attacks come in many different forms ranging from spoofing to crashing systems. They can involve techniques like hidden field manipulations, cookie poisoning, exploiting application debug options left within the code by mistake, buffer overflow attacks, stealth commanding by gleaning a legitimate website, system misconfigurations by 3rd party vendors, exploiting known vulnerabilities, parameter tampering within a URL's source code, cross site scripting where an attacker is able to redirect page locations, and forceful browsing where an attacker can access website visitor information by parsing the buffer areas without directly accessing a database. In order to maintain a proactive defensive posture, a ritual of daily monitoring and auditing of the protected network should be practiced religiously. Attune your senses to the normality of traffic behavior so you're able to distinguish abnormal traffic behavior when it happens. Those conditions may indicate a break-in attempt, a Ddos attack, or misconfigurations somewhere in the core.

Network Monitoring.

Network Based Intrusion Detection Systems (NIDS) are strategically placed passive monitoring probes that provide a real time analysis of traffic traversing

the network. NIDS operate by matching attack signature patterns provided in a database. When it suspects an attack, it logs an alert to a management PC. A prior risk analysis study of your network resources should be performed because placement of the NIDS is of critical importance. Cisco System's best practice white paper on network security suggests categorizing risk analysis levels at (3) stages:

- Low Risk are systems or data that will not disrupt the business or impact any financial transactions. This type of risk should be monitored on a weekly basis.

- Medium Risk are systems or data that will cause moderate disruption of the business or any financial transactions and requires a moderate effort to repair. This type of risk should be monitored on a daily basis.

- High Risk are systems or data that will extremely impact the business or any financial transactions and requires a significant effort to repair. This type of risk should be monitored on an hourly or earlier basis.

Network IDS is not the catchall solution though some may think, they do have their limitations. First, they can only detect intrusion activity that passes in front of them and capture attacks if the attack signature is contained in the signature database. Second, they cannot perform heuristic scans to recognize brand new attacks. And third, NIDS is incapable of detecting payload contents if the traffic is encrypted via SSL or IPSec protocols.

Logging and Auditing.

Another important factor would be the logging of events and system auditing of the network's daily functions. You should selectively choose system events that are in accordance with the company's security policy for tracking transactions and violations on the network. It is recommended to have all types of security logs reside on a separate partition or on a dedicated secured server because these logs can grow to epic proportions on a daily basis. Examining the logs for security breaches can be a painstaking effort, however, there is one program I discovered called Logsurfer (ftp://ftp.cert.dfn.de/pub/tools/audit/logsurfer.) Its ability to parse the logs in real time mode and generate alerts by configuring selective expressions within the configuration file simplifies this exercise. Logs are excellent security instruments by nature of the detailed information they contain but they're only as effective if system administrators examine them. Be particularly mindful in practicing diligence for daily log monitoring. Justifiably, there is a hack technique by which a hacker can intentionally flood the log with false information, consuming free space on the disk as the log grows towards capacity. Once the logs are full, logging functionality terminates, resulting in concealment of a hacker's activities on the network.

Backups.

Backups are critically important for they provide redundancy and a safety net in emergency situations that require falling back to the last good known state of a resource. There are different methodologies of backups with inherent dilemmas of either having faster backups, slower restores or faster restores, slower backups. Security policies should dictate requirements and methods as they relate to system backups. They should identify:

- The preferred backup method – Grandfather, Father, Son or "Tower of Hanoi"
- Backup media retention and rotation schedules.
- Authorized media to use for backups.
- Preference of backup schema - Full, Incremental, or Differential.
- Storage management – On-site or Off-site.

Good security practice should require having a 'golden copy' image of the system's hard drive. It's an image copy that's made before the server was connected to the network.

Conclusion.

Practice best efforts to maintain a stern security posture by researching up-to-date security headlines and alerts from industry leaders like Microsoft, Cisco, McAfee, Symantec, and Trend Micro. Subscribe to well known mailing lists such as Bugtraq and NTBugtraq to receive the latest discovery on exploits and vulnerabilities. Revise and amend procedures in the security policy to adapt with environmental changes and execute policy enforcement to the target community. Popular security websites as (www.securityfocus.com), (www.incidents.org), (www.securiteam.com), and (www.ntsecurity.net) disseminate beneficial information for the industry. Their publications discover the latest security and exploit trends that will compliment any company's security portfolio.

There are current predictions that new breeds of worms are morphing with viruses; virus infections are infiltrating through HTTP port 80; and packet sniffers like TCPdump or SNORT now have trojanized versions. There are mounting reasons to justify applying continuous security core hardening. For starters, I've read excerpts from underground documents on the Internet and found that the basic requirements for one to engage in hacking are one installed operating system, two network security tools, and access to one knowledge base. With this awareness and a bit of intrepidity, he or she is well underway into the realm of practicing a newly discovered skill. You can venture into the hacker's underground (http://www.hackers.com/html/hyperlinks.html) and visit the thirty-seven hacker links where hackers frequent or (http://www.hackpalace.com/usa) for archival papers on cracking, hacking, phreaking, etc. But before hurling yourself into that void, tactically install a good anti virus scanner containing the latest virus signatures along with a personal firewall configured on paranoid setting. Just in case!

Resources:

1. Microsoft TechNet, “Secure Internet Information Services 5 Checklist.” URL: http://www.microsoft.com/technet/prodtechnol/iis/tips/iis5chk.asp?frame=true

2. Microsoft TechNet, “From Blueprint to Fortress: A Guide to Securing IIS 5.0.” URL:http://www.Microsoft.com/serviceproviders/security/iis_security_P73766.asp

3. Microsoft TechNet, “Security Considerations for End Systems.” URL: http://www.microsoft.com/technet/security/bestprac/bpent/sec2/sconsid.asp?frame=true.

4. Microsoft TechNet, “Security Entities Building Block Architecture.” URL: http://www.microsoft.com/technet/security/bestprac/bpent/sec2/secentbb.asp?frame=true.

5. Cisco Tech Note, “Improving Security on Cisco Routers.” URL: http://www.cisco.com/warp/public/707/21.html

6. Lusignan, Russell, Steudler, Oliver, Allison, Jacques, “Managing Cisco Network Security”, Syngress Publishing, Inc., 2000

7. Norberg, Stefan, “Securing Windows NT/2000 Servers for the Internet”, O’Reilly & Associates, Inc, January 2001.

8. Grimes, Roger A., “Malicious Mobile Code, Virus Protection for Windows”, O’Reilly & Associates, Inc, August 2001.