Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Hardening Bastion Hosts

This paper discusses some of the benefits to using hardened bastion hosts. These hosts allow you to have complete control over how each service interacts with the network. They also allow you to monitor activity to prevent unauthorized access. By adding them to your Defense in Depth strategy, you can slow an attackers progress and protect the confidentiality, integrity and availability of your private network.

Copyright SANS Institute
Author Retains Full Rights

AD

Todd Jenkins – GSEC Version 1.2e – Hardening Bastion Hosts

Introduction

You've just been asked by your manager to install a hardened bastion host. The company needs to strengthen the security between the Internet and the company's internal network. You unsuspectingly accept the challenge and tell your manager you need to do some research. How hard could it be?

Management often likes to use technical jargon even when they might not know what it means. Your manager and a peer from another company were discussing how the other company had just installed a hardened bastion host. They had gotten a dedicated circuit to the Internet installed just a few weeks before your company did. The peer says how well it's working for them when your manager suddenly decided your company needs one since it's working so well at the other company. That's where you come in.

What is a bastion host?

Now you're probably asking yourself, "What is a bastion?" I'd never heard of a "hardened bastion host" before I researched this paper. In fact, several of my peers hadn't either. You probably know what it is but didn't know it by that terminology.

> "Bastions are the highly fortified parts of a medieval castle; points that overlook critical areas of defense, usually having stronger walls, room for extra troops, and the occasional useful tub of boiling hot oil for discouraging attackers. A bastion host is a system identified by the firewall administrator as a critical strong point in the network's security. Generally, bastion hosts will have some degree of extra attention paid to their security, may undergo regular audits, and may have modified software." (Steves, Kevin)

Bastion hosts are typically designed with one function in mind: to allow information to flow securely between the Internet and the internal network without directly exchanging packets. It can be a single system or there can be multiple systems in the firewall. It is wise to remember the more systems the firewall is made with, the greater the risk of compromise. You can have a bastion host in the firewall configuration, but without hardening it, the probability of a successful attack increases. The process called "hardening" will allow these hosts to resist attacks from external sources thus protecting the internal network.

There are numerous considerations when it comes to bastion hosts: roles, design, documentation, installation, and verification. I will briefly describe each of these in general detail since it is impossible to cover every facet of each section.

Roles

The most common roles of bastion hosts to be used as: router, DNS, FTP, SMTP, News, and/or Web servers. A bastion host can be as simple as a router or as complex as a SMTP and DNS server. Bastion hosts are typically a gateway, on the perimeter network, between the Internet and the internal network. Whatever the use, its main function is to protect the network behind it. The more roles the host has to play, the greater the likelihood of overlooking a security hole.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

"Much of what the bastion host does is act as a proxy server for various services, either by running specialized proxy server software for particular protocols (such as HTTP or FTP), or by running standard servers for self-proxying protocols (such as SMTP)." (Zwicky, Elizabeth D., Simon Cooper and Brent D. Chapman. Page 131.)

What role will this host play in the overall network? Is there a genuine need for this function or is it merely pressure from users? Pressure from the users can result in a way around security because of the inconvenience the security policy causes.

Now you need to identify what the host will be used for and verify whether or not it meets your network security policy specifications.

"A network security policy identifies the resources that need protection and the threats against them. It then defines how they can be used and who can use them, and stipulates the actions to be taken when the policies are violated." (Firewalls and Virtual Private Networks. Page 2.)

If you don't have a network security policy, you can find a guide to writing Security Policy and other documentation at: http://www.sans.org/infosecFAQ/policy/shelfware.htm. You can also find a Security Policy checklist at: http://queeg.com/~brion/security/secpolicy.html.

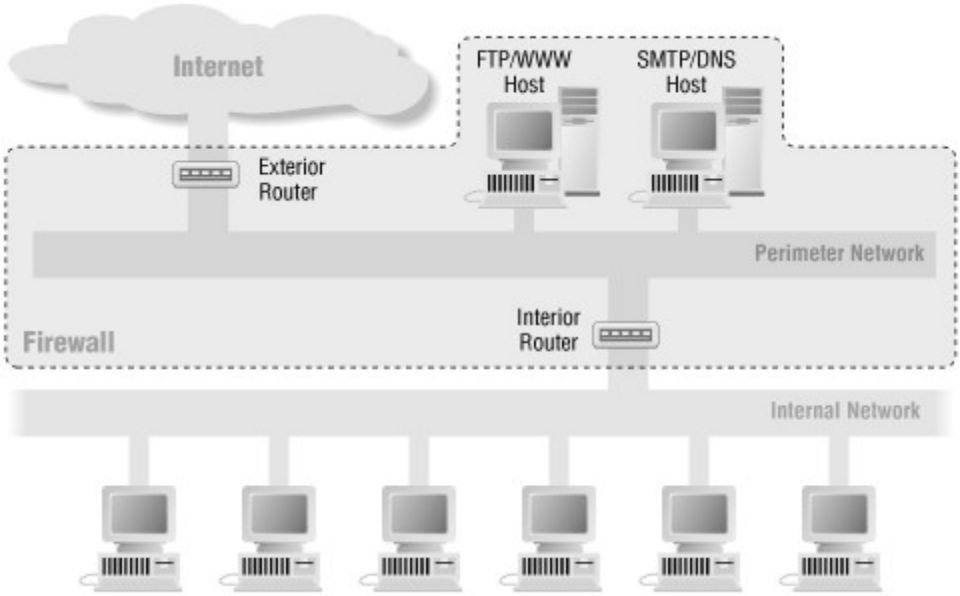
Design

You must ultimately decide which services need to be on a bastion host. Ideally you would have one service per host but this does not usually work since the cost alone is typically prohibitive. It is easier to secure a single service on a single host. If your company can afford the costs of multiple bastion hosts, you must decide if you are willing to maintain multiple points of attack.

"Only the services that the network administrator considers essential are installed on the bastion host. The reasoning is that if a service is not installed, it can't be attacked." (Semeria, Chuck. Internet Firewalls and Security.)

The Department of Defense defines Defense in Depth as "The sitting on mutually supporting defense positions designed to absorb and progressively weaken attack, prevent initial observations of the whole position by the enemy, and to allow the commander to maneuver his reserve." (U.S. Military with Rod Powers.) A way to use the Department of Defense's Defense in Depth strategy is to design a Screened Subnet Architecture. In a Screened Subnet Architecture, the bastion host sits between an exterior router and an interior router.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.



Architecture using two bastion hosts (Zwicky, Elizabeth D., Simon Cooper and Brent D. Chapman. Page 138.)

This design provides an additional layer of security between the Internet and the internal network. It prevents attackers from seeing the whole network from their initial vantage point. Even if they break through the exterior router, they still only have a limited view of the perimeter network. An attacker must penetrate the exterior router, a bastion host, and the interior router to gain access to the internal network. By the time an attacker gets through all three layers, you should been alerted and will have taken a defensive position.

Documentation

It is important to thoroughly document your work. It is equally important to maintain and update the documentation as changes occur. How many times have you heard about a system crash and the Systems Administrator found the backup was bad or not working? This not only helps you to rebuild should your system fail, but also allows you to examine the steps taken to ensure nothing is missed.

You should document every step taken to install and test a bastion host. This allows you and/or Systems Administrators to troubleshoot problems more expeditiously. This will also allow you and/or a new Systems Administrator to recreate the build on a new host in the event of a disaster. By documenting your testing techniques, you and/or a new Systems Administrator will easily see when you need to test using new techniques.

Hardware and Software

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

When choosing hardware and an operating system, it is critical to use a combination that you are familiar with. You don't want to put your company at risk while learning to secure an unfamiliar server. This often leads to security holes and unknown vulnerabilities.

A bastion host generally doesn't have to be a fast machine since it is limited by its connection to the Internet. In fact a slower machine is often a deterrent to a would-be attacker since a slower machine will not have the resources waiting idle like a fast machine. The machine should have enough hardware to complete the installation and for maintenance. Once the machine is built, Systems Administrators will often remove items such as the CD-ROM and floppy drives for additional security.

Physical security is often an underestimated step in the security process. As you can see from Jay Beale's article, "… any attacker with physical access to a computer, a little ingenuity, and sufficient time can compromise the system." The machine(s) should be placed in a restricted access area with proper cooling, ventilation and a backup power system.

Be sure to allow for a tape drive for making backups. A detachable CDRW or removable hard drive can be used for making system images using utilities such as Symantec's Ghost.

Installation

Bastion hosts must be installed and maintained with two questions in mind:

- Is it protected from attackers?
- When it is compromised, will the integrity of the internal network still be protected?

You must assume the system will be compromised in order to take all measures to reduce that risk. Ask yourself these questions with each step you take to ensure you haven't left a hole. An installation checklist is invaluable.

"The basic hardening process is as follows:

1. Secure the machine.
2. Disable all non-required services.
3. Install or modify the services you want to provide.
4. Reconfigure the machine from a configuration suitable for development into its final running state.
5. Run a security audit to establish a baseline.
6. Connect the machine to the network it will be used on."
   (Zwicky, Elizabeth D., Simon Cooper and Brent D. Chapman. Page 131.)

You will need to install a secure version of the Operating System. Installing the base Operating System and then installing Patches or Service Packs generally accomplishes this. Be sure to check the Operating System developer's website for their list of updates. You should also check reliable sources such as SANS and CERT for current system bugs and vulnerabilities.

Here are a few reliable security advisories:

- http://www.cert.org/

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- http://www.ciac.org/
- http://www.sans.org/

Disable or remove any service that isn't specifically needed for the host to operate properly. Don't forget about the dependency services. You will need to verify if any dependency services, of services you've turned off, are needed for the host's functionality. Turn off services one at a time and test for functionality. If the system continues to function properly, document the change and move on to the next service. If the system fails, restore the service and evaluate its impact on security. You should pay special attention to services that cannot be disabled.

User accounts should not exist on bastion hosts because users should not be accessing the hosts from the console. The chances are greater for an accidental or intentional security breach with more than the essential accounts on the host. Unused, harmless looking, accounts that were installed with the Operating System are inviting attackers to exploit them. You should remove all unnecessary accounts.

Routing and trusts are dangerous to the overall security scheme if not implemented properly. Make sure routing is not enabled unless of course you are using a bastion host as a router. Routing weakens the purpose of the bastion host's security posture. The bastion host should also have limited trust relationships with other systems. If the host can route to a system or connect to a trusted system on the internal network, then you have one less layer of defense.

Verification

Once the bastion host is installed, you need to establish a baseline. There are several methods to establish a baseline. Checking processor utilization to see current system loads and taking a snapshot of the system logs will give you an understanding of how the system normally runs. There are also software packages available to automate this process.

The host needs to be tested before being placed on the live network. As a final evaluation, you need to go over the documentation again and make sure none of the steps were left out.

If you have to modify or install services that haven't been tested in your environment, test them after installation to verify whether or not they work with your network security policy.

If possible, it is a good idea to run a network weakness scanner such as NESSUS, NMAP, SATAN. These tools will assist you in detecting weaknesses in your host. You can take these results and fortify your host to prevent real attacks. Note that this should ONLY be done on a separate test network. Port scanning and other various system probing has been known to crash entire networks as well as entire careers!

System logs are invaluable tools for detecting and terminating attacks. These logs should also be preserved so an attacker who gains access cannot alter the integrity of the logs. You must decide what you want to log and how frequently. Logs filled with excessive information can slow the process of tracking an attacker. Too little logged information can result in missed intrusion detection. You should only log information that is necessary to monitor the system on a regular basis.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Setup a schedule for examining the logs periodically to verify the integrity of the host. You can find an example of an Intruder Detection Checklist at:
http://www.cert.org/tech_tips/intruder_detection_checklist.html

Once the system has been verified, reconfigure the host so it can be placed into production.

Summary
There are many benefits to using hardened bastion hosts. These hosts allow you to have complete control over how each service interacts with the network. They also allow you to monitor activity to prevent unauthorized access. By adding them to your Defense in Depth strategy, you can slow an attackers progress and protect the confidentiality, integrity and availability of your private network.

You should now be able to go back to your manager feeling confident that you can accomplish the challenge presented to you earlier. I've touched on the topics above generally and you should investigate further before configuring a bastion host in your environment. This should be a good starting point and I've listed references that can take you on your own journey.

© SANS Institute 2001, Author retains full rights.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

References:

Steves, Kevin. "Building a Bastion Host Using HP-UX 11". May 26, 2001. URL: http://people.hp.se/stevesk/bastion11.html. (June 24, 2001).

Zwicky, Elizabeth D., Simon Cooper, and Brent D. Chapman. Building Internet Firewalls. Sebastopol, CA: O'Reilly & Associates, Inc., June 2000.

"Firewalls and Virtual Private Networks". URL: http://www.wiley.com/legacy/compbooks/press/0471348201_09.pdf. (June 24, 2001).

Semeria, Chuck. "Internet Firewalls and Security – A Technology Overview". URL: http://www.linuxsecurity.com/resource_files/firewalls/nsc/500619.html#Bastion%20Host. (June 26, 2001).

"U.S. Military with Rod Powers". URL: http://usmilitary.about.com/careers/usmilitary/library/glossary/d/bldef01834.htm. (June 24, 2001).

Beale, Jay. "Anyone with a Screwdriver Can Break In!". August 28, 2000. URL: http://securityportal.com/cover/coverstory20000828.html. (July 1, 2001).

"Intruder Detection Checklist". July 20, 1999. URL: http://www.cert.org/tech_tips/intruder_detection_checklist.html. (July 1, 2001).

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 24th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced