The Design, Implementation, and Review of a Bastion Host

Alex Hurd and Eric Richter

April 20, 2014

Introduction

COSI hosts many services in the server room, many of which that are not exposed to the whole internet. Machines that are not, instead require that connections come from a particular location. The current attempt at a solution is Isengard, a virtual machine that is intended to be a security harded machine that would act as a gateway to the rest of the world. However, Isengard has become rather out of date and is likely full of unpatched security vulnerabilities as it is currently unmaintained. The documentation is also rather sparse, thus we are unsure of what exactly it provides.

We rebuilt Isengard by taking the following steps, each of which will be embellished further in this document.

1. Investigated the current system
2. Identified new requirements, and designed a new system
3. Built the new system in accordance with these needs
4. Tested the replacement
5. Adapted to the results

1 Investigation

Isengard currently has a page (`http://docs.cslabs.clarkson.edu/wiki/Isengard_Setup_Process`) for the initial setup process, however the page has not been updated since its initial creation. The original Isengard was a CentOS 5.3 x86-64 system with a variety of services disabled, elevated levels of logging, and DenyHosts installed. CentOS 5.3 was released 31 March 2009, making Isengard one of the servers with the oldest operating system in COSI. CentOS 5 lost full update support on 8 January 2013 and will lose all maintenance updates on 31 March 2017.

2 Design

After some deliberation we decided to keep the bashtion host as a VM so as to be able to have a redundant system in the future, we do not feel that this poses any additional security concerns nor did we find information to the contrary. The operating system we chose was OpenBSD 5.4 we made this choice as OpenBSD has always had a reputation of valuing securty over everything else this is a quote from their website, "Try to be the #1 most secure operating system." OpenBSD backports all of the patches and makes it easy to upgrade a system to the most current version. As part of our enhanced security we developed a simple password checking utility that looks for a specified level of entropy. An audit of the current network state of the COSI lab lead us to devise a new network plan the new plan involves subdividing the network into three distinct VLANs and creating an isolated internal network for the servers to communicate on.

- 144 VLAN - ITL & COSI Computers plus all open ports in CS Labs

- 145 VLAN - Only CS Lab critical servers
- 146 VLAN - Research and Student Projects

The network switches will also be divided into 4 external segments and 3 internal segments:

- External Switches
  - COSI - Ports in the COSI side of the Lab will connect to this sub-group of switches.
  - ITL - Ports in the ITL side of the Labs will connect to this sub-group of switches.
  - Unisys Rack - Servers in this rack will connect to this switch.
  - IBM Rack - Servers in this rack will to this switch.
- Internal Switches
  - ITL - Internal Ports in the ITL side of the Labs will connect to this switches.
  - Unisys Rack - Servers in this rack will connect to this switch.
  - IBM Rack - Servers in this rack will to this switch.

The internal network will all be connected together but isolated from any outside connections. We will also be adding a network monitoring box (henceforth referred to as the HyperCube), this box will monitor each segment of the external network for suspect activity. The HyperCube will be a stateful firewall and network traffic monitor with the capabilities for deep packet inspection.

3 Implementation

All of the documentation pertaining to the set of the Bastion Host is on the COSI Wiki (`http://docs.cslabs.clarkson.edu/wiki/Bastion_Host`).

4 Testing

We ran wireshark on a computer connected to the network and did not find any source of information leaks.

5 Adaptation

This phase is never over, anytime we make a change to the system we will need to reevaluate the Bastion Host and make changes to any security holes we introduce.