Global Information Assurance Certification Paper

Practical Assignment for

GIAC Firewalls, Perimeter Protection, and Virtual Private Networks

Version 1.6

SANS San Diego, October 14 – October 22, 2001

Weihan Chang

0. Table of Content

Assignment 1 –Security Architecture
1.1 Overview
1.2 Access Requirement
1.3 Security Architecture
1.4 Security Considerations
1.5 GIAC Logical Network Diagram

Assignment 2 – Security Policy
2.2 Border Router
2.3 External Firewall
2.4 Primary Firewall
2.4.1 Gauntlet Configuration Tutorial
2.5 VPN Gateway

Assignment 3 – Audit Your Security Architecture
3.1 Technical Audit Overview
3.2 nmap scans
3.3 System Access and Authentication
3.4 OS and Patche Levels
3.5 System and Software Configurations
3.5.1 System Software
3.5.2 Examine all set-id Files
3.5.3 File Permissions
3.5.4 Network Security Tuning
3.5.5 Trusts
3.6 Review In-House Codes

Assignment 4 – Design Under Fire
4.1 Overview
4.2 Attack Plan
4.3 Compromise Web Server
4.4 DOS Against External Firewall
5.0 References

Assignment 1 – Security Architecture 12.22.2001

1.1 Overview

GIAC is an e-business which deals in the online sales of fortune cookie sayings. The goal is to define a security architecture that enables conduct of business while protecting the informational assets of GIAC. The objective of the security architecture is to identify the risks and to achieve a balance between risks and costs. Without a good security architecture we may err by either being overly protective or on the other extremely, failing to take reasonable precautions.

1.2 Access Requirements

The access needs of GIAC to conduct business consist of 5 user groups:

- Casual Browsers. There is a company web site accessible to all internet community.
  - Services: http, DNS
  - Systems: web, DNS server

- Customers. These are the companies that purchase bulk online fortunes. The customers access a customer web site that provides a web interface to search, view, and order bulk fortunes. A new customer goes through an online registration process to create a customer profile and get a unique username and password to access the customer web site. The customers have the options of downloading the bulk fortunes via the customer web interface or having the bulk fortunes PGP encrypted and placed on an ftp server for retrieval. The ftp option requires the customer to include at least one PGP key in their customer profile. The Customer web site is ssl only.
  - Services: ssl, ftp, DNS
  - Systems: web, DNS, ftp, Fortune Database, Fortune Application Server

- Suppliers. These are the authors of fortune cookie sayings. The suppliers are mostly up and coming authors (read starved) or part-time freelance work-from-home entrepreneurs. In order to facilitate and organize this group of resource, the suppliers access a supplier web site that provides a web interface to a groupware/collaboration application in addition to interface to compose and upload sayings to the fortune cookie saying database. Each supplier is provided a unique username and password to log on to the supplier web site. The Supplier web site is ssl only.
  - Services: ssl, ftp, DNS
  - Systems: web, Groupware/Collaboration, ftp, DNS, Fortune Database,

Fortune Application Server

- Partners. The partners translate and resell fortunes in other markets. The partners access a partner web site which provides a web interface to view, search, and download bulk fortunes. The partner web interface also allows partners to maintain a profile including contact and billing information. There is also an ftp option for the partners to request bulk sayings PGP encrypted and placed on ftp server for retrieval. The ftp option requires the supplier to include at least one PGP key in their partner profile. Each partner is supplied a unique username and password to log on to the partner web site. The Partner web site is ssl only.
  - Services: ssl, ftp, DNS
  - Systems: web, ftp, DNS, Fortune Database, Fortune Application Server

- GIAC Employees. The employees consist of onsite staff and telecommuters. They include managers, IT staff, support-administrative staff, salespeople, and project managers.

  - Onsite employees. Each employee has a desktop and/or laptop system connected to the GIAC internal network. They essentially have complete access to all GIAC internal network. Access to systems are granted by job role and responsibilities. Externally, employees only have web and email access.
  - Telecommuters. Each is provided a DSL or cable modem connection to their home office. A firewall is maintained at each telecommuter office. A laptop is provided for each telecommuter with VPN client. The company laptop is used strictly for company business use. The VPN client is configured to not allow split horizon.

  Each employee is required to sign an agreement indicating that GIAC system resources should only be used for GIAC business related work and that there are no expectations of privacy when using the system resources.
  - Services: http, ssl, smtp, IPSec, NetBIOS, DNS
  - Systems: web, mail, VPN, DNS, Fortune Database, Fortune Application Server, desktop, laptop

1.3 Security Architecture

The Security Architecture is based on VISA's Ten Commandments[1] and some industry best practices to the extend practical.

1. Install and maintain a working network firewall to protect data accessible via the Internet.

[1] CNN.com Aug. 15, 2000

2. Keep security patches up to date.
3. Encrypt stored data accessible from the Internet.
4. Encrypt data sent across networks.
5. Use and regularly update anti-virus software.
6. Restrict access to data by business need to know.
7. Assign Unique ID's to each person with computer access to data.
8. Track access to data by unique ID.
9. Regularly test security systems and processes.
10. Don't use vendor-supplied defaults for system passwords and other security parameters.
11. Develop a backup and recovery plan procedure.
12. Develop a documentation repository for GIAC.
13. Limit physical access to business critical systems.
14. Establish procedure on change management of any security policies and yearly review of security policy and change management procedure.
15. Establish a Perimeter Protection Team responsible for maintaining all network and system security devices and enforcing security policy and incident handling.

1.4 Security Considerations

Assets to protect:

- Hardware: Servers, workstations, laptops, network equipments, printers.
- Software: Operating systems, applications – both in-house developed and off the shelf.
- Data: Fortune cookie sayings, email, system configurations, user information, web contents, system logs, documentations.

Possible threats:

- Unauthorized access to systems.
- Data theft/unauthorized modifications.
- Denial of service.
- System crashes, software errors/loss of use.
- Natural and manmade catastrophic events. (Earthquakes, floods, terrorist activities, civil unrest.)

Risk Analysis

The following definitions are used for the risk analysis. Here we follow the excellent paper by Cisco available at http://www.cisco.com/warp/public/126/secpol.html.

Resource – A system, network, network resource, or data.
User Relationship – User groups accessing a resource. These are identified in 1.1 Access Requirements as Casual Browsers, Customers, Suppliers, Partners, and GIAC Employees.
Data Sensitivity – The data contained in Resource. The categories are:

- Sensitive – information that requires special precautions to assure the integrity of the information, by protecting it from unauthorized modification or deletion.
- Confidential - information that is intended strictly for use within GIAC. Its unauthorized disclosure could seriously and adversely impact GIAC, its stockholders, its partners, and/or its customers.
- Private - information that is personal in nature and intended for use within GIAC. Its unauthorized disclosure could seriously and adversely impact GIAC and/or its employees.
- Public - information that does not clearly fit into any of the above three categories. While its unauthorized disclosure is against policy, it is not expected to impact seriously or adversely GIAC, its employees, partners and/or its customers.

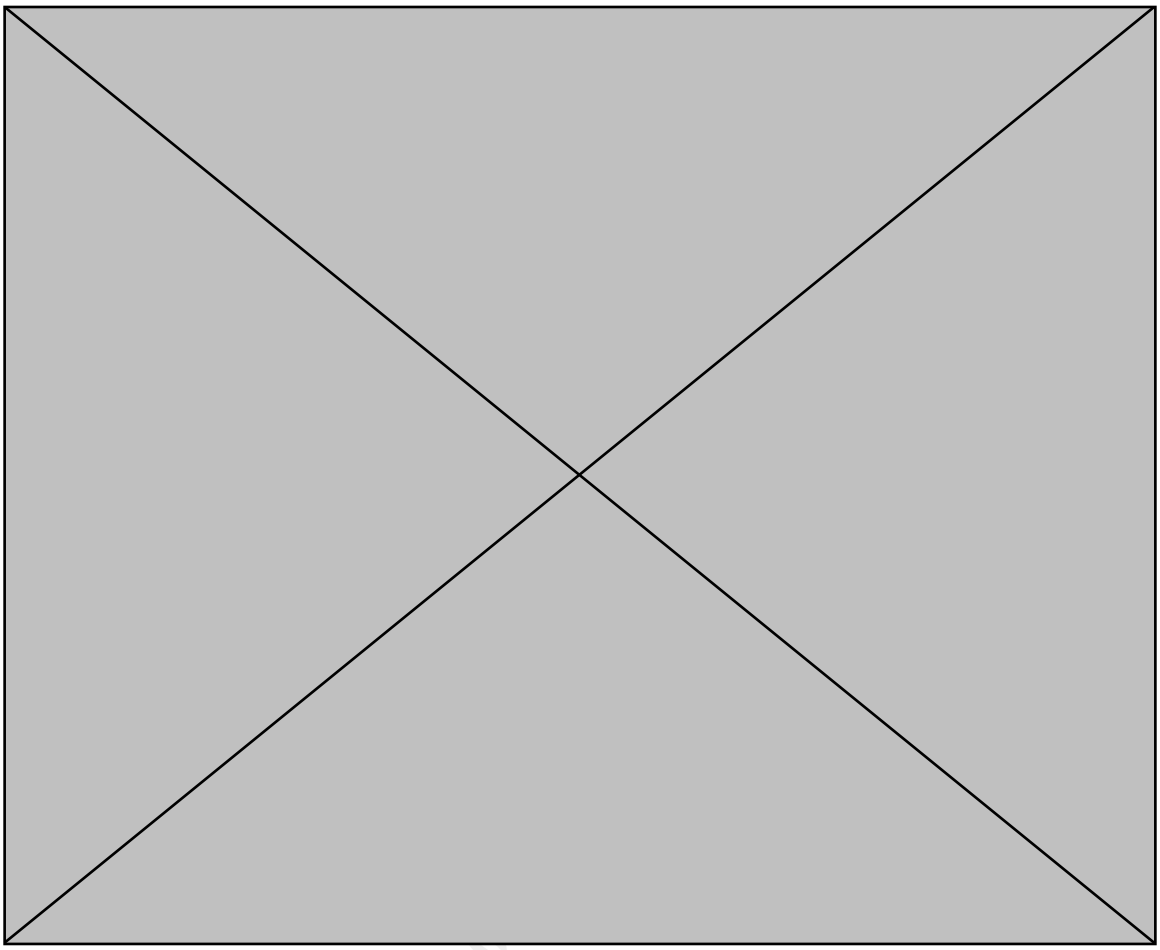
Risk Level –

- Low – if compromised would not disrupt the business or cause legal or financial ramifications. The targeted system or data can be easily restored and does not permit further access of other systems. The targeted system or data can be easily restored and does not permit further access of other systems.
- Medium - if compromised would cause a moderate disruption in the business, minor legal or financial ramifications, or provide further access to other systems. The targeted system or data requires a moderate effort to restore or the restoration process is disruptive to the system.
- High - if compromised (data viewed by unauthorized personnel, data corrupted, or data lost) would cause an extreme disruption in the business, cause major legal or financial ramifications, or threaten the health and safety of a person. The targeted system or data requires significant effort to restore or the restoration process is disruptive to the business or other systems.

Resource	**User Relationship**	**Data Sensitivity**	**Risk Level**

Web Server – Public site	Casual Browsers	Public	Low
Web Server – Customer, Supplier, Partner sites	Customers, Suppliers, Partners	Sensitive	High
ftp	Customers, Suppliers, Partners	Sensitive	Medium
Supplier Groupware/Collaboration	Suppliers	Sensitive, Private	High
Fortune Saying Database	Customers, Suppliers, Partners, Employees	Sensitive	High
VPN	Employees	Sensitive	High
Intranet Web Server	Employees	Confidential	High
Syslogs	Employees	Confidential	Medium
Perimeter Protection Support Server	Employees	Confidential	High
Firewalls	Everybody	Confidential	High
IDSs	Employees	Sensitive	Low
Desktops and Laptops	Employees	Private	Low

1.5 GIAC Logical Network Diagram



GIAC Detailed Component Diagram