Global Information Assurance Certification Paper

Case Study in Information Security
[GIAC GSEC Version 1.4b Option 2]

Survivable Systems Analysis Method

Assessing the Security Architecture of a Regional Non-Profit

Greg Porter

December 2nd, 2003

1. Abstract

The purpose of this paper is to review and outline the steps taken to assess the security architecture of a regional non-profit organization using the survivable systems analysis (SSA) method. This assessment encompassed defining and examining the organization's network infrastructure and identifying:

- Essential, mission-critical services and assets that must survive attack
- Potential vulnerabilities in the system architecture
- Likely attack scenarios based on the system environment and risks
- Architecture improvement strategies to enhance survivability

This paper has been researched and written in order to fulfill the practical component of the SANS (System Administration, Networking, and Security) Institutes GIAC (Global Incident Analysis Center) GSEC (GIAC, Security Essentials Certification).

2. Before Snapshot

I was contacted by the Information System's (IS) Manager of a regional non-profit organization, referred to as Company Z, to analyze their network architecture and overall security posture. Company Z is involved with real estate and new business development in a mid-sized metropolitan area and consists of approximately 105 employees. Their line of work requires personnel to obtain, store, and process sensitive financial documents, such as bank loans and customer's credit history reports, as well as legal documentation, covering for example, property deeds and zoning ordinances. To facilitate these objectives, efficient and effective communication across boundaries is paramount. Company Z must have the ability to exchange information with a diverse array of stakeholders ranging from employees and clients, to banks and law firms, both locally and globally based.

The IS Manager expressed to me that because of the nature of their business they were beginning to rely on electronic communications more and more. He mentioned that features such as e-mail and voice over IP (Internet Protocol) had significantly reduced their shipping, faxing, and phone costs and that overall, management was pleased with efficiencies gained in lower bidding and negotiation processes.

As their reliance on electronic communication increased, Company Z's GroupWise email system quickly became an integral component of their daily business transactions. The IS Manager was concerned that as the company further entrusted their sensitive communications to technology, improvements in efficiency may come at the expense of increased network security risks. Specifically, he expressed a strong interest in preserving system availability and placed a great deal of emphasis on their GroupWise email system. He mentioned that a Denial of Service attack was a legitimate concern and that Company Z

recently granted users Internet access in the absence of any type of acceptable use policy. In addition, he stated that of the few security policies they had managed to develop over the years, most were never effectively implemented much less enforced. This further served to legitimize the IS Manager's concerns over potential threats and vulnerabilities from outside the network and served as good fodder when considering the company's security posture.

The IS Manager asked me to conduct a low cost risk assessment that would assess their overall security posture by identifying gaps in their current network architecture. I chose the Survivable Systems Analysis (SSA) method (formerly the Survivable Network Analysis (SNA)) developed by Carnegie Mellon University's Software Engineering Institute (SEI) as my assessment framework. I utilized the SSA method in the past and knew that it would help me gain a detailed understanding of Company Z's network, while minimizing client costs. In particular, the SSA method would enable me to identify:

- The essential functions of Company Z's system that must survive attacks and failures,
- Likely attack scenarios based on their system environment and risks,
- Potential softspot components within their infrastructure, and
- System architecture changes to enhance survivability.

Company Z's network is comprised of 110 personal computers, 3 servers, 1 router, and 1 firewall to support the needs of 105 employees along with network traffic from clients outside of the organization.

A brief overview of the SSA method follows.

2.1 Overview of the Survivable Systems Analysis Method

Survivability Concepts

The convergence of uncertainty, interdependency, and credible threats often necessitate the need to network from a defensive posture. As organizations become increasingly dependant on their information systems, preserving system survivability and mission critical functionality is a key risk management step. Survivability is the capability of a system to fulfill its mission in a timely manner, even in the presence of attacks or failures[1]. A tenet of survivable systems is that they are able to deliver essential services during an attack and offer rapid recovery as conditions improve. The focal point of my assessment effort will be to utilize the SSA method to aid Company Z in identifying and preserving mission critical assets and services before, during and after an attack or accident.

[1] Ellison, http://www.sei.cmu.edu/publications/documents/00.reports/00tr013.html

The Three R's: Resistance, Recognition, and Recovery

Survivability achieves its objectives of delivering essential services and preserving essential assets via three primary capabilities: *resistance*, *recognition*, and *recovery*.

Resistance focuses on a systems ability to repel attacks and may be enhanced, for instance, by the use of signature-based antivirus software, strict firewall configuration, and unified security policies.

Recognition is the capability to recognize attacks in real-time while also being able to evaluate the extent of damage and level of compromise. Recognition can be improved through several means, such as vigilant server and system log monitoring, installing a properly configured IDS (intrusion detection system), and implementing file integrity tools.

Recovery is the capability of providing essential services and assets during an attack and being able to achieve full service restoration after a compromise has taken place. Recovery can be significantly improved, for example, via redundant facilities, running hot-spares, and implementing a tape back-up system.

Survivable System Analysis: The Process

The SSA method was developed by the SEI CERT® (Computer Emergency Response Team) Coordination Center as a means for organizations to understand survivability in the context of their operating environment. Principally, the SSA method seeks to help one understand what functions must survive attack? What intrusions could occur? How could intrusions affect survivability? What are the business risks and how could architecture modifications reduce these risks[2]? By systematically considering these questions, the SSA method can be used to identify risks and spearhead the creation of effective mitigation strategies.

The SSA Method is comprised of four specific steps:

I. Step One: System Definition

The initial step is focused on understanding the mission objectives of the organization and what system requirements are used to achieve them; the system's architecture and operational risks are identified in step one. This information is obtained by meeting with all of the stakeholders involved and helps the assessment team identify the network's topology and operating environment.

II. Step Two: Essential Capability Definition

After a firm understanding of the network architecture is achieved, the identification of essential services, those that support the enterprise mission and must be accessible in the face of attacks and failures are identified as are the systems essential assets, those whose integrity, confidentiality, and availability must be maintained during an attack. Essential services and assets are characterized by usage scenarios so as to delineate the steps and components

[2] Software Engineering Institute, http://www.cert.org/archive/pdf/sna-tutorial.pdf

needed to fulfill mission objectives. All scenarios are displayed as traces through the network architecture to identify *essential components* whose survivability must be ensured[3].

III. Step Three: Compromisable Capability Definition

Next are intrusion scenarios, which are derived from the assessment of network risks and an attacker's potential skill level. Intrusion scenarios are mapped onto the network's architecture in order to identify the *compromisable components* (components that could be penetrated and negatively impacted by intrusion).

IV. Step Four: Survivability Analysis

Once the compromisable components of the architecture have been identified, strategies for survivability begin to take shape. By analyzing steps two and three, we can discover *softspot components* within the architecture. Softspot components are elements of the network infrastructure that are both essential and compromisable. After the softspot components have been identified, the next step is to begin implementing defensive strategies using a survivability map. A survivability map outlines procedures for applying the three R's of survivability based on the network's softspots. The survivability map serves as an action plan for enhancing survivability by visibly organizing information about the current architecture, vulnerabilities, and recommended mitigation strategies.

Deliverables

Utilizing the SSA method produces the following deliverables:

- Essential services and assets, and their related architectural components
- Architecture vulnerabilities and softspots
- Representative intrusion scenarios and the compromisable components likely to be exploited
- Mitigation strategies for resistance, recognition, and recovery
- System survivability map

These deliverables are provided in a final report and briefing that is to be presented to Company Z's management team. The aim of the report is to provide a basis for adequate risk analysis, identify cost/benefit trade-offs, and ultimately improve the system's survivability.

Benefits

The SSA method helps an organization enhance its security posture by providing management with a roadmap for improving and hardening their system's architecture. By increasing survivability awareness, a company can address potential threats and vulnerabilities to their network proactively as opposed to dealing with exposures from a reactive position. Clearly, it is more advantageous to manage survivability risks up front rather than managing damage control later.

[3] Ellison, http://www.sei.cmu.edu/pub/documents/98.reports/pdf/98tr014.pdf

3. During Snapshot

3.1 STEP 1: System Definition

The primary business objective of Company Z is to assist in the launching and expansion of new city businesses and real estate development projects, a mission that brings employment, tax revenues and healthy commercial districts to the surrounding community. The organization deemed their GroupWise 5.5 messaging system as a critical component of their system and one that helps them preserve their business mission by ensuring communication across several departments as well as to their outside customers. In addition, the CZ-1 server (Figure 1) holds all organizational data files, and supporting legal, financial, core services, and strategic business information regarding current and prospective transactions.

Thus, the primary components of Company Z's network architecture that help them achieve their business mission are

- CZ-1 server
- GroupWise 5.5 messaging system (CZ-2 server)

To obtain the information above, I met with Company Z's IS Manager to identify the scope of work to be completed as well as the boundaries of the system to be analyzed. I was able to meet with other stakeholders of the network as well, such as departmental managers and end users, and received their feedback as to what they believed were the critical functions and components of the system and how they interacted with the organizations overall business mission. A very useful aspect of the SSA method is that it creates a forum for system clarification and security awareness among users. It may be the case that the enterprise or company service areas are not aware of their own system's architecture. Through inquiry, it becomes evident what employees know about their network and what they do not.

I. Company Z Network Architecture and Components

The following figures list the software and hardware components comprising Company Z's internal network architecture. In this case study there were no boundaries that required administrative control changes.

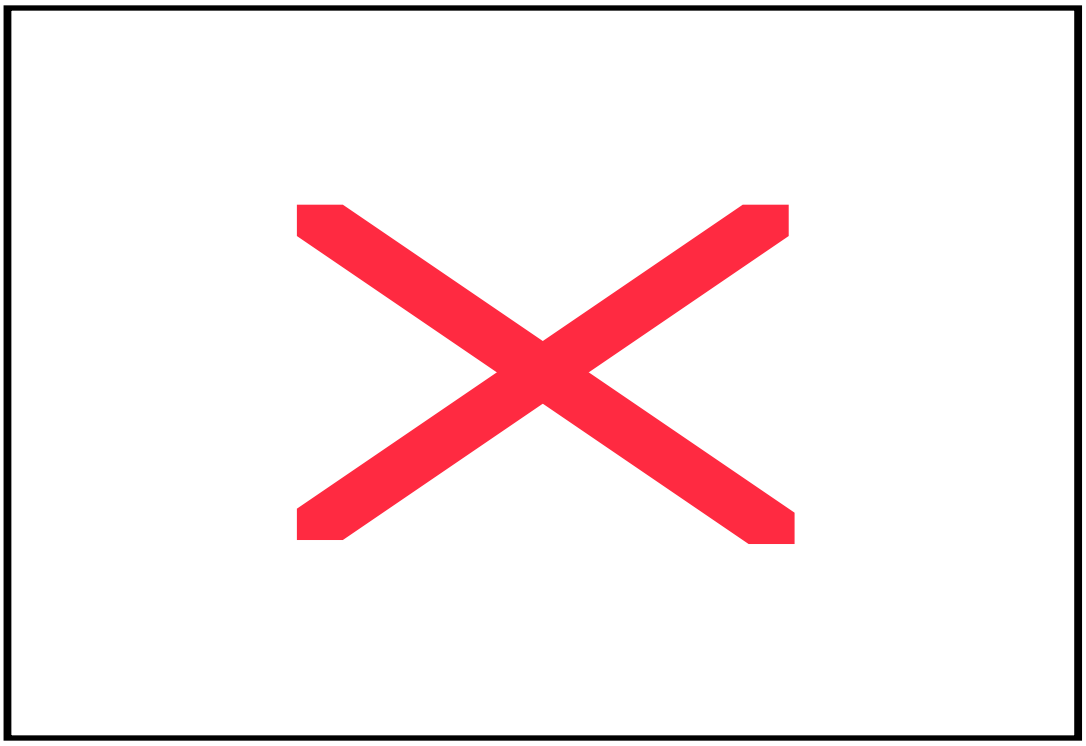

Figure 1

Listed below are the components of the network architecture in the above diagram. These components are fundamental to the system and served as the focus of my analysis:

- Internet Service Provider (ISP)
- Symmetric Digital Subscriber Line (SDSL)
- Cisco 678 Series Router
- Cisco PIX Firewall- State Configuration
- Antivirus server (Norton)
- CZ-1 Company data file server
- CZ-2 GroupWise e-mail server
- PC Workstation Configuration
- Novell Consultant pcAnywhere (not shown)

Quantity	Hardware	Software
3	Compaq Proliant 1600	Messaging System – GroupWise 5.0

	Servers	
110	Compaq Desktop PC's	Network OS-Novell 5.0
10	HP Printers	Database – Rbase 6.0
4	3-Com Switches	Anti-Virus- Norton Corporate Edition 7.6
3	3-Com Hubs	Desktop OS- Windows 98
1	Cisco 678 Router	Cisco device software
1	Cisco PIX Firewall	Cisco device software

Figure 2

II. Company Z Users and Functional Requirements

Discussions with the client produced the network's users, services, and access levels. The table below describes those relationships.

User	Access Level	Services
Information System's Team & Network Administrator's	Full network access	Password administration, antivirus server configuration, Rbase updates
Administrative Staff running Windows 98	Desktop PC access	GroupWise e-mail system, Internet, personal files
Novell Consultant	Full network access	Full network privileges

Figure 3

The following functional requirements for Company Z's network were identified:

- Availability of e-mail services is critically important.
- Personnel must be able to access shared subdirectories and files
- Personnel must be able to query database for business related functions

Interviews with the client enabled me to get a good idea of how users interact and utilize the system. A user is only granted access to his/her specific departmental directory. For example, there is an executive directory (h:\exechome), which contains several sub-directories. All of the members of the executive group have access to the entire executive directory but do not have access to the finance directory. Finance would have access to the finance directory but not to the executive directory and so on. Thus, each member of a particular department has full access to their departmental directory but not to other departmental directories outside of their scope of responsibilities. However, there are some public areas that are universally accessible. Typically, photos, document templates, and gaming, for instance are saved to this area in order to be shared with all users. There are also database files that are assigned to users on an as needed basis

3.2 STEP 2: Essential Capability Definition

I. Normal Usage Scenarios

Stakeholders

To identify the essential services for Company Z's system, I first listed all normal usage scenarios based on four users groups. Below is a brief description of the participants and their roles within the assessment.

- General Staff (Executive, Administration, and Information Services)
- Specialized Staff (Legal, Financial, Internal Audit, Housing and Real Estate)
- Information Systems Staff (Technical Support Team, Network Administrators)
- Novell Consultant.

Normal Usage Scenarios for General Staff

NUS1: Utilize e-mail server for internal and external correspondence
The General Staff of Company Z utilizes the GroupWise e-mail system for communications between clients, business partners, and other associates.

NUS2: Gain access to shared sub-directories and files relevant to job title and function
The General Staff of Company Z accesses the file server for attachments saved from e-mails during their internal and external communications as well as various other documents, such as word and or excel spreadsheets for example.

Normal Usage Scenarios for Specialized Staff

NUS3: Query database for business-related functions in order to generate reports
The Specialized Staff of Company Z need to access the database system to generate various types of reports such as financial and legal.

NUS4: Query database to download data into documents or spreadsheets for manipulation and analysis for attachments
The Specialized Staff needs to access the database system to generate individual files for data manipulation and analysis.

Normal Usage Scenarios for Information Systems

NUS5: Provide system and network support with full network access rights
The Information Systems Staff need to have full access in order to administer the network and provide support for users.

NUS6: Recover files through the data recovery policy
The Information Systems Staff need to follow the data recovery policy in the event of an accident, intrusion, or disaster. A disaster could range anywhere from an accidentally deleted file to a worst-case scenario of total data and or equipment loss. These scenarios need to be accounted for in a documented policy.

NUS7: Provide user account administration
The Information Systems Staff handles user account administration. They need to have the ability to add and delete users when necessary.

Normal Usage Scenarios for Novell Consultant

NUS8: Applies patches and upgrades to the system remotely.
The Novell Consultant is responsible for the application of system patches and upgrades on a remote basis through Virtual Private Network (VPN) access. The GroupWise e-mail system must be capable of distributing any patches or upgrades sent from the Novell Consultant.

NUS9: Access to the full complement of network services in order to address system issues
The Novell Consultant, through a VPN connection into Company Z's internal network, can gain access to all system components in order to address any system issues or problems. The GroupWise e-mail system must be available for the Novell Consultant to check and/or fix if necessary, it also provides a means of communication with Company Z personnel. In addition, this access enables the Novell Consultant to post action items should notification of downtime for any system be necessary or when a "downed system" would again be available.

By tracing each of the normal usage scenarios, I was able to determine the essential services, assets, and components.

II. Essential Services

- E-mail communication
- Ability to save mission critical documents and contact information

The two major functions of Company Z's system are to facilitate communication services between internal and external entities and to store all mission critical data and information.

III. Essential Assets

- GroupWise e-mail system
- CZ-1 file server
- Mission sensitive data/files

Company Z's GroupWise e-mail system is the client-identified essential asset. It is essential for continued communication between Company Z and its clients and or business associates. However, during my assessment of the system it became apparent that the true essential asset was the company's file server (CZ-1). The CZ-1 file server and the tape-back-up system contain all of the data and information necessary for Company Z to fulfill their mission. This server contains financial transaction data and proposal documents, for instance, and needs to be fortified.

IV. Essential Components

Six essential components were identified within Company Z's network architecture:

- Cisco Router 678
- Cisco PIX Firewall
- Antivirus server
- CZ-1 Server – Company data files
- CZ-2 Server – GroupWise e-mail
- PC Workstations

3.3 STEP 3: Compromisable Capability Definition

I. Attacker Profiles

I identified the four most likely threats to Company Z's system (listed below). Although there are many other possible threats, such as terrorists and natural disasters, in order to provide the client with maximum benefit, I focused on realistic and logical scenarios.

Attacker	Recreational	Disgruntled Employee	Competitor/Spy	Activist
Resources	• Range of skill levels:	• Moderate to high level of	Moderate to high skill level	Moderate to high skill level

	• Script Kiddies • Intermediate • Expert • Internal	skill • Familiarity with network		
Time	• Unlimited time • Very patient	• Variable time input • Generally cannot devote long hours but waits for opportunity.	Variable, desired information may have limited shelf life	Patient, but desired information may be needed quickly
Tools	• Generally available scripts and tools • Social Engineering	• Existing access & knowledge • Available scripts and tools • Social Engineering	• Generally available scripts and tools • Social Engineering • Customized tool set	• Generally available scripts and tools • Social Engineering • Customized tool set
Risk	• External: little knowledge of potential risks • Internal: likely to be risk averse	Risk Averse, particularly if still employed[4]	Risk averse, particularly if major competitor	Risk averse
Access	• External (Dialup/Internet) • Internal: on the network	• Internal: on the network • External (Dialup/Internet/ VPN)	External (Dialup/Internet)	External (Dialup/Internet)
Objectives	• Personal recognition • Curiosity • Develop hacking skills	• Revenge, retribution. • Theft of financial and/or legal information • Personal gain	• Gain advantages for bids and legal proceedings. • Political interest.	Disrupt construction and legal procedures
Level of Attack	Target-of-Opportunity Attack	Intermediate to High	Sophisticated attack	Sophisticated attack
Probability	Medium	High	Low	Low

Figure 4

II. Intrusion Usage Scenario

IUS1: Malicious code attack

[4] Ellison, http://www.stsc.hill.af.mil/crosstalk/2000/10/linger.html

- What is the attack
  Users download malicious code (e.g. Trojan horses, viruses) from outside the network either accidentally or intentionally.
  Intruder installs malicious code directly.
- Who is the attacker
  Insiders (disgruntled employees, former employees).
  Outsiders (hackers, activists, spies).
- What are their objectives
  Compromise data confidentiality, integrity, privacy and availability
- Category of attack pattern
  Application content

IUS2: Legitimate login by unauthorized user / Spoofing attack

- What is the attack
  An unauthorized user logs in using a compromised password obtained via network sniffing or social engineering. User then views, modifies or deletes company data.
- Who is the attacker
  Insiders (disgruntled employees, former employees).
  Outsiders (hackers, activists, spies).
- What are their objectives
  View, modify or delete company data.
- Category of attack pattern
  User access

IUS3: Unauthorized access by insiders

- What is the attack
  Inside intruder accesses servers physically or via system administrator access rights in order to view, modify or delete data.
- Who is the attacker
  Insider (disgruntled employees)
- What are their objectives
  View, modify or delete private data.
- Category of attack pattern
  User access

IUS4: Buffer overflow attack

- What is the attack
  An outside intruder initiates a denial-of-service attack by sending more data than the application's buffer can hold, causing the application or entire system to crash.
- Who is the attacker
  Outsider (Hackers, Activists, Spies)
- What are their objectives

To compromise the availability of servers and applications by overloading them with data. Disclose private data to gain advantages for bids proceedings.

- Category of attack pattern
  Component access

III. Vulnerabilities

The execution of the IUS revealed various component vulnerabilities.

- IUS1 demonstrates that Company Z's applications do not follow sufficient defense in depth measures and thus lack adequate protection mechanisms to keep malware at bay.
- IUS2 illustrates that Company Z's system does not offer multi factor authentication or an intelligent way of auditing user activity.
- IUS3 demonstrates that Company Z's network adheres to a trusted group model thus permitting a single user to gain heightened privileges once the appropriate login identity is captured.
- IUS4 shows that the company's system does not run applications under the principle of least privilege nor are they applying *any* vendor patches or software updates with needed frequency.

IV. Compromisable Components

Based on the intrusion usage scenarios above, an attacker could potentially compromise the following network components:

Cisco 678 Series Router

- A vulnerability exists in Cisco routers such that a router which is configured to suppress source routed packets with the following command:

  ```
  no ip source-route
  ```

  may allow traffic which should be suppressed[5].
- By sending a large packet of data to the Dynamic Host Configuration Protocol (DHCP) port (547), it is possible to freeze the Customer Premise Equipment (CPE). DHCP service is enabled by default.
- Cisco's 678 Router Software contains a flaw that permits the successful prediction of TCP Initial Sequence Numbers. It only affects the security of TCP connections that originate or terminate on the affected Cisco device itself; it does not apply to TCP traffic forwarded through the affected device in transit between two other hosts[6].

[5] CERT CC, http://www.cert.org/advisories/CA-1993-07.html

[6] CISCO Security Advisory, http://www.cisco.com/warp/public/707/CBOS-multiple2-pub.html

Impact

These vulnerabilities can allow unauthorized traffic to pass through the router/gateway creating a number of attack scenarios for an individual with malicious intent.

Cisco PIX Firewall

- The Cisco PIX Firewall product is shipped with a management application known as PIX Firewall Manager, or PFM. PFM includes a limited HTTP server. The PFM HTTP server runs on Windows NT computers. A vulnerability in the PFM HTTP server allows any attacker who can connect to the server to retrieve any file known in advance to exist on the Windows NT host. In almost all cases, this means that the host is vulnerable to attack by any user inside the firewall, but not by users outside the firewall[7].
- Allows a remote attacker to send IP packets with spoofed addresses through the firewall.
- Allows a remote attacker to cause a denial of service condition in certain restricted situations.
- When telnet/SSH access is enabled on the firewall's internal network for at least one internal host, a remote user can repeatedly send TCP SYN packets to the IP address of the subnet that the PIX is on, possibly causing a denial of service condition. The firewall will respond to the TCP SYN packet, completing the TCP three-way handshake with any external host that targets the subnet address[8].

Impact

- If prerequisites are met, attackers can retrieve any file or files on the NT host on which PFM is installed, as well as any file or files on network servers accessible through that host's file system[9].
- If a PIX firewall is configured to allow "established" connections, an intruder who can establish a connection to any port on a machine behind the firewall can, for at least a few minutes, establish a connection to ANY port on that machine, thus defeating the purpose of the firewall in the first place. The existence of any connection between an inside and an outside host is sufficient for the *established* command to permit connections from the outside host to the inside

[7] CISCO Security Advisory, http://www.cisco.com/warp/public/770/pixmgrfile-pub.shtml

[8] Security Tracker, http://www.securitytracker.com/alerts/2002/Nov/1005590.html

[9] Win2000 Archives, http://www.ntware.com/2000/bugs/cisco__2.html

host. The direction in which the original connection was made is not checked.

- This is particularly concerning if an intruder can establish an FTP connection to an FTP server that supports the PORT command. This may enable an intruder to establish a connection to virtually any machine behind the firewall if any machine behind the firewall has a vulnerable FTP server, and runs a publicly available service[10].
- An attacker may be able to establish a connection between the FTP server machine and an arbitrary port on another system[11]. This connection may be used to bypass access controls that would otherwise apply.

CZ-1 Server Data Files

All data is sent across the internal and external (Internet) network unencrypted.

Impact

- Interception of plaintext data in transit.
- Modification to programs or data.
- Insertion of communications/code injection.
- Blocking of traffic

CZ-2 GroupWise Server

- When NDS (Netscape Directory Service) browsing via the web server is enabled, any attacker that can reach port 80 on the server can also enumerate information such as user names, group names, and other system information.
- Poor handling of GET commands will allow GroupWise Web access servers to display indexes of the directories instead of HTML files.

Impact

- Program/data modification
- IP/user ID spoofing
- Man in the middle attacks

Below is a depiction of the compromisable components:

[10] CERT CC, http://www.kb.cert.org/vuls/id/6733

[11] CERT CC, http://www.cert.org/tech_tips/FTP_port_attacks.html

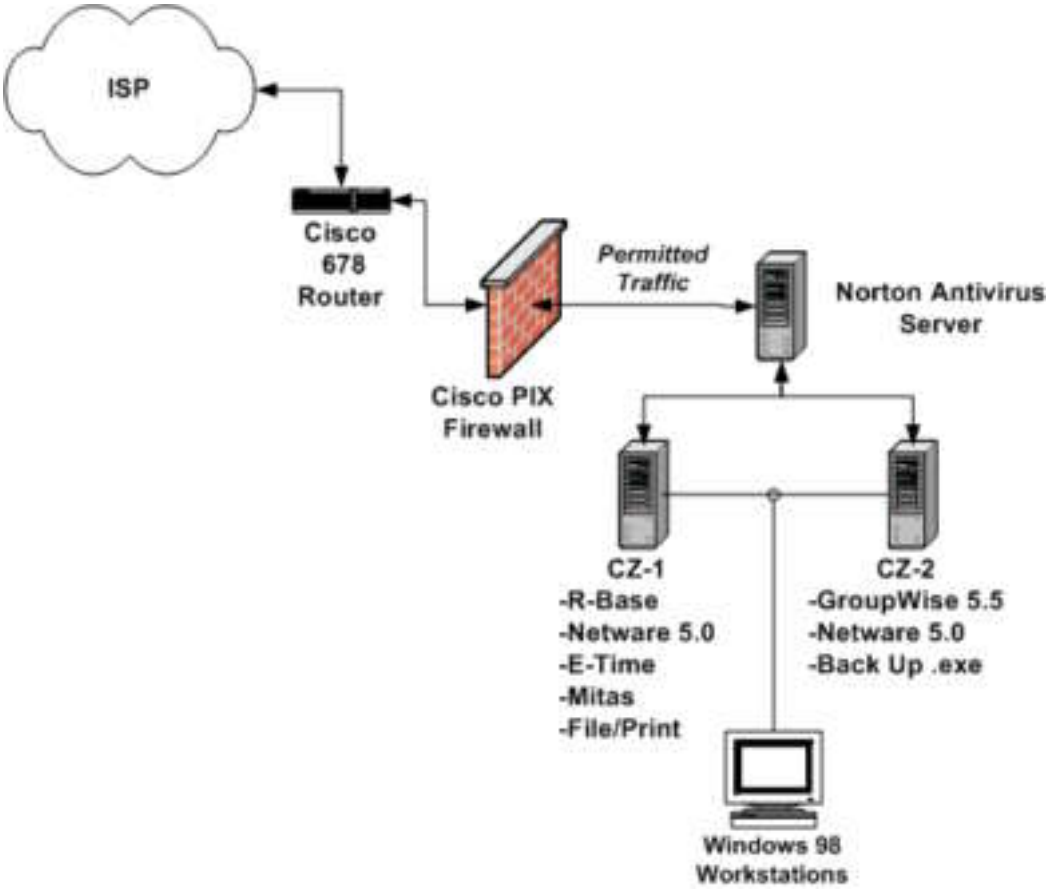

Figure 5

4. After Snapshot

4.1 STEP 4: Survivability Analysis

I. Softspot Components

Softspot components are the system components that are both essential and compromisable. The softspot components are:

- Cisco 678 Series Router
- Cisco PIX Firewall- State Configuration
- Antivirus server (Norton)
- CZ-1 Company data file server
- CZ-2 GroupWise e-mail server
- PC Workstation Configuration

In IUS-1, IUS-2, and IUS-3, all of the compromisable components are identified as softspot components as well. This is by definition, as softspot components are those that are both essential and compromisable. The components vulnerable to malicious code attacks and/or unauthorized access attempts are outlined in the network trace below:

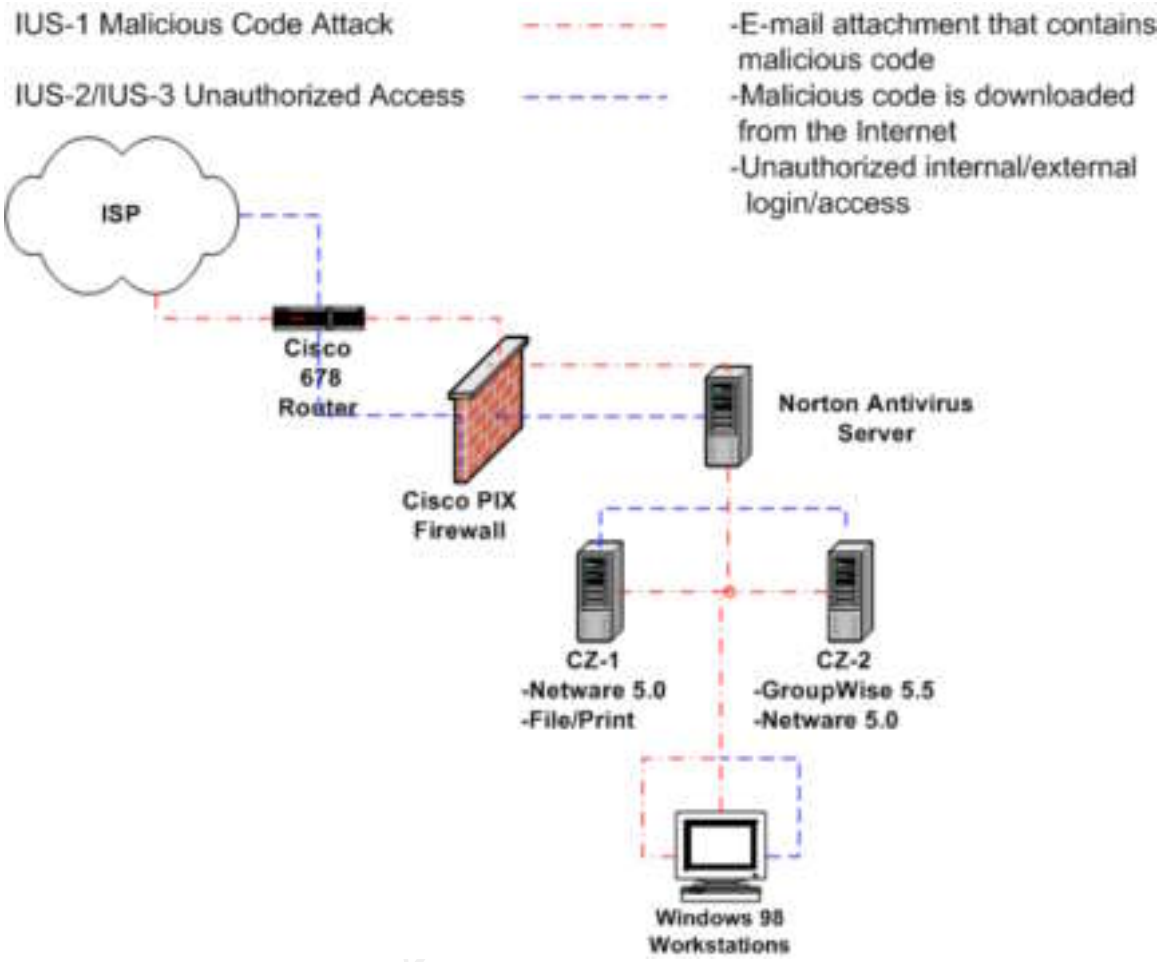

Figure 6

The network trace for IUS-4 can be seen below. Buffer overflows can bear fruit in the form of denial-of-service attacks (DoS). For the scope of this paper, DoS attacks will be limited to malicious code crafted to deny access to a system, network, application, or information to a legitimate user. Since most DoS attacks originate from spoofed IP addresses, the ISP, router, and firewall, are also

included as softspot components.

Figure 7

II. Policy Recommendations

P1. Establish acceptable use policy and Internet disclaimer

Sound security strategy is intrinsically linked to a comprehensive security policy; policies that are not only well defined, but implemented and understood by the organizations management team and system users alike. Currently, Company Z does not have a well defined, documented, or implemented policy regarding material viewed or downloaded by employees from the Internet. Clearly, the danger of the Internet to anyone reading this paper is fairly evident, however, it is the education of the everyday, typical user that needs to be addressed. Users need to be cautioned that the Internet includes offensive, sexually explicit, and at times inappropriate material in combination with data that can serve as an invaluable resource. For most users, it is difficult to avoid at least some contact with offensive material while utilizing the Internet. Even innocuous search requests can lead to sites with dubious content. In addition, having an email address on the Internet can lead to receipt of unsolicited email or "spam" which may contain offensive information. Users that access the Internet do so at their own risk and need to understand the situations and circumstances that may subject them to policy enforcement as determined by Company Z's policies and procedures.

P2. Establish an information protection policy

Guidelines for processing, storing, and transmitting information by Company Z employees or contractors must be explicitly outlined, reviewed, and established. The purpose of this policy is to ensure that the company's sensitive and proprietary information maintains its integrity and is appropriately protected from modification or disclosure.

P3. Establish a user account policy

Policies and procedures documenting and outlining the requirements for requesting and maintaining user accounts on computing services located at or operated by Company Z need to be implemented.

P4. Establish a remote access policy

A policy that details the guidelines for remotely accessing computing systems and facilities located at or operated by Company Z would be well served. This includes, but is not limited to, any computer, server, or network provided or supported by the company. The purpose of these types of policies and procedures are to ensure that all employees and partners using Company Z's computing facilities do so in an effective, authorized and secure manner.

P5. Establish a more thorough backup policy

While Company Z informally discussed their backup procedures with me during our meetings, what I did not observe was a well defined, documented, formal backup policy in order to recover from an accident or security incident. Such a policy is needed and will go a long way in terms of providing explicit instructions on when to back up the system in order to maintain a high level of data integrity and availability.

P6. Establish security awareness training procedures

Security awareness and training is an essential component of IT delivery and Company Z's computing resources are no exception. Security training for all personnel interacting with the company's computer resources should be routine and performed in accordance to organizational policies and procedures. Security training could range from good password management to reporting network anomalies within the system. Training is an ongoing process and should be focused on enabling personnel to stay abreast of current security practices and technology.

P7. Monitor and update system security

Maintaining vigilance over the security of the system is essential to the survivability of Company Z's computing resources. Monitoring the system could range from tracking network traffic to reporting strange individuals in the building. System security needs to be constantly reviewed and updated to reflect changes in the outside world as well as the internal network environment.

III. Architectural Recommendations

R1. Install content filtering software on the GroupWise mail server

Type:	Application
Strategy:	Resistance, Recognition
Intrusion:	IUS1, IUS4
Rationale:	Content filtering software is able to detect and remove unnecessary e-mails and or information. It is especially useful when the mail server is "mail-bombed" (i.e. inundated with unsolicited e-mail messages)
Result:	Decreases the amount of unnecessary trash mails, reduce Mail Server load and Mail storage.
Implementation:	A vendor provided, compatible content filtering solution can be quickly purchased to operate with the existing mail server, and at a reasonable cost, $100-$1500 depending on the number of users and platform desired.

R2. Install redundant mail server at ISP or other location

Type:	Infrastructure
Strategy:	Recovery
Intrusion:	IUS4
Rationale:	When the primary mail server fails, redundancy definitely helps. A back up mail server is a critical component for an organization that relies so heavily on electronic communication. Once the original server is back on line, the redundant server can then transfer the queued e-mails.
Result:	No mail will be lost or returned when the existing mail server fails.
Implementation:	The redundant mail server does not require a standalone installation. Any server can be configured to serve as a backup server for the primary e-mail repository. It may be possible to use the ISP's mail server for redundancy purposes.

R3. Advanced/Centralized logging

Type:	Infrastructure
Strategy:	Recognition
Intrusion:	IUS2, IUS3, IUS4
Rationale:	Advanced/centralized logging provides a better way to handle system logs. A dedicate log server can keep log files from all other machines and is more unlikely to be compromised. If any host is compromised, the log server provides excellent repository for analysis and return traces.
Result:	Logging can be processed and monitored in one place. Less worry regarding losing log data when an intrusion happens.
Implementation:	It is best to have a dedicated log server which runs a logging service exclusively. Other servers will have to duplicate their system logs to this log server by using a remote logging mechanism.

R4. Secure e-mail (Pretty Good Privacy (PGP) or Secure ID)

Type:	Application
Strategy:	Resistance, Recognition

Intrusion:	IUS1, IUS2, IUS3
Rationale:	Digital signatures provide an excellent way to identify both senders and receivers. Strong encryption and message digests can ensure the confidentiality and integrity of the document(s) . PGP provides one of the best low cost options for exchanging emails securely. Version 6.5 can still be obtained as freeware.
Result:	Email is secure, authenticated and kept confidential. Increases the difficulty to spoof emails.
Implementation:	Staff, consultants, and business associates who wish to share secure e-mails should have their own Secure ID or PGP keypair.

R5. Enforced password management

Type:	Application
Strategy:	Resistance, Recognition
Intrusion:	IUS2, IUS3
Rationale:	A weak password can be cracked in minutes. By running password-cracking software regularly, one may quickly reduce the number of weak/easily-cracked passwords. In addition, passwords should be changed on a regular basis, such as monthly or quarterly.
Result:	Passwords would be less vulnerable to cracking, guessing, and unauthorized access.
Implementation:	Install password-cracking software and enable automated periodic cracking. Use software to initiate changing passwords regularly and policy to enforce.

R6. Implement cryptographic checksums

Type:	Application
Strategy:	Recognition
Intrusion:	IUS1, IUS2, IUS3, IUS4
Rationale:	Measures the validity of the user-identified criteria such as time and date stamps. Checksums are a solid way to validate the integrity of data already in the system and provides an excellent means of recognizing when the data is compromised.
Result:	Intrusions and incorrect file configuration(s) may be discovered. Store checksum values in other secure place
Implementation:	Tripwire or application-level checksum could be used.

R7. Install a network based intrusion detection system (NIDS)

Type:	Infrastructure

Strategy:	Recognition
Intrusion:	IUS1, IUS2, IUS3, IUS4
Rationale:	A properly configured intrusion detection system can recognize known intrusion signatures and provide an opportunity to discover improperly configured system or firewall settings.
Result:	Intrusions and incorrect system configuration(s) may be discovered. This hardens the security posture of the organization and makes an intruders attack and penetration attempts all the more difficult
Implementation:	Install a network-based IDS system to monitor traffic between the firewall and the Intranet, less expensive as well.

Modified network architecture based on recommendations:

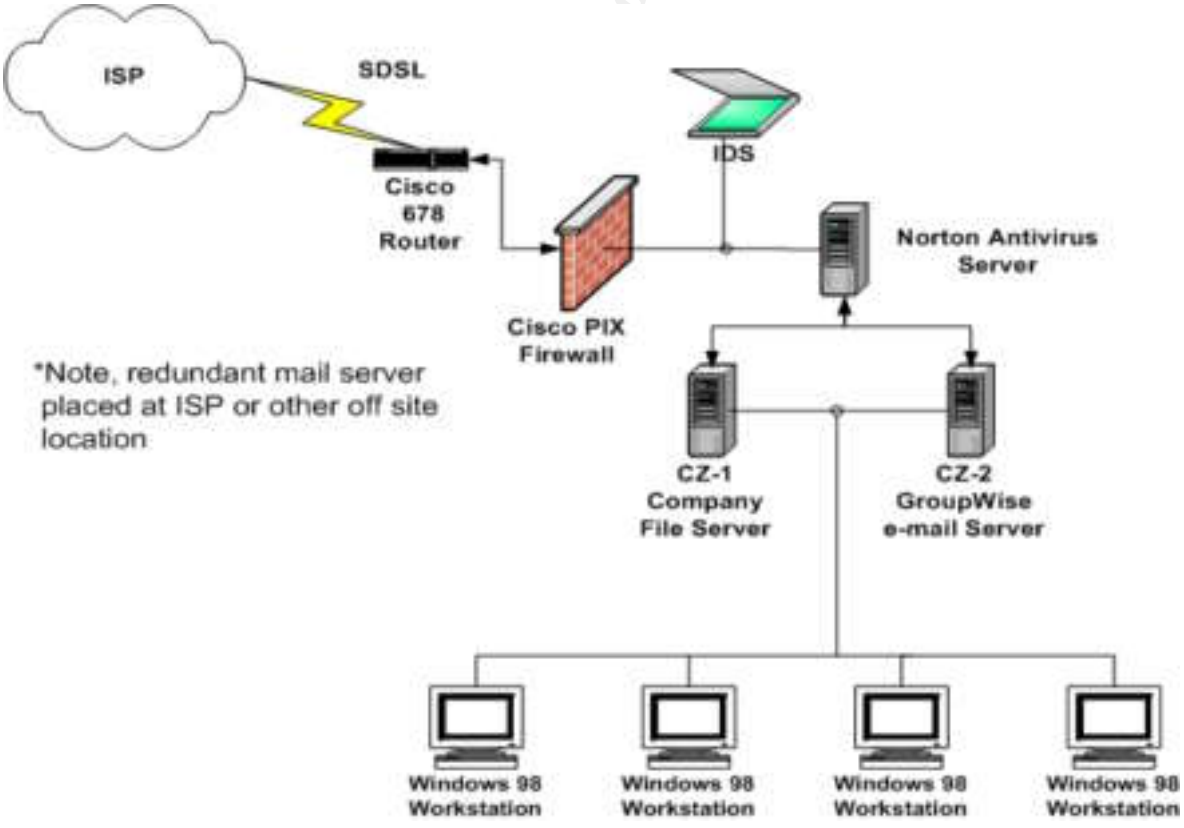

Figure 8

IV. Survivability Map

Intrusion Usage Scenario	Softspot Effect	Architecture Strategies		
		Resistance	**Recognition**	**Recovery**
1) Malicious Code Attack	• Antivirus Server • CZ-1 Server • CZ-2 Server • PC Workstation	**Current**: Antivirus software	**Current**: Antivirus software	**Current**: Antivirus software
		Recommended: • Security Awareness and Training • Content filtering software	**Recommended**: Network based Intrusion Detection System (NIDS)	**Recommended**: • Password management policies and procedure • Backup/Restore procedure
2) Unauthorized Access by External Intruder/ Spoofing Attack	• Router • Firewall • Antivirus Server • CZ-1 Server • CZ-2 Server • PC Workstation	**Current**: Password management	**Current**: User recognition	**Current**: Manually rebuild system
		Recommended: • Upgrade OS • Secure device configurations • Apply patches regularly • Strong password policy • Login/Screensaver timeouts	**Recommended**: • Intrusion Detection System • Advanced/centralized logging • Regular review of logs	**Recommended**: • Password changing procedure • Backup/Restore procedure

Intrusion Usage Scenario	Softspot Effect	Resistance	Recognition	Recovery
3) Unauthorized Access by an Internal User	• Antivirus Server • CZ-1 Server • CZ-2 Server • PC Workstations	**Current**: • Password management • Threat of punishment	**Current**: • User recognition • Basic logging	**Current**: Disciplinary action
		Recommended: • Strong password policy • Access controls • Encryption / SSL	**Recommended**: • Advanced/centralized logging • Regular review of logs	**Recommended**: • Password changing procedure • Backup/Restore procedure
4) Buffer overflow/D0S attacks	• Router • Firewall • Antivirus Server • CZ-1 Server • CZ-2 Server • PC Workstation	**Current**: • Firewall • Mail filters	**Current**: • Firewall logs • User recognition	**Current**: Ad hoc ISP point-of-contact
		Recommended: • Content filtering software • Redundant mail server	**Recommended**: • Intrusion Detection System • Regular review of logs	**Recommended**: • Predetermined ISP point-of-contact • Secondary connectivity

V. Timeline Phasing of Recommendations

Type	Short Term 1-6 months	Mid Term 6-12 months	Long Term 18+ months
Policy	• P1-Establish acceptable use policy & Internet disclaimer • P2- Establish an information protection policy • P3- Establish a user account policy • P5- Establish a more thorough backup policy	• P4-Establish a remote access policy • P6- Establish security awareness and training procedures	P7-Monitor and update system security
Architecture	• R1-Content Filtering • R3-Advanced/centralize logging • R5-Enforced password management	• R2- Redundant mail server • R4-Secure e-mail (PGP) • R6-Cryptographic checksum	R7-Host based IDS

VI. Estimated Relative Resources to Implement Recommendations

Recommendation	Labor	Cost
P1. Establish acceptable use policy and Internet disclaimer	Low	Low
P2. Establish an information protection policy	Low	Low
P3. Establish a user account policy	Low	Low
P4. Establish a remote access policy	Medium	Low
P5. Establish a more thorough backup policy	Medium	Low
P6. Establish security awareness and training	Medium	Existing
P7. Monitor and update security	High	Medium-High
R1. Install content filtering software on mail server	Low	Medium
R2. Install redundant mail server	Low	Medium-High
R3. Advanced/Centralized logging	Medium	Existing
R4. Secure e-mail (PGP/Secure ID)	Medium	Low-Medium
R5. Enforced password management	Medium	Medium-High
R6. Cryptographic checksum	Medium	Medium
R7. Network based IDS	Medium	Medium-High

Labor	Cost
• Low = 0-1 Person Month • Medium = 1-3 Person Month • High = 3+ Person Month	• Existing = Current Equipment • Low = $0 - $1K • Medium = $1 - $5K • High = $5+K

5. Client Highlights

One of the difficulties in working with non-profit agencies often involves the lack

of necessary funding to facilitate technological improvements. Company Z was no different in this respect. However, both the stakeholders and I felt that the results of the SSA method could be used to improve the overall security architecture of the organization on several levels, many of which can be implemented at little to no cost to the organization. Some of the client identified highlights included:

- Greater understanding of their network architecture and survivable concepts.

A very useful aspect of the SSA method is that it creates a forum for system clarification and security awareness amongst users. It may be the case that the enterprise or company service areas are not aware of their own system's architecture. Through inquiry it becomes very clear what employees know about their system and what they do not. This can help the organization to gain a better grasp of their technological culture, which can be useful when developing security policies, procedures, and training. In addition, the SSA method provides a methodology for identifying softspot components within the network's architecture. Once they have been identified company personnel can begin to address security deficiencies specific to each component and gain an appreciation for hardening weak links.

- Survivability Map

The Survivability Map defines where security gaps exist within Company Z's environment and will be very useful over the near to mid term by providing suggestions for the planning, architecture, design and implementation of survivability controls and measures to address deficient areas.

- Timeline phasing of recommendations.

This part of the SSA method enabled the stakeholders to see what improvements needed to be made to their system architecture and in what timeframe. Many stakeholders were surprised to hear that some of their security concerns could be addressed through basic security policy development and implementation. Because policies can be written by existing personnel at relatively low cost they are usually quickly embraced. Most organizations welcome the establishment of policies and procedures that provide direction and support for information security and ensure that measures are in place to govern the administration and operation of information systems.

6. Conclusion

A critical component to conducting an effective security assessment involves gaining a firm understanding of the client's business environment and

methodologies. It is difficult to make sound system recommendations if the mission of the business is not clearly understood. To this end, the SSA method is a very beneficial assessment framework as it is directly anchored to such identification. The SSA method serves to identify what assets and services, in particular, are essential to preserving mission functionality and survivability. If a company is not fully aware of what critical systems must survive attacks and failures they are putting their entire organization, and their customers at risk.

The current architecture of Company Z's system is not survivable because the loss of one component, the CZ-2 server and or the CZ-1 server, would thoroughly compromise mission fulfillment. A solution based on the recommendations and findings of the SSA method is a well-directed first step towards meeting and preserving their mission objectives. A primary reason for the architectures current state is the underestimation of the significance of the system to the major stakeholders in positions high enough to initiate change. One of the main drivers behind why Company Z's system fails, within the context of survivability, is that management is focused on cost avoidance and inhibiting change. This type of thinking, along with a lack of adequate funding, has established an organizational culture whose focus is on day-to-day operations as opposed to long-term system survivability. However, while this scenario is understandable given the bureaucracy of the public sector, their current network survivability can be enhanced rather quickly with minimal initial expenditures. For example, developing and implementing unified organizational security policies can be a low cost initiative towards incrementally improving system survivability. In addition, these types of changes can be implemented over time to slowly transform Company Z's culture and overall outlook on the importance of security.

Survivability and security are ongoing processes, as no individual component is immune to all attack scenarios, disasters, and network architecture flaws. System security must consider the direct interaction between an organization's business mission and its technological infrastructure. By having a broad view of the system, one can begin to architect a survivable network that not only fulfills its mission in a timely manner in the presence of attacks, failures, and accidents but one that is adaptive to changes in client needs and organizational culture alike.

7. References

1) Ellison, Robert. Longstaff, Thomas. Mead, Nancy. McHugh, John. "Survivable Network Analysis Method". September, 2000. URL: http://www.sei.cmu.edu/publications/documents/00.reports/00tr013.html

2) Software Engineering Institute. Carnegie Mellon University. "Assessing Survivability of Critical Systems". September 1999. URL: http://www.cert.org/archive/pdf/sna-tutorial.pdf

3) Ellison, Robert. Longstaff, Thomas. Mead, Nancy. McHugh, John. "A Case Study in Survivable Network System Analysis". September 1998. URL: http://www.sei.cmu.edu/pub/documents/98.reports/pdf/98tr014.pdf

4) Ellison, Robert. Longstaff, Thomas. Mead, Nancy. McHugh, John. "The Survivability Imperative: Protecting Critical Systems". CrossTalk: The Journal of Defense Software Engineering. October 2000. URL: http://www.stsc.hill.af.mil/crosstalk/2000/10/linger.html

5) CERT® Coordination Center. "Cisco Router Packet Handling Vulnerability". Advisory CA-1993-07 September 19, 1997. URL: http://www.cert.org/advisories/CA-1993-07.html

6) Cisco Security Advisory. "More Multiple Vulnerabilities in CBOS". May 22, 2001. URL: http://www.cisco.com/warp/public/707/CBOS-multiple2-pub.html

7) Cisco Security Advisory. "Cisco PIX Firewall Manager File Exposure. September 2, 1998. URL: http://www.cisco.com/warp/public/770/pixmgrfile-pub.shtml

8) Security Tracker. "Cisco PIX Firewall can be Crashed by Remote Users When in a Certain Configuration. November 9, 2002. URL: http://www.securitytracker.com/alerts/2002/Nov/1005590.html

9) Win2000 Archives. "Cisco #2, Cisco PIX Firewall". URL: http://www.ntware.com/2000/bugs/cisco__2.html

10) CERT® Coordination Center. "PIX 'established' and 'conduit' command may have unexpected interactions". Vulnerability Note VU#6733 January 3, 2002. URL: http://www.kb.cert.org/vuls/id/6733

11) CERT® Coordination Center. "Problems with the FTP Port Command or Why You Don't Want Just Any Port in a Storm" April 28, 1998. URL: http://www.cert.org/tech_tips/FTP_port_attacks.html#1

Last Updated: July 27th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS