Vulnerability Assessment

Prepared for:

Sample Company

Prepared On:

January 2012

Notice

This document and supporting materials may contain sensitive and confidential information. Care should be taken to protect the contents of this document and any supporting materials from unauthorized disclosure.

Table of Contents

Table of Figures and Tables

Executive Summary

1 Background

Sample Company (SampCo) provides various services to numerous industries in over 30 countries around the world. These services are provided primarily through client web portals available over the Internet. SampCo's customers include many that are bound by government and industry regulations such as HIPAA, PCI, GLBA, and EU Privacy Laws. As such, SampCo is very concerned about maintaining the confidentiality of information stored on and accessed from its information systems.

SampCo engaged BTB Security (BTB) to provide information security consulting services in order to:

- Obtain a current snapshot of SampCo's IT information security posture
- Identify weaknesses in SampCo's information security technical and procedural controls
- Determine appropriate next steps to improve SampCo's information security posture

2 Scope of Work

BTB has executed a series of tasks in order to meet the aforementioned information security objectives. Leveraging its extensive experience with managing, developing, and assessing information security, BTB assembled a scope of work to achieve these goals. More specifically, BTB provided the services outlined below.

- ***Information Security Vulnerability Assessment***
  - Vulnerability Identification
  - Interviews with Key Stakeholders (e.g., system administrators, information security management)
  - System Architecture and Implementation Review (e.g., servers, workstations)
  - Network Architecture and Implementation Review (e.g., routers, switches)
  - Security Architecture and Implementation Review (e.g., firewalls/segmentation, monitoring, endpoint protection)
  - Procedure Documentation Review

3 Summary of Results

During this engagement BTB identified strengths and weaknesses within SampCo's information security program. BTB recommends that strengths be leveraged to mitigate the weaknesses and to aid in the advancement of the information security maturity level. The identified themes are listed below and include a visual depiction of the results to help focus efforts in the appropriate areas of concern.

3.1 Strengths

BTB identifies a *strength* as an item or theme that meets or exceeds leading security practices or provides mitigating controls to address risks to information security. The following *strengths* were identified during this assessment:

- SampCo employs intrusion protection capabilities and application firewalls that automatically block IP addresses that are determined to be staging attacks against SampCo Internet resources. Activities such as port scanning, brute force web application scanning, and repeated failed authentication attempts are shunned.
- SampCo provides multiple levels of segmentation and filtering based on an internally-defined data classification standard by which every system is mapped.
- System administrators must use a token-based multifactor authentication solution to gain access to production portal frontend and backend systems.
- All internal systems and devices use SampCo's Active Directory for authentication and strong password controls have been implemented (e.g., 14 character minimum, complexity).

3.2 Distribution of Findings

The chart below provides a graphical view of the distribution of security findings by remediation category. These results indicate that SampCo should focus its efforts on securing web applications and securing system and device configurations.

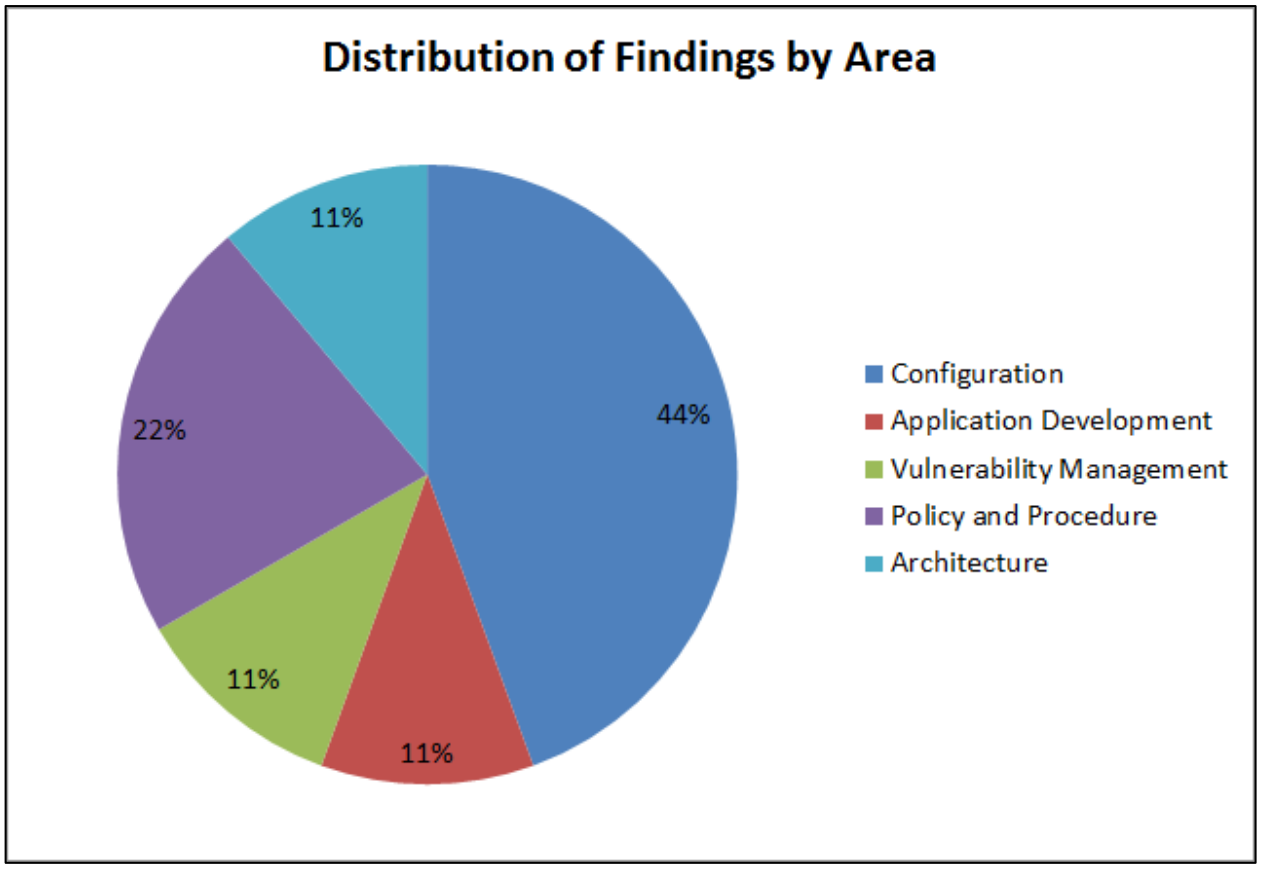

Figure 1 Vulnerability Distribution by Category

The chart below provides a graphical view of the distribution of security findings by risk level. The majority of vulnerabilities represent a medium level of risk to SampCo.

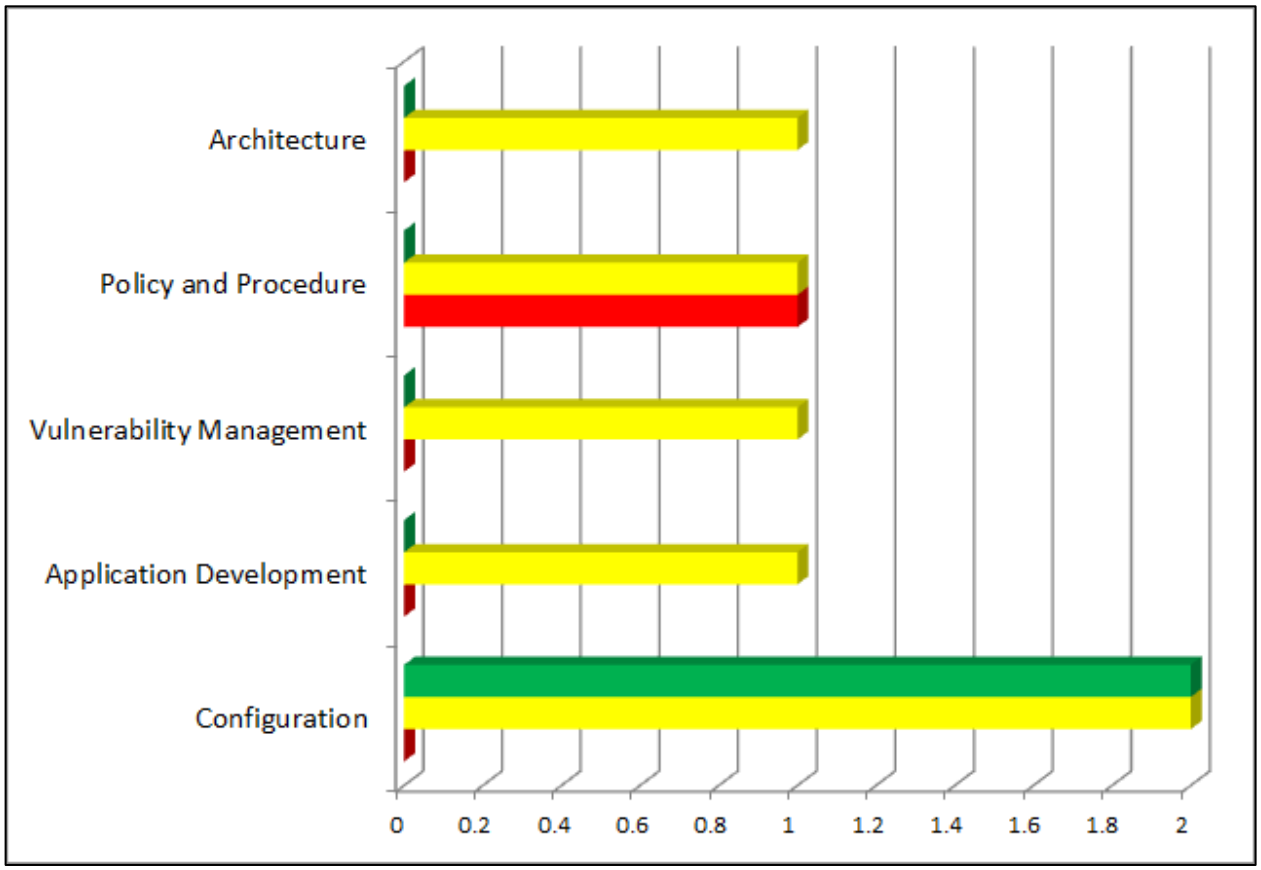

Figure 2 Vulnerability Distribution by Risk Level

3.3 Weaknesses

BTB identifies a *weakness* as an item or theme that exposes SampCo to excessive risk of a security compromise. While this list is not exhaustive, it is intended to bring attention to those areas that are considered to be most significant.

- SampCo is unable to actively or centrally monitor the environment for security related events and depends on user reports or administrators observing anomalous system behavior for detection.
- SampCo does not perform a regular access control reviews to identify retired accounts or accounts that have inappropriate permissions assigned.
- SampCo has not defined standard encryption controls to protect sensitive information in transit or at rest; while encryption is employed in various places throughout SampCo, the implementations are not consistent and some sensitive data remains unencrypted in databases and on mobile devices (e.g., laptops, smart phones).
- SampCo's Vulnerability Management process does not address exposures present on 3rd party and proprietary systems deployed within SampCo's environment (e.g., VoIP phone system).

4 Next Steps

SampCo should leverage the results of this assessment and testing to identify areas in the greatest need of improvement. Additionally, the specific findings are ranked with the highest risk level and lowest remediation effort first; this will help SampCo to prioritize remediation efforts to those that will provide the most benefit with the least expense of time or money. Some strategic areas that SampCo can focus on to make significant improvements to its information security posture are as follows:

- Security monitoring capabilities and incident response
- Data loss prevention
- Regular validation of implemented controls (e.g., configuration management)
- Standard encryption controls and implementing or consolidating to those controls
- Standards focused on managing 3rd party systems/devices deployed within SampCo

BTB recommends that SampCo continue to assess its information security posture through regular security assessment and testing by leveraging internal resources on an ongoing basis and third parties as a validation point when possible.

Assessment Results

The findings detailed in the following sections are a "snapshot in time" and do not landscape all potential vulnerabilities within the environment. Due to the dynamic nature of security vulnerability, not all potential vulnerability can be known at the time of testing, and no warranty can be made to the completeness of this list. BTB has made efforts to remove false positive findings and to draw conclusions based on observations made during this engagement. A strong information security program consists of active monitoring and regular assessment to identify emerging threats to information security.

All recommendations for remediation should be tested in a development environment before implementation. The resources required level depicts requirements for implementation of the recommendation, but may not take into account additional requirements set forth by change management, etc.

1 Definition of Risk Level

High	Immediate or unauthorized access to the system or information can be gained by direct exploitation of the vulnerability. Either the vulnerability requires no special programming code, or concept code, if needed, is readily available (from the Internet, etc.).
Medium	Immediate access may not be available by successful exploitation of the vulnerability, or concept code is not readily available. It is possible, however, that several other vulnerabilities can be combined to gain access to the system or sensitive information.
Low	No access is gained to sensitive information or the system, but the vulnerability can provide an attacker with information that can be used to further their attack.

Table 1 Risk Levels Defined

2 Definition of Resources Required for Remediation

High	Effort required for remediation is greater than one business week and/or requires a software or hardware purchase greater than $10,000 (USD).
Medium	Effort required for remediation is greater than one business day, but less than one business week and/or requires a software or hardware purchase less than $10,000 (USD).
Low	Effort required for remediation is less than one business day and requires no purchase of hardware or software

Table 2 Resources Required for Remediation Levels Defined

3 Detailed Findings

Index	Area	Finding	Affected	Business Risk	Recommendation	Risk Level	Level of Effort/Cost Required
1.1	Architecture	SampCo has not deployed a centralized logging or security monitoring solution. Identifying security events requires administrators to review local event logs on numerous hosts, many of which do not have sufficient storage to retain logs for more than one day.	N/A	Lack of this control makes it difficult for security administrators to detect and respond to threats to information security in a timely fashion.	Implement centralized event logging and correlation capabilities that alert on defined security threats as well as abnormal behavior occurring within the environment. The solution should be able to interpret log data from network, server, and application platforms.	**Medium**	**High**
2.1	Policy and Procedure	The noted host has been configured with an insecure default password value.	Internal: 10.0.0.23	This vulnerability may lead to unauthorized access to the device, and potentially modifying the configuration or gaining access to sensitive information stored within the host.	Configure a strong and unique username and password for each authorized user.	**High**	**Low**
2.2	Policy and Procedure	Sensitive information such as financial data, PHI, and personnel information used by Human Resources is stored on laptops that do have disk encryption and in several databases that store data for customer-facing web portal applications. A compromised database or system would result in the disclosure of this information.	Internal: Database servers Laptops	This vulnerability may lead to information disclosure in the event that a device is lost or stolen, or access to the affected databases is obtained.	Define encryption standards for data in transit and at rest. Apply encryption to all classes of data that warrant it based on the organizational data classification policy.	**Medium**	**High**

Assessment Results — *Detailed Findings*

Index	Area	Finding	Affected	Business Risk	Recommendation	Risk Level	Level of Effort/Cost Required
3.1	Vulnerability Management	The noted host(s) appears to be running a version of the Microsoft SMTP server that is vulnerable to information disclosure and denial of service (DoS) issues. The SMTP service does not properly process malformed DNS MX requests, which may allow an attacker to craft a request that causes the service to fail, creating a DoS. Additionally, the Microsoft SMTP service does not properly allocate memory, which may allow an attacker to craft SMTP commands (specifically STARTTLS) that results in the display of random fragments of email messages. Note that this vulnerability only affects hosts running the Microsoft SMTP service.	External: 127.0.0.23 127.0.0.80 127.0.0.128 Internal: 10.0.0.23 10.0.0.150	This vulnerability may be leveraged by an attacker to cause a denial of service attack against the affected hosts.	Microsoft has released an update (MS10-024) to address this issue, apply the update. See http://www.microsoft.com/technet/security/bulletin/ms10-024.mspx (Microsoft Security Bulletin)	**Medium**	**Low**

Assessment Results — *Detailed Findings*

Index	Area	Finding	Affected	Business Risk	Recommendation	Risk Level	Level of Effort/Cost Required
4.1	Application Development	The noted web server contains pages which are vulnerable to cross-site scripting (XSS) attacks. Cross-site scripting vulnerabilities become possible when the web server does not properly perform input validation on all user provided data. This allows a malicious user to insert characters (i.e., <, >, ') into web server input fields which are processed and possibly stored by the application. When a legitimate user later views the page containing the attacker's code, the user's web browser processes the malicious script.	External: 127.0.0.62 /search.aspx	This vulnerability may be leveraged by an attacker in a social engineering exercise to gain access to a user's session or to attack the end user.	Review the vulnerable pages and implement controls to review and sanitize all user provided input. Only server-side validation controls effectively review all user input, as attackers often circumvent client-side input sanitization. Analyze the types of data required by the application to determine specific requirements for special characters and code the application such that only known, non-malicious characters are interpreted by application code. In addition to data validation and sanitization, HTML encoding can be used on all user supplied output to ensure that potentially dangerous characters are encoded. For example, the less than symbol, <, would be represented as <.	**Medium**	**High**

Assessment Results — *Detailed Findings*

Index	Area	Finding	Affected	Business Risk	Recommendation	Risk Level	Level of Effort/Cost Required
5.1	Configuration	Windows cached logons is enabled to store the last interactive logon (i.e., console logon) to authenticate users in the event that the host cannot connect to the Domain Controller. Cached logons are enabled to cache 10 passwords by default. However, if an attacker obtains administrative access to the system (privileged account or software vulnerability), they may be able to obtain the hashes of the cached passwords, crack the password hashes offline, and gain access to cached domain credentials (including domain administrative accounts).	Internal: SAMPDOM hosts	This vulnerability may lead to unauthorized access to systems and data.	Disable cached logon for the hosts either by modifying the group policy, the local security policy, or registry. Using group policy is a preferred method since it is easier to apply consistent policy to all systems in the domain. Set the Windows security option 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' under Local Policies\Security Options to 0. Note: Certain systems like laptops and some mobile systems may require cached logons since they may not have a reliable connection to the domain controller to perform authentication of domain users. For those systems, set the cached logons to 1 and be sure the roaming user is the last to log into the system before it is disconnected from the domain.	**Medium**	**Low**

Index	Area	Finding	Affected	Business Risk	Recommendation	Risk Level	Level of Effort/Cost Required
5.2	Configuration	The SSLv3.0/TLSv1.0 protocols contain a weak CBC Mode vulnerability that may allow an attacker that is able to intercept network traffic to capture and decrypt sensitive information between the client and server. Exploiting this vulnerability requires a relatively sophisticated attack; however there are tools available to simplify the attack process.	External: 127.0.0.1 127.0.0.7 127.0.0.17 127.0.0.20	This vulnerability may lead to Information disclosure, including data and logon credentials	Upgrade to TLS v1.1 or v1.2 or disable CBC mode ciphers. Note that the TLS upgrade could break functionality with some clients or interaction with other services that do not yet support the newer protocol. Comprehensive testing should be performed to choose the most appropriate remediation.	**Medium**	**Medium**
5.3	Configuration	The IPSec VPN is configured to allow Aggressive Mode authentication. Using Aggressive Mode with a pre-shared key (PSK) allows the VPN pre-shared secret hash to be obtained. An attacker may mount an off-line dictionary or brute force attack and potentially crack the PSK hash and obtain the pre-shared key. PSKs are used for group authentication for an IPsec VPN, usually in addition to user authentication.	External: 127.0.0.1	This vulnerability may allow a remote attacker to gain access to SampCo's internal network via the VPN.	IKE Aggressive mode with pre-shared keys should be avoided where possible. Otherwise a strong pre-shared key should be chosen and changed periodically.	**Low**	**Low**
5.4	Configuration	The name server allows zone transfers to occur. The zone transfer feature is used to synchronize the domain (also called a zone) from the master server to the slave server(s). Only the slave name servers should be able to perform zone transfers.	External: 127.0.0.23 127.0.0.50	This vulnerability may lead to information disclosure that provides an attacker with additional targets.	The zone transfer feature should be restricted so that DNS servers can only perform a zone transfer with other DNS servers in the same domain. In the case of a single DNS server, simply disable zone transfer to prevent unauthorized users from exploiting this feature from a remote system.	**Low**	**Low**

Table 3 Detailed Findings

Appendix A – Sample Vulnerability Exploits

1 Cross Site Scripting

The `/search_results` CGI does not properly sanitize or encode user-supplied input that is reflected back to the user. This situation results in the ability to inject code or content into the query that can be used to execute client-side scripts in an unsuspecting victim's browser. The example below shows displaying the user's cookies back to the screen when the following query is made:

```
https://foo.myportal.local/search_result?cb35f<script>alert(document.cookie)</script
>b1ecca54a9d=1
```

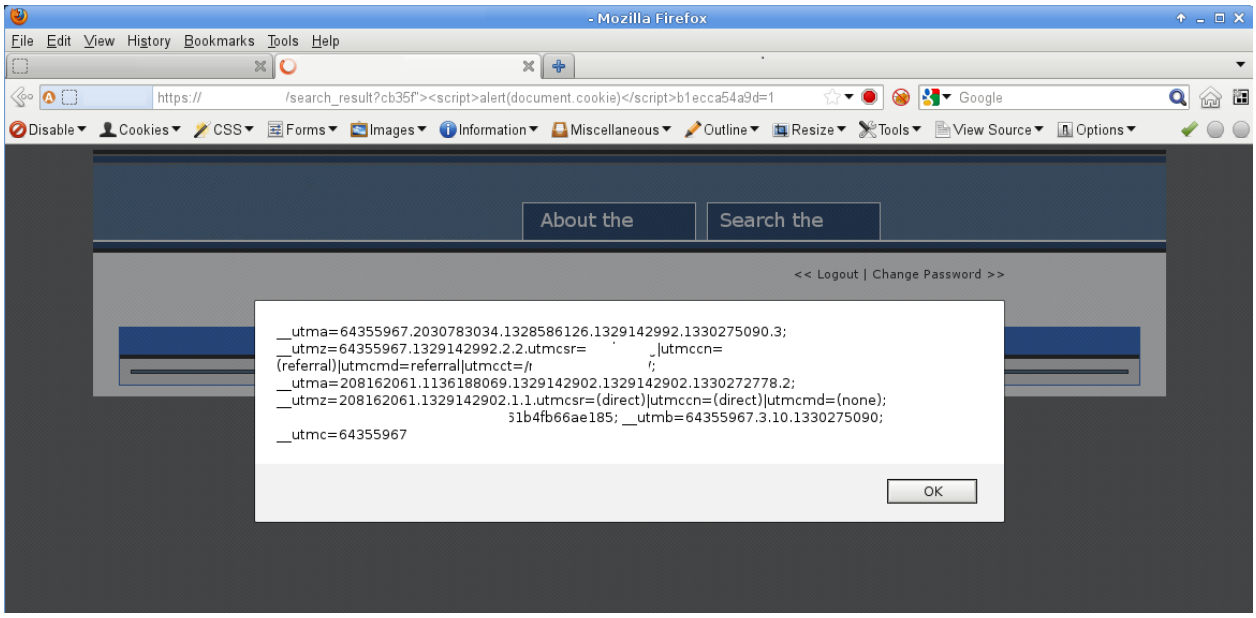

Figure 3 Cross Site Scripting Vulnerability

Appendix B - Targets

1 Scanning Targets

- 10.0.0.0/24
- 192.168.50.0/24
- 127.0.0.0/24

2 System Configurations

- SampCoDC01
- SampCoDC02
- SampCoApp01
- SampCoApp02
- SampCoDb01
- SampCoDb02
- SampCoFile01
- SampCoSNMP01

3 Network Devices

- SampCoRtr01
- SampCoSw01
- SampCoFW01
- SampCoFW02

Appendix C - Interviews

Topic	Date	SampCo Attendees	BTB Attendees
Security Management	Jan 1, 2012	SampCo Employee	BTB Consultant
Microsoft Windows	Jan 1, 2012	SampCo Employee	BTB Consultant
IBM AIX	Jan 1, 2012	SampCo Employee	BTB Consultant
Network Architecture	Jan 1, 2012	SampCo Employee	BTB Consultant
Application Development	Jan 1, 2012	SampCo Employee	BTB Consultant
Help Desk	Jan 1, 2012	SampCo Employee	BTB Consultant

Table 4 Interviews

Appendix D – Internet-Facing Services

IP	Hostname	Port	Protocol	Typical Service
127.0.0.1	127-0-0-1.localdomain	22	tcp	ssh
127.0.0.1	127-0-0-1.localdomain	443	tcp	https
127.0.0.1	127-0-0-1.localdomain	541	tcp	uucp-rlogin
127.0.0.5	127-0-0-5.localdomain	21	tcp	ftp
127.0.0.5	127-0-0-5.localdomain	22	tcp	ssh
127.0.0.5	127-0-0-5.localdomain	990	tcp	ftps
127.0.0.7	127-0-0-7.localdomain	443	tcp	https
127.0.0.10	127-0-0-10.localdomain	21	tcp	ftp
127.0.0.10	127-0-0-10.localdomain	22	tcp	ssh
127.0.0.10	127-0-0-10.localdomain	443	tcp	https
127.0.0.13	127-0-0-13.localdomain	443	tcp	https
127.0.0.17	127-0-0-17.localdomain	80	tcp	www
127.0.0.17	127-0-0-17.localdomain	443	tcp	https
127.0.0.20	127-0-0-20.localdomain	443	tcp	https
127.0.0.20	127-0-0-20.localdomain	6001	tcp	cisco-6001
127.0.0.23	127-0-0-23.localdomain	53	tcp	domain
127.0.0.23	127-0-0-23.localdomain	53	udp	domain
127.0.0.28	127-0-0-28.localdomain	80	tcp	www
127.0.0.28	127-0-0-28.localdomain	443	tcp	https
127.0.0.41	127-0-0-41.localdomain	443	tcp	https
127.0.0.43	127-0-0-43.localdomain	80	tcp	www
127.0.0.43	127-0-0-43.localdomain	443	tcp	https
127.0.0.44	127-0-0-44.localdomain	443	tcp	https
127.0.0.46	127-0-0-46.localdomain	80	tcp	www
127.0.0.46	127-0-0-46.localdomain	443	tcp	https
127.0.0.47	127-0-0-47.localdomain	80	tcp	www
127.0.0.47	127-0-0-47.localdomain	443	tcp	https
127.0.0.49	127-0-0-49.localdomain	80	tcp	www
127.0.0.49	127-0-0-49.localdomain	443	tcp	https
127.0.0.50	127-0-0-50.localdomain	53	tcp	domain
127.0.0.50	127-0-0-50.localdomain	53	udp	domain
127.0.0.51	127-0-0-51.localdomain	443	tcp	https
127.0.0.57	127-0-0-57.localdomain	80	tcp	www
127.0.0.57	127-0-0-57.localdomain	443	tcp	https
127.0.0.67	127-0-0-67.localdomain	80	tcp	www
127.0.0.67	127-0-0-67.localdomain	443	tcp	https
127.0.0.70	127-0-0-70.localdomain	80	tcp	www
127.0.0.70	127-0-0-70.localdomain	443	tcp	https
127.0.0.79	127-0-0-79.localdomain	80	tcp	www
127.0.0.79	127-0-0-79.localdomain	443	tcp	https
127.0.0.83	127-0-0-83.localdomain	80	tcp	www
127.0.0.83	127-0-0-83.localdomain	443	tcp	https

Table 5 Internet-Facing Services