Global Information Assurance Certification Paper

Network Vulnerability Assessment Strategy for Small State and Local Government Agencies

Prepared for:

SANS GIAC
Auditing Networks, Perimeters, and Systems (GSNA) Practical Assignment
Version 2.1 (amended July 5, 2002)
Option 2 – Permission Granted

Location of Course Work:

SANS FIRE Boston, MA June 2002

Prepared by:

Ken Sweltz

November 17, 2002

TABLE OF CONTENTS

Page

CASE STUDY

CASE STUDY SAMPLE REPORT

1.0 BACKGROUND

1.1 Document Abstract/Summary

This paper provides a strategy to perform Network Vulnerability Assessments (NVA) for small state and local government agencies. A framework is discussed that allows for tailoring existing standards or methodologies to accommodate the budget, schedule, and personnel constraints of these agencies. This includes the following:

- **NVA Strategy.** The main body of the document provides the strategy to perform a NVA for small state and local government agencies. This is divided into the following sections:
  - Background - provides an overview of the topic
  - Target Organization Overview – discusses information about small state and local agencies
  - Applicability of Existing Assessment Methodologies and Standards – discusses examples of existing methodologies that can be used with this strategy
  - Assessment Activities – provides details of assessment activities and tools
  - Conclusion – provides a summary of what was discussed in this paper.
- **Case Study.** A case study based on an implementation of the NVA Strategy is found in Appendix A. This appendix includes tabs that contain a case study sample report, detailed results summary, detailed results, an organizational questionnaire, and a services and confidentiality agreement.
- **Nominal Schedule.** A nominal schedule to perform a tailored NVA for state and local agencies is found in Appendix B.
- **HTML Report Index.** A sample format for an HTML report index is provided in Appendix C.
- **Acronyms.** Acronyms used in this paper are found in Appendix D.
- **References.** Sources used in this paper are found in Appendix E.

1.2 Purpose

The purpose of this document is to discuss a network vulnerability assessment strategy that is tailored for the unique needs of small state and local government agencies. Many local and state entities need outside assistance in dealing with cyber risks and would clearly benefit from a network vulnerability assessment and information assurance solution service. An area of particular importance is support for local area emergency responders. According to the July 2002 "National Strategy for Homeland Security" emergency response will be increasingly dependent on compatible communications and an information technology (IT) infrastructure. [1] Other examples include city and county governments that require IT services that are secure and reliable. This includes protection measures for public web sites and ensuring the confidentiality and integrity of sensitive information such as court proceedings and tax

[1] Office of Homeland Security. "The National Strategy for Homeland Security." July 16, 2002. URL: http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf. page xi.

records. Small agency networks are especially susceptible to hackers and can be used as part of larger cyber attacks, criminal activities, and pornographic distribution schemes.

1.3 Overview

The rapid and dramatic increase in IT has generated tremendous benefits. In today's environment, almost every organization is dependent on a network-centric IT infrastructure. State and local agencies that serve the public in critical areas such as emergency response, homeland defense, government, commerce, finance, health care, and public utilities rely on a variety of hardware and software solutions to develop, track, and exchange information. Along with the substantial benefits in the use of IT have also come significant and unprecedented risks in dealing with an increasing number of vulnerabilities and threats. The vulnerabilities include poorly written software, failure to properly apply patches, lack of encryption, weak user security practices, and insufficient physical protection measures. The threats exploiting these vulnerabilities include external cyber attackers, hackers within an organization, and malicious software such as Code Red and NIMDA.

Cyber incidents are increasing in number, sophistication, severity, and cost. The 2002 Computer Crime and Security Survey—conducted by the Computer Security Institute (CSI) and the Federal Bureau of Investigation (FBI)—indicates "that the threat from computer crime and other information security breaches continues unabated, and that the financial toll is mounting."[2] The impact of cyber incidents can cause delays in emergency response, disruption of critical operations, fraudulent use of government resources, financial loss, and exposure of confidential information. In many cases, the interdependencies in our IT infrastructure and how well it will function often are not known until a crisis or disaster occurs.

Because of limited resources and expertise, state and local agencies to include emergency response centers, city and county offices, and public schools are especially vulnerable to cyber risks. A recent International City/County Management Association (ICMA) survey indicated more than half of local governments do not have polices and procedures in place for Web-site security.[3] According to a December 2001 report by the National State Auditors Association and the United States General Accounting Office, typical weaknesses in local and state organizations include:

- Lack of formal security policies that result in haphazard reactions to incidents
- Inadequate configuration management of software programs
- Lack of security awareness
- Inadequate technical staff to address security problems
- Failure to use industry best security practices

[2] Computer Security Institute Press Release. "Cyber crime bleeds U.S. corporations; financial losses from attacks climb for third year in a row." April 7, 2002 2002. URL: http://www.gocsi.com/press/20020407.html.

[3] International City/County Management Association. "Electronic Government 2002 Survey Results, Question 10c." URL: http://icma.org/download/cat15/grp120/sgp224/egov2002web.pdf. page 3.

- Failure to properly update antivirus software
- Inadequate business continuity and disaster recovery planning.[4]

The increasing reliance on a network-centric IT infrastructure requires a vigilant and aggressive approach to identify the vulnerabilities and counteract the threats. According to the September 2002 "National Strategy to Secure Cyberspace" document, the cost of a severe computer attack can be greater than the preemptive investment in an information assurance program to identify the vulnerabilities and perform corrective actions.[5] Everyone must act to secure their parts of cyberspace. A July 2002 report for the National Association of State Chief Information Officers on public-sector information security stated, "It is crucial that organizations evaluate the positive aspects and shortcomings of their current security program, and then design improved programs to meet organizational needs."[6]

2.0 TARGET ORGANIZATION OVERVIEW

2.1 Description of the Target Organization

The target organization that this paper addresses is a small state or local public organization; e.g., school districts, county and city governments, and emergency responders such as police and fire departments. The scope of their IT infrastructure is usually very limited. Typically it would be less than 100 hosts, an Internet connection, possibly a small DMZ with email and web servers, and some application servers. They usually have one or two IT staff supporting their entire infrastructure and often rely on outsourcing to handle non-routine technical issues and perhaps to do their web hosting. The motivation and dedication of the IT professionals is good but they often don't have the experience and time to handle both keeping the network up and implementing a good security architecture. What I have found is that personnel in these organizations need help, but based on schedules and budgets what can be provided is typically very limited. Even in "pro bono" situations, they are often so overburdened that they can't commit enough of their own time to accommodate outside assistance.

2.2 Importance of a NVA for Small State and Local Agencies

"The National Strategy to Secure Cyberspace" states, "… all critical infrastructure and cyberspace protection plans and actions shall take into consideration the needs, activities, and responsibilities of State and local governments and first responders."[7] The closest relationship we will have with our government is at the local level. State and local agencies provide or coordinate much of the key infrastructure we use

[4] National State Auditor's Association and U.S. General Accounting Office. "Management Planning Guide for Information Systems Security Auditing." December 10, 2001. URL: http://www.gao.gov/special.pubs/mgmtpln.pdf. pages 4-5.
[5] The President's Critical Infrastructure Protection Board. "The National Strategy to Secure Cyberspace." September 2002. URL: http://www.whitehouse.gov/pcipb/cyberstrategy-draft.pdf. page 5.
[6] Heiman, Don. "Public-Sector Information Security: A Call to Action for Public-Sector CIOs." July 23, 2002. URL: http://endowment.pwcglobal.com/pdfs/HeimanReport.pdf. page 3.
[7] The President's Critical Infrastructure Protection Board. "The National Strategy to Secure Cyberspace." September 2002. URL: http://www.whitehouse.gov/pcipb/cyberstrategy-draft.pdf. page 8.

everyday and that is especially needed in the time of crisis. This includes government services, utilities, police, and emergency response. All these organizations rely on a network centric information technology infrastructure to support them and communicate with us. This IT infrastructure can include everything from controlling the power grid to providing access to key data repositories. Since much of this infrastructure is so interdependent, it is often difficult to predict what the impacts will be when a portion becomes unavailable. That is why it is so critical that all reasonable measures be taken to protect it**.** The following are some of the most important reasons why these agencies need to assess and improve the security of their networks:

- Regulatory Compliance. In some instances agencies are required to perform audits in order to comply with local and state regulations and laws.
- Maintain Public Confidence. All state and local agencies serve the public in some capacity. A web site defacement or interruption of electronic services can impact the public's confidence in the agency's abilities to properly perform their functions.
- Prevent Financial Loss. Many agencies complete public and agency financial transaction via the web. An example is the issuing of driver's, hunting, and fishing licenses via credit card transactions. These sites and transactions must remain secure to prevent financial loss.
- Emergency Response. Emergency response is primary provided by local governments. These responders increasingly rely on information technology for communication and information sharing. It is imperative that they have secure and compatible data and communication systems in place.
- E-Government. Many state and local government agencies are using data communications to perform the functions of government. This includes information dissemination, online services, and even public voting. The trend is to provide more e-government services. This will require additional emphasis on having a secure information technology infrastructure.

2.3 Challenges for State and Local Agencies

The dilemma for state and local agencies is that our IT architecture has a seemingly endless number of vulnerabilities that include such things as buffer overflows, improperly secured data, and input validation issues on web sites. I have seen first hand how difficult it is for even the most dedicated and professional network engineer in small local agencies to keep a network both operational and secure. At the same time that they are trying to keep their networks and IT assets operational and available, they must also protect them against an increasing number of threats. They face attacks from a growing number of individuals. The attack hierarchy includes click or script kiddies who may not have a truly malicious intent but still can cause a huge number of problems. They must also deal with more sophisticated attackers who engage in industrial espionage, fraud, and organized crime activities. They also face the possibility of an asymmetrical threat from a rouge state or a cyber terrorist. In addition, they have to deal with crisis or disaster that can be natural or manmade.

Our state and local agencies face a number of challenges. They will be the first to respond and the last to leave. In time of crisis, there may be competing jurisdictions, difficulty in exchanging information, and unclear chains of command. For example, during the Columbine shooting over 23 local agencies along with two State and three Federal agencies responded to the incident.[8] All of this is compounded by financial and personnel constraints that are much more challenging than what Federal agencies or private industry have to deal with. This includes salaries that are less competitive than what is offered in the private sector. As a result, it is difficult to attract the top talent. In some cases there is a misconception by agency management that because of their small size they won't be targeted for attack. In other cases, agencies have a misunderstanding that because firewalls or other limited security measures are being used that they are totally secure.

3.0 APPLICABILITY OF EXISTING ASSESSMENT METHOLOGIES AND STANDARDS

3.1 Overview

The strategy discussed in this paper is not bound to any specific existing standard or methodology and it is not my intent to replace any of these. Rather, I want to provide guidance on how to draw useful aspects from them that can be applied to small state and local agencies. As with all things, this requires compromise. Because the target organization I have identified is often severely bound by schedule, personnel, and budget constraints, the focus has to be on protecting the most critical assets and prioritizing solutions. As a result, it is often only feasible to use a select subset of ideas or controls form any standard. In addition, much of the information gathered is through an interview process with only a technical hands-on review of select devices. Although the assessment has to be tailored and bound, significant improvement of the agency's security posture can still be achieved. This is because the "as is" security posture is so poor that even a tailored approach will provide big rewards. Based on research and personal experience, I will provide a framework for a tailored assessment strategy to fit the needs of small state and local government agencies.

3.2 Existing Methodologies, Standards, and Checklists

The following are examples of some existing methodologies that can be applied to small state and local government agencies. I provide this only as a starting point and concede there are many other choices available.

3.2.1 Control Objectives for Information and related Technology (COBIT) â

The Information Systems Audit and Control Association (ISACA) is the source for COBIT. COBIT contains best practices across a domain and process framework with an emphasis on business orientation. The COBIT Framework has 34 high-level control

[8] Office of Homeland Security. "The National Strategy for Homeland Security." July 16, 2002. URL: http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf. page 56.

objectives and 318 detailed control objectives that are mapped to the following four domains:

- Planning and organization
- Acquisition and implementation
- Delivery and support
- Monitoring.[9]

COBIT's generally accepted control objectives apply to personal computers, mini-computers, mainframes, and distributed environments.[10] COBIT is particularly useful to state and local agencies for "bridging the gaps between business risks, control needs and technical issues."[11] For information about downloading COBIT go to http://www.isaca.org/ct_dwnld.htm.

3.2.2 INFOSEC Assessment Methodology (IAM) and Information Assurance – Capability Maturity Model (IA-CMM)[12]

The IAM is produced under the auspices of the National Security Agency (NSA). The IAM consists of the following baseline activities:

- Analyzing information criticality
- Identifying customer concerns
- Producing an assessment plan
- Gathering information through interviews, documentation review, and system demonstrations in 18 categories (examples include: account management; auditing; virus protection; contingency planning; and back-ups)
- Providing a documented report with findings and recommendations.

The IAM methodology is particularly useful for its' approach to risk assessment and the identification of critical data. This is discussed in more detail in section 4. Also the IAM emphasis on interviews and policy reviews is often a good approach to take when agencies have very limited funding.

The IA-CMM is based on the System Security Engineering Capability Maturity Model and focuses on an assessment organization's ability to properly perform INFOSEC assessments using the IAM. The IA-CMM contains nine process areas and an organization is graded using a capability maturity model rating from Level 0 to Level 5. These ratings can be used by organizations seeking assessment assistance to guide them to quality assessment organizations.

If state or local agencies require some type of proof that an assessor is credible, an IA-CMM maturity level will be useful in making their selection.

More information about IAM and IA-CMM is available at http://www.iatrp.com/.

---

[9] "COBIT®. 3rd Edition Executive Summary." July 2002. pages 3-12.
[10] "COBIT FAQ." URL: http://www.isaca.org/faq_r.htm#r3.
[11] "COBIT. 3rd Edition Executive Summary." July 2002. page 3.
[12] "IA-CMM Capability Maturity Model. Version 2.1. February 2002. URL: http://www.iatrp.com/. pages 7-9.

3.2.3 Computer Security Institute (CSI) Information Protection Assessment Kit (IPAK) [13]

The CSI IPAK is a toolkit that contains security controls in 11 categories; e.g., physical security; backup and recovery measures; web security; and Internet commerce. Each of the 11 categories contains 20 controls along with a grading criteria from 1 to 10 for each control. The IPAK comes both in printed copy and as an Microsoft® Excel® spreadsheet for automated scoring.

Because the CSI IPAK has all the controls listed in hard copy format ready for manual grading or in an Excel spreadsheet for automatic grading, this is an economical and quick means to determine control compliance for state and local agencies.

The IPAK toolkit is sold for approximately $197. For more information refer to https://wow.mfi.com/csi/order/publications.html.

3.2.4 International Standards Organization (ISO)/ International Electrotechnical Commission (IEC) 17799[14]

ISO/IEC 17799 is an internationally recognized standard that provides a set of controls for best information technology security practices. ISO/IEC 17799 provides guidance on the following 10 areas:

- Security Policy
- Organizational Security
- Asset Classification and Control
- Personnel Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Systems Development and Maintenance
- Business Continuity Management
- Compliance

This standard has great background information that can be used to prepare for an assessment. There are also toolkits available for sale that include security policies and audit checklists. I have not personally reviewed any of these toolkits, but they are a possible source to use when performing an assessment.

One source to obtain a copy of the standard is http://www.ihs.com/index.html.

3.2.5 Open-Source Security Testing Methodology Manual (OSSTMM)[15]

As implied by the name this is an open source methodology. It is based on the idea that security testing should be done from an "unprivileged" perspective; i.e., from the outside

[13] "CSI Publications: CSI IPAK." URL: https://wow.mfi.com/csi/order/publications.html.
[14] "ISO/IEC 17799." First Edition. December 12, 2000.
[15] Herzog, Pete. "Open-Source Security Testing Methodology Manual." Release 2.0 Candidate 6. February 26, 2002. pages 4-16.

to the inside. This means the assessor has no special access or permissions. The OSSTMM does include risk assessment steps. The manual is written for someone experienced in security testing with a focus on what should be tested and in what order. The OSSTMM covers the following six areas:

- Internet Security
- Information Security
- Social Engineering
- Wireless Security
- Communications Security
- Physical Security.

Although I have not personally used this manual in the actual performance of an assessment, I find the format very appealing. The identification of expected results and the tasks to perform to meet each test objective provides useful guidance to a more experienced auditor who would want to use it to support this strategy.

For a copy of OSSTMM go to http://www.ideahamster.org/download.htm.

3.2.6 Security Consensus Operational Readiness Evaluation (SCORE)

SCORE is a joint effort between SANS and the Center for Internet Security (CIS). SANS, CIS and other security professionals have developed a minimum set of standards and best practices. There are a variety of checklists on the SCORE web site (http://www.sans.org/SCORE/) to include those on Windows NT; Windows 2000; UNIX; Linux; Handhelds; Cisco devices; firewalls; and web applications.[16] On the CIS web site (http://www.cisecurity.org/) there are a variety of benchmark and scoring tools available. The CIS benchmarks provide security configuration settings and steps to secure your system. There are two levels of benchmarks:

- CSI Level-I. This is for system administrators with limited experience and would be good for those working at small state and local organizations. The use of these benchmarks is non-invasive and CIS Scoring Tools can monitor them.
- CIS Level-II. These are for more experienced system administrators who can apply them to fit their own unique networking environments.

The CIS Scoring tools provide a means to assess networks against the CIS Benchmarks.[17]

The checklists, benchmarks, and scoring tools are valuable and can be used with this strategy as a source of controls, guidelines, and verification when auditing a system.

3.2.7 National Institute of Standards and Technology (NIST) Special Publications

NIST has a variety of resources available for information security professionals primarily through their Computer Security Resource Center (CSRC). One document that is particularly useful and relevant to NVAs is the NIST Special Publication 800-26: Security Self Assessment Guide for Information Technology Systems. This publication contains a large number of security related questions that can be asked on an

[16] "SCORE Website." URL: http://www.sans.org/SCORE/.
[17] "CIS Website (Use the "What are the benchmarks?" link)." URL: http://www.cisecurity.org/.

assessment. The questions are divided into three major control areas that include Management Controls; Operational Controls; and Technical Controls. These major control areas are further sub-divided into a total of 17 control areas. The questions are rated on five levels from Level 1 – control objective documented in a security policy to Level 5 – procedures and security controls are fully integrated into a comprehensive program.[18]

NIST is also currently in the process of establishing a standard process to certify and accredit IT systems within the federal government. The guidelines for this process will be in NIST Special Publication 800-37: Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems; NIST Special Publication 800-53: Minimum Security Controls for Federal Information Technology Systems; and NIST Special Publication 800-53-A: Techniques and Procedures for the Verification of Security Controls in Federal Information Technology Systems. Related guidelines that are an integral part of this process are NIST Special Publication 800-30: Risk Management Guide for Information Technology Systems and NIST Special Publication 800-18: Guide for Developing Security Plans for Information Technology Systems. NIST Special Publication 800-37 was released in draft form on October 28, 2002 for comment. NIST Special Publications 800-53 and 800-53A are pending release in draft form.

The following is some additional information on these guidelines:

- SP 800-37. Defines the standardized security certification and accreditation process for IT systems.
- SP 800-53. Defines the standardized information technology controls for confidentiality, integrity, and availability.
- SP 800-53A. Defines standardized techniques and procedures to verify correctness and effectiveness of security controls.
- SP 800-18. Provides guidance on developing a security plan
- SP 800-30. Provides guidance on a risk assessment process related to security assessments.[19]

Although the SP 800-37 has just been recently released in draft format, I have attended NIST briefings on this process and believe this process will provide very useful guidance and applicable controls not only for the intended federal agencies but for small state and local agencies as well.

More information on NIST Special Publications 800-37, 800-53, and 800-53A can be obtained at http://csrc.nist.gov/sec-cert/.

---

[18] Swanson, Marianne. "NIST Special Publication 800-26: Security Self Assessment Guide for Information Technology Systems." August 2001. URL: http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf. pages 1-12.

[19] Ross, Ron and Swanson, Marianne. "Draft: NIST Special Publication 800-37: Guidelines for the Security and Accreditation of Federal Information Technology Systems." Version 1.0. October 2002. URL: http://csrc.nist.gov/sec-cert/SP-800-37-v1.0.pdf. pages viii - 6.

4.0 ASSESSMENT ACTIVITIES

4.1 Overview

When it comes to assessments, one size does not fit all. Each assessment will be performed based on the size of the organization and their budget and time constraints. At the beginning of the process questionnaires and interviews can be used to scope and bound activities and a risk assessment and identification of critical assets performed to ensure the highest priority systems are reviewed first. Based on this initial process, detailed checklists are developed to provide the baseline against which performance will be measured.

It is best if the assessment team and personnel from the assessed organization work together in a cooperative manner. Non-attribution is usually a good thing. The goal is to improve the security posture of the agency and not to fix blame. Finally an actionable report should be presented at the end. This report must summarize all the raw data that was generated. High level findings and key issues should be articulated for senior managers with hyperlinks to details, raw scanning results, and patches for those interested in technical specifics.

When performing an assessment consider doing the following:

- Holistic approach that looks at process, people, and technology
- Tailored approach based on the needs and constraints of the agency involved
- Risk analysis and identification of critical assets for use in the development of a prioritized list of assessment areas and targeted devices
- Interviews with key managers, engineers, and users
- Policy and procedural reviews including checks for best practices and determination of compliance levels within the organization
- Internet exposure analysis to determine public availability of information
- War dialing to identify open modems that may be circumventing security boundaries
- War driving to identify wireless vulnerabilities and exposure to unauthorized users
- Network mapping and vulnerability scanning to include host discovery, identification of services and open ports, and validation that updated security patches are installed
- Device assessment and log review to identify vulnerabilities and insecure configurations
- Web and database analysis to identify vulnerabilities and development flaws
- Virus detection reviews to determine compliance with best practices and verify the use of updated anti-virus software
- Password checking to determine compliance with recommended best practices and to test the susceptibility of password files to cracking
- Submission of a detailed report with findings, recommendations, applicable references, and resources.

Throughout the performance of the above activities, the assessment team must assure the agency that there is complete confidentiality of all information gathered.

4.2 Information Gathering Techniques

Prior to gathering information it is important that the agency's senior management has provided permission for the activities you will perform. This can usually be done via services and confidentiality agreements. I have provided a simple example in Tab 5 to Appendix A. Most organizations that perform assessments will have their own proprietary forms to do this that contain much more legalese.

The NSA has a Vulnerability Discovery Triad consisting of three levels. Level One: Assessments is primarily programmatic and is focused on identifying critical systems, reviewing documentation, and conducting interviews. Level Two: Evaluations is more hands on and involves scanning and spending more time with the technical aspects of the network. Level Three: Red Teaming is very technical and involves penetration testing.[20] My recommended approach for assessments of small state and local agencies is to complete Level One activities and do as much Level Two activity as the budget and schedule allow.

After working with the agency's technical team to bound the scope of the assessment and when applicable service and confidentiality agreements have been signed, it will be time to start gathering information. The first step will be the use of an organizational questionnaire to gain background information so that the assessment can be further tailored and the personnel with the right skills can be selected to be on the assessment team. An example of a questionnaire is contained in Tab 4 to Appendix A. Along with the questionnaire, the collection of existing network diagrams or network maps will provide useful information. However, most small organizations will lack these diagrams. In addition, any information supplied on the questionnaire will have to be verified during the actual performance of the assessment. Sometimes network administrators will not know the answers to the questions or will provide incorrect data.

The next thing to do is obtain any existing security and network policies and procedures. It is useful to review these prior to the actual onsite assessment so that you can compare what an agency says it should be doing to what has actually been done. Once onsite, information will be collected through interviews, review of log files, system demonstrations, performing network mapping and vulnerability scans, using password-cracking tools, and conducting war dialing.

Some examples of key individuals to interview would include:

- Agency Heads
- Network Administrators
- Security Administrators
- Database Administrators

[20] "IA-CMM Capability Maturity Model. Version 2.1. February 2002. URL: http://www.iatrp.com/. page 6.

- Managers
- Users
- Web Developers
- Human Resources Personnel
- Physical Security Manager/Guards

Some examples of key documents to review include:

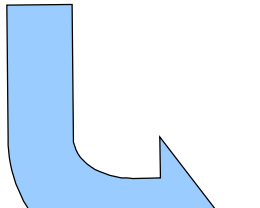
- Security Plan
- Security Procedures
- Test Plans
- User Guides
- Disaster Recovery Plan
- Business Continuity Plan
- Training Plans
- Network Diagrams
- Configuration Management Plans
- Human Resources Policy

4.3 Risk Analysis and Identification of Critical Assets

Because you will be working under budget and schedule constraints, it is important to identify the critical data and assets so checks can be made on their security first. The risk assessment and identification of critical assets should not be an end in itself. It should be a means to facilitate the remainder of the assessment. This is a pre-assessment activity that should be done in one day or less.

The first step is to identify the critical data, determine what system it is part of, and determine the impact if the risk occurred. Criteria such as confidentiality, integrity, and availability can be used; e.g., if the confidentiality of data in a performance review is compromised it would have a high impact on the organization. Precise objective definitions can be developed for what constitutes a high, medium, and low impact. However, because of the constraints in which this strategy must be executed, it is usually sufficient to obtain a subjective consensus of the agency's participants. Following this, the level of risk for each system is determined by the highest level of risk for any critical data on that system. Figure 1 contains an example of this process and this is also done in the risk assessment section of the case study in Appendix A. [21]

Critical Data	System	Confidentiality	Integrity	Availability
Performance Reviews	**HR**	**High**	**High**	**Medium**
Pay Records	**Payroll**	**High**	**High**	**High**
Office Supplies	**Inventory**	**Low**	**Medium**	**Low**
Computer Widgets	**Inventory**	**Low**	**High**	**Medium**



System	Confidentiality	Integrity	Availability
HR	**High**	**High**	**Medium**
Payroll	**High**	**High**	**High**
Inventory	**Low**	**High**	**High**

As discussed in section 3.0 there are numerous existing methodologies that can be tailored to provide controls or questions that can be used on an assessment of small state and local government agencies.

To be successful, a comprehensive review must be conducted. The following four high-level areas need reviewed:

- Policy and Procedures
- Technology
- People
- Physical Security Measures

The best place to start the assessment will be to identify and review any existing security policy and procedures and use this as a basis to determine the level of compliance throughout the remainder of the assessment. In many cases this will be an area of evident weakness with small state and local agencies. There will often only be policies and procedures of very limited scope. However, because of the large number of example policies available from organizations like SANS this is also an area that can be quickly and easily remedied as a follow-on activity.

The technical reviews will be an important part of the assessment. Because of the constraints of the assessment, the emphasis must be on priority items and choosing a good subset of network devices that exemplify the organization. Examples of the technical areas will include reviewing access control lists on routers, performing vulnerability scans, reviewing log files, checking intrusion detections systems, etc.

It is very important to check physical measures. This would include the use of badges, locks, and guards. It would also include looking at areas such as surge protection, backup electrical power, and protection from natural disasters.

Perhaps the most susceptible area in our security posture is the people who use it. The "Human Firewall Manifesto" stresses that IT is not just a technology concern but is also a people issue.[22] In the end despite all other measures, people can knowingly or unknowingly compromise your system. This is comparable to our highway infrastructure. Even though we design safe vehicles and have properly engineered roads, these will not protect us from the individual who dangerously exceeds speed limits, talks on their cell phone during rush hour traffic, or drives drunk. Damage that can be caused by network users can either be deliberately malicious as in the case of an insider attack or unintentional as in the case of a user posting their password near their computer.

The following are examples of specific technical and programmatic areas that can be assessed (In the case study in Appendix A, I illustrate the use of 13 of these areas).

[22] "The Human Firewall Manifesto." URL: http://www.humanfirewall.org/rhfwm.htm.

Auditing	Accounts and Passwords
Anti-Virus	Assessments
Authorization	Backup and Recovery
Business Continuity Planning	Database Security
Disaster Recovery Planning	Encryption
Firewalls	Intrusion Detection Systems
Incident Handling	Internet Security
Personal Digital Assistants	Personnel
Physical Security	Public Key Infrastructure
Remote Access	Risk Management
Routers and Switches	Security Policy and Procedures
War Dialing	Web Applications
Windows Systems	Wireless
UNIX and Linux Systems	Virtual Private Networks

4.5 Nominal Schedule

Because of budgetary and schedule constraints, a typical assessment needs to be completed over an approximate ten day period. This does not mean ten full days of work for all individuals. The actual onsite work will normally require less than one day of risk analysis and identification of critical assets and three days or less of assessment activities. The remainder of the time will be spent setting scope, establishing service agreements, gathering preliminary information, compiling reports, and presenting in-briefs and out-briefs. Appendix B has an example of a nominal schedule that can be used for an assessment. The schedule is divided into pre-assessment, assessment, and post-assessment activities.

4.6 Team Organization

4.6.1 Overview

The NVA team should be composed of individuals with both programmatic and technical skills. This will allow for management of the NVA; reviews of management and operational type controls; and review of technical controls. If possible, it is best if team members are cross-trained and have the ability to perform any function on the team. It is best to have engineers who are experienced with both network and security matters. Examples of the technical skills needed include:

- Microsoft Windows host and server platforms
- *NIX server and host platforms
- Email servers and clients
- Firewalls, routers, and switches
- Intrusion detection systems
- Database applications
- Web applications
- Vulnerability scanners
- Wireless applications
- Incident handling and incident analysis

4.6.2 Roles and Responsibilities

A team should be composed of four to five members. Sometimes it may only be necessary to have a team member with specialized skills (e.g., database or web developer) participate for only a portion of the assessment. The following are the roles and responsibilities for a nominal team.

a. Team Leader

- Responsible for overall performance to meet project requirements including technical, schedule, and cost
- Provides oversight and assistance to all assessment team members
- Negotiates commitments and performs planning with the agency being assessed
- Performs assessment activities with a focus on management and operational type controls
- Augments the engineering team in more technical assessment areas as required
- Prepares the assessment report and is the lead for in-briefs and out-briefs
- Performs quality assurance reviews of work products

b. Lead Engineer

- Assists the Team Leader in overseeing the performance of an assessment
- Serves as lead for technical areas of the assessment
- Performs reviews of assigned areas during an NVA
- Provides guidance and assistance to the Engineering Group
- Contributes to and assists in the completion of the assessment report

c. Engineering Group (Size and skills dictated by scope of NVA)

- Provides systems, network, and security engineering support
- Participates in the performance of the NVA on assigned technical areas; e.g., UNIX systems; Windows systems; network devices; security devices; database applications, Web applications, etc.
- Contributes to and assists in the completion of the assessment report

d. Technical Writer (Optional. Team Leader may do these functions.)

- Assists in the preparation of the assessment report
- Reviews presentations and reports prior to delivery to the agency

4.6.3 Task Responsibility Matrix

It is recommended that work be assigned using a Task Responsibility Matrix. An example of such a Task Responsibility Matrix can be found in the case study.

4.6.4 Training Requirements

In order to perform professional and credible NVAs, the NVA team must be trained and certified in both programmatic and technical areas. The performance of an NVA requires personnel with specialized technical and programmatic skills; e.g., project management, network operations, network management, network modeling, and information assurance. These skills need to be developed through both operational

experience and quality training. Table 1 provides an example of the types of training needed.

Table 1: Sample Training Matrix

Course/Certification C – Certification Required P – Training Preferred R – Training Required	Team Leader	Technical Lead	Engineering Group*
Project Management Professional (PMP)	C		
Certified Information Systems Auditor (CISA)	C		
Certified Information Systems Security Professional (CISSP)	C	C	C
SANS GIAC Certified Incident Handler (GCIH)	C	P	P
SANS GIAC Security Essentials Certification (GSEC)	P	P	P
SANS GIAC Certified Intrusion Analyst (GCIA)	P	C	P
SANS GIAC Certified Windows Security Administrator (GCWN)			C
SANS GIAC Certified UNIX Security Administrator (GCUX)			C
SANS GIAC Systems and Network Auditor (GSNA)	C	P	P
SANS GIAC Certified Firewall Analyst (GCFW)		P	C
Microsoft Certified Systems Engineer (MCSE)			P
*At least one person on engineering group should have this skill			

4.7 Assessment Tools

4.7.1 Choosing Tools

I take a vendor neutral approach to assessment tools. There are many good options and often it is a matter of personal preference. If an agency has particular tools they like, I would first look at using those. I do support the use of open source products because they are free; have been vetted in the security community; are customizable; and are often as good or better than more expensive commercial options.

4.7.2 Assessment Tools

NIST Special Publication 800-42: Draft Guideline on Network Security Testing is a good source for possible assessment tools. This document provides a list of common security testing tools along with their capabilities, cost, operating system compatibility, and applicable website.[23]

Based on use during assessments, the following are some of the free tools that I can recommend:

- Backdoors: Netcat

[23] Wack, John, Tracey Miles. "NIST SP 800-42: Draft Guidelines on Network Security Testing." pages 39-43.

- File Integrity Checkers: Tripwire
- Intrusion Detection System: Snort
- Network Mapping: Nmap
- Network Sniffer: Ethereal and TCPDump
- Password Cracker: John the Ripper
- Routers (Cisco): Router Audit Tool (RAT)
- Scanning: SuperScan and Sara
- Vulnerability Scanning: Nessus and Sara
- War Dialing: ToneLoc
- Windows Scanning: Microsoft Baseline Security Advisor (MBSA)
- Wireless: NetStumbler

4.8 Deliver Actionable Reports

As part of the post-assessment activities, a report on the assessment activities should be provided to the agency. An example of a report is provided as part of the case study in Tab 1 to Appendix A. The report starts at a high level and gets increasingly more granular; i.e., form an executive summary to the raw scanning data. A report is much easier to navigate if hyperlinks are provided to move between high-level summaries and low-level details. Senior management may not get past the executive summary so include the key points here in a concise and readable format. Items to include in the overview would be:

- Who participated in the assessment
- What specific areas where reviewed
- When did the assessment take place
- Where did the assessment occur
- Why were certain areas assessed or not assessed.

The findings should include both good and bad points. The findings should start as a high-level summary of what was found with a hyperlinks to more detailed results. It is important to describe what impact the vulnerability will have on an organization. All recommendations should be actionable by the organization; e.g., it doesn't make sense to recommend a $100,000 security solution to a small government agency that doesn't even have that much money in their total budget. An example of a good recommendation would be to hire a part time local college computer science intern versus hiring a more expensive full time network administrator to assist with improving security.

A variety of controls can be found in the methodologies discussed in Section 3. If you develop your own controls avoid ambiguity. The control/questions should be precise and clearly worded. The following should be considered when providing details about the controls/questions used during the assessment:

- Control – provide a number for each control and state what the control is.
- Category – provide the high-level category the control is part of.
- Risk – identify what the risk is if the control is not implemented.
- Type – state whether the control will be subjectively or objectively evaluated.

- Testing – provide a means to determine if the control is effectively used.
- Evaluation Criteria – identify the goal needed to achieve an acceptable rating for each control/question.
- Rating – provide the rating the agency received for the control/question.
- Comments – provide any details about what was found for the control/question.
- Scanning – if applicable include or provide a link to raw scanning results.
- Reference – provide a reference to obtain more detail on mitigating the control.

An example of the use of controls can be found in the case study.
The raw scanning data can be voluminous. It is best to provide this information electronically both to save paper and because many of the scanners provide HTML style reports that include links to more information and possible corrective actions.

If desired, a list of follow-on activities that the agency may want to take can be provided in the report. Some examples of these follow-on activities include training, device configuration, log audit assistance, and policy development. A list of follow-on activities is contained in the case study report.

The report should be presented as a hard copy and on a CD-ROM. Appendix C contains an example of a HTML index that can be used for a report on a CD-ROM. In addition, to the actual report a presentation should be developed and an out brief conducted with the agency's senior management. This should include time for discussion, questions, and clarifications.

5.0 CONCLUSION

This paper has presented a strategy to perform network assessments for small state and local government agencies. The recommended approach was to use an existing standard or methodology and tailor that to the budget, schedule, and personnel constraints of the target organization. This normally requires that only a subset of controls from any methodology be used. It is important to perform a risk assessment so that critical systems can be identified and prioritized with the goal of targeting these assets. The strategy discussed in this paper focuses on an interview process to gather information with technical hands-on work limited to available schedule and budget. When feasible, open source tools are recommend for the technical assessment. Upon completion of the assessment, it is important to provide an actionable report that can be used by agency personnel. This needs to include realistic recommendations that the agency can implement based on their limited budget and experience. In addition to the strategy discussed in the body of this document, a case study was presented to illustrate the practical application of the strategy.

APPENDICES

Appendix A
Case Study

1.0 BACKGROUND

This case study provides a practical demonstration of the strategy discussed in the main body of this document. The case study is based on a composite of information gathered during a number of actual assessments. Information has been added, deleted, and changed to obfuscate any connection to an actual organization. The organization discussed in this case study does not exist. The information provided in the case study sample report is done for illustrative purposes and is a subset of what would be included in an actual report; e.g., only 18 representative controls are discussed in the case study sample report.

2.0 OVERVIEW

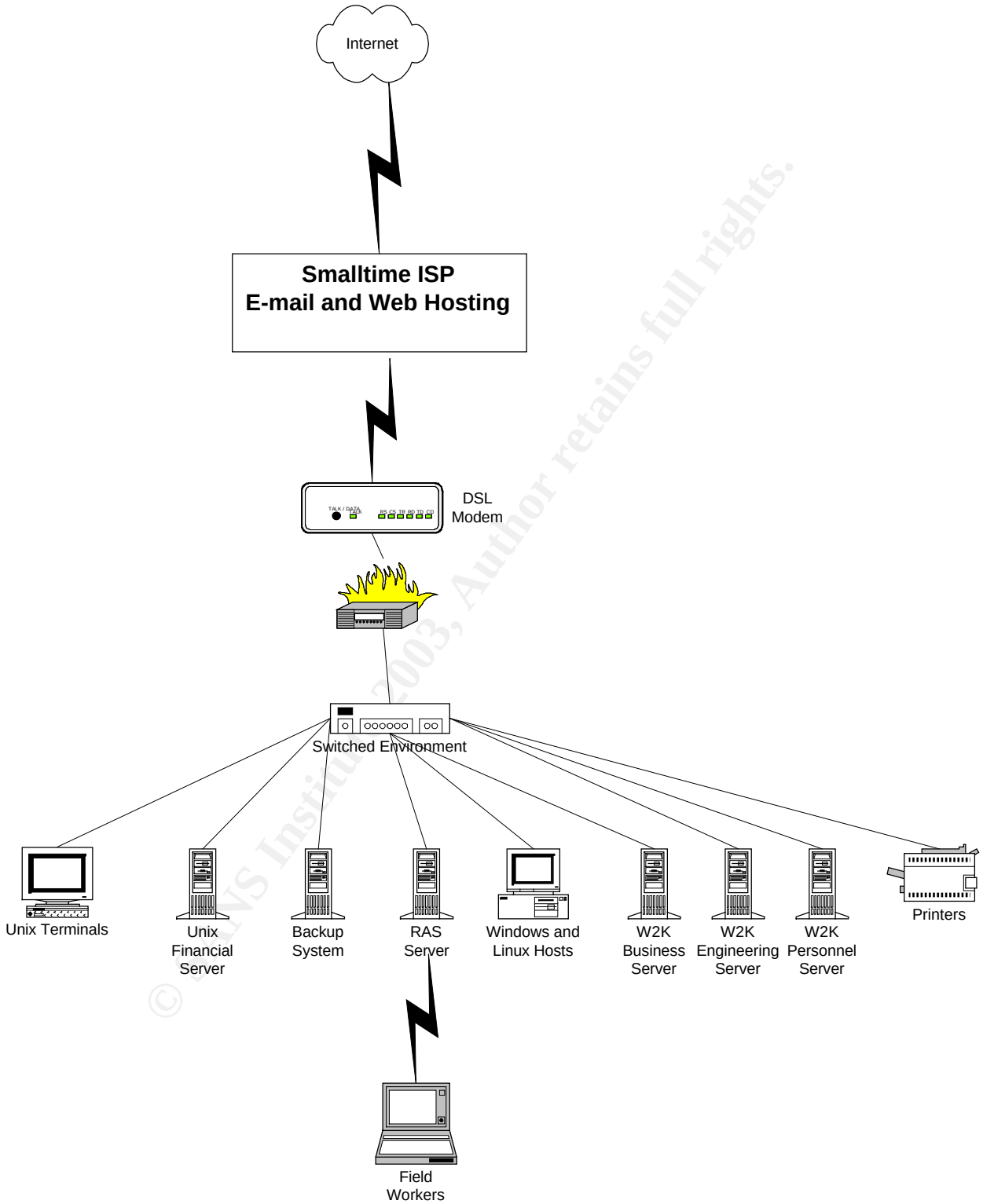
The organization assessed is the fictionalized Local Government Office Agency (LGOA) located in Trailrock, Idaho. This organization has approximately 92 employees. LGOA primarily has a Windows environment, but there are some hosts running Linux, and a UNIX server accessed by dumb terminals. They have approximately 85 clients and 10 UNIX dumb terminals on their network. LGOA's Internet connectivity is through a Digital Subscriber Line (DSL) Modem. Smalltime is their Internet Service Provider (ISP) and provides external hosting of their E-mail and web servers. In addition, Smalltime remotely maintains the LGOA UNIX server. LGOA has two network/security administrators with limited experience. A high-level LGOA network diagram is provided in Case Study Figure 1.

Because of their limited expertise and need for assistance, LGOA obtained the services of the fictionalized Lonesome River Consulting Company (LRCC) to perform an assessment on their network and information technology infrastructure. The results of that assessment are contained in the following tabs:

Tab 1: Case Study Sample Report
Tab 2: Detailed Results Summary
Tab 3: Detailed Results
Tab 4: Organizational Questionnaire
Tab 5: Services and Confidentiality Agreement

Appendix A
Case Study

Case Study Figure 1: LGOA High-Level Network Diagram



Tab 1 to Appendix A
Case Study Sample Report

1.0 EXECUTIVE SUMMARY

During October 2002, the Lonesome River Consulting Company (LRCC) performed a Network Vulnerability Assessment (NVA) of the Local Government Office Agency (LGOA) network located in Trailrock, Idaho. The purpose of the NVA was to provide the LGOA computer personnel with feedback on the security posture of the LGOA network. The purpose of this document is to summarize the activities of the NVA.

The strengths noted during the assessment include the following:

- Professional and dedicated computer personnel
- Outsourced upstream border protection and Internet services
- Network Address Translation (NAT) on Digital Subscriber Line (DSL) connections to hide the internal network addresses from the outside

The vulnerabilities noted during the assessment include the following:

- Use of weak passwords
- Evidence of failure to install latest patches
- Lack of controlled access to Computer Room
- Unlimited internal access to firewall
- Failure to update anti-virus signatures
- Open Telnet sessions to UNIX server
- Evidence of possible open modems
- Lack of periodic vulnerability scanning
- Limited review of log files
- Limited security training and awareness for general users
- No use of log-on security banners
- Lack of detail in security policy and inadequate security procedures
- No separation of duties between network and security adminstrators
- Limited incident handling procedures
- No alternative hardware to recover backups
- Backup tapes stored on site
- No user agreements
- Lack of Disaster Recovery Plan

Recommendations to eliminate or mitigate identified vulnerabilities are provided in Section 4.3. Summary and detailed results of the NVA are contained in Tab 2 to Appendix A and Tab 3 to Appendix A respectively.

The results of the assessment indicate there are many positive security practices in place. The LGOA computer personnel are doing a professional and competent job. When a specific capability cannot be met in-house, it has been outsourced; e.g.,

Internet services and upstream perimeter defense are provided by Smalltime. On a periodic basis, it would be prudent to assess Smalltime's ability to provide quality Internet connectivity and adequate security for hosted Internet services. Recent security measures—such as the scheduling and completion of this NVA, and the publication of a Security Policy—are positive steps. However, there is a need to add more technical and programmatic security controls; to review the security of the UNIX server; to provide additional security training and awareness; and to develop more robust policies and procedures.

In today's environment, it is likely that the LGOA network will be exploited. Therefore, it is imperative that adequate measures be in place to detect and properly respond to an incident. It is recommended that periodic network vulnerability assessments be continued, using either in-house staff or through a third party.

2.0 ASSESSMENT ACTIVITIES

The LRCC Team performed an NVA of the LGOA network, located in Trailrock, Idaho from October 7, 2002 to October 21, 2002. The results of the assessment activities are contained in this document.

2.1 Organization of the Document

This document is organized into the following sections:

- Section 1 EXECUTIVE SUMMARY provides a high-level overview.
- Section 2 ASSESSMENT ACTIVITIES provides details on the scope of the assessment.
- Section 3 RISK ASSESSMENT AND IDENTIFICATION OF CRITICAL ASSETS provides details on identifying the agency's critical systems.
- Section 4 ASSESSMENT RESULTS provides the high-level findings and recommendations from the assessment.
- Section 5 RESOURCES AND REFERENCES provides material to be used to improve the information assurance posture of the LGOA network.
- Section 6 FOLLOW-ON ACTIVITIES provides possible options that LRCC can perform to improve the network security posture of the LGOA.
- Section 7 CONCLUSION contains summary comments about the performance of this NVA.

2.2 Objective of the Network Vulnerability Assessment

LRCC performed an NVA to identify the vulnerabilities on the LGOA network by reviewing organizational policy and procedures and analyzing communication links, operating systems, hosts, servers, protection devices, detection devices, and services. The LRCC methodology included the following:

a. Confidentiality. LRCC personnel were briefed that all information gathered was confidential, proprietary, and was not for disclosure outside of LRCC.

b. **Customized Approach.** LRCC used a questionnaire, contained in Tab 4 to Appendix A, to gather information about the LGOA network. In addition, LRCC met with Sally Jones of the LGOA to define expectations and limitations. These activities resulted in a tailored approach for the performance of this assessment.

c. **Policy and Procedural Review.** There was limited policy and procedural documentation available for review. During the interview process, discussion included the type of informal processes and procedures that are in use.

d. **Vulnerability Scanning.** As provided in the Services Agreement, LRCC, in coordination with LGOA technical personnel, conducted vulnerability scans in as non-invasive a manner as possible. This included host and service discovery, operating system identification, and checks for known vulnerabilities and patches.

e. **Device Assessment.** LRCC conducted a review of the configuration and vulnerabilities on select servers, hosts, and firewalls.

f. **Virus Detection.** A review of virus detection policy and procedures was conducted, and checks were made to determine if updated anti-virus software was being properly used.

g. **Reporting of Assessment Results.** Assessment results were analyzed and interpreted. The results are provided in this proprietary written report listing the details of the assessment, recommended remedial actions, and sources and references that can be used to correct identified vulnerabilities.

2.3 NVA Scope

The scope of the NVA was limited to those items deemed most critical. These items were identified in a kick-off meeting conducted October 7, 2002, between LRCC personnel and Sally Jones of the LGOA and in a risk assessment and identification of critical data session conducted on October 8, 2002. Items were prioritized and, in some cases, only a subset of activities could be assessed.

The following table includes a snapshot of the assessed areas and LRCC personnel responsible for each area.

Tab 1 to Appendix A
Case Study Sample Report

Case Study Table 1 - Task Responsibility Matrix

Team Lead: Joe Tuffy **L - Lead** **P - Participant**	**Jack Mack**	**Mark Mays**	**Jill Parker**	**Joe Tuffy**	**Harold Smuthers**	**LGOA POC Sally Jones**
Pre-Assessment Activities						
Define Scope and expectations with agency	P			**L**		Sally Jones
Service and Confidentiality Agreement completed				**L**		Sally Jones
Organizational Questionnaire completed	P			P	**L**	Sally Jones
Perform risk assessment and ID critical systems	P	P	P	**L**	P	Sally Jones
Identify and prepare controls/questions	**L**			P	P	Sally Jones
Identify and select assessment tools	**L**	P	P	P	P	Sally Jones
Obtain and review policy and procedures	P	P	P	**L**	P	Sally Jones
Assessment Activities						
Conduct assessment in-brief	P	P	P	**L**	P	Sally Jones
Verify policy and procedure compliance	P	P	P	**L**	P	Sally Jones
Conduct technical assessments	**L**	P	P	P	P	Sally Jones
Perform network and host scans	P	**L**	P	P	P	Bill Smiles
Perform password cracking	P	**L**			P	Sally Jones
Analyze data collected	P	P	P	**L**	P	Sally Jones
Post-Assessment Activities						
Prepare Assessment Report	P	P	P	**L**	P	Bill Smiles
Conduct Out Brief	P	P	P	**L**	P	Sally Jones

This assessment did not include the following:

- Smalltime-hosted Internet services such as the File Transmission Protocol (FTP) server, email server, and Web server.
- Smalltime provided upstream border protection
- Smalltime provided Web content services
- Smalltime provided maintenance of the UNIX server. However, LRCC did conduct a vulnerability assessment of the UNIX server operating system, and identified numerous vulnerabilities, along with recommendations for corrective action.

2.4 NVA Participants

Tables 2 and 3 list the key participants in the NVA.

Case Study Table 2: LRCC Participants

Name	Role
Joe Tuffy	Team Leader
Jack Mack	Technical Lead
Mary Mays	Engineer Team
Jill Parker	Engineer Team
Harold Smuthers	Engineer Team

Case Study Table 3: LGOA Participants

Name	Role
Sally Jones	Network Manager
Bill Smiles	Network Administrator

3.0 RISK ASSESSMENT AND IDENTFICATION OF CRITICAL ASSETS

During the pre-assessment phase, a risk assessment and identification of critical assets was performed. Table 4 identifies the critical data; what system the data resides on; and the level of impact if the risk occurred.

Case Study Table 4: Critical Data by System

Critical Data	System	Confidentiality	Integrity	Availability
Inventory Database	Business	Low	Medium	Medium
Customer Calls Database	Business	Medium	Medium	Medium
Engineering Drawings	Engineering	Medium	Medium	Low
Engineering Studies	Engineering	Medium	Medium	Medium
Personnel Records	Personnel	High	High	Medium
Payment Tracking	Financial	High	High	High
External Transactions	Financial	High	High	High
Web Site	Web Server	Low	Medium	Medium

Based on the information identified in Table 4 and in coordination with key personnel at LGOA, Table 5 contains a ranking of the systems (the system ranked number one is most important) and the associated impact if the risk occurred.

Case Study Table 5: System Rankings

Rank	System	Confidentiality	Integrity	Availability
1	Financial	High	High	High
2	Personnel	High	High	Medium
3	Engineering	Medium	Medium	Medium
4	Business	Medium	Medium	Medium
5	Web Server	Low	Medium	Medium

4.0 ASSESSMENT RESULTS

4.1 Overview

A high-level summary of the strengths and vulnerabilities found during the NVA are contained in Sections 4.2 and 4.3. Section 4.3 also contains recommended corrective

actions to eliminate or mitigate the vulnerabilities. A "Detailed Results Summary" is contained in Tab 2 to Appendix A. The "Detailed Results" are contained in Tab 3 to Appendix A.

4.2 Strengths

The following strengths were noted during the performance of the NVA.

1. The LGOA computer personnel are professional and dedicated. They are mission-oriented and work diligently to ensure the best possible network performance while providing network security. The cooperation of the computer personnel was a key factor in accurately obtaining data for this assessment.

2. Because of limited networking personnel, the LGOA has chosen to use Smalltime as a third party to provide upstream border protection and to host Web, File Transmission Protocol (FTP), and email services. It would be prudent to conduct periodic assessments of Smalltime's ability to provide quality Internet connectivity and adequate security for hosted Internet services.

3. Using Network Address Translation (NAT) on the Digital Subscriber Line (DSL) connection is an effective method to hide the internal network addresses from the outside.

4.3 Vulnerabilities

This section includes a list of the vulnerabilities found on the NVA; a discussion of their possible impacts; and recommendations to eliminate or mitigate the vulnerability.

4.3.1 Use of Weak Passwords

Discussion. There was evidence that numerous platforms and applications had weak or nonexistent passwords, e.g., dictionary words, password same as login ID, and blank password accepted for access. 10 of the 15 UNIX passwords were cracked within one minute using the John the Ripper password cracker. When weak or nonexistent passwords are in use, an attacker can gain access to the network, cover the intrusion, and conduct malicious activities.

Applicable Controls. 1001

Recommendations

- Advise users to update their passwords using guidelines similar to those provided by the National Information Protection Center
- Conduct user awareness training on how to develop a strong password
- Advise users not to use common dictionary words as passwords
- Enforce password controls through the operating system environment
- Consider a stronger form of authentication, such as the combined use of a token and password

4.3.2 Evidence of Failure to Install Latest Patches

Discussion. During network scans and in interviews with LGOA personnel, it was found that patches and hot fixes are not installed consistently and expeditiously. The failure to install patches in a timely manner can leave known vulnerabilities on the network and provide opportunities for attackers to access the network.

Applicable Controls. 1002

Recommendations

- Contact your outsourced Unix maintenance provider and discuss the results of the patch scan performed on this NVA
- Conduct periodic scans to identify what patches are needed
- Identify the most critical network assets and ensure patches are applied to these devices first

4.3.3 Lack of Controlled Access to Computer Room

Discussion. There was no controlled access to the computer room for most of the workday. Although the facility is locked at night, any employee can enter the computer room during daylight hours. This could result in unintentional or malicious activity, and a compromise of sensitive or critical information.

Applicable Controls. 1003

Recommendations.

- Install cipher locks or some other form of controlled access to the computer room
- Have non-LGOA employees sign a logbook when they enter and leave the computer room.

4.3.4 Unlimited Internal Access to Firewall

Discussion. The firewall is configured in a secure manner with regard to inbound traffic from the Internet. The firewalls are blocking most forms of outside access and are performing Network Address Translation (NAT) so that the internal IP addresses are hidden from the Internet. However, internal access to the firewall is a concern: The firewall is configured with the default administrative passwords, and any host with an IP address on the network could access the firewall remotely and attempt to login.

Applicable Controls. 1004

Recommendations

- Change the default administrative password
- Upgrade to a newer version of firmware
- Enable remote host administration security so that only one administrative workstation has rights to manage the firewall remotely
- Enable the "Discard PING from WAN side" option.

4.3.5 Failure to Update Anti-Virus Signatures

Discussion. In interviews with the network administrators and in a physical review by the auditors, it was determined that the anti-virus software is not being updated on all host platforms. The failure to update anti-virus signatures at periodic intervals makes the network susceptible to the introduction of malicious code.

Recommendations

- Establish a procedure that outlines the frequency and steps to be taken to ensure anti-virus signatures are being updated
- Provide a means to update signatures on host machines automatically. This could be by pushing updates out from a local server

4.3.6 Open Telnet Sessions to UNIX Server

Discussion. It was discovered that unencrypted Telnet sessions are being made to the UNIX server that contains sensitive financial data. An attacker could use a sniffer to capture the unencrypted root password, and then use it to compromise the system.

Applicable Controls. 1006

Recommendations

- Contact Smalltime, the maintainer of the UNIX server, to correct this vulnerability
- Use Secure Shell (SSH) to encrypt data. SSH is a de facto standard for remote logins. Refer to http://www.ssh.com/products/ssh/ for additional information.

4.3.7 Evidence of Possible Open Modems

Discussion. War dialing was conducted on the majority of phone extensions within LGOA. This resulted in the discovery of numerous modems. Budget and schedule constraints did not allow the LGOA NVA Team to determine what these modems were used for and if they were connected to stand alone devices or networked devices. If open modems do exist they can provide an easy means for attackers to circumvent the security perimeter and gain access to the LGOA network.

Applicable Controls. 1007

Recommendations

- Conduct additional war dialing to identifying all possible open modems on LGOA devices
- Determine if the modems are used for a legitimate purposes and if they are connected to stand alone or networked devices
- Implement security controls that reduce the possibility that attackers can access the network through modems; e.g., turn off auto answer
- Provide user awareness training on the security consequences of improperly using or installing unauthorized modems on LGOA devices

4.3.8 Lack of Periodic Vulnerability Scanning

Discussion. Because of limited technical personnel and other priorities, vulnerability scanning has not been conducted. This can result in vulnerabilities or anomalies going unrecognized, allowing an attacker to use these vulnerabilities to gain access to the network.

Applicable Controls. 1008

Recommendations

- Use open source scanning tools, e.g., Nessus, to conduct periodic scans of the network to identify vulnerabilities
- Provide training to LGOA computer personnel on the use of scanning tools and the proper interpretation of the data generated from them
- Establish procedures to take corrective actions on the vulnerabilities identified during scanning

4.3.9 Limited Review of Log Files

Discussion. Because of limited technical personnel and other priorities, the log files of critical devices are not being audited. This can result in attacks or anomalies going unrecognized, allowing an attacker to gain access to the network without the knowledge of LGOA computer personnel. In addition, it requires frequent reviews of log files to understand what the baseline data should look like so that anomalies can be more easily identified.

Applicable Controls. 1009

Recommendations

- Initiate procedures to conduct reviews of log files
- Consider outsourcing to ensure that a timely and thorough review of log files is performed
- Determine what log file information should be archived for future analysis
- Develop procedures for collection of forensic data

- Send individuals to the System Administration, Networking and Security (SANS) incident analysis training to enhance their abilities to properly interpret log files

4.3.10 Limited Security Training and Awareness for General Users

Discussion. There is only limited information security training and awareness being conducted for general users. One of the biggest security risks is the intentional or unintentional failure of the human in the loop to properly execute their security responsibilities. Even if there are strong technical security solutions in place, the lack of training and awareness can result in reduction of the overall security posture of the organization.

Applicable Controls. 1010

Recommendations

- Include security awareness and training requirements in the Security Policy
- Conduct both formal and informal security training and awareness campaigns
- Provide email notifications on prudent security practices
- Ensure that managers brief their personnel on security

4.3.11 No Use of Log-on Security Banners

Discussion. There was no use of log-on security banners for users accessing the network. Failure to use security banners can result in users not understanding the rules of engagement when they access and use the LGOA network, and can make it more difficult to bring legal or punitive action against an individual for violating security policies and practices.

Applicable Controls. 1011

Recommendations

- Include the wording for a log-on security banner in the Security Policy
- Apply security banners to all devices on the network so that users will be notified of the restrictions under which they operate

4.3.12 Lack of Detail in Security Policy and Inadequate Security Procedures

Discussion. The Security Policy lacks sufficient detail and, in many cases, there are either inadequate or no accompanying procedures. All security practices, procedures, and implementations should be traceable back to a robust Security Policy. The entire security posture of the organization is at risk without a good Security Policy.

Applicable Controls. 1012

Recommendations

Consult the following resources to improve the Security Policy:

- Primer for Developing Security Policies
  http://www.sans.org/newlook/resources/policies/Policy_Primer.pdf
- Security Policy Templates
  http://www.sans.org/newlook/resources/policies/policies.htm#template

4.3.13 No Separation of Duties Between Network and Security Administrators

Discussion. The same individuals perform both the network and security administrator roles on the LGOA network. This lack of checks and balances can result in intentional circumvention or unintentional failed execution of prudent security practices.

Applicable Controls. 1013

Recommendations

- Consider using a third party to periodically review the activities of the network and security administrators

4.3.14 Limited Incident-Handling Procedures

Discussion. There were only limited incident-handling procedures and practices in place. As a result, an incident could escalate on the LGOA network while it is determined how to handle the situation. This could also result in inappropriately shutting down critical systems in response to an incident or failure.

Applicable Controls. 1014

Recommendations

- Identify a reporting chain, and develop escalation procedures to handle incidents
- Identify an individual(s) to authorize actions to mitigate the incident
- Develop forensic-gathering procedures to secure evidence related to an incident
- Use http://www.incidents.org/Incident_forms/ as a resource to improve incident handling
- Provide guidance in the Security Policy on how to handle incidents
- Conduct administrator and user awareness training on how to handle incidents

4.3.15 No Alternative Hardware to Recover Backups

Discussion. Although backups of critical network devices are conducted, there are no alternative hardware devices identified to do the recovery if the facility or hardware is destroyed. There are also no warm or hot sites identified for use in recovery operations. As a result, it will be difficult to quickly restore operations and provide critical services in a timely manner and ad hoc and on the fly steps will need to be taken to bring operations back on-line.

Applicable Controls. 1015

Recommendations

- Procure and maintain redundant devices for use in recovery operations
- Identify other non-local LGOA assets that can be used to support LGOA recovery operations

4.3.16 Backup Tapes Stored On Site

Discussion. Backup tapes of LGOA critical devices are stored on site. Industry best security practices recommend storing tapes away from the originating facility. Failure to store tapes without enough geographic dispersion can result in loss of the backups in the event of damage to the originating facility.

Applicable Controls. 1016

Recommendations

- Determine a method to store tapes at an offsite location. Storing the tapes in a local bank safe deposit box is one possibility
- On a weekly basis, send backup tapes or CD-ROMS to an alternative facility outside of the Trailrock, Idaho geographic area

4.3.17 No User Agreements

Discussion. There is no user agreement that clearly outlines what should and should not happen on the LGOA network. Without such agreements, it is not clear what users are entitled to do, and it becomes more difficult to take disciplinary or warning actions against individuals when they circumvent policies and procedures.

Applicable Controls. 1017

Recommendations

- Develop applicable user agreements as part of the Security Policy
- Require users to sign the appropriate agreement and keep these agreements on file with Human Resources
- Conduct awareness training on what can and cannot be done as a user

4.3.18 Lack of Disaster Recovery Plan

Discussion. There is no disaster recovery plan or disaster recovery guidance. In the event of a disaster, the lack of detailed plans and procedures could have a negative business impact by delaying the recovery of the network.

Applicable Controls. 1018

Recommendations

- Conduct a Business Impact Analysis (BIA) to identify a prioritized list of LGOA functions and the impact of not maintaining these functions following a disaster
- Based on the BIA, develop a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)
- Determine if it is necessary to contract with a BCP/DRP provider for resources that would be needed in the event of a disaster
- Practice the execution of the BCP/DRP
- Maintain a copy of the BCP/DRP at an offsite location.

5.0 RESOURCES AND REFERENCES

This section contains a list of references that are useful in improving the information security posture of your network. The references are contained in the following table. For the purposes of this case study only a subset of references were included.

Case Study Table 1

Reference	Description
Center for Information Security	An organization that develops security tools and benchmarks via a consensus process.
CERT Coordination Center	An organization that publishes security advisories and information assurance guidance.
NIST Special Publications	The 800 series of documents covers a broad range of information security issues.
SANS Institute	An organization that provides training and resources within the fields of systems administration, networking, and security.

6.0 FOLLOW-ON ACTIVITIES

If desired, the performance of additional services can be obtained through a follow-on effort with LRCC. Additional services would be performed after LRCC develops and delivers—and the LGOA approves—appropriate technical and cost proposals.

Additional services available through LRCC include the following:

a. **Security Architecture Planning.** Recommendations to improve the security architecture of the LGOA, such as network redesign and inclusion of additional security devices.

b. **Training.** Training on relevant security topics, such as social engineering, basic security measures, hardening of the perimeter, and insider threats.

c. **Network Device Configuration.** Assistance in improving the configuration of network devices such as routers, switches, servers, and firewalls.

d. **Development of Policies and Procedures.** Development or revisions to security policy and procedural documents.

e. **Installation of Security Products.** Installation of security products such as firewalls, intrusion detection systems, and vulnerability assessment tools.

f. **Network Modeling.** Development of network models to demonstrate ways to improve network performance and security.

g. **Network Management.** Implementation of network management applications to provide centralized monitoring of resources.

h. **Audit Log Analysis.** Assistance in explaining audit log data and in establishing procedures to continue this process after LRCC departs.

i. **Backup and Recovery.** Assistance to improve backup and recovery procedures and technologies.

7.0 CONCLUSION

The results of the assessment indicate there are many positive security practices in place. The LGOA computer personnel are doing a professional and competent job. When a specific capability cannot be met in-house, it has been outsourced; e.g., Internet services and upstream perimeter defense are provided by Smalltime. On a periodic basis, it would be prudent to assess Smalltime's ability to provide quality Internet connectivity and adequate security for hosted Internet services. Recent security measures—such as the scheduling and completion of this NVA, and the publication of a Security Policy—are positive steps. However, there is a need to add more technical and programmatic security controls; to review the security of the UNIX

server; to provide additional security training and awareness; and to develop more robust policies and procedures.

In today's environment, it is likely that the LGOA network will be exploited. Therefore, it is imperative that adequate measures be in place to detect and properly respond to an incident. It is recommended that periodic network vulnerability assessments be continued, using either in-house staff or through a third party.

Tab 2 to Appendix A
Case Study Sample Report: Detailed Results Summary

Category	Note: Although grading for a 104 controls is shown in this table, the case study included only detailed results on 18 controls. Comments	Acceptable	Partially Acceptable	Not Acceptable	Total
	Total	33	29	42	104
Accounts and Passwords	• 10 of 15 Unix server passwords cracked within one minute • Unix root password cracked within 15 hours • Weak or non-existent passwords in use • No formal procedures or guidance on use of strong passwords	2	2	3	7
Anti-Virus	• Hosts are not automatically pushed the latest anti-virus definition files	2	3	2	7
Auditing	• No vulnerability scanning is being performed • No log files are being reviewed	2	3	4	9
Authorization	• There are no log-on security banners in use	3	2	2	7
Backup and Recovery	• There is no alternative hardware to perform recovery operations • Backup tapes are not stored offsite or in a secure location	2	2	4	8
Disaster Recovery Planning	• There is no Disaster Recovery Plan	1	1	4	6
Firewalls	• Firewalls are configured with default admin passwords	2	2	3	7
Incident Handling	• There was only limited guidance on incident handling.	2	2	3	7
Personnel	• Only limited ad hoc security training and awareness is being performed • There is no separation of duties between network and security administrators • There are no user agreements in place	3	2	3	8
Physical Security	• There is no controlled access to the computer room during normal working hours	4	2	3	9
War Dialing	• Nine possible open modems were detected	2	2	2	6
Security Policy & Procedures	• The security policy lacks sufficient detail and only limited procedures are available.	3	2	3	8
Unix and Linux Systems	• 52 applicable and recommended security patches were not installed • SSH was not being run on Unix server	5	4	6	15

Tab 3 to Appendix A
Case Study Sample Report: Detailed Results

1001: ARE STRONG PASSWORDS IN USE?

Category: Accounts and Passwords

Risk: When weak or nonexistent passwords are in use, an attacker can gain access to the network, cover the intrusion, and conduct malicious activities.

Type: Objective

Testing: The auditor shall run password-cracking software on password files.

Evaluation Criteria:
Acceptable - Less than 5% of passwords cracked within 24 hours.
Partially Acceptable - Less than 10% of passwords cracked within 24 hours.
Not Acceptable - More than 10% of passwords cracked within 24 hours. Root or administrator password cracked within 24 hours.

Rating: Unacceptable

Comments: Weak passwords are in use. 10 of 15 user passwords on the UNIX server were broken in one minute using the password cracker. Root was cracked after 15 hours of running the password cracker. Some accounts were accessible with only the user name and null password. Some account names and passwords were identical.

Scanning: The results of the password scanning are provided in a confidential file that is not included in this case study sample report.

Reference to Mitigate Issue: National Infrastructure Protection Center Password Protection 101 http://www.nipc.gov/publications/nipcpub/password.htm

1002: DOES THE SYSTEM HAVE THE LATEST SUN SECURITY PATCHES INSTALLED?

Category: UNIX and Linux Systems

Risk: The failure to install patches in a timely manner can leave known vulnerabilities on the network and provide opportunities for attackers to access the network.

Type: Subjective

Testing: The auditor shall use Sun's Patch Manager or Patch Check to determine the patch levels on the system and conduct interviews with the system administrator to determine how often patches are installed.

Tab 3 to Appendix A
Case Study Sample Report: Detailed Results

Evaluation Criteria: Based on the testing criteria the auditor will make a subjective determination of the rating. Examples indicative of an unacceptable rating include: no checks for or updates of security patches within last 48 hours; no procedures for applying patches; limited or no knowledge of where to obtain patches

Rating: Unacceptable

Comments: 52 applicable and recommended security patches were not installed. The LGOA UNIX maintenance and administration is outsourced and the LGOA network administrator did not know when or how patches were being applied.

Scanning: The following is a nominal listing of scanning results for illustrative purposes:

ID	Ins Rev	Lat Rev	Age	Synopsis
103867	N/A	04	153	SunOS 5.5.1: jsh, sh and rsh patch
103891	N/A	08	187	SunOS 5.5.1: ksh and rksh patch
103995	N/A	02	347	SunOS 5.5.1: rpc.nispasswdd patch
104212	N/A	15	391	SunOS 5.5.1: /kernel/drv/hme patch
104637	N/A	04	431	SunOS 5.5.1: /usr/ccs/lib/libcurses.a patch

Reference to Mitigate Issue: SunSolve Patch Support Portal
http://sunsolve.sun.com/pub-cgi/show.pl?target=patchpage

1003: IS ACCESS TO THE COMMUNICATION AND COMPUTER ROOMS CONTROLLED?

Category: Physical Security

Risk: Uncontrolled access to the computer room could result in unintentional or malicious activity resulting in a loss or compromise of sensitive or critical information.

Type: Subjective

Testing: Review written procedures, conduct employee interviews, and inspect physical protection measures.

Evaluation Criteria: Based on the testing criteria, the auditor will make a subjective determination of the rating. Examples indicative of an unacceptable rating include; verification of uncontrolled access; lack of locks; lack of or inadequate procedures for access control.

Rating: Unacceptable

Comments: Based on the testing criteria, it was determined that:

- There are no procedures for controlling access to the computer room.
- During the day, the computer room is unlocked and there is no controlled access.
- The computer room is locked at night.

Scanning: Not applicable

Reference to Mitigate Issue: U.S. Department of Commerce Manual of Security Policies and Procedures
http://www.osec.doc.gov/osy/SECURITYMANUAL/Chapter39.htm

1004: ARE PROPER ACCESS CONTROLS USED ON THE FIREWALL?

Category: Firewalls

Risk: Firewalls without proper access control are subject to modification or tampering by unauthorized individuals.

Type: Subjective

Testing: Review written procedures, conduct employee interviews, and physically attempt to access the firewall using default or null passwords.

Evaluation Criteria: Based on the testing criteria, the auditor will make a subjective determination of the rating. Examples indicative of an unacceptable rating include: no passwords required for administrator access and default administrator passwords in use.

Rating: Unacceptable

Comments: The firewalls are configured with default admin passwords.

Scanning: Not applicable

Reference to Mitigate Issue: SCORE Firewall Checklist
http://www.sans.org/SCORE/checklists/FirewallChecklist.doc

1005: ARE VIRUS SIGNATURES PROPERLY UPDATED?

Category: Anti-Virus

Risk: The failure to update anti-virus signatures at periodic intervals makes the network susceptible to the introduction of malicious code.

Type: Objective

Testing: Compare date of virus definition file with vendor's latest release; Determine if an automatic update process is being used; Interview administrators about virus update practices.

Evaluation Criteria:
Acceptable - Latest virus definition file is installed and an automatic update process is in place.
Partially Acceptable - Latest virus definition file is installed but there is no automatic update process in place.
Unacceptable - Latest virus definition file is not installed.

Rating: Unacceptable

Comments: A random check revealed that at least five hosts did not have the latest virus definition file installed. The network administrator indicated that there was not an automatic virus definition file update procedure in place.

Scanning: Not applicable

Reference to Mitigate Issue: SANS
http://www.sans.org/newlook/resources/policies/Anti-virus_Guidelines.pdf

1006: ARE TELNET SESSIONS CONTAINING SENSITIVE DATA ENCRYPTED?

Category: UNIX and Linux Systems

Risk: Unencrypted Telnet sessions could be compromised to reveal sensitive data or passwords that could lead to financial loss or compromise of the system.

Type: Objective

Testing: Review Unix settings to determine if SSH is being run at start time; e.g., /usr/local/sbin/sshd2. Look for SSH server configuration files in /etc/ssh2 and server binaries in usr/local/sbin.

Evaluation Criteria:
Acceptable - ssh is available with latest patches and is being run at start time;
Unacceptable - ssh is not available or is not being run at start time

Rating: Unacceptable

Comments: A check of the UNIX server indicated that SSH was not installed.

Scanning: Not Applicable

Reference to Mitigate Issue: SSH Communications Security, www.ssh.com

Tab 3 to Appendix A
Case Study Sample Report: Detailed Results

1007: ARE OPEN MODEMS IN USE WITHIN THE ORGANIZATION?

Category: Wardialing

Risk: Open modems can provide an easy means for attackers to circumvent the security perimeter and gain access to the LGOA network.

Type: Objective

Testing: The auditor will perform war dialing on the organization's phone extensions.

Evaluation Criteria:
Acceptable - No unauthorized open modems detected.
Unacceptable - One or more unauthorized open modems detected.

Rating: Unacceptable

Comments: War dialing was conducted on the majority of phone extensions within LGOA. This resulted in the discovery of numerous modems. Budget and schedule constraints did not allow the LRCC NVA Team to determine what these modems were used for or if they were connected to stand alone devices or networked devices.

Scanning: Scanning was done using ToneLoc. Scanning was done from a LGOA internal analog line, but the outgoing line prefix ("9") was used to simulate dialing from the outside.

Phone ranges scanned: 123-44XX; 123-46XX to 123-50XX; 123-51XX to 123-52XX

Total numbers dialed: 125
Start time: 10/1502 1830
End time: 10/16/02 0340

Number of busy signals detected: 3
Number of Carriers detected: 25
Number of Carriers identified as FAX machines: 15
Number of Carriers identified as modems: 9
Unknown: 1

Extensions of detected modems: 4610; 4611; 4612; 4710; 4711; 4712; 4810; 4811; 4812

Reference to Mitigate Issue: @Stake War dialing Brief
http://www.atstake.com/research/reports/acrobat/wardialing_brief.pdf

1008: ARE VULNERABILITY SCANS BEING PERFORMED ON A REGULAR BASIS?

Category: Auditing

Risk: Lack of vulnerability scanning can result in vulnerabilities or anomalies going unrecognized with the possibility that an attacker will use these vulnerabilities to gain access to the network.

Type: Subjective

Testing: The evaluator shall review policy and procedures to determine if there are requirements to perform vulnerability assessments. Through the interview process with network and security engineers determine if vulnerability scanning is being performed.

Evaluation Criteria:
Acceptable - Three criteria are required to receive an acceptable rating: 1. Policy and procedures require vulnerability scanning; 2. Scanning is being performed on all devices on the network on a regular basis; 3. There is evidence that discovered vulnerabilities are being corrected or mitigated.
Partially Acceptable - Scanning is being performed on at least the critically identified network devices on a regular basis.
Unacceptable - Lack of policy and procedures on vulnerability scanning; Limited or no scanning and not done on a regular basis.

Rating: Unacceptable

Comments: No vulnerability scanning is being performed.

Scanning: Not Applicable

Reference to Mitigate Issue: CERT/CC
http://www.cert.org/security-improvement/practices/p095.html

1009: ARE LOG FILES BEING REVIEWED ON A PERIODIC BASIS?

Category: Auditing

Risk: Not reviewing log files on a periodic basis can result in attacks or anomalies going unrecognized, allowing an attacker to gain access to the network without the knowledge of LGOA computer personnel. In addition, it takes frequent reviews of log files to understand what the baseline data should look like, so that anomalies can be identified more easily.

Type: Subjective

Testing: The evaluator shall review policy and procedures to determine if there are requirements to perform reviews of log files. Through the interview process with network and security engineers determine if reviews of log files are being performed.

Evaluation Criteria:
Acceptable: Three criteria are required to receive an acceptable rating: 1. Policy and procedures require reviews of log files; 2. Review of log files on critical devices are being performed on a daily basis; 3. There is evidence that issues discovered during log reviews are being investigated and corrected.
Partially Acceptable - reviews of log files on critical devices are being done on at least a weekly basis.
Unacceptable - Lack of policy and procedures on performing log reviews; Limited or no review of log files; e.g., longer than a week goes by without logs on critical devices being reviewed.

Rating: Unacceptable

Comments: No log files are being reviewed.

Scanning: Not applicable

Reference to Mitigate Issue: CERT/CC
http://www.cert.org/security-improvement/practices/p095.html

1010: IS THERE A SECURITY TRAINING AND AWARENESS PROGRAM FOR GENERAL USERS?

Category: Personnel

Risk: Even if there are strong technical security solutions in place, the lack of training and awareness can result in reduction of the overall security posture of the organization.

Type: Subjective

Testing: The evaluator shall review policy and procedures to determine if there are requirements to perform security awareness and training. Through the interview process with the user population determine if security training and awareness is being performed. Determine if training/personnel records have evidence of security and awareness training.

Evaluation Criteria:
Acceptable - Two criteria are required to receive an acceptable rating: 1. Policy and procedures require at least annual security and awareness training; 2. Review of training/personnel records indicated that at least 85% of personnel have received annual security and awareness training.
Partially Acceptable - Two criteria are required to receive a partially acceptable rating:

1. Policy and procedures require at least annual security and awareness training; 2. Review of training/personnel records indicated that at least 60% of personnel have received annual security and awareness training.
Unacceptable - There are no policy and procedures in place requiring annual security training and awareness and/or less than 60% of personnel have received annual security and awareness training.

Rating: Unacceptable

Comments: There is no policy or procedure requiring annual security training and awareness. Approximately 25% of the personnel appear to be participating in ad hoc or informal training.

Scanning: Not Applicable

Reference to Mitigate Issue: NIST Special Publication 800-50: Building an IT Security and Awareness Program http://csrc.nist.gov/publications/drafts/draft800-50.pdf

1011: ARE LOG-ON SECURITY BANNERS BEING USED?

Category: Authorization

Risk: Failure to use security banners can result in users not understanding the rules of engagement when they access and use the network, and can make it more difficult to bring legal or punitive action against an individual for violating security policies and practices.

Type: Objective

Testing: Review policy and procedures for requirements to have log-on security banners.

Evaluation Criteria:
Acceptable - There is security policy and procedures in place requiring the use of log-on banners and log-on banners are being shown when a user attempts to access the network.
Partially acceptable - Log-on banners are being shown when a user attempts to access the network but there is no policy or procedure requiring their use.
Unacceptable - Long-on banners are not being used.

Rating: Unacceptable

Comments: There was no use of log-on security banners for users accessing the network.

Scanning: Not Applicable

Reference to Mitigate Issue: CERT/CC Acceptable Use Policy
http://www.cert.org/security-improvement/practices/p034.html

1012: ARE ADEQUATE SECURITY POLICY AND PROCEDURES IN PLACE?

Category: Security Policy and Procedures

Risk: All security practices, procedures, and implementations should be traceable back to a robust Security Policy. The entire security posture of the organization is at risk without a good Security Policy.

Type: Subjective

Testing: A review of security policies and procedures shall be performed. The evaluator shall make a subjective analysis as to whether adequate policy and procedures are in place.

Evaluation Criteria:
Acceptable - Security policy and procedures exist and are less than one year old or have been reviewed within the past year. Based on the judgment of the evaluator, these documents have a required level of detail to ensure good security practices are implemented in the organization.
Partially Acceptable: Security policy and procedures are in place but lack sufficient detail and are older than one year or more than a year has gone by since they were last reviewed.
Unacceptable: No security policy or procedures are in place or policy or procedures have not been reviewed in over two years. Grossly insufficient detail is evident in the security policies and procedures.

Rating: Partially Acceptable

Comments: The Security Policy lacks sufficient detail and, in many cases, there are either inadequate or no accompanying procedures.

Scanning: Not Applicable

Reference to Mitigate Issue: SANS Primer on Security Policy
http://www.sans.org/newlook/resources/policies/Policy_Primer.pdf

1013: IS THERE EVIDENCE OF SEPARATION OF DUTIES BETWEEN NETWORK AND SECURITY ADMINISTRATORS?

Category: Personnel

Risk: Lack of separation of duties and checks and balances can result in intentional circumvention or unintentional failed execution of prudent security practices.

Type: Subjective

Testing: The evaluator shall review policy and procedures to determine if there are requirements to have separation of duties. Perform interviews to determine if separation of duties is practiced and if there are checks and balances in place to review security practices.

Evaluation Criteria:
Acceptable - Policy and procedures are in placing delineating the separation of duties and are being followed within the organization.
Partially Acceptable - Policy and procedures are in placing delineating the separation of duties and these are only partially being followed within the organization.
Unacceptable - No policy and procedures are in placing delineating the separation of duties and no checks and balances are being used to review that proper security procedures are being used.

Rating: Partially acceptable

Comments: The same individuals perform both the network and security administrator roles on the LGOA network. There is limited independent individual checking on the activities of the network administrators.

Scanning: Not Applicable

Reference to Mitigate Issue: NIST SP 800-18 Guide for Developing Security Plans for IT Systems, http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.PDF

1014: ARE INCIDENT HANDLING PROCEDURES IN PLACE?

Category: Incident Handling

Risk: If there are inadequate incident handling procedures in place, an incident could escalate on a network while it is determined how to handle the situation. This could also result in inappropriately shutting down critical systems in response to an incident or failure.

Type: Subjective

Testing: The evaluator shall review policy and procedures to determine if there are adequate incident handling procedures in place. Perform interviews to determine if administrators and users are aware of incident handling procedures.

Evaluation Criteria:

Acceptable - There are policies and procedures in place to handle incidents and at least 90% of administrators and users are aware of these procedures.
Partially Acceptable - There are policies and procedures in place to handle incidents and at least 60% of administrators and users are aware of these procedures.
Unacceptable - There are no policies and procedures in place to handle incidents or less than 60% of administrators and users are aware of these procedures.

Rating: Unacceptable

Comments: There was only a short paragraph on incident handling in the security policy that inadequately covered what to do. Only 25% of the personnel interviewed knew what to do if an incident occurred.

Scanning: Not applicable

Reference to Mitigate Issue: CERT/CC Take appropriate actions
http://www.cert.org/security-improvement/practices/p100.html

1015: IS ALTERNATIVE HARDWARE AVAILABLE FOR RECOVERY OPERATIONS?

Category: Backup and Recovery

Risk: If there is no alternative hardware for recovery operations, it will be difficult to quickly restore operations and provide critical services in a timely manner and ad hoc and on the fly steps will need to be taken to bring operations back on-line.

Type: Objective

Testing: Through interviews and visual inspection, the evaluator will determine if there are alternative hardware devices available for recovery operations.

Evaluation Criteria:
Acceptable - There are alternative recovery devices available for all critical systems.
Partially Acceptable - There are alternative recovery devices available for some critical systems.
Unacceptable - There are no alternative recovery devices available for critical systems.

Rating: Unacceptable

Comments: There are no alternative recovery devices available if the primary device is lost. There are no warm or hot sites identified for use in recovery operations.

Scanning - Not applicable

Reference to Mitigate Issue: NIST SP 800-34 Contingency Planning Guide for IT Systems http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf

1016: ARE BACKUP TAPES STORED IN A SECURE OFFSITE LOCATION?

Category: Backup and Recovery

Risk: Failure to store tapes without enough geographic dispersion can result in loss of the backups in the event of damage to the originating facility.

Type: Objective

Testing: Through interviews and visual inspection, the evaluator will determine if backup tapes are stored offsite.

Evaluation Criteria:
Acceptable: Two criteria are required for an acceptable rating: 1. Policy and procedure requires that backup tapes be stored offsite; 2. Backup tapes are taken off site at least on a weekly basis.
Partially Acceptable - There is no policy or procedure requiring backup tapes to be stored offsite, but in actual practice backup tapes are being stored offsite.
Unacceptable - There is no policy or procedure requiring backup tapes to be stored offsite and backup tapes are not being stored offsite.

Rating: Unacceptable

Comments: Backup tapes are being stored onsite in the same room as the originating device. Backup tapes are not stored in a fireproof or secure location.

Scanning: Not Applicable

Reference to Mitigate Issue: NIST SP 800-34 Contingency Planning Guide for IT Systems http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf

1017: ARE USER AGREEMENTS BEING USED?

Category: Personnel

Risk: Without user agreements, it is not clear what users are entitled to do, and it becomes more difficult to take disciplinary or warning actions against individuals when they circumvent policies and procedures.

Type: Objective

Testing: The evaluator will review the security policy to determine if there is a requirement for users to sign agreements. The evaluator will determine if there are copies of signed agreements on file.

Evaluation Criteria:
Acceptable - Two criteria are required for an acceptable rating: 1. There is policy requiring that user agreements be signed; 2. At least 95% of users have signed an agreement.
Partially Acceptable - Two criteria are required for an acceptable rating: 1. There is policy requiring that user agreements be signed; 2. At least 75% of users have signed an agreement.
Unacceptable - There is no policy requiring that user agreements be signed or less than 75% of users and administrators have signed agreements.

Rating: Unacceptable

Comments: There is no user agreement that clearly outlines what should and should not happen on the LGOA network.

Scanning: Not Applicable

Reference to Mitigate Issue: SANS Acceptable Use Policy
http://www.sans.org/newlook/resources/policies/Acceptable_Use_Policy.pdf

1018: IS THERE A DISASTER RECOVERY PLAN?

Category: Disaster Recovery Planning

Risk: In the event of a disaster, the lack of detailed plans and procedures could have a negative business impact by delaying the recovery of the network.

Type: Objective

Testing: The evaluator will review documentation to determine if there is a Disaster Recovery Plan.

Evaluation Criteria:
Acceptable - There is a Disaster Recovery Plan that has been published or reviewed within the past year.
Partially Acceptable - There is a Disaster Recovery Plan that has not been reviewed or published in the last year but has been reviewed or published within the last 18 months.
Unacceptable - There is no Disaster Recovery Plan or it has been longer than 18 months since it was published or reviewed.

Rating: Unacceptable

Comments: There is no disaster recovery plan or disaster recovery guidance.

Scanning: Not Applicable

Reference to Mitigate Issue: NIST SP 800-34 Contingency Planning Guide for IT Systems http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf

Tab 4 to Appendix A
Case Study Sample Report: Organizational Questionnaire

Organizational Information		
Organization Name: **Local Government Office Agency (LGOA)**		
Point of Contact/Email/Phone: **Sally Jones / sallyjones@lgoa.net / 123-123-4567**		
Address of POC: **LGOA Trailrock, Idaho**		
Number of employees at the site: **92**		
Has a network vulnerability assessment been performed at your organization before? **No**		
Operating Environment		
Total systems at this site: **100**	# Servers and # Clients: **5 servers; 85Clients; 10 UNIX Terminals**	
Operating Systems **Windows 2000; Red Hat Linux; Sun Solaris**		
Information Systems		
Are you currently using any of the following systems?	*(Y/N)*	*Type*
Internet Firewall	**Y**	**Cisco**
Departmental Firewall	**N**	
Intrusion Detection Systems	**N**	
Internet Web Servers	**N**	**Hosted by 3rd Party**
Remote Access/Dialup	**Y**	
Wireless Local Area Networks	**N**	
Virtual Private Networks (VPN)	**N**	
Certificate Servers	**N**	
Anti-virus	**Y**	**Norton Anti-Virus**
DNS Hosting	**N**	
Email Services	**N**	**Hosted by 3rd Party**
Data Backup Systems	**Y**	**ARCServe**
Vulnerability Scanning Tools	**N**	
File Integrity Systems	**N**	
Dynamic Host Configuration Protocol (DHCP)	**Y**	

Tab 4 to Appendix A
Case Study Sample Report: Organizational Questionnaire

Network Information	
Are network diagrams available? **No**	
Number and types of Internet/WAN Connections: **Not sure**	Who is your Internet Service Provider? **Smalltime**
Are there trained network/computer security personnel employed by your organization? **Yes**	Does your organization perform user network/security awareness training? **No**
Does your organization have written security policies and or statements? **Yes**	Does your organization have an information system disaster recovery/business continuity plan? **No**
Does your organization employ login security banners? **No**	Does your organization have formal password procedures? **No**
Does your organization require personnel to have signed network user agreement forms prior to accessing the network? **No**	Does your organization have either written or unwritten incident handling procedures? **No**
Add other questions as deemed necessary.	
Additional Comments	
We need help.	

Tab 5 to Appendix A
Case Study Sample Report: Services and Confidentiality Agreement

LRCC shall conduct a Network Vulnerability Assessment (NVA) of the LGOA's information technology infrastructure at their LGOA Trailrock, Idaho location. LRCC personnel shall be briefed that all information gathered must remain confidential. LGOA network and security personnel shall be made available to work with LRCC in the performance of the NVA and made aware of all activities being conducted. All assessment activities shall be conducted in as non-invasive manner as possible. Certain activities may take place after normal working hours to further minimize any impact. LRCC shall perform the following activities:

- Policy and procedural reviews to ensure consistency with prudent security practices.
- Internet exposure analysis to determine what types of information and resources are publicly accessible from the Internet.
- External and internal network and host mapping to identify operating systems, ports, and services.
- Vulnerability scanning to identify known vulnerabilities and determine if applicable patches are in place.
- Network device reviews to determine if they are securely configured; e.g., firewalls, routers, switches, Virtual Private Network (VPN) gates, Intrusion Detection Systems (IDS), Remote Access Services (RAS), etc.
- Log file reviews to look for anomalies or signs of internal or external probes or attacks.
- Anti-virus detection procedural and implementation reviews to ensure that updated anti-virus software is being appropriately used.
- Password file analysis to identify weak passwords. This shall involve password scanning and cracking to identify weak paswords.
- War dialing to determine if there are open modems in operation that are circumventing firewalls and security boundaries.

LGOA provides permission for LRCC to conduct the activities identified in this agreement.

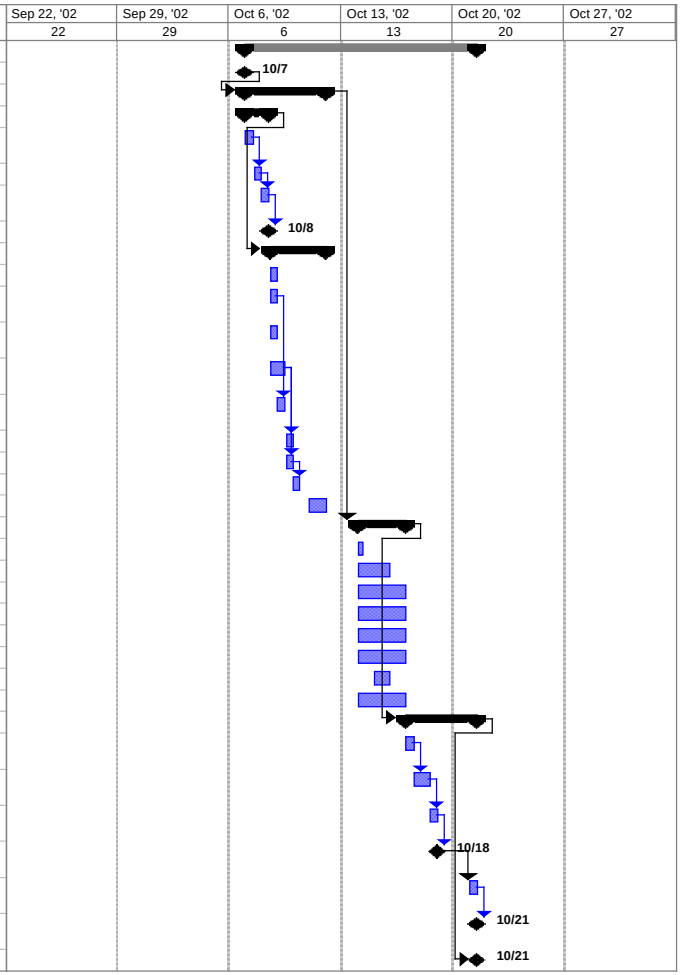
==========

Signed by LRCC Senior Management and Contracts Representative

Signed by two LGOA Senior Managers

Appendix B
Nominal Schedule

ID	Task Name	Duration	Start	Finish
0	**GSNA_Nominal_Schedule**	**10.5 days**	**Mon 10/7/02**	**Mon 10/21/02**
1	Start Assessment Activities	0 days	Mon 10/7/02	Mon 10/7/02
2	**Pre-Assessment Activities**	**5 days**	**Mon 10/7/02**	**Fri 10/11/02**
3	**Define Scope**	**1.5 days**	**Mon 10/7/02**	**Tue 10/8/02**
4	Define Scope and Expectations with Agency	0.5 days	Mon 10/7/02	Mon 10/7/02
5	Prepare Servic e Agreement	0.5 days	Mon 10/7/02	Mon 10/7/02
6	Agency Reviews Service Agreement	0.5 days	Tue 10/8/02	Tue 10/8/02
7	Signed Service Agreement	0 days	Tue 10/8/02	Tue 10/8/02
8	**NVA Prep**	**3.5 days**	**Tue 10/8/02**	**Fri 10/11/02**
9	ID NVA Team Members	0.5 days	Tue 10/8/02	Tue 10/8/02
10	Gather Information about Agency's NW	0.5 days	Tue 10/8/02	Tue 10/8/02
11	Complete organizational questionnaire	0.5 days	Tue 10/8/02	Tue 10/8/02
12	Perform Risk Assessments and ID Critical Systems	1 day	Tue 10/8/02	Wed 10/9/02
13	Obtain and review policies and procedures	0.5 days	Wed 10/9/02	Wed 10/9/02
14	Customize checklists	0.5 days	Wed 10/9/02	Wed 10/9/02
15	ID NVA Tools	0.5 days	Wed 10/9/02	Wed 10/9/02
16	Brief Assessment Team	0.15 days	Thu 10/10/02	Thu 10/10/02
17	Schedule Slack	1 day	Fri 10/11/02	Fri 10/11/02
18	**Assessme nt Activities (On Site)**	**3 days**	**Mon 10/14/02**	**Wed 10/16/02**
19	NVA In-Brief	0.15 days	Mon 10/14/02	Mon 10/14/02
20	Verify Policy & Procedures	2 days	Mon 10/14/02	Tue 10/15/02
21	Conduct Interviews	3 days	Mon 10/14/02	Wed 10/16/02
22	Technical Assessments	3 days	Mon 10/14/02	Wed 10/16/02
23	Conduct Network Scans	3 days	Mon 10/14/02	Wed 10/16/02
24	Conduct Selective Host Scans	3 days	Mon 10/14/02	Wed 10/16/02
25	Conduct Password Checks	1 day	Tue 10/15/02	Tue 10/15/02
26	Analyze Data Collected	3 days	Mon 10/14/02	Wed 10/16/02
27	**Post-Assessment Activities**	**2.5 days**	**Thu 10/17/02**	**Mon 10/21/02**
28	Team member report input	0.5 days	Thu 10/17/02	Thu 10/17/02
29	Prepare Assessment Report	1 day	Thu 10/17/02	Fri 10/18/02
30	Internal Review and Approval of Report	0.5 days	Fri 10/18/02	Fri 10/18/02
31	Assessment Report	0 days	Fri 10/18/02	Fri 10/18/02
32	Provide Assess ment Out Brief	0.5 days	Mon 10/21/02	Mon 10/21/02
33	Assess ment Report Submitted to Agency	0 days	Mon 10/21/02	Mon 10/21/02
34	End Assessment Activities	0 days	Mon 10/21/02	Mon 10/21/02



APPENDIX C
Sample HTML Report Index

Lonesome River Consulting Company (LRCC)

Local Government Organization Agency (LGOA)
Network Vulnerability Assessment Results
October 2002

NVA Report	Scanning Results
Final Report	Summary of Scanning Results
Executive Summary	MBSA Scan of Windows Hosts
Detailed Results Summary	Nessus Scan of UNIX Server
Services and Confidentiality Agreement	Nessus Scan of Windows Servers and Hosts
References	War Dialing Results
Organizational Questionnaire	NMAP Scan of Network
Network Diagram	Patch Scan of UNIX Server

NVA Report Presentation

APPENDIX D
ACRONYMS

CIS	Center for Internet Security
CISA	Certified Information Systems Auditor
CISSP	Certified Information Security Professional
COBIT	Control Objectives for Information and related Technology
CSI	Computer Security Institute
CSRC	Computer Security Resource Center
DSL	Digital Subscriber Line
GCFW	SANS GIAC Certified Firewall Analyst
GCIA	SANS GIAC Certified Intrusion Analyst
GCIH	SANS GIAC Certified Incident Handler
GCUX	SANS GIAC Certified UNIX Security Administrator
GCWN	SANS GIAC Certified Windows Security Administrator
GIAC	Global Information Assurance Certification
GSEC	SANS GIAC Security Essentials Certification
GSNA	GIAC Systems and Network Auditor
IA-CMM	Information Assurance – Capability Maturity Model
IAM	INFOSEC Assurance Methodology
IEC	International Electrotechnical Commission
IPAK	Information Protection Assessment Toolkit
ISACA	Information Systems Audit and Control Association
ISO	International Standards Organization
ISP	Internet Service Provider
LGOA	Local Government Office Agency
LRCC	Lonesome River Consulting Company
MBSA	Microsoft Baseline Security Advisor
MCSE	Microsoft Certified Systems Engineer
NAT	Network Address Translation
NIPC	National Information Protection Center
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVA	Network Vulnerability Assessment
OSTMM	Open Source Testing Methodology Manual
PMP	Project Management Professional
RAS	Remote Access Services
RAT	Router Audit Tool
SANS	System Administration, Networking and Security
SCORE	Security Consensus Operational Readiness Evaluation

APPENDIX E
REFERENCES

"CIS Website (Use the "What are the benchmarks?" link)." URL: http://www.cisecurity.org/.

"COBIT®. 3rd Edition Executive Summary." July 2002.

"CSI Publications: CSI IPAK." URL: https://wow.mfi.com/csi/order/publications.html.

"IA-CMM Capability Maturity Model. Version 2.1. February 2002. URL: http://www.iatrp.com/.

"ISO/IEC 17799." First Edition. December 12, 2000.

"National Security Agency's INFOSEC Assessment Methodology Student Manual".

"The Human Firewall Manifesto." URL: http://www.humanfirewall.org/rhfwm.htm.

CERT CC. "Develop and Promulgate and Acceptable Use Policy for Workstations." URL. http://www.cert.org/security-improvement/practices/p034.html.

CERT CC. "Monitor and Inspect System Activities for Unexpected Behavior." URL: http://www.cert.org/security-improvement/practices/p095.html.

CERT CC. "Take Appropriate Actions Upon Discovering Unauthorized, Unexpected, or Suspicious Activity." http://www.cert.org/security-improvement/practices/p100.html.

CIS IPAK Information. URL: https://wow.mfi.com/csi/order/publications.html.

COBIT Download. URL: http://www.isaca.org/ct_dwnld.htm.

COBIT FAQ." URL: http://www.isaca.org/faq_r.htm#r3.

Computer Security Institute Press Release. "Cyber crime bleeds U.S. corporations; financial losses from attacks climb for third year in a row." April 7, 2002. URL: http://www.gocsi.com/press/20020407.html.

Guel, Michelle D. "SANS A Short Primer for Developing Security Policies." 2001. URL: http://www.sans.org/newlook/resources/policies/Policy_Primer.pdf

Herzog, Pete. "Open-Source Security Testing Methodology Manual." Release 2.0 Candidate 6. February 26, 2002.

IAM and IA-CMM Information. URL: http://www.iatrp.com/.

Incident.org Incident Forms. URL: http://www.incidents.org/Incident_forms/.

International City/County Management Association. "Electronic Government 2002 Survey Results, Question 10c." URL: http://icma.org/download/cat15/grp120/sgp224/egov2002web.pdf.

ISO/IEC 17799 Purchase. http://www.ihs.com/index.html.

Kingpin. "Wardialing Brief." URL: http://www.atstake.com/research/reports/acrobat/wardialing_brief.pdf.

Naidu, Krishni. "SCORE Firewall Checklist." URL: http://www.sans.org/SCORE/checklists/FirewallChecklist.doc

National State Auditor's Association and U.S. General Accounting Office. "Management Planning Guide for Information Systems Security Auditing." December 10, 2001. URL: http://www.gao.gov/special.pubs/mgmtpln.pdf.

APPENDIX E
REFERENCES

NIPC Password Protection 101. URL: http://www.nipc.gov/publications/nipcpub/password.htm.

NIST SP 800-37 Information. http://csrc.nist.gov/sec-cert/.

Office of Homeland Security. "The National Strategy for Homeland Security." July 16, 2002. URL: http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf.

OSSTMM Download. http://www.ideahamster.org/download.htm.

Ross, Ron and Swanson, Marianne. "Draft: NIST Special Publication 800-37: Guidelines for the Security and Accreditation of Federal Information Technology Systems." Version 1.0. October 2002. URL: http://csrc.nist.gov/sec-cert/SP-800-37-v1.0.pdf.

SANS Guidelines on Anti-Virus Process. URL: http://www.sans.org/newlook/resources/policies/Anti-virus_Guidelines.pdf.

SANS INFOSEC Acceptable Use Policy. URL: http://www.sans.org/newlook/resources/policies/Acceptable_Use_Policy.pdf.

SANS Security Policy Templates. http://www.sans.org/newlook/resources/policies/policies.htm#template.

Score Website. URL: http://www.sans.org/SCORE/.

SSH Website. URL: http://www.ssh.com/products/ssh/.

Sun Patches. URL: http://sunsolve.sun.com/pub-cgi/show.pl?target=patchpage

Swanson, Marianne. "NIST SP 800-18: Guide for Developing Security Plans for Information Technology Systems." December 1988. URL: http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.PDF.

Swanson, Marianne. "NIST Special Publication 800-26: Security Self Assessment Guide for Information Technology Systems." August 2001. URL: http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf..

Swanson, Marianne; Wohl, Amy; Pope, Lucinda; Grance, Tim; Hash, John; Thomas, Ray. "NIST SP 800-34: Contingency Planning Guide for Information Technology Systems." June 2002. http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf.

The President's Critical Infrastructure Protection Board. "The National Strategy to Secure Cyberspace." September 2002. URL: http://www.whitehouse.gov/pcipb/cyberstrategy-draft.pdf.

"U.S. Department of Commerce Manual of Security Policies and Procedures." URL: http://www.osec.doc.gov/osy/SECURITYMANUAL/Chapter39.htm.

Wack, John, Tracey Miles. "NIST SP 800-42: Draft Guidelines on Network Security Testing."

Wilson, Mark and Hash, John. "NIST SP 800-50: Building an Information Technology Security and Awareness Training Program." 1st Draft. July 2002. URL: http://csrc.nist.gov/publications/drafts/draft800-50.pdf.

Last Updated: July 23rd, 2017

Upcoming Training

SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS AUD507 (GSNA) @ Canberra 2017	**Canberra, Australia**	**Oct 09, 2017 - Oct 14, 2017**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**