Global Information Assurance Certification Paper

G I A C FOUNDATION

PROTECTING ITS "CROWN JEWELS"

GIAC Information Security Officer (GISO)
Practical Assignment – Version 1.2

Bobbi Spitzberg
October 17, 2002

ABSTRACT

The GIAC Foundation (GF) is a small, private foundation. The mission of the Foundation is to support promising scientific research. We are especially interested in funding research that may not qualify for funding by the Federal Government. We also support scientific policy development and graduate educational opportunities in pure and applied scientific research.

The intention of this paper is to inform the reader about the business of the Foundation, the IT infrastructure and overall security posture, including the critical IT security risks to the Foundation and planned and/or implemented processes to address and mitigate these risks. We will address all of this in the context of GF's mission and how we do business to achieve that mission.

Since unauthorized access to the Foundation's IT infrastructure and its associated servers and data would adversely affect the accomplishment of the Foundation's mission, we include a proposed new password policy and procedures at the end of this document. Stronger authentication will help to mitigate the risk of unauthorized access.

THE GIAC FOUNDATION – A DESCRIPTION

The GIAC Foundation is a small, private foundation whose mission is to support promising scientific research. We are especially interested in funding research that may not qualify for funding by the Federal Government. We also support scientific policy development and graduate educational opportunities in pure and applied scientific research through grant awards of varying duration and amounts. Grant submission and review is totally electronic. We have recently included the digital signing of proposals to the application submission process.

GIAC FOUNDATION IT INFRASTRUCTURE

To best protect the Foundation's IT resources from external and internal threats, we have adapted a defense-in-depth strategy. Defense-in-depth does not rely on one single defensive mechanism. It is a methodology that uses several layers of defense against an intruder and can easily be applied to IT security to protect against cyber intruders. The layers work to reinforce each other. For example, we do not rely only on our perimeter firewall for protection of our internal network. We have various layers of network protection, a rigorous system configuration policy, and are continually working to strengthen user authentication.

Our first layer of defense is a Cisco 3660 Series router at the perimeter. We use some of the secure administration suggestions from Bang Shuh Tan's paper on Cisco routers. [1] We use ACLs on the routers only to stop specific inbound and outbound traffic. For example, we block all traffic to and from ports 137 through 139 (NetBIOS) as well as telnet (port 23) and ftp (ports 20 and 21). We believe that routers should primarily be used for what they are designed for – moving packets, not stopping them.

For stopping packets, we use firewalls. We have chosen Lucent VPN Firewall Brick ™ 201 because of the following features:

- State of the art distributed denial of service attack protection
- Strict TCP and IP packet validation
- Virus scanning
- Operates as a Layer 2 bridge, so it is invisible on the network. [2]

We have been happy with the performance, ease of use, and security features of these firewalls.

We are currently in the process of purchasing additional firewalls so that we can have redundancy in this important area of our IT security architecture. One of the features of the Lucent bricks and the Lucent Security Manager Server (LSMS) is subsecond stateful failover. Stateful failover means that the primary and the secondary firewall exchange session-state information over a dedicated

[1] Tan
[2] Lucent

private link. If one firewall were to fail, the other would take over without session interruption. The secondary firewall continues processing traffic. [3] This works so quickly that if the primary firewall were to fail during a secure copy (scp) session, no data would be lost because of the failure of the firewall. This eliminates the firewall as a single point of failure.

We have one Lucent 201 brick in front of our external servers – email server, external Domain Name Server (DNS), and our external web server. It limits the network traffic to only those protocols that are intended for the appropriate use of these hosts. One of the 3 outbound interfaces of this brick goes to a switch that connects to the email server and the DNS server. Another interface connects to a switch connected to the primary and secondary web servers. The rule set in the firewall isolates the traffic between these machines.

In this layer, we have the Cisco 3000 series concentrator, which we use for our VPN. All our System and DBA administrators use the VPN to access our servers remotely when necessary for off-site problem determination and resolution. GF has provided each of them with a Dell Inspiron 8000 laptop configured with a Cisco VPN client for this purpose. The Cisco VPN concentrator maps the username and password of each authorized remote user to a pre-determined subnet of the VPN IP address range. These subnets have very specific access rules in all the GF firewalls. For example, the subnet associated with the System Administrators will have ssh access to the production servers. RAAs and reviewers are also provided with a VPN client and use it to access their GF email accounts. RAAs also have limited SQLNET access to the database.

We have positioned a second Lucent Brick 201 in front of our internal network. One interface is connected to a switch for our internal network PCs, internal email server and internal name server. The second interface connects to a switch in front of our production database server cluster as well as our Storage Area Network (SAN) – our "crown jewels". The third interface connects to a third Lucent brick that isolates development and test environments from the production environment.

The web servers use Secure Socket Layer (SSL) for its increased security through authenticated and encrypted communication between the clients and the GF server. The cipher used is RC4 with 128-bit encryption and MD5 message authentication. This is the second strongest cipher available next to Triple DES, which uses a 168-bit encryption. [4] Therefore, grant transmissions and digital signature verifications, as well as other sensitive Foundation business, are reasonably secure as they traverse the Internet.

---

[3] Fratto
[4] Introduction to SSL

An important part of our security posture is to separate the development environment from the productions servers and data. Production databases are separated from test/development data by zones created on the SAN as well as restricting access by careful firewall rule formulation. We are also investigating the feasibility of procuring additional servers devoted exclusively to the test environment.

Our production web servers are Sun Microsystems SunFire™ V480, each with 4 900 MHz processors with 8 Gigabytes of memory. The Operating system is Solaris 8. The Application Server software is Oracle Application Server 9iAS version 1. Although there are redundant hardware features in these servers, we are considering clustering our web servers in the future. We may use Tru64 Unix and TruCluster running on HP Alphaservers in the middle tier as we presently do in the backend. In order to increase availability in our present environment, we have configured primary and secondary web servers. We have developed our own procedure for accomplishing failover from the primary to the secondary server if necessary. Files on the web servers are synchronized using rdist. The OS and Oracle Application Server configurations are identical. The failover procedure checks for a heartbeat on the primary server every 30 seconds and uses other checks to determine if it is necessary to switch from the primary to the secondary server. In this way we have eliminated the web server as a single point of failure. Nevertheless, this solution does not provide us with the kind of high availability that we would like to achieve.

Our production database server is clustered using 2 HP Alphaserver ES45 each with 4 1.25 GHz Alpha processors and 16 G of memory. The development/test environment is also clustered. For that environment we currently use 2 HP AlphaServer DS20's with 2 500 MHz processors and 4 Gigabytes of memory. All of our HP servers are running Tru64 Unix Release 5.1A, patch kit 4. We have 2 HP SAN storage cabinets, one for the production environment and one that is used by the test/development cluster. The production database is mirrored on the SAN. We have sufficient disks on the production SAN for database hot backups, full database exports, incremental exports as well as full Unix level cold backups. The backend RDMS is Oracle, version 8.1.7.2. We are planning to upgrade to 9i in early 2003.

For tape backups we use HP StorageWorks Enterprise Backup Solution.

BUSINESS OPERATIONS

GF uses its web site to disseminate information about the foundation, search the awarded grants database, review grant applications, obtain information about the process of proposal submission, and the actual electronic submission of grant proposals. These various uses require correspondingly varied security requirements. Since so much of the Foundation's business depends on the

World Wide Web, the availability of the network and the web server is essential to accomplishing the Foundation's mission.

All grant proposals are submitted electronically through the Foundation's web site. Application authenticity is verified by Registered Authorizing Authorities (RAA) who, by digitally signing an application, verify the identity of the grantee (Principal Investigator, PI) named on the application as well as the authenticity of the grant proposal itself. Digital signatures are obtained in a similar manner to electronically filed tax returns. RAAs authenticate to the appropriate "signing" screen by providing not only their GF database password, but also their social security number, date of birth, and last name. A "digital signature" is obtained by the RAA clicking on the **Sign** button of the appropriate screen. The National Science Foundation's FastLane digital signing system has been used as a model for GF's digital signing procedure. More information on NSF's FastLane can be found at the URL, https://www.fastlane.nsf.gov/guides/EB_Proposal_Submission.pdf.

Scientific research grants are awarded directly to individuals with proven scientific research ability and creativity. It is the mission of the Foundation to support research that might otherwise not have found adequate support. For example, we support research projects that might not be able to obtain funding from the Federal Government, e.g. embryonic cells lines created after August 9, 2001 which are ineligible for federally funded research. [5]

The grant application review process utilizes external reviewers who need to access the grant applications they review before their review council meets. Until a grant is awarded, the application and evaluation information is considered sensitive. Even though we are not a Federal agency, we use the IT Security Policies and Guidelines of the Federal government as guidelines for our security posture. A listing of these policies can be found at the web site for the National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC), at the following URL, http://csrc.nist.gov/policies/.

Reviewers access grant applications by authenticating to the web site. They can only see and review specific grant applications. The access is controlled by roles defined in the database.

Internal users access the internal network from their workstations. The internal network serves the entire Foundation staff. The firewall rules and individual access rights on the various applications and platforms control appropriate access for this staff. For example, internal users are allowed outbound access to external web servers. System administrators and database administrators have the capability for remote monitoring through the VPN.

[5] National Institutes of Health

Email is another important IT function to the Foundation. Much of the inquiries about the program are from email initiated from the web site. Email is also an important way that reviewers communicate with the foundation and with each other. All reviewers are given foundation email addresses. Access to their GF mail accounts is via a VPN. We have also set up Outlook Secure Email. All email between reviewers and the Foundation is required to be digitally signed using secure email.

All Personnel IT functions are outsourced. Independent suitability investigations of employees are done by the HR contractor in much the same way they would be done for accessing sensitive Federal grants applications. This is particularly important for the Systems and Database Administrator staff. The Foundation does have a small HR staff on site.

GF is dependent on the availability of all processes and data associated with Electronic Proposal Submission. This includes the web server for the submissions as well as the database containing grants proposals, information about the investigators and reviewers. Proposals can be submitted from anywhere in the world, requiring 24 by 7 availability. The Computer Operations group is responsible for making sure of that availability for the servers and databases. Network Operations is concerned with all issues of connectivity and network security.

The responsibilities of these groups include:

- All issues concerning secure, reliable access to the Internet. This includes routers, firewalls, external and internal DNS servers, monitoring appropriate logs, and intrusion detection software (IDS). For our IDS, we currently use snort, a well-respected and very flexible Network Intrusion Detection (NID) freeware tool, http://www.snort.org/.
- Server configuration.
    - The database backend servers are HP (formerly Compaq Alpha) boxes running Tru64 Unix in a 2-member cluster.
    - The web servers are Sun Microsystems SunFire™ V480 running Solaris 8.
    - The mail servers are Microsoft Exchange servers that run Exchange 2000 Version 5.5.
- All workstation support (configuration and maintenance). The Dell Optiplex workstations are currently running Windows 2000 Professional OS SP-2. Dell Inspiron Laptops use the same standard configuration as Foundation desktops with the addition of Cisco VPN 3000 clients to assure secure connectivity offsite.
- Disaster/Recovery planning and testing. The Computer Operations staff work with Foundation business process management to coordinate D/R with Contingency planning.
- Hardware/software planning, configuration and maintenance.

- Anti-Virus software – Norton Antivirus Corporate Edition 8.0.

IDENTIFICATION OF THE PRIMARY RISKS

The Foundation has identified 3 critical risks. They are:

- Unavailability of the Foundation's web server
- Unauthorized access to the grants proposal database including digital signature information
- Inadequate backup and recovery procedures

THE RISKS

Risks are potentials for loss or harm. GF's business is totally dependent on the World Wide Web and the integrity and availability of our database. Any threat to the availability of the web server and database and the integrity and confidentiality of the data represents a risk to GF.

The factors involved in security risks are the value of the information, the threat to that information and the vulnerabilities that exist that would allow these threats to occur. [6] A threat could be intrinsically high, but the vulnerability may be low or non-existence at GF and it would, therefore, not constitute a risk. For example, the threat of a compromise of a Microsoft IIS server is fairly high. But at GF, this does not exist as vulnerability and therefore represents no risk. In the detailed discussion of GF's critical risks, we will analyze the severity of the threat in the context of the likelihood it will occur.

UNAVAILABILITY OF WEB SERVER

The threat

The GF web server **is** the Foundation to the outside world. All grant proposals are submitted via the web. Without the web server, no foundation business could proceed. Since this is so integral a part of the business goals of the Foundation, the loss of the web server is a major threat.

Impact of this risk on GF

A loss of the web server would lead to a loss of confidence in the foundation. Since we promote and facilitate scientific research, the loss of such a visible technological resource would be viewed particularly negatively.

The web server is a gateway to sensitive, confidential information. This includes grant proposals, the roster of our reviewers, and the information required to provide digital signatures. Corruption of any of this information would severely harm the Foundation's ability to do business and possibly irrevocably harm its public image.

Likelihood of occurrence

By definition, all public web servers are exposed to attacks or they wouldn't be public web servers. Microsoft IIS web servers are the most frequently attacked with Linux environments running Apache being the second most frequently attached web server environments. [7] Our Unix platform web servers are less likely to be attacked, but the threat is still real and still highly likely.

---

[6] SANS Institute, Track 9, Information Security Officer Training, Book 9.1, p.1-10.

[7] Farrow

Mitigation strategy

We migrated our web servers to the Unix platform several years ago because Windows Internet Information Server (IIS) is known to be very popular with hackers and new exploits are continually developed.[8] We believe Unix to be a more robust platform than Windows.

As part of our high availability solution, we have clustered the production database server. We are using HP Alphaservers running Tru64 Unix. We have 2 identical servers. One is configured as the primary server. When the primary server becomes unavailable, the primary database server automatically rolls over to the other server.

Our web servers are redundant, but not clustered. We use a homegrown failover procedure, which checks for a heartbeat from the primary web server and fails over to the secondary server within 2 minutes. This has worked well on the few occasions when we have had to use it, but is still not as good as a clustered environment.

All servers are connected to a central Universal Power Supply (UPS) in the server room. We are also investigating having the production web servers and database backend on their own UPS. We have experienced outages because of failures in the UPS unit and during UPS testing and maintenance.

We have been following Best Practices for securing web servers from the National Institute of Standards and Technology (NIST). [9] We also are developing more stringent configuration management procedures including development of a standard configuration template. At GF, securing the web server begins with planning the OS installation. We utilize NIST's "Securely Installing and Configuring the Web Server Checklist" which is described in the very helpful NIST guide for securing web servers. [10] We are in the process of fully incorporating the other NIST checklists for securing web servers into our architecture.

Encryption is currently used to protect the information flow to and from the web server on the Internet via SSL.

We are also investigating establishing more redundancy on the network. We currently use HP's NetRAIN (Redundant Array of Network Adapters) to protect us from network interface failures on the backend database servers. We still have no failover capability for our firewalls. The firewall, therefore, represents a single point of failure. We want to upgrade our firewall configuration to eliminate the firewalls as a single point of failure. As part of our network security strategy, we

[8] Pisetsky
[9] Dillard
[10] NIST, Guidelines for Securing Public Web Servers

review our firewall rules and network design quarterly. This is all in addition to our exploration of the feasibility to clustering the web server.

Since web servers are popular targets for exploits and are such an essential part of our business we will continue to develop mitigation strategies. Our current program does bring the web servers into an acceptable level of risk.

We have studied the SANS Institute Top 20 vulnerabilities and attempted to mitigate as any as we could.[11] For example, we do not use the Remote Procedure Calls and have implemented SANS recommendations for Apache server configuration and CGI scripts.

[11] The SANS Institute Top 20 List, http://www.sans.org/top20.htm

UNAUTHORIZED ACCESS

The threat

The “crown jewels” at GF are the grant proposals. The integrity of the proposals must be protected. All proposals have to be submitted through a verification process that includes obtaining the digital signature of a Registered Authorizing Authority (RAA.) Not only must the integrity of the proposals themselves be protected, but it is essential that only RAA verified proposals be entered.

Our reputation is interconnected with the quality of research we support. It would be very destructive to the Foundation if the scores entered by the reviewers were changed enabling the rewarding of a grant to an undeserving project. The RAA database is just as important since the RAA assures the authenticity of the Principal Investigator and the associated proposal.

Impact of this risk on GF

One of the most important “products” of a non-profit foundation is its reputation. Any event that adversely affects the reputation of the Foundation reduces its effectiveness. Also affected are the grantees, since the credibility of the merit of the awards themselves would be at risk. Grant amounts could also be falsified by any unauthorized access, possibly causing a direct adverse financial impact on the Foundation. The potential for financial loss is high.

Likelihood of occurrence

The likelihood of attempted unauthorized access occurring is high. Because we do not currently enforce a strong password policy, the vulnerability of this occurring is also high. We view unauthorized access as a high risk for us.

Mitigation strategy

Our network architecture does provide protection for us. A strong network architecture is only part of a good defense-in-depth strategy. Strong authentication policies and procedures are also necessary. We also do not use operating systems configurations “out of the box.” The System Administrators regularly monitor the appropriate LISTSERVs for the COTS products and operating systems we use for security alerts and new patches. We apply these patches quickly to our test environment and migrate them to the production environments as soon as adequate testing has been done.

In order to provide more reliable authentication we will develop a strong password policy. Passwords have a minimum length of 6 characters and require at least one numeric and one alphabetic character. The password history depth is 5 and a minimum time between password changes is established. Such a time criteria prevents users from cycling easily through the history until they can reestablish the original password. Triviality checks are built into the password

selection checking module. A password lifetime is essential. Failed login attempts as well as password changes need to be audited. Protecting the integrity of the audit logs is another essential part of this overall strategy. Periodically, password cracking programs will be run.

Essential to the success of any policy is compliance and management support. Policy development will be coupled with a strong security awareness program. We want to make sure that management buys into our efforts and understands the importance of general IT security and strong authentication as an important part of the total security posture. The awareness program will be an important part of our security program in the future.

No group accounts will have login access to the servers themselves for more direct accountability. Stricter password guidelines such as shorter password lifetimes will be developed for users with administrative access to servers than for general users.

How the initial password is conveyed to the users is an important part of password policies that is often overlooked. Email must not be used unless it is encrypted and digitally signed. Nor should passwords be routinely faxed. Passwords should be given to the users directly, either in person or directly on the phone. No matter what method is chosen, the identity of the user must be confirmed before the password is divulged.

Authentication for RAA signatures must be particularly meticulous.

INADEQUATE BACKUP AND RECOVERY PROCEDURES

The Threat

Having grant proposals available for review and being able to authenticate and digitally sign new grants is the essence of the business of the Foundation. If data is corrupted either by accident or malicious intent, the databases need to be restored in a timely fashion and with accuracy.

Impact of this risk on GF

The impact of a failure to restore data and/or the Operating System environment in a timely fashion is great. The Foundation's "products" are its philanthropy, its reputation, and its extensive database containing information about significant current scientific research efforts. The loss of this data is as significant to us as the loss of manufacturing proprietary information would be for a manufacturing business.

Likelihood of occurrence

Within the last year, we experienced a 3 day outage of our primary database server because of poor Operating System maintenance and backup procedures. We have since developed more robust procedures for both OS maintenance and backup/recovery. Therefore the current vulnerability for this threat is relatively low. We will continue to evaluate and improve our backup strategy when necessary. As part of ensuring that this vulnerability remains low, we will continue to vigorously test our recovery procedures.

Mitigation strategy

Regular backups are taken. A variety of backups are available for the databases. Currently full exports (weekly) and incremental exports (daily) are used as well as hot backups (twice daily). Weekly OS level backups are also taken. The hot backups are done to disk on the SAN.

Backups are run automatically. Email is sent to the System and Database Administrators when the backup script is started and upon successful completion of the backups. If the backup completes abnormally, an email is sent with error messages indicating the reason for the failure.

Backups of the OS are also done weekly to tape. Log and audit files are backed up separately as well. There are plans to isolate all logs to a separate log server that is inaccessible from the Internet for even greater security.

The full backups are on a 6 week cycle so there is more than a full month of backups. We also run quarterly backups which are retained for 15 months and

year end backups which are retained for 2 years. All backup tapes are stored offsite, but can be on site within 1 hour if necessary.

Having a robust backup schedule and redundancy of backups is important, but no backup strategy is complete without frequent and thorough recovery testing. We test our recovery procedures at least once a month. We do hot site testing twice a year. We are in the process of evaluating our Disaster/Recovery Plan and seeing how it and our backup/restore procedures may be improved.

We are hopeful that the procedures outlined above reduce our risks for database unavailability because of poor backup and recovery procedures.

SECURITY POLICY EVALUATION AND DEVELOPMENT

Security policy is important because it provides a framework and justification for making security related decisions. Policy is used to help establish the behaviors required to strengthen and conform to an organization's business goals and to discourage those behaviors that detract from them. Dan McGinn-Combs in his excellent article on developing security policy articulates the objectives of security as enabling the business to operate without being adversely affected by externally caused interruptions, allowing the organization to conduct its essential business communications that require the Internet as well as identifying and responding to any attempted or actual disruptions of the organization's business. McGinn-Combs also emphasizes the importance of being able to measure security policy compliance and the tremendous value that conformance has for the organization.[12]

Security policy protects both the information and the people accessing this information.[13] A clearly articulated policy and its associated procedures allow people to take the actions and make the decisions associated with the areas covered by the policy without fear of reprisals. At GF, we are determined that any policy we develop will achieve a balance between access, business needs and security. By access, we mean that increased security will not adversely affect performance or ease of use. By security, we mean the traditional security triad – confidentiality, integrity and availability.

There are 3 generally accepted types of security policies – program policy, issue-specific policy, and system-specific policy. The new password policy we are developing is an issue-specific policy.

Conducting a risk assessment is an essential first step in the security policy formulation process. We have already determined one of GF's critical risks is unauthorized access. One of our mitigation strategies for this risk is to strengthen passwords. Our new policy is an important part of that.

We at GF are actively moving toward revising and developing security policies as part of our proactive strategy in managing IT risk. We are adapting the 4-step approach for Using Security Policy to Manage Risk as outlined by Stephen Northcutt in the Class 9.4 notes for the GIAC Information Security Officer Track.[14] The first step is to identify the risks. Possibly the most important step is to communicate the outcome of this risk assessment to management. Without their support and understanding of the risks and mitigation strategies, nothing will change, except possibly to erode the security of your organization.

---

[12] McGinn-Combs
[13] SANS Institute, Track 9 – Information Security Officer Training, 9.4, p. 4-A.
[14] Northcutt, Stephen, Basic Security Policy, v 1.7, SANS Institute, Information Security Officer training materials, 9.4,p. 10-A.

The third step is to develop any new policies that are needed and review and update existing policy when necessary. We emphasis the importance of compliance, which is the fourth step. If it is not possible to measure compliance, then you can't enforce the policy. A policy that can't be enforced is of little or no value.

EVALUATION OF AN EXISTING POLICY

In order to better address the risks involved with unauthorized access, we at GIAC Foundation have decided to make strengthening our password policy a priority. We have used the Internet as a resource to find existing password policies to use as guides for the development of our own policy and procedures. We found the policy of the National Energy Research Scientific Computing Center, High Performance Computing Center especially interesting because of its requirement to have users sign a user policy form before an account/password would be issued. Their password policy can be found at http://hpcf.nersc.gov/policy/password.html.

We will analyze the NERSC policy before adapting it for our own use. We do not want to imply any negative criticism of the NERSC policy. The policy is well formulated for their purposes. This analysis is part of an effort to customize their policy to meet the requirements of GF. Therefore, it should not be construed to be in any way negatively about the inherent value in the policy itself.

The complete text of the NERSC policy can be found can be found in Appendix B.

Purpose. The Summary statement box serves as the statement of the policy's purpose. It defines user identifiers and passwords and summarizes very briefly some of the features of the policy. However, it does not articulate the importance of good password selection to the security of the organization and how the policy will establish the necessary standards for strong password selection, the protection of those passwords, and issues relating to password aging.

Related Documents. The general page for Policies, Procedures and Request Forms, URL: http://hpcf.nersc.gov/policy/, contains the information that the policies and procedures at NERSC originate from DOE regulations, DOE and NERSC management, and user requests. NERSC is part of the Lawrence Berkeley National Laboratory whose researchers are funded by the Department of Energy Office of Science. This is very helpful for obtaining general information about NERSC's security policies.

Cancellation. No information is given about the policy having been superceded or canceled. The assumption is therefore that this policy does not supercede an existing policy, but we can't determine that definitely.

Background. No background section is included. This is an optional section for policies. The Related Documents section does serve some of the same purpose as a background section would.

Scope. There is no specific Scope section but the scope is clearly defined in the Summary box. The scope of a policy refers to the people to whom the policy applies or the entity to which the policy applies. The policy applies to all users on each of the NERSC systems. Each user must have a unique account.

Policy statement. The policy statement needs to define what decisions and actions fall within the scope of the policy. It also needs to define the associated appropriate actions covered by the policy. The NERSC identified and clearly presented the policy for new users, login failures, obtaining new passwords, changing passwords, how initial passwords are obtained, differences between different systems.

Responsibility. The responsibilities of the user is scattered throughout the policy. There is some mention of the responsibilities of the Account Support Group as well. It would be clearer to have the responsibilities organized into one section.

Action. This is the strongest part of the policy. New users know how they have to obtain an account, how they will obtain the initial password, the time frame required for a new user to activate their account, etc. It is easy for the new user to obtain the form required and understand what happens next.

The policy has very good content. However, in order for the policy to be clearer, it needs to include separate scope, responsibility and policy sections.

PASSWORD POLICY FOR GIAC FOUNDATION

We have used the analysis above to adopt the NERSC policy to the GIAC Foundation. There are both similarities and differences between the research environment at NERSC and GF.

1.0 Purpose

This policy is intended to reduce the risk of unauthorized access to servers and databases essential to the mission of the GIAC Foundation. It defines:

- strong password standards
- password lifetimes
- standards for password policy verification
- standards for the establishment of passwords and modification of passwords
- Compliance and enforcement procedures

This policy addresses the risk of weak passwords as well as password disclosure – intentional or unintentional, malicious or benign – and hence, unauthorized access to servers and data.

2.0 Background

It is a well-established principle of IT security that strong passwords are an important part of any organization's security posture. Weak passwords can lead to unauthorized access. Such access would threaten the confidential grant proposals, Registered Approval Authorities, grant review scores and other information whose integrity is essential to the mission of the Foundation. Easily guessable passwords are one of the most common ways to accomplish unauthorized access to any system. The National Institute of Standards and Technology suggests several ways to assist in the mitigation of the risks associated with unauthorized access by using better password policies in their document Generally Accepted Principles and Practices for Securing Information Technology Systems, URL; http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf. NIST suggests that organizations clearly specify required password attributes. These should include minimum and maximum lengths, the type of characters that are acceptable, and contextual criteria. NIST goes on to suggest that passwords should be changed periodically and that users should be trained in good password selection.

3.0 Scope

This policy applies to all users who access GF servers and databases, including development and test servers and databases, as well as the personal workstations used to access these server and databases.

4.0 Policy

4.1 General Requirements

- Each user must have a unique username and password combination.
- Each user must have had a satisfactory suitability designation form completed and have been sponsored by either the Human Resources Department or an RAA.
- Each user must have a signed and dated user policy form on file before an account and password will be issued.
- Initial passwords must be communicated to the user securely.
- Initial passwords are pre-expired.
- New users must change the initial password by logging into the system within 5 days of issue.
- System level passwords, passwords for application administrative accounts, system administrator accounts, and database administrator accounts must be changed at least every 90 days.
- General user passwords must be changed at least every 6 months.
- Accounts associated with passwords that have been expired for more than 45 days will be deleted.
- All user level and system level passwords must conform to the password standards listed below.

4.2 Password Formulation Standards

- Password length must be between 6 and 10 non-blank characters.
- Must contain a mixture of alpha and numeric characters, as well as special characters.
- At least one special character must appear in the first 5 characters.
- The first and last characters must not contain numbers.
- The password cannot contain the user's login name.
- The password cannot contain the user's own or close friend's or relative's name, employee number, social security number, birthday, significant anniversary, telephone number, address, or any other information about the user that could be easily guessed or discovered.
- Passwords must not contain common words or words found in any dictionary.
- Keyboard patterns cannot be used.
- Simple guessable patterns cannot be used, e.g. qwerty.

4.3 Password Change Requirements

- A password history of 6 generations is kept. This is to prevent frequent reuse of the same password.
- Passwords changes must be at least 24 hours apart to discourage cycling through the password history to obtain the same password.
- New passwords cannot be a simple change of the previous password, e.g. adding a number at the beginning or end, changing one letter or number.
- Passwords must be changed immediately if they have been given to someone else.
- Passwords must be changed as soon as possible after a compromise and within one business day.
- A password must be changed if directed to do so by GF Account Support Group Staff.
- Passwords are not shared across systems. Changing a password on one GF system does not change it on another.

4.4 Protecting Passwords

- Password cracking tools will be run periodically. Users will be notified of weak passwords and have no more than 1 day business day to change them. After that time, the account will be locked.
- The account will be locked after 3 consecutive unsuccessful login attempts
- Automatic password aging controls will be configured into the Operating System.
- Dictionary triviality checks will be configured in the Operating System where feasible.
- To prevent accidental disclosure the following precautions must be taken:
  - Passwords must not be disclosed to anyone, including anyone claiming to be Account Support Group Staff or high ranking Foundation management.
  - Passwords must be stored in an encrypted form on any file, including a PDA.
  - Users should not communicate his/her password or password paraphrase in an email.
  - Passwords should not be written down.

4.5 Passwords Within Applications

- Authentication must be to individual users, not groups.
- Passwords cannot be stored in clear text anywhere within the application or within a file.
- Role management should be used in order for users to only have access to the data they must access.

5.0 Responsibility

The Accounts Support Group (ASG) is the point of contact for users requiring new accounts, password changes, reporting of possible compromises or any other issues involving user account currency and password issues. The ASG also acts as a liaison between the user and the System Administration Group(SAG). The ASG works with the Personnel staff to ensure that accounts are closed on all relevant servers and applications where a user account is no longer needed.

The System Administration Group (SAG) sets up user accounts according to this policy when contacted by ASG. No new account is established until the user has signed a user policy form that has been validated by the ASG. The SAG ensures that password-cracking checks are run at the frequency established in this policy as well as notifying the ASG of the users with weak passwords. It is their responsibility to ensure that uncorrected accounts are locked.

The Security Team (ST), chaired by GF's Security Officer, is responsible for ensuring that this policy is followed. It is also responsible for all changes to this policy. The ST is responsible for auditing the compliance with the policy. The ST makes recommendations for modifications that it deems necessary to the Foundation's CEO, CIO and IT manager.

Users are responsible for protecting their passwords and reporting any compromise promptly to the ASG. They are also responsible for selecting strong passwords.

Management is responsible for ensuring that users are aware of this policy. They also must be consistent in the enforcement of this policy.

6.0 Compliance

Compliance is monitored by regularly scheduled, but random, running of password cracking tools. All servers have the Operating System configured to enforce this policy. The ASG does periodic "social engineering" checks to ensure that users do not divulge passwords. Users who repeatedly choose weak passwords are subject to termination if they choose weak passwords for four consecutive months.

7.0 Enforcement

If password policy violations are not corrected within one business day, the account is locked. If repeated violations occur, the employee is subject to termination. Management ensures the uniform enforcement of this policy.

8.0 Revision history

This is a new policy. There is no existing policy that is made obsolete by this policy.

PASSWORD POLICY PROCEDURES

The purpose of the new account password procedures that are described below is for the establishment of user accounts and initial passwords as well as password strength checking procedures. A unique username is required for all users of GF's servers, workstations and databases. To better protect the IT resources of the Foundation, these procedures have been developed in order to adhere to the requirements of the Password Security Policy. The following procedures strive to balance the requirements of the Foundation's security policies with the convenience of its IT users.

Account Initiation.

1. A suitability determination is completed and documented for all internal and external users who require login access to any GF host. This includes any laptop and/or desktop personal computer.
2. Human Resources, if they are a Foundation employee, or an RAA, if they are an external user, certifies the user's need for access by Completing a Sponsor Authorization Form.
3. After receiving the completed suitability determination form and the completed Sponsor Authorization Form, the new user completes and signs a use policy form. No password is assigned without completing this. The Computer Use Policy Form is a summary of appropriate use and responsibilities for users of the IT resources, including desktops. The form is available online, but it must be printed out and signed.
4. The above verifications that an account is needed are presented to the ASG, either in person or via FAX. The ASG verifies that the user who signed the Computer Use Policy Form is the same person that was authorized for use. This can be done by verifying user information on the phone directly or in person. These procedures ensure that only persons whose need to access GF's IT has been verified will be granted access.
5. The ASG communicates with the SAG to set up the account and password. The appropriate password lifetime is also communicated at that time.
6. ASG securely obtains the initial password for the user from the System Administrator(s) of the requested hosts. Secure transmission of passwords means encrypted, digitally signed email or in person, or via phone after the identities of both parties have been adequately confirmed. Certified USPS mail is also acceptable.
7. System administrators ensure that passwords will be pre-expired and, therefore, must be changed at the first login. They also ensure that passwords are given to the ASG in a secure manner.
8. It is the ASG's responsibility to communicate the password to the user in one of the acceptable secure methods at the discretion of the Account Support Group in collaboration with the user. Digitally signed and

encrypted email may be used to communicate the initial password to the user.

User Login

9. The user is instructed to login to the system within 5 business days.
10. The account is removed from the system automatically if there is no initial login within this time period.
11. Audit reports citing new accounts and their status – activated, non-yet activated, and locked are reviewed by the ASG and Security Officer daily.
12. All GF systems limit users to 3 consecutive unsuccessful login attempts. All systems are configured so that the fourth unsuccessful attempt will disable the account. The ASG must be contacted to unlock an account.

Password Auditing

13. The appropriate System Administrator runs weak password detection software at no more than 30-day intervals. The interval between runs must vary. Too predictable an interval should not be chosen.
14. Each GF IT system connects to the same reporting system for weak passwords.
15. The weak password checking programs are run on the same day to simply enforcement of the policy. User workstations are checked outside of normal business hours.
16. This procedure automatically sends email to any user found to have a weak password notifying him/her of the weakness and the procedure to correct that weakness. Copies of this email are also sent to the ASG and Security Officer.
17. All users found to have weak passwords will have their passwords checked by the weak password detection software within 5 days of the password policy violation. If a violation still exists, the account will be locked and email sent. A report will be sent to ASG noting the violations corrected and those that exist and have had their account locked.

Responsibilities

Users

- Each user must change his/her initial password within 5 days.
- Each general user must change his/her password at least every 6 months.
- Each system or administrative user must change his/her password at least every 3 months.
- Password selection must be done in accordance with the Foundation's current password policy. Guidelines for strong password selection appear on the Computer User Policy Form. (Please see Appendix C for this form.) It is the users' responsibility to be aware that accounts with expired passwords that have not been changed within 45 days of their expiration will automatically be deleted by the System Administrator or the Operating System, whichever is the most feasible.

- Each user must protect his/her password.
- Each user must report any suspected compromise of the account to the ASG within one business day of the suspected compromise.
- Each user is responsible for all actions taken by this account.

ASG

- The ASG verifies that the user who has signed the Computer Use Policy Form is the same person that has authorized for use.
- The ASG obtains the initial password for the user from the System Administrator(s) of the requested hosts by direct communication with SAG staff (no email or voice-mail contact).
- The ASG is responsible for communicating the password to the user, after verification of the user's identity in person or via postal mail at the discretion of the Account Support Group in collaboration with the user.
- The ASG checks audit output from the password compliance checking software for each monthly run of the report.
- The ASG communicates to users the need to change any compromised password. The ASG works with the SAG to ensure that the password for such compromised accounts are locked if they have not been changed in the required time frame.

Systems Administration Group (SAG)

- The SAG runs password-checking programs on a regular, random basis.
- This group ensures that the infrastructure – operating system and database software – is configured in a manner that enforces GF's password policy.

The Security Officer

- The Security Officer reviews all audit logs associated with account initiation and password strength weekly. This analysis is reported the Security Team monthly.

The Security Team

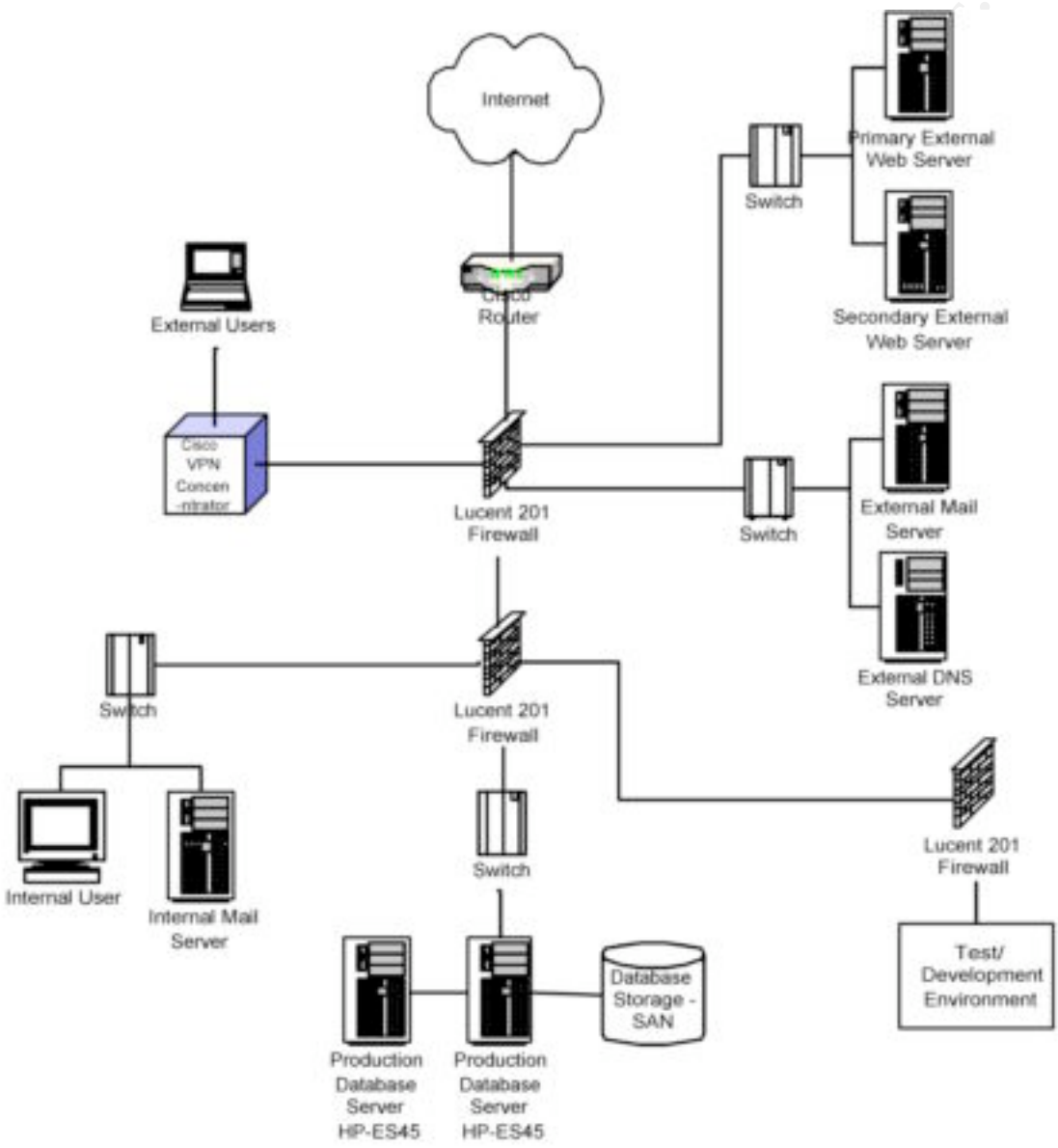
- The Security Team determines if the password policy and procedures require modifications.
- Compliance is also checked. A list of users who require actions from their supervisor or RAA is compiled.

Auditing of the password policy

The Security Team will review the password policy quarterly for effectiveness as well as staff compliance. It will recommend any modifications that it feels are necessary to the Security Officer, CIO and IT managers.

The Security Officer reviews the monthly weak password report. This review includes looking for staff who appear periodically on the report. The Security Officer will meet with such staff and their supervisor or RAA.

APPENDIX A – GIAC INFRASTRUCTURE NETWORK DIAGRAM



APPENDIX B – NERSC PASSWORD POLICY

You are here: hpcf / policy / password **You came from:**

Password Policy and Procedures

- New Users
- Login Failures
- Obtaining a New Password
- Changing Your Password
- AFS Passwords
- HPSS/DCE Passwords

Summary
A user identifier known as a username and password are required of all users. Passwords are managed separately on each NERSC system. Passwords must not be shared with any other person. The password must be changed as soon as possible after an unacceptable exposure or suspected compromise.

Passwords and accounts may not be shared. NERSC will disable a user who shares any one of her/his usernames with another person.

See Account Ownership Policy.

New Users
NERSC must have a signed user policy form on file before assigning you a password on a NERSC system. Once this form has been signed, the Account Support group will contact you by phone to assign you a temporary password and then activate your username(s) on the appropriate systems. You will have to change this password the first time you login.

Note that if you don't login and change your original password within 5 working days of its being assigned on one of the Crays or servers, your username will be removed from that system. Contact Support to have a new password assigned.

Login Failures

If you have three login failures while entering your password on a NERSC machine, your password will be disabled; contact the Account Support group to obtain a new one.

Obtaining a New Password from NERSC Support

If you have forgotten your password, contact the Account Support group to get your password reset. You will have to change this password the next time you login.


Back to top of page.

Changing Your Password

Passwords must be changed under any one of the following circumstances:

- At least every six months.
- Immediately after giving your password to someone else.
- As soon as possible, but at least within one business day after a password has been compromised or after you suspect that a password has been compromised.
- On direction from NERSC staff.

To change your password, use the passwd command. When your password expires you will be automatically prompted to change it when you next login. First you will be prompted to enter your current password, then to enter your new password twice in a row. Your password must contain at least 8 characters, of which at least two must be letters and at least one non-letter character. Your new password must differ from the old one by at least 3 characters.

Note that passwords are not shared across any NERSC systems or resources. Changing your password on one NERSC system does not change it on other NERSC system.

General Password Requirements

The following requirements conform to the Dept of Energy Guidelines regarding passwords, namely DOE Order 205.3.

http://www.directives.doe.gov/pdfs/doe/doetext/neword/205/g2053-1.html

Different NERSC systems have different software environments, and therefore minor variations in software constraints on passwords.

When users are selecting their own passwords for use at NERSC, the following guidelines should be used. It is the responsibility of the user to select passwords that follow these guidelines, even if the system software on a particular system does not force the user to follow them.

- Passwords must contain at least eight nonblank characters;
- Passwords must contain a combination of letters (preferably a mixture of upper and lowercase letters), numbers, and at least one special character within the first seven positions;
- Passwords must contain a nonnumeric letter or symbol in the first and last positions;
- Passwords must not contain the user login name;
- Passwords must not include the user's own or (to the best of his or her knowledge) a close friend's or relative's name, employee number, Social Security number, birthrate, telephone number, or any information about him or her that the user believes could be readily learned or guessed;
- Passwords must not (to the best of the user's knowledge) include common words from an English dictionary or a dictionary of another language with which the user has familiarity;
- Passwords must not (to the best of the user's knowledge) contain commonly used proper names, including the name of any fictional character or place;
- Passwords must not contain any simple pattern of letters or numbers such as "qwertyxx".


Back to top of page.

AFS Passwords

The Andrew File System (AFS) is accessible on the PVP cluster and the T3E through an NFS/AFS gateway.

To change your password, you must connect to the machine dano.nersc.gov and follow the menu instructions.


Back to top of page.

HPSS/DCE Passwords

HPSS uses DCE (Distributed Computing Environment) for user authentication. You can change your password by using **ssh** to connect to **auth.nersc.gov**, and following the detailed instructions shown on the HPSS page.

Page last modified: Monday, 20-May-2002 16:35:13 PDT
Page URL: http://hpcf.nersc.gov/policy/password.html
Contact: Webmaster <webmaster@nersc.gov>
Privacy and Security Notice

APPENDIX C – MODIFIED USER POLICY FORM

Computer Use Policies Form

This is a list of general computer use policies and security rules that apply to all users of GIAC Foundation (GF) computers or networks. **GF must have a signed copy of this form on file for every user.** If you are reading this form online, please print out a copy; sign and return to GF (see fax and U.S. address below).

Computer Use	Computers, software, and communications systems provided by GF are to be used only for GF-sponsored work. The use of GF resources for personal or non-work-related activity is prohibited. GF systems are provided to our users without any warranty. GF will not be held liable in the event of any system failure or loss of data.
Data Retention	When a user account is deleted, all permanent files (in home directories and GF storage systems) are assigned to the sponsoring RAA, if appropriate or supervisor if that is appropriate, who is responsible for deleting unneeded files.
User Accountability	Users are accountable for their actions and may be held accountable to applicable administrative or legal sanctions.
Passwords and Usernames	A user identifier known as a username and password are required of all users. Passwords must be changed at least semi-annually for general users and quarterly for system and administrative users. Passwords must be between six (6) and ten (10) non-blank characters, not found in a dictionary, must contain a mixture of alpha and numeric characters, as well as special characters. At least one special character must appear in the first 5 characters. The first and last characters must not contain numbers. Passwords must not be shared with any other person. The password must be changed as soon as possible after an unacceptable exposure or suspected compromise.
Unauthorized Access	Users are not to attempt to receive unintended messages or access information by some unauthorized means, such as imitating another system, impersonating another user or other person, misuse of legal user credentials (usernames, passwords, etc.), or by causing some system component to function incorrectly.

Software Use	All software used on GF computers must be appropriately acquired and used according to the appropriate licensing. Possession or use of illegally copied software is prohibited. Likewise, users shall not copy, store or transfer copyrighted software or data, except as permitted by the owner of the copyright.
Altering Authorized Access	Users are prohibited from changing or circumventing access controls to allow themselves or others to perform actions outside their authorized privileges.
Reconstruction of Information or Software	Users are not allowed to reconstruct or recreate information or software for which they are not authorized.
Data Modification or Destruction	Users are prohibited from taking unauthorized actions to intentionally modify or delete information or programs.
Malicious Software	Users must not intentionally introduce or use malicious software such as computer viruses, Trojan horses, or worms.
Denial of Service Actions	Users may not deliberately interfere with other users accessing system resources.
Notification	Users must notify GF immediately when they become aware that any of the accounts used to access GF has been compromised.
Account Usage	Users are not allowed to share their accounts with others.

GF personnel and users are required to address, safeguard against and report misuse, abuse and criminal activities. Misuse of GF resources can lead to temporary or permanent disabling of accounts, loss of GF allocations, and administrative or legal actions.

Sign and return to GF Account Support Group.

I have read the GF Policies and Procedures and understand my responsibilities in the use of GF resources.

Signature:

Print Name:

Organization:

Email Address:

Work Phone Number:

Registered Authorizing Authority (or Supervisor):

Date:

REFERENCES

"NIH/OER Implementation Issues for Human Embryonic Stem Cell Research Frequently Asked Questions", http://grants1.nih.gov/grants/stem_cell_faqs_topic.htm#funding

Dillard, Clayton T, "eCommerce and Defense in Depth", http://rr.sans.org/ecommerce/defense_indepth.php.

"Securing Microsoft's IIS Web Server", http://www.sans.org/IIS/sec_IIS.htm.

Tracy, Miles, Wayne Jensen, and Mark Lamon, Guidelines on Securing Public Web Servers, Recommendations of the National Institute of Standards and Technology, Special Publication 800-44, http://csrc.nist.gov/publications/nistpubs/800-44/sp800-44.pdf

Mortensen, Jason, "Password Protection: Is This the Best We Can Do?", August 20, 2001, http://rr.sans.org/authentic/pass_protect.php

Sherrod, David H, "Securing Access: Making Passwords a Legitimate Corporate Defense", January 15, 2002, http://rr.sans.org/authentic/sec_access.php.

State of Michigan Security Policy http://www.michigan.gov/hal/1,1607,7-129-2783-2301--,00.html

Krychiw, Steven, "SecurID: A Secure Two-Factor Authentication", February 28, 2001, http://rr.sans.org/authentic/securid.php.

Berlind, David, "Now is the time for two-factor security", October 25, 2001, http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2819968,00.html

National Science Foundation FastLane, https://www.fastlane.nsf.gov/guides/EB_Proposal_Submission.pdf

SANS password policy, http://www.sans.org/newlook/resources/policies/Password_Policy.pdf

SANS database password policy, http://www.sans.org/newlook/resources/policies/DB_Credentials_Policy.pdf

PSC password policy, http://www.psc.edu/general/policies/passwords/password.html

NERSC password policy,
http://hpcf.nersc.gov/policy/password.html

Hurley, Edward, “Proper password policy is imperative”, 08 Jul 2002, SearchSecurity,
http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci837272,00.html

Introduction to SSL,
http://developer.netscape.com/docs/manuals/security/sslin/contents.htm

Tan, Bang Shuh, “Securing The Network With Cisco Router”, May 18, 2002
http://rr.sans.org/netdevices/sec_cisco.php

Cisco VPN Series 3000 Concentrators product information,
http://www.cisco.com/warp/public/cc/pd/hb/vp3000/

Lucent Technologies,
http://www.lucent.com/products/solution/0,,CTID+2017-STID+10080-SOID+1224-LOCL+1,00.html

HP AlphaServer ES45 system information,
http://www.compaq.com/alphaserver/es45/

Compaq Proliant servers,
http://www.compaq.com/products/servers/proliantdl760/index.html

Sun info
http://www.sun.com/servers/entry/v480/index.html

Fratto, Mike, “Enterprise Firewalls”, December 10, 2001,
http://www.networkcomputing.com/1225/1225buyers3.html

SANS top 20, http://www.sans.org/top20.htm

StorageWorks enterprise backup solution, For High Performance SANs in Heterogeneous Environments,
http://www.compaq.com/products/storageworks/ebs/ebsdatacenters.html,

“Snort, The Open Source Intrusion Detection System”, http://www.snort.org/

Pisetsky, Ariel, Securing e-Commerce Web Sites,
http://rr.sans.org/web/sec_ecom.ph.

McGinn-Combs, Dan, “Defining Policies Using Meta Rules”, http://rr.sans.org/policy/meta_rules.php

Farrow, Rik, “How to secure your web server”, http://www.gocsi.com/pdfs/alert1201b.pdf.

Northcutt, Stephen, Basic Security Policy, v 1.7, SANS Institute, Information Security Officer training materials.

Generally Accepted Principles and Practices for Securing Information Technology Systems, URL; http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf.

The John D. and Catherine MacArthur Foundation, http://www.macfound.org/

Last Updated: May 30th, 2017

Upcoming Training

SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
Community SANS Seattle MGT512	Seattle, WA	Aug 14, 2017 - Aug 18, 2017	Community SANS
Community SANS New Orleans MGT512	New Orleans, LA	Aug 21, 2017 - Aug 25, 2017	Community SANS
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS New York MGT512	New York, NY	Aug 28, 2017 - Sep 01, 2017	Community SANS
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Toronto MGT512	Toronto, ON	Sep 18, 2017 - Sep 22, 2017	Community SANS
Community SANS Columbus MGT512	Columbus, OH	Sep 25, 2017 - Sep 29, 2017	Community SANS
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced