Global Information Assurance Certification Paper

A Content Delivery Case Study

Name: James Robinson
Certification: GSEC
GIAC Assignment Version: 1.4b Option 2
Timeframe: original
Submission: original

Class Information:
Start Date: 6/23/2003
City: Bloomington
State: IL
Mentor/Instructor: Bob Hillary
Company: State Farm Insurance Company

Abstract
This paper is a case study outlining the second option for the GSEC practical guidelines. Within this paper I will take you thought the process of deploying a content delivery network intended for the use of Media Streaming. Some of the high level parts of this paper include project kick off/security requirements, testing, vulnerability research, pilot, deployment and transition. The project was tasked with deploying a solution that would allow international communications of media streaming. Evaluation and selection of vendors for both testing and implementation, and risks associated with each product. Finally, I will work you thought the deployment of the solution within an enterprise network.

Before
During the Internet boom everything in the IT industry grew. Technology pushed the processing power of the super computer, mainframe, network and desktop computer farther then anyone had expected. With thousands of clients connecting to public and private infrastructures data could be sent from Beijing, to Palo Alto, to Boston, across the Atlantic to London, and back to Beijing in milliseconds. With these speeds I could send a few DVD movies across the world in minutes. Osborne (1). A one time transfer speed close to 1 GB/sec is more than we could have envisioned just a few years ago. However, when a transfer contains this much data and the transfer is multiplied by users it becomes infrastructure crushing at exponential rates.

With large data transfers in mind the company I work for, General Mutual Sales, GMS here after, saw a need to find a solution or an appliance that could off load its data to specific locations closer to our business partner's end user. A solution like this is called a content delivery network. Basic content delivery networks are an up and rising technology used to store static content in a specific location for end user request. A content delivery network will consist of caching engines or CEs. By placing these devices in key locations a large file transfer like a streaming video could be pulled multiple times without performance hits on the origin server or key infrastructure links. GMS began by compiling a team of analysts to look at the risks involved with a solution like a content delivery network.

GMS is a very large organization, before a project is funded it is proposed at an executive level. During the beginning of the project, risk was looked at from an enterprise business perspective. The risks associated at this level are not technical, but deal with the bottom line cost to the enterprise.

Project Kick Off/Security Requirements- Security 0% complete

If the project is approved it is given to a group. This group consists of one or more business partners and a combination of both business and technical system analysts. As the members of this group we were brought together and formed a project called "Media Streaming 2003". Each analyst was responsible

for writing or providing information for initial requirements. The requirements are a composite of documents that are used to create a solution. To build these requirements each analyst was able to use their own tools for risk assessment. A risk assessment is defined by Symantec's glossary to be

"The computation of risk. Risk is a threat that exploits some vulnerability that could cause harm to an asset. The risk algorithm computes the risk as a function of the assets, threats, and vulnerabilities. One instance of a risk within a system is represented by the formula (Asset * Threat * Vulnerability). Total risk for a network equates to the sum of all the risk instances."

Any issues or risks were documented in a central project collaboration system and a copy was sent to the Project Manager for further categorization. As a new security analyst this was going to my first experience with a tool called SPRINT. SPRINT is "Simplified Process for Risk Identification" and was created by the Information Security Forum. In my organization SPRINT has been tailored to include a Business Impact Assessment and Technical Impact Assessment. The BIA portion of the SPRINT assessment is to be done with the business partner. In this portion of the SPRINT assessment questions and answer are to be presented from a worst case scenario. The majority of these questions is categorized and included the three bedrock principles outlined in SANS "SANS Security Essential with CISSP CBK. As you will see below there are also two other categorizes involved in our assessment.

- Confidentiality focused on both the data the content delivery system would deliver as well as the configuration data
- Integrity was focused on the loosing the integrity of the data accidentally or maliciously
- Availability dialed in on the individual components of the solution and the complete uptime associated with the solution.
- Financial/operational risk is assessed by looking at failure to protect assets.
- Compliance by asking questions about failure to comply with policy and regulations.

To perform the business assessment I setup a meeting and allocated 1 ½ hours. In this meeting invite I included not only a time, place and date but also a primer and some general questions to prep the business partner. A few weeks later I had concluded my assessment. With this information I compiled the information in a table format for easy circulation. This information is scored on a 1 to 5 range with 1 being low risk and 5 being very high risk.

Confidentiality	3	secure configuration data
Integrity	3	secure configuration data
Availability	4	Major purpose for solution
Financial/Operational	1	Cost of network
Compliance	2	records management and retention

Once the BIA assessment was completed I could look at the Technical Impact Assessment portion of the complete risk assessment. The TIA is used to assess key threats and vulnerabilities to the solution from a technical stand point. This can be done in a number of ways. Because of a lack of technical solutions peers from different technical aspects should participate. The first way to get participation is by setting up a meeting with peers. By setting up a meeting with peers I was able to speak openly with everyone in a formal or informal manor. The second way to asses the technical vulnerabilities is to communicate your findings via white paper or e-mail. The benefit to this method is your peers are able to respond at their leisure which may encourage more thought and participation. The solution's threats and vulnerabilities follow the same categories as mentioned in the business impact portion of the assessment. Each category is looked at from every option that the solution could use. Below is the outcome of the technical assessment.

Confidentiality	3	
Integrity	3	
Availability	4	
Financial/Operational	1	
Compliance	2	

During the TIA a security analyst is expected to look at any and every direction the project could take. I needed to look at each of these paths because the project was not at a point where any one solution had been created. I then took these paths or possible solutions and looked at the associated risks directly involved with them. With the TIA risk information I used a formula similar to the one included in the risk assessment definition above to copulate overall risk. The outcome of the technical assessment with my peers determined that only public available information should transverse this network. This decision was made due to the lack of industry knowledge and maturity of the technology. Other recommendations were made including, the solution comply with our infrastructure management process and data management and retention processes.

Once the technical assessment is complete my peers and I worked to find controls that help keep the business risks within acceptable levels. The information gathered was pulled together and written as an overall overview. In

the overview I discussed technical recommendations and any risks that pertain to the project and foreseen solutions. Identifying risks are an ongoing process within GMS's project management system and any risks identified are compiled with other project risks and reviewed on a scheduled basis. With the overview and technical controls and early risks gathered I worked with the business partner to find an agreed action plan to mitigate security threats identified during the technical assessment. Since there were a number of solutions that could be implemented and each of the solutions proposed different security risks the project team decided that any security that would be implemented should be decided during the technical assessment of the products. This decision was acceptable but the project still needed security requirements to give to vendors for a Request for Proposal (RFP). After consolidation and more research the following are the security requirements that were given.

A. Which security/directory models is your application compatible with? (e.g. Active Directory, LDAP, ACF2 etc.)
    a. This question was used to drive out integration in to our network. The answer was supposed to drive out the management of data and users.

B. Are all passwords used in your application encrypted?
    a. Passwords are overlooked during many product evaluations. This question would table any password issues early in product evaluations.

C. If dial-in support for your product is necessary, is it possible for you to use GMS's centralized solution for dial access? If no, explain:
    a. This is a direct question that would allow the product to align to GMS's central management system

D. Will the application perform if secured using NT Challenge-and-Response techniques?
    a. Our solution would use windows media streaming servers so windows native authentication was a must.

E. Is the hosting server behind a firewall?
    a. Some solution foreseen could have need internet access or have unnecessary protocols and services that may have need to be closed or secured by a firewall. By verifying that the vendor's product could sit safely behind a firewall GMS could control access to the devices.

F. Are the hosting servers contained in a secured (locked) room, away from unauthorized access?

a. This was to drive out physical security and remote configuration of the devices.

G. Will GMS Streaming media information be logically and physically separate from departments companies' information?
   a. This was to verify that data could be stored and transferred to the solution on a needed basis.

H. Will any third party have access to GMS information (other than GMs or your company)?
   a. Questions like this help to determine if the company is a new acquire, or house information with any other companies.

I. Will GMS information be stored on a server in an encrypted format? If yes, what cryptographic method and key length is used to encrypt the data?
   a. Many applications can not actively use encryption. Since confidential data should be secure both in transit and storage this question helped to drive out the file structure of the solution and necessary ways to ACL the data if necessary.

J. Does your application encrypt all transmissions between your company and any outside companies (including GMs)? If yes, what cryptographic method and key length is used to encrypt the transmission?
   a. Question J drove out communications from us to the vendor.

K. What type of authentication is your application compatible with (PKI, NTLM, etc.)?
   a. K was very beneficial to model how the authentication model would be used. If the question was answered saying PKI, GMS may need to order keys or even deploy a PKI system if the solution was chosen.

L. Can application logon id and passwords be synchronized with GMS logon id and passwords? If yes, is password synchronization bi-directional (updates from product synchronized in GMS and vice versa)?
   a. Synchronization of passwords help to maintain password policies.

M. Are all security administration tasks logged to a location that can be modified?
   a. Logging or Accounting is very important to enterprise security. Proper logs can point out security risks and penetration.

N. What flexibility is provided in password administration relating to length, makeup (use of numbers, letters, upper/lower case), time to expire and invalid attempt retries/lockout?
    a. Like L, N helped to verify if the solution could use the same password rotation techniques GMs used.

O. Are all ids and passwords stored in a directory encrypted? If yes, what cryptographic method and key length is used to encrypt the password?
    a. Another question about storage of confidential data. This question again pertains to 1, use of directory and 2, use of a crypto system.

P. Can detailed audit and logging capabilities for users and user groups be provided?
    a. Auditing being an intricate part to enterprise security can help to ensure user accountability.

While the RFPs were send out to multiple vendors there were other tasks I had to complete, one of which was a test strategy. In my organization a test strategy would be used to score each product brought in for evaluation. The test strategy was compiled of many test cases. With each test case there was a field explaining how to test and a field where a Pass/Fail could be marked. After scratching down some ideas my security counterpart to the project and I thought it would be beneficial to white board and categorizing our ideas. From our ideas the following chart was created.

Testing-Security 25% complete

What is tested	**Why it was important to test**
Installation	
1. What Id's/accounts are created default?	Identify any accounts that could be used for a back door or attack
a. local?	
b. remote?	
c. service accounts?	
2. views on configs	Identifies what information will be seen by users
3. os finger print	Allows the security analyst to identify vulnerabilities
4. open ports	Allows the security analyst to identify vulnerabilities
Administration	
1. OS Type	Determines what type of skills will be needed to administrate
2. SNMP information	SNMP can be a very useful protocol/service if exploited
a. Is it needed?	
3. Administration tools	Administrative tools are dangerous cause they can lead to back doors
a. Fat client?	Fat Clients require installation on dedicated workstations
i. Encryption available?	
b. Thin client?	Thin clients applications are preferred over Fat
i. Web-based?	Web services have a tendency to be exploited
ii. Encryption available?	
4. Access controls	Allows customizable controls to be placed on resources to limit exposure
5. Able to configure users and services	Allows for authorization and accounting

6. Able to communicate via ext. authorities? a. Active Directory b. LDAP c. Kerberos	Allows use of existing groups for use and administrations authentication and authorization
7. Process for patches a. Local auth. Required? b. Remote auth required?	So devices require remote or local access to apply patches and must be done out of band

Content Delivery Operations

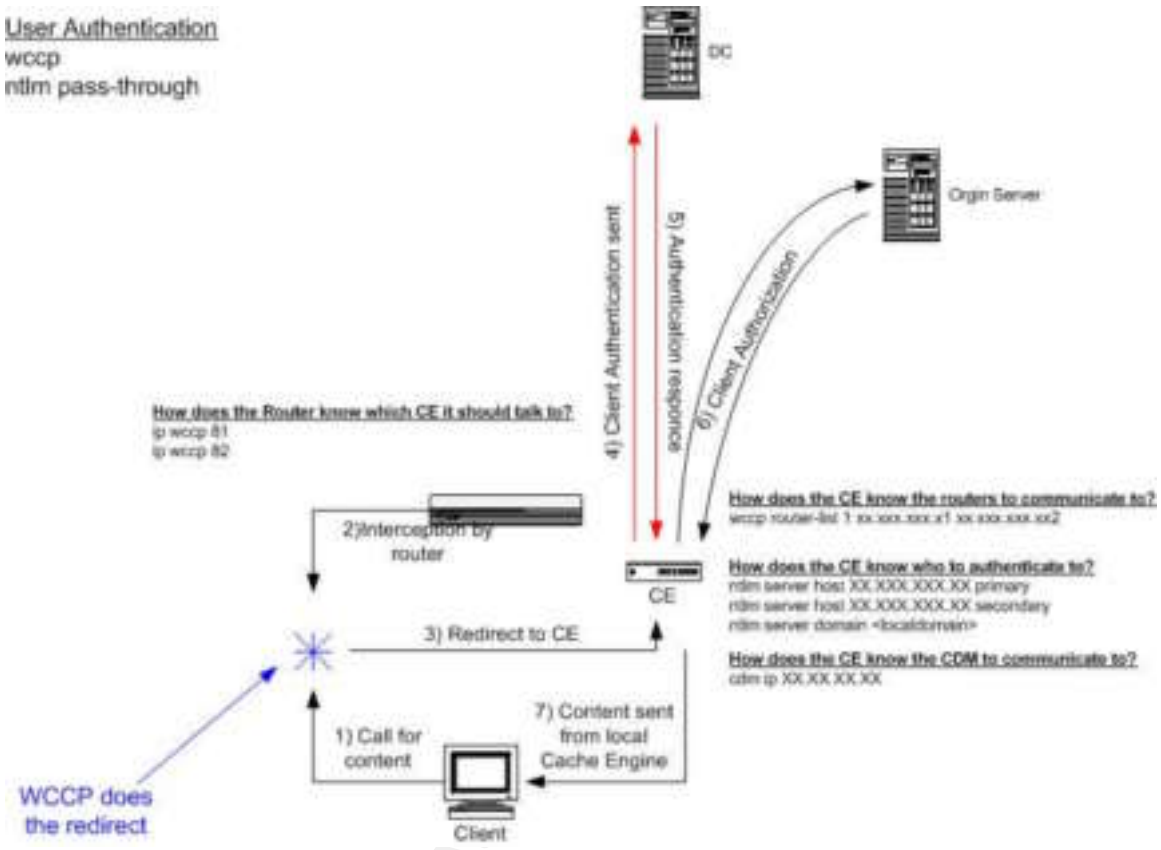
1. Service accounts to push content	This allows process to run out of context to comply with our least privileged application model and limits full exploit of device.
2. Data push to proper locations	Important if sensitive data is being streamed
3. data push inherits ACLs	Important if sensitive data is being streamed
4. Test replay of information a. Encrypt sensitive streams	If important information is streamed can it be captured and replayed or will it reveal sensitive information like passwords?
5. Windows media 9 a. Digital rights management	This was a business requirement that falls in line with the compliance portion of the SPRINT assessment.

Auditing

1. view logs	Logs are very important to maintain a secure enterprise.
2. reverse engineer transactions a. user\ip b. time\date c. resource name d. function e. result code	Reverse engineering allows replay attacks and disclosure of sensitive information

Once the RFPs were returned the project team began nailing down what vendors would be asked to come in for a proof of concept and functionality testing. This decision was done between a few project team meetings. Some of the RFPs included Microsoft solutions, Linux based solutions, and hardware appliances. Due to the projects timeline, support, infrastructure integration and the business partner's requirements two products were brought in for testing.

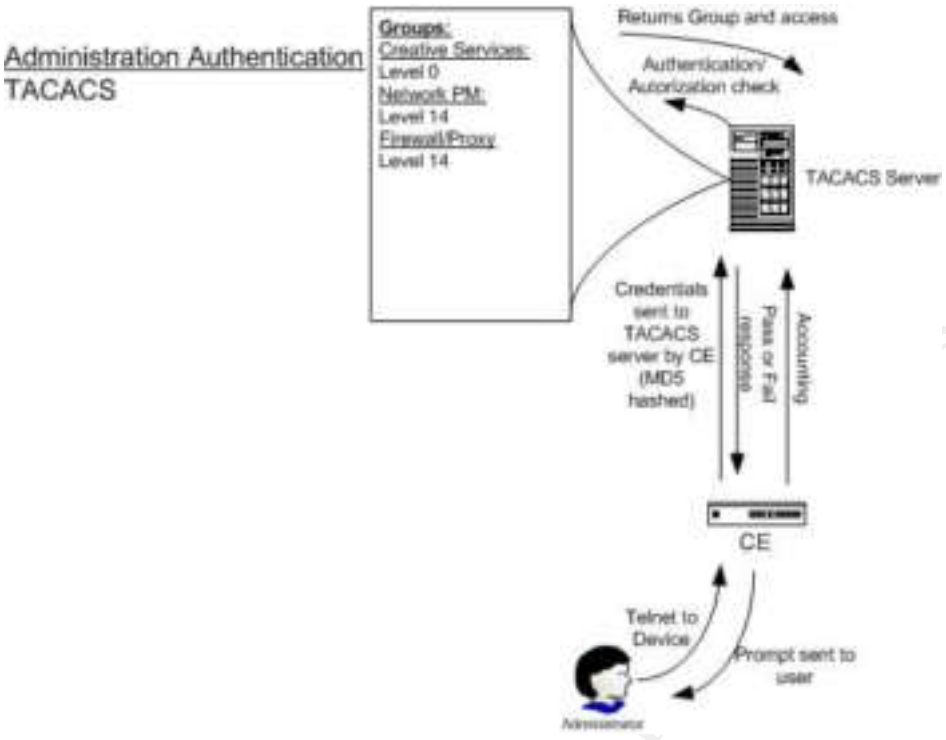
Due to legal and business concerns I can not go into depth why one vendor was choose over another. I can say that our test results for each vendor were very close and the project team's decision came down to a security concern with NTLM pass-through and business partner functionality testing. Since NTLM pass-through authentication was a security issue with one of the evaluated vendors I had to give a presentation to my team members on what the technology was and why it was essential for our network. Since the team had seen it work for one of the vendors it was easiest to model from it. For this presentation I came up with a drawing that I would use for project documentation. I have included this drawing below.



The authentication model I drew above brought a lot of concerns and questions so I have included the notes I had for each drawing.

Drawing Notes:
• WCCP-Web Cache Communication Protocol- in lemans terms listens for requests on certain tcp/udp ports and redirects traffic to devices for retrieval. • Origin Server is the server that will house the originating media streams • Authentication methods used in GMS's Content Delivery Network will work with pass-trough authentication. Pass-through authentication can be used with LDAP, AD (Basic, ntlm, ntml^{V2} and Kerberos)

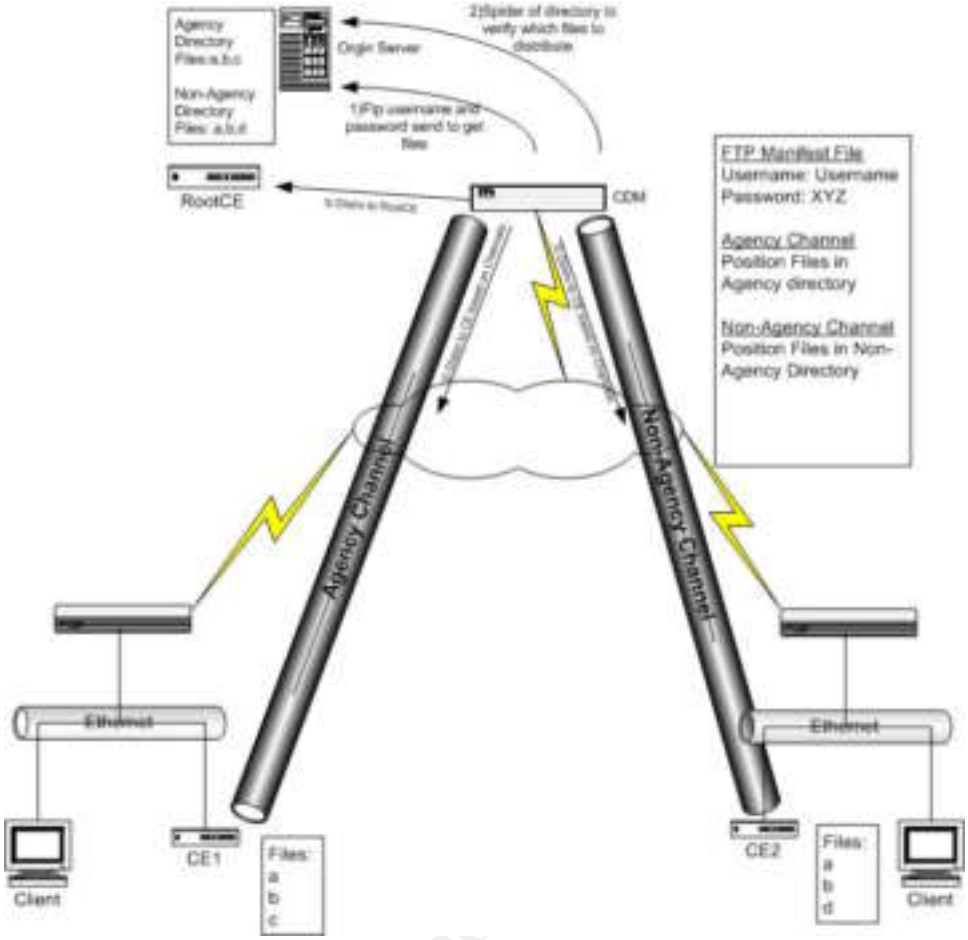
During the same week I had a security team meeting in which I was to present data on this project for a peer review. I included the following drawings explaining administration authentication and logical data management and preposition. The first drawing is administration authentication. Since the product chosen for our network was able to integrate nicely within our existing TACACS system I decided I would inform my team members about how TACACS works.



Drawing Notes:
• Individual users are members of groups • Groups are used to maintain GMS's least privileged model • The credentials and communications are sent to the TACACS server via MD5 hashes. Though this is not a super secure communication method is better then clear text.

The next drawing I presented to my security peers was a diagram explaining the data and hardware management. This was not a very hard process for my project team to work though since data (streaming media) confidentiality would

not play a very big role within our network.



Drawing notes:
• The file directories on the origin servers are locked down using least privilege ACLs • FTP process is used to spider the directory for content to position • FTP process is used to transfer files to the CE • Each FTP process uses separate passwords.

Vulnerability Research- Security 55% complete

The project had decided on a vendor, it was time for me to do some vulnerability research. I would use my research to create documentation on the security vulnerabilities associated with the solution. I began by looking at security advisories on Cisco's website for any vulnerabilities that were repeating and/or currently open to the Cisco platforms and protocol implementations we were using. Using ISS I ran a port and vulnerabilities scan but comeback with many false positives. Because of the false positives I also did further research within Secunia's security vulnerability DB. A search of the DB revealed the same OpenSSL vulnerability listed on Cisco's website but since our Applications and Content Networking System (ACNS) software version was the latest and greatest the issue had to been patched. I also looked at the authentication methods and

decided it would be beneficial to document the vulnerabilities with TACACS and MD5 stream-cipher encrypted communications. Since MD5 is considered a secure hashing technique the weakness was in maintaining the shared key. I decided the risk was not sufficient enough to document and dismissed it.

I then began looking at the vulnerabilities that we associated with the Windows Media Service. The main purpose for this was because the current servers that were not in our enterprise had never had a vulnerability scan or documented security issues. I was not worried about Windows OS exploits since the associated exploits for our base load and service pack levels was already well documented. I was not able to find anything associated with Windows Media Server when I did a scan with internet Security System (ISS) and this alarmed me. Because of the poor results with the scan I did a search on the ISS website and came back with 157 documented vulnerabilities that I had to pick through to verify their validity within our network. The link provided above will show my search results.

PILOT- Security tasks 75% complete

The day was approaching were the project was going to do a controlled pilot. GMS has a network that spans international lines so the project decided to use sites located a great distance from our corporate headquarters. By doing so the pilot could mimic true network traffic since the pilot was going to be integrated into the enterprise solution. The devices were installed with generic configurations configured at the home office. The reason for this was to provide known information like Admin password, Interface IP addresses, Origin Server IP information, NTLM Authentication information and WCCP information. By configuring the appliance before shipping the project was able to limit the need for onsite configuration and made the standup process very simple. The devices were sent in almost working order. The only thing that was not turned on was WCCP at the router.

Before security would allow the devices to cache our company's data we had to configure a management system so administrative accountability could be maintained. The system chosen was TACACS and a few things had to be hashed out between the Network Automation Analyst and me before we could configure TACACS. The first was users and the level of access to the devices. Since the data that would be used in the pilot was owned, maintained and updated by the business partner it was decided that they needed access to the web interface. I was not willing to give the business partner full access to the web interface so it was decided that we would also have groups within the web interface. The table below will outline the different access rights to the devices.

TACACS	Team/Group names	Level of access
	Media Services	0
	Network Problem Management	14

	Content Caching and Access	14
WEB INTERFACE	TEAM/GROUP NAMES	LEVEL OF ACCESS
	Media Services	Limited
	Network Problem Management	Full control
	Content Caching and Access	Full control

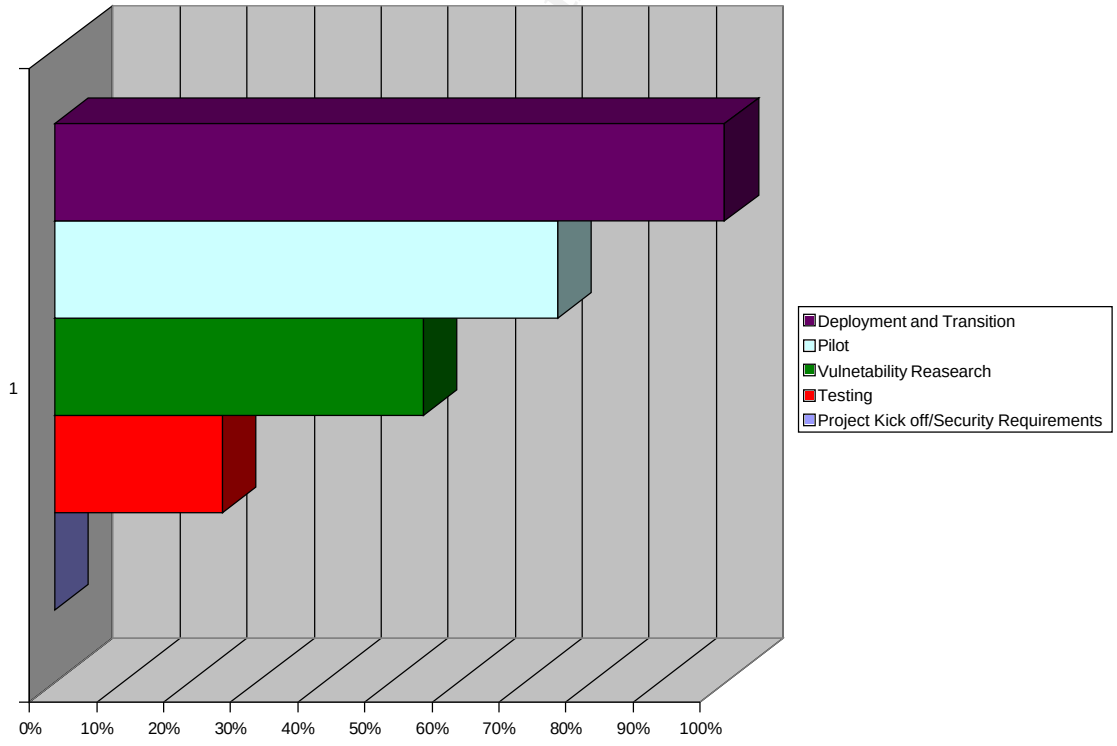
My first instinct was to limit all control to the command line interface for the creative services group. This was not possible because the web interface uses TACACS users for access and our TACACS implementation can not limit command line access, to integrate we had to give them user rights which would not allow them to see any sensitive information or change any of the device configurations. I would also like to add that the TACACS users that were given level 14 accesses are allowed to change any piece of the device configuration except disable or changing the TACACS configuration. I also for sake of documentation, because this use for TACACS and networking devices was new to GMS, created a flow chart to explain the process to create a new user for the system, this is below.

Deployment and Transition- Security 95% to 100% complete

For the Media Streaming Project to be able to deploy it had to first show successful implementation into the pilot network. Since this was done the Network analysts worked with field employees to install devices in geographical locations. Since security was not needed for production deployment I started to write the final documentation and transition of the project to Service Team. This documentation included my requirements, drawing, and research of vulnerabilities and flowcharts of the processes defined.

Conclusion

This paper has taken you though my work on the Media Streaming 2003 project. When this project started GMS was not in a position to broadcast communications to employees located internationally by any means other then travel or electronic documents. As the project went through its cycles, charted below, a solution was created that was scalable and secure that offered availability and integrity of data presentations.



Though this project's intent was to be able to stream media the general direction for the next phases of this solution is to provide application and active web page deployment solutions.

Osborne, Brian. “New Internet speed record” 10 Mar 2003 URL:http://www.geek.com/news/geeknews/2003Mar/gee20030310019018.htm (25 Nov 2003).

Cole, Eric., Fossen, Jason,. Pomeranz, Hal,. Northcutt, Stepher. “SANS Security Essential with CISSP CBK.” The SANS Institute: 04 (10 Oct 2003).

[0]“Webopedia” (2001) URL:http://www.webopedia.com/TERM/C/CDN.html (12 Dec 2003).

“Symantec” URL:http://securityresponse.symantec.com/avcenter/refa.html#risk (12 Dec 2003).

“Information Security Forum.” URL:http://www.securityforum.org/html/current.htm#risk_tool (12 Dec 2003).

“Cisco Systems” URL:http://www.cisco.com/en/US/products/sw/conntsw/ps491/ (12 Dec 2003).

“Internet Security Systems” URL:http://www.iss.net/search.php?config=corporate&pattern=Windows+media+service (12 Dec 2003).

“Secunia” URL:http://www.secunia.com/advisories/9891/ (12 Dec 2003).