



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Managing Cybersecurity Initiatives & Effective Communication (Cybersecurity L
at <http://www.giac.org/registration/gcpm>

A Project Management Approach to Writing a GIAC Gold Paper

GIAC (GCPM) Gold Certification

Author & Project Manager: Sally Vandeven, sallyvdv@gmail.com

Advisor: Stephen Northcutt

Accepted: September 1, 2014

Abstract

Writing a GIAC Gold paper may seem like a daunting task to those who have not written a research paper since their college days. This paper guides the reader through a project management approach to writing a Gold paper by applying the concepts taught in MGT525, for example, defining a scope statement, developing a work breakdown structure, establishing a project schedule. It will also provide a document framework to help a Gold paper project progress to a quick and rewarding completion.

1. Introduction

The SANS reading room has published thousands of papers on a wide range of computer security related topics at <http://www.sans.org/reading-room>. The reading room contains Analyst papers, Vendor Whitepapers and Gold papers. The majority of the papers are Gold papers, which must pass a well-defined peer review process in order to be accepted for publication. According to the SANS website, “More than 75,000 unique visitors read papers in the Reading Room every month...” (SANS Institute, n.d.). By publishing a Gold paper, the author is able to easily share her expertise with security community peers.

Producing a research paper for publication for the SANS reading room requires an amount of effort and time that may seem intimidating. This paper will attempt to reduce that barrier to entry by considering the Gold paper a typical IT project and applying common project management techniques and tools in order to provide the author with an easier to manage and more time efficient approach.

This paper is not meant to be an exhaustive how-to on writing research papers but instead will focus on managing a Gold paper project using the tools and techniques prescribed by the Project Management Institute. The terminology and techniques used throughout this paper are taken from the Project Management Institute’s “PMBOK Guide,” (PMBOK Guide, 5th ed., 2013). A Gold paper author will be referred to as both the author and the project manager for the purposes of this paper.

A survey was conducted for this paper that polled 50 previous Gold paper authors asking questions designed to provide feedback that might benefit future authors. The results of this survey are discussed throughout this paper and the results are shown in their entirety in Appendix E.

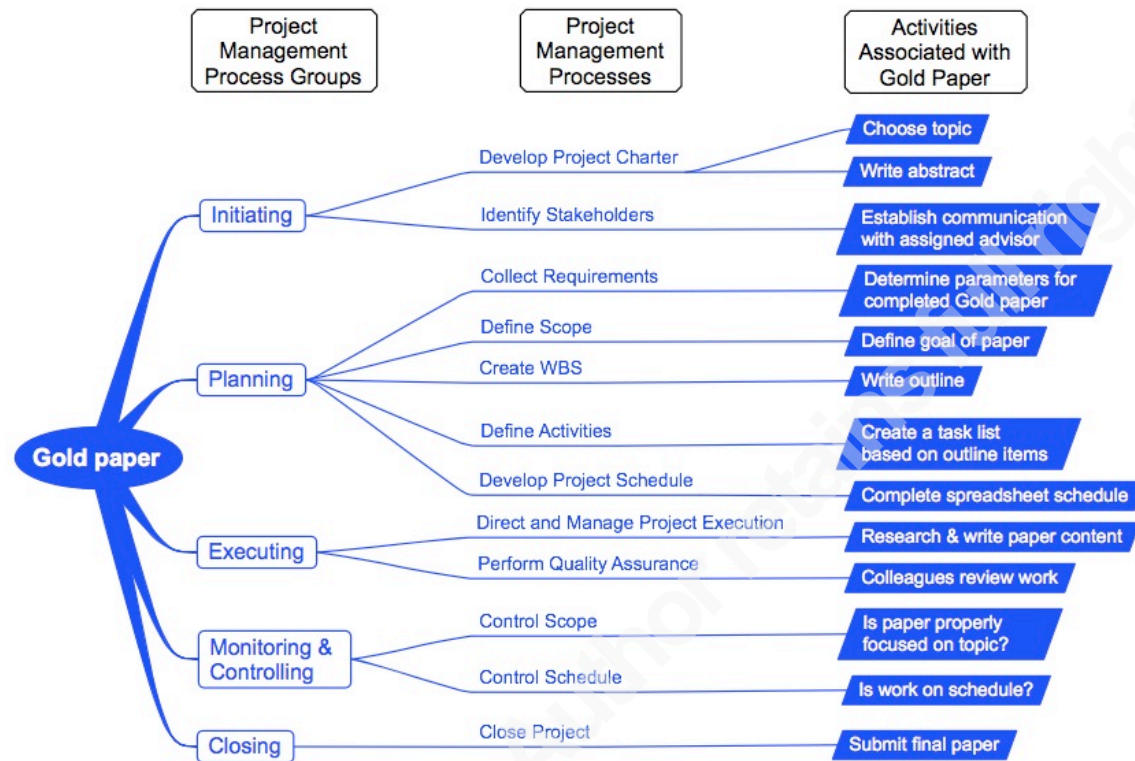
2. Project vs. Product

According to the Project Management Institute (PMI), the activities involved with any project are considered either *project management* processes or *product-oriented*

processes. *Project management* processes are those activities involved with initiating, scheduling, managing and monitoring a project. *Product-oriented* processes are the activities involved with producing the output of the project (PMBOK Guide, 5th ed., 2013, p. 47). In this paper, the project is defined as writing a GIAC Gold paper, therefore, the *project management* processes will define and measure the activities required to complete the Gold paper. In contrast, the *product-oriented* processes refer to creating the paper's intellectual content. Put another way, *project management* processes will help the author/project manager stay organized in order to write and complete the paper and the *product-oriented* processes will help the project manager develop content for the paper. The body of this paper will focus primarily on *project management* processes and *product-oriented* process guidance will be included in the appendices.

There are 47 project management processes defined by the Project Management Body of Knowledge (PMBOK Guide, 5th ed., 2013, p. 61). The 47 processes are divided into 5 process groups. Every project, large or small, will have at least one process in each of the process groups. The five process groups are: *Initiating*, *Planning*, *Executing*, *Monitoring & Controlling* and *Closing* (PMBOK Guide, 5th ed., 2013, Ch. 3). While writing a research paper can represent a big undertaking for a single person, in the world of project management it represents a small project and therefore will not require all 47 processes.

Figure 1



Five process groups and 12 of the 47 project management processes.

Figure 1 illustrates a mind map outlining the five process groups described. These process groups are depicted with the associated processes. These processes are then related to each of the specific activities necessary for the production of a Gold paper.

Sections 3 through 7 will describe each of the five process groups, the associated processes and specific activities required to complete a GIAC Gold paper. Each section will begin with a definition from the PMBOK Guide of the goal for that process group in general. It is followed by a statement of goals for that process group as they apply specifically to a Gold paper project.

3. Initiating Process Group

The secret of getting ahead is getting started. The secret of getting started is breaking your complex overwhelming tasks into small manageable tasks, and starting on the first one. – Mark Twain

The purpose of the initiating group processes is to establish an agreement between two parties that marks the start of the project (PMBOK Guide, 5th ed., 2013, p. 54).

Goal – General

The initiating processes describe the first steps taken in a project resulting in a *project charter*. The *project charter* is an agreement between the party requesting the project and the party managing the project.

Goal – Gold paper project

Choose a topic and submit an abstract summarizing the topic. When GIAC approves the topic, the author will receive e-mail notification that functions as the *project charter*. The author and assigned advisor will then initiate their regular communication.

3.1. Develop Project Charter

The *project charter* establishes a formal agreement between the student wishing to write a Gold paper and GIAC and is an acknowledgement that the project has been authorized and may begin.

3.1.1. Choose a topic

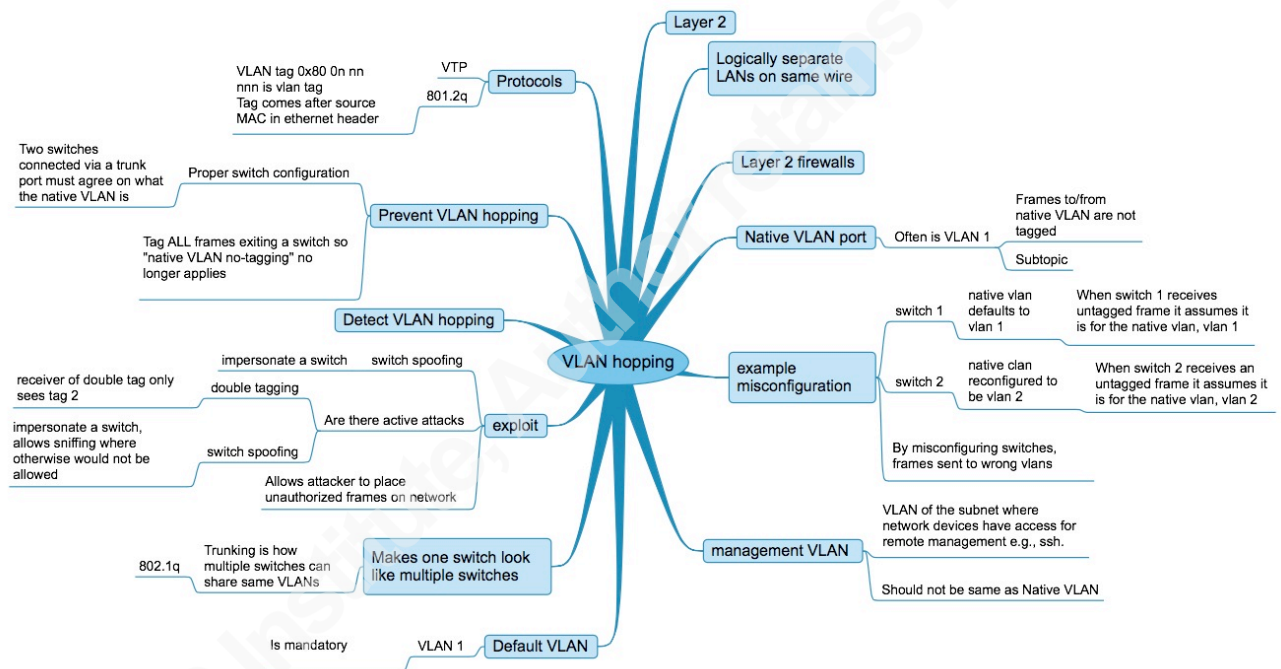
Based on a survey done of 50 previous Gold paper authors, results show that one of the most difficult aspects of a Gold paper project is establishing a feasible topic. GIAC has published a video that provides suggestions on choosing a topic as well as a list of interesting topics at <http://www.giac.org/certifications/gold>. A GIAC Gold paper has a maximum length of 30 pages and will not be accepted if it exceeds that limit, making it imperative that the paper has a narrow enough scope to accommodate this limitation (GIAC, 2014).

Many of the previous Gold paper authors that responded to the survey recommended that an author choose a topic that is either interesting to him or required by his employer or both. Choosing a general topic that is interesting may not be too difficult. Determining whether or not it would make a suitable topic for a Gold paper and

then narrowing the scope to make it a feasible project is likely to present more of a hurdle. Mind mapping is a technique that can help at this stage (Pinola, 2013).

Figure 2 shows an example of a mind map used to brainstorm a potential topic (Novamind, n.d.). The example topic is VLAN hopping, a known attack technique against a network switch (McClure, Scambray, Kurtz, 2009). The figure was created with a mind-mapping tool and is the result of approximately 10 minutes of brainstorming.

Figure 2

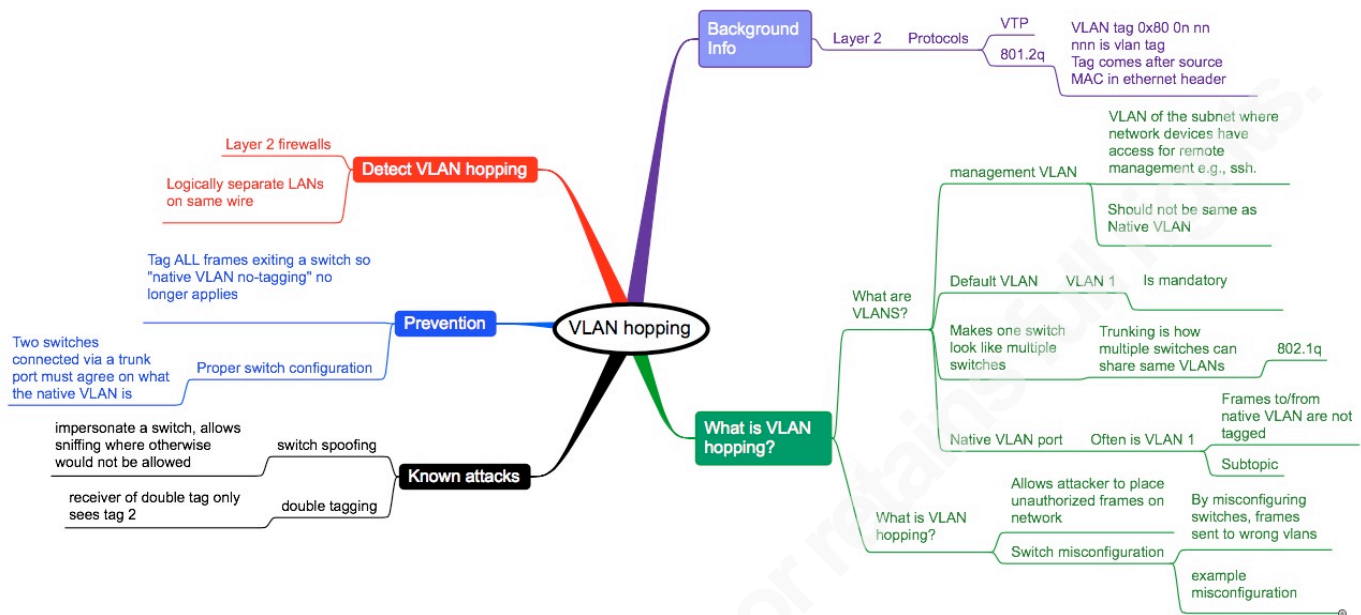


The mind-mapping tool¹ allows for easy reorganization and reformatting of the diagram so that ideas can be grouped in a more logical way after the initial brainstorming session as shown in Figure 3.

¹ A video about using mind mapping tools is at URL

https://www.youtube.com/watch?v=YIOHw_dw7W4

Figure 3



Colorize and rearrange the mind map to help focus the topic.

3.1.2. Write and submit an abstract

In order to initiate a GIAC Gold paper, the author must write an abstract concisely describing the paper. In general, the purpose of an abstract is to gain readers' attention and should describe why the chosen topic is interesting, what problem the author is trying to solve and how she will attempt to solve it. This is a *descriptive* abstract as defined by the Purdue University Online Writing Lab (Driscoll, 2012). The "readers" at this point in the project are the Gold paper advisors, so the purpose of the abstract is to convince them that the paper will be valuable to the security community. This version of the abstract may contain supporting information if the project manager feels it would be useful to the Gold paper advisors. The project manager then submits the abstract to GIAC². After the abstract is accepted and the appropriate fee is paid, an advisor will be assigned. Notification of the assigned advisor can be considered the *project charter*. Figure 4

² The normal procedure for submitted an abstract begins by logging in to your SANS portal account, selecting *Certificate History* and then *Go Gold* for the relevant certificate. STI students may have a different procedure that is curriculum version dependent.

shows a sample abstract from a GIAC Gold paper application submitted in August 2014 by Vinay Pereira and reprinted with his permission.

Figure 4

Abstract for paper titled *Security Assurances for Organizations that use Software as a Service*:

The world is moving to software as a service because of the many benefits it offers to all types of organizations. There is no question that it offers organizations cost benefits, agility and use of the expertise and custom software provided by SAAS vendors. The expertise of the SAAS vendors release organizations from IT infrastructure costs. For security professionals this raises a number of questions, there is a perceived lack of visibility and control over public cloud infrastructure. SAAS vendors do offer a number of assurances but security professionals who are mostly a skeptical bunch need written or visual evidence that the security controls, monitoring and assurance are evident. SAAS vendors have recently been espousing the fact that they are certified to the ISO 27001 standard or provide SOC (Service Organization Control) reports. This paper will discuss the differences of ISO 27001 and SOC reporting to provide security professionals guidance when assessing SAAS vendor security controls. ISO 27001 certification and SOC reports provide Organizations assurance that the chosen SAAS vendors have taken steps in the right direction to ensure that security is embedded in their processes and infrastructure.

A Gold paper abstract submitted by Vinay Perieira.

3.1.3. Scope creep

Scope creep is an expression used to describe a project that has expanded beyond its original objective and can negatively affect the outcome of a project if not managed properly (Heldman, 2013, p. 509). The survey in Appendix E further suggests that scope creep has presented problems for many Gold paper authors. Managing a paper's scope will be detailed in section 6.1 but is introduced here because the scope of a Gold paper is initially shaped by the abstract. Writing an abstract that accurately defines a research topic will help guide the project manager in establishing a concise scope statement during the planning phase.

3.1.4. The value of original research

By definition, the goal of original research is to produce new and/or noteworthy results and as such would benefit both the author and the security community. Choosing a topic that requires original research is suggested and welcomed by GIAC, although it is not required (Ullrich, 2014).

3.2. Identify Stakeholders

The stakeholders in a project are people or groups directly or indirectly involved with the project. In a Gold paper project, the stakeholders will be at least the author/project manager, the assigned advisor, and GIAC. The project manager may elect to involve peer reviewers at a later stage and depending on the type of research required for a particular topic, there may be additional stakeholders.

After an abstract has been accepted, the project manager will receive an e-mail containing the contact information for the assigned advisor. The project manager should initiate contact with the advisor via email at this point and the planning phase can begin. A detailed outline will be sent to the advisor during the planning phase.

3.3. Initiating Process Group Outputs

At this point in the Gold paper project, the completed outputs that make up the *project charter* includes: the paper topic, the written abstract and the acceptance email from GIAC.

4. Planning Process Group

Organization is what you do before you do something, so that when you do it, it's not all mixed up. – A. A. Milne

The planning processes will define the project, define the scope of the project and map out the activities that will need to be completed in order to bring the project to the defined outcome. (PMBOK Guide, 5th ed., 2013, p. 55).

Goal – General

The goal of the planning process group is to articulate the objectives of a project and plan all activities and develop the schedules required to meet those objectives.

Goal – Gold paper project

Determine all the administrative parameters regarding the paper, develop a scope statement, create a list of required tasks and complete a spreadsheet to establish the project's schedule, including target completion date.

4.1. Collect Requirements

The goal of this process is to determine the exact requirements for a GIAC Gold paper. Most of the parameters are defined on GIAC's website (GIAC, 2014), however, those pursuing a Master's degree through the SANS Technology Institute (STI) may have different requirements. At the time of this writing, the relevant parameters regarding Gold papers are:

- Must be completed 6 months from date of acceptance/payment
- Submit outline within 10 days of abstract acceptance
- Submit a final draft to advisor for review within 5 months of acceptance/payment
- Submit final paper to advisor who will submit to GIAC
- Paper recommended length 15-20 pages, maximum length 30 pages (excluding appendices)
- Passing score of 70% according to grading rubric at http://www.giac.org/media/certifications/gold/gold_rubric.pdf
- Paper template with proper formatting at http://www.giac.org/media/certifications/gold/GIAC_Gold_Template.doc

- Use APA style and reference formatting (APA, 2014)

The Gold paper advisor may have additional requirements such as how often drafts of the paper should be submitted for review. This will be incorporated into the project schedule in section 4.4.

4.2. Define Scope

The output from the Planning process is a *project scope statement*. A scope statement is a detailed description of the project, included what the final project outputs are and perhaps also what they are not. The scope statement should be revisited throughout the project, especially during the *Monitoring & Controlling* processes, to verify that the project has not expanded beyond its originally stated scope. For a Gold paper, the scope statement should be a detailed description of what the author intends readers of the final paper to learn. The scope statement in this case can function like a mission statement. Before adding new content to the paper, the project manager can revisit the scope statement to determine if it should be included or not. The scope statement provides the author guidance while writing the paper but it is not a statement that is included in the paper itself.

Example scope statement for a Gold paper about certificate revocation:

After reading this paper, the reader should have a thorough understanding of what certificate revocation is, why it is important and what the current revocation checking capabilities are of the major web browsers.

The scope statement can be saved in a separate document or added to the project schedule for easy reference while performing the *Monitoring and Controlling* processes.

4.3. Create Work Breakdown Structure

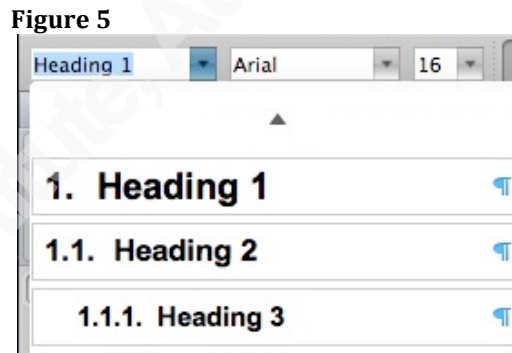
The Project Management Institute defines a work breakdown structure (WBS) as a subdivision of the project into smaller, workable pieces and encompasses the entire project (PMBOK Guide, 5th ed., 2013, p. 125). In the case of a Gold paper, a detailed outline functions as the WBS.

The Gold paper template, found at <http://www.giac.org/certifications/gold>, is an ideal tool for creating the outline because it already contains the correct APA formatting styles that will be required for the paper itself. An outline created in this way is ready to be expanded into the Gold paper by adding content to each section during the course of the research project.

At this stage of the project, the outline should include section headings and subheadings as well as a sentence under each heading describing the purpose of that section. See Appendix C for a sample outline.

GIAC requires the paper to be formatted using a numbered heading style and recommends that it be no more than three levels deep as described in the template document. The first, second and third level heading styles are included in the GIAC Gold paper template and can be selected from the style pull-down menu in Microsoft Word as shown in

Figure 5.



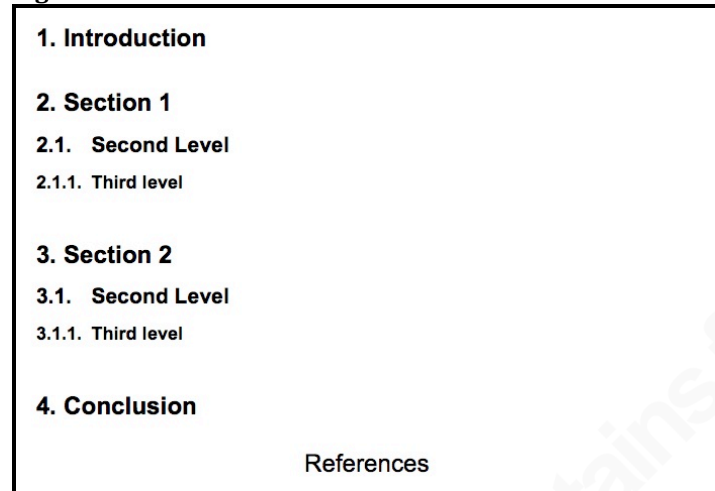
Correct APA heading styles built-in to Gold paper template

Using the numbered headings provides an efficient method of developing the WBS or outline as shown in Figure 6. Note that first and second level headings use *title case*³ and third level headings use *sentence case*⁴. See Appendix A for more APA style considerations for a Gold paper.

³ Title case uses capitalization for principle words like a title.

⁴ Sentence case capitalizes only the first word of the sentence and any proper nouns.

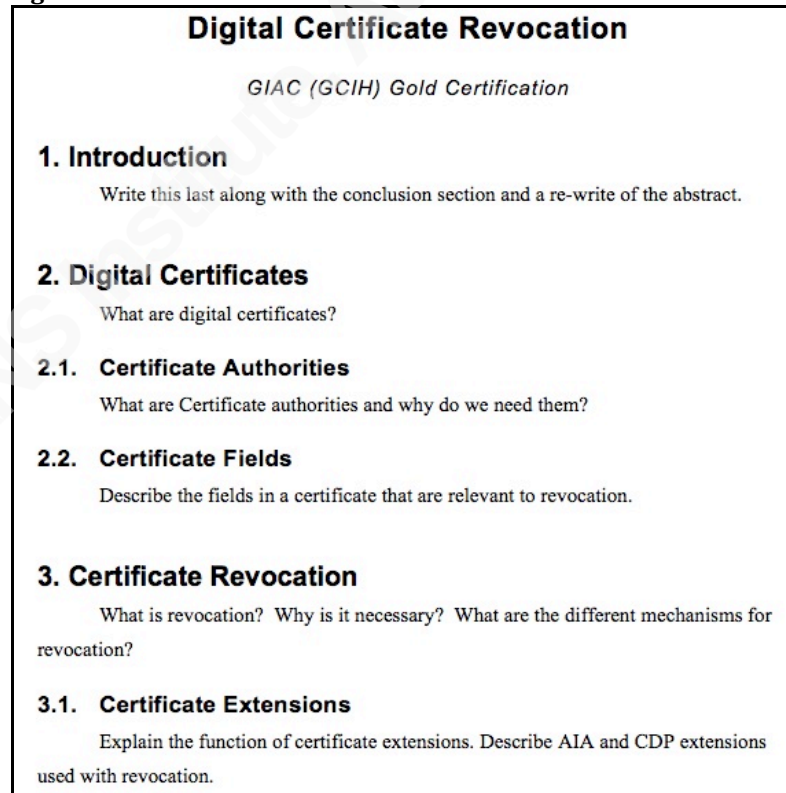
Figure 6



Example of nested numbered headings according to APA style

The completed outline can be sent to the advisor according to the requirements gathered in section 4.1. Figure 7 shows an excerpt from a completed outline.

Figure 7



Part of a completed outline submitted during the planning phase

4.4. Develop Project Schedule

“Work expands to fill the time available.”

-- C. Northcote Parkinson, 1955.

Using the WBS as a guide, the project schedule can be developed using the spreadsheet template at <http://www.giac.org/certifications/gold>. In other words, the outline will dictate the granular tasks that should be completed for each section of the paper and the schedule will assign a deadline for each task. According to the PMBOK Guide, there is a project management process named *define activities* that generates an activity list and a milestone list. These two outputs represent a detailed list of tasks to be completed. The tasks are grouped in categories called *milestones*. Since a Gold paper is a small project, *define activities* and *develop project schedule* can be combined, resulting in a detailed project schedule that contains a comprehensive list of tasks that is grouped by milestones.

Taking time to identify and schedule all activities and dividing them into groups representing project milestones will serve to keep the project manager on track time wise and provide an overview of the logical subdivisions of the project. Including as many activities as possible will provide a more granular overview of tasks and will ultimately help to create more accurate time estimates and target dates. Some of the milestones that may need to be included are:

- Set up and verify a test network.
- Design tests to prove/disprove hypothesis
- Analyze test results
- Write and revise paper
- Periodically submit draft to advisor⁵
- Control scope and schedule

⁵ How often this is required should be determined during the collect requirements process described in section 3.1

- Format according to GIAC requirements
- Have colleague(s) review paper
- Include time at end of project called *project buffer* to accommodate small schedule variances

Although the abstract is positioned at the beginning of the paper, before the introduction, it should be scheduled for completion last or nearly last because it contains a summary of the paper (“The Abstract”, n.d.). The written abstract submitted during the *Initiating* phase can be used as a starting point for the abstract that will be included with the final version of the Gold paper. Similarly, it may be logical and more efficient to schedule writing the introduction and conclusion sections after completing the body of the paper as well.

The PMBOK Guide describes a technique used to help develop the project schedule called the *critical chain method* (PMBOK Guide, 5th ed., 2013 p. 178). One of the ways that the critical chain method helps to prevent project finish date extensions is by allotting time at the end of the project that can be used if needed. This is called the *project buffer*.

Figure 8

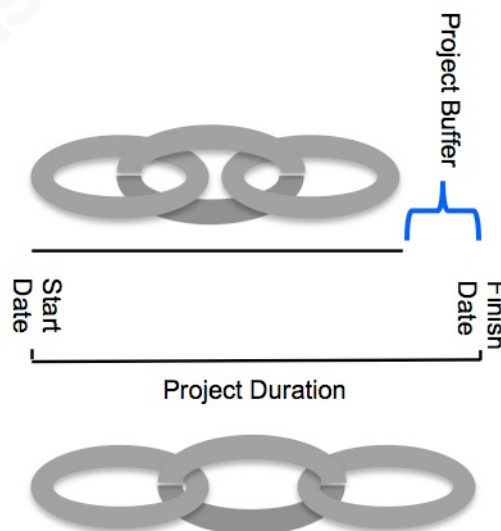


Figure 8 shows the project represented by links in a chain. Some of the links overlap because some tasks may happen in parallel or some tasks require less than one

day. Since the smallest time division in the project schedule template is one day, when multiple short tasks are completed in one day they appear to occur in parallel on the project schedule. Building extra time in at the end of the project allows some of the links to “stretch out” when needed, using up the project buffer without revising the finish date.

The project schedule template has two tabs. The first tab is for the project schedule, the second tab is a Gantt chart based on the project schedule. A Gantt chart is a graphical view of the project schedule (PMBOK Guide, 5th ed., 2013, p. 182). The Gantt chart is automatically generated using the data in the project schedule. A Gantt chart offers a visual overview of the tasks mapped to their allotted scheduled execution times.

Figure 9 shows a sample of a project schedule, divided into groups of tasks called milestones, developed for a GCFA Gold paper. See Appendix D for an example of a complete schedule.

Figure 9

Title: Forensic Images for Your Viewing Pleasure Scope Statement: This paper should make crystal clear to readers what forensic images are and what they are not. It will describe the different ways to access images and explain when you would use each method.						
		7/22/14		9/12/14		
ID	Task	Start Date	Days to Complete	Stop Date	Status	Notes
	Project Initiation	7/22/14	9	7/30/14		
	Select topic	7/22/14	2	7/23/14	Complete	Choose own topic or choose from https://
	Research to determine if topic suitable for gold paper	7/22/14	2	7/23/14	Complete	This is like a feasibility study. See gold p
	Write abstract	7/22/14	3	7/24/14	Complete	See "Sample-Abstract.pdf"
	Write supporting information for gold application	7/24/14	1	7/24/14	Complete	When you apply to write a gold paper yo
	Complete online "Go Gold" application	7/24/14	1	7/24/14	Complete	https://exams.giac.org/ Login and click c
	Receive notification of acceptance	7/25/14	1	7/25/14	Complete	each STI curriculum level may have diffe
	Submit payment to GIAC according to instructions in email (or STI specific instructions)	7/25/14	1	7/25/14	Complete	STI Students: http://www.sans.edu/stude
	Backup project documents	7/25/14	1	7/25/14	Complete	Others: Click on "Gold Applications" in p
	Complete Project Initiation				Complete	Zipped and uploaded to Google docs "G
Milestone 1						
	Create Detailed Outline					
	Create detailed outline	7/26/14	2	7/27/14	Complete	The outline serves as the Work Breakdo
	Establish references section	7/26/14	1	7/26/14	Complete	Set up a references page at end of outlin
	Add sentence or short paragraph to each item in outline	7/26/14	2	7/27/14	Complete	Started. Ultimately use APA citation form
	Refine the project schedule (this document) to reflect expected milestones. Add target dates.	7/26/14	2	7/27/14	Complete	use at least 3 published books as referen
	Send outline and project schedule to advisor					This can be very informal, but is meant t
						stating the goal of that section. Add tem
						The more time spent on the outline, the t

The project schedule allocates blocks of time for each task and is grouped by milestones.

4.5. Planning Process Group Outputs

The outputs from the planning phase are: the requirements for the paper, a scope statement, an outline and a schedule of tasks.

5. Executing Process Group

The three great essentials to achieve anything worth while are: Hard work, Stick-to-itiveness, and Common sense. – Thomas A. Edison

The executing process group consists of processes that lead toward completing the output of the project (PMBOK Guide, 5th ed., 2013, p. 56). In a Gold paper project, this phase corresponds with managing the tasks and time needed to complete the research paper.

Goal – General

This is when the project objective is carried out. Typically, more time is spent during this process group than any of the others.

Goal – Gold paper project

Conduct research and write the paper. Additionally, review and revise the paper's content during the executing phase.

The executing process group starts with the research and writing of the Gold paper and ends when the advisor accepts the final draft of the paper. Most of the project time is spent during this phase and is executed in tandem with the *Monitoring & Controlling* processes. At the start of each milestone group as well as after completing the tasks in each milestone group, execute the *monitor scope* and *monitor schedule* processes in the *Monitoring & Controlling* process group as described in section 6. Doing so will help ensure that the paper's content stays in scope and that the project stays on schedule.

5.1. Direct and Manage Project Execution

5.1.1. Research and write paper

The project schedule dictates the order in which the author performs the research and writing tasks to complete the paper. Before starting the tasks in any milestone group, execute the *monitor scope* and *monitor schedule* processes. This requires little time but does provide the author/project manager with a fresh reminder of the goal of the paper as well as any upcoming deadlines.

Perform the tasks associated with the current milestone group. Appendices A and B may provide helpful information during this phase of the project as they provide product-oriented process assistance such as formatting and citations.

When the tasks in each milestone are complete revisit the *monitor scope* and *monitor schedule* processes again for that milestone for schedule and scope verification.

5.1.2. Perform quality assurance

Submit a draft to either the advisor or colleagues for review as prescribed by the project schedule. The Gold paper survey results show that many previous Gold paper authors find that having peers frequently review their work is very helpful.

Work can begin on the next group of tasks while the current draft is out for review. When all of the content sections of the paper have been completed, compose the abstract, introduction and conclusion sections and prepare any planned appendices.

After receiving feedback from reviewers and making final changes to the document, submit a final draft to the advisor. This is the last draft for which the advisor will provide feedback prior to peer review and grading.

5.1.3. Final document check and submission

The example project schedule template contains several suggested tasks that will help to prepare a Gold paper for the grading and peer review process. Work through these and any other tasks that are included in the project schedule for the *Final Document Check* milestone. Many of the tasks concern APA formatting and are described in Appendix A.

When finalizing the document edit the metadata and enter the title of the paper in the *title* field of the document properties. Google indexes PDF files based on the contents of the *title* field so add the paper title or relevant key words to the *title* field (Google, 2011).

After completing the tasks in the *Final Document Check* milestone, submit the final revision of the paper to the advisor for peer review.

6. Monitoring & Controlling Process Group

Determine never to be idle. No person will have occasion to complain of the want of time who never loses any. It is wonderful how much may be done if we are always doing. – Thomas Jefferson

The processes in this phase will allow the project manager to measure both the project's progress as well as the project's scope. These processes are executed in parallel with the *executing* process groups (PMBOK Guide, 5th ed., 2013, p. 57).

Goal – General

This process group is revisited throughout the *Executing* project phase with a goal of examining the project's current status with respect to scope and schedule and taking corrective action when necessary.

Goal – Gold paper project

Review the paper's content before and after every milestone to determine if the content still satisfies the stated goal in the scope statement. Review the project schedule before and after every milestone to determine if the project is still progressing as scheduled.

6.1. Control Scope

The process of conducting research and writing a paper based on that research might naturally lead the author to investigate new ideas not initially considered when the

abstract was accepted. This may, in turn, alter the outline or the flow of the paper. Revisiting the scope statement will help to determine if the change in flow also results in a change in the scope of the paper. Changes during the course of the project are inevitable but uncontrolled changes are what lead to scope creep (PMBOK Guide, 5th ed., 2013, Section 5.6). While writing a Gold paper, changes in scope can be controlled by revisiting the scope statement before and after every milestone and evaluating the change. If the proposed change still provides content that is in line with the stated scope statement then it may be acceptable. Otherwise, consider removing the new content or including it in an appendix. If the author explicitly decides to add the out of scope content, update the scope statement⁶ so that it accurately reflects the new direction of the paper.

6.2. Control Schedule

At the end of every milestone, update the project schedule to reflect the newly completed tasks. Reviewing the next scheduled milestone group and the target deadlines will help the project manager proceed through the process of writing the paper in an organized manner. Figure 10 shows a section of a project schedule for a Gold paper project. Milestone 2 is complete and several tasks in milestone 3 that are being executed simultaneously are still in progress.

Figure 10

	Refine the project schedule (this document) to reflect expected milestones. Add target dates.	7/26/14	2	7/27/14	Complete	Note that as you progress through paper, these
	Send outline and project schedule to advisor for guidance/comments	7/27/14	1	7/27/14	Complete	Must be submitted to advisor within 10 days of
	Backup project documents	7/27/14	1	7/27/14	Complete	Zippped and uploaded to Google docs. 508-Gol
Milestone 2	Complete Detailed Outline				Complete	
	Set up test lab					
	Create small test VMs for imaging - Window7 & Linux	7/28/14	2	7/29/14	Complete	
	Create test image using FTK imager - Windows & Linux	7/28/14	2	7/29/14	In progress	Check out the images at http://www.forensicloc
	Create test image using Encase - Windows & Linux	7/28/14	2	7/29/14	In progress	
	Create test image using dd - Windows & Linux	7/28/14	2	7/29/14	In progress	
	Create multi-volume disk for imaging - Windows	7/28/14	2	7/29/14		
	Test image mounting and accessing files	7/30/14	3	8/1/14		
	Create and test mounting encrypted volume - bde mount	7/30/14	3	8/1/14		
	Backup project documents	8/1/14	1	8/1/14		
Milestone 3	Complete Section 3					

Example project schedule that will be updated as tasks are started and completed.

⁶ This may require a revision of the final abstract.

During the Executing process group unanticipated delays or roadblocks may occur. Schedule variances may not always require schedule revisions because small variances might be able to be absorbed in the extra buffer time built in to the schedule initially. A buffer of extra time built in to the end of the project is called the project buffer, as described in section 4.4. If the project buffer cannot absorb the schedule variances then the project schedule should be revised and updated with the new target dates.

7. Closing Process Group

Success is dependent on effort. -- Sophocles

Goal – General

Ensure that all project objectives have been met and perform any administrative tasks associated with formally finishing the project.

Goal – Gold paper project

Make revisions as required based on GIAC feedback and perform final administrative tasks.

7.1. Close Project

Once a project has met all of its objectives it can be closed or finalized. In the case of a GIAC Gold paper this would occur after the final revision of the paper has been sent to the advisor for grading and peer review. GIAC will send either a notice of acceptance to the author or a notice that revision of some sort is required. Perform any required revisions as requested by GIAC.

After the notice of acceptance is received, perform any remaining administrative tasks such as creating a final backup to close out the project.

8. Conclusion

Finding the time to research and write a Gold paper is one of the biggest hurdles that authors face, according to the survey respondents. Using the tested tools of project management to organize one's time can help an author use his valuable time more efficiently. Establishing a project schedule with deadlines for each task helps to keep the author on track and moving toward successful completion of the project.

The templates discussed throughout the paper are described in Appendices C and D. They are meant to further reduce the amount of time and anxiety required to finish a paper by providing assistance with the more mundane tasks like creating an outline, creating a schedule and formatting and sorting citations.

Using the project management processes for quality review provides a mechanism to detect scope creep and project delays earlier rather than later in the project. Using project manage tools and techniques when writing a GIAC Gold paper adds some administrative overhead, however, careful organization may help the author produce a better quality paper in a more time efficient manner.

References

- (2010). *Publication manual of the American Psychological Association*. 6th ed. Washington, DC: American Psychological Association.
- APA. (2014, January 1). The basics of APA style [Tutorial]. Retrieved from <http://www.apastyle.org/learn/tutorials/basics-tutorial.aspx>
- Driscoll, D. (2012, December 3). Technical reports & report abstracts [Reference document]. Retrieved from <https://owl.english.purdue.edu/owl/resource/656/1/>
- GIAC. (n.d.). Gold overview [Web page]. Retrieved from <http://www.giac.org/certifications/gold>
- Heldman, K. (2013). *PMP: project management professional exam : study guide*. 7th ed. Indianapolis, Ind.: Wiley.
- Illyes, G. (2011, September 1). PDFs in Google search results [Blog post]. Retrieved from <http://googlewebmastercentral.blogspot.com/2011/09/pdfs-in-google-search-results.html>
- McClure, S., Scambray, J., & Kurtz, G. (2009). *Hacking exposed 6: Network security secrets & solutions*. New York: McGraw-Hill.
- Novamind. (n.d.). Brainstorming using mind maps [Blog post]. Retrieved August 12, 2014, retrieved from <http://www.novamind.com/mind-mapping/brainstorming/#mmcontent>
- Pinola, M. (2013, September 9). How to use mind maps to unleash your brain's creativity and potential [Article]. Retrieved from <http://lifehacker.com/how-to-use-mind-maps-to-unleash-your-brains-creativity-1348869811>
- Project Management Institute. (2013). *A guide to the project management body of knowledge (PMBOK Guide, 5th ed.)*. Newtown Square, Pa: Project Management Institute.

SANS Institute: Reading Room [Web page]. (n.d.). Retrieved from
<https://www.sans.org/reading-room>

Sargent, A. Mamishev. Murray. (2013). *Creating research and scientific documents using Microsoft Word*. [S.l.]: Microsoft Press.

Snyder, C. Stackpole. (2013). *A user's manual to the PMBOK guide-- fifth edition*. 2nd ed. Hoboken, N.J.: J. Wiley.

Strunk, W. (2012). *The elements of style: 18 essential rules for good writing in English*. New ed. Thousand Oaks, Ca: Lakewood Pub..

The Abstract - Organizing Your Social Sciences Research Paper - LibGuides at University of Southern California [Web page]. (n.d.). Retrieved from
<http://libguides.usc.edu/content.php?pid=83009&sid=621164>

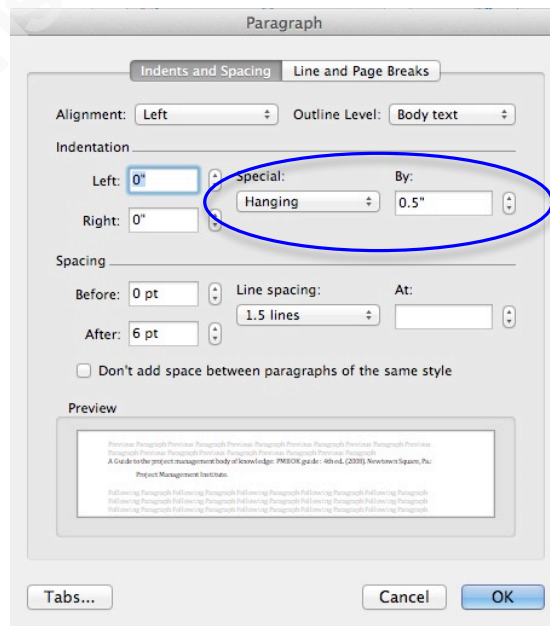
Ullrich, J. (2014, January 17). How to write a GIAC gold paper [Video]. Retrieved from
<https://www.youtube.com/watch?v=kAjv3e4DTbo>

Appendix A

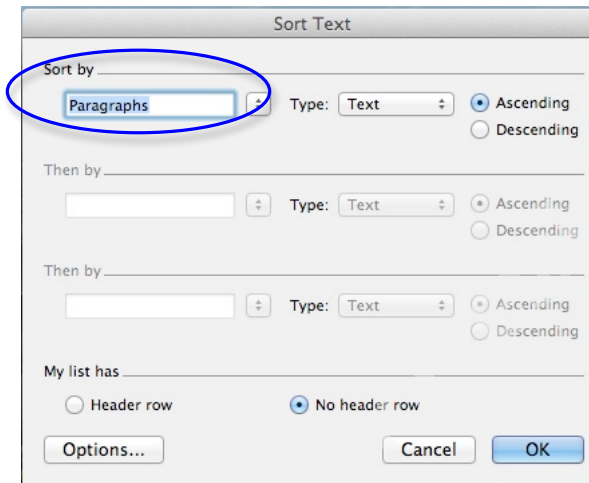
APA Style Considerations for a GIAC Gold Paper

The following recommendations are taken from the *Publication Manual of the American Psychological Association*, 6th ed, 2010 and the SANS Gold paper guidelines found at <http://www.giac.org/certifications/gold>.

1. According to APA style, the References section should only include materials from which specific information is cited or discussed in the text. It should not include materials that were used for general research on the topic.
2. Specific guidelines on reference formatting can be found at <http://www.apastyle.org/learn/quick-guide-on-references.aspx> and <http://blog.apastyle.org/apastyle/2010/11/how-to-cite-something-you-found-on-a-website-in-apa-style.html>.
3. Format references with hanging indent: highlight all references, right-click and choose Paragraph... Then choose Indentation *Hanging* with next lines indented by 0.5".



4. Add references to your list as you use them without attention to order. When all references for the paper have been added to the reference list sort alphabetically by highlighting all entries and sorting by paragraph.



5. Within the body of the document, citations should use the formats shown in the following examples for one, two or three+ authors.

One author:

Full citation in References section:

Rescorla, E. (2001). *SSL and TLS: Designing and building secure systems*. (1st ed.). Montreal, Canada: Addison-Wesley Professional.

All in text citations: (Rescorla, 2001, p. 121)

Two authors:

Full citation in References section:

Kanclirz, J., & Baskin, B. (2008). *Netcat power tools*. Burlington, MA: Syngress Pub.

All in text citations: (Kanclirz and Baskin, 2008)

Three or more authors:

Full citation in References section:

Corbet, J., Rubini, A., Kroah-Hartman, G., & Rubini, A.
(2005). *Linux device drivers*. Beijing: O'Reilly.

In text citation first occurrence:

(Corbet, Rubini, Kroah-Hartman and Rubini, 2005)

Subsequent occurrences:

(Corbet et. al., 2005)

6. Any citations that are direct quotations from another text (even if from your own previously written work) must include the author, the year and the exact page or paragraph from the original text. See Chapter 6 of the APA Publication Manual.
7. The *Title* of the paper and other labels such as *References*, and *Appendix* should not be in bold or numbered. These labels should be centered on the page and use Arial 18 point font.
8. Heading levels 1 & 2 use title case (capitalized like a title would be) and level 3 uses sentence case with first word capitalized and rest not like a sentence. (page 62 APA book).
9. All Headings, levels 1, 2 & 3 should be in bold. Heading 1 uses Arial, 16 point, bold-faced font. Heading 2 uses Arial, 14 point, bold-faced font. Heading 3 uses Arial 12 point, bold-faced font.
10. Footnotes should use the same size and spacing as body of the paper, which is Times New Roman, 12 point with 1.5 spacing between each line.
11. In contrast to the APA style recommendations, the introduction should be labeled as Introduction and included in the label-numbering scheme of the document (<http://www.giac.org/certifications/gold>).

Appendix B

Gold Paper Tips From Previous Authors

This appendix includes suggestions from previous Gold paper authors. The name of the author has been included when known otherwise the suggestion was submitted anonymously.

1. Set deadlines and then go for it. Writing a paper is a great learning experience.
2. Select a topic that you are passionate about and that is practical to your everyday work... You will be more motivated to do work on it. Also, do original research & development... – *J. Brouwer*
3. Deadline approaches fast. Make sure you leave ample room for unforeseen events, don't leave too much work to be done at the end of the timeframe, and try to avoid scope-creep.
4. Start early. It will take 2-3 times the amount of time you initially think it will. As an author with knowledge, you will notice things that need to be added or revised while editing and rereading your paper. Have at least one layperson and two technical people review the paper for both content and grammar mistakes. Seriously consider their criticisms. Do not submit a paper of substandard quality or presenting poor grammar. It reflects poorly. I've read papers in the SANS Reading Room that would reduce my inclination to hire someone were they looking and I were conducting their career background check. This paper is going to be in the Reading Room is forever, far after you learn to write properly, so make it an A+ effort.
5. Don't submit your topic until you have written at least a few pages and done some of the research. You don't want to be stuck with a dead-end topic. – *M. Pokladnik*
6. If any part of the project involves interaction with an operating system make SURE you are working on a VM. – *S. Northcutt*
7. Look at examples of other submitted papers. This can give you a good idea of the level of writing needed and how to successfully organize the topic. Write the first

- draft and allow yourself to not get it perfect the first time. I had to do two serious revisions of the paper before I was satisfied with lots of smaller passes for minor adjustments. Getting the first draft out made editing and revising easier. – *N. McKellar*
8. Write your paper on something you are knowledgeable about (unless you want to put added stress on yourself and write a paper about something you know nothing about). Also, have a few coworkers review your paper for technical detail and soundness. Have a none technical person read your paper to ensure it makes sense and flows well. – *E. Nooden*
 9. Make sure that your paper scope is appropriate from the beginning. A very broad paper becomes difficult to reign in. Reach out to instructors for topics and then hone them to get the right scope. Start reading references BEFORE you submit your topic to get confirmation that your scope is correct. – *D. Fletcher*
 10. Carve out 2 hours each morning. – *R. Eubanks*
 11. From my experience writing and as an advisor, it is critical that they have an additional qualified resource for proof reading. On gold papers I will often do grammar revisions, change sentence structure, and make sure things like third-person are utilized throughout the paper. These are sent to the student as suggestions for revision. – *T. Purcell*
 12. Ask advisor for access to turnitin.com and submit your paper to make sure you have properly attributed all quotes from other texts.
 13. Start early, work the outline, leverage your advisor.
 14. Interview multiple advisers before submitting. The approach required by SANS/GIAC is unfair as it's first-come-first-serve for the advisers.
 15. Topic selection is critical. Spending hours for several days researching a topic is not wasted time. What challenges do you struggle with in information security? Has anyone written about that? If not, other people probably have that question too, and it remains unanswered. The pre-research also helps you discover if there is enough of a base to build your paper on, and helps you head off challenges in

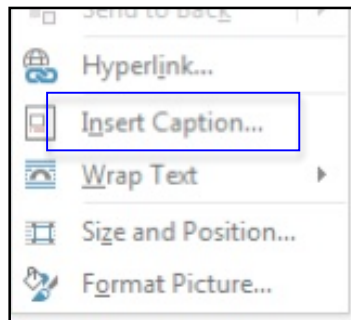
- scope or content. Don't worry as much about whether your work is completely "original" - all work is built on the shoulders of giants, and sometimes combining or building on previous research to reach a new or practical answer is more helpful to the community as doing some theoretical exercises. I'd also say it's helpful to make a small project plan or schedule. You may stray from it, but having clear checkpoints (even if they're arbitrary) will prevent you from placing your GIAC Gold paper on the back burner. – *C. Imbert*
16. Early on, be sure to identify all the questions that the reader might have about the topic, and make sure the outline addresses all the questions.
17. Spend the time upfront understanding the exact research question you are going to answer first. Create an outline and stick to it. Might also be helpful to read a research book (like *The Craft of Research*) first to help you get organized. – *C. Blais*
18. Keep it simple. Choosing a narrow topic will help keep the paper writing straightforward and on target. – *T. Bond*
19. They say the goal is 15-20 pages that you can read in one sitting. Put any details that distract from the flow of the paper in an appendix or end notes. – *M. Pokladnik*
20. (Informed by both my own experience and experience as a Gold advisor/grader.) Try to focus on a specific, academically interesting QUESTION or controversy, or a limited set of questions, rather than surveying a field or describing a project. If you are describing a novel product or process, a HOWTOs can be OK, but it is best to know what a thesis is, and to have one. If the conclusion of your paper merely summarizes the preceding narrative rather than settling an argument, you have not done this. – *R. Graves*
21. Spent the time to fully understand the APA style of writing especially when it comes to references and citing. Do not complete this at the conclusion of writing your paper, do this as you write it. Review this regularly with your mentor so you stay organized and on top of it. – *T. Salka*

22. Try to be as narrow and specific with your scope as possible. Broad or poorly defined topics tend to cause scope creep or create a paper with little valuable detail.
23. Start early (don't procrastinate). Choose a topic you really like because you're committed to it for months. Can this paper help you elsewhere, eg. for a possible job promotion? Try to come up with an original topic instead of rehashing existing work; who wants to read about a topic written about a dozen times over in the same venue? Enjoy the experience as it will make the quality of work done better. – *A. Warren*
24. 1) Interact with your Adviser early and often. Quality was improved on papers where I had more interaction with advisers. 2) Avoid zero progress weeks. Get at least something done every week. Once you stop, static friction is harder to overcome. 3) Target your finish for 1 month before deadline. This will give you time to set it down and come back and read it with fresh eyes. Papers finished at the last minute will show the flaws. 4) Read the Grading Rubric before you start. 5) Collect and document References as you go. You read the Rubric correct? References factor in to the grade. Online Note services work well for this. – *G. Farnham*
25. Approach it in a structured manner. Use the guide provided to help structure your paper. Seek input from peers and SMEs (dependent on subject) as well as the advise of the SANS Advisory Council, where warranted. Be familiar with the format and structure for writing research paper but make it your own. Check it twice and then check it again before submitting (spelling, grammar, logic/flow, etc.). – *C. Brown*
26. Briefly, be entirely prepared to write the paper(s) for the topics you apply for. I wouldn't say you have to already have a complete outline and rough draft, most of your research complete, charts graphics and screenshots ready, all your sources gathered and cataloged, and reviewers lined up ... but if you do it will be a much smoother and more pleasant experience and you will be able to focus on your

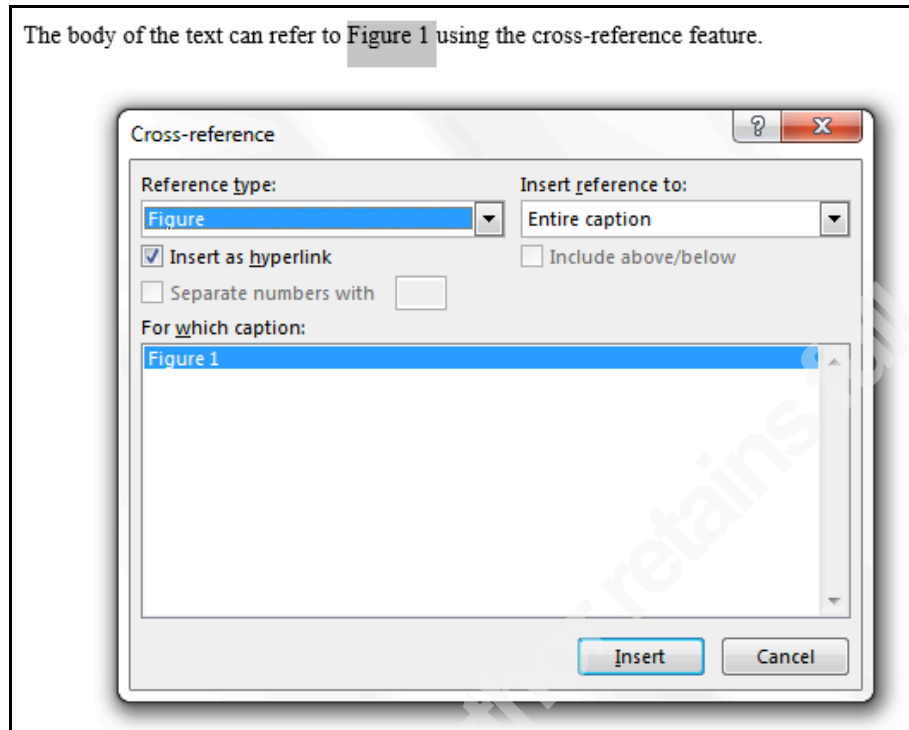
content and message and not have to spend time and energy on mechanics. – *B. Knowles*

27. Save your document often. As Word documents become larger they seem to get less stable. Save and make backups! If you do have a problem documents are often recoverable. See this post <http://studioscribbles.blogspot.com/2011/04/how-to-retrieve-lost-word-document.html>.
28. Build figures and tables in separate documents. I use a folder called Figures and have a separate WORD document for each. When you are happy with the figure, take a snapshot and include it as a picture in your document. This makes formatting the final document easier especially when converting to PDF file later.
29. When adding a figure or table to your document, add a caption to it with the built-in MS Word caption feature. This way you can use a cross-referenced hyperlinked field. Doing it this way allows you to move or insert figures without having to renumber previous figures.
30. On Windows and OS X:

Right click on a picture and select insert Caption...



To insert a link to the figure or table from within the text select Cross-reference from the **Insert** tab:



When inserting a table or figure into the middle of a document causing the numbering of the other figures/tables to change, you need to update all hyperlinked fields so that they still correspond to the correct figure or table. Do this by selecting all text (left-click in the document and enter CTRL-A for Windows or ⌘-A on OS X). With all text selected right-click and select *Update Field*.

Appendix C

Sample Outline for a GIAC Gold Paper

This outline shows an example that could be sent to the Gold paper advisor during the planning phase. Use the outline to develop a project schedule as shown in Appendix D. Under each item jot down a sentence or two that reflects the focus of that section.

Digital Certificate Revocation

GIAC (GCIH) Gold Certification

1. Introduction

Write this last along with the conclusion section and a re-write of the abstract.

2. Digital Certificates

What are digital certificates?

2.1. Certificate Authorities

What are Certificate authorities and why do we need them?

2.2. Certificate Fields

Describe the fields in a certificate that are relevant to revocation.

3. Certificate Revocation

What is revocation? Why is it necessary? What are the different mechanisms for revocation?

3.1. Certificate Extensions

Explain the function of certificate extensions. Describe AIA and CDP extensions used with revocation.

3.2. Certificate Revocation Request Authentication

Authentication of revocation requests is important to reduce likelihood that certificate gets revoked accidentally, deliberately or wrongfully.

3.3. How to Check Revocation Status

Show what it looks like when a browser encounters a revoked certificate. The two methods for checking the revocation status of certificates, CRL and OCSP, will be discussed in separate sections.

3.4. Certificate Revocation Lists

This is the first and oldest method. Explain how it works.

3.4.1. How CRLs work

3.4.2. What are current sizes of some CRLs?

Find common CRLS and measure. Show examples.

3.4.3. Revocations over time

Show how revocation numbers have changed since Heartbleed. ISC has tool for this.

3.5. Online Certificate Status Protocol (OCSP)

OCSP is a newer method for checking certificate revocation status and is outlined in RFC 6960. Why was it developed – to solve what problem with CRLs?

3.5.1. How OCSP works

Explain, noting that it requires separate HTTP requests that occur outside the SSL session.

3.5.2. OCSP stapling

What is it and why was it developed? What problem was it intended to solve?

3.5.3. OCSP must staple

This exists in theory and the exact implementation is currently being debated. What problem would it solve? What are the hurdles to implementing it?

4. Browser Behavior

This section will talk about specific browsers handling of certificate revocation. Describe current defaults as well as optional settings.

4.1. Chrome

Chrome gets its own section because it does things so differently.

4.1.1. Public key pinning

What is it?

4.1.2. Chrome CRLSets

What are they and who uses them? How do certificates get included in CRLSets?

4.2. Browser Comparison

Make a table comparing Chrome, IE, Firefox and Safari.

5. Conclusion

References

Appendix A
Digital Certificates in Depth

Appendix B
Viewing CRLSets

Appendix C
Revocation Reasons

Appendix D

Project Schedule Template

This spreadsheet template can be downloaded from

<http://www.giac.org/certifications/gold>. This template has been filled in with example dates. When using this template, fill in tasks by milestone group. Enter the start date for a task followed by the number of days you believe it will require to complete. The stop dates are calculated automatically. Use the pull-down menu in the status column to show tasks that are in progress or complete.

Title of Paper:		Start Date	Finish Date			
Scope Statement:		<Enter	8/1/14			
Milestones	Task	Start Date	Day to Complete	Stop Date	Status	Notes
	Project Initiation					
	Select topic	8/1/14	1	8/1/14		Choose own topic or choose from https://isc.sans.edu/gold/topics
	Research to determine if topic suitable for gold paper	8/1/14	3	8/3/14		Gold paper guidance video https://www.youtube.com/watch?v=kAv3e4DTb0
	Write abstract	8/3/14	3	8/5/14		See "Sample-Abstract.pdf"
	Write supporting information for gold application	8/4/14	1	8/4/14		When you apply to write a gold paper you must give supporting information about why this topic is relevant for this certification.
	Complete online "Go Gold" application	8/4/14	1	8/4/14		https://exams.giac.org/ Login and click on "Go Gold" for applicable certification. Process varies for STI student and each STI curriculum level may have different procedure.
	Receive notification of acceptance	8/4/14	14	8/17/14		
	Submit payment to GIAC according to instructions in email (or STI specific instructions)	8/17/14	1	8/17/14		STI Students: http://www.sans.edu/students/registration Others: Click on "Gold Applications" in portal account and follow payment instructions.
	Backup project documents	8/4/14	1	8/4/14		
Milestone 1	Complete Project Initiation					
	Create Detailed Outline					
	Create detailed outline	8/5/14	3	8/7/14		The outline serves as the Work Breakdown Structure for this project. The more time spent on the outline, the easier the paper will be to write.
	Establish references section	8/8/14	1	8/8/14		Set up a references page at end of outline document so as not to lose track of any valuable resources as you get started. Ultimately use APA citation formatting but start with at least valid URLs. NOTE: STI students are required to use at least 3 published books as references.
	Add short paragraph to each item in outline	8/8/14	2	8/9/14		This can be very informal, but is meant to help you stay focused on scope for that section.
	Refine the project schedule (this document) to reflect expected milestones. Add target dates.	8/8/14	1	8/8/14		Note that as you progress through paper, these milestones may change.
	Send outline and project schedule to advisor for guidance/comments	8/9/14	1	8/9/14		Do not include references document with outline
	Backup project documents	8/9/14	1	8/9/14		
Milestone 2	Complete Detailed Outline					
	Write Section 2					
	Research section 2	8/10/14	3	8/12/14		"Introduction" is section 1. Write Introduction and Conclusion last.
	Write section 2	8/10/14	3	8/12/14		
	Proofread section 2	8/13/14	1	8/13/14		
	Backup project documents	8/13/14	1	8/13/14		Save paper as ...Milestone3.doc
Milestone 3	Complete Section 2					
	Write Section 3					
	Research section 3	8/14/14	3	8/16/14		
	Write section 3	8/14/14	3	8/16/14		
	Proofread section 3	8/17/14	1	8/17/14		
	Backup project documents	8/17/14	1	8/17/14		Save paper as ...Milestone4.doc
Milestone 4	Complete Section 3					
	Write Section 4					
	Research section 4	8/18/14	3	8/20/14		
	Write section 4	8/18/14	3	8/20/14		
	Proofread section 4	8/21/14	1	8/21/14		
	Backup project documents	8/21/14	1	8/21/14		Save paper as ...Milestone5.doc
Milestone 5	Complete Section 4					
	ADD MORE SECTIONS AS NEEDED					
	Document Assembly					

Continued on next page

Continued from previous page

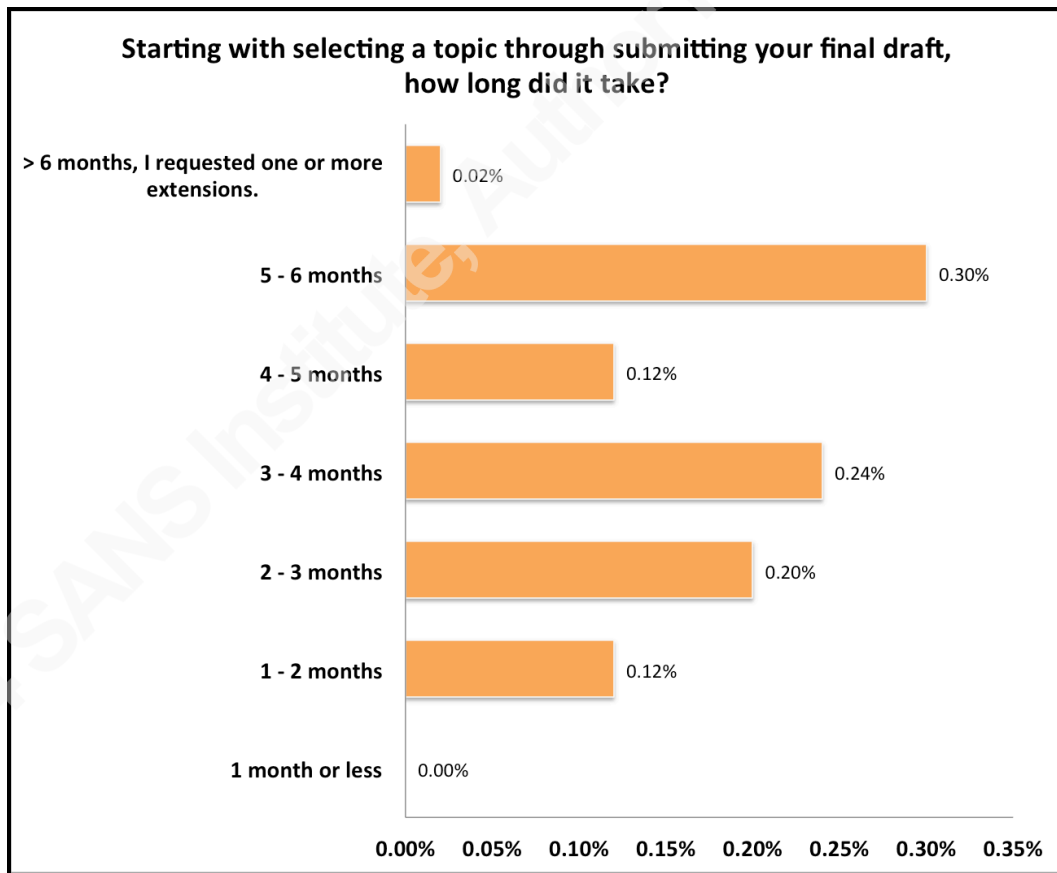
Milestone	Task	Start Date	End Date	Duration	Notes
ADD MORE SECTIONS AS NEEDED					
Document Assembly					
	Write Introduction	8/22/14	8/22/14	1	
	Write Conclusion	8/22/14	8/22/14	1	
	Write/revise abstract	8/22/14	8/22/14	1	Use the initial abstract as starting point.
	Proofread and revise entire document	8/22/14	8/22/14	1	
	Submit to colleague 1 for review	8/22/14	8/24/14	3	
	Revise document using feedback	8/24/14	8/24/14	1	
	Submit to colleague 2 for review	8/22/14	8/24/14	3	
	Revise document using feedback	8/24/14	8/24/14	1	
	Submit draft to advisor for review	8/25/14	8/29/14	5	This will be a pre-final version. Advisor will help you decide if the paper is ready to be formally submitted for peer review.
	Revise document using feedback from advisor	8/29/14	8/29/14	1	
Milestone 6	Complete Document Assembly				
Final Document Check & Submission					
	Run spell check	8/24/14	8/24/14	1	
	Run Grammar check	8/24/14	8/24/14	1	
	Check for consistency of capitalization and acronym usage	8/24/14	8/24/14	1	If you use a large number of acronyms consider building a glossary.
	Ensure two spaces between all sentences	8/24/14	8/24/14	1	
	Validate formatting of reference page	8/24/14	8/24/14	1	http://www.citefast.com
	Check figure and table numbering	8/24/14	8/24/14	1	Use update field option in MS Word
	Check Header and Footer	8/24/14	8/24/14	1	Header should include title and page number, Footer should include authors name and email.
	Check metadata in Word properties	8/24/14	8/24/14	1	
	Submit final document to advisor for peer review	8/30/14	8/30/14	1	
Milestone 7	Final Document Check & Submission Complete				
Project Closing					
	Receive Feedback or Acceptance from GIAC	8/30/14	9/12/14	14	May take about two weeks for response from GIAC
	Revise paper according to feedback	9/12/14	9/12/14	1	This may be simple formatting or it may require revisions in the paper.
	Check PDF formatting	9/12/14	9/12/14	1	Save as a PDF document and make sure conversion does not cause problems with figures etc.
	Make backup of entire project	9/12/14	9/12/14	1	Zip and archive
	STI students only - update course of study plan	9/12/14	9/12/14	1	Email dsardi@sans.edu upon receiving paper acceptance email. CC Toby Gouker, update personal records with Gold status.
Milestone 8	Project Complete		Finish Date 8/1/14		

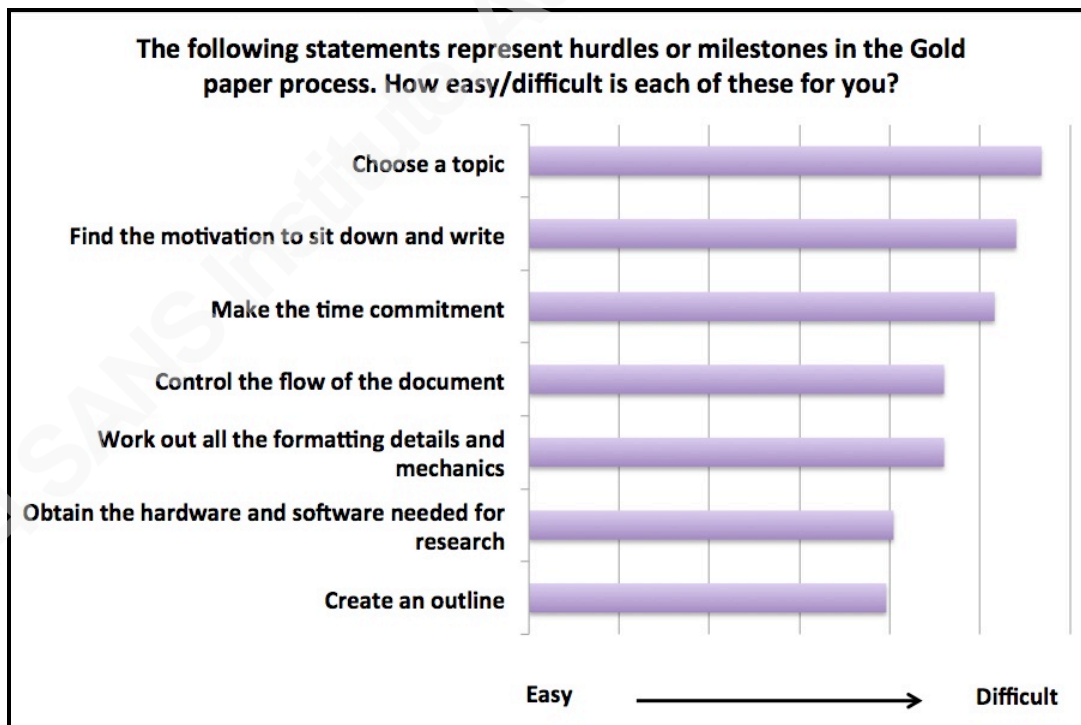
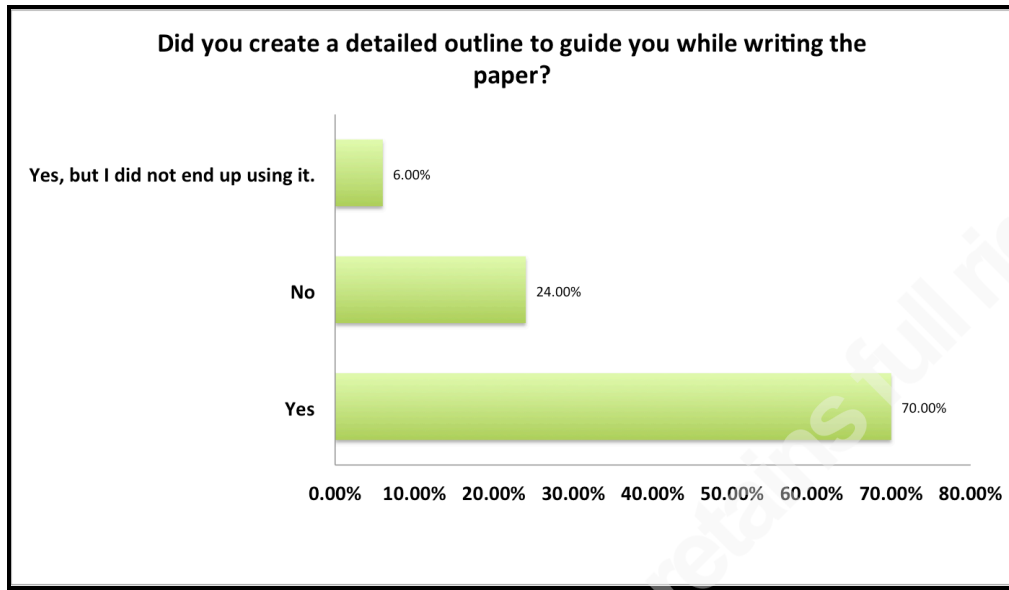
Appendix E

Gold Paper Survey Results

Some of the information included in the body of this paper referenced an online survey that was conducted. The 50 respondents to the survey are previous Gold paper authors.

The results from 5 of the questions are shown below. Answers provided to the open-ended question requesting “tips for future authors” have been included in Appendix B.





What trouble, if any, did you have managing the scope of your topic?

- 6 respondents answered “none”.
- Information on the topic was not always available from research sources.
- The biggest issue is outside reviewers, they seem to always want either more or less coverage on topics. Facing this right now with an analyst paper, which is similar to gold.
- First topic was overly broad for a 20-some page paper. Lots of useful information but choppy writing. Second was intended to be narrowly focused, but it's both extremely technically involved, making it hard to address the audience, and overlaps with a real work project, so has kinda expanded to encompass all aspects of that project.
- The adviser has an idea of what you need to include, sometimes it is different than the writer's idea.
- I kept finding myself wanting to deep dive on a particular section. I had to tell myself often that time and resources were limited so just keep going.
- For GSEC it seemed "boring" so I tried to add stuff. GCIA just took a large amount of data processing, GCIH.. do much time doing the research
- None, but the expectations were much different back then.
- Resources in finding information online.
- My topic was not focused enough so I ended up feeling like I had to cover everything. My paper was on the order of 40 pages as a result.
- Had some trouble with scope creep, but the outline and reaching out to my advisor helped a lot.
- Number of pages went long until I narrowed the scope
- I picked a topic that I was weak in because I wanted to learn more about it. I did learn a lot but I don't recommend doing this for a gold paper because the expectations of the grader were so high (expecting broad and advanced coverage).
<snipped>
- In general, I tended to want to put in too much detail on caveats, special cases and things that cluttered things up.
- Scope is a challenge. It can't be too small or too big. I would start with a general idea of what I wanted to do and then during research, I would find that someone already did that, so the scope would need to be changed. Also, when you start pulling threads on a topic, the scope of it expands and you have to just leave stuff out of the paper.
- Everything is bigger than you think
- Of course, picking the topic and defining the scope is the hard part. For me, just getting started was the hard part. Once I got going, it typically didn't take too long to finish it. Typically, around 3-4 weeks.
- You have to be brutal with scope. The ideal GIAC Gold paper is about 20 pages, which seems like a lot, but can easily be eaten up by unnecessary depth. There were times when I specifically wrote "this is not in scope". GIAC Gold papers are

rabbit holes, and whenever you think your topic is specific enough, you find you can write a thesis on it. It's just that the range of knowledge is so big on just about every topic that you have to select something as specific as possible, and even then, be careful about how deep you delve into it. I found adhering to my outline was most helpful.

- Just the adviser
- The scope looks different once you get into the research
- Really understanding the breadth or depth and what level of detail the chosen topic needed. I was in the programs early days and at that time it was hit or miss on grading.
- Scope was less of an issue than the initial topic selection
- Not really - I spent a lot of time on my outline and I kept with it.
- Oh wow it just kept getting longer and longer and longer. I didn't really manage it, just turned it in.
- I was lucky to have dedicated time from my job to work on this paper, so this question doesn't apply to me as much.
- None, I had more of a problem getting enough material into my paper.
- Staying on topic and not expanding the scope.
- My topic was on visualization, which required intense, high-density graphics. This was hard to represent in the whitepaper format.
- Not much for GSEC. The paper was something I'd already been thinking about for a while. GCWN was also fairly straightforward. With GCIA, I had a lot of trouble finding any definite attacks, even though there were a lot of indicators, and ended up using a bunch of different methods to try and analyze the data.
- Both times scope was fairly easy - they directly related to issues I was dealing with or could apply in my work.
- The only trouble was fitting in all the information that I wanted to present in the page count. i.e. too much information, too little space to put it on.
- I had a scope on one of the papers, which actually came out to 85 pages, I had a big fight with the advisor and other SANS people, but I won and the paper was published.
- It was intimidating. I looked over other papers available at the time and there were some excellent red team paper exercises and malware research topics as examples, which I felt I would have trouble doing. In the end, I chose to write about an incident we had at my place of work which had resulted in the decision to send someone on an incident handling course. The scope was built in once I made this decision.
- Very little once topic was chosen. I've always been good at writing papers.
- I had significant difficulty in determining appropriate scope (number of topics), depth (how far in-depth to go on each), and identifying a theme or thesis. My advisor was some help with this, but only at the very end of the project.
- Lots. I always have to whittle down the topic. Would be better to start narrow because papers tend to expand.

What trouble, if any, did you have with time management while writing the paper?

- 5 respondents answered “none”.
- I use the Google calendar and block the time.
- Some - conflicts with work.
- Research always takes the majority of the time--not writing.
- I love to read and got carried away with reading other people's technical work, leading to good but perhaps way too many references.
- Adviser response time.
- Was just hard to get started. Once started, the ideas and content seemed to flow.
- Lack of training on APA style. Have to figure it out much independently which is good for learning but bad for rework and time. There should be a formal training with instructor prior to writing a paper. A link to a website is not sufficient in my opinion. Understanding APA reference in advance of the writing the document would be very useful I worked with Kees Leune, he helped me to better understand APA. He is an excellent mentor.
- Life. Kids. Work. etc
- I procrastinated a great deal and ended up doing the bulk of the work in the few weeks before the deadline.
- Getting dedicated time to think through the flow of the paper.
- Due to the broad focus, I spent a LOT of time researching and trying to find all of the right answers
- I spend significantly amount of time on the papers, taking several months to choose a topic, research and get to the point of an outline. The actual writing goes much faster. The research tends to get pushed out in priority for me since there typically is no deadline for it other than the one I set.
- I grew terribly bored with the writing and found myself writing a few sentences and then doing ANYTHING other than writing the paper.
- None - was noticeable distracted by being done towards the end of the review with my advisor. I think it was just gold paper fatigue.
- I usually waited too long to get drafts to the advisor putting me in a bind if they didn't respond relatively quickly.
- Getting time to complete the paper.
- Research can sometimes take longer than expected.
- Just normal procrastination and leaving most of the work till the end.
- Need to know when to quit researching and start writing. That is the only thing that will help with scope.
- Just like any assignment, procrastination raised its ugly head. Again, once I got into the paper, it went pretty fast.
- Certain things were hard to quantify for time such as programming/scripting or testing something in different environments.
- Very difficult. The biggest challenge of writing a Gold paper. I planned on allocating two hours per day when writing my Gold papers, but found there were

times when I just could not even manage a half hour per day. When I get a chance to "binge write" on the weekends or have the energy to write late at night, I take advantage of it. Juggling work, home, and Gold papers is tough, but I think practicing time management with Gold papers is beneficial.

- None--I worked on it after work in the evenings.
- None really, just the usual juggling work and school at the time.
- With kids, time management is not easy at all, since the paper is written after work hours
- I'm a natural procrastinator. I put off most of the writing until the last month.
- Writing the paper took away from family time as it was done after working hours.
- Had an unplanned operation near the end of the deadline, which meant finishing the paper from the hospital bed. Should have left more time in the end to plan for unfortunate events.
- It was very easy to over research the topics or get distracted by other interesting technical information.
- None. Had lots of time.
- The only trouble with time I had was getting it written between work and kids.
- There were lots of things after my attention, but I made this a priority.
- The second time around was very difficult to manage time since I did not have the college class structure driving me. I don't manage time well in most things, so this naturally impacts papers as well.
- The toughest part is just to start - once you get going, it tends to start flowing.
- I did not manage my time, but completed both papers within the allotted time period, maybe a little sooner.
- Very little. To cover the rest of the course material, I had set a schedule for myself in the evenings. I used this time to write the paper as I finished covering the course.
- Very little outside of juggling getting my paper done with my work schedule and life outside work.
- I had significant difficulty in determining appropriate scope (number of topics), depth (how far in-depth to go on each), and identifying a theme or thesis. My advisor was some help with this, but only at the very end of the project.
- Not too much.