Preparing for the GSE

Kevin Bong, MSISE, GSE

Misconceptions About the GSE:

Let's start with some misconceptions that I think make the GSE seem intimidating:

Misconception: It's a waste of time and money because I'm likely to fail.
Not true. The great majority of people who sit for the GSE have passed it. If you read through my suggestions for how to prepare and what you should know, and feel comfortable you can achieve them, then I think it's very likely you'll pass the first time.

Misconception: I need to be a Linux/Snort/Cisco/etc. guru to pass.
Not True. The caliber of students that passed the GSE with me in 2006 was impressive; however, from my experience, all of my peers in the STI Masters program and many of the students I've worked with at SANS conferences are also of that same caliber and, from my perspective, would not find it difficult to pass the GSE.

Misconception: The challenges will be tricky or use obscure software.
Not True. GIAC wants you to pass. The best thing for GIAC to promote the GSE is to have more people achieve the GSE. The questions and challenges are not built to trick you or demonstrate obscure knowledge. The GSE is meant to have you demonstrate the knowledge of the important information in these domains and ability to apply it. The majority of the skills, tools, and techniques used in the challenges come directly fromSEC 401-GSEC, SEC 503-GCIA, and SEC 504-GCIH.

Misconception: I need to be a programmer to pass.
Not True. While the expectation may differ for the GSE-Malware, a lack of programming experience will not limit your ability to pass the GSE. I don't expect you'll be asked to decompile, evaluate something in a debugger or disassembler, or to build or deeply analyze malware. You do need to understand common programming mistakes and vulnerabilities such as buffer overflows, format strings, parameter injection, and cross site scripting, mainly so you can identify and correct it.

Misconception: I need to be a forensic investigator/security consultant by trade to pass.
Not True. It can help if these tools, concepts, and techniques are part of your daily life, but the GSE is not testing for a preponderance of experience doing these actions in the real world. It is more important that you understand the concepts, know how to use the tools, and are able to demonstrate the techniques and put multiple pieces together into an integrated attack, defense, or response. You can't just be book smart, you need to be able to perform the actions, but it's not too different from performing them in your labs during class or working with them in your test environment at home.

Preparing for the Multiple Choice Exam - General Section

This section is not GSE specific; it outlines the suggestions I've given to everyone who's asked me how to study for a GIAC proctored exam.

Create an index
In my opinion, almost all of the studying and preparation for any SANS multiple-choice test can be tied into generating a good index.
Make sure your index helps you find the right page quickly
You will have enough time to look up the answers you can't remember...as long as you have built yourself a good index with good keywords or phrases that get you to the right page.

Know the easy ones
Having a good index to use during the test seems like cheating — but it's not. You won't have enough time to look up every answer during the exam. You should be comfortable answering at least a third of the questions without touching your books or your index.

Understand the material
This is another reason having an index isn't cheating. If you don't understand a page or a concept in the courseware, you are not going to have time during the exam to figure it out. While you are building your index, don't just blindly copy keywords from every page. Stop on each page and consider if you understand the concept or action that's happening on that page. If you don't, stay there, study it further, try it yourself, or pull in other resources to figure it out until you understand it.

Index the labs
Don't forget to include the labs and any evening/bootcamp sessions when you create your index; all that content is utilized as the exams are built.

Have other references ready
There are a few other key references you'll likely find handy. The first are the SANS Incident Handling cheat sheets as well as the SANS TCP/IP and tcpdump quick reference guide.
Windows Intrusion Discovery Cheat Sheet
Linux Intrusion Discovery Cheat Sheet
TCP/IP handbook
You should also print out the help documentation or man pages from key commands or tools that you're likely to encounter, such as mount, dd, tcpdump, netcat, nmap. There are also a number of good common Linux command references available on the internet if you are less familiar working in Linux.

Don't use someone else's index
It is generally accepted that SANS' code of ethics would allow you to use a basic index that someone else created. However, I have seen a definite pattern, among people I've talked to, that people who build their own index pass more SANS exams the first time; and people who use someone else's index, or don't build a good index, fail. As my suggestion above reflects, when you build your own index you get familiarity, a review of all the material, and a chance to dig into the things you don't understand. You also have a better sense what keywords and phrases will help lead you to specific content much faster when you have built the index yourself. This is also the reason I don't post or give out copies of the indexes I've created.

Don't get thrown by streaks during the test
I've noticed this pattern in many of the tests I have taken, so I've asked other people about it and they often say, Yeah, that happened to me, too. Things are going well, then you start to get a whole bunch of questions wrong straight in a row. I don't know why, but the tough questions/wrong answers can group together and not be spread evenly through the test. It's easy to get flustered when this happens, but don't. Keep a cool head and focus on each question by itself, confident that this is not a trend but rather a blip that a lot of people experience.

Here's the step by step process I use to create a SANS index prior to taking an exam:
Kevin's way of making a SANS index

The GSE Lab:

#1. Know the material inside and out
This one's easy. After all the work you've done to study for the multiple-choice exams and index the material, you'll have a really good handle on it. You can spend your time on the activities below to practice and tune your abilities to use the tools and apply the knowledge hands-on.

#2. Be comfortable working in Linux and Windows
Be able to boot and navigate around in the live Linux CDs provided by SANS and listed on the GSE page. Be familiar with the configuration files and options in Linux, common utilities and commands, and logfile locations and contents. Know how to read, write, edit, and manipulate files using common text editors and other OS commands. Again, many people have put together good references of common Linux commands; if you don't feel strong in this area, look for them on Google.

#3. Prepare to demonstrate your knowledge of hacker techniques
In the SANS courses, the hacking tools and techniques are introduced one at a time, with a description of how it works. To show your understanding, you'll likely be asked to look at the tools a little differently and think like a hacker. Given different situations or scenarios and a goal, how would you achieve it? Some examples could be breaking into a webserver, hiding traffic on the network, covering tracks in logfiles, or placing and using a backdoor on a compromised host. Be sure you are able to create a planned attack, following and building on the different phases outlined in the courseware. What tools work best in different situations at each phase to accomplish the goal?
Be sure you are well practiced at using the hacker tools highlighted in the courseware. Key ones to know will be tools used in the labs and tools available on the live CDs described on the GSE page. You should be able to set yourself a goal and use the tool to achieve it without referring to your courseware or following a lab step by step. Get some practice using the help documents, saving your output from the different tools, and interpreting your results. In addition to the courseware labs, there are a lot of good YouTube and similar videos available on the internet demonstrating use of the tools.

#4. Prepare to demonstrate your incident handling abilities
Much of the GSE is focused on demonstrating your adeptness with the technology, but you will also need to show your ability to be thorough and methodical in your approach to handling an incident. Be able to walk through the response to an incident following the process laid out in the SEC 504 courseware (Hacker Techniques, Exploits, and Incident Handling). What activities are appropriate

at each step for different incident scenarios? Just like in the real world, you'll need to be able to document your response activities in an accurate, clear, and concise manner.
You'll also need to be able to demonstrate your knowledge of best practices. Given an incident, what technology or practices would have prevented it, what changes should be made to prevent a recurrence?

#5. Prepare to demonstrate your intrusion detection abilities
This is another key area where you'll need to be able to integrate and apply the knowledge from the different GSE domains. You need to be able to configure and run traffic capture and analysis tools like Wireshark, Tcpdump, and Snort. You need to be able to generate, filter, and interpret output. You need to be able to recognize and interpret output from different sources, like Windows Event Logs, Linux log files, Snort IDS alerts, and Cisco router and firewall events.

When I talk about interpreting output, you should be able to look at a series of packets in a capture or a series of events in a log and recreate in your mind the scenario that created the information. What ports and protocols are being used? What can we learn from the source and destination addresses and other protocol header information? What can be deduced from the timestamps? What was the purpose or intent of the traffic, what program or tool may have been used to create it? Is this normal traffic or something malicious?

It can help to get some practice looking at normal and abnormal traffic. If you have the ability and permission to sniff and review logs on a healthy, trusted network you can get familiar with normal traffic patterns and events, and more quickly ignore them when searching through captures and logs that you may be provided during the GSE. There are downloads available on the internet of captures taken during different hacking competitions that you can also review to practice looking at malicious traffic. A good place to start could be a Google search for defcon packet capture torrent or something similar.

Apart from packet captures, how would you go about analyzing a potentially compromised system? What key things would you look at or look for on a windows box and a Linux box? What tools would you use or what commands would you run to analyze the system?

Conclusion:

I hope you have found this information to be helpful. For details about the GSE, you should review the information provided by GIAC about the GSE.