A Guide to Preparing for the GSM Capstone Exam

by: Courtney Imbert, courtneyimbert@gmail.com

Last update: November 11, 2015

An Overview of the GSM Capstone Exam

The GSM (GIAC Security Manager) is the capstone exam MSISM candidates take toward the end of their curriculum.

The two-day exam is a proctored, lab-based exam that is taken live at a SANS event. Practical exams like this one are designed to test the real-world performance of candidates. During this exam, you'll balance organizational needs with secure practices, apply standards-based approaches to information security risk management, and devise incident response strategies.

The GSM tests on the following knowledge areas, broken down throughout this guide:

- Common Information Security Technical Concepts
- Security Policy Development
- Web Application Vulnerability Scanning
- Incident Handling
- Risk Management
- Project Management
- Communication
- Auditing & Assessment

Each section of this guide includes suggested activities for practicing for the lab.

General Strategies for GSM Success

Review Courseware and Labs

The GSM is based on the core MSISM curriculum, including these courses.

- ISM 5000: Research and Communications Methods (SANS class MGT305)
- ISM 5100: Enterprise Information Security (SANS class MGT 512, GIAC GSLC)
- ISM 5200: Hacking Techniques and Incident Response (SANS class SEC504, GIAC GCIH)
- ISM 5300: Building Security Awareness (SANS class 433)
- ISM 5400: IT Security Planning, Policy, and Leadership (SANS class MGT 514)
- ISM 5600: Law of Data Security and Investigations (SANS class LEG523, GIAC GLEG)
- ISM 5800: IT Security Project Management (SANS class MGT525, GIAC GCPM)
- ISM 6000: Standards Based Implementation of Security (SANS class SEC566, GIAC GCC)

- ISM 6200: Auditing Networks, Perimeters and Systems (SANS class AUD507, GIAC GSNA)

Therefore, reviewing the courseware is a critical step in preparing for the capstone. A well-prepared candidate is one who can complete the labs in these courses with minimal guidance, and understands each step.

Connect with other information security professionals

Other information security professionals, particularly students in the MSISM program, can be a helpful resource when preparing for the exam. Others can recommend preparation strategies, provide insight or experience, and act as partners in accountability or goal-setting.

If you've received over a 90% on a GIAC exam, you are eligible to participate in the GIAC Advisory Board. This email-based forum often discusses real-world situations, with advice and ideas from experienced information security practitioners. The SANS Technology Institute also has an email forum open to students and faculty at sti-edu@lists.sans.org .

Several member-run forums are dedicated to helping students through SANS classes and exams, including an SANS STI student/alumni group (sans-sti-students@googlegroups.com) and a GIAC exam study group (giac-study@googlegroups.com). Though these groups are "unofficial" and not moderated by SANS/GIAC or STI, the archives and email discussions can provide valuable resources to students preparing for an exam.

In addition to online groups, you may find it helpful to join a local career networking group focused on Information Security or management, like the Information Systems Security Association (ISSA), ISACA, PMI, or Infragard. These organizations often schedule local meetings, presentations, or classes that help members meet other professionals in the same field.

Take Advantage of Opportunities at Work

The lab-based capstone is based on a wide variety of skills, guaranteeing the successful candidate is well-rounded. Most candidates do not have the opportunity to perform all these tasks on a day-to-day basis.

Seek out opportunities in your work environment to practice the skills you'll need on the lab exam. For example, if you have the opportunity to volunteer for a project and gain visibility into the project management process, take it! Request a cross-training session with a member of your team who performs technical tasks. Since the exam is designed to test real-world skills, on-the-job experience can provide valuable training and practice.

Play Netwars or another interactive scenario-based simulation

There are plenty of "Capture the Flag" events online for information security professionals. These can help you become comfortable working in unfamiliar or time-pressured environments. They also provide data or services to practice on using information security tools and technical skills. Though many of these events are competitive, they provide opportunities for learning new skills, practicing weak areas, and networking with other players.

Netwars is a multi-level event that can be completed at a SANS conference or at home. Information is available at https://www.sans.org/netwars.

Common Information Security Technical Concepts

This knowledge area is designed to test the candidate's ability to use Unix and Windows system tools to review the system's configuration and tasks. In order to succeed at this section, you'll also need to understand how to use a basic network sniffer and scanner, understand basic networking, encryption techniques, technologies, and applications, including hashing, signing, decrypting, and managing keys.

Download a Linux distribution, and learn to navigate the system and run basic commands.

Virtualized environments make it easy to practice tasks on a variety of operating systems. There are several options for virtualization software, but VMware is a popular option supported by most SANS classes. A free version, VMware Workstation Player, is available at http://www.vmware.com/products/player/. This version has the ability to "play" pre-created virtual machines and tweak configuration. To create virtual machines from scratch or use more advanced features like snapshots, a VMware Workstation license is required. Other virtual machine applications include Oracle's VM VirtualBox (https://www.virtualbox.org/), Windows Virtual PC, and QEMU (http://wiki.qemu.org/Main_Page).

You may already have pre-configured virtual machines saved from your SANS classes. You can copy and use these to run through the class exercises, or practice navigating through the system.

If you'd prefer to practice on a new virtual machine, you can download pre-configured Linux VMs from reputable sites. Many information security professionals work with Kali Linux, an Offensive Security Linux distribution that comes with many common security tools. You can download Kali at https://www.kali.org/downloads/ . There are images pre-configured for virtual environments, like VMware player or VirtualBox, available at https://www.offensive-security.com/kali-linux-vmware-arm-image-download/ .

Windows virtual machines require a license if they are used beyond an initial 30 days, similar to Windows installed on a physical machine. You may choose to use a new Windows license to create or activate a virtual machine, or use the Windows host itself for practice.

One advantage of using virtual machines is that the networking is also virtual, making it simple to connect VMs together! For example, VMware permits you to create a *host-based network*, with names like VMnet0. Though a host-based network is safely isolated from the Internet, the host and any running VMs on the same host-based network can "talk" to each other. This creates the ability to ping, transfer files, and run security scans or other tasks with low risk. To find out more about basic networking in VMware, read http://www.vmware.com/support/ws55/doc/ws_net.html .

Once you've designated both a Linux and a Windows machine for exam preparation, practice on them. You may want to begin by running through the labs in the courses you've taken, practicing simple network configuration and finding common security settings on the machines. Change the IP address and see if you can get a Windows and Linux VM to "talk" to one another, both through IP addresses and computer or domain names. Move files back and forth using SCP or other tools. As you become comfortable with basic security tasks, you can practice performing a security audit on the systems, verifying results, and making and executing a remediation plan.

Prepare Printed Resources for the Lab

According to the GSM policy, you are permitted to take written or printed materials into the exam with you. Since the exam is timed, it may be difficult to find the resources you need in hundreds of pages of courseware. It is a good idea to prepare "cheat sheets" or other printed resources for quick reference. You may find it helpful to create your own printed resources or templates as you study, with common tasks and examples.

Security Policy Development

In the Security Policy Development section of the GSM, you are expected to be familiar with the development, review, and implementation of information security policies. You should be able to align the policies with information security best practices, the resources available to you, and the overall goals of an organization.

Read and Revise Sample Policies

SANS provides a library of information security templates to the community, available at https://www.sans.org/security-resources/policies/ . These policies were developed by seasoned practitioners, but they must be customized to any organization. Download a few

policies. Create a checklist of components you would expect the policies to include, like enforcement measures and a revision / change management history. Next, review the policies with a critical eye, and list the revisions you would make for them to fit into your organization. Would these policies need to be revised to align with organizational goals, resources, pre-existing policies, and other environmental factors?

Web Application Vulnerability Scanning

During the GSM lab, you'll be expected to understand common web application flaws and vulnerabilities, recognize and verify them either with or without automated tools, and recommend mitigating controls for those flaws.

Read the OWASP Top 10

The OWASP Top 10 (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project) is a commonly-used compendium of the most common and critical web application security flaws. The documents are designed to be understandable for managers as well as technical staff, with examples of attack scenarios and recommendations for mitigating controls.

Practice using web application scanning tools

There are several deliberately vulnerable web applications available, both hosted online and downloadable as virtual machines. These are web applications designed for training and demonstrations by security practitioners. Though there are too many to list here, here are a few well-maintained, reputable ones:

- OWASP Broken Web Application
  https://www.owasp.org/index.php/OWASP_Broken_Web_Applications_Project
- Damn Vulnerable Web Application
  http://www.dvwa.co.uk/
- Gruyere
  http://google-gruyere.appspot.com/

There are also "Hack this site" websites, but these are controlled and hosted by external parties, and may focus primarily on penetration testing competition rather than training.

It is important that you scan *only* those websites you have explicit permission to test - either by starting your own virtual machine that hosts the web application locally, or with the express permission of the site. Once you have a designated practice site, practice finding and verifying vulnerabilities. This should be done both manually (by entering a SQL injection test into a field, for example) and with common web vulnerability scanning tools.

Auditing and Assessment

During the GSM, you'll be expected to perform an audit or assessment of network devices using common automated tools, review the assessment and audit results, and recommend actions based on the results of the audit.

Practice a simulated audit on your home network

Unfortunately, it can be a bit difficult to create a realistic network environment to practice the auditing process at home. However, you can step through a small-scope audit using the tools listed in your AUD507 workbook against your home network configuration, or virtualized network devices. As a bonus, by remediating the issues you uncover through your audit, you may end up with a more secure home network!

Incident Handling, Risk & Project Management

In the Incident Handling section of the GSM, you will be expected to understand incident handling phases and best practices, and recommend both short- and long-term actions in response to an incident. In addition, you will be expected to produce project-related documents such as a project charter, requirements, and scope, using the PMI framework. For risk management, you will be expected to assess and explain organizational risk, and prioritize projects or actions based on that risk. You should be familiar with special information security risks for industries like healthcare, finance, and government.

Read Case Studies and News Stories of Incidents

It may be helpful to become familiar with the types of information security incidents organizations encounter, and how they react both short- and long-term to these incidents. Participating in the remediation of incidents at work is great practice! If you don't have access to this information at work, it may help to seek out information about current incidents, and compare that information with the six phases of the incident handling process. Occasionally, case studies appear in the SANS reading room (https://www.sans.org/reading-room) or in blog posts of the Internet Storm Center (https://isc.sans.edu), as well as many information security blogs and news sites like Krebs on Security (http://www.krebsonsecurity.com/). Since organizations often hesitate to release details until the post-mortem of an incident, you may want to research information security incidents that occurred several months ago. Reading about incident response with a critical eye will help you become familiar with typical incidents and possible ways to respond to them.

One valuable exercise is to select a breach and discuss it with coworkers or a study group. Brainstorm for actions that would have mitigated the threat, or detected the attack.

Do a "Dry Run" of an Incident

Many organizations practice their incident response procedures with drills or live tests. If your work doesn't do incident response drills or permit you to observe them, you can practice for the exam by stepping through the phases of an incident on your own or with a study group. Select a common incident from the news stories you've read. Here are some sample scenarios:

- A large amount of proprietary or PII data has been published online
- Hardware has been stolen from an office
- A virus outbreak affecting an entire department
- A disgruntled employee has sabotaged important data

Consider the six phases of the incident process for your scenario: what would you do? What additional information would you need, and how would you get it? What risks are associated with the incident, and do you suspect any regulatory or legal requirements might come into play? Finally, practice writing communication summarizing the incident and recommending next steps for both technical and management audiences.

In addition to simulating an incident yourself, you may have the opportunity to observe an incident response team in action. In the USA, most counties or states have an Emergency Management Agency (EMA). Some EMAs schedule regular simulated tabletop disaster scenarios, and many will allow the public to observe. Although the scenario is not necessarily an information security incident, it can be helpful to observe the management strategies, processes, and teamwork that an experienced team uses to handle incidents.

Organizational Communication

During the GSM, you will be expected to write clearly to a target audience from a set of complex information, and create an executive summary for an incident, project, or situation.

Practice targeting and summarizing communication

Whatever your role at work, there are many real-world opportunities to improve on your communication skills. Practice taking notes at meetings or during a work session to collect the most important points, then create an executive summary. You can also use projects you're working on, complex technical problems, or incidents to practice your written communication skills. Be sure your communication is accurate, but understandable. For more in-depth practice, imagine you must send three memos on the same subject: one to an executive team, one to

your organization's customers, and the other to the technical team assigned to work on the problem. Develop the memos in tandem to practice targeting important points and the style of communication to specific audiences.

Get feedback from others

Often, the text we've written seems clear to us, but may be confusing from another perspective. As you practice your writing, ask trusted partners to read and critique it for clarity, targeted communication, and grammar or spelling.

Questions?

The SANS Technology Institute and GIAC teams are here to help you! If you have questions about the capstone itself, preparing for it, or the MSISM curriculum, email info@sans.edu or info@giac.org .