Five Steps to Security+ Certification Success

By: Pierre J. Askmo

NOTE: This report is not aimed at teaching you the subject knowledge to pass the exam. This is a paper about exam structure, pass scores, question structure and type, as well as what you can expect from succeeding at the Security+ exam.

REPORT SPONSORED BY: CertBlaster®

be ready!

www.certblaster.com/Security+

CONTENTS

Bonus section:

How the exam is made and why you should care

Industry representatives from the leading computer vendors set the Exam Objectives. This means that, based on, their day to day needs, they define which skills the exam should address. In this phase of the exam definition the industry representatives also decide what areas to prioritize over others. They do that by assigning different weights to the different Exam Objectives (more on this later). Once these areas of expertise have been established by the industry representatives the next step is to write exam questions within those areas of expertise. This is done by Subject Matter Experts – SMEs. These are experts in the various computer fields that know which questions will help reveal if a candidate knows the topics covered by the Exam Objectives. There are a few more steps but I am not going to bore you with the details. Here's your take home from this though; the exam objectives are subject to interpretation. Why? Because when the exam objectives are handed over by the industry representatives the SMEs read in to these what *they* see. Now, most of the time it's what you and I would expect. However there will be cases where there is a difference of views. This means that you have to read the objectives very carefully and make sure you understand each of them. Don't interpret them too narrowly since the process does leave the SMEs with room for interpretation.

How the exam is configured

To become Security+ Certified you need to pass Exam SY0-401. This credential has the following recommended but not mandatory prerequisites for the IT security professional:

A. A minimum of 2 years' experience in IT administration with a focus on security
B. Day to day technical information security experience
C. Broad knowledge of security concerns and implementation including the topics in the domain list below

The Security+ Certification, like all CompTIA exams, is organized around its list of Exam Objectives that are published on their website. These Exam Objectives consist of a handful of "Main Domains" (the high level topic definition) and under each of the Main Domains, "Sub-Objectives" that narrow down to the specifics of what you should know in preparation of the exam. Here are the Exam main domains for with their relative weights:

Security+ Exam SY0-401

Domain	**Percentage of Examination**
1.0 Network Security	20%
2.0 Compliance and Operational Security	18%
3.0 Threats and Vulnerabilities	20%
4.0 Application, Data and Host Security	15%
5.0 Access Control and Identity Management	15%
6.0 Cryptography	12%
Total	100%

This table shows the main Exam Objectives (Domains) and how much weight they each should have on the exam. Why do the relative weights matter? Because they give a good indication of how many questions each domain will present at your exam.

How many questions are there and how are they distributed?

The exam consists of 90 questions and you have an hour and a half to answer them so on average a little under one minute per question. This is in line with certification best practices for multiple choice based tests but it will require you to get organized and focused to not run out of time. Thankfully there are methods and tools available to you to make sure you don't get overwhelmed by the quantity of questions. For that see our article "Test Taking Strategies for IT Certification"

Security+ Exam SY0-401

Domain	**Approximate# of questions**
1.0 Network Security	18
2.0 Compliance and Operational Security	16
3.0 Threats and Vulnerabilities	18
4.0 Application, Data and Host Security	13
5.0 Access Control and Identity Management	13
6.0 Cryptography	12
Total	90 questions

On CompTIA's Exam Objectives document you can read:

***Note: The lists of examples provided in bulleted format below each objective are not exhaustive lists. Other examples of technologies, processes or tasks pertaining to each objective may also be included on the exam although not listed or covered in this objectives document.*

This is the kind of statement you want to take seriously. It will require you not only to master the terms on the various lists but what they can do and different ways they can do it. This can be tricky but should impact how you study for the exam.

What is the passing score in plain English?

The grading scale is a bit funky as you are evaluated on a scale from 100 to 900. The passing score on the CompTIA Security+ SY0-401 exam is 750. What this works out to in terms of percentages is a score of about 90%. This means that with a total of 90 questions per exam you will need at least 80 correct answers. Because the objectives are so wide ranging and unless you have a lot of professional experience, it will take a fair amount of work to prepare for this exam. If you doubt this just take a look the Security+ objectives as published by CompTIA: You are looking at 23 pages mainly of lists of items you could get a question on…

The question types you will see on the exam

By and large the most common question type is the multiple choice type of questions. The basic four alternatives – three detractors and one correct choice is the most common question type on the exam. Typically these questions will include one correct answer, one detractor that is very similar to the correct answer and a different detractor that is still wrong and finally the nonsense detractors. The nonsense detractor is the one a candidate with no idea about the topic at hand could pick. In some of these you will be facing more than one alternative that you will feel is correct, in those situations you are expected to pick the "best" answer. By that CompTIA means the alternative that is the more direct and clearly related to the question as asked.

When you are facing the four alternatives – three detractors and one correct choice, you will see that the clickable area is a radio button. When you see a question that has check boxes instead of radio buttons, that will be a multiple choice – multiple answer type question. With these questions you can expect that five alternatives will contain two correct answers and six alternatives will contain three correct answers.

Typical multiple choice single answer format:

Which of the following network devices allows for full-duplex communication?

a) Hub
b) Bridge
c) Switch
d) Firewall

In addition to the multiple choice questions you will see two more question formats: Scenario based and Performance based questions.

The scenario based questions are essentially multiple choice questions just with a longer question text.

The scenario based question sets up a situation that you are expected to respond to by choosing one of the alternatives. Here is an example of that:

A network administrator just finished removing spyware from a computer and now they are not able to connect to any websites. Which of the following is the MOST likely cause?

a) Automatic configuration
b) Network card driver is damaged
c) Proxy settings
d) The Internet is not functioning

Because these are CompTIA exams the scenario is a "scenario of few words"… CompTIA is known for its short and terse questions.

So what is the answer? The most likely answer here would be c) Proxy Settings. Malware often reconfigures proxy settings, or in some cases initiates them, to enable their programs to operate optimally. Often this could go unnoticed by the user and the program will run indefinitely undetected. Proxy settings is the MOST likely answer because you are told in the question that "A technician just finished removing spyware". Although in b) a damaged network card driver would cause inability to connect to the network it is not induced by malware removers and so does not qualify for the MOST likely cause. a) Automatic configuration will not disable internet connectivity by design as it is non-routable. Finally, d) if the Internet was not functioning in the workplace it's safe to assume yours would not be the only complaint!

As opposed to A+ and Network+ certification, the Security+ exam often asks questions that have no direct relationship with computing and everything to do with criminal investigative techniques. That is why having a lot of computing and networking experience does not guarantee you'll do well on the Security+ exam. You need to prepare thoroughly for the criminal side of Security+. This is an example of those types of questions:

Below is a list of the six steps taken for damage control at a crime scene. Order these from the most urgent step on top and the remaining steps in decreasing order of urgency.

Secure physical security features.

Neutralize the suspected perpetrator from harming others (*if applicable*).

Contact the response team.

Report the incident to security or the police.

Confront any suspects (*if applicable*).

Quarantine electronic equipment.

When an illegal or unauthorized incident occurs that involves a computer or other electronic device that contains digital evidence, it is critical that action be taken immediately. When it comes to securing a crime scene, a delay of even just a few minutes can allow the digital evidence to become contaminated by other users or give a perpetrator time to destroy it. When such an event occurs, it is incumbent on those individuals in the immediate vicinity to apply best practices for damage control in order to minimize any loss of evidence.

The correct answer/order is as below:

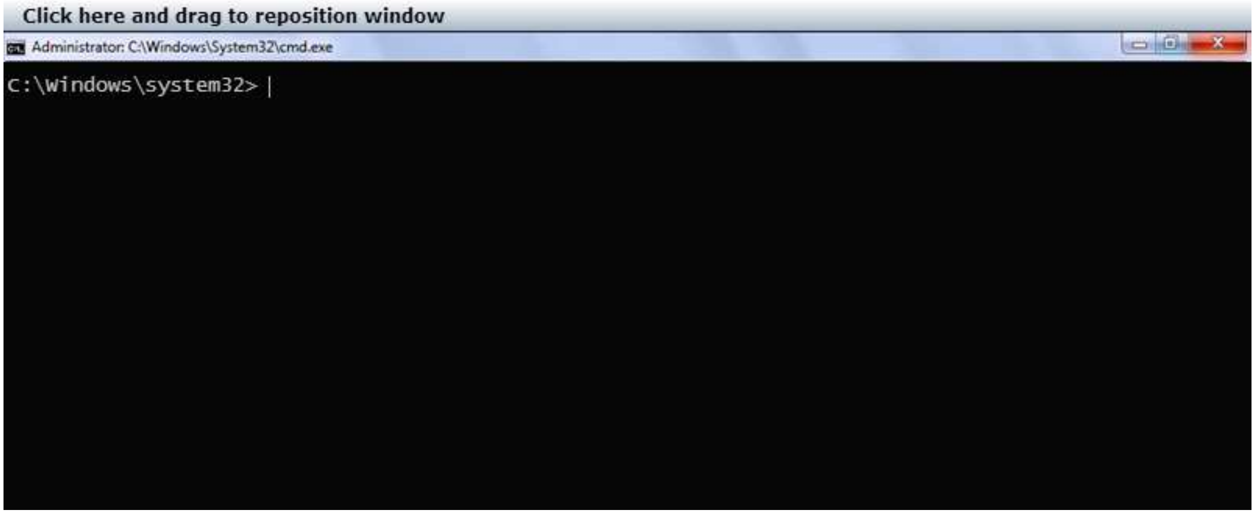
1. Report the incident to security or the police.
2. Confront any suspects (*if the situation allows*).
3. Neutralize the suspected perpetrator from harming others (*if necessary*).
4. Secure physical security features.
5. Quarantine electronic equipment.
6. Contact the response team.

IMPORTANT NOTE ON SCENARIO BASED QUESTIONS: There is a potential for fair amount of scenario based questions in Exam SY0-401. You get that from studying the CompTIA Exam Objectives documents. The exam objectives for Exam SY0-401 lists 11 objectives starting with "Given a scenario…" This is significant and no Main Domain (the high level objectives) is free from these. To get the CompTIA Exam Objectives documents click on Security+ Exam Objectives.

Performance Based Questions

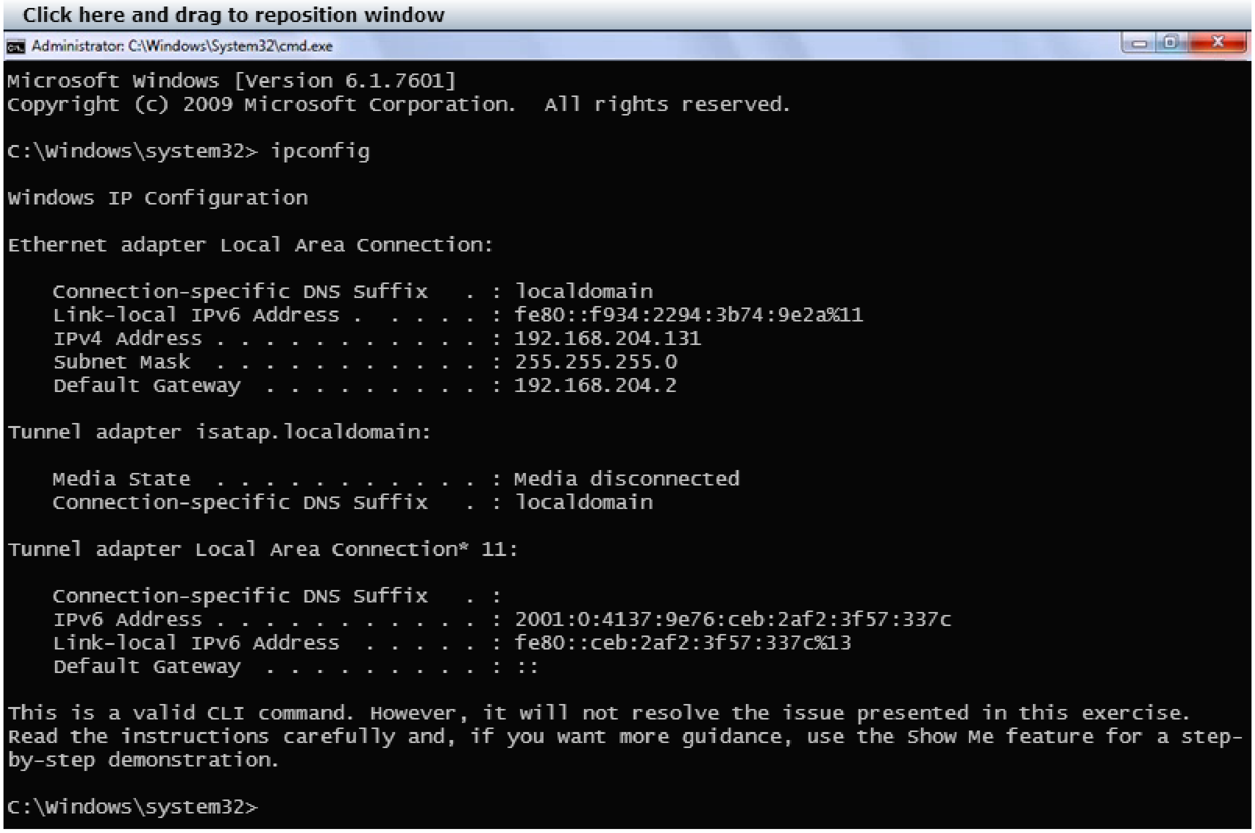
The performance based questions are exercise based. You complete a task in a Windows simulator or a command line interface simulator and you come to the correct answer through entering the right command or navigating correctly in the Windows menu. Here is an example of a performance based question:

What is the IPv4 address on this machine?


Click here and drag to reposition window
Administrator: C:\Windows\System32\cmd.exe

```
C:\Windows\system32> |
```

This question is testing your knowledge of the TCP/IP utilities and the associated commands. For you to answer this question you have to know that IPCONFIG is the command that will reveal the IP address.


Click here and drag to reposition window
Administrator: C:\Windows\System32\cmd.exe

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32> ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::f934:2294:3b74:9e2a%11
   IPv4 Address . . . . . . . . . . . : 192.168.204.131
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.204.2

Tunnel adapter isatap.localdomain:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : localdomain

Tunnel adapter Local Area Connection* 11:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:4137:9e76:ceb:2af2:3f57:337c
   Link-local IPv6 Address . . . . . : fe80::ceb:2af2:3f57:337c%13
   Default Gateway . . . . . . . . . : ::

This is a valid CLI command. However, it will not resolve the issue presented in this exercise.
Read the instructions carefully and, if you want more guidance, use the Show Me feature for a step-
by-step demonstration.

C:\Windows\system32>
```

After entering ipconfig you can see that the IPv4 address is: 192.168.204.131.

BONUS SECTION

What's so special about Security+ Certification?

Security+ Certification was the first vendor neutral cyber security certification to gain any traction in the market place. This is important and, till this day still relevant, as it ensures that if you pass, you get a credential that is recognized and wanted by the whole computing industry - not just one vendor. Security+ is also a "gateway certification". It is a great stepping stone to further certification such as CompTIA Advanced Security Practitioner (CASP) or towards the Certified Information Systems Security Professional (CISSP) among others.

Being one of the leading IT certifications for IT security professionals, with over 200,000 certified individuals Security+ sets the standard for both the profession and other certification developers.

The bottom line is that Security+ has credibility and that's all you really want and need from a credential.

Practicalities at the Testing Center

You can make your appointment for the Security+ exam at https://home.pearsonvue.com/.

On exam day you will be asked for two forms of ID bearing your signature, one of which must include your picture. After your identity has been confirmed you will fill out some paperwork. General information. Then you will be asked to sit for a mugshot which becomes part of your grading summary so look sharp!

Good luck!

REPORT SPONSORED BY: CertBlaster®

be ready!

www.certblaster.com/Security+