GCWN Exam Tips

The **GIAC Certified Windows Security Administrator (GCWN)** certification exam tests security professionals on their ability to secure Microsoft Windows clients and servers with PowerShell in an Active Directory environment.

For the latest information about the GCWN exam, testing facilities and exam contents, please visit **https://www.giac.org/GCWN**.

Purpose

How can you more easily prove your specific expertise in Windows security to others? How can employers identify qualified candidates for hire in Windows environments where security skills are required? The GCWN exam tests practical, real-world skills needed to secure Windows using PowerShell.

Exam Content and Tips

The six-day Securing Windows course (SEC505) covers all of the material that is tested on the GCWN exam. No further study guides or outside materials need to be purchased. If the instructor mentions something verbally, and that tool or topic mentioned is not in any of the the manuals, then that tool or topic is not on the exam. All GCWN questions come from the manuals, not the lecture.

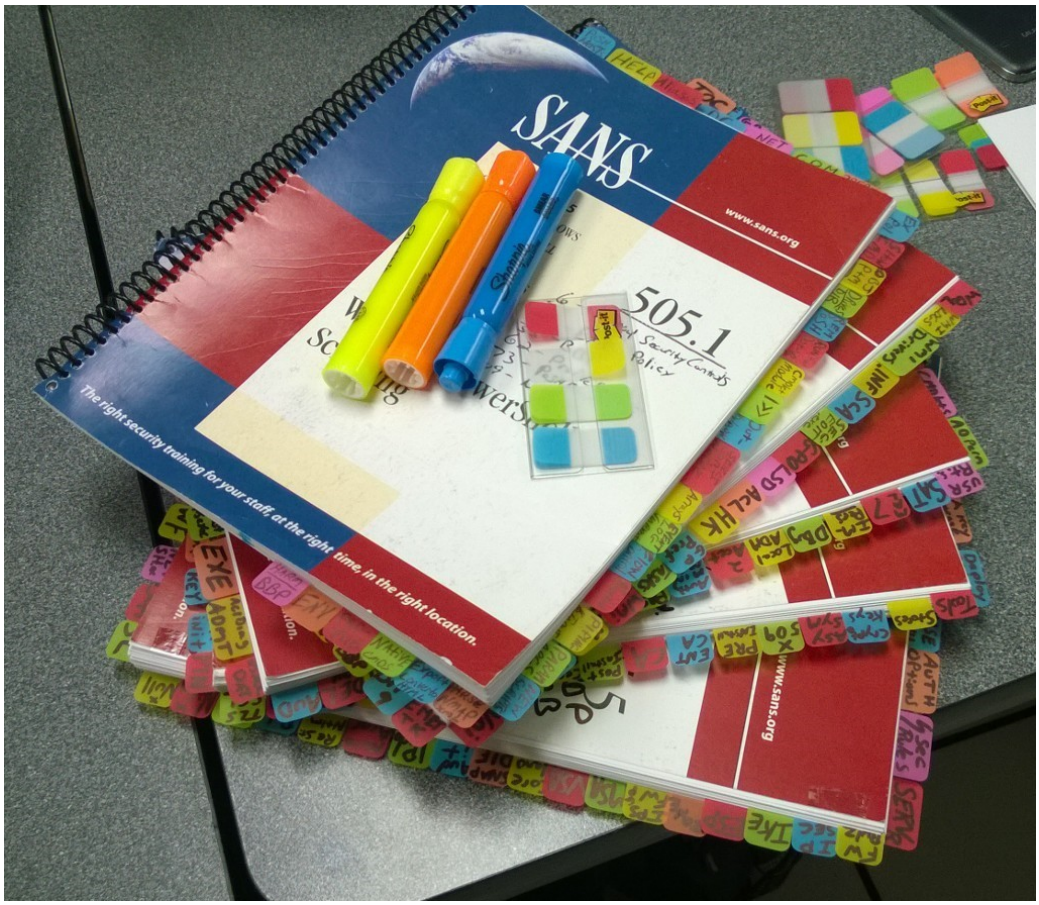
On the www.giac.org website, check the current minimum passing score and the current time limit for the exam. These can change as course topics change.

The exam is open book. You may have the entire set of SEC505 manuals beside you when you take the exam, including any highlighting, handwritten notes or tabs that you wish to add to the manuals. Don't forget that the appendices are testable too.

Purchase two or more colors of highlighters. Use different colors for different meanings, e.g., blue for new keywords, orange for difficult topics to review the night before the exam, yellow for the essential two or three points in each paragraph, and so on. The patterns of colors on each page can help you to remember where particular tools, topics or keywords are discussed.

When highlighting, ask yourself, "Does this look like a good exam question topic? Is this something I would put in the exam were I a GIAC exam writer?" If yes, then highlight *that*. The people who write the exam questions are IT people just like you.

Add tabs to your manuals with PostIt Notes or tape which labels the major sections and tools so that you can quickly turn to those topics again during the exam. Remember too that every manual has a table of contents at the front with slide titles and page numbers. Some of these lines can be highlighted too.



Keep in mind that the manuals are *much* more detailed than the exam questions themselves, e.g., the manuals list KB article numbers, obscure command-line switches, the date of important events in Windows or PowerShell history, and other items which are far too specific to ask on an exam. (Don't panic!)

The exam is timed. During the exam, do not get bogged down on one question. Skip questions about which you are unsure of your answer and move on to the next question. You will be able to return to skipped questions at the end. A later question might jog your memory for the answer to a previous skipped question. At the very end, with only a few minutes remaining on the exam, if you have to guess the answer to a question, stick with your first guess, don't double-doubt your instincts.

Do not invest too much time creating an index. Most attendees are probably better off not creating an index at all. Focus on the table of contents at the front of each manual and your own sticky tabs with keywords. The more time you spend trying to create an exhaustive index, the less time you will have reviewing the manuals and labs.

After taking the course, read the manuals cover-to-cover, including the appendices, and do the labs again. Have fun playing around and experimenting while doing the labs. The labs are designed to spark your interest in possibilities. The labs are more like cheat sheets rather than step-by-step recipies for robotic application in real life. Having fun while experimenting takes more time, but it can help you to recharge your mental batteries and improve overall memorization.

Do not take the practice exams until after you have read all the manuals. The purpose of a practice exam is not to learn new material, but to identify areas of weakness. After taking the first practice exam, study your area(s) of weakness before taking the next practice exam. Repeat.

Do not stay up late the night before the exam while drinking caffeine. Your exam performance is better served by being well-rested and hydrated than whatever last few facts can be crammed in between midnight and 3:00 AM.

Sample Questions

The following questions are not on the exam, but they indicate the *types* of questions and security topics you might find on it.

When trying out these sample questions, see if the tabs and highlighting in your manuals would have helped you.

Which of the following command-line tools can be used to manage permissions in the Active Directory database?

A) repadmin.exe
B) dsacls.exe
C) ldifde.exe
D) ntdsutil.exe

Answer: B

What is the minimum operating system version necessary to enable Active Directory change auditing, i.e., the logging of pre- and post-change values?

A) Windows Server 2008
B) Windows Server 2008-R2
C) Windows Server 2012
D) Windows Server 2016

Answer: A

How many PowerShell profile scripts exist on the hard drive by default?

A) 4
B) 3
C) 2
D) 1
E) 0

Answer: E

AppLocker is best described as a technology to achieve what purpose?

A) Lock down the registry settings of Microsoft applications.
B) Lock down the registry settings of third-party applications.
C) Store usernames, passwords and credit card numbers safely.
D) None of the above.

Answer: D

```
What protocol(s) may be used to access the Windows Management
Instrumentation (WMI) service over the network on Windows 10?

A) WSMAN
B) RPC
C) WSMAN and RPC
D) LDAP
E) The WMI service cannot be accessed over the network.

Answer: C
```

```
What is the easiest way to remove digital certificates from users'
computers when those certificates are revoked by the PKI admins?

A) Group Policy.
B) The removal must be performed manually by a local administrator.
C) With a PowerShell logon script and the wmic.exe utility.
D) Enable archived private key auto-deletion at the CA.

Answer: A
```

```
Which of the following authentication protocols are supported by the
built-in Windows IPsec driver?

A) Kerberos.
B) Certificate.
C) Pre-shared key.
D) All of the above.

Answer: D
```

How did you do? Don't worry, all of these questions are covered in the course, and on the exam you do not have to score 100% in order to pass.

Good Luck!