

# The GCWN Exam and Sample Questions

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

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

## Purpose

The Microsoft Certified System Engineer (MCSE) certification is widely known, but even with the security elective included, the fact is that the MCSE is not highly regarded within professional security circles. And yet there is great demand for security professionals who specialize in Windows because there are more than a billion computers around the world running Microsoft's operating systems.

How can you more easily prove your specific expertise in Windows security to others? How can employers identify qualified candidates for Windows environments where security is a must? The GCWN certification is intended to bridge this gap. The GCWN exam tests practical, real-world skills needed to secure recent versions of Windows clients and servers.

## Exam Content and Tips

The six-day Securing Windows course (SEC505) covers all of the material that is tested for GCWN exam. No further study guides or outside materials need to be purchased.

The exam is open book, so you may have the entire set of SEC505 manuals beside you when you take the exam, including any highlighting, handwritten notes or tabs you wish to add to them.

**Exam Tip:** 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.

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 and other items which are far too specific to ask on an exam.

**Exam Tip:** Highlight the keywords in each section so that you can quickly find them again when skimming the manual looking for answers. When highlighting, ask yourself, "Does this look like a good exam question topic? Is this something I would put in the exam?" *Highlight that!*

## Sample Questions

When you sign up for the GCWN exam you will later receive an e-mail with a username and password for logging onto the GIAC web site at www.giac.org (please double-check that SANS has your correct e-mail address on your course registration form).

On the giac.org web site you will have access to an exam FAQ, contact information for additional questions, and some sample GCWN exam 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 2003

B) Windows Server 2003-R2

C) Windows Server 2008

D) Windows Server 2008-R2

Answer: C

If all your DNS servers are Active Directory integrated, do you need to leave zone transfers enabled on those DNS servers in order to replicate changes to DNS records to your other AD-integrated DNS servers?

A) No, zone transfers are not needed for replication in this case.

B) Yes, even AD-integrated DNS servers use zone transfers to replicate.

C) There is no such thing as "Active Directory integrated" DNS anymore.

D) It is not possible to convert all DNS servers to Active Directory integrated mode since at least one domain controller, usually the PDC Emulator, must be a standard primary DNS server.

Answer: A

"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 Group Policy feature would be used to place a custom global group into the local Administrators group on all servers in a particular Organizational Unit?

A) AppLocker

B) Restricted Groups

C) Block Inheritance of Groups

D) Group Account Control

Answer: B

What is the best way to remove digital certificates from users' computers when those certificates are revoked?

A) Group Policy.

B) The removal must be performed manually by a local administrator.

C) With a logon script and the dsacls.exe utility.

D) Enable archived private key auto-deletion at the CA.

Answer: A

Which of the following authentication protocols are supported by the 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!*