Last updated June, 2000. Click here for updates.

Click here to see additional documents related to this study guide.

Contents

Cramsession™ for W2K Designing Security

Abstract:

This is one of the three so-called architecture exams. This exam is an optional choice. The MOC 2150 is a five-day class that was designed to help develop the skills to lay out a security framework for a small, medium and enterprise network. According to Microsoft, before taking course 2150 you should have either taken course 1560, Updating Support Skills from Windows NT 4.0 to Microsoft Windows 2000 or course 2154, Implementing and Administering Microsoft Windows 2000 Directory Services. Like most Microsoft Windows 2000 exams, the not all objectives covered in this exam are found in the courseware.

Microsoft Exam 70-220

Designing Security for a Microsoft Windows 2000 Network

- Each question on this exam will take the form of a case study. First, you will be given background information that will be provided in a graphic. These case studies graphic will then be broken down into various sections, delineated by tabs. For example, the tabs may contain things like the background of the problem, the way the organization is laid out, a statement of the problem you are facing, the way the current technical environment is laid out, and the way the technical environment will be laid out when you are finished with the project. In addition, there will be one tab that contains all the information. Be sure to read all the information, and take notes on whatever you feel may be pertinent to the questions.

Analyzing Business Requirements.

- This set of objectives and the set of objectives on Analyzing Technical Requirements may not lead to direct test questions, i.e. what company model is this enterprise using, but it will be important information to assimilate as criteria for making decisions in the scenarios.

Analyze the existing and planned business models.

- In this section, you are looking for information about the way the business is currently being operated as well as how the company may be operated in the future. You will be asked to make decisions based on this information. Again, there will not be questions asked specifically about this objective, but you need to be sensitive to the information provided.

Analyze the company model and geographical scope. Models include regional, national, international, subsidiary and branch offices.

- When you look at the company model, you are primarily looking for information on how the company will be managed and who the decision makers will be. In the real world, this can be key to the success or failure of any project. In the testing environment this section rears its head as part of the Case Study when you background information from various levels of management. The company model is important in the way you weight the information provided. For example, if the company CEO says there is a problem, that opinion carries much more weight than someone from the mailroom.

Geographical Scope	Impact
Regional	Very little impact on testing scenario.
National	Very little impact on testing scenario, except when it comes to installing and configuring Virtual Private Networks between locations.
International	Important to testing scenario because some technologies that can be used in the United States and Canada may not be used in other countries
Subsidiary	Important from a testing scenario because a subsidiary is more likely to be a "stand alone" or self-managed entity than a branch office. A subsidiary may have different impacts on the design of an active directory implementation. For example, a subsidiary may be a separate tree in the forest.
Branch Offices	Usually the impact of branch offices will be in the design of the Active Directory tree, for example you may give the branch office an Organization Unit, depending on the size of the office. May also impact decisions relating to Group Policy objects.

Analyze company processes. Processes include information flow, communication flow, services and product life cycles, and decision-making.

- As alluded to above, this objective is put here to clue you into the corporate subtleties of problem definition and long-term strategies. You should also pay attention to information flow and communication flow, especially if it tracks across different offices in different locations. This may be a key that a VPN is called for, or it may be a signal to explore how Kerberos can be used effectively.

Analyze the existing and planned organization structures. Considerations include the management model; company organization; vendor, partner and customer relationships, and acquisition plans.

- This is another one of the informational, red-flag kind of objectives. If you are reading through the case study and you see things the CEO saying that he/she wants to switch their businesses module from bricks and mortar to

point-and-click, you should key in on things like firewall layout or protection of web sites, using special protocols for e-business, or how are you going to allow a trusted partner to access certain areas of the network while not having access to other areas of the network. These are more of the red flags that you should be writing down on your notepaper so they can be addressed during the questions.

Analyze factors that influence company strategies.

- **Identify company priorities.**
- **Identify the projected growth and growth strategy.**
- **Identify the relevant laws and regulations.**
- **Identify the company's tolerance for risk.**
- **Identify the total cost of operations.**

- This is another informational red-flag objective. In this objective, the things to key on in the case study are how is the company planning on growing? If the company is planning on going on an acquisition binge, you may get a tree design question that will need to take that information into consideration. From a security perspective, the things to feature will be if any information is crossing International boundaries. If it is, there are certain technologies that may not be appropriate due to treaty restrictions.
- Other things to key in on include the company's tolerance to risk. The solutions that may be put in place for a small company may not be sufficient for a larger company that is jumping on the e-business bandwagon. You should also be able to make the jump between the company's tolerance for risk and the total cost of operations. For example, a corporate executive may decide that a particular security solution may not be appropriate after seeing what the impact is on the cost of operation. The security solution may cost more than the information or resource is worth to the company.
- This objective tests your ability to prioritize projects and solutions.

Analyze business and security requirements of the end user.

- This is another informational red-flag objective. For this objective, make note of any special use situations, or decide if there are ways Group Policy Objects can be used to standardize security.

Analyze the structure of IT management. Considerations include type of administration such as centralized or decentralized; funding model; outsourcing; decision making process, change management process.

- The Windows 2000 IT management model calls for decentralized management wherever possible. Here are you looking for ways to create security groups based on job function or workgroup. Once this has been

accomplished, you can then assign ownership and management of that security group to someone in the group, giving them the ability to control the group.

Analyze the current physical model and information security model.

Analyze internal and external risks

- To provide solutions that will map to this objectives, you need to be on the lookout for areas where a site may be defined. You can create sites by defining a group of subnets connected by a high speed, reliable connection. The network administrator determines what is a high-speed reliable connection. Knowing when to create sites will assist you later where you design and implement Group Policy Objects. GPO's can be assigned at the domain, organizational unit or site level.

Analyze Technical Requirements.

- Here, again, this entire group of objectives can be described as for your information. These objectives are based on project management of a large rollout. You need the information contained here to make the decisions necessary to plan security.

Evaluate the company's existing and planned technical environment.

- **Analyze company size and user and resource distribution.**
- **Assess the available connectivity between the geographic location of work sites and remote sites.**
- **Assess the net available bandwidth.**
- **Analyze performance requirements.**
- **Analyze the method of accessing data and systems.**
- **Analyze network roles and responsibilities. Roles include administrative, user, service, resource ownership and application**

The things to key in on for these objectives are things like:

- Is there a natural distribution of users and resources that would lead to the placement of a domain, organizational unit or site?
- Is there the high-speed reliable connection that would give the ability to create a site?
- Is there the connectivity that would make it possible to create a virtual private network?

- Is there anything special about the ways the users are accessing data or systems that will have to be taken into consideration when the security plan is in place?
- Are there the personnel available to handle the management of the security plan you may want to put in place?

Analyze the impact of the security design on the existing and planned technical environment.

  - **Assess existing systems and applications.**
  - **Identify existing and planned upgrades and rollouts.**
  - **Analyze technical support structure.**
  - **Analyze existing and planned network and systems management.**

- Here again, you are going through the case studies, analyzing ways that you can put known security tools to use. For example, in this objective, be on the lookout for questions that may relate to the upgrade or rollout of applications. In other words, how can you use the Windows 2000 security tools to guarantee that the rollout or upgrade of an application will be using the real software? As you will see in a later objective, you can use Authenticode to insure that the users are getting what you want them to get.

Analyzing Security Requirements.

- We are getting closer to the real meat of the test, honest! There is still just one more set of objectives that will act as red flags for information to pay attention to in the case study. Once we get by these, you will be actually looking at some Windows 2000 security technology.

Design a security baseline for a Windows 2000 network that includes domain controllers, operations masters, application servers, file and print servers, RAS servers, desktop computers, portable computers and kiosks.

Identify the required level of security for each resource. Resources include printers, files, shares, Internet access and dial in access.

- So, what kinds of red flags are you looking for here? First of all, there are all sorts of things that may have security implementations. For example, there are RAS servers, dial in access and portable computers. RAS servers and dial in access can be wonderful things, but they can also cause a security concern if they are improperly placed. If you see mention of portable computers in the case study, be alert for mention of the Encapsulating File System (EFS). Much of the Windows 2000 documentation stresses the way EFS can protect a company against the loss of data due to the loss or theft of a laptop computer.

- Internet access is another area where you should pay close attention to the case study. In this case, the design issue may include firewalls, network address translation, the use of a proxy server, or the use of a virtual private network connection.

Designing a Windows 2000 Security Solution

- Finally! By this stage of the objectives, you should be ready to stop reading the case studies and ready to get on to the task at hand, answering the questions!

Design an audit policy.

Things to know about an audit policy:

- Know that you can turn on the *Audit Directory Service Access* category to audit objects on a domain controller.
- Know that you can turn on the *Audit Object Access* category for auditing objects on a member server or a Windows 2000 Professional System
- Know that auditing is implemented from the Local Security Policy selection of Administrative tools
- Know that you audit the success or failure of an event.
- Know that auditing is not deterministic, in other words when an event gets written to the audit log, it will write that Fred Flintstone accessed in file in this folder. It does not determine whether Flintstone should have been able to access to the file.
- Know that auditing puts stress on the machine it is implemented on.

Design a delegation of authority strategy

- This was mentioned above. The designers of the Windows 2000 security curriculum are very big on distributing administration and giving non-IT types the ability to manage security groups. Remember this concept.

Design the placement and inheritance of security policies for sites, domains and organizational units.

Security policies can be implemented through Group Policy Objects.

- GPO's can be implemented at the site, domain or organizational unit level.
- Know how security policies are implemented and what role inheritance plays.
- Know the priority of inheritance.
- Know how an enterprise administrator can force inheritance.
- Know how inheritance of security policies can be blocked and when you would use that.

- Be able to pick out which policy will be in effect, after inheritance, given a certain situation.

Design an Encrypting File System strategy.

- Know that you can encrypt files or folders.
- Know how to encrypt files or folders.
    - From Microsoft Explorer, highlight the folder or file, choose Properties and select Advanced. There is a check box that will encrypt the file or folder.
- Know who can decrypt files or folders.
    - The owner of the file or the designated recovery agent (usually the administrator).
- Know that the Recovery Agent will have access to the encryption key.
- Know that the encryption key should be exported to removable media and stored in a locked, offsite location.
- Know that you should keep a backlog of encryption keys.
- Know that the EFS only works on Windows 2000 NTFS volumes.
- Know that files are only encrypted when they are stored. If you are going to store a file in an encrypted folder on a server, the file is not encrypted in transit to the server.

Design an authentication strategy.

Select authentication methods. Methods include certificate-based authentication, Kerberos authentication, clear-text passwords, digest authentication, smart cards, NTLM, RADIUS and SSL.

- Know that Windows 2000 comes with the ability to provide certificate-based authentication without use of a third party vendor.
- Know that Kerberos v5 is the default authentication protocol of Windows 2000.
- Know that you want to avoid clear text passwords at all costs.
- Know what a smart card is and when it should be used.
- Know that NTLM is the backwardly compatible authentication protocol that is used in mixed mode domains. It provides authentication between NT 4 BDC's and the Windows 2000 security system.
- Know that RADIUS is used to provide authentication in dial-up situations.
- Know that SSL is used to provide secure communication between a web browser and a web site.

Design an authentication strategy for integration with other systems.

- With Windows 2000, the default authentication protocol is Kerberos v5. This protocol can be used for cross platform authentication.
- Note: In the testing world, Kerberos v5 provides for cross platform authentication. In the real world, you may require the use of some third party solutions.

Design a security group strategy.

- This was mentioned above. The designers of the Windows 2000 security curriculum are very big on distributing administration and giving non-IT types the ability to manage security groups. Remember this concept.
    - Know the different types of groups, including the default security groups in Windows 2000 and how they are implemented.
    - Know how to group users and computers into special groups so that they can be controlled.
    - Know the default security groups available in a Windows 2000 implementation.

Design a Public Key Infrastructure

Design Certificate Authority (CA) hierarchies.

- Know that certificate services works in a hierarchical structure and how you can implement that structure.
- Know that some of the CA's may actually not even be connected to the network.

Identify certificate server roles.

- Enterprise CA
    - Active Directory must be present.
    - Has access to certificate templates
- Standalone CA
    - Used when Active Directory is not present.
    - Does not have access to certificate templates
- Issuing CA
    - This is the CA that actually gives out the certificate.

Manage Certificates

- Know that there are different types of certificates.
- Know that you can control certain features of certificates, including their time to live.
- Know what to do if a certificate has been compromised, and how to revoke a certificate.

Integrate with third-party CA's.

- Know that Windows 2000 will work with third party CA's.

Map certificates

- Certificate mapping is where a certificate issued by a third party CA is assigned to a particular user and associated with that user account in Active Directory.
- Software like Internet Explorer can be used to authenticate the user that is connecting to a resource over the Internet using the functionality of Active Directory.
- Certificates can be mapped only to individual user accounts, not to security group accounts.

Design Windows 2000 network services security

Design Windows 2000 DNS security.

- Know that Windows 2000 uses dynamic DNS.
- Know that DNS is integrated into the Active Directory.
- Know that DNS zone replication is now handled by Active Directory.
- Know that DNS zones can be configured to use a secure dynamic update.
- Know that groups of users can be configured to be able to update DNS through judicious use of the ACL.

Design Windows 2000 Remote Installation Services Security

- Know that RIS is used to build Windows 2000 workstations.
- Know how to connect to the RIS server.
- Know that the administrator can configure if the RIS server will even talk to clients.
- Know that there are RIS Group Policy Options that can be applied to RIS installations. This will help define what can and cannot connect to the RIS server.

Design Windows 2000 SNMP security.

- SNMP Basics -
    - SNMP Manager
        - The host that gathers information and depending on the implementation, displays alerts if necessary.
    - SNMP Agent
        - The reporting piece of the puzzle. The agent can be hardware or software. The agent reports to the manager on any kind of a defined event like startup, shut down, access, etc.
    - Management Information Base (MIB)
        - The defined events that the agents will use for reporting.
    - SNMP works with either IP or IPX
    - SNMP agents are gathered in communities. Communities report to SNMP managers using TRAP messages. Information is usually sent in a plain text format.
- SNMP Security is defined by the way Community Managers can be granted permissions to get information from agents. There are five levels of permissions that can be used to provide SNMP security
        - None - No communication will occur.
        - Notify - The same as None.
        - Read Only - The agent will only process requests that get information. It will not process configuration requests.
        - Read Create - The agent will process requests to get information and also for configuration.
        - Read Write - The same as read create
- SNMP messages can also be configured to make use of IPSec, providing data encryption while the message is on the wire.

Design Windows 2000 Terminal Server security.

The Terminal Services security features include:

- Encryption - Data transmitted between the Terminal Server and host session can be encrypted to Low, Medium or High levels depending on the administrator's choices.
- Administrators can limit logon attempts as well as limit connection times.
- Security can be added to the connections by way of permissions applied to group. The default groups are:
    - System
    - Administrators
    - Users
    - Guests

- User connections can be managed using Terminal Server User profiles.
- Terminal Servers use Remote Desktop Protocol (RDP) which uses port 3389. If there is a firewall in play, that port should be opened.

Designing a Security Solution for Access Between Networks

- This objective starts by looking at the ways you can control access to the Internet from your private network, so read that as Proxy Server or network address translation.
- The remaining parts of this objective could be considered Virtual Private Network basic training. These objectives look at ways to implement a Virtual Private Network.
- Virtual Private Networks can be created to assist with two scenarios:
    - Remote client connecting to private network using the public network (usually the Internet) as a backbone.
    - Connecting two sections of a private network using tunneling. This can be done using either sections of the public network or sections of the private network for increased security.
- Virtual Private Networks create a tunnel between the server and the client. All data sent through the tunnel is encrypted.

Provide secure access to public networks from a private network.

- Many companies feel that one of the greatest security costs they bear is controlling access to the Internet. Companies can suffer tremendous losses due to lost productivity because of employees surfing the Internet.
- Ways this can be controlled includes:
    - Use a proxy server or firewall to control where on the Internet users can go and when they can go there.
- Another problem with Internet use is the user can unknowingly provide information about the private network. This can include the internal addressing scheme of the private network. In this case, using Network Address Translation (NAT) can help protect the private network. The only address that is "published" is that of the gateway. NAT also helps provide large number of IP addresses for the private network.

Provide external users with secure access to private network resources.

- In this case, the external user creates a VPN session between the client workstation station, and a VPN server using the public network as a transport medium. The public network is usually the Internet. The VPN server can be located in front of the corporate firewall, behind the corporate firewall, or in a screened subnet. A screened subnet is also referred to as a DMZ.

Provide secure access between private networks.

- **Provide secure access within a LAN.**
- **Provide secure access within a WAN**
- **Provide secure access across a public network**.

- Here again, you are expected to be able to pick out ways that VPN's can be utilized. You would use a VPN across a LAN to provide a secure connection between two departments where interdepartmental communication must be encrypted.
- Secure access across a WAN could see a VPN put into play for the very same reason, to connect two departments. It can also be used to protect information traveling between two different locations (regional offices, subsidiaries, etc).
- The most common use of a VPN is to provide secure access across a public network. This would be a demonstration of how to create a VPN between two routers, using the Internet as the corporate backbone.

Design Windows 2000 security for remote access users.

- This objective did not deal with the intricacies of RAS configuration and permissions as much as it dealt with the proper placement and use of a RAS server. Too often, administrators will configure a secure network with properly placed and designed firewalls, only to have a RAS server that is pretty much open to the world located behind the firewall.
- This objective deals with placing the RAS server in the DMZ between firewalls, and controlling the access from the RAS server to the rest of the private network.

Designing Security for Communication Channels.

Design an SMB-signing solution.

- Server Message Blocks (SMB) are ways of bypassing constraints between NTFS and the Network File System (NFS) used in the Unix world. Know when it would be used.

Design an IPSec solution.

- IP Security (IPSec) is the default transport protocol used in the creation of a VPN. This is the way that you can configure the security it provides.

Design an IPSec encryption scheme.

- You can define the level of encryption in IPSec. The key thing to remember for testing purposes is that the encryption level must be the same on both the client and the server or communication cannot occur. Remember all the ways back to the first objective, about defining whether you are dealing with an International company? Here is where it comes to play. Suppose you have an IPSec solution that uses 128-bit encryption. If you have to add an International connection to the mix, suddenly you have to provide a lower level of encryption due to treaty constraints, or provide for another VPN Server.

Design an IPSec Management strategy.

- Due to the nature of the IPSec connection, they can be very intensive. After all, the tunnel has to be created, which means that somehow, someone must provide a list of IP addresses for the server to give out, and then once the connection has been established it must be maintained. Maintenance not only means making sure the connection stays up, but it means that the system must encrypt and decrypt all these packets. The IPSec management strategy is to define who can use IPSec connections, how they can use them and what level of encryption will be used.

Design negotiation policies.

- When an IPSec server and client start talking they negotiate the way the communication will be handled. This can include things like key length, key life, whether the key will be dynamically changed during the course of the connection and whether to use Authentication Headers (AH) or Encapsulating Security Payloads (ESP) for the protocol. Again, the client and the server must agree for communication to occur. The negotiation policy defines the parameters of these items.

Design security policies.

- There are several default group policies that can be used to secure IPSec communications. These policies are configured using the MMC, for example for local computer policy. You can configure the system as to how it handles requests from non-IPSec aware clients or how it handles communications from IPSec aware clients. Again, you are simply defining the base parameters for the beginning of communications. For testing purposes remember that if both sides do no agree, communication will not occur.

Design IP filters.

- IP filters help the IPSec server to decide who it is going to talk too. The IP filter will either allow or deny access to the IPSec server depending on the address of the specific computer or the subnet it resides on.
- There are also some port filters to be aware of. IPSec uses IP ports 50 and 51 and UDP port 500. These ports should be opened at the firewall if communication is going to occur between a remote user and the VPN server behind a firewall.

Define security levels.

These security levels are:

- Accept unsecured communication, but always respond using IPSec
    - This communication setting allows unsecured communication initiated by another computer but requires the computers to which this policy applies to always use secure communication when replying or initiating.
- Allow unsecured communication with non-IPSec-aware computers
    - This communication setting allows unsecured communications to or from another computer. This is used if the computers in the IP filter list are not IPSec enabled. If negotiation for security fails, this will disable IPSec for all communication to which this rule applies.
- Session Key Perfect Forward Secrecy
    - This communication setting ensures that session keys or keying material are not reused. Selecting *Session Key Perfect Forward Secrecy* also ensures that new Diffie-Hellman exchanges will take place after the session key lifetimes have expired.

Special thanks to Gary Govanus for writing this Cramsession.