Study guide by ExamNotes.net

Exam 70-220

Designing Security for a Microsoft® Windows® 2000 Network

Abstract

This ExamNotes Study Guide intends to provide you with information to prepare for the Microsoft W2K 70-220 Exam.

ExamNotes Study Guide Topics Covered

Exam topics covered include Controlling and Auditing Access to Resources, Authentication, Encryption, VPN, IPSec, and Analyzing Risk & Security Requirements.

Before you start

This study guide provides you with information on the many different aspects of "W2K Network Security Design". You should not use this information as your first step into W2K, as this exam is targeted towards candidates with solid background on Networking.

Before you proceed with this subject, please read through the study material for the following:

- 70-215
- 70-216
- 70-217

You should already have exposure to topics like file and share permissions, OUs, IPSec, Kerberos V5, PKI, IPSec, VPN … etc.

By all means read more than one book on the subject and make sure you understand the material well enough so that you could be ready for the scenario questions. EVERY QUESTION IS CASE STUDY QUESTION! There is no quick way to succeed for this topic. You must fully understand all the related concepts and be able to think intelligently to decide what is correct and what is not. This study note can only provide you with a certain degree of assistance in preparation. You must study real hard before even trying to sign up for the exam.

Business Requirement

Again, you see this topic in the exam. You just have to make sure you have the business sense of administration (or that you have a business degree…..), such as Centralized VS decentralized model, regional VS departmental…etc.

For any operation that spread across different regions, VPN is always the choice. However, if the operation is cross border, especially when it reaches area that are outside of North America, there are international treaties and regulations that limit the technology that can be used as security measures.

When you plan for a strategy, there are certain factors you must consider:

- Company priorities
- Growth strategy
- Relevant laws and regulations
- Risk Tolerance
- Total cost of operations

It does not make sense if the security solution costs too much compare to the overall financial figures.

Risks

When we talk about risk, we want to know where they come from. Sources could include but not limited to:

- Internal Attack
- Social Engineering
- Organizational Attack
- Accidental Security Breach
- Automated Computer Attack

Accidental Security Breach is usually the administrators' mistakes that users are placed in the wrong group or are granted incorrect permissions.

Regarding the type of attacks, attackers either want to steal information from you, or to stop your services. The Denial of Service Attacks can block access to resources, flood your network, degrade your network performance, cause your server to fail, or even result in loss of service and revenue.

Your strategy to protect your internal network should cover the following areas: Administrative Access, User Accounts, Windows 2000–based Computers, File, Folder, Print Resources, Communication Channels, and Non-Microsoft Clients. You should also consider the following areas:

- Remote User Access to Network from home or other locations
- Remote Office Access to NetworkRemote Partner Access to Network
- Internet User Access to Internal Network

- Internal User Access to Internet

The task of security management can include:

- Secure Physical Systems and Devices
- Manage Users, Groups, and Policies
- Define and Implement Authentication and Data Transmission Security
- Control and Monitor Access to Shared Resources
- Create and Implement an Audit Policy
- Create and Implement a Backup and Recovery Plan
- Create and Implement Desktop Policies

W2K Security

Win2K Active Directory's security boundaries are defined using domains. With AD, we can support security settings using OUs, and can enjoy the delegation of administration flexibility. Group policy can be deployed at various levels to implement security.

Regarding user authentication, we have the options of:

- Kerberos V5 Authentication
- Certificate-based Authentication
- NTLM Protocol for Authentication

The good thing about the default Kerberos V5 used in W2K is the cross platform compatibility according to Microsoft.

After authentication, you want to encrypt your data and transmission too. For encrypting application data, we have EFS and S/MIME. For encrypting communication, we have IPSEC and TLS. EFS protects stored data and uses file encryption key to encrypt the data. The key itself is encrypted by the user's public key and the EFS recovery agent's public key. For transmission encryption, you need to know that IPSec works at the IP layer while SSL and TLS work at the application layer. PKI allows for the use of Digital Certificates for Authentication, although you will need to deal with the complexity of setting up Certification Authorities.

To encrypt files or folders, from Windows Explorer you highlight the folder or file, then choose Properties and select Advanced. To decrypt files or folders, one must be the owner of the file or the designated recovery agent – he/she will have access to the encryption key.

To be 100% safe, the encryption key should be exported to removable media and stored in a separate location. The administrator should always keep a backlog of all encryption keys.

Security Identifiers SID are automatically created when an object is added, are for identifying users, groups, or computers, and are used to grant access rights and permissions to resources. To control access to resources, we use DACL to specify Access Permissions for resources, and use ACEs within the DACL to list actions That users or groups can perform on those resources. We can also use SACL for auditing.

To maintain logical security setting, we should focus on:

- Restrictive Logon Hours
- Strong passwords (8 characters)
- Active Directory User Account Options
- Workstation Access Restrictions

One good idea is to encourage the use of RUN AS - running applications with alternate credentials. This could avoid the need to grant special permissions to some users.

User Account and Applications

The tasks of user account planning and management involves the following:

- Account Policies and Group Policy Design
- Account Creation and Location Plan
- Delegation of Authority
- User Account Audits

During the policy design phrase, the following have to be taken care of: Designing Account Policies, Prioritizing Group Policy Application, Filtering Group Policy, and Designing for Group Policy Inheritance. As you know, different account policies require different domains. Also, take into consideration the flow order of GPO application:

1. Local Computer
2. Site
3. Domain
4. Parent OUs
5. Child OUs

The later one is always the one that is effective. Also be careful about the No Override and the Inheritance Blocked options. All these bring into extra complications.

By the way, as a smart administrator, you want to carefully design a template, and then use it to generate user accounts with the help of scripting.

Auditing is implemented from the Local Security Policy selection of Administrative tools. You can turn on the Audit Directory Service Access category to audit objects on a domain controller, or turn on the Audit Object Access category for auditing objects on a member server or a Windows 2000 Professional System. Keep in mind that for auditing Success and Failure, a Success can document an actual security breach, while a Failure is only indicating an attempted security breach.

On a w2K computer, a member of the Users group cannot run most programs that are NOT designed for W2K. You should use one of the following methods to work around the issue:

- Install a version of the program that is for W2K.
- Move users from the Users group into the Power Users / Admin group. Of course, this option is not encouraged.
- Use the Compatible security template to change the default security permissions for the Users group.

Protecting the Computers

Believe it or not, PHYSICAL SECURITY is a very important concern. The following options are worth to consider:

- Placing Servers in Locked Rooms
- Physically Securing Network Devices
- Configuring Devices As RADIUS Clients for better authentication

To strengthen the password security, you use Password Encryption Key to encrypt all passwords, and then use the System Key utility SYSKEY to encrypt the Password Encryption Key. What if someone try to turn off and reset your computer? Use power on password to protect the configuration detail and prevent BIOS modification!

Once the physical aspect is secure, you want to proceed with evaluating security requirements, designing security configuration templates, evaluating security configuration, and deploying security configuration templates.

Security Templates

Security template files are text-based files that describe the security settings for each security area, including:

- Account Policies
- Local Policies
- Event Log
- Restricted Groups
- System Services
- Registry
- File System

Once the templates are created, an administrator can apply them to specific users.

We most likely will use the Security Templates snap-in to create security template files in GUI. Alternatively, we can use Secedit.exe, a utility that is a command-line version of the Security Configuration and Analysis utility, for analyzing and configuring computers based on security template settings.

Some predefined templates that come with W2K are:

- Basic: Basicwk.inf (Windows 2000 Professional), Basicsv.inf (Windows 2000 Server), and Basicdc.inf (domain controller)
  They specify default security settings for all security areas, with the exception of user rights and group membership.
- Secure: Securews.inf (Windows 2000 Professional)and Securedc.inf (domain controller)
  They provide increased security for areas of the operating system that are not covered by permissions.
- Highly Secure: Hisecws.inf (Windows 2000 Professional) and Hisecdc.inf (domain controller)
  They are provided for Windows 2000-based computers that operate in native Windows 2000 environments only, and requires that all network communications be digitally signed and encrypted at a level that can only be provided by Windows 2000.
- Compatible: Compatws.inf (Windows 2000 Professional)
  They open up the default permissions for the Local Users group so that legacy programs are more likely to run. They make the environment less secure.

It is very important for you to know that the security templates modify security settings incrementally and do not include the default security settings, meaning computers that are upgraded from Windows NT do not use the default Windows 2000 security settings, but instead use whatever security settings were in place prior to the upgrade.

Security Policies

Security policy is a security configuration file that is stored as part of a Group Policy object. You create this file using the Security Configuration Tool Set MMC snap-in. Please note the order of precedence for security policies, as those associated with Active Directory domains and OUs take precedence over policies established at the local level. From the lowest to highest precedence, the ranking order is: Local Policy; Domain Policy; and OU Policy.

Tools available for Security Configuration include:

- Security Settings Extension to Group Policy – for configuring security policies for domains and OUs.
- Active Directory Users and Computers Snap-in – for performing administrative tasks.
- Security Templates snap-in – allows the creation of a text-based template file that contains security settings for all security areas.

Certificate Authority

Microsoft Windows 2000 provides two types of CAs: an enterprise CA or a stand-alone CA. And within these classes, there can be two types of CAs – a root or a subordinate. You should install an enterprise CA if you will be issuing certificates to users or computers inside an organization that is part of a Windows 2000 domain, as an enterprise CA requires that all users requesting certificates have an entry in Active Directory. Otherwise, you should install a stand-alone CA if you will be issuing certificates to users or computers outside of a Windows 2000 domain.

CAs are organized into hierarchies with the root CA at the top. All other CAs in the hierarchy are subordinate CAs, and are trusted only because the root is trusted. This is why the enterprise root CA is the trust point in the enterprise. Note that there can be more than one enterprise root CA in a Windows 2000-based domain, and thus more than one hierarchy. It is also possible to mix and match stand-alone and enterprise CAs in a hierarchy.

Windows 2000 works with third party CA. Certificate mapping is where a certificate issued by a third party CA is assigned to a particular user and associated with that user object in the Active Directory database. Note that certificates can be mapped only to individual user accounts, not to security group accounts.

All enterprise CAs have a special policy module that enforces how certificates are processed and issued. Information used by these modules is stored centrally in a CA object in Active Directory.

In a stand-alone hierarchy, the stand-alone root CA is at the top, and each new stand-alone root CA starts a new hierarchy. It has a very simple policy module and does not assume that Active Directory service is available.

IPSec

With Internet Protocol Security (IPSec), you can provide data privacy, integrity, authenticity, and anti-replay protection for network traffic in the following scenarios:

- End-to-end security from client-to-server, server-to-server, and client-to-client using IPSec transport mode.
- Secure remote access from client-to-gateway over the Internet using Layer Two Tunneling Protocol.
- Secure gateway-to-gateway connections across outsourced private wide area network (WAN) or Internet-based connections using L2TP/IPSec tunnels or pure IPSec tunnel mode.

IPSec security for all unicast IP traffic is either requested but optional, or requested and required, as set up by the administrator's configuration of the server. With this model, clients need only a default policy for how to respond to security requests from servers. Once IPSec security associations are established, they remain in effect for 1 hour after the last packet was sent between them. After that the client cleans up the security associations and return to the initial "respond only" state.

If the server is directly accessible from the Internet, the client must receive an IPSec policy so that it requests IPSec security for traffic when it attempts to send data to the server. Additionally, clients and servers can have specific rules for permitting, blocking, or securing only certain network packets based on protocol or port.

Keep in mind that IPSec uses IP ports 50 and 51 and UDP port 500. These ports should be opened at the firewall if communication is going through it.

VPN Security

User attempting the PPTP connection is authenticated using PPP-based user authentication protocols such as EAP, MS-CHAP, CHAP, SPAP, and PAP. For PPTP connections, EAP-TLS using smart cards or MS-CHAP version 2 is highly recommended for mutual authentication.

PPTP inherits MPPE encryption which uses RSA RC4 stream cipher, and is only available when either the EAP-TLS or MS-CHAP authentication protocols are running. MPPE can use 40-bit, 56-bit, or 128-bit encryption keys, although the 40-bit key is only for providing backward compatibility. The highest key strength supported by the VPN client and VPN server is negotiated during the process of connection establishment.

Since IP datagrams sent across the Internet can arrive in a different order from the one in which they were sent, MPPE for VPN connections changes the encryption key for each packet, meaning the decryption of each packet is independent of the previous packet. This is why MPPE includes a sequence number in the MPPE header, so that if packets are lost or arrive out of order, the encryption keys are changed relative to the sequence number.

A PPTP-based VPN server typically has two physical interfaces, one on the public network and another one on the private intranet. For the VPN server to forward traffic, IP forwarding must be enabled on all interfaces. To protect the intranet from all traffic not sent by a VPN client, PPTP packet filtering must be configured so that the VPN server only performs routing between VPN clients and the intranet and not between potentially malicious users on the shared or public network and the intranet.

Authentication of the VPN client can occur at two different levels: the computer and then the user. Mutual computer authentication is performed when you establish an IPSec ESP security association through the exchange of computer certificates. To use L2TP over IPSec, a computer certificate must be installed on both the VPN client and the VPN server.

User attempting the L2TP connection is authenticated using PPP-based user authentication protocols such as EAP, MS-CHAP, CHAP, SPAP, and PAP. Since PPP connection establishment process is encrypted by IPSec, any PPP authentication method can be used. Mutual user-level authentication occurs if you use MS-CHAP v2 or EAP-TLS.

In addition, L2TP can authenticate the endpoints of an L2TP tunnel during the tunnel establishment process. This is known as L2TP tunnel authentication. However, Windows 2000 does not perform L2TP tunnel authentication by default.

There are two approaches to using a firewall with a VPN server. Either the firewall is between the VPN server and the intranet, or the firewall is attached to the Internet and the VPN server is between the firewall and the intranet. In the case of a VPN Server in Front of the Firewall, you need to add packet filters to the Internet interface that only allow VPN traffic to and from the IP address of the VPN server's interface on the Internet. For incoming traffic, when the tunneled data is decrypted by the VPN server, it is forwarded to the firewall that employs filters to allow the traffic to be forwarded to the intranet. This prevents VPN users from accessing specific intranet resources and prevents the sharing of File Transfer Protocol or other intranet resources with non-VPN Internet users.

When the VPN Server is behind the firewall, this is effectively a demilitarized zone DMZ. The firewall must be configured with input and output filters on its Internet interface to allow the passing of tunnel maintenance traffic and tunneled data to the VPN server. Additional filters would allow the passing of traffic to servers on the DMZ. Since the firewall does not have the encryption keys for each VPN connection, it can only filter on the plaintext headers of the tunneled data. This should not be a security concern as the VPN connection requires an authentication process that prevents unauthorized access beyond the VPN server.

Other Security Issues

SNMP messages can be configured to make use of IPSec. Same for Terminal services: 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 and connection times. Keep in mind that Terminal Service uses Remote Desktop Protocol, which uses port 3389. If there is a firewall in between, make sure that port is opened.

One issue we frequently ignore is that of controlling access to the Internet. Companies can suffer tremendous losses due to lost productivity, since employees are spending time surfing the Internet. To control, you can use proxy server or firewall to determine where on the Internet users can go. You can also limit when they can go. To prevent user from unknowingly leaking information about the private network, use Network Address Translation NAT to protect the private network by hiding internal IP addresses, so that the only address published is that of the gateway.

RAS is another important piece of the network we need to pay attention to. One of the best ways to protect the RAS server is to place it in the DMZ between firewalls, and controlling the access from the RAS server to the rest of the private network. A DMZ Demilitarized Zone is used by a company that wants to host its public services without sacrificing unauthorized access to its private network. The DMZ typically sits between the Internet and an internal network's line of defense - usually some combination of firewalls and bastion hosts. It contains devices accessible to Internet or other dial-in traffic. And remember, CLEAR TEXT is always a bad choice. Avoid it.