Cram Guide for Exam 70-220 Designing Security for a Microsoft Windows 2000 Network

Security Punchlist

Analyze Corporate Business Objectives.

1. Identify any statements about company priorities, tolerance to risk, recent security breaches, relevant laws, regulations, or standards.
2. Understand the business model in terms of information, physical constraints, and whether it's distributed or networked.
3. Identify specific requirements for end users, special groups, and business partners.
4. Understand the management model/structure as centralized or decentralized, functional areas and scopes of responsibility, and geographical constraints in relation to LAN/WAN.

Analyze the Technical Requirements

5. Evaluate the technical structure:
   - Physical distribution of users and resources
   - Methods of system access: networked, remote, Internet
   - Inventory of services and methods of access to these services
   - Current and projected demands on available bandwidth
   - Roles and responsibilities in terms of security and resource permissions

Analyze Security Risk

6. IT security controls include availability of services or resources, optimized use of resources, compliance, reliability, integrity, and confidentiality.
7. This chart compares the three attack modalities:

Dimension	Interference	Interception	Impersonation
Active	Access control	Integrity	Authenticity
Passive	Availability	Compliance, Non repudiation	Confidentiality

8. This chart shows examples of security breaches:

Dimension	Interference	Interception	Impersonation
Active	Denial of service	Web page redirection	Spoof, replay, crack
Passive	Active viruses, bacteria	Wire taps	Trap door, Trojan horse

9. Determine a security baseline that includes users, groups, and services.
10. Analyze the impact of security design on both current and projected environments.
11. Identify required levels of security for resources and services.

Designing Security Solutions

Distributed Services Security Design

12. In a security design, consider the strategic areas of authentication methods, security group membership and placement, delegation of authority, Group Policy inheritance, loopback support, and audit policy.

Physical Topology

13. A site is a set of computers in one or more IP subnets, described as well connected, providing efficient exchange of information.
14. There is no correlation between physical structure and domain structure nor a connection between sites and domain namespaces.
15. Active Directory allows multiple domains in a single site, as well as multiple sites in a single domain.
16. Remember the order of GPO processing using the acronym SDOU (site, domain, Organizational Unit (OU), OU within OU).

Network Protocols

17. The following chart shows which security protocols map to which layers of the Open Systems Interconnection (OSI) model:

7	Application	API	Secured Multipurpose Internet Mail Extensions (SMIME); Kerberos protocol and otehr AAA servers; Proxy services; Secured Electronic Transactions (SET) service; IPSec--Internet Key Exchange Protocol (formerly ISAKMP/Oakley)
6	Presentation		
5	Session		
4	Transport	TDI	SOCKS (Sockets for Unix compatibility); Secured Sockets Layer, Transport Layer Security (SSL3/TLS1)
3	Network	NDIS	IPSec--Authentication Header (AH), Encapsulated Security Payload (ESP); Packet filtering; Point-to-Point Tunneling Protocol (PPTP); Challenge Handshake Authentication Protocol (CHAP); Password Authentication Protocol (PAP); Microsoft CHAP (MS-CHAP)
2	Data Link		
1	Physical	Physical	Hardware CSP

Trusts

18. A trusting (resource) domain points to a trusted (master, account) domain; the direction of user access is in the reverse direction of the arrow.
    - *Two-way*--All domain trusts in a Windows 2000 forest
    - *One-way*--Windows 2000 domains in different forests, NT 4 domains, and Kerberos 5 realms
    - *Transitive*--Always two-way and unbounded, flows upward through domain tree
    - *Nontransitive*--One-way by default; in mixed mode, all trusts are nontransitive; bounded by the two domains, does not flow upstream; nontransitive trusts are the only form of trust possible between the following pairs of items: a Windows 2000 domain and an NT domain, a Windows 2000 domain in one forest and another Windows 2000 domain in another forest, and a Windows 2000 domain and a Kerberos 5 realm

Security Configurations

19. The security templates, designed to satisfy common security needs, are:
    - *Basic (basicwk.inf, basicsv.inf, basicdc.inf)*--Default workstation, server, domain controller for Windows 2000 respectively. Templates reapply default settings to all security areas except user and group rights.
    - *Compatible (compatws.inf)*--Compatible workstation or server. **Not a secure environment.** Templates implement an ideal user configuration but a less secure power user configuration; the template lowers security levels on specific files, folders, and Registry keys accessed by software applications so that they run successfully under a user security context.
    - *Secure (securews.inf, securedc.inf)*--Secure workstation, server, or domain controller respectively. Templates implement security settings for all areas except files, folders, and Registry keys; these objects are configured by default or permissions.
    - *Highly Secure (hisecws.inf, hisecdc.inf)*--Highly secure workstation, server, or domain controller respectively. These templates for IPSec-enabled traffic and protocols between Windows 2000 machines must be digitally signed and encrypted.
    - *Dedicated Domain Controller (dedica*.inf)*--Templates implement ideal file system and Registry permissions settings, especially for local users on Windows 2000 DCs.

Network Services Security Design

Certificate Services

20. There are four types of Certificate Authorities (CAs):
    - *Enterprise CA*--Integrated into AD; validates users it issues certificates for against AD accounts database. Can be root or subordinate.
    - *Root CA*--The first CA in the organization and therefore the most trusted.
    - *Subordinate CA*--Either subordinate to the root CA or another subordinate, it is certified by its parent. Usually handles some dedicated service like smart card authorization.
    - *Standalone CA*--Not automatically integrated with AD; usually handles Internet requests for certificate services.

Encryption

21. Public key (Diffie-Hellman algorithm) encryption is another name for asymmetric encryption; it uses two keys instead of one symmetric encryption key.
22. Message digest (hash) is a fixed-size block generated when a one-way mathematical function (hash algorithm) is applied to an arbitrary amount of data.
23. MD5 is a one-way message digest hash algorithm developed by RSA Data that creates 128-bit hash values. Challenge Handshake Authentication Protocol (CHAP) uses a challenge response with one-way MD5 hash as the

© Copyright 2004 CertTalk.com/Adaptive Learning Systems, Inc. All Rights Reserved.

response.

24. Secure Hash Algorithm (SHA) is a message digest that generates a 160-bit hash value. SHA-1 is used with Digital Signature Algorithm (DSA) in the Digital Signature Standard (DSS).
25. EAP-MD5 CHAP is a type of Extensible Authentication Protocol (EAP) using Point-To-Point Protocol (PPP)-based CHAP, but both challenge and response are sent as CHAP.
26. EAP-TLS, the strongest authentication and key exchange method, is an EAP type that smart cards must use in security environments; it provides mutual authentication, negotiation of encryption method, and secure key-exchange.

Remote Connectivity Issues

Remote Access from Outside the Network

27. The Routing and Remote Access Services (RRAS) order of authentication (from strongest to weakest) is:
    - *Extensible Authentication Protocol (EAP)*--Must configure EAP-TLS methods when using smart cards
    - *Challenge Handshake Authentication Protocol (CHAP)*--Uses MD4
    - *Microsoft CHAP version 2 (MSCHAP2)*--Provides for mutual authentication
    - *Microsoft CHAP version 1 (MSCHAP1)*--Uses MD5
    - *Password Authentication Protocol (PAP)*--Uses plaintext; least secure
    - *Shiva Password Authentication Protocol (SPAP)*--Proprietary; for Shiva router

Remote Access Involving Private Networks (VPN)

28. Configure the RRAS as a VPN; use one of two protocols: L2TP or PPTP. L2TP uses IPSec and requires computer certificates for both server and client. PPTP uses any RRAS protocol. Use MSCHAP2; if it isn't available, then use MSCHAP1. With smart cards, PPTP uses EAP-TLS.

Secured Access Using Firewall Technologies

29. Firewall technology operates on one of two basic strategies; *default permit*--what is not expressly prohibited is, by default, permitted--and *default prohibit*--what is not expressly permitted is, by default, prohibited.
30. The default prohibit (or deny) strategy requires more management but is more conservative in its restrictive approach to the passage of data across the firewall.
31. Packet filtering uses both firewall and network interface as a router; it inspects packets relayed across the network interface for specific IP addresses or protocols.
32. Screened-host architectures use a computer (host) as a gateway behind the packet-filtering (screening) external network interface. The host or bastion can have a single network adapter card (single-homed host or bastion) or two network adapter cards (dual or multiple-homed host or bastion).
33. Screened-subnet architecture, called a demilitarized zone or DMZ, is the most secure because is an isolated subnet between two screening packet filters.

Security for the Communications Channel

34. The following chart shows the VPN effectiveness of several network security protocols:

Connection Type	PPTP	L2TP	L2TP/IPSec	IPSec Transport	IPSec Tunnel
End-to-end (no NAT)	Good	Good	Good	Good	Good
End-to-end (NAT)	Good	Good	Not good	Not good	Not good
Client-to-gateway	Good	Good	Good	Good	Not good
Gateway-to-gateway	Good	Good	Good	Good	Fair

35. The following chart shows a comparison of IPSec security services by protocol:

Protocol	Access Control	Integrity	Authentication	Partial Sequence Integrity*	Confidentiality
AH	Yes	Yes	Yes	Yes	No
ESP (encryption only)	Yes	No	No	Yes	Yes
ESP (encryption plus authentication)	Yes	Yes	Yes	Yes	Yes

*The rejection of packets not in sequence protects against replay attacks.

Secured Resources

36. When using Encrypting File System (EFS), only files and folders on NTFS volumes can be encrypted and only the user/owner who encrypted the file can reopen it. System files and compressed files cannot be encrypted.
37. Encrypted files can be decrypted if moved to a FAT volume.
38. Data transmitted across a network is not encrypted until it is saved to disk. Use SSL or IPSec to encrypt data during transmission.
39. A recovery policy is automatically implemented the first time a file or folder is encrypted. You can use a recovery agent to decrypt the files if you lose your encryption certificate.

© Copyright 2004 CertTalk.com/Adaptive Learning Systems, Inc. All Rights Reserved.