The 70-214 Cram Sheet

This Cram Sheet contains the distilled, key facts you need for Exam 70-214, Implementing and Administering Security in a Windows 2000 Network. You should review this information as the last thing you do before you enter the testing center, paying special attention to areas where you feel that you need the most review. You can transfer any of these facts from your head onto the blank sheet of paper that the testing center provides immediately after you are seated in the testing room, before you begin the exam.

1. Templates provided by default include `basic` (basic security), `compat` (reduced security), `secure` (medium security), `hisec` (high security), `ocfile` (for applications such as certificate servers), and `setup security` (the security setup on the computer when it was installed).
2. Templates used during installation are `dwup.inf` and `dsup.inf` for upgrades and `defltwk.inf` and `defltsv.inf` for normal installations. `deftlldc.inf` is applied during `dcpromo`.
3. Simply changing a setting in a security template has no effect on the security on any machine. For security templates to change security, they must be applied.
4. The password policy is set in the default domain security policy for all domain accounts.
5. The password policy for local accounts can be set locally or in the password policies of GPOs linked to OUs within which the computer account resides.
6. The Additional Restrictions for Anonymous Connections security option can prevent leakage of security information. Selecting the anonymous restriction setting prevents enumeration but allows anonymous connection.
7. The Digitally Sign Client Communication settings can help prevent man-in-the-middle attacks because they require mutual authentication between the server and client for SMB connections.
8. If a computer is out of touch with its domain for a long period of time, the password synchronization process can fail, causing the computer to be unable to log on.
9. Because every service represents running code that may have a vulnerability, you should severely restrict the services that run on a system.
10. If a group is added to the Restricted Groups section of the security template, the next time the template is applied, only group members listed in the template remain in the group.
11. Using the Security Configuration and Analysis console to apply security settings is a one-time event that makes direct changes to the registry.
12. `secedit` is the command-line version of the Security Configuration and Analysis program. The following command analyzes the current settings against the `baseline.inf` template: `secedit /analyze /DB c:\mysettings\test.sdb /CFG C:\mysettings\baseline.inf /log`.
13. Anyone can schedule a task by using the Task Scheduler; however, the user's code will execute only if the user has the proper access rights and privileges. Only an administrator can use the `AT` command, which runs under the security context of the Task Scheduler service.
14. The security settings in group policy are automatically refreshed, regardless of changes, every 16 hours, and a SceCli event 1704 is written to the event log.
15. All GPOs are created in a domain and then linked to the chosen site, domain, or OU.
16. GPOs are applied locally and then from the site, from the domain, and from the OU.
17. Block policy inheritance blocks settings from the GPOs being applied; however, the No Override setting enforces security settings.
18. To ensure that the user settings from the computer's GPO are always applied, no matter what user logs on, you use loopback processing.
19. If several GPOs are linked to the domain or to a single OU, the order in which they are applied starts at the bottom of the list and ends at the top of the list. In other words, the GPO at the top of the list is the last one applied.
20. Additional security should be added for IISs, including the use of URLScan and the IIS Lockdown tool.
21. You can gain additional security for client systems by using group policy (administrative templates), by directly modifying the registry, by modifying the schema, and by identifying security zones.
22. To enable Windows Installer to install programs using system privileges, you must set group policy to allow this in both the user and computer administrative templates.
23. Preferences (made by users) directly edit the registry, whereas policies create settings in the Policy branch of the registry. Policies override preferences.
24. If settings are made in both the computer and user administrative templates, in most cases the computer setting takes precedence when there is a conflict.
25. The Windows Update service is an online service that can be used to update Windows computers. Windows XP Dynamic Update is a service that runs only at the beginning of a Windows XP installation.
26. MBSA uses a custom version of `hfnetchk` and downloads a current copy of the `mssecure.xml` file from Microsoft. MBSA then scans computers for common security misconfiguration and hotfix installations and reports the results.
27. Group policy software can be used to push service pack installations to existing client computers. An `update.msi` file is necessary for this.
28. When multiple hotfixes are installed using a batch file, inappropriate installation of DLLs is possible because of the way information about necessary files is managed by the update process. To resolve this issue and allow multiple updates to be installed, you should use the `qchain` utility.
29. SUS is installed on a server on the local network, and it downloads critical updates to a repository on the server. After administrator approval, the updates can be delivered to the user systems. User systems can be pointed to the SUS server instead of to Windows Update for updating.
30. BITS (which is required for clients to use SUS) may not start on Windows 2000 Server machines with Terminal Services installed. You can remove Terminal Services or set BITS to start automatically on boot.
31. To configure Automatic updates using group policy, you add the `wuau.adm` template to the GPO.
32. After an IPSec policy is assigned (that is, activated), the policy is triggered by some event. If the policy requires encryption between all hosts on a subnet, a packet with a destination address for one of these hosts triggers negotiation of a connection and, upon successful completion, encryption of the data that passes between the two hosts.
33. IPSec Phase I, Main Mode, involves authentication of hosts, sharing of data required to calculate the master key, the calculation of the master key, and the establishment of an IKE SA or secure channel.
34. IPSec Phase II, Quick Mode, consists of the use of the master key by both hosts to create session keys to be used for encryption of data and the establishment of multiple SAs, one for each protocol and direction (in or out) required by the policy.
35. IPSec authentication occurs via Kerberos, certificates, or shared secret.
36. Both ESP and AH provide data integrity, antireplay protection, and host authentication, but only ESP can provide confidentiality (via encryption).
37. The Security Method page of the IPSec rule displays the area where AH and ESP can be configured as well as how often session keys will be recreated.
38. In order for a certificate to be used by IPSec, it must be stored in a computer account machine store, contain an RSA public key with a corresponding private key that can be used for RSA signatures, be valid, and be from a trusted CA, and the CAPI module must be able to construct a valid CA chain.
39. A CA chain is the result of the computer tracing the links up a hierarchical chain of CAs to the root.
40. A CRL is a list of certificates that have been revoked. Checking this list enables a process to determine whether a valid certificate has been presented.
41. The Windows 2000 IPSec Monitor (`ipsecmon`) displays only the outbound SA. IKE negotiation cannot be seen there, either, but it can be displayed by using the `netdiag.exe /test:ipsec /v` command.
42. A log (`Oakley.log`) of IKE events is created in the `%systemroot%\debug` folder if the registry key `EnableLogging` at `HKLM\system\currentcontrolset\services\policyagent\Oakley` is set to `1` and if the IPSec policy agent and related IPSec services are reset.
43. IPSec in Windows 2000 does not work with NAT.
44. 802.11 WLANs only use device identification, not authentication.
45. 802.1x uses EAP for authentication message exchange. EAP can be EAP-TLS (for certificates and smart cards), PEAP with EAP-MS-CHAP (for passwords), or PEAP with EAP-TLS (for protected EAP encryption information, such as the certificate information, to provide better protection).
46. Security for WLANs can be improved by using a unique SSID, by preventing broadcasting of the SSID, by enabling WEP, by using MAC address filtering, by requiring VPNs, and by using RADIUS and 802.1x.

47. SSL can be required or merely supported, depending on Web site configuration.
48. Client certificates can be mapped to accounts in IIS or mapped to Active Directory accounts.
49. You enable LDAPS (in which communications are encrypted) by installing properly formatted certificates.
50. Both OWA and SMTP client access to email can be secured by using SSL.
51. You should not require every Exchange virtual directory to require certificates. Instead, you should merely require SSL usage on the Exchange virtual roots (Exchange and Public).
52. The Kerberos Policy Enforce User Logon Restrictions option forces the KDC to validate requests for session tickets by verifying that the user has the right to log on locally or to access from the network and that the account is still valid.
53. The authenticator is unique material that accompanies ticket requests and resource access requests. It is used to prevent replay attacks.
54. Ticket information is cached on the client in volatile memory, where only processes running in the LSA's security context can access it. This memory is never paged to disk, and the objects stored there are destroyed when the user logs off or the system is shut down.
55. To access resources in remote domains of the forests, a service ticket is obtained by following a referral chain. Parent and child domains share interdomain keys and can thus pass requests up or down until the required TGT can be acquired.
56. Lack of access to a domain controller, lack of trust, or exceeding clock skew time may be the reason for authentication failure.
57. LM separates a password into two seven-character segments and converts them to uppercase.
58. NTLM does an MD4 hash of the entire password, preserving the case.
59. Use of NTLMv2 allows configuration that can eliminate the use of the LM password in the challenge.
60. Loading the Active Directory client on Windows 9x allows selection and use of NTLMv2 by these clients.
61. A private/public key pair stored on a smart card is used instead of a shared secret key, which is derived from a user password.
62. You can give trusted users from nontrusted domains certificates and provide access to them by mapping their certificates to Windows 2000 domain accounts.
63. The `ksetup` command is used to configure Kerberos realms, `ktpass` to set a password, `klist` to examine the Kerberos credentials cache, and `gssclient` and `gssserver` to test RFC 1964 interoperability.
64. Services running on Unix systems can be configured with the service instance account in Active Directory so that they are accessible to Kerberos clients.
65. Unix clients and services can authenticate to the Windows 2000 domain, and Windows 2000 clients can authenticate the Kerberos services that support the GSS API.
66. By default, Windows 2000 requires all accounts to use preauthentication.
67. Digest authentication is not as secure as Integrated Windows authentication because the user's password must be saved in the database of the Windows 2000 domain controller as reversible encrypted text.
68. MS-CHAPv2 is a more secure protocol than CHAP and MS-CHAP: It does not allow LM-encoded responses or password changes; it provides mutual authentication; it uses a different cryptographic key for each connection; and it uses different keys for data traveling in different directions.
69. Windows XP can be configured for remote help. A connection is established after the client issues an invitation and provides a helper that has password access.
70. A PPTP VPN cannot use certificates for authentication, cannot provide data integrity or data authentication, and must use MS-CHAP or MS-CHAPv2 in order to provide MPPE encryption.
71. An L2TP VPN can protect all PPP authentication types, uses IPSec for encryption, and provides data integrity and data authentication.
72. If the root CA of the CAs that issued server and client certificate differs, each computer must have a copy of the root CA certificate of the hierarchy of the issuing CA for the other computer in their own Trusted Root CA certificate store.
73. In a router-to-router configuration, the user account that is present and identified in the connection on one server must be entered on the other server.
74. After a network connection is configured, a route must be added to each server to allow access by clients to the internal subnets.
75. One IAS server can be used by multiple RRAS servers. Thus, remote access policies and accounting can be centralized.
76. Firewall input and output filters must be configured to use UDP port 500, to allow IKE traffic to and from the VPN server, and protocol ID 50, to allow IPSec traffic to and from the VPN server.
77. To configure a firewall to allow PPTP traffic, you need to configure filters for TCP port 1723 for tunnel maintenance traffic and protocol ID 47 to allow tunneled data.
78. The default RRAS policy says that all users may have access if their accounts are configured for dial-up access. (By default, no account is configured with dial-up access.)
79. Remote access policies consist of conditions (authentication type, called station, IP address of client, and day and time restrictions) and profile settings (session idle disconnect, encryption settings, and packet filters).
80. Although one Windows 2000 CA can perform all the services that are necessary, best practices dictate the use of multiple CAs for security reasons, for resilience, and to distribute loads.
81. CSPs are the algorithms that perform encryption and decryption.
82. A CA hierarchy consists of a root CA, intermediate CAs (which receive their CA certificates from the root and are used only to issue CA certificates), and issuing CAs (which actually issue certificates for use by users or computers).
83. The CA certificate can be downloaded from the location embedded in the certificate and specified in the AIA.
84. It is possible that information on revoked certificates will not be available immediately after revocation due to cached CRLs that have not expired.
85. Certificate trusts lists are used to indicate limited trust for certificates.
86. If Windows 2000 Enterprise CA is used to issue certificates for users and computers, the certificates are automatically bound to the user account and published in Active Directory. Certificates produced otherwise can be mapped to an account in Active Directory.
87. The presence of IIS is critical. If you restore a CA to a server on which the IIS metabase is corrupt or missing, because IIS cannot start, the CA will not start.
88. The earlier version of KMS generated its own certificates. X.509 version 3 S/MIME certificates can be generated only by KMS for Microsoft Outlook 98 and above. S/MIME certificates for Outlook Express and other clients may be obtained through the Web enrollment pages of the CA.
89. The private signing key is never transmitted to or stored in the KMS because if it were, there would always be the possibility that a message could be signed by someone other than the person who should be able to sign it.
90. Windows XP does not automatically create an EFS recovery agent. Although Windows XP–based EFS can use a recovery agent if one is present, by default it does not.
91. To place EFS-encrypted files on a file server, first the file server must be trusted for delegation, as must the user's account. Second, the file server must have a copy of the user's EFS certificate and private key.
92. Windows XP–encrypted files can be stored using WebDAV. The remote computer does not need to be trusted for delegation, nor does a copy of the user's profile need to reside there because all encryption and decryption occurs on the user's computer. Files stored remotely using WebDAV remain encrypted as they traverse the network.
93. With Windows XP it is possible to share encrypted files. The encryptor of a file can allow others to encrypt and decrypt his or her files. To do so, the encryptor merely has to make his or her certificate available on his system and select it through the file property page.
94. To disable EFS in Windows XP, you must change the registry value `EfsConfiguration` to `1` at `HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\EFS`.
95. To disable EFS for Windows 2000, you remove the recovery agent certificate. When there is no recovery agent, there is no encryption.
96. The default audit policy of the domain controller security policy sets all audit categories to No Auditing. This policy overrides any audit policy that is enabled in the local security policy of domain member workstations and servers.
97. To match event 528 (successful logon) or event 540 (successful network logon) to a logoff (event 538), you use the logon ID number that is part of these events.
98. You should filter for events 528 or 540, in which the domain name matches the computer name; this means that a local SAM account was used to log on.
99. A large number of successful events with event ID 540 can be ignored, for the most part, because they represent network logons such as those used when mapping a drive.
100. Looking for successful logons, 528 (interactive) and 540 (network), that occur after a number of failed logons can signal a successful attack.
101. When user accounts are disabled and then deleted (events 629 and 630), you should determine whether it is legitimate or whether it is an attacker covering tracks.
102. If a disabled account is enabled (event 626) and then disabled (event 629) soon after, this could be evidence of an attack.
103. Object audit events are written to the logs when the object handle is accessed, not when the object is actually manipulated.
104. You should look for legitimate, clean shutdown preceding startup. An unplanned shutdown could be evidence of an attack. Event 6006 indicates that the event log service was stopped. Event 6008 indicates an unexpected restart.