



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Securing Windows and PowerShell Automation (Security 505)"
at <http://www.giac.org/registration/gcwn>

Auditing the Windows 2000 Authentication Process

Apr 01,2001

Author: **Julio Silveira**

© SANS Institute 2000 - 2005, Author retains full rights.

Contents

<u>1</u>	<u>Introduction:</u>	3
<u>2</u>	<u>The W2K authentication Process:</u>	3
<u>2.1</u>	<u>Let's talk a little bit about LM, NTLM and NTLM v2:</u>	3
<u>2.1.1</u>	<u>How does the LM / NTLM / NTLMv2 authentication process work?</u>	4
<u>2.1.2</u>	<u>The differences between LM / NTLM and NTLMv2:</u>	4
<u>2.1.3</u>	<u>How W2K uses LM/ NTLM and NTLMv2?</u>	6
<u>2.2</u>	<u>Let's talk about Kerberos:</u>	6
<u>2.2.1</u>	<u>How Kerberos works:</u>	7
<u>2.3</u>	<u>Kerberos Implementation in Windows 2000:</u>	9
<u>2.3.1</u>	<u>Multiple domains</u>	11
<u>2.3.2</u>	<u>Mixed environment</u>	12
<u>3</u>	<u>Security Events Created in the W2K Authentication Process:</u>	12
<u>4</u>	<u>How to capture security events</u>	13
<u>4.1</u>	<u>Setting the Log Size and the Retention Period:</u>	14
<u>4.2</u>	<u>Setting the Audit Policy</u>	15
<u>5</u>	<u>How to view the events</u>	18
<u>6</u>	<u>Lab: Authentication events :</u>	19
<u>6.1</u>	<u>Success logon events:</u>	19
<u>6.1.1</u>	<u>Interactive logon on W2K servers:</u>	19
<u>6.1.2</u>	<u>Interactive logon on NT4 servers :</u>	23
<u>6.1.3</u>	<u>Network logon from W2K server to W2K</u>	24
<u>6.1.4</u>	<u>Network logon from W2K to NT4</u>	25
<u>6.1.5</u>	<u>Network logon from NT4 to W2K</u>	27
<u>6.2</u>	<u>Failed logon events:</u>	28
<u>6.2.1</u>	<u>Interactive logon on W2K servers:</u>	28
<u>6.2.2</u>	<u>Interactive logon on NT4 servers :</u>	31
<u>6.2.3</u>	<u>Network logon from W2K server to W2K</u>	32
<u>6.2.4</u>	<u>Network logon from W2K to Nt4</u>	34
<u>6.2.5</u>	<u>Network logon from NT4 to W2K</u>	37
<u>7</u>	<u>Archiving and Analyzing security events:</u>	39
<u>7.1</u>	<u>Real time Analyzes:</u>	39
<u>7.2</u>	<u>Archiving and Reports:</u>	42
<u>7.2.1</u>	<u>Step 1 : Dump the security logs in a txt file</u>	42
<u>7.2.2</u>	<u>Step 2: Import the data (text files) to a SQL 2000 DB:</u>	42
<u>7.2.3</u>	<u>Step 3 : Create reports</u>	48
<u>8</u>	<u>Bibliography:</u>	51

2 Introduction:

This paper will describe the Windows 2000 authentication process, and how to collect and use the security events created in the authentication process in order to audit your system.

This is mainly a practical validation of the information collected from several publications about Windows 2000 authentication. The source of the information is not referenced directly in the text; it is listed in the bibliography.

3 The W2K authentication Process:

Kerberos is the default authentication method for network logon among Windows 2000 systems, but W2K also supports LM, NTLM and NTLMv2 in order to keep backwards compatibility.

3.1 *Let's talk a little bit about LM, NTLM and NTLM v2:*

Prior to Windows NT 4.0 Service Pack 4 (SP4), Windows NT supported two kinds of challenge/response authentication:

- LanManager (LM) challenge/response (NT supports this authentication protocol in order to keep backward compatibility with Lan Manager clients on DOS, Windows for Workgroup and Windows 95)
- Windows NT challenge/response (also known as NTLM challenge/response)

To allow access to servers that only support LM authentication, Windows NT clients prior to SP4 always use both, even when talking to Windows NT servers supporting NTLM authentication.

The backward compatibility caused NT to inherit some significant security weaknesses from the way LM authentication protocol—hashes passwords and authenticates the network. LM authentication uses a challenge/response mechanism for logon to eliminate the need to transmit the password over the network. But LM's vulnerabilities let intruders listen on a network segment, capture the challenge/response, and crack the logon.

NT supports NTLM, but is still has the same vulnerabilities because, to support pre-NT clients and servers, it automatically sends and accepts the LM responses, which is a

dangerous weakness.

Posing a threat to NT is L0phtCrack, a popular password-cracking tool from L0pht Heavy Industries. L0phtCrack comes with a challenge/response sniffer that can capture logons as they occur on the network. Using these challenge/response pairs, L0phtCrack further exploits LM's weaknesses to recover the actual password. L0phtCrack 2.5 has an enhanced GUI sniffer integrated into the main L0phtCrack engine. The new GUI sniffer, SMB Packet Capture Output, eliminates the need for a special packet driver, which the previous version required. This tool lets even novice intruders easily learn the passwords of everyone logging on to the intruder's network segment.

With NT SP4, Microsoft released an enhancement to NTLM called NTLMv2. NTLMv2 has several enhancements that address authentication problems and session security requirements for confidentiality, integrity, and 128-bit encryption. The problem is that even with SP4, the NT clients will still use LM and NTLM by default. Users will need to change the LMCompatibilityLevel registry value, in order to control what responses the client sends to the server and what responses the server accepts. You can find more information about the LMCompatibilityLevel settings in the following places:

- <http://support.microsoft.com/support/kb/articles/q147/06/06.asp>
- Windows 2000 magazine article id 7072 (Inside sp4 NTLMv2 Security enhancements – Randy Franklin Smith)
- Alex Park's SANS practical assignment

3.1.1 How does the LM / NTLM / NTLMv2 authentication process work?

When a user needs to connect to a server, the server authenticates the user with a challenge/response protocol:

1. The server issues a random string of bytes called a *challenge* to the client.
2. The client encrypts the challenge with the hash of the user's password and sends the encrypted challenge back as the response.
3. The server decrypts the response with the official password hash stored in the user's account.
4. If the decrypted response matches the original challenge, the user is authentic.

NT clients, by default, send two responses in reply to the server's challenge: the LM response and the NTLM response

3.1.2 The differences between LM / NTLM and NTLMv2:

LM Challenge and Response:

The Lan Manager password is based on the OEM character set and is not case sensitive.

Passwords are forced to uppercase before encryption. The password can be up to 14 characters long. The first 7 bytes of the password are used to compute the first 8 bytes of the 16-byte Lan Manager One-Way Function (OWF) password. The second 7 bytes of the password are used to compute the second 8 bytes of the OWA password. (It means that the algorithm allows passwords longer than 7 characters to be attacked in 7 character chunks). A constant is encrypted using the cleartext password and DES.

During Network logons, the client is given a 16-byte challenge. The Lan Manager client encrypts the 16-byte challenge with the 16-byte Lan Manager OWF password to produce a 24-bit response. The challenge-response is passed to the NT server.

The Local Security Authority (LSA – LSASS.exe) is the one managing the NT authentication. LSA invokes the native authentication package, MSV1_0, to perform the authentication. MSV1_0.dll is in the system32 directory) MSV1_0 consists of two parts : the top half is in the client and the lower half is in the system that contains the requested domain SAM database (for a local logon, both parts are in the same computer). The client half of the MSV1_0 passes the domain name, the user name, the original challenge and the Lan Manager challenge-response to the server half of the MSV1_0 authentication package. The MSV1_0 authentication package computes its own challenge-response using the LM OWF password from the SAM and the challenge. If the result matches the challenge and response passed to it, the client is authenticated.

NTLM Challenge and Response:

The NT password is based on the Unicode character set. It is case sensitive and can theoretically be up to 128 characters long. (The NT interface limits the actual password to 14 characters.) A NT OWF password is computed using RSA MD-4 encryption to compute a 16-byte message digest of the password.

Network logon works much the same as for the Lan Manager client except the MSV1_0 authentication package on the server is passed the NT OWF in addition to the LM OWA. The MSV1_0 authentication package computes its own challenge-response using the NT OWF password from the SAM. Because the SAM stores both an LM OWF and an NT OWF, case sensitivity can be enforced when using NT, but the inclusion of both passwords allows backwards compatibility. It's this storage of the LM OWF and the passage of the LM OWF across the network that then allows cracking of the NTLM password.

NTLMv2 Challenge and Response:

The keyspace in NTLMv2 is 128 bits. It enables clients to control whether the LM OWF is created and/or used by the client and/or the server. It can prevent the LM challenge . Sessions between sp4 NT clients and sp4 NT servers can require negotiation of message

confidentiality, message integrity using separate keys, and the HMAC-MD5 algorithm (RFC 2104), 128-bit encryption, and NTLMv2 session security. These controls are implemented with registry entries. (Item 2.1 has references to it.)

It the reason that LM authentication is not as strong as NTLM or NTLMv2 because the algorithm allows passwords longer than 7 characters to be attacked in 7 character blocks. This limits the effective password strength to 7 characters drawn from the set of uppercase alphabetic, numeric, and punctuation characters, plus 32 special ALT characters.

3.1.3 How W2K uses LM/ NTLM and NTLMv2?

Windows 2000 computers are configured to use LM, NTLM, NTLMv2 or Kerberos to ensure backwards compatibility. The following table shows the possible authentication processes that might take place between the operating systems.

	Windows 95	Windows 98	Windows 95 or 98 with AD client	Windows NT	Windows 2000
Windows 95	LM	LM	LM	LM	LM
Windows 98	LM	LM	LM	LM	LM
Windows 95 or 98 with AD client	LM	LM	LM or NTLMv2	LM or NTLMv2	LM or NTLMv2
Windows NT	LM	LM	LM or NTLMv2	NTLM or NTLMv2	NTLM or NTLMv2
Windows 2000	LM	LM	LM or NTLMv2	NTLM or NTLMv2	Kerberos , NTLM or NTLMv2

3.2 Let's talk about Kerberos:

Kerberos is the default authentication process between W2K systems, and before we look at the Microsoft implementation of Kerberos, let's take a quick look at the standard:

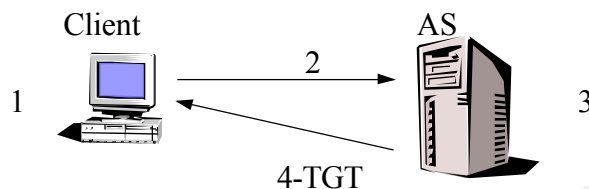
Kerberos is a distributed authentication service that allows a process (a client) running on behalf of a principal (a user) to prove its identity to a verifier (an application server, or just server) without sending data across the network that might allow an attacker or the verifier

to subsequently impersonate the principal. Kerberos optionally provides integrity and confidentiality for data sent between the client and server. Kerberos was developed in the mid-'80s as part of MIT's Project Athena. As use of Kerberos spread to other environments, changes were needed to support new policies and patterns of use. To address these needs, design of Version 5 of Kerberos (V5) began in 1989. Though V4 still runs at many sites, V5 is considered to be standard Kerberos. It is described in the IETF RFC 1510.

3.2.1 How Kerberos works:

The authentication service exchange:

It is the first action in the Kerberos authentication, when the client requests authentication:

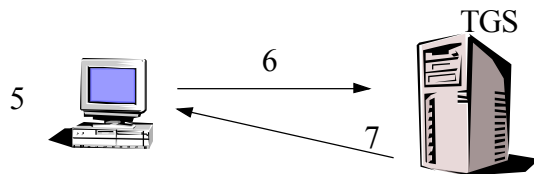


1. The user logs on by entering a user id and password.
2. The Kerberos client software prepares a message by combining this information (the password is never sent in clear text across the network) with details about the client and the Kerberos server(s). The message is sent to the Kerberos Authentication server (AS). This message is the KRB_AS_REQ.
3. The Kerberos Authentication Server looks up the client in its database, the Kerberos Key Distribution Center (KDC). The AS uses this information, as well as the information in the message, to determine how it should respond.
4. If everything is ok, the Kerberos server prepares a response (The Kerberos Authentication Server Reply, or KRB_ASREP) that includes a ticket and returns it to the client. In the standard, the ticket is either one that is useful for accessing an application server or one that can be used with a Ticket-Granting Server (TGT) to obtain a ticket to be used with the application server.

The reply data includes a ticket and some additional information. Part of the reply (the ticket) is encrypted using the key of the server to which it will be presented, and part of the response is encrypted using the client's key. The client can use the ticket and cache it for the user later or can cache it at this time.

The ticketing-Granting Service Exchange:

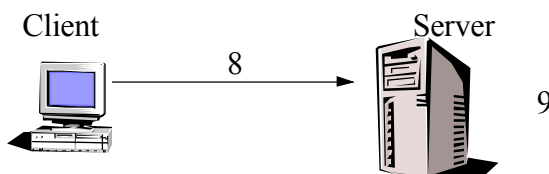
After getting the TGT steps must be taken for the user to complete his logon and work with resources in the network.



5. The user attempts to access a file or another resource on the network.
6. The Kerberos client submits the previously cached ticket to a TGS along with a request for a ticket to connect to the server that holds the file. This message is the KRB_TGS_REQ, the Kerberos Ticket-Granting Service Request.
7. The TGS can decrypt the ticket provided by the client because it is encrypted using its key. It validates the information and, if the request server is in its realm, provides a ticket to access the server in a KRB_TGS_REP (Kerberos Ticket Granting Service Reply).

The Client/Server Authentication Exchange

The whole purpose here is to allow properly authorized access to resources. That process, however, first requires proof that the user has the right to access the network, and then to pass the credentials to the file server.



8. With the appropriate ticket in hand, (included in the Kerberos Client/Server Request, or KRB_AP_REQ), the client heads for the file server.
9. After validating the ticket, the file server allows the connection. It can decrypt the ticket because the ticket has been encrypted with its key.

3.3 Kerberos Implementation in Windows 2000:

The Kerberos Distribution Center (KDC) is implemented as a domain service. It is a process that includes two services: The Authentication Service (AS) and the Ticket Granting Service (TGS). The Active Directory is used as the account database. Each domain server has a KDC; therefore, any domain controller can accept authentication requests and ticket-granting requests addressed to the domain KDC. The KDC runs in the process space of the Local Security Authority (LSA).

Windows 2000 doesn't implement the Kerberos replication protocol; it uses its own replication process.

The following will show the Windows 2000 implementation of the Authentication Service Exchange, the Ticket- Granting Service Exchange and the Client/Server Exchange.

Authentication Service (AS) Exchange

- a. User A, at a W2K machine, logs on to a Microsoft Windows 2000 network, typing the user name and password. The Kerberos client running on A's workstation converts the password to an encryption key,
- b. The Kerberos client sends a message to the Key Distribution Server (KDC), of type KRB_AS_REQ (Kerberos Authentication Server Request). This message has two parts:
 - An identification of the user, A, and the service for which he is requesting credentials, the TGS (Ticket-Granting Service)
 - Pre-authentication data, intended to prove that A knows the password. This is simply an authenticator encrypted with A's master key. The master key is generated by running A's password through an OWF.
- c. The KDC, upon receipt of KRB_AS_REQ from A, looks up the user A in its

database (the Active Directory), gets the master key, decrypts the pre-authentication data, and evaluates the time stamp inside. If the time stamp passes the test, the KDC can be assured that the pre-authentication data was encrypted with A's master key, and is not merely a captured replay.

- d. Finally, once the KDC has verified A's identity, it will create credentials that the client program on the workstation can present to the Ticket Granting Service (TGS). The credentials are created and deployed as follows
 - A brand new logon session key, encrypted with A's master key.
 - A second copy of the logon session key and A's authorization data, in a Ticket Granting Ticket (TGT), encrypted with the KDC's own master key.
 - Next, the KDC sends these credentials back to the client by replying with a message of type KRB_AS_REP (Kerberos Authentication Response).
 - When the client receives the reply, it decrypts the logon session key via application of A's master key. The session key is then stored in the client workstation's ticket cache. The TGT is extracted from the message, and stored in the cache as well.

Ticket-Granting Service (TGS) Exchange

- e. At this stage, the Kerberos client running on A's workstation is going to actually request credentials to access the target server, user B, by sending a message of type KRB_TGS_REQ (Kerberos Ticket-Granting Service Request), to the KDC. This message consists of the following components:
 - Identity of the target service for which the client is requesting credentials
 - Authenticator encrypted with the user's logon session key
 - TGT acquired from the AS Exchange
- f. The KDC decrypts the TGT with its master key, and extracts A's logon session key. A's logon session key is used to decrypt A's authenticator. If A's

authenticator passes the test, the KDC invents a new session key for A to share with B. Two copies of this new session key are sent back to A in a single message, encrypted as follows.

- One copy is encrypted using A's logon session key.
 - The second copy is encrypted using the target server's master key, in a ticket along with A's authorization data.
- g. A decrypts the target server session key, using the logon session key, and stores the session key in the cache, along with the target server ticket.

Client-Server (CS) Exchange

- h. A's Kerberos client is now ready to be authenticated by the target server, B. A's client sends B a message of type KRB_AP_REQ (Kerberos Application Request). This message contains:
- An authenticator encrypted with the session key for B
 - The ticket for sessions with B, encrypted with B's master key
 - A flag indicating whether the client requests mutual authentication.
- i. B decrypts the ticket, and extracts A's authorization data and session key. B uses the session key to decrypt A's authenticator, and evaluates the time stamp. If the authenticator passes the test, B looks for a mutual authentication flag. If this flag is set, B uses the session key to encrypt the time from A's authenticator, and returns the result to A in a message of type KRB_AP_REP (Kerberos Application Reply)
- j. A decrypts the reply with the session key. If the authenticator is identical to the one that she sent B, the client is assured that the server is genuine, and the connection proceeds.

3.3.1 Multiple domains

Authentication can be completed across domains. It is enabled by sharing an interdomain key, and it automatically happens when a trust is established between two Windows 2000 domains. A description of the process follows:

- The client in domain A wants to access a service in domain B. It will send the ticket request to the TGS in domain A.
- The TGS in domain A notices that the service resides in domain B.
- The TGS encrypts a TGT with the interdomain key it shares with domain B.
- It sends the TGT (known as the referral ticket) to the client.
- The client uses the referral ticket and sends a request for the session ticket to the TGS in domain B.
- The TGS in domain B uses its copy of the interdomain key to decrypt the ticket, and sends to the client a session ticket to the service in its domain.
- The client uses the ticket to access the resource.

On networks with more than one domain, the domains will not store interdomain keys for every domain. Each domain stores an interdomain key for the domain one step above and one step below it in the AD tree. When necessary, a referral path can be generated that enables the client to obtain referral tickets, one after another, until it obtains one for the domain it needs.

3.1.2 Mixed environment

Even in a native mode Windows 2000 domain, Kerberos is not the only Security Support Provider (SSP) for the entire network. Clients other than Windows 2000 clients will log on using other network authentication protocols, and even in a domain with only W2K machines, NTLM will still be available in case of Kerberos failure.

The application can specify a particular Security Support Provider or it can allow the SSP interface to negotiate for the most secure protocol available.

4 Security Events Created in the W2K Authentication Process:

Windows NT and Windows 2000 can be monitored in a very detailed way by enabling success and failure auditing of the "Logon" category activity in the system's Audit policy. This can generate the following events, depending on whether you are auditing successes or failures or both:

528 Successful Logon
529 Logon Failure: Reason: Unknown user name or bad password
530 Logon Failure: Reason: Account logon time restriction violation
531 Logon Failure: Reason: Account currently disabled
532 Logon Failure: Reason: The specified user account has expired
533 Logon Failure: Reason: User not allowed to logon at this computer
534 Logon Failure: Reason: The user has not been granted the requested logon type at this machine
535 Logon Failure: Reason: The specified account's password has expired
536 Logon Failure: Reason: The NetLogon component is not active
537 Logon Failure: Reason: An unexpected error occurred during logon
538 User Logoff:
539 Logon Failure: Reason: Account locked out
540 Successful Network Logon

Windows 2000 Only:

541 IPsec security association established.
542 IPsec security association ended.
Mode: Data Protection (Quick mode)
543 IPsec security association ended.
Mode: Key Exchange (Main mode)
544 IPsec security association establishment failed because peer could not authenticate.
545 IPsec peer authentication failed.
546 IPsec security association establishment failed because peer sent invalid proposal.
547 IPsec security association negotiation failed.

In each of these events, description text gives detailed information about each specific logon.

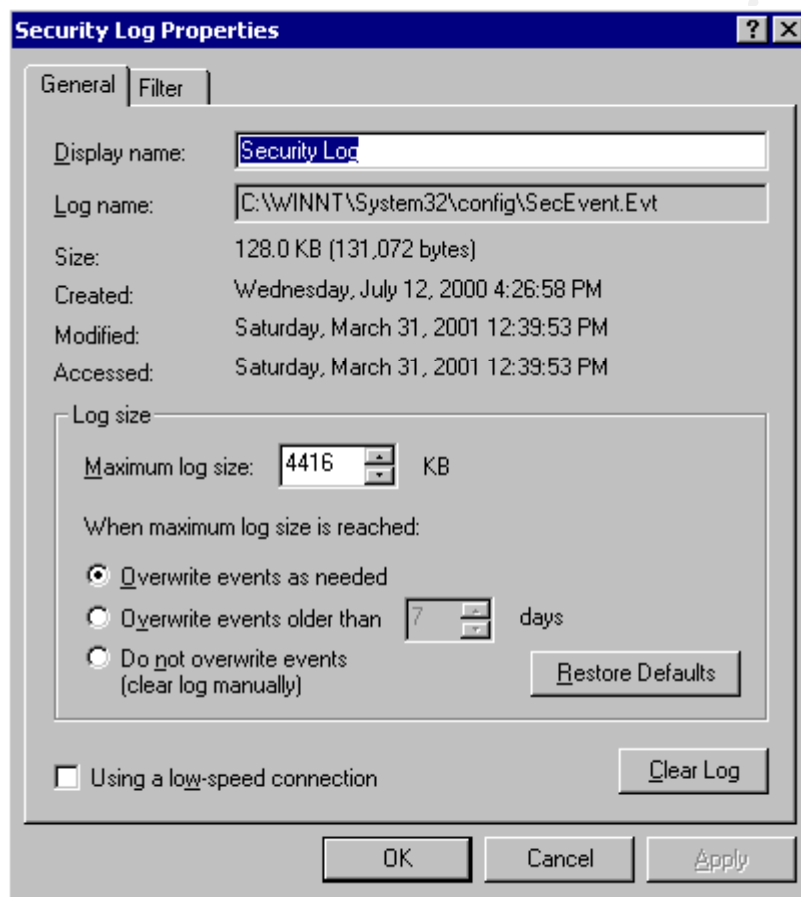
Additionally, on Windows 2000, you can enable success and failure auditing of the "Account Logon" category of events, which enables the following events:

672 Authentication Ticket Granted
673 Service Ticket Granted
674 Ticket Granted Renewed
675 Pre-authentication failed
676 Authentication Ticket Request Failed
677 Service Ticket Request Failed
678 Account Mapped for Logon
679 Account could not be mapped for logon
680 Account Used for Logon
681 The logon to account: <client name> by: <source> from workstation: <workstation> failed. The error code was: <error>
682 Session reconnected to winstation
683 Session disconnected from winstation

5 How to capture security events

Security events are not collected by default in a W2K or NT4 systems, and before you start collecting those events, you need to configure your log and archive process. There is no recipe for the best settings considering the volume of events is different from installation to installation and from server to server. I recommend that you monitor your system before deciding for the best settings.

In order to check the options you have, open the event viewer in a W2K server, right click the security log, and select Properties. Here is an example of settings in one of my servers:



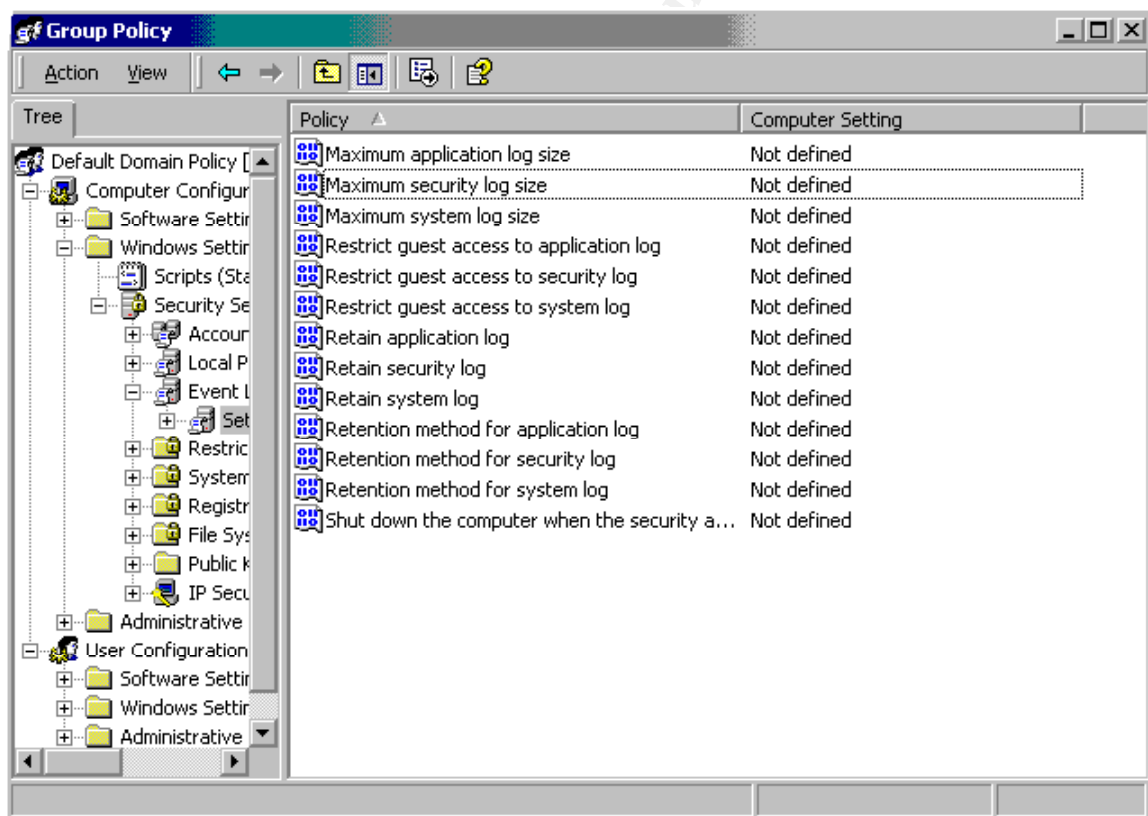
5.1 Setting the Log Size and the Retention Period:

In Win2K, Group Policy centrally controls even log settings. It fixes NT's inconvenient requirement to configure each system separately. To help you centralize settings

configuration, Group Policy offers a variety of options, including GPOs that link to OUs. Using Group Policy, you can configure multiple systems simultaneously with the same event-log settings.

The following steps will show you how to configure all the systems in your domain to have maximum Security-log size of 4032 KB and retention of 2 days:

1. Open the Active Directory Users and Computers snap-in.
2. Open your domain's Properties dialog box.
3. Go to the Group Policy tab.
4. Select the Default Domain Policy GPO, and click Edit.
5. In the left pane, go to Computer Configuration, Windows Settings, Security Settings, Event Log, Settings for Event Log



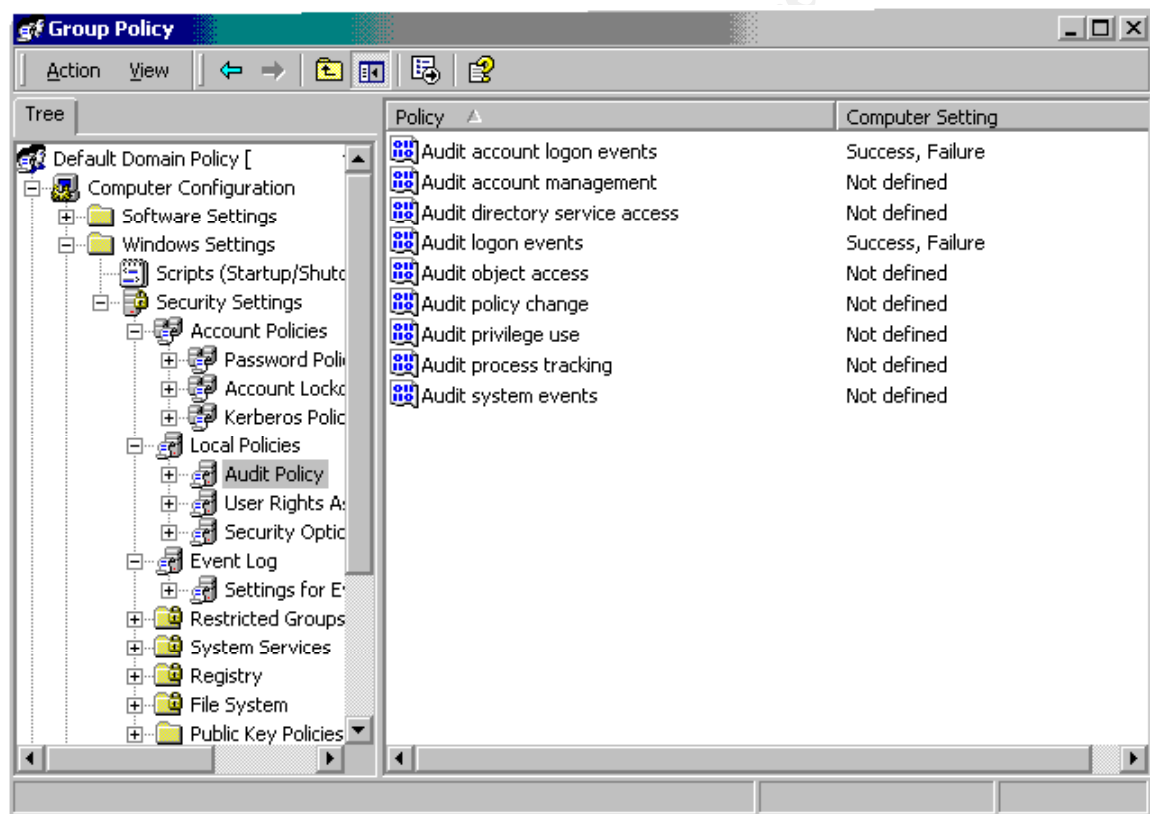
6. Right click "Maximum security log size", select Security, define a log size of 4032 KB, and then click OK.
7. Right click "Retain Security log", select Security, define retention period of 2 days, and then click OK.

8. Right click “Security Settings” and select reload.

5.2 Setting the Audit Policy

Security events are not collected by default in NT or W2K computers, so you won't see Security-log events until you activate the system's audit policy. To specify a standard audit policy for every system in your domain, you can edit the Default Domain Policy GPO.

1. Open the edit window for the Default Domain Policy GPO, and go to Computer Configuration, Windows Settings, Security Settings, Local Policies, Audit Policy.



2. Right-click an audit category and select Security.
3. Define the policy setting to audit for the success or failure of that category's event.
4. Right click “Security Settings” and select reload.

I have described how to make settings for the entire domain, but you can make different settings for groups of machines.

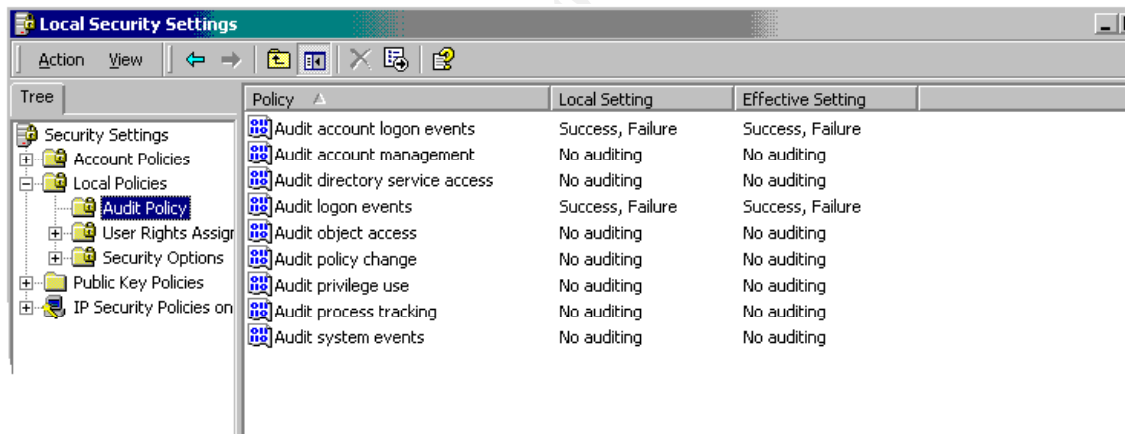
Policies will get applied at startup/logon and also at regular intervals: 60 to 120 minutes for Member servers and 5 minutes for the DC. You can also force policy refresh with the command :

`secedit /refreshpolicy machine_policy`

When Win2K applies Group Policy, it creates a composite of all the GPOs that link to a computer's site, domain, and OUs. The order the policy gets applied is:

- First local policies
- Then any sites policies
- Then any domain policies (you can have more than one policy in the domain)
- Then any OU policies (OUs can also contain OUs)

This means that settings can get misplaced. To determine a system's current audit policy, open the MMC Local Security Policy snap-in and go to Security Settings, Local Policies, Audit Policy. The important one is the Effective Setting column, which shows you the system's current settings after Win2K applies all relevant GPOs.



Tree	Policy	Local Setting	Effective Setting
Security Settings	Audit account logon events	Success, Failure	Success, Failure
Account Policies	Audit account management	No auditing	No auditing
Local Policies	Audit directory service access	No auditing	No auditing
Audit Policy	Audit logon events	Success, Failure	Success, Failure
User Rights Assign	Audit object access	No auditing	No auditing
Security Options	Audit policy change	No auditing	No auditing
Public Key Policies	Audit privilege use	No auditing	No auditing
IP Security Policies on	Audit process tracking	No auditing	No auditing
	Audit system events	No auditing	No auditing

Win2K includes three new categories: Audit logon events, Audit account logon events, and Audit directory service access. You can use the Audit logon events category to track local logon events in the same way you use NT's Logon and Logoff category; the other new categories apply to domain controllers.

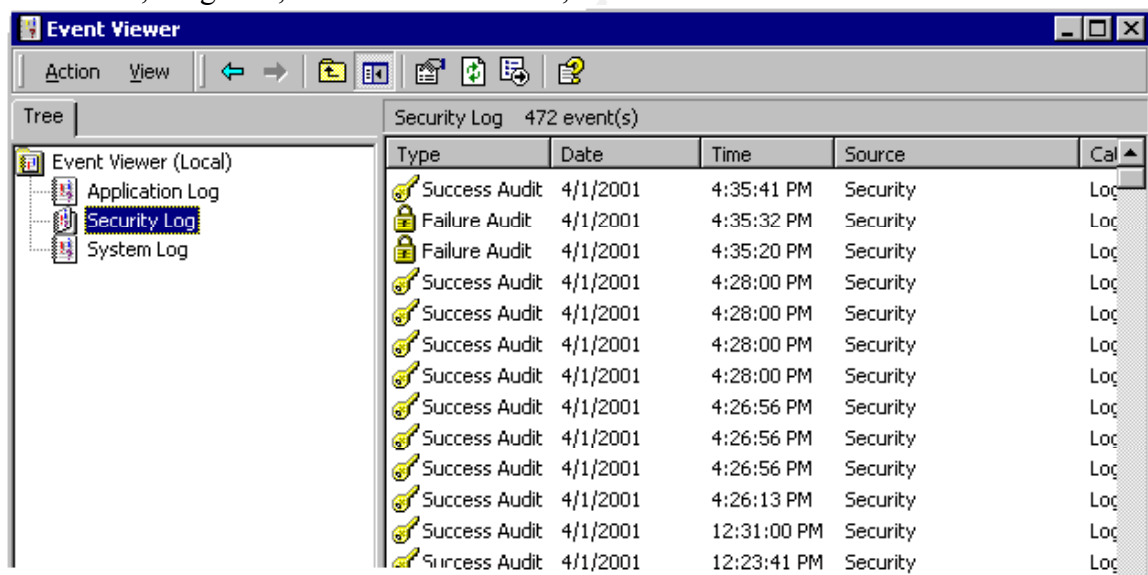
Win2K uses the Audit logon events category when a user logs on interactively or remotely. The Logon Type field in the event's description contains a number that means: interactive (2), network (3), batch (4), service (5), unlocked workstation (7), network logon using a cleartext password (8), or impersonated logons (9).

Win2K's new Audit account logon events category captures authentication events in centralized locations: on your domain controller. When a user enters a domain account to log on at a workstation, the workstation contacts the DC to verify that the user is authentic and to determine account status and restrictions. When the user then connects to a server over the network, the DC again provides authentication service.

6 How to view the events

To view the Security log events , use Event Viewer:

Click Start, Programs, Administrative Tools, Event Viewer:



You can also create custom consoles. For example, you can add a copy of the Event Viewer snap-in for each system you need to monitor.

Type	Date	Time	Source	Category	Event	User
Success Audit	4/1/2001	12:03:55 PM	Security	Account ...	680	SYSTEM
Failure Audit	4/1/2001	12:03:55 PM	Security	Account ...	677	SYSTEM
Success Audit	4/1/2001	12:03:52 PM	Security	Logon/Lo...	538	SYSTEM
Success Audit	4/1/2001	12:03:45 PM	Security	Account ...	673	SYSTEM
Success Audit	4/1/2001	12:03:43 PM	Security	Logon/Lo...	538	SYSTEM
Success Audit	4/1/2001	12:03:43 PM	Security	Logon/Lo...	540	SYSTEM
Success Audit	4/1/2001	12:03:43 PM	Security	Logon/Lo...	538	SYSTEM
Success Audit	4/1/2001	12:03:43 PM	Security	Logon/Logoff	540	SYSTEM
Success Audit	4/1/2001	12:03:40 PM	Security	Logon/Lo...	538	SYSTEM
Success Audit	4/1/2001	12:03:40 PM	Security	Logon/Lo...	540	SYSTEM
Success Audit	4/1/2001	12:03:40 PM	Security	Logon/Lo...	538	SYSTEM
Success Audit	4/1/2001	12:03:40 PM	Security	Logon/Lo...	540	SYSTEM
Success Audit	4/1/2001	12:03:39 PM	Security	Logon/Lo...	538	SYSTEM
Success Audit	4/1/2001	12:03:39 PM	Security	Logon/Lo...	540	SYSTEM
Success Audit	4/1/2001	12:03:39 PM	Security	Logon/Lo...	538	SYSTEM
Success Audit	4/1/2001	12:03:39 PM	Security	Logon/Lo...	540	SYSTEM
Success Audit	4/1/2001	12:03:38 PM	Security	Logon/Lo...	538	QEL016\$
Success Audit	4/1/2001	12:03:38 PM	Security	Logon/Lo...	540	QEL016\$
Success Audit	4/1/2001	12:03:38 PM	Security	Account ...	673	SYSTEM
Success Audit	4/1/2001	12:03:38 PM	Security	Logon/Lo...	540	QEL016\$
Success Audit	4/1/2001	12:03:38 PM	Security	Account ...	673	SYSTEM

7 Lab: Authentication events :

In order to verify the security events created when the audit logon events and audit account logon events are turned on, I set up a lab with a Windows 2000 domain controller, Windows 2000 member servers, NT 4 member servers, NT 4 Workstations and W2K Professional. The events on Workstation and Professional are similar to the server events, so I will show only the events in the following machines:

W2K DC for domain SANS : machine SANS034

W2K member server: machine SANS016

W2K member server: machine SANS009

NT4 member server: machine SANS007

NT4 member server: machine SANS021

Let's take a look in the events and I will add some comments about things that may help during the audit process.

7.1 Success logon events:

7.1.1 Interactive logon on W2K servers:

The audit logon events category is reporting events 528 (type 2: interactive) in the local W2K server for success logins and events 538 for logoff.

The following 528 and 538 events are from a logon with a local account. Note that the domain name is the computer name, and it is one way to identify logins using local account. For some installations, login using a local account, mainly administrator account, means a security breach.

Event Type: Success Audit
Event Source: Security
Event Category: Logon/Logoff
Event ID: 528
Date: 3/18/2001
Time: 12:13:52 PM
User: SANS009\juliole
Computer: SANS009
Description:
Successful Logon:
 User Name: juliole
 Domain: SANS009
 Logon ID: (0x0,0x4874B)
 Logon Type: 2
 Logon Process: User32
 Authentication Package: Negotiate
 Workstation Name: SANS009

Event Type: Success Audit
Event Source: Security
Event Category: Logon/Logoff
Event ID: 538
Date: 3/18/2001
Time: 12:17:11 PM
User: SANS009\juliole
Computer: SANS009
Description:
User Logoff:
 User Name: juliole
 Domain: SANS009
 Logon ID: (0x0,0x4874B)
 Logon Type: 2

The following event is from a logon using a domain account:

Event Type: Success Audit
Event Source: Security
Event Category: Logon/Logoff
Event ID: 528
Date: 3/18/2001
Time: 12:56:38 PM
User: SANS\sans1
Computer: SANS016
Description:
Successful Logon:
 User Name: sans1
 Domain: SANS
 Logon ID: (0x0,0xAC8F)
 Logon Type: 2
 Logon Process: User32
 Authentication Package: Negotiate
 Workstation Name: SANS016

Each session starts with an event 528 and ends with an event 538, and they can be related by the logonID, so it makes it easy to create reports showing how long the user has been logged on.

The Audit Account logon category is reporting the Kerberos authentication events in the Domain Controller when login with a domain account:

Event Type: Success Audit
Event Source: Security
Event Category: Account Logon
Event ID: 672
Date: 3/18/2001
Time: 12:56:38 PM
User: NT AUTHORITY\SYSTEM
Computer: SANS034
Description:
Authentication Ticket Granted:
 User Name: sans1
 Supplied Realm Name: SANS
 User ID: SANS\sans1
 Service Name: krbtgt
 Service ID: SANS\krbtgt
 Ticket Options: 0x40810010
 Ticket Encryption Type: 0x17
 Pre-Authentication Type: 2
 Client Address: 10.45.15.16

These events happen when the server or workstation contacts a local DC and requests a TGT. If the username and password are correct, the DC grants the TGT and logs event ID 672 (authentication ticket granted).

Note that the User field for this event won't help you to determine who the user was because the field always reads SYSTEM. You should look at the User Name field

One field that is extremely useful is the Client Address, which identifies the IP address of the workstation from which the user logged on. All Kerberos events, including failed logon attempts, include Client Address. In NT, you can track failed logon attempts for an individual system, but you have no idea where the attempts are coming from. In Win2K, you not only have centralized logon activity records on DCs but also can tell where the logon events originate.

After an event 672 there is an event 673:

Event Type: Success Audit
Event Source: Security
Event Category: Account Logon
Event ID: 673
Date: 3/18/2001
Time: 12:56:38 PM
User: NT AUTHORITY\SYSTEM
Computer: SANS034
Description:
Service Ticket Granted:
 User Name: sans1
 User Domain: SANS.SEC01.LOCAL
 Service Name: SANS016\$
 Service ID: SANS\SANS016\$
 Ticket Options: 0x40810010
 Ticket Encryption Type: 0x17
 Client Address: 10.45.15.16

Event ID 672 lets you track initial logons through the granting of TGTs. Event ID 673 (service ticket granted) lets you monitor the granting of service tickets. In this case the service ticket granting was to access the local server.

Event 672 just indicates that you got your authentication, but you still don't have access to any system. Note that in the previous examples, the server after getting the TGT immediately requested a service ticket (event 673), so the user would be able to use the local server.

When I tried to access another server I got another 673:

Event Type: Success Audit
Event Source: Security

Event Category: Account Logon
Event ID: 673
Date: 3/18/2001
Time: 12:56:38 PM
User: NT AUTHORITY\SYSTEM
Computer: SANS034
Description:
Service Ticket Granted:
 User Name: SANS016\$
 User Domain: SANS.SEC01.LOCAL
 Service Name: SANS034\$
 Service ID: SANS\SANS034\$
 Ticket Options: 0x40810010
 Ticket Encryption Type: 0x17
 Client Address: 10.45.15.16

When login with a local account, event 680 is getting recorded in the local W2K server:

Event Type: Success Audit
Event Source: Security
Event Category: Account Logon
Event ID: 680
Date: 3/18/2001
Time: 12:13:52 PM
User: NT AUTHORITY\SYSTEM
Computer: SANS009
Description:
Account Used for Logon by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Account Name:
 juliole
Workstation:
 SANS009

7.1.2 Interactive logon on NT4 servers :

Like in a W2K logon, the audit logon events category is reporting events 528 (type 2 : interactive) in the local NT4 server for success logins and events 538 for logoff :

Event Type: Success Audit
Event Source: Security
Event Category: Logon/Logoff
Event ID: 528

Date: 3/18/2001
Time: 1:06:07 PM
User: SANS\sans1
Computer: SANS021
Description:
Successful Logon:
 User Name: sans1
 Domain: SANS
 Logon ID: (0x0,0x2DAB42)
 Logon Type: 2
 Logon Process: User32
 Authentication Package:
 MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
 Workstation Name: SANS021

NT 4 does not use Kerberos, so the Audit Account logon category is reporting the event 680 in the Domain Controller when login with a domain account:

Event Type: Success Audit
Event Source: Security
Event Category: Account Logon
Event ID: 680
Date: 3/18/2001
Time: 1:12:33 PM
User: NT AUTHORITY\SYSTEM
Computer: SANS034
Description:
Account Used for Logon by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Account Name:
 sans1
Workstation:
 SANS021

7.1.3 Network logon from W2K server to W2K

The audit logon events category is reporting events 540 (type 3 : network) in the W2K server for success network logon.

NT 4 uses event 528 for every type of logon. W2K uses event 540 for network logons and event 528 for the other logons. This event allows us to separate network logons from the other logons :

Event Type: Success Audit
Event Source: Security
Event Category: Logon/Logoff
Event ID: 540

Date: 3/18/2001
Time: 2:17:55 PM
User: SANS\admsans
Computer: SANS009
Description:
Successful Network Logon:
 User Name: admsans
 Domain: SANS
 Logon ID: (0x0,0x4AAF2)
 Logon Type: 3
 Logon Process: Kerberos
 Authentication Package: Kerberos
 Workstation Name:

Note that the logon process is Kerberos. The two machines are W2K.

The Audit Account logon category is reporting the Kerberos authentication event 673 in the W2K DC. The user already has the TGT and it requests the service ticket:

Event Type: Success Audit
Event Source: Security
Event Category: Account Logon
Event ID: 673
Date: 3/18/2001
Time: 2:17:55 PM
User: NT AUTHORITY\SYSTEM
Computer: SANS034
Description:
Service Ticket Granted:
 User Name: admsans
 User Domain: SANS.SEC01.LOCAL
 Service Name: SANS009\$
 Service ID: SANS\SANS009\$
 Ticket Options: 0x40810010
 Ticket Encryption Type: 0x17
 Client Address: 10.45.15.16

We can tell by the client address that it was machine SANS016 accessing machine SANS009. SANS034 is the DC, where the event got logged.

7.1.4 Network logon from W2K to NT4

The audit logon events category is reporting events 528 (type 3 : network) in the NT 4

servers for success network logon:

Event Type: Success Audit
Event Source: Security
Event Category: Logon/Logoff
Event ID: 528
Date: 3/18/2001
Time: 1:50:32 PM
User: SANS\admsans
Computer: SANS021
Description:

Successful Logon:

User Name: admsans
Domain: SANS
Logon ID: (0x0,0xE139)
Logon Type: 3
Logon Process: KSecDD
Authentication Package:
MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Workstation Name: \\SANS016

The Audit Account logon category is reporting the Kerberos authentication event 677 in the W2K DC. The user admsans was trying to connect from a W2k machine to a NT server, and the W2k is requesting a service ticket but it fails because the NT4 server does not support Kerberos.

Event Type: Failure Audit
Event Source: Security
Event Category: Account Logon
Event ID: 677
Date: 3/18/2001
Time: 1:56:42 PM
User: NT AUTHORITY\SYSTEM
Computer: SANS034
Description:

Service Ticket Request Failed:

User Name: admsans
User Domain: SANS.SEC01.LOCAL
Service Name: HOST/SANS021
Ticket Options: 0x40810010
Failure Code: 7
Client Address: 10.45.15.16

This error is transparent to the user, because the W2K will try NTLM, and event 680 gets logged in the DC:

Event Type: Success Audit

Event Source: Security
Event Category: Account Logon
Event ID: 680
Date: 3/18/2001
Time: 1:56:42 PM
User: NT AUTHORITY\SYSTEM
Computer: SANS034
Description:
Account Used for Logon by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Account Name:
admsans
Workstation:
\\SANS016

7.1.5 Network logon from NT4 to W2K

Now it is a NT4 server accessing a W2K share, so the NT4 will use NTLM.

The audit logon events category is reporting events 540 (type 3 : network) in the W2K server for success network logon. Recall that W2K logs 540 instead of 528 for Network logon.

Event Type: Success Audit
Event Source: Security
Event Category: Logon/Logoff
Event ID: 540
Date: 3/18/2001
Time: 2:04:54 PM
User: SANS\admsans
Computer: SANS016
Description:
Successful Network Logon:
User Name: admsans
Domain: SANS
Logon ID: (0x0,0x1BFC5)
Logon Type: 3
Logon Process: NtLmSsp
Authentication Package: NTLM
Workstation Name: \\SANS021

NT 4 does not use Kerberos, so the Audit Account logon category is reporting the event 680 in the Domain Controller when login with a domain account:

Event Type: Success Audit
Event Source: Security
Event Category: Account Logon

Event ID: 680
Date: 3/18/2001
Time: 2:04:54 PM
User: NT AUTHORITY\SYSTEM
Computer: SANS034
Description:
Account Used for Logon by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Account Name:
admsans
Workstation:
\\SANS021

We have seen the success logon events, and these events are normally used in order to create reports showing who has been accessing the network, but the most important events for auditing are the failed logon events.

7.2 Failed logon events:

7.2.1 Interactive logon on W2K servers:

The audit logon events category is reporting events 529 in the local W2K server when an invalid local user or invalid password are entered:

Event Type: Failure Audit
Event Source: Security
Event Category: Logon/Logoff
Event ID: 529
Date: 3/18/2001
Time: 12:20:31 PM
User: NT AUTHORITY\SYSTEM
Computer: SANS009
Description:
Logon Failure:
Reason: Unknown user name or bad password
User Name: fakeuser
Domain: SANS009
Logon Type: 2
Logon Process: User32
Authentication Package: Negotiate
Workstation Name: SANS009

The Audit Account logon category is logging event 681 in the local W2K, when an invalid local user or an invalid password is entered.

Bad user:

Event Type: Failure Audit
Event Source: Security
Event Category: Account Logon
Event ID: 681
Date: 3/18/2001
Time: 12:20:31 PM
User: NT AUTHORITY\SYSTEM
Computer: SANS009

Description:

The logon to account: fakeuser
by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
from workstation: SANS009
failed. The error code was: 3221225572

Bad password:

Event Type: Failure Audit
Event Source: Security
Event Category: Account Logon
Event ID: 681
Date: 3/18/2001
Time: 12:18:20 PM
User: NT AUTHORITY\SYSTEM
Computer: SANS009

Description:

The logon to account: julirole
by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
from workstation: SANS009
failed. The error code was: 3221225578

Note that the error code is different, and it means:

Error Code	Hexadecimal Value Error Code	Cause
3221225572	C0000064	User logon with misspelled or bad user account
3221225578	C000006A	User logon with misspelled or bad password
3221225583	C000006F	User logon outside authorized hours
3221225584	C0000070	User logon from unauthorized workstation
3221225585	C0000071	User logon with expired password
3221225586	C0000072	User logon to account disabled by administrator

3221225875	C0000193	User logon with expired account
3221226020	C0000224	User logon with "Change Password at Next Logon" flagged
3221226036	C0000234	User logon with account locked

When entering an invalid domain account, the Audit Account logon category also logs two different events in the DC. It logs event 675 with failure code 24 when the password is invalid, and event 676 with failure code 6 when the domain account is invalid:

Event Type: Failure Audit
Event Source: Security
Event Category: Account Logon
Event ID: 675
Date: 3/18/2001
Time: 12:54:01 PM
User: NT AUTHORITY\SYSTEM
Computer: SANS034
Description:
Pre-authentication failed:

User Name: sans1
User ID: SANS\sans1
Service Name: krbtgt/SANS
Pre-Authentication Type: 0x2
Failure Code: 24
Client Address: 10.45.15.16

Event Type: Failure Audit
Event Source: Security
Event Category: Account Logon
Event ID: 676
Date: 3/18/2001
Time: 1:02:41 PM
User: NT AUTHORITY\SYSTEM
Computer: SANS034
Description:
Authentication Ticket Request Failed:

User Name: fakeuser
Supplied Realm Name: SANS
Service Name: krbtgt/SANS
Ticket Options: 0x40810010
Failure Code: 6
Client Address: 10.45.15.16

Note that in addition to user name and domain, the event has the IP address of the system from which the logon attempt originated.

7.2.2 Interactive logon on NT4 servers :

Like in a W2K logon, the audit logon events category is reporting events 529 in the local NT4 server when we try an invalid user or password (local or domain account):

Event Type: Failure Audit
Event Source: Security
Event Category: Logon/Logoff
Event ID: 529
Date: 3/18/2001
Time: 1:03:08 PM
User: NT AUTHORITY\SYSTEM
Computer: SANS021
Description:
Logon Failure:
Reason: Unknown user name or bad password
User Name: juliotre
Domain: SANS021
Logon Type: 2
Logon Process: User32
Authentication Package:
MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Workstation Name: SANS021

The Audit Account logon category is reporting the event 681 in the Domain Controller when there is an invalid login with a domain account:

Invalid password:

Event Type: Failure Audit
Event Source: Security
Event Category: Account Logon
Event ID: 681
Date: 4/1/2001
Time: 12:20:53 PM
User: NT AUTHORITY\SYSTEM
Computer: QEL034
Description:
The logon to account: admsans
by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
from workstation: QEL021
failed. The error code was: 3221225578

Invalid user:

Event Type: Failure Audit
Event Source: Security
Event Category: Account Logon
Event ID: 681
Date: 4/1/2001
Time: 12:21:30 PM
User: NT AUTHORITY\SYSTEM
Computer: QEL034
Description:

The logon to account: admsan
by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
from workstation: QEL021
failed. The error code was: 3221225572

The error code is different for bad user and bad password. See the table with the error codes for event 681 in the item 6.2.1.

7.2.3 Network logon from W2K server to W2K

The audit logon events category is reporting events 529 for invalid password or invalid user:

Event Type: Failure Audit
Event Source: Security
Event Category: Logon/Logoff
Event ID: 529
Date: 3/30/2001
Time: 11:06:47 AM
User: NT AUTHORITY\SYSTEM
Computer: SANS009
Description:

Logon Failure:
Reason: Unknown user name or bad password
User Name: admxxx
Domain: SANS
Logon Type: 3
Logon Process: NtLmSsp
Authentication Package:
MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Workstation Name: SANS016

The Audit Account logon category is reporting the event 676 failure code 6 in the

Domain Controller for invalid domain user. It is also reporting event 681 in the DC:

Event Type: Failure Audit
Event Source: Security
Event Category: Account Logon
Event ID: 676
Date: 3/30/2001
Time: 11:06:47 AM
User: NT AUTHORITY\SYSTEM
Computer: SANS034
Description:

Authentication Ticket Request Failed:

User Name: admxxx
Supplied Realm Name: SANS
Service Name: krbtgt/SANS
Ticket Options: 0x40810010
Failure Code: 6
Client Address: 10.45.15.16

Event Type: Failure Audit
Event Source: Security
Event Category: Account Logon
Event ID: 681
Date: 3/30/2001
Time: 11:06:47 AM
User: NT AUTHORITY\SYSTEM
Computer: SANS034
Description:

The logon to account: admxxx
by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
from workstation: SANS016
failed. The error code was: 3221225572

The Audit Account logon category is reporting the event 675 failure code 24 in the Domain Controller for invalid password. It is also reporting event 681 in the DC:

Event Type: Failure Audit
Event Source: Security
Event Category: Account Logon
Event ID: 675
Date: 3/30/2001
Time: 10:56:01 AM
User: NT AUTHORITY\SYSTEM

Computer: SANS034

Description:

Pre-authentication failed:

User Name: admsans
User ID: SANS\admsans
Service Name: krbtgt/SANS
Pre-Authentication Type: 0x2
Failure Code: 24
Client Address: 10.45.15.16

Event Type: Failure Audit

Event Source: Security

Event Category: Account Logon

Event ID: 681

Date: 3/30/2001

Time: 10:56:02 AM

User: NT AUTHORITY\SYSTEM

Computer: SANS034

Description:

The logon to account: admsans

by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0

from workstation: SANS016

failed. The error code was: 3221225578

7.2.4 Network logon from W2K to Nt4

The audit logon events category is reporting events 529 for invalid password or invalid user:

Event Type: Failure Audit

Event Source: Security

Event Category: Logon/Logoff

Event ID: 529

Date: 3/30/2001

Time: 11:03:20 AM

User: NT AUTHORITY\SYSTEM

Computer: SANS021

Description:

Logon Failure:

Reason: Unknown user name or bad password
User Name: admxxx
Domain: SANS
Logon Type: 3

Logon Process: KSecDD
Authentication Package:
MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Workstation Name: \\SANS016

The Audit Account logon category is reporting the Kerberos authentication event 677 failure code 7 in the W2K DC. W2K is requesting a service ticket but it fails because the NT4 server does not support Kerberos:

Event Type: Failure Audit
Event Source: Security
Event Category: Account Logon
Event ID: 677
Date: 3/30/2001
Time: 11:09:38 AM
User: NT AUTHORITY\SYSTEM
Computer: SANS034
Description:
Service Ticket Request Failed:
User Name: SANS016\$
User Domain: SANS.SEC01.LOCAL
Service Name: HOST/SANS021
Ticket Options: 0x40810010
Failure Code: 7
Client Address: 10.45.15.16

The Audit logon category is also reporting event 676 failure code 6 and event 681 for invalid domain user :

Event Type: Failure Audit
Event Source: Security
Event Category: Account Logon
Event ID: 676
Date: 3/30/2001
Time: 11:09:38 AM
User: NT AUTHORITY\SYSTEM
Computer: SANS034
Description:
Authentication Ticket Request Failed:
User Name: admxxx
Supplied Realm Name: SANS
Service Name: krbtgt/SANS
Ticket Options: 0x40810010
Failure Code: 6
Client Address: 10.45.15.16

Event Type: Failure Audit
Event Source: Security
Event Category: Account Logon
Event ID: 681
Date: 3/30/2001
Time: 11:09:38 AM
User: NT AUTHORITY\SYSTEM
Computer: SANS034

Description:

The logon to account: admxxx

by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0

from workstation: \\SANS016

failed. The error code was: 3221225572

The Audit Account logon category is reporting the event 675 failure code 24 in the Domain Controller for invalid password. It is also reporting event 681 in the DC:

Event Type: Failure Audit
Event Source: Security
Event Category: Account Logon
Event ID: 675
Date: 3/30/2001
Time: 11:25:02 AM
User: NT AUTHORITY\SYSTEM
Computer: SANS034

Description:

Pre-authentication failed:

User Name: admsans
User ID: SANS\admsans
Service Name: krbtgt/SANS
Pre-Authentication Type: 0x2
Failure Code: 24
Client Address: 10.45.15.16

Event Type: Failure Audit
Event Source: Security
Event Category: Account Logon
Event ID: 681
Date: 3/30/2001
Time: 11:25:02 AM
User: NT AUTHORITY\SYSTEM
Computer: SANS034
Description:

The logon to account: admsans
by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
from workstation: \\SANS016
failed. The error code was: 3221225578

7.2.5 Network logon from NT4 to W2K

The audit logon events category is reporting event 529 for invalid account and invalid password:

Event Type: Failure Audit
Event Source: Security
Event Category: Logon/Logoff
Event ID: 529
Date: 3/18/2001
Time: 2:11:06 PM
User: NT AUTHORITY\SYSTEM
Computer: SANS016
Description:
Logon Failure:
Reason: Unknown user name or bad password
User Name: fakeuser
Domain: SANS
Logon Type: 3
Logon Process: NtLmSsp
Authentication Package:
MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Workstation Name: \\SANS021

The Audit Account logon category is reporting the event 681 in the Domain Controller:

Event Type: Failure Audit
Event Source: Security
Event Category: Account Logon
Event ID: 681
Date: 3/18/2001
Time: 2:11:14 PM
User: NT AUTHORITY\SYSTEM
Computer: SANS034
Description:
The logon to account: fakeuser
by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
from workstation: \\SANS021
failed. The error code was: 3221225572

During the tests, I noticed a huge volume of irrelevant events 540, 538 and 673 where the user name is the computer name ending with a dollar sign (\$) character. It is mainly related to machine authentication and I would filter it out when archiving the security events .

Besides the events I showed here, the audit logon events category also logs:

Event 531 when the user has a disabled account.

Event 539 when the user is locked out (It is an important event to monitor)

Event 530 when a user tries to log on outside the times or days permitted for that account.

Event 532 when the account has reached the expiration date

Event 536 when the Netlogon component is not active.

Event 535 when a user's password has expired

The audit account logon category logs:

675 ,676 and 677 with different failure code, like for example 676 with failure code 18 when the account gets locked out:

Event Type: Failure Audit

Event Source: Security

Event Category: Account Logon

Event ID: 676

Date: 3/18/2001

Time: 7:25:11 PM

User: NT AUTHORITY\SYSTEM

Computer: SANS034

Description:

Authentication Ticket Request Failed:

User Name: admsans

Supplied Realm Name: SANS

Service Name: krbtgt/SANS

Ticket Options: 0x40810010

Failure Code: 18

Client Address: 10.45.15.16

I didn't find in the MS WEB site a list of failure code and the meaning.

8 Archiving and Analyzing security events:

There are several commercial tools that collect, archive and analyze NT security logs and I recommend you take a look at those tools. They may be expensive, but they are worth it.

I will give some basic examples of what can be done with the authentication events that are getting logged in the security event log, and these can help you to identify what is important in a commercial tool.

After you turn on the audit logon events and audit account logon (you can see how to do it in the item 4.2) , some of the data analysis can be done in real time and other analyses will be done after collecting and archiving the data from all the servers in a central database.

8.1 Real time Analyzes:

For the real time analyses you don't need to archive the data, just read the logs and react to the events that are getting created.

An example is the following VB program that can run on servers and send an email to an operator when there are more than 5 events 529 in 2 minutes (it may indicate a logon violations attempt). The program is using WMI in order to read the security event log. It is looking for invalid login in the local server, so it will catch local and domain accounts. You may want to run it only in the W2K DCs and look for events 675 or 676 and catch domain account violations.

Private Sub Form_Load()

```
*****
!*****      In order to run this program:
!*****      - Load it in VB
!*****      - Go to Projects -> References
!*****      - Add "Microsoft WMI Scripting V1.1 Library"
!*****      - Select File -> Make, and save the exe as Monitor529.exe
!*****      - Run the Monitor529.exe in the servers
!*****
```

```
*****
```

```
Dim services As SWbemServices
Dim WbemEventSource As SWbemEventSource
Dim strQuery As String
Dim ObjEvent As SWbemObject
Dim Total529 As Integer
Dim AlertMessage As String
```

```
On Error Resume Next
Set services =
GetObject("winmgmts:{impersonationLevel=impersonate,(security)}")
strQuery = "SELECT * FROM __instancecreationevent " & _
"WHERE TargetInstance ISA 'Win32_NTLogEvent'"
```

```
Set WbemEventSource = services.ExecNotificationQuery(strQuery)

Do
Set ObjEvent = WbemEventSource.NextEvent(120000) ' Wait 120 seconds

If Err <> 0 Then
    If Err.Number = wbemErrTimedout Then      ' The call timed out

        Total529 = 0                        ' reset after 120 seconds

    Else
        AlertMessage = "The program monitoring logon violations on machine "
& _
        ObjEvent.TargetInstance.ComputerName & _
        " failed with error : " & _
        Err.Number & " " & Err.Description

        Alert (AlertMessage)                ' alert if program crashes

    End
End If

Else

    If ObjEvent.TargetInstance.eventcode = 529 And _
        ObjEvent.TargetInstance.SourceName = "Security" Then
        Total529 = Total529 + 1
        If Total529 > 5 Then

            AlertMessage = "You got more than 5 logon violations in a period of
120 seconds on " & _
            ObjEvent.TargetInstance.ComputerName

            Alert (AlertMessage) ' Alert if there is violation

            Total529 = 0        ' reset after alert
        End If
    End If

End If

Loop
```

End Sub

Sub Alert(AlertMessage)

```
*****  
' This sub will send an email. Change the email addresses  
,  
,  
' If you don't want an email, you can change this  
' sub in order to do something else,  
' like for example : MsgBox(AlertMessage)  
*****
```

```
Set myMail = CreateObject("CDONTS.NewMail")  
myMail.From = "julio.silveira@xyz.com"  
myMail.To = "julio.silveira@xyz.com"  
myMail.Subject = "You may be having a logon violation"  
myMail.Body = AlertMessage  
myMail.Send  
Set myMail = Nothing
```

End Sub

The same type of program could also monitor event 539 (account locked out) or you could disable an account and use it as a honey pot and start monitoring for event 531. By the way, it is just a simplified example and I don't recommend that you put it in production.

The program uses WMI, which is installed by default on W2K. You need to install WMI on NT4. It also sends email to the SMTP, and if you don't have one configured or don't want to use email, you can change the program in order to use a net send, or just a msgbox.

8.2 Archiving and Reports:

In order to automate your security event log archiving, you will need a utility that can import the security log to a file. You will need to schedule the dump of your logs considering the volumes of events you get on your servers and the maximum size of your event log.

Microsoft Resource kit has the Dumpel utility, which dumps the event log in a tab-delimited, or space delimited text file. You can also filter for specific events.

There are several other tools that can do it better than Dumpel, like Dumpevt, eventsave, or eldump.

I will show you an example of how to create some reports from the Security logs. I will use Eldump (Jester Lauritsen toll, which can be downloaded from <http://www.ibt.ku.dk/jesper/eldump/>) to dump my logs and archive it in a SQL 2000 DB.

8.2.1 Step 1 : Dump the security logs in a txt file

Save the security logs from your servers as .evt files.

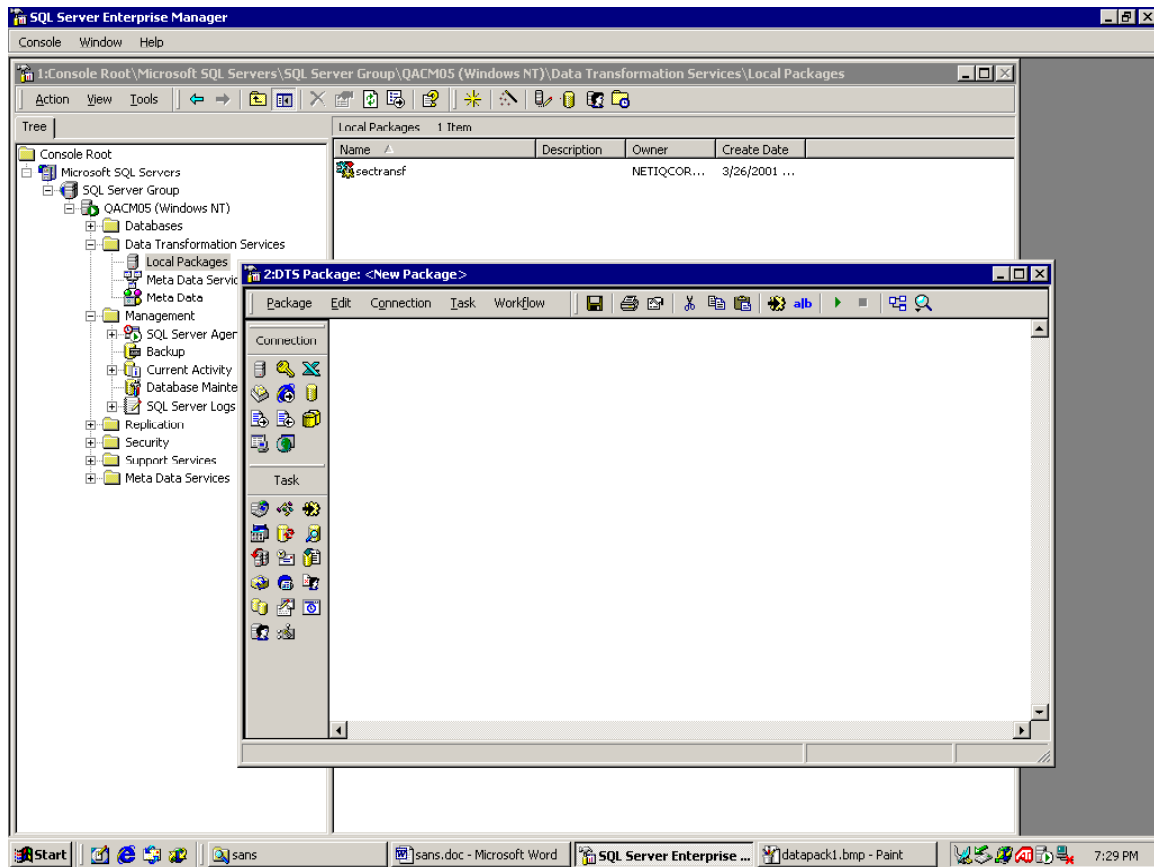
Execute the Eldump.

Eldump -F c:\SANS009.evt SANS016.evt -l security -e 528 538 -m security -M -c # > sec2.tx (M dumps only the message strings in the description).

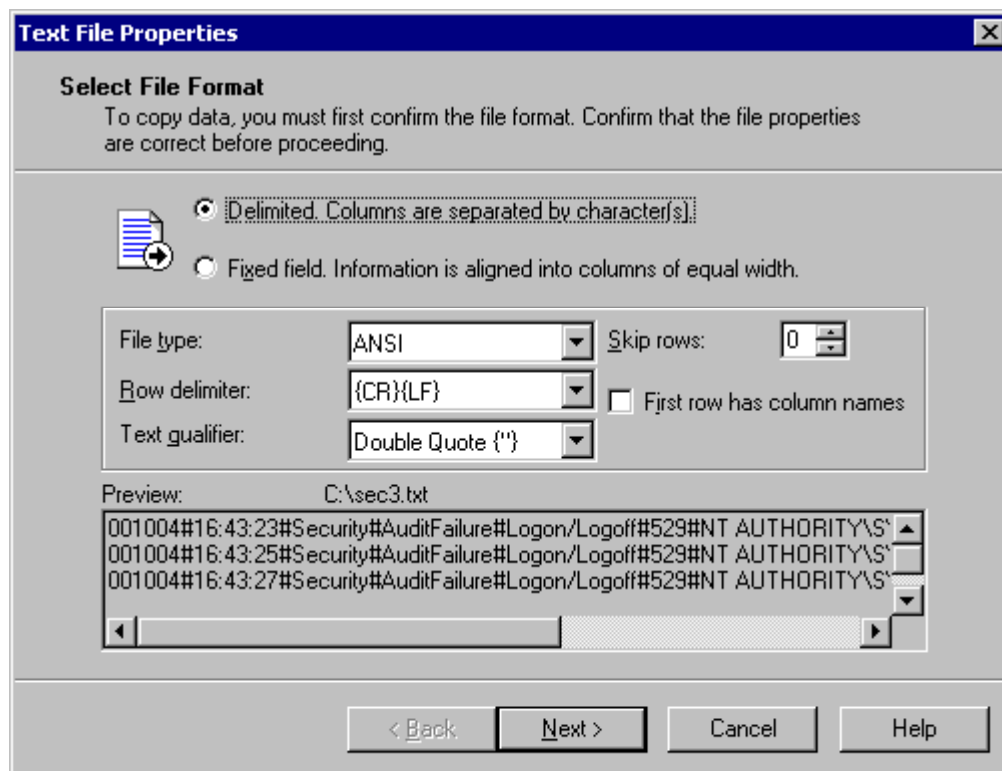
8.2.2 Step 2: Import the data (text files) to a SQL 2000 DB:

The logs can be imported in a SQL DB. The following steps show how:

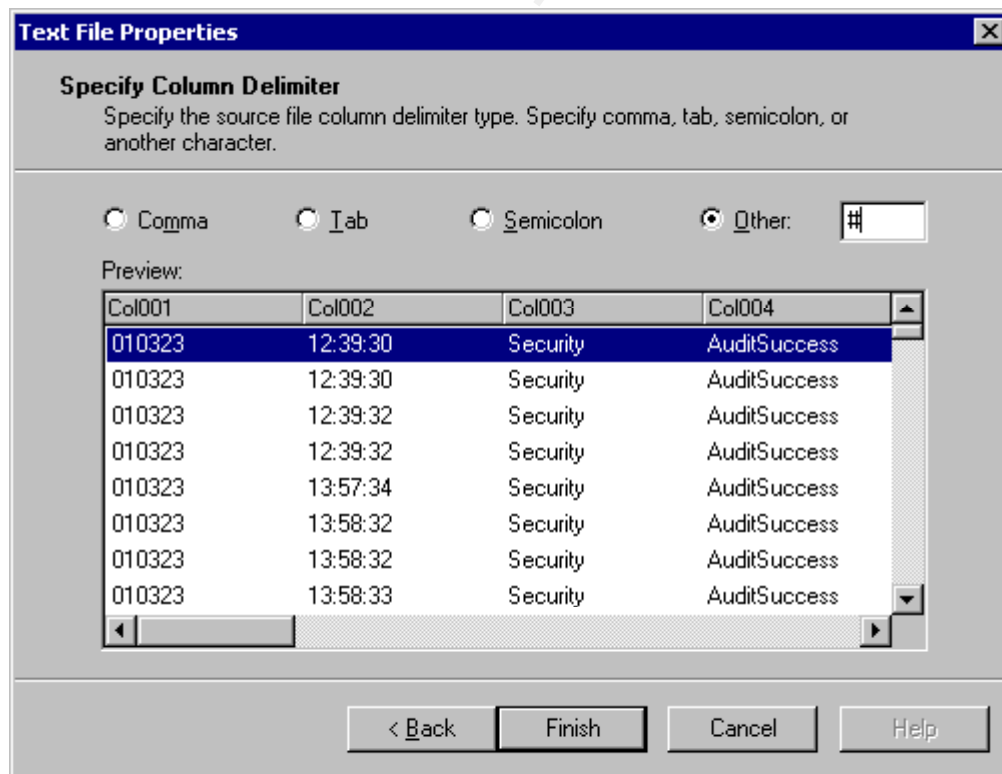
1. Open the SQL server 2000 Enterprise Manager.
2. Expand the Data Transformation Services Folder.
3. Right click over Local Package and select "New Package".
4. The following page will get open:



5. Select Connection.
6. Select Text File (Source).
7. Select the log file.
8. Select Delimited and next



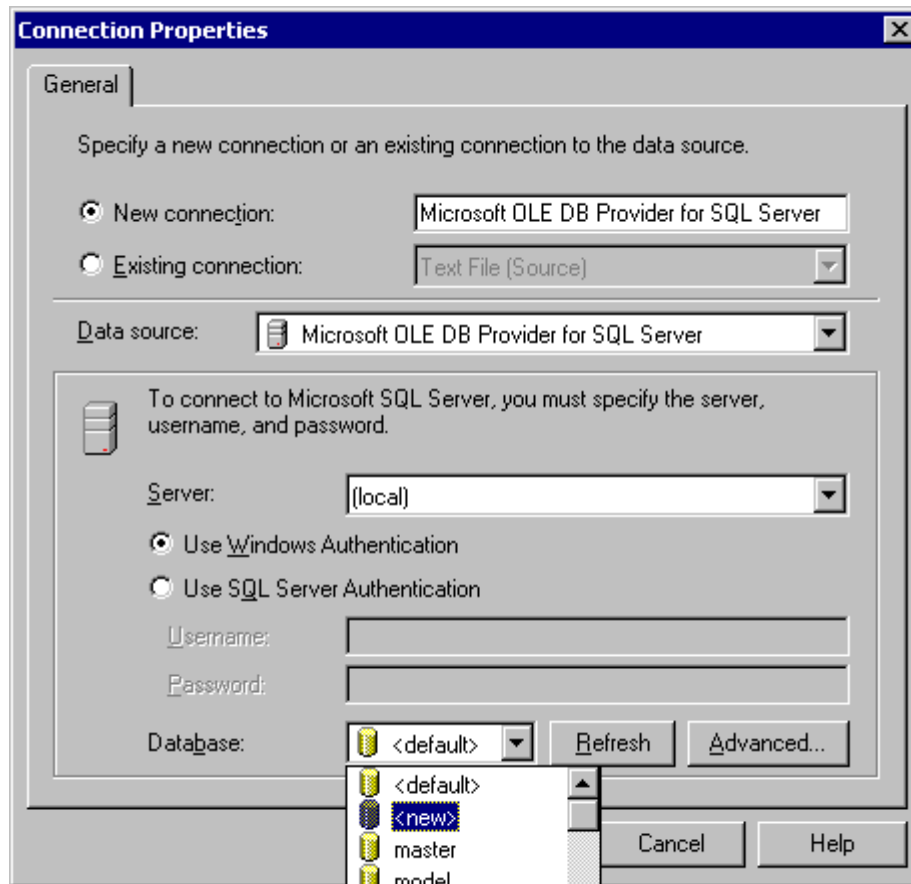
9. Select Other and enter the character #.



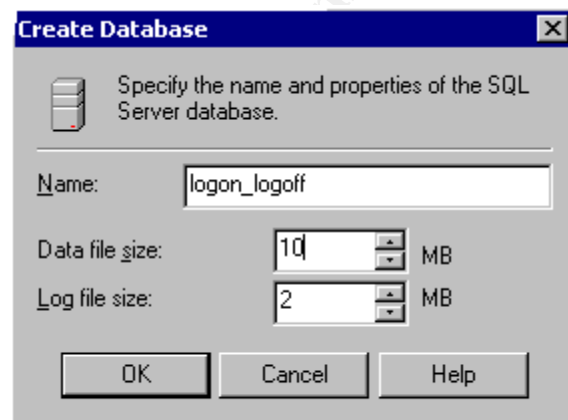
10. Press Finish.

11. Press ok.

12. In the DTS page, select connections , Microsoft OLE DB Provider for SQL Server.

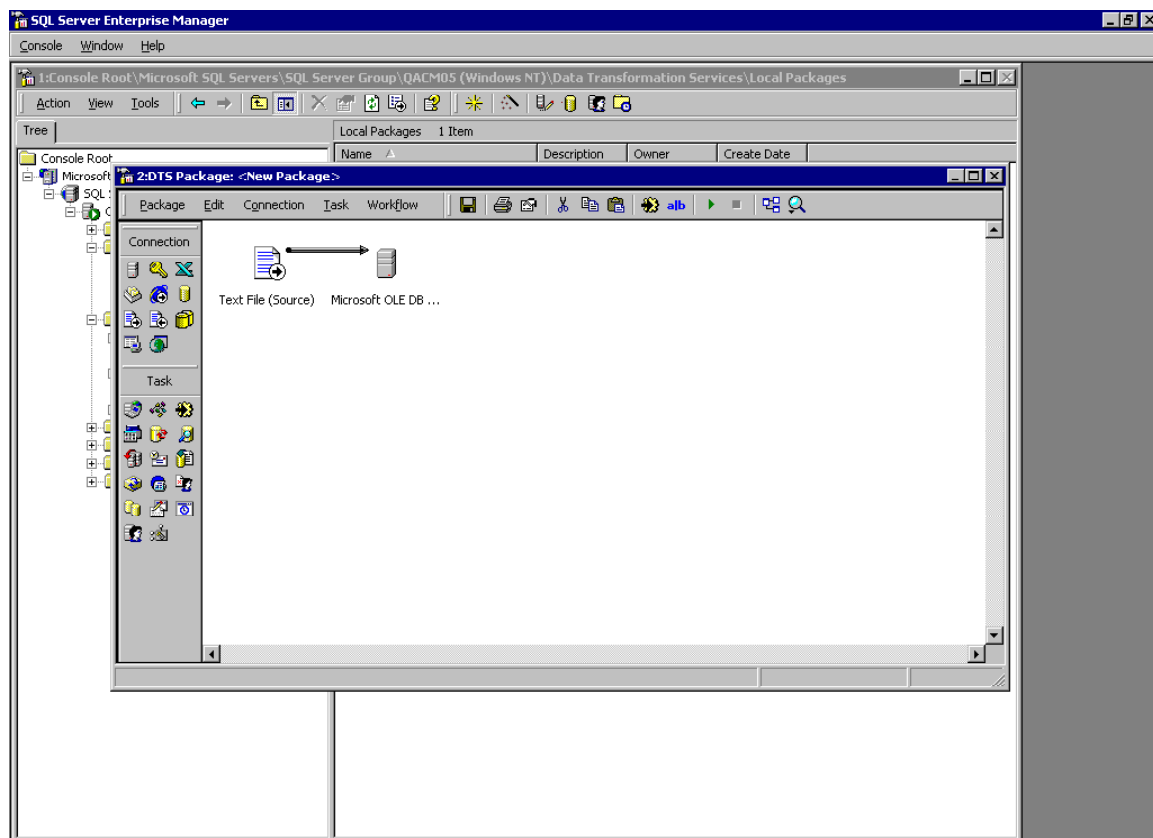


13. Enter the name of a new DB.



14. Drag a “Transform Data Task” from the toolbar (left side of the interface) and

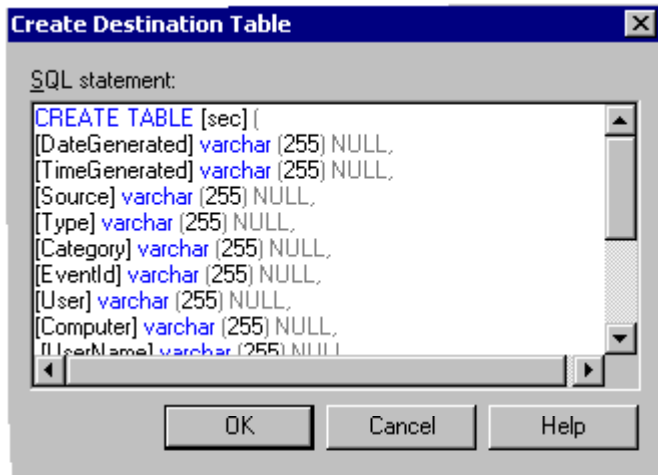
select the text connection as the source and the OLE DB connection as the destination.



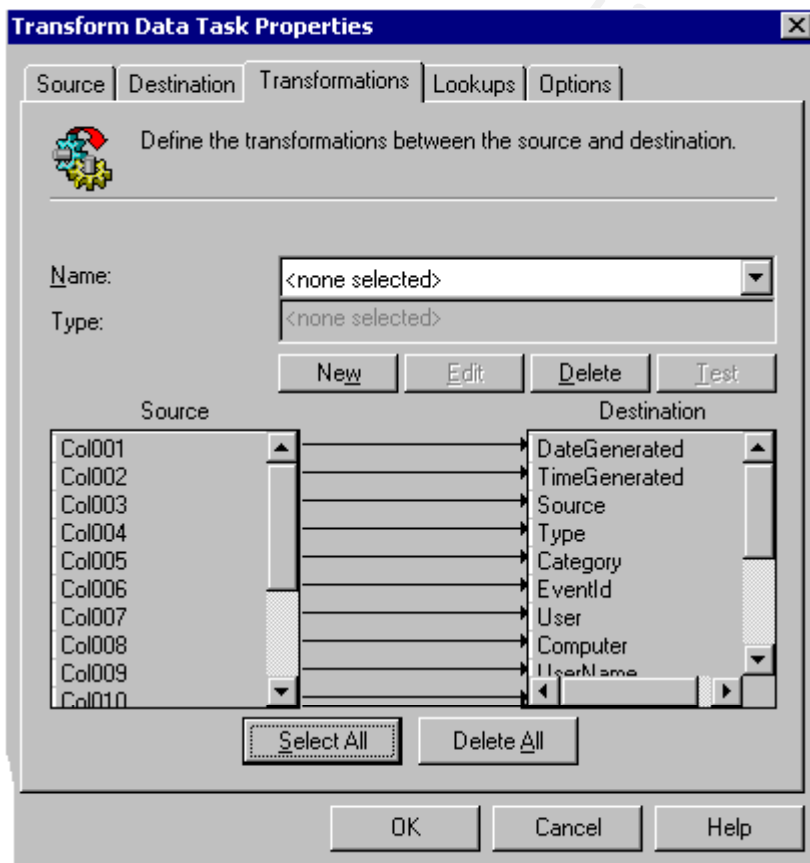
15. Right click over the arrow and select properties.

16. Select the destination folder, and replace the SQL statement for:

```
CREATE TABLE [sec] (  
[DateGenerated] varchar (255) NULL,  
[TimeGenerated] varchar (255) NULL,  
[Source] varchar (255) NULL,  
[Type] varchar (255) NULL,  
[Category] varchar (255) NULL,  
[EventId] varchar (255) NULL,  
[User] varchar (255) NULL,  
[Computer] varchar (255) NULL,  
[UserName] varchar (255) NULL,  
[Domain] varchar (255) NULL,  
[LogonID] varchar (255) NULL,  
[LogonType] varchar (255) NULL,  
[LogonProcess] varchar (255) NULL,  
[AuthenticationPackage] varchar (255) NULL,  
[Workstation] varchar (255) NULL )
```

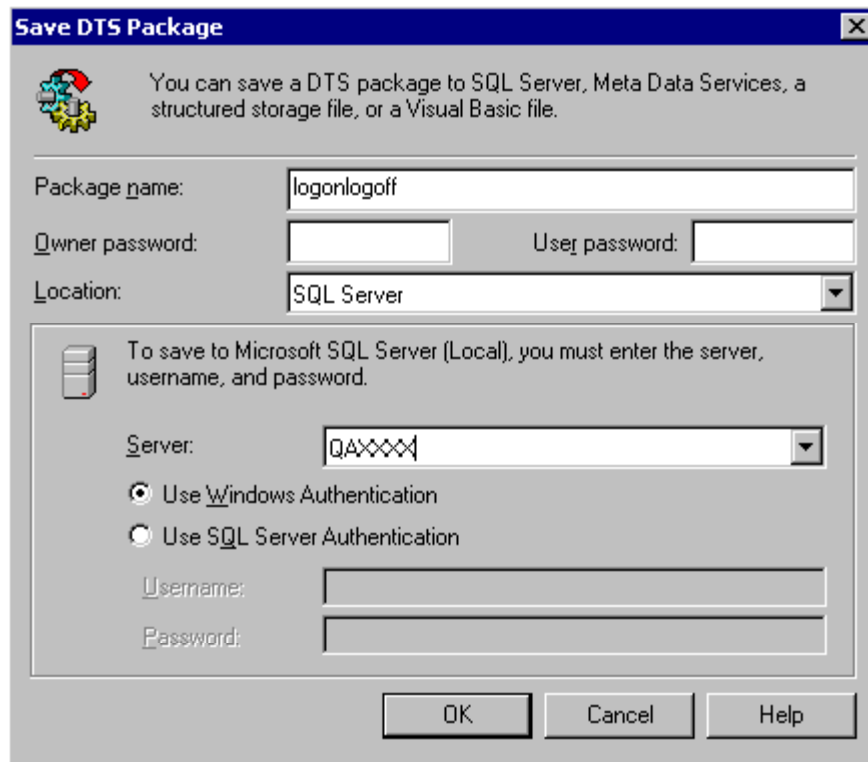



17. Click ok.
18. Select the Transformation tab.
19. Select "Select all".



20. Click ok.

21. Select Package, save as and save the package.



22. Execute the package.

23. A DB Logon_Logoff got created, and the table sec has all the data from the log.

8.2.3 Step 3 : Create reports

Run the following query in the “SQL Query Analyzer Tool “and you will get the logon time and logoff time report.

```
select a.username as Name, a.computer as Computer , a.logontype as Type,
a.dategenerated as Logon_Date,
a.timegenerated as Logon_Time, b.dategenerated as Logoff_Date,
b.timegenerated as Logoff_Time
from sec as a join sec as b
on a.eventid = 528 and b.eventid = 538 and a.logonid = b.logonid
```

You can use MS Access or Crystal Reports in order to format reports. The query example will create the following report:

Name	Computer	Type	Logon_Date	Logon_Time	Logoff_Date	Logoff_Time
User1	SANS009	2	010323	13:58:34	010323	14:23:00
User2	SANS009	2	010223	14:24:23	010223	15:00:04
User1	SANS016	2	010223	13:58:03	010223	15:03:08

Following the same steps, you can create other Tables with different events and create reports like:

- network logons (event 528 type 3 on NT4 and 540 on W2K)
- Failed logon (event 529)
- Account lockout (event 539)
- Disabled account (event 531)
- Failed Kerberos logon and reasons (events 675 and 676 from DCs)
- Kerberos authentication ticket granting – success Domain logon (events 672)

Note that the fields in the output file generated by the ELDUMP tools may be in different positions for different events, so you will need to change the SQL statement that creates the table.

An example is events 675 and 676. In order to create a new table with those events:

- Run ELDUMP, creating an output files with events 675 and 676. These events are getting created on W2K DCs:
- eldump -F c:\SANS034_675676.evt -l security -e 675 676 -m security -M -c # > sec3.txt
- Open the data transformation package that you have just created. You will find the package in the SQL Server Enterprise Manager -> Data Transformation Services and select the package you have created
- Right click over the Source and point to the new sec3.txt file with events 675 and 676.
- Right click over the arrow linking the Source and the Destination, and select properties.

- Select the destination folder, select create and enter :

```
CREATE TABLE [Kerberos_Failed] (  
[DateGenerated] varchar (255) NULL,  
[TimeGenerated] varchar (255) NULL,  
[Source] varchar (255) NULL,  
[Type] varchar (255) NULL,  
[Category] varchar (255) NULL,  
[EventId] varchar (255) NULL,  
[User] varchar (255) NULL,  
[Computer] varchar (255) NULL,  
[UserName] varchar (255) NULL,  
[UserId] varchar (255) NULL,  
[ServiceName] varchar (255) NULL,  
[Auth_Type] varchar (255) NULL,  
[FailureCode] varchar (255) NULL,  
[IPAddress] varchar (255) NULL )
```

- Open the transformations folder and select “remove all transformations and redo auto-mapping”.
- Execute the package, and the new table Kerberos_Failed will get create with events 675 and 676.

An example of report from the Kerberos_Failed table is:

Failed Logon because of Invalid user:

Name	Domain	Logon_Date	Logon_Time	IP Address
Userx	SANS	010324	13:38:34	10.45.15.16
Usery	SANS	010224	13:42:23	10.45.15.09
Userz	SANS	010224	13:56:03	10.45.15.16

9 Bibliography:

1. Roberta Bragg. Windows 2000 Security. New Riders, 2001. "It is a great book"
2. Stefan Norberg. Securing Windows NT/2000 Servers for the Internet. O'Reilly, 2001
3. Mark Minasi, Crysta Anderson, Brian Smith, Doug Toombs. Windows 2000 Server.
4. SQL Server 7.0 System Administration. Microsoft Press, 1999
5. Jason Fossen. Securing Windows NT, Step-by Step. SANS Security, 2001
6. Windows 2000 Magazine articles:
 - Audit Account Logon Events. Feb 2001
 - Introducing the NT security Log. Jan 2000
 - Archiving and Analyzing the NT security Logs. Jun 2000
 - Windows NT security: A collection of topics. Jun 1998
 - Security Administrator. March 2001
 - Windows NT logons. Jun 1997
 - Kerberos in W2K. Sep 1999
 - Inside SP4 NTLMV2 Security Enhancements. Aug 1999
 - Where NT stores passwords. Aug 1999
7. Microsoft Web Site
 - KB article Q174074
 - KB article Q273499
 - KB article Q182918
 - KB article Q147706
 - KB article Q102716
 - Technet: Interpreting the NT security Log
 - Technet: Windows 2000 Startup and Logon Traffic Analysis
 - Security Briefs by Keith Brown
 - W32_NTLogEvent
 - WMI SDK
 - Msdn.Microsoft.com/library/psdk/cdo/_denali_newmail_object_cdonts_library.htm
 - Msdn.Microsoft.com/library/periodic/period99/feb99_security_security.htm