Auditing: Section 1 Transcript

Introduction

Welcome to the Auditing module.

Auditing can be used for a variety of reasons and purposes, including forensic analysis, monitoring user activity, and troubleshooting. During this module, you will learn about security auditing features in Windows and how these features enhance network security.

Throughout this module, you will be presented with opportunities to assess and apply what you've learned.

At the end of this module, you will be able to:

- Describe the features of auditing,
- Identify auditable events,
- Identify various Windows audit logs, and
- Use command-line tools to interact with auditing polices and settings.

Bypass Exam Introduction

If you are already familiar with the subject matter presented in this module, you can choose to take a Bypass Exam to skip this module.

The Bypass Exam option provides a single opportunity to successfully demonstrate your competence with the material presented within the module. If you pass, you'll receive credit for completing the module, unlocking the content within, and you will be free to proceed to the next module. If you do not pass, you will need to successfully complete the module, including all exercises and the Module Exam, to receive credit.

Click the Next Section button to begin the Bypass Exam.

If you do not wish to take the Bypass Exam, you can use the Content Menu to proceed to the next section of the module.

Auditing: Section 2 Transcript

What is Auditing? 1/10

What is Auditing?

Auditing is the way in which Windows detects and records important security-related events or attempts to create, access, or delete system resources. Logon identifiers record the identities of all users, making it easier to trace anyone who performs an unauthorized action.

Auditing tracks user performed actions and the success or failure of events as defined by audit policies.

Audit policies can:

- Track the success or failure of an event,
- Identify unauthorized use of resources, and
- Maintain a record of activity.

Once Security Auditing is enabled and the audit policies are established, the security logs can be viewed in the Event Viewer.

Auditing Basics 2/10

Let's look at the basic concepts of how auditing works. To protect an object such as a file or folder from unauthorized access or use, you need to establish permissions. As you learned in previous modules, these permissions are referred to as Access Control Lists (ACLs).

An ACL defines the permissions of an object in Windows. The ACL is divided into two parts: the Discretionary Access Control List (DACL) and System Access Control List (SACL). By having two different lists in each ACL, permissions and auditing can be managed separately.

If a user wants to access an object, then they need access permissions for that object, which are stored in the object's DACL. This works well for permissions like read and write but not for auditing.

The SACL identifies which users and groups to audit when they successfully access or fail to access an object. It enforces audit policies and determines whether an event should be recorded in the Event Log.

In short, the DACL stores access permissions, and the SACL stores auditing permissions.

In XP and earlier versions of Windows, Security Auditing is turned off by default. There are two steps to enable auditing:

1. From a command prompt, enter `auditpol /enable`.
2. Use the graphical user interface (GUI) to choose the objects to audit.

To disable Security Auditing, run the command `auditpol /disable`.

In Windows 2003 and Vista+, Security Auditing is turned on by default.

Auditing Basics

The audit policy of the local system, or Local Security Policy, controls the decision to audit a particular action. The Local Security Policy is maintained by the Local Security Authority Subsystem (LSASS) and configured by the Local Security Policy Editor.

Here's an overview of the auditing process:

1. When the system initializes (or when policy changes), the LSASS sends messages to the Security Reference Monitor (SRM) to inform it of the auditing policy.
2. The LSASS receives the audit records from the SRM, edits the records to add pertinent details, and sends them to the Event Logger.
3. The Event Logger writes the audit records to the Security Log.

Audit records are queued and sent to the Local Security Authority (LSA) as they are received, not in timed or queued batches.

Audit records are moved from the SRM to the security subsystem in one of two ways:

1. If the audit record is smaller than 256 bytes, then it is sent as an LPC message.
2. If the audit record is larger than 256 bytes, then the SRM uses shared memory to make the message available to LSASS and passes a pointer to the LPC message.

Auditing Basics

To determine the audit settings on a computer, access the following key in the registry:

Administrators do not have access to this information by default, so permissions on the registry keys must be changed accordingly. This location contains a string of numbers, with the following format:

To better understand which auditing policies are enabled, use the table provided.

If any of the values (A,B,C,D,E,F,or G) are set to 1, successes are audited on those areas.

If any of the values are set to 2, failures are audited on those areas.

If any of the values are set to 3, both successes and failures are audited on those areas.

If the value of Z is 1, the policy is enabled; if it is 0, auditing is disabled.

If you would like a downloadable version of the table, access the Resources for this module to find the Audit Policy Table reference.

Event Types

Now that you've seen the auditing configurations available, let's discuss the event types that can be logged and viewed.

There are five types of events that can be logged:

- Error,
- Warning,
- Information,
- Success Audit, and
- Failure Audit.

All of these have well-defined common data and can include event-specific data.

Click each event type for more information.

Error: An event that indicates a significant problem such as loss of data or loss of functionality. For example, if a service fails to load during startup, an Error event is logged.

Warning: An event that is not necessarily significant, but may indicate a possible future problem. For example, when disk space is low, a Warning event is logged. If an application can recover from an event without loss of functionality or data, it can generally classify the event as a Warning event.

Information: An event that describes the successful operation of an application, driver, or service. For example, when a network driver loads successfully, it may be appropriate to log an Information event. Note that it is generally inappropriate for a desktop application to log an event each time it starts.

Success Audit: An event that records an audited security access attempt that is successful. For example, a user's successful attempt to log on to the system is logged as a Success Audit event.

Failure Audit: An event that records an audited security access attempt that fails. For example, if a user tries to access a network drive and fails, the attempt is logged as a Failure Audit event.

Security Log Events

Each Event type is associated with an Event ID. The event, within the Event Viewer, is a link that can be clicked to access more information about the specific ID.

The list of possible Event IDs is extensive; however, here is a list of Event IDs that are most relevant.

Click each Event ID for more information.

513 | 4609

513: Windows is shutting down (Win2k, WinXP)

4609: Windows is shutting down (Win2k8, Vista+)

Events 513 and 4609 are important security events. For example, if you are connected to a host machine and lose connectivity, it will be important to determine why, once you re-establish

connectivity. If you are able to reconnect to the host, you should review the host's event logs to determine if the user of the host machine simply rebooted the machine. If the host machine was rebooted, you should be able to see Event ID 513. If Event ID 513 is not present in the log file, you may need to conduct further analysis to determine what occurred.

528 | 4624

528: Successful Logon (Win2k, WinXP)

4624: Successful Logon (Win2k8, Vista+)

Events 528 and 4624 are logged whenever an account logs on to the local computer, except for network logons, which are seen as Event 540. Event 528 is logged whether the account used for logon is a local Security Account Manager (SAM) account or a domain account. This event can be helpful when trying to determine which users are logging on locally.

529 | 4625

529: Logon Failure - Unknown user name or bad password (Win2k, WinXP)

4625: Logon Failure - Unknown user name or bad password (Win2k8, Vista+)

Events 529 and 4625 are logged on the workstation or server where the user failed to log on. For example, in a brute-force attack, you may see hundreds of the 529 or 4625 events in the logs since each failed attempt would be recorded.

540

540: Successful Network Logon (Win2k, WinXP)

Event 540 gets logged when a user on the network connects to a resource like a shared folder on a network drive. This information helps to better understand what network resources a user can access.

577 | 4673

577: Privileged Service Called (Win2k, WinXP)

4673: Privileged Service Called (Win2k8, Vista+)

Events 577 and 4673 indicate when a user has used their escalated privileges. That is, when a user does something that requires escalated privilege, which is set to be audited.

636 | 4732

636: Security Enabled Local Group Member Added (Win2k, WinXP)

4732: Security Enabled Local Group Member Added (Win2k8, Vista+)

Events 636 and 4732 indicate privilege escalation or a user being added to a privileged group.

5031

5031: The Windows Firewall Service blocked an application from accepting incoming connections on the network. (Vista+)

Applications trying to accept incoming connections are not always a bad thing; however, the Windows Firewall may prevent this from occurring. That being said, event 5031 can also be an indicator of a compromised application or malware.

861 | 5154

861: The Windows Firewall has detected an application listening for incoming traffic (WinXP)

5154: The Windows Filtering Platform has permitted an application or service to listen on a port for incoming connections (Win2k8, Vista+)

Events 861 and 5154 document each time the Windows Filtering Platform (WFP) allows a program to begin listening on a TCP or UDP port for incoming connections and documents the program, port, and filter that allowed it.

Auditable Events 7/10

Windows typically maintains three Event Log files:

- Application,
- System, and
- Security.

These files are generally found in the C:\Windows\system32\config directory. Server versions of the OS may maintain additional Event Logs, such as:

- DNS Server.evt,
- Directory Service.evt, and
- File Replication Service.evt.

Each log file consists of a Header record and the Body. The body consists of Event records, the Cursor record, and unused space.

It's important to note that, in comparison, Vista+ records a higher number of events than Windows XP and 2003, and the Event IDs used by Vista+ are also different.

Finally, Vista+ uses an XML file with the extension .evtx, and is found in the C:\Windows\System32\winevt\Logs directory.

Click each one of the events for a brief description.

System: User restarts or shuts down the computer

Logon: User logs on or off the local computer

Object Access: User gains access to a file folder or printer

Privilege Use: User exercises a right such as taking ownership of a file

Detailed Tracking: Application performs an action

Policy Change: Change is made to the user security options, user rights, or Audit policies

Account Management: Administrator creates, changes, or deletes a user account or group

Directory Service Access: User gains access to an Active Directory object

Account Logon: Domain controller receives a request to validate a user account

Tools 8/10

Now that you've seen several aspects of auditing in Windows, let's introduce some of the tools that can be used to edit audit policies and view event logs:

- AuditPol.exe,
- EventQuery.vbs, and
- PSLogList.exe.

AuditPol is a command-line tool native to Windows that enables, disables, and changes audit policy.

EventQuery is a built-in tool used to query and view Windows event logs. EventQuery has multiple options to filter queries and enables an administrator to list the events and event properties from one or more event logs.

PSLogList is a tool that allows you to login to remote systems in situations where your current set of security credentials do not permit access to in the event log. In those instances, PSLogList retrieves message strings from the computer on which the event log resides.

For more information on the tools that can be used for editing audit policies and viewing event logs, access Resources for this module to find the Auditing Tools reference.

Tools 9/10

After running AuditPol, this is the typical output; however, the output may vary based on the version of the operating system (OS).

Click each audit category for a brief description.

AuditCategorySystem: Audits any attempts to shutdown or restart the computer. Also, audits events that affect system security or the security log.

AuditCategoryLogon: Audits any attempts to log on to or off of the system. Also, audits any attempts to make a network connection.

AuditCategoryObjectAccess: Audits any attempts to access securable objects, such as files.

AuditCategoryPrivilegeUse: Audits any attempts to use privileges.

AuditCategoryDetailedTracking: Audits specific events, such as program activation, some forms of handle duplication, indirect access to an object, and process exit.

AuditCategoryPolicyChange: Audits any attempts to change policy object rules.

AuditCategoryAccountManagement: Audits any attempts to create, delete, or change user or group accounts. Also, audits password changes.

AuditCategoryDirectoryServicesAccess: Audits any attempts to access the directory service.

AuditCategoryAccountLogon: Audits logon attempts by privileged accounts that log on to the domain controller. These events are generated when the Kerberos Key Distribution Center (KDC) logs on to the domain controller.

Exercise Introduction

It is time for an Exercise. In order to successfully complete the Exercise, you are expected to use your notes and any available resources presented throughout the course, in addition to conducting your own Internet research.

Auditing: Section 3 Transcript

Summary

You have completed the Auditing module.

During this module, you learned about security auditing basics and features as well as some of the command-line tools that are used to interact with auditing policies. Then you applied what you learned in practical exercises, using command-line tools to edit audit policies.

You should now be able to:

- Describe the features of auditing,
- Identify auditable events,
- Identify various Windows audit logs, and
- Use command-line tools to interact with auditing policies and settings.

To receive credit and advance to the next module, you must achieve a passing score on the Module Exam.

Click the Next Section button to begin the Module Exam.