Anonymous Logon

ANONYMOUS LOGON (S-1-5-7) basically means someone or something without associated credentials (no username, no password).

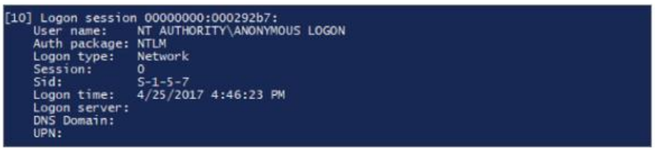
The important thing to notice is that anonymous logon, by default, is supported only by NTLM authentication, because Kerberos does not have Service Principal Name registered for the NT Authority\ANONYMOUS LOGON built-in security principal.

Multiple scenarios exist in the Windows world when an anonymous user might appear. In this section you will find information about the most common scenarios where an ANONYMOUS LOGON account is used.

Default ANONYMOUS LOGON Logon Session

By default, when a Windows operating system starts, the local ANONYMOUS LOGON session is automatically created. The LOCAL SYSTEM, LOCAL SERVICE, NETWORK SERVICE, and ANONYMOUS LOGON built-in accounts create their logon sessions at **system startup**. These sessions are then used to run processes under these accounts.

You can verify the list of current active logon sessions using the logonsessions.exe tool from Microsoft, which was discussed in the “Successful Local User Account Interactive Logon” section. Figure 4-7 shows an example of logonsessions.exe output showing the default ANONYMOUS LOGON logon session.

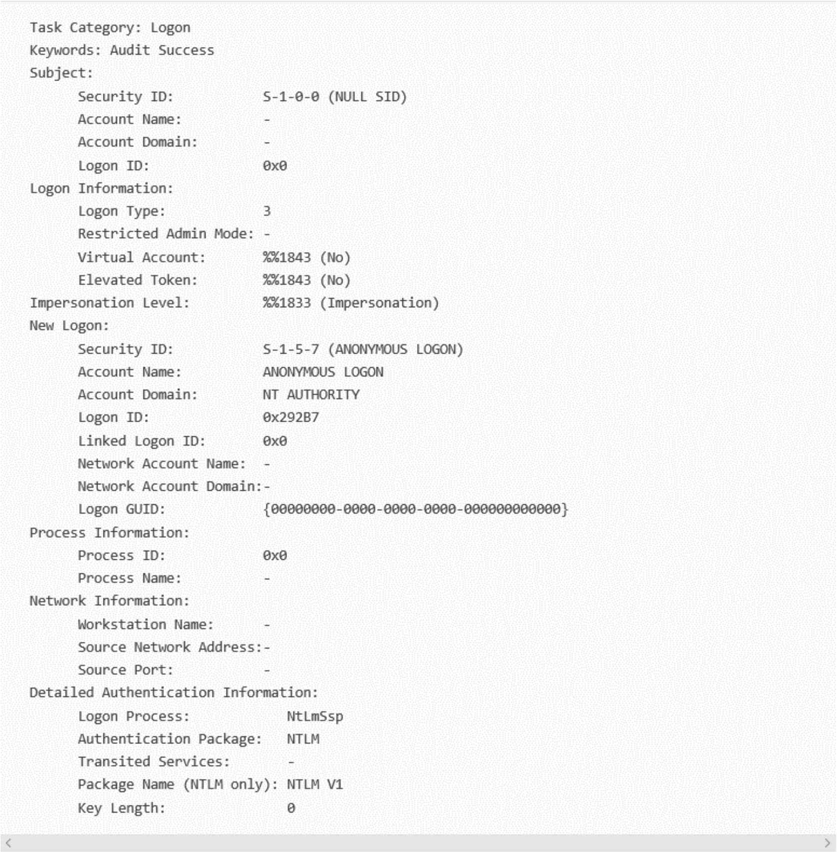


```
[10] Logon session 00000000:000292b7:
    User name:    NT AUTHORITY\ANONYMOUS LOGON
    Auth package: NTLM
    Logon type:   Network
    Session:      0
    Sid:          S-1-5-7
    Logon time:   4/25/2017 4:46:23 PM
    Logon server:
    DNS Domain:
    UPN:
```

Figure 4-7: Default ANONYMOUS LOGON logon session

Listing 4-48 is an example of the security event generated at startup for the session in Figure 4-7.

Listing 4-48: Event ID 4624: An account was successfully logged on.

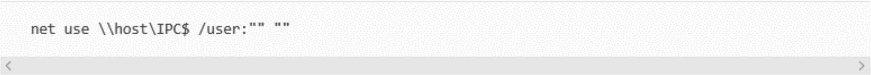


```
Task Category: Logon
Keywords: Audit Success
Subject:
      Security ID:           S-1-0-0 (NULL SID)
      Account Name:          -
      Account Domain:        -
      Logon ID:              0x0
Logon Information:
      Logon Type:            3
      Restricted Admin Mode: -
      Virtual Account:       %%1843 (No)
      Elevated Token:        %%1843 (No)
Impersonation Level:         %%1833 (Impersonation)
New Logon:
      Security ID:           S-1-5-7 (ANONYMOUS LOGON)
      Account Name:          ANONYMOUS LOGON
      Account Domain:        NT AUTHORITY
      Logon ID:              0x292B7
      Linked Logon ID:       0x0
      Network Account Name:  -
      Network Account Domain:-
      Logon GUID:            {00000000-0000-0000-0000-000000000000}
Process Information:
      Process ID:            0x0
      Process Name:          -
Network Information:
      Workstation Name:      -
      Source Network Address:-
      Source Port:           -
Detailed Authentication Information:
      Logon Process:            NtLmSsp
      Authentication Package:   NTLM
      Transited Services:       -
      Package Name (NTLM only): NTLM V1
      Key Length:               0
```

Explicit Use of Anonymous Credentials

Some applications might be hardcoded to use anonymous credentials. This will generate logon attempts with an ANONYMOUS LOGON account.

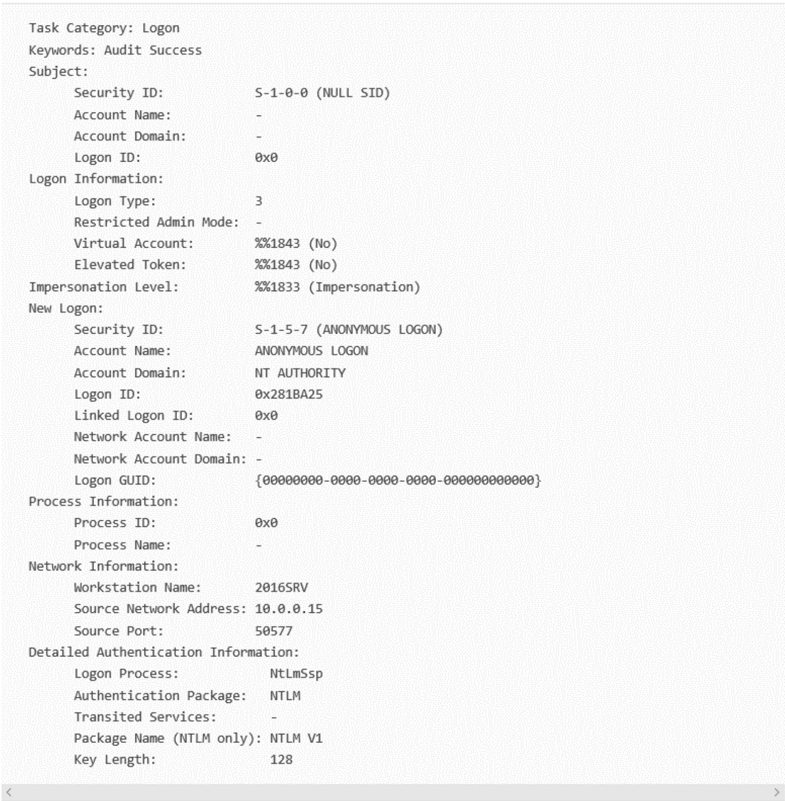
You can test this behavior using the net use built-in Windows command-line application. Use the following command in order to try anonymous access to the remote machine:



```
net use \\host\IPC$ /user:"" ""
```

This command requests anonymous access to the target's Inter-process Communications (IPC$) share. You can find more information about the IPC$ share in Chapter 15.

The result of the net use command with anonymous access might be, if successful, as shown in Listing 4-49.



Listing 4-49: Event ID 4624: An account was successfully logged on.

```
Task Category: Logon
Keywords: Audit Success
Subject:
      Security ID:            S-1-0-0 (NULL SID)
      Account Name:           -
      Account Domain:         -
      Logon ID:               0x0
Logon Information:
      Logon Type:             3
      Restricted Admin Mode:  -
      Virtual Account:        %%1843 (No)
      Elevated Token:         %%1843 (No)
Impersonation Level:          %%1833 (Impersonation)
New Logon:
      Security ID:            S-1-5-7 (ANONYMOUS LOGON)
      Account Name:           ANONYMOUS LOGON
      Account Domain:         NT AUTHORITY
      Logon ID:               0x281BA25
      Linked Logon ID:        0x0
      Network Account Name:   -
      Network Account Domain: -
      Logon GUID:             {00000000-0000-0000-0000-000000000000}
Process Information:
      Process ID:             0x0
      Process Name:           -
Network Information:
      Workstation Name:       2016SRV
      Source Network Address: 10.0.0.15
      Source Port:            50577
Detailed Authentication Information:
      Logon Process:            NtLmSsp
      Authentication Package:   NTLM
      Transited Services:       -
      Package Name (NTLM only): NTLM V1
      Key Length:               128
```

In this event you might see the hostname (Workstation Name) and IP address (Source Network Address) from which the logon was initiated. The Workstation Name field contains the name of a source machine only if NTLM-family protocol is used, which is the case for anonymous logons, because only Kerberos does not support anonymous authentication.

The Detailed Authentication Information section contains additional details about the authentication protocol, logon process, and authentication package. The Logon Process and Authentication Package fields were discussed in the “Step 9: Local User Logon: MSV1_0 Answer” section earlier this chapter. For more information about the Transited Services, Package Name (NTLM only), and Key Length fields.

Use of Account That Has No Network Credentials

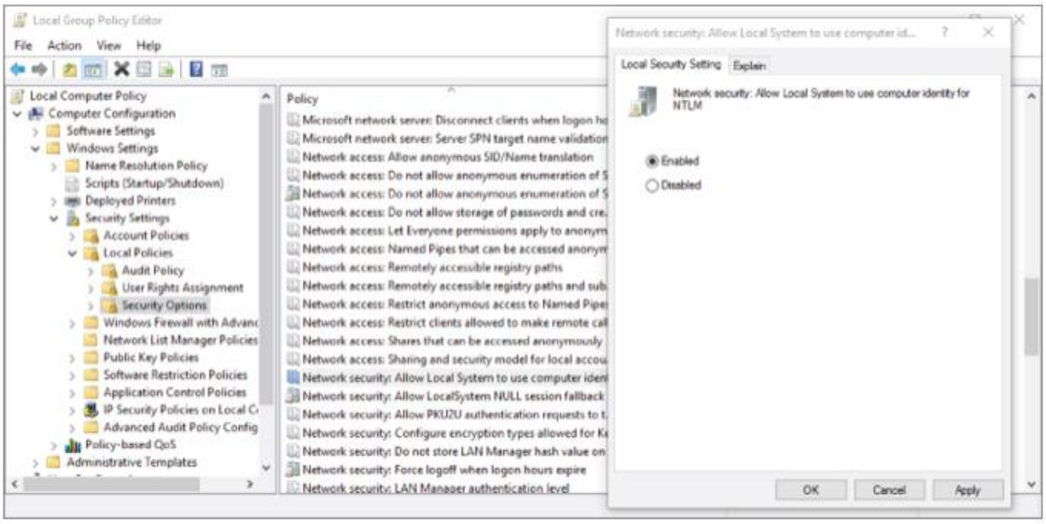
Some of the accounts, such as the LOCAL SERVICE account, exist only within a host and when these accounts are used for network communications the system uses ANONYMOUS LOGON. It is easy to reproduce this by creating a scheduled task that runs under the LOCAL SERVICE account, as an Action set something like explorer \\ *remote_host_name* \c$. When you run this scheduled task you will receive an ANONYMOUS LOGON logon event on the target host.

Computer Account Activity from Non–Domain-Joined Machine

When computer account identities (LOCAL SYSTEM, NETWORK SERVICE) are used to access any network resource from a non–domain-joined machine, the system tries anonymous access. You can reproduce such activity using the method described in the previous section. Create a scheduled task on non–domain-joined machine, which runs under a LOCAL SYSTEM or NETWORK SERVICE account, as an Action set something like explorer \\ *remote_host_name* \c$. When you run this scheduled task, you will receive an ANONYMOUS LOGON logon event on the target host.

Allow Local System to Use Computer Identity for NTLM

There is legacy compatibility behavior in which processes running as a LOCAL SYSTEM account would become anonymous if they fell back to NTLM authentication. Back in Windows NT4, computers were not first-class principals and could not perform user authentication. As a result, processes that ran as the system were anonymous in network authentication. Prior to Windows 7 and Windows Server 2008 R2, this remained the default behavior in order to preserve compatibility with Windows NT4. In Windows 7 and Windows Server 2008 R2, the default behavior was changed and the “Network security: Allow Local System to use computer identity for NTLM” policy setting was added to control this behavior. The policy setting is located under Computer Policy\Windows Settings\Security Settings\Local Policies\Security Options. The policy setting can be applied to Windows Vista or Windows Server 2008 hosts. Figure 4-8 shows an example of this group policy setting.



Microsoft network server: Disconnect clients when logon ho
Microsoft network server: Server SPN target name validation
Network access: Allow anonymous SID/Name translation
Network access: Do not allow anonymous enumeration of S
Network access: Do not allow anonymous enumeration of S
Network access: Do not allow storage of passwords and cre.
Network access: Let Everyone permissions apply to anonym
Network access: Named Pipes that can be accessed anonym
Network access: Remotely accessible registry paths
Network access: Remotely accessible registry paths and sub
Network access: Restrict anonymous access to Named Pipe
Network access: Restrict clients allowed to make remote call
Network access: Shares that can be accessed anonymously
Network access: Sharing and security model for local accou
Network security: Allow Local System to use computer iden
Network security: Allow LocalSystem NULL session fallback
Network security: Allow PKU2U authentication requests to t.
Network security: Configure encryption types allowed for Ke
Network security: Do not store LAN Manager hash value on
Network security: Force logoff when logon hours expire
Network security: LAN Manager authentication level

Network security: Allow Local System to use computer identity for NTLM

● Enabled
○ Disabled

Figure 4-8: “Network security: Allow Local System to use computer identity for NTLM” group policy setting

Considering this information, computers running Windows versions prior to Windows 7 and Windows Server 2008 R2 will use ANONYMOUS LOGON for NTLM authentication when a LOCAL SYSTEM account is used. Also, the same behavior will occur if the “Network security: Allow Local System to use computer identity for NTLM” policy setting is **disabled** on a host.

A 4776 event generates on the host where account credentials are stored and when this host receives a credential validation request for that account. The Authentication Package field contains the name of the authentication package that handled NTLM authentication. The only default package name you should see in a Windows environment is MICROSOFT_AUTHENTICATION_PACKAGE_V1_0.

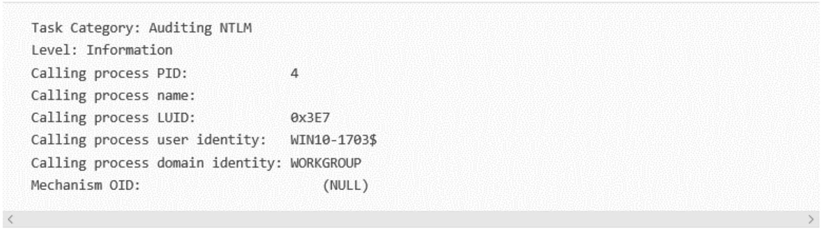
The Logon Account field contains the name of the account for which credentials were validated.

The Source Workstation field contains the name of the host from which the credentials validation request was received.

The Error Code field contains the error code for unsuccessful credential validations, which will be discussed later in this chapter. For successful credentials validation this field always has a value of 0x0.

In addition to these security events, for each successful NTLM authentication using a local user account, the event in Listing 9-3 is triggered in the Windows NTLM event log.

Listing 9-3: Event ID 8002: NTLM server blocked audit: Audit Incoming NTLM Traffic that would be blocked.



```
Task Category: Auditing NTLM
Level: Information
Calling process PID:            4
Calling process name:
Calling process LUID:           0x3E7
Calling process user identity:  WIN10-1703$
Calling process domain identity: WORKGROUP
Mechanism OID:                       (NULL)
```

The Calling process PID field contains the process identifier (PID) of the local process on the destination host that handled the authentication request, in decimal format. It does not contain information about the process that invoked authentication from the source host.

The Calling process name field contains the process name of the local process on the destination host that handled the authentication request. It does not contain information about the process name from the source host. For system process (PID 4) this field will be empty.

The Calling process LUID field contains the logon ID of the user account logon session for the account specified in the Calling process user identity field.

The Calling process user identity field for local account authentication contains the name of the account, under which the process that handled the authentication on the destination host runs. Keep in mind that the LOCAL SYSTEM or LOCAL SERVICE account may “hide” behind the computer account name. They will have different Calling process LUID field values:

- **0x3E4**: LOCAL SYSTEM
- **0x3E5**: LOCAL SERVICE

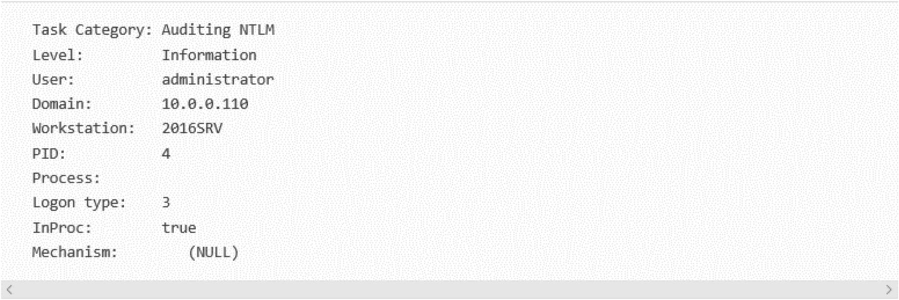
The Calling process domain identity field contains the domain or workgroup name (if the destination host is not domain-joined) to which the Calling process user identity account belongs.

The Mechanism OID field contains the object identifier (OID) of the SSPI mechanism being used for authentication. For example, the OID 1.3.6.1.4.1.311.2.2.10 is related to NTLM-family protocols (MS-NLMP specification). This field is not always populated.

Generally speaking, the 8002 event for local accounts does not provide information about from where the NTLM-family protocol request originated. It shows you only that an NTLM-family protocol request was received.

If a destination host is *joined to an Active Directory domain*, an 8003 event will be generated in the Windows NTLM event log on the destination host, in addition to an 8002 event. The 8003 event is shown in Listing 9-4.

Listing 9-4: Event ID 8003: NTLM server blocked in the domain audit: Audit NTLM authentication in this domain



```
Task Category: Auditing NTLM
Level:         Information
User:          administrator
Domain:        10.0.0.110
Workstation:   2016SRV
PID:           4
Process:
Logon type:    3
InProc:        true
Mechanism:        (NULL)
```

The User field contains the account name for which the authentication attempt was performed.

The Domain field contains the IP-address of a host to which the user account, specified in the User field, belongs.

The Workstation field contains the hostname from which the authentication request was received.

The PID field contains the process identifier (PID) of the local process on the destination host that handled the authentication request, in decimal format. It does not contain information about the process that initiated authentication from the source host.

The Process field contains process name of the local process on the destination host that handled the authentication request. It does not contain information about the process from the source host. For system process (PID 4) this field will be empty.

The Logon type field contains the type of logon that was initiated from the source host. Table 4.1 contains the available logon type codes.

The Mechanism field contains the object identifier (OID) of the SSPI mechanism being used for authentication. For example, the OID 1.3.6.1.4.1.311.2.2.10 is related to NTLM-family protocols (MS-NLMP specification). This field is not always populated.

Step 3: NTLM Type 3 Message

After a response is generated (Step 2), the source host sends it to the destination host in an NTLM Type 3 message. The destination host receives the Type 3 message, extracts all additional fields if required, and performs the same operations with the user's locally stored password hash. If the destination host gets the same results as the source host, the destination host considers the password to be legitimate/valid. If the results are not the same, the password is not valid.

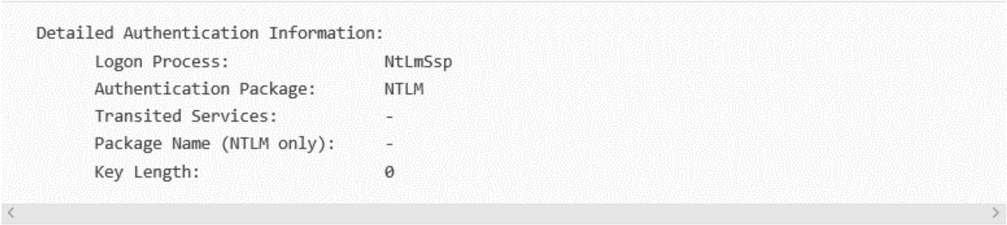
The destination host sends the response back to the source host with authentication results.

Unsuccessful Local Account Authentication

On a source host, the same 8001 NTLM event will be generated, whether or not the authentication is successful.

Only an 8002 NTLM event will be generated on the destination host for unsuccessful authentication. An 8003 event is generated only for successful NTLM authentications and only on the domain-joined hosts. There is no difference between successful and unsuccessful authentication 8002 events.

A 4625 security event will be generated instead of a 4624 event and will usually contain the following information in the Detailed Authentication Information section:

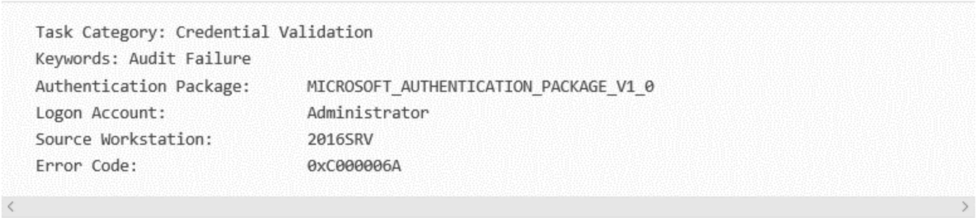


```
Detailed Authentication Information:
        Logon Process:                NtLmSsp
        Authentication Package:       NTLM
        Transited Services:           -
        Package Name (NTLM only):     -
        Key Length:                   0
```

A 4625 event does not usually provide information about the NTLM-family protocol name (Package Name (NTLM only)) and NTLMv1/v2 Session Security key length (Key Length).

For each unsuccessful NTLM authentication using a local user account, event in Listing 9-5 is generated in the Windows security event log on the destination host where the account's credentials are stored.

Listing 9-5: Event ID 4776: The computer attempted to validate the credentials for an account.



```
Task Category: Credential Validation
Keywords: Audit Failure
Authentication Package:      MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Logon Account:               Administrator
Source Workstation:          2016SRV
Error Code:                  0xC000006A
```

4776 events were discussed with Listing 9-2. This is an Audit Failure event, which informs you that credentials validation failed.

The Error Code field contains a hexadecimal failure code. The most common error codes for 4776 events are presented in Table 9-1.

Table 9-1: 4776 Event Error Codes

ERROR CODE	DESCRIPTION
`0xC000005E`	There are currently no logon servers available to service the logon request.
`0xC000006D`	Unknown user name or bad password. Issue with NTLM-family protocol version negotiation.
`0xC0000064`	User logon with misspelled or bad user account.
`0xC000006A`	User logon with misspelled or bad password.
`0xc000019b`	Duplicate or incorrect SID was detected.
`0xC000006F`	User logon outside authorized hours.
`0xC0000070`	User logon from unauthorized workstation.
`0xC0000071`	User logon with expired password.
`0xC0000072`	User logon to account disabled by administrator.
`0xC00000DC`	Indicates the Sam Server was in the wrong state to perform the desired operation.
`0xC000015B`	The user has not been granted the requested logon type (logon right) at this machine.
`0xC000018C`	The logon request failed because the trust relationship between the primary domain and the trusted domain failed.
`0xC0000192`	An attempt was made to logon, but the Netlogon service was not active.
`0xC0000193`	User logon with expired account.
`0xC0000224`	User is required to change password at next logon.
`0xC0000225`	Unknown error occurred during logon.
`0xC0000234`	User logon with account locked.
`0xC00002EE`	Unknown error occurred during logon.
`0xC0000413`	The machine you are logging onto is protected by an authentication firewall. The specified account is not allowed to authenticate to the machine.

Domain Account Authentication Figure 9-11 illustrates the **NTLM-family** challenge-response mechanism for authentication using a domain account to the domain-joined destination host, if the destination host is not a domain controller. If a host is a domain controller, the challenge-response mechanism is similar to that described for a local account in the "Local Account Authentication" section earlier in this chapter.

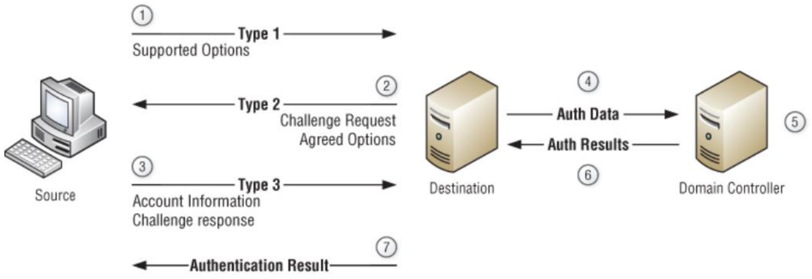


Figure 9-11: Challenge-response for domain accounts

The numbers in the following list correspond to the numbers in Figure 9-11:1–3.

1. These are the same as they are for a local account as described previously in this chapter.
2. 4. Because the destination host does not have access to domain user credentials, it cannot perform credentials validation. The destination host sends all data that is required for validation, such as username, initial challenge string, and challenge response, to one of the domain controllers for validation.
3. 5. The domain controller performs credentials validation using the method described in the "Local Account Authentication" section.
4. 6. After credentials validation is finished, the domain controller sends the authentication results back to the destination server.
5. 7. The destination server sends the results back to the source host.

Successful Domain Account Authentication

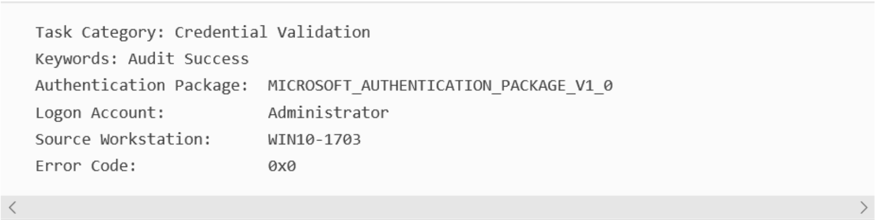
From an auditing perspective, some differences exist between successful local and domain accounts authentication.

An 8001 event on the source host is the same as the 8001 event discussed in the "Local Account Authentication" section.

On a destination host you will find all events that you saw in the "Local Account Authentication" section, except the **4776 event**, because the destination server cannot validate credentials for a domain account. Credentials for domain accounts are stored on domain controllers.

On an Active Directory domain controller, the event in Listing 9-6 occurs in the Windows security event log after successful NTLM-family protocol authentication for domain accounts.

Listing 9-6: Event ID 4776: The computer attempted to validate the credentials for an account.



```
Task Category: Credential Validation
Keywords: Audit Success
Authentication Package:  MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Logon Account:           Administrator
Source Workstation:      WIN10-1703
Error Code:              0x0
```

This event was discussed after Listing 9-2. Some parts of this event are specific to domain controllers.

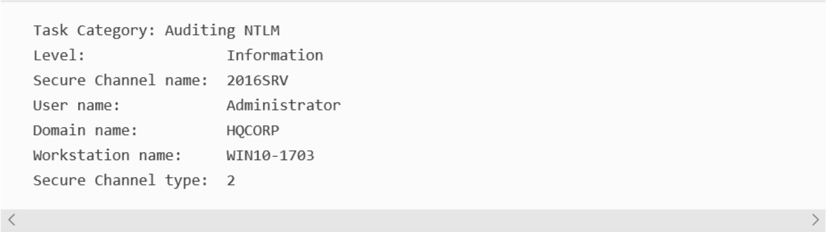
The Logon Account field shows the name of the domain account for which credentials were validated.

Source Workstation shows the name of the host from which a validation request was received by the destination host.

There is no information about the authentication target host (destination) in this event.

In addition to a 4776 event, the 8004 event in Listing 9-7 is generated in the NTLM event log on the domain controller.

Listing 9-7: Event ID 8004: Domain Controller Blocked Audit: Audit NTLM authentication to this domain controller.



```
Task Category: Auditing NTLM
Level:                 Information
Secure Channel name:   2016SRV
User name:             Administrator
Domain name:           HQCORP
Workstation name:      WIN10-1703
Secure Channel type:   2
```