帐户登录流程v0.1译版

初始化
系统帐户登录
安全包加载
获取身份验证数据并创建DWM会话
身份验证数据事务
本地用户帐号
初始化后
域用户帐户
登录类型
4688
4688
4608
4624
4627
4622
4610
4688
4648
4624
4627
4673
4611
4622
4610
4676
4648
4624
4627
4672
4688
4688
4648
4624
4624

Winlogon进程初始化

Winlogon是一个系统组件（是一个过程），充当用户和Windows身份验证子系统内部组件之间的代理组件。它还负责切换Windows桌面和处理安全注意序列（SAS）

LSASS 初始化

在步骤1的第二部分中，将初始化本地安全机构子系统服务（LSASS）过程。LSASS组件是一个过程，其中包含Windows安全子系统的组件。

系统启动成功

LSASS.EXE启动并初始化审核子系统时，将记录此事件。

```
Windows is starting up.
This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.
```

本地系统帐户登录

即使“本地系统”帐户是代表计算机本身的内置特殊帐户，它也会执行对系统的登录。

组成员信息

```
Group membership information.

Subject:
    Security ID:        S-1-5-7
    Account Name:       ANONYMOUS LOGON
    Account Domain:     NT AUTHORITY
    Logon ID:           0x0

Logon Type:             0

New Logon:
    Security ID:        S-1-5-18
```

安全程序包已由本地安全机构加载

A security package has been loaded by the Local Security Authority.

C:\Windows\system32\lsasrv.dll : Negotiate
C:\Windows\system32\negoexts.DLL : NegoExtender
C:\Windows\system32\kerberos.DLL : Kerberos
C:\Windows\system32\msv1_0.DLL : NTLM
C:\Windows\system32\tspkg.DLL : TSSSP
C:\Windows\system32\pku2u.DLL : pku2u
C:\Windows\system32\cloudAP.DLL : CloudAP
C:\Windows\system32\wdigest.DLL : WDigest
C:\Windows\system32\schannel.DLL : Schannel
C:\Windows\system32\schannel.DLL : Microsoft Unified Security Protocol Provider

```
Event 4622, Microsoft Windows security auditing.
General  Details
A security package has been loaded by the Local Security Authority.
Security Package Name:   C:\Windows\system32\lsasrv.dll : Negotiate
```

使用的安全系统扩展

本地安全机构已加载身份验证包。此身份验证包将用于对登录尝试进行身份验证。

```
Event 4610, Microsoft Windows security auditing.
General  Details
An authentication package has been loaded by the Local Security Authority.
This authentication package will be used to authenticate logon attempts.
Authentication Package Name:   C:\Windows\system32\msv1_0.DLL : MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
```

身份验证数据收集

LogonUI的目的是收集用户凭证并将它们传递给LSASS进行验证。每次需要从用户收集/收集经过身份验证的数据时，Winlogon都会调用LogonUI。LogonUI获取用户的凭据并将其传递给LSASS之后，它将终止。

```
A new process has been created.

Creator Subject:
    Security ID:        S-1-5-18
    Account Name:       DESKTOP-OIUVHRF$
    Account Domain:     WORKGROUP
    Logon ID:           0x3E7

Target Subject:
    Security ID:        S-1-0-0
    Account Name:       -
    Account Domain:     -
    Logon ID:           0x0

Process Information:
    New Process ID:         0x270
    New Process Name:       C:\Windows\System32\LogonUI.exe
    Token Elevation Type:   %%1936
    Mandatory Label:        S-1-16-16384
    Creator Process ID:     0x2e4
    Creator Process Name:   C:\Windows\System32\winlogon.exe
    Process Command Line:   "LogonUI.exe" /flags:0x0 /state0:0xa3bc9855 /state1:0x41c64e6d
```

SID	INTEGRITY LEVEL
S-1-16-0	Mandatory Label\Untrusted Mandatory Level
S-1-16-4096	Mandatory Label\Low Mandatory Level
S-1-16-8192	Mandatory Label\Medium Mandatory Level
S-1-16-12288	Mandatory Label\High Mandatory Level
S-1-16-16384	Mandatory Label\System Mandatory Level

试图使用显式凭据登录。

```
A logon was attempted using explicit credentials.

Subject:
    Security ID:        S-1-5-18
    Account Name:       DESKTOP-OIUVHRF$
    Account Domain:     WORKGROUP
    Logon ID:           0x3E7
    Logon GUID:         {00000000-0000-0000-0000-000000000000}

Account Whose Credentials Were Used:
    Account Name:       DWM-1
    Account Domain:     Window Manager
    Logon GUID:         {00000000-0000-0000-0000-000000000000}
```

桌面Windows管理器（DWM）登录

```
Logon Information:
    Logon Type:             2
    Restricted Admin Mode:  -
    Virtual Account:        Yes
    Elevated Token:         Yes

Impersonation Level:        Impersonation

New Logon:
    Security ID:            S-1-5-90-0-1
    Account Name:           DWM-1
    Account Domain:         Window Manager
    Logon ID:               0xEA7D
    Linked Logon ID:        0xEB09
    Network Account Name:   -
    Network Account Domain: -
    Logon GUID:             {00000000-0000-0000-0000-000000000000}

Process Information:
    Process ID:             0x2e4
    Process Name:           C:\Windows\System32\winlogon.exe

Network Information:
    Workstation Name:       -
    Source Network Address: -
    Source Port:            -

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

组成员信息

```
Group membership information.

Subject:
    Security ID:        S-1-5-18
    Account Name:       DESKTOP-OIUVHRF$
    Account Domain:     WORKGROUP
    Logon ID:           0x3E7

Logon Type:             2

New Logon:
    Security ID:        S-1-5-90-0-1
    Account Name:       DWM-1
    Account Domain:     Window Manager
    Logon ID:           0xEA7D
```

将凭据从Winlogon发送到LSASS

凭据提供程序从用户获取身份验证数据后，Winlogon调用LsaLogonUser函数将身份验证数据传递给LSASS。LsaLogonUser函数使用LSASS的ALPC端口LsaAuthenticationPort进行通信。

```
A privileged service was called.

Subject:
    Security ID:        S-1-5-18
    Account Name:       DESKTOP-OIUVHRF$
    Account Domain:     WORKGROUP
    Logon ID:           0x3E7

Service:
    Server:     NT Local Security Authority / Authentication Service
    Service Name:   LsaRegisterLogonProcess()

Process:
    Process ID:     0x334
    Process Name:   C:\Windows\System32\lsass.exe

Service Request Information:
    Privileges:     SeTcbPrivilege
```

已注册了受信任的登录过程

由于在此事件中成功地调用了LsaRegisterLogonProcess（）函数explain。现在信任此登录进程提交登录请求。此事件包含使用LsaRegisterLogonProcess（）成功注册的登录进程的名称（登录进程名称）。

```
Event 4611, Microsoft Windows security auditing.
General  Details
A trusted logon process has been registered with the Local Security Authority.
This logon process will be trusted to submit logon requests.

Subject:
    Security ID:        S-1-5-18
```

本地用户方案

如果该帐户是本地用户帐户，则将用户的凭据传递到协商安全支持提供程序（SSP），然后将其传递给MSV1_0安全支持提供程序/身份验证包（SSP / AP）。协商SSP在Kerberos SSP / AP和MSV1_0 SSP / AP之间进行选择。对于本地帐户交互式登录，选择了MSV1_0 SSP / AP。您将发现多个4622事件，这些事件通知您lsass.exe加载了特定的安全软件包（SSP / AP）。安全软件包名称具有Nfollowing格式：软件包DLL位置：软件包

使用的安全系统扩展

本地安全机构已加载身份验证包。此身份验证包将用于对登录尝试进行身份验证。

本地用户登录：MSV1_0应答

MSV1_0从SAM管理器获取用户的帐户哈希后，会将其与从用户提供的凭据生成的哈希进行比较。

```
The computer attempted to validate the credentials for an account.

Authentication Package:  MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Logon Account:   Andrei
Source Workstation:  DESKTOP-OIUVHRF
Error Code:      0x0
```

尝试使用显式凭据登录

该事件显示正常交互登录的登录启动尝试。它由本地SYSTEM帐户启动。

```
A logon was attempted using explicit credentials.

Subject:
    Security ID:        S-1-5-18
    Account Name:       DESKTOP-OIUVHRF$
    Account Domain:     WORKGROUP
    Logon ID:           0x3E7
    Logon GUID:         {00000000-0000-0000-0000-000000000000}

Account Whose Credentials Were Used:
    Account Name:       Andrei
    Account Domain:     DESKTOP-OIUVHRF
    Logon GUID:         {00000000-0000-0000-0000-000000000000}
```

帐户已在本地成功登录

此事件中的某些信息与4648事件中的信息相同。

```
New Logon:
    Security ID:            S-1-5-21-3560676733-2118901975-1824268897-1001
    Account Name:           Andrei
    Account Domain:         DESKTOP-OIUVHRF
    Logon ID:               0x301F8
    Linked Logon ID:        0x30233
    Network Account Name:   -
    Network Account Domain: -
    Logon GUID:             {00000000-0000-0000-0000-000000000000}

Process Information:
    Process ID:             0x1e8
    Process Name:           C:\Windows\System32\svchost.exe

Network Information:
    Workstation Name:       DESKTOP-OIUVHRF
    Source Network Address: 127.0.0.1
    Source Port:            0

Detailed Authentication Information:
    Logon Process:          User32
    Authentication Package: Negotiate
    Transited Services:     -
    Package Name (NTLM only):   -
    Key Length:             0
```

组成员信息

在每个4624成功登录事件之后，将调用4627事件。它包含用户所属的所有组的SID。

```
Group membership information.

Subject:
    Security ID:        S-1-5-18
    Account Name:       DESKTOP-OIUVHRF$
    Account Domain:     WORKGROUP
    Logon ID:           0x3E7

Logon Type:             2

New Logon:
    Security ID:        S-1-5-21-3560676733-2118901975-1824268897-1001
    Account Name:       Andrei
    Account Domain:     DESKTOP-OIUVHRF
    Logon ID:           0x301F8
```

```
Group Membership:
    %{S-1-5-32-544} (BUILTIN\Administrators)
    %{S-1-1-0}      (Everyone)
    %{S-1-5-11}     (NT AUTHORITY\Authenticated Users)
    %{S-1-16-16384} (Mandatory Label\System Mandatory Level)
```

分配给新登录的特殊特权。

如果用户的提升的令牌具有特殊特权之一，则将生成4672事件，其中包含所有检测到的特殊特权。

```
Special privileges assigned to new logon.

Subject:
    Security ID:        S-1-5-21-3560676733-2118901975-1824268897-1001
    Account Name:       Andrei
    Account Domain:     DESKTOP-OIUVHRF
    Logon ID:           0x301F8

Privileges:     SeSecurityPrivilege
                SeTakeOwnershipPrivilege
                SeLoadDriverPrivilege
                SeBackupPrivilege
                SeRestorePrivilege
                SeDebugPrivilege
                SeSystemEnvironmentPrivilege
                SeImpersonatePrivilege
                SeDelegateSessionUserImpersonatePrivilege
```

Userinit.exe

在本地交互式登录身份验证过程结束时，Winlogon将信息发送到userinit.exe进程，该进程将加载用户的文件。加载用户配置文件后，userinit.exe创建一个本地shell，调用explorer.exe进程。您将看到两个4688事件：一个用于userinit.exe，另一个用于explorer.exe。Winlogon.exe创建userinit.exe，然后userinit.exe创建explorer.exe。

```
A new process has been created.

Creator Subject:
    Security ID:        S-1-5-18
    Account Name:       WIN10$
    Account Domain:     WINDOMAIN
    Logon ID:           0x3E7

Target Subject:
```

Explorer.exe

Userinit.exe 创建explorer.exe

```
A new process has been created.

Creator Subject:
    Security ID:        S-1-5-21-975009023-2096196009-2744413307-500
    Account Name:       Administrator
    Account Domain:     WINDOMAIN
    Logon ID:           0x23D0FF3

Target Subject:
    Security ID:        S-1-0-0
    Account Name:       -
    Account Domain:     -
    Logon ID:           0x0

Process Information:
    New Process ID:         0x528
    New Process Name:       C:\Windows\explorer.exe
    Token Elevation Type:   %%1936
    Mandatory Label:        S-1-16-8192
    Creator Process ID:     0x243c
    Creator Process Name:   C:\Windows\System32\userinit.exe
    Process Command Line:   C:\Windows\Explorer.EXE
```

域用户方案

协商SSP选择适当的身份验证包来处理身份验证请求。它将始终首先尝试Kerberos AP。如果Kerberos AP能够继续该请求，则将数据发送到域控制器进行验证。

试图使用显式凭据登录。

该事件显示正常交互登录的登录启动尝试。它由本地SYSTEM帐户启动。

```
A logon was attempted using explicit credentials.

Subject:
    Security ID:        S-1-5-18
    Account Name:       WIN10-1703$
    Account Domain:     HQCORP
    Logon ID:           0x3E7
    Logon GUID:         {00000000-0000-0000-0000-000000000000}

Account Whose Credentials Were Used:
    Account Name:       Administrator
    Account Domain:     HQCORP
    Logon GUID:         {120fa028-8ce9-1908-bbf6-3a08d2084e5e}

Target Server:
    Target Server Name:     localhost
    Additional Information: localhost

Process Information:
    Process ID:         0x258
    Process Name:       C:\Windows\System32\svchost.exe

Network Information:
    Network Address: 127.0.0.1
    Port:            0
```

域控制器上的凭据验证

如果Kerberos或MSV1_0程序包能够访问域控制器，则域控制器将验证凭据。

域帐户已在本地成功登录

```
An account was successfully logged on.

Subject:
    Security ID:        S-1-5-18
    Account Name:       WIN10-1703$
    Account Domain:     HQCORP
    Logon ID:           0x3E7

Logon Information:
    Logon Type:             2
    Restricted Admin Mode:  -
    Virtual Account:        No
    Elevated Token:         Yes

Impersonation Level:        Impersonation

New Logon:
    Security ID:            S-1-5-21-1913345275-1711810662-261465553-500
    Account Name:           Administrator
    Account Domain:         HQCORP
    Logon ID:               0x1AD56B
    Linked Logon ID:        0x0
    Network Account Name:   -
    Network Account Domain: -
    Logon GUID:             {120fa028-8ce9-1908-bbf6-3a08d2084e5e}

Process Information:
    Process ID:             0x258
    Process Name:           C:\Windows\System32\svchost.exe

Network Information:
    Workstation Name:       WIN10-1703
    Source Network Address: 127.0.0.1
    Source Port:            0

Detailed Authentication Information:
    Logon Process:          User32
    Authentication Package: Negotiate
    Transited Services:     -
    Package Name (NTLM only):   -
    Key Length:             0
```

- **Identification (%%1832):** The process knows the client's identity information (such as group membership, account name and so on) and can perform access validation checks, but it cannot impersonate the client (act on behalf of a client). This type of impersonation is useful for access validation attempts, when there is no need to act as a client.
- **Impersonation (%%1833):** The process can completely impersonate the client on the local machine and act on behalf of the client. This type of impersonation does not allow the process to impersonate a client outside of the system, as such connecting to other hosts on behalf of the client.
- **Delegation (%%1840):** The process can completely impersonate the client on the local and remote machine. This type of impersonation is usually set up in Active Directory environments by using the Delegation tab for the computer or user object.

帐户已成功登录

- RemoteInteractive Logon (10)
- RemoteInteractive Logon Cached Credentials (12)
- Interactive Logon With Cached Credentials (11)
- Network Logon (3)
- NetworkCleartext Logon (8)
- Unlock Logon (7)

https://twitter.com/rimpq

Special thanks to **Andrei Miroshnikov** for awesome book **"Windows Security Monitoring: Scenarios and Patterns"** https://www.amazon.com/gp/product/B07BGHYF61

GitHub

翻译版下载地址：https://github.com/12306Bro/Hunting-guide/blob/master/windows_account_logon_flow_v0.1.pdf