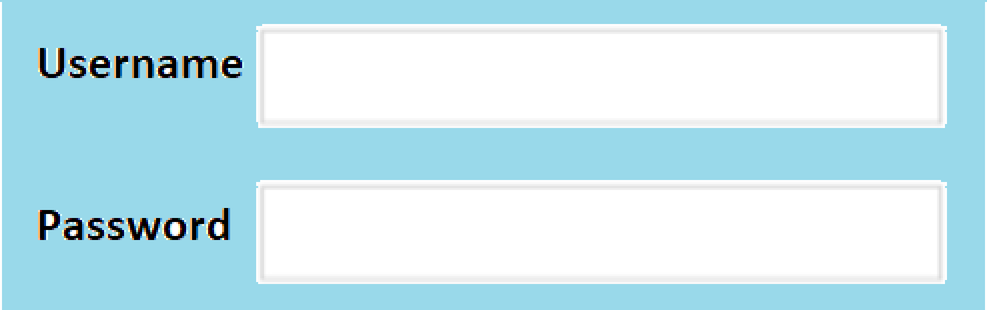
בס''ד

LOGON TYPE

Windows Logon Types and how they contribute to SOC Analyst

Zissi Skarzhinski for CyberSafe, 2021

How does an interaction between a user and a machine start?



Username

Password

There are several types of Windows LOGONs that add to our knowledge about successful or failed logon of the user.

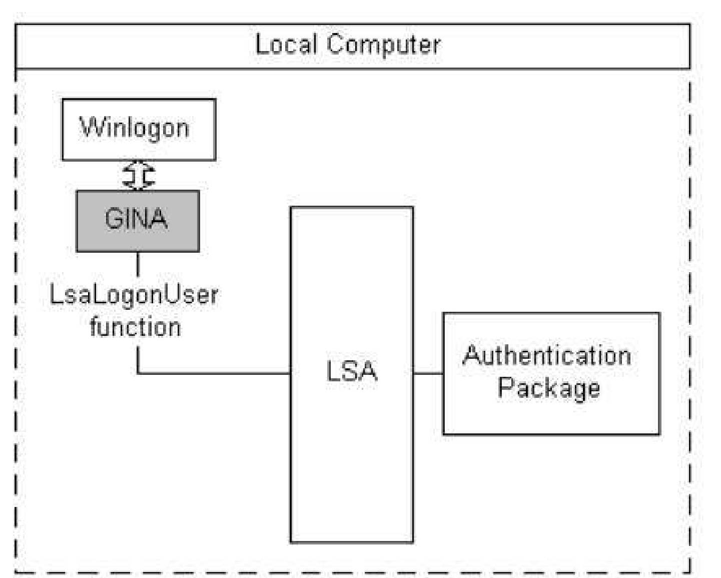
When we have Logon type, we are able to know, was the user in front of the computer, or connected remotely, did he unlock the save screen, or may be it was not a human – but a service?

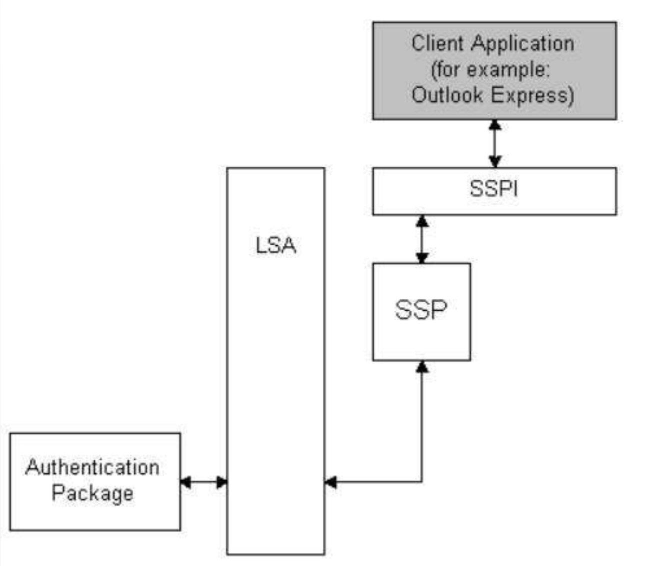
How can it help SOC Analyst?

Knowing the way the user has connected gives us a tool to separate suspicious Logons from benign ones.

INTERACTIVE LOGON VS NONINTERACTIVE LOGON

- Type 2 – Interactive
- Type 3 – Network
- Type 7 - Unlock
- Type 10 – RemoteInteractive (Terminal services, Remote Desktop Services)





Interactive logon process begins either when a user enters **credentials** in the credentials entry dialog box, or when the user inserts a **smart card** into the smart card reader, or when the user interacts with **a biometric** device. Users can perform an interactive logon by using a local user account or a domain account to log on to a computer.
Non-interactive user Logon is performed by a **client app** or an OS component **on behalf** of a user. These Logons do not require the user to supply an Authentication factor. Instead, the device or **client app uses a token or code** to authenticate or access a resource on behalf of a user. These logons happen in the background of the user's activity.
Domain logon - combines necessary elements for a local logon, such as account name and password or certificate, and Active Directory domain information.

GINA Graphical Identification and Authentication (DLL). loaded by the Winlogon, implements the authentication policy of the interactive logon model, performs all identification and authentication user interactions

EXAMPLES OF NONINTERACTIVE LOGON

- A client app uses an OAuth 2.0 refresh token to get an access token.
- A client uses an OAuth 2.0 authorization code to get an access token and refresh token.
- A user performs single sign-on (SSO) to a web or Windows app on an Azure AD joined PC.
- A user signs in to a second Microsoft Office app while they have a session on a mobile device using FOCI (Family of Client IDs).

- During the investigation of SolarWinds there was a branch in Threat Hunting process, when the Microsoft Researches checked , if the malicious actor used a sensitive app to gain “Data Access”

Audit the creation and use of service principal and application credentials. Sparrow will detect modifications to these credentials. Look for unusual application usage, such as inactive or forgotten applications being used again. **Audit the assignment of credentials to applications that allow non-interactive sign-in by the application.** *Look for unexpected trust relationships that have been added to Azure AD.*

https://techcommunity.microsoft.com/t5/azure-sentinel/non-interactive-logins-minimizing-the-blind-spot/ba-p/2287932

LOGON PROCESSES

Logon Process field in a Windows log provides a hint at how the user **tried to access the system**: at its console, through Server Message Block (SMB – for shared files) or Common Internet File System (CIFS - network filesystem protocol used for providing **shared access to files** and printers) for shared-folder access, or through IIS. Some logon processes are authentication-protocol specific as shown in the chart below.

Process	Explanation
Winlogon	Windows Logon Process
Schannell	Secure connection such as SSL, TLS
Secondary Logon Service	(runas)- SecLogo
IKE	Internet Key Exchange protocol process
Advapi	Web-based logon: IIS logon processes
PKU2U	User-2-User Public Key Cryptography
Kerberos	Ticket-based, for secure nodes communication over non-secure network, domain
NtLmSsp	NT Lan Manager Hash-based – used locally

https://medium.com/@robert.broeckelmann/kerberos-and-windows-security-kerberos-on-windows-3bc021bc9630

SECURITY SUPPORT PROVIDERS - SSP

An SSP is a software module that performs security validation.

Negotiate – SSP that acts as application layer between SSPI (interface) and other SSP. When an application calls into SSPI to log on to a Network, it calls Negotiate, that can choose the best SSP to handle the request based on customer-configured security policy.

KERBEROS protocol security package - industry-standard security package. Has 3 parts: Client, Server and Key Distribution Center with 2 components: Authentication service and Ticket-granting-Ticket service.

NTLM Security Package - This was the primary security package for NTLM (NT (New Technology) LAN Manager) networks. Uses Hashes. Two parts: Client and Host. Works with generated hashes sent over a Network.

SCHANNEL SSP - implements the Microsoft Unified Protocol Provider security package, which unifies SSL, private communication technology (PCT), and transport level security (TLS) into one security package. Schannel is primarily used for Internet applications that require secure Hypertext Transfer Protocol (HTTP) communications.

WDIGEST - a challenge/response protocol that was primarily used in Windows Server 2003 for LDAP and web-based authentication. It utilizes Hypertext Transfer Protocol (HTTP) and Simple Authentication Security Layer (SASL) exchanges to authenticate.
(there are some more)

LOGON TYPES

2

Logon Type 2 – Interactive.

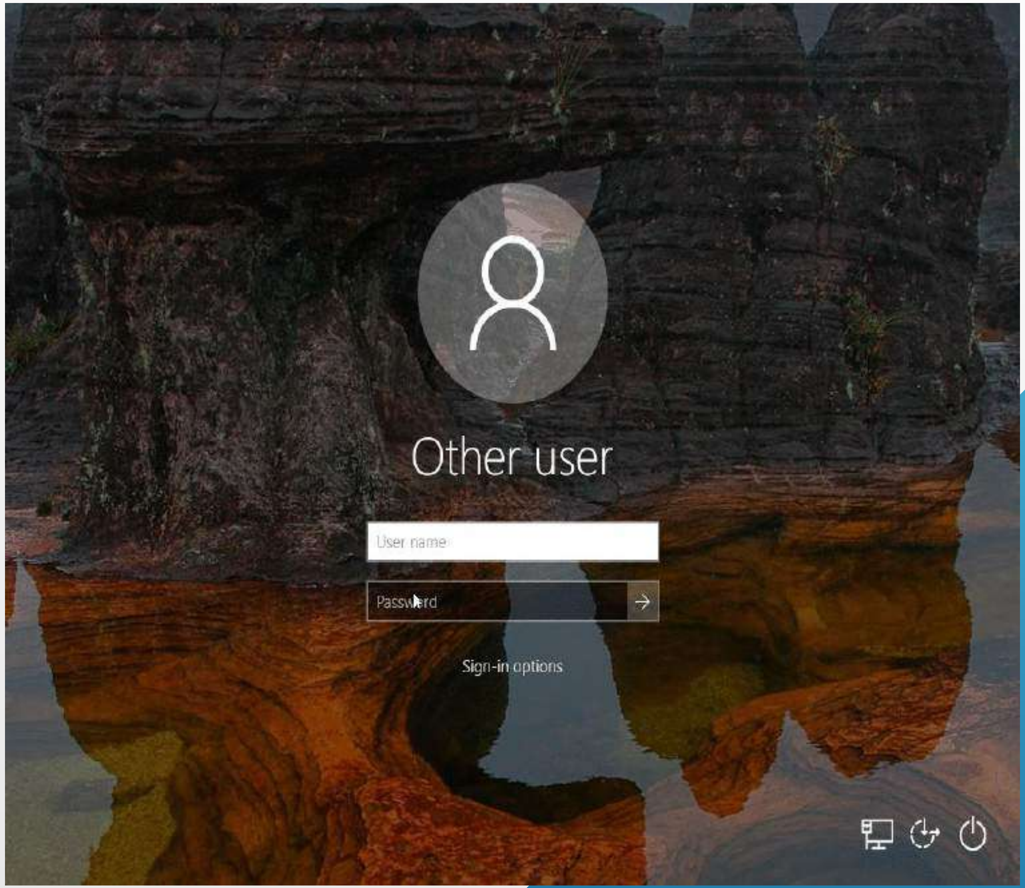
This is just logging on a local computer, typing user name and password.

User logs on with a local or a domain account.

This logon type will appear only when a user really authenticated in the **domain** (by a domain controller). In case the DC is not available, but the user provided valid domain credentials cached in the local PC, Windows will log an event with logon type = 11 (CachedInteractive).

Authenticators: Password, Smartcard

> A local logon grants a user permission to access Windows resources on the local computer.
> A local logon requires that the user has a user account in the Security Accounts Manager (SAM) on the local computer.



LOGON TYPES

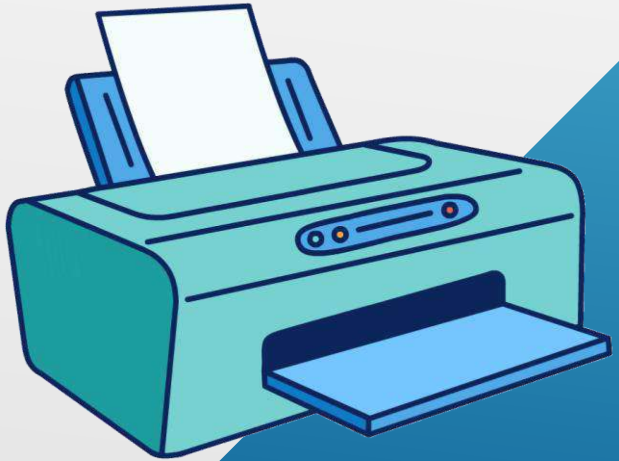
3

Logon Type 3 – Network.

A computer was accessed from the Network. Mostly connecting to shared resources (like shared folders) and printers**.**
A network logon grants a user permission to access Windows resources on the local computer **in addition** to any resources on networked computers, as defined by the credential's access token. Only **after** local authentication.

Most logons to **I**nternet **I**nformation **S**ervices (**IIS**) are Type 3, the exception is basic authentication which is explained in Logon Type 8.

[Because IIS is a service for hosting a website, that can be put on a Windows machine, it's like accessing a machine from Network]
Authenticators**:** Password, Kerberos ticket, NT Hash.



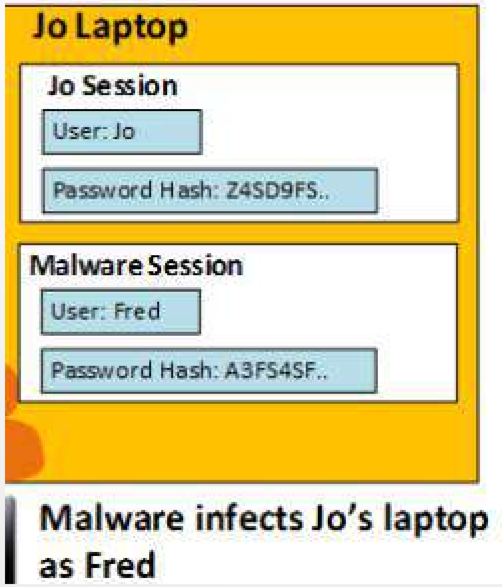
Detection:

3

Pass-the-Hash Detection:

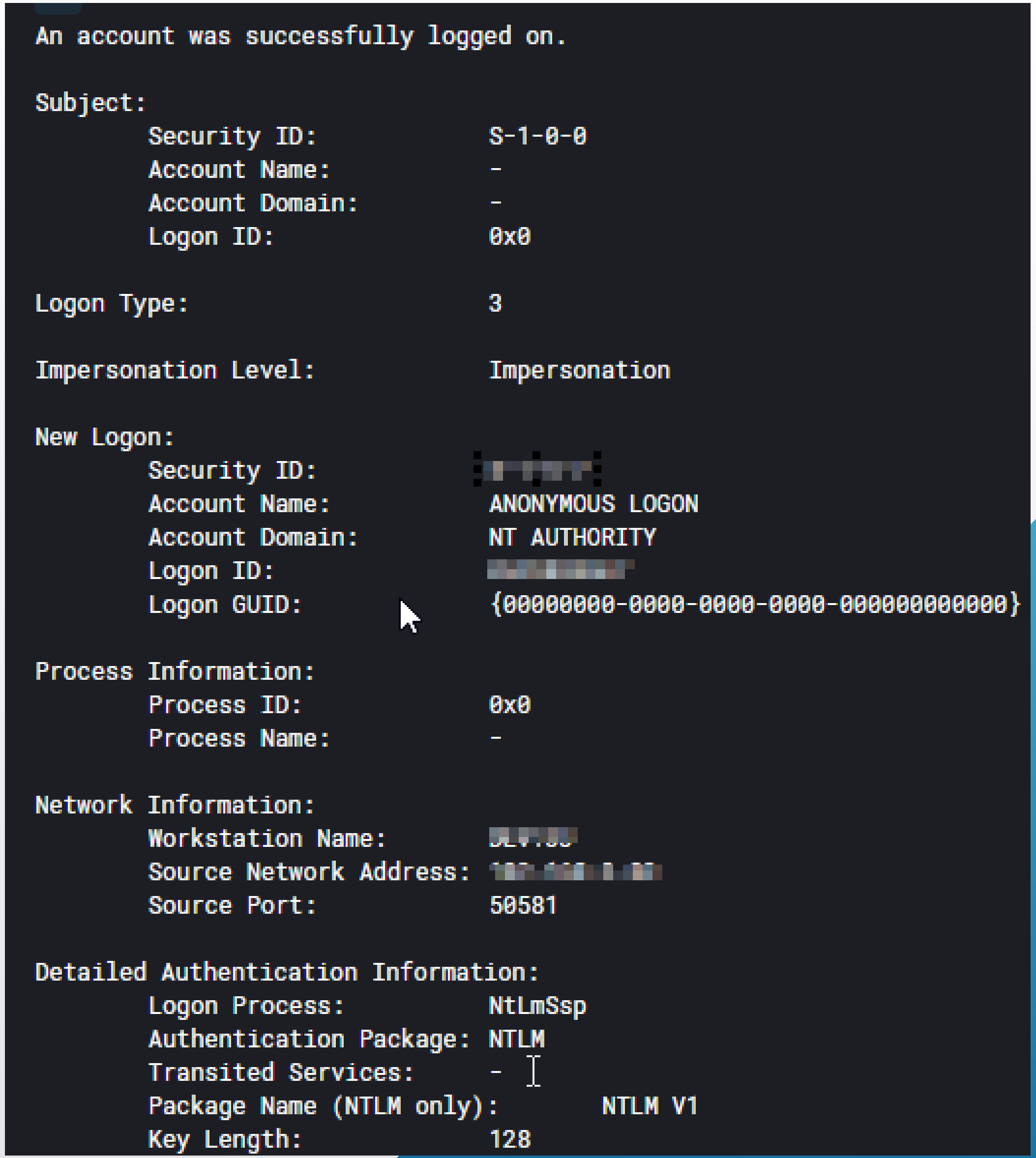
After a computer in a network has been compromised by a remote actor,

lateral movement of PtH attempts can be seen between workstations:



Malware infects Jo's laptop as Fred

- Microsoft Event Security Log ID **4624**
    - LogonType **3** using **NTLM**
    - Event level **information**
    - Authentication is NOT a domain and NOT anonymous
    - Security ID is commonly null for PtH attacks



```
An account was successfully logged on.

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

Logon Type:                     3

Impersonation Level:            Impersonation

New Logon:
        Security ID:            [redacted]
        Account Name:           ANONYMOUS LOGON
        Account Domain:         NT AUTHORITY
        Logon ID:               [redacted]
        Logon GUID:             {00000000-0000-0000-0000-000000000000}

Process Information:
        Process ID:             0x0
        Process Name:           -

Network Information:
        Workstation Name:       [redacted]
        Source Network Address: [redacted]
        Source Port:            50581

Detailed Authentication Information:
        Logon Process:          NtLmSsp
        Authentication Package: NTLM
        Transited Services:     -
        Package Name (NTLM only):       NTLM V1
        Key Length:             128
```

LOGON TYPES

4

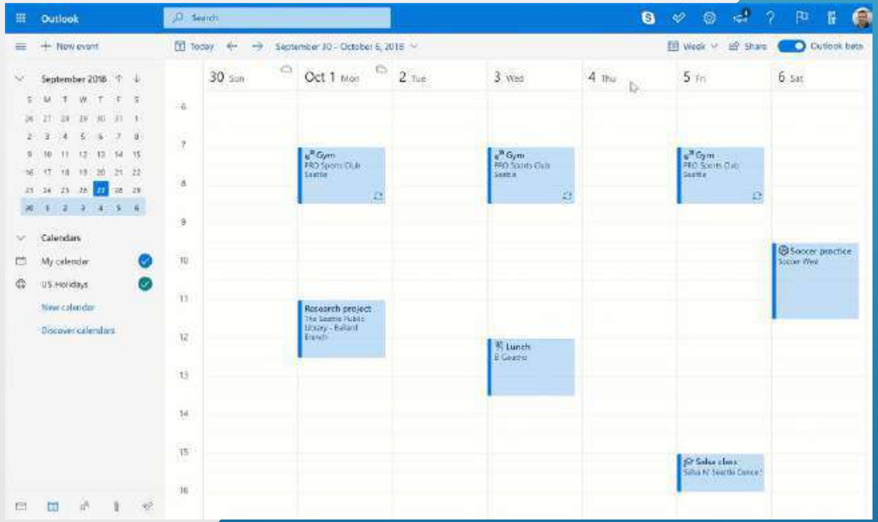
Logon Type 4 – Batch

This concerns Scheduled Tasks.

When Windows executes a scheduled task, the Scheduled Task service first creates a **new logon session** for the task so that it can run under the **authority** of the **user account specified**, when the task was created.

Logon type 4 events are usually benign, but a **malicious user** could try to guess the password of an account through scheduled tasks. Such attempts would generate a **logon failure** event where **logon type is 4.**

But logon failures associated with scheduled tasks can also result from an **administrator entering the wrong password** for the account at the time of task creation or from the password of an account being changed **without modifying the scheduled task** to use the new password.
Authenticators: Password (usually stored as LSA secret)
It is recommended to monitor **schtasks.exe** and **at.exe** (old) and their parent processes.



CyberSafe

LOGON TYPES

5

Logon Type 5 – Service

Each **service** is configured to run as a **specified user account**.

Example: running tomcat9.exe as Administrator.

When a service starts, Windows first creates a logon session for the specified user account which results in an event with logon type 5. **Failed logon** events with logon type 5 usually indicate the password of an account has been changed without updating the service.

But the changes can be made by **malicious user**, who has Admin rights, because for creating a new service or editing an existing service **high privileges required**.
Authenticators: Password (usually stored as LSA secret)

LOGON TYPES

7

Logon Type 7 – Unlock

When user leaves the computer for a period of time, there possibly is a screen saver, that locks the computer, so that unattended workstation is protected from malicious use.
Logon type 7 occurs, when user comes back to his computer and unlocks it.

Failed logons with logon type 7 indicate either a **user** entering the **wrong password** or a **malicious user** trying to unlock the computer by **guessing** the password.
We monitor Successful Logins to DC with logon type 7.

LOGON TYPES

8

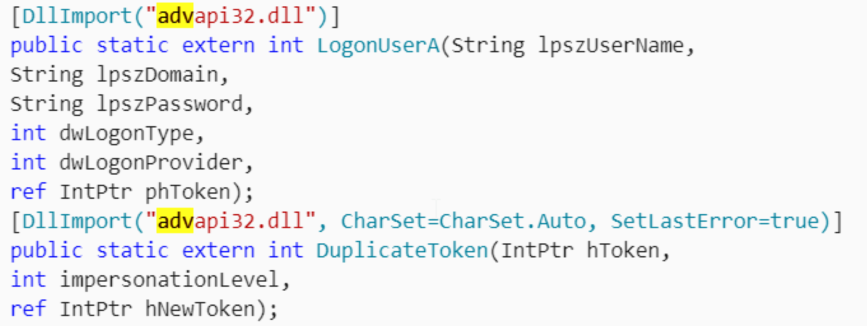
Logon Type 8 – NetworkCleartext

Similar to network logon type 3, but here the **password** was sent over the network in the **clear text**.

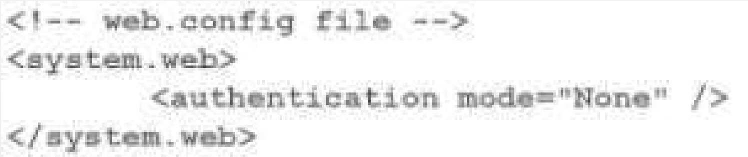
[Windows server doesn’t allow connection to shared files or printers with clear text authentication.]

Those can be logons from **within an ASP script** using the **ADVAPI**, or when a user logs on to IIS using **IIS’s basic authentication mode**. In both cases the logon process in the event’s description will list advapi. Basic authentication is dangerous, if it isn’t over an SSL session (i.e. https).

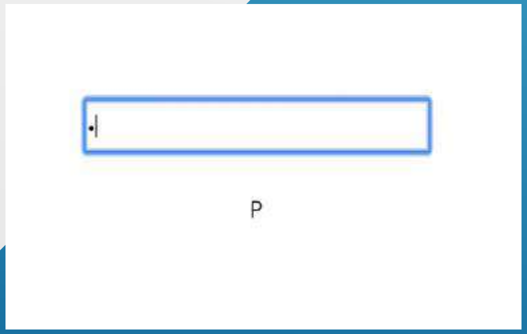
The password shall not be embedded in source code in ASP script. It is a bad practice for maintenance purposes, as well as risk that someone malicious will view the source code and get the password.



```
[DllImport("advapi32.dll")]
public static extern int LogonUserA(String lpszUserName,
String lpszDomain,
String lpszPassword,
int dwLogonType,
int dwLogonProvider,
ref IntPtr phToken);
[DllImport("advapi32.dll", CharSet=CharSet.Auto, SetLastError=true)]
public static extern int DuplicateToken(IntPtr hToken,
int impersonationLevel,
ref IntPtr hNewToken);
```



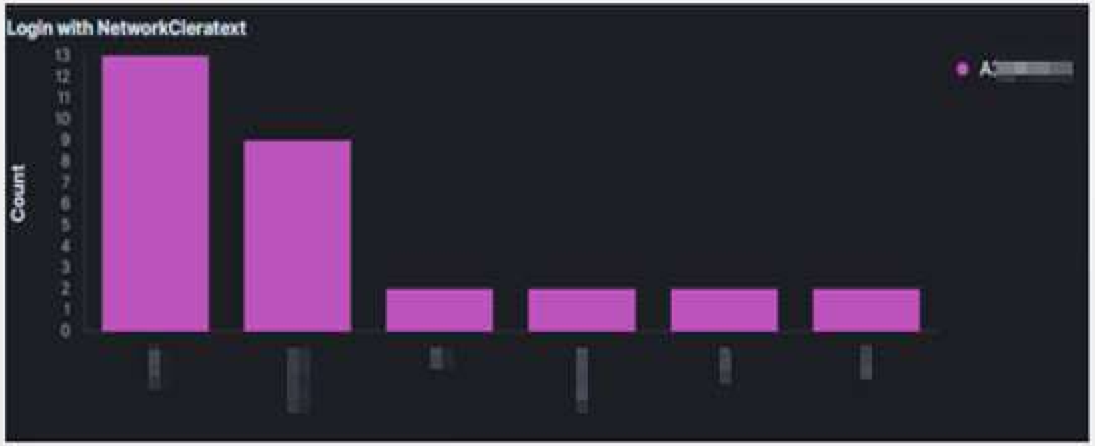
```
<!-- web.config file -->
<system.web>
        <authentication mode="None" />
</system.web>
```

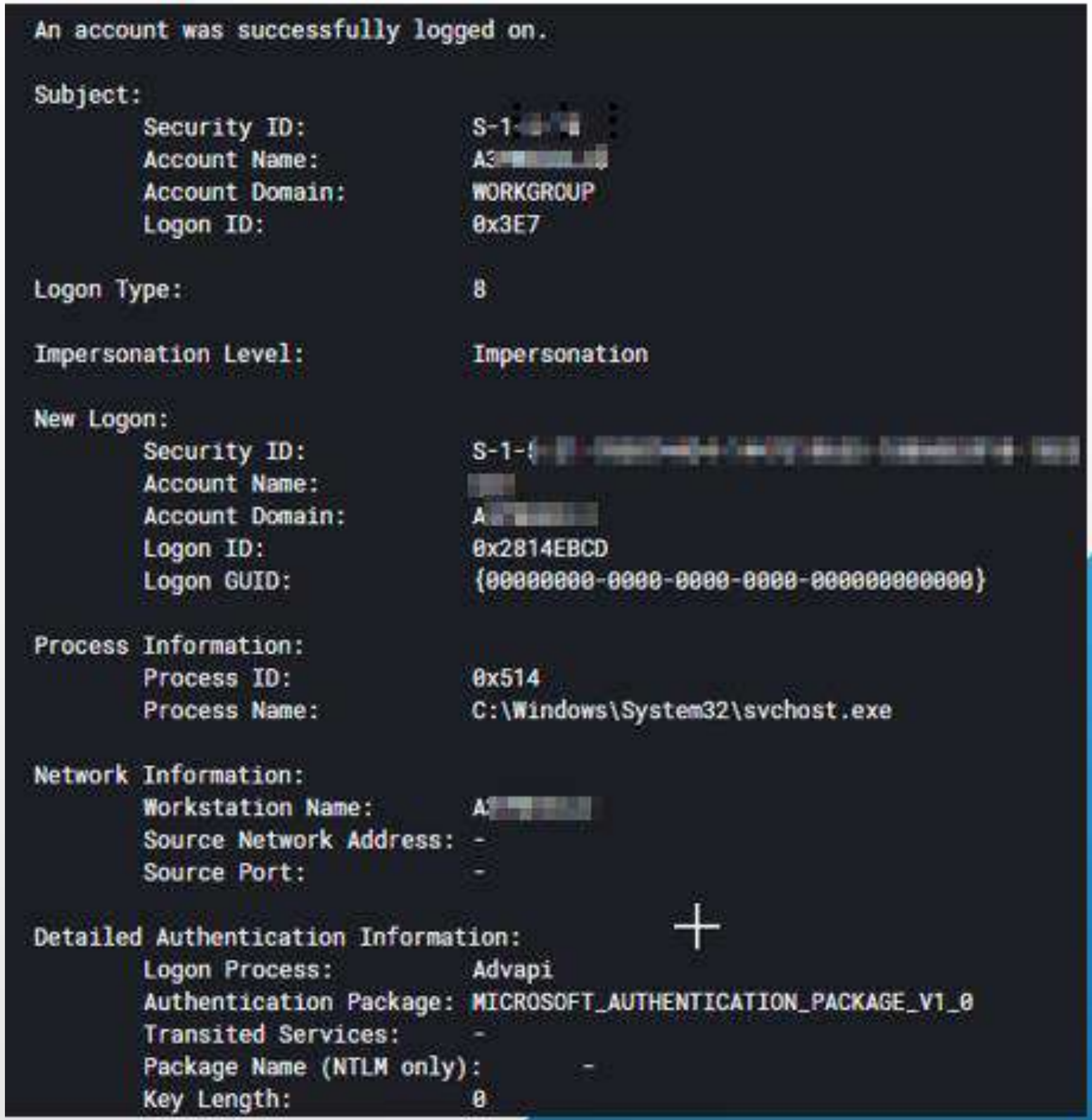


*ADVAPI = Advanced Windows 32 Base API, Advapi32.dll; it is an **API services library** that supports security and registry calls. advapi32.dll **includes a token** that allows the local machine admin user to Logon. This token can be copied and used to impersonate the local machine admin allowing remote users to log into windows*

Logon Type 8 – NetworkCleartext

Example:





```
An account was successfully logged on.

Subject:
        Security ID:            S-1-[redacted]
        Account Name:           A3[redacted]
        Account Domain:         WORKGROUP
        Logon ID:               0x3E7

Logon Type:                     8

Impersonation Level:            Impersonation

New Logon:
        Security ID:            S-1-[redacted]
        Account Name:           [redacted]
        Account Domain:         A[redacted]
        Logon ID:               0x2814EBCD
        Logon GUID:             {00000000-0000-0000-0000-000000000000}

Process Information:
        Process ID:             0x514
        Process Name:           C:\Windows\System32\svchost.exe

Network Information:
        Workstation Name:       A[redacted]
        Source Network Address: -
        Source Port:            -

Detailed Authentication Information:
        Logon Process:          Advapi
        Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
        Transited Services:     -
        Package Name (NTLM only):       -
        Key Length:             0
```

LOGON TYPES

9

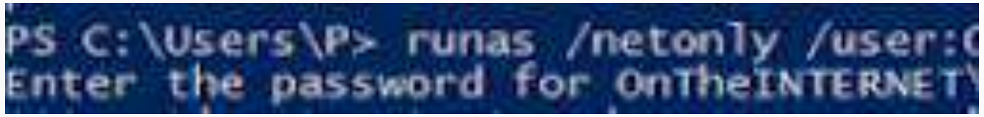
Logon Type 9 – NewCredentials

Using the **RunAs** command to start a program under a different user account, and specifying the **/netonly** switch, will result in Windows record a logon event type 9.

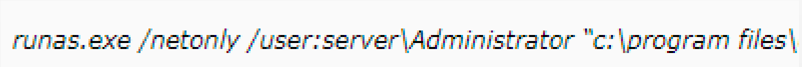
Example: run a program, but grant it extra permissions for network computers, specify user Administrator and provide the password, when prompted.

Using runas /netonly allows you to run your application **locally as you**, while authenticating over a **network** with **another user**.

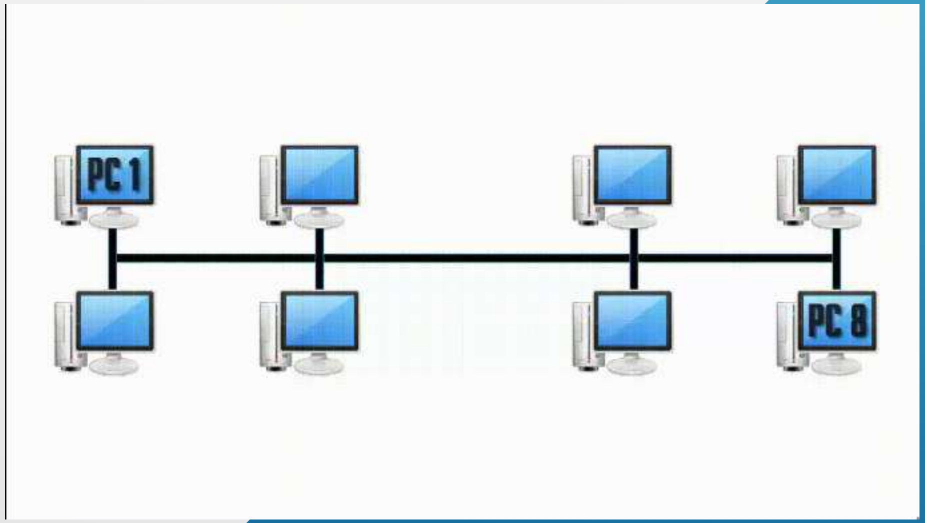
Without /netonly Windows runs the program on the local computer and on the network as the specified user, and records the logon event as type 2.



```
PS C:\Users\P> runas /netonly /user:O
Enter the password for OnTheINTERNET\
```



```
runas.exe /netonly /user:server\Administrator "c:\program files\
```



http://www.pseale.com/pretend-youre-on-the-domain-with-runas-netonly
https://ss64.com/nt/runas.html

Detection: PtH

9

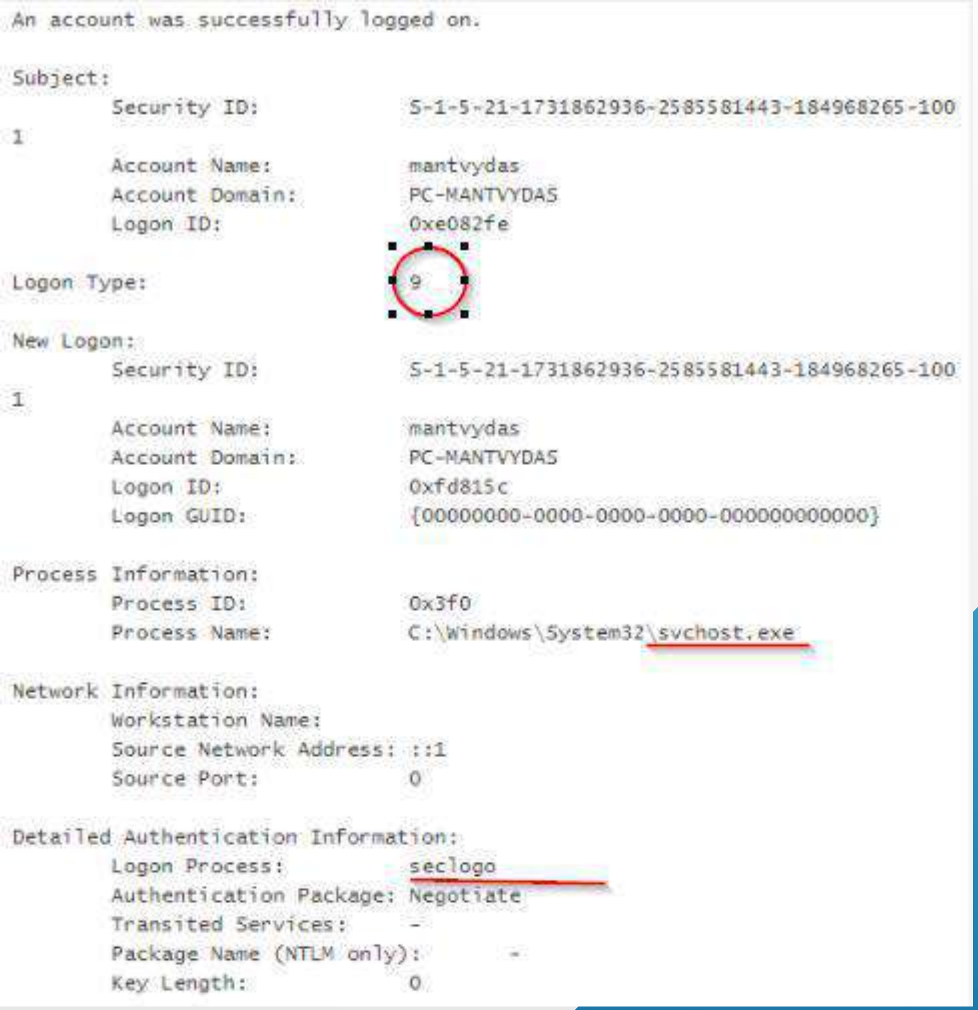
Logon Type 9 – NewCredentials

Can help to detect Pass-the-Hash Attack:

event ID: 4624
Logon process: Seclogo
Logon type: 9
Authentication Package = Negotiate

Logon type 9 means that any network connections originating from new process will use the new credentials.

Here: user mantyvdas ran a command:
runas /user:low /netonly cmd =>

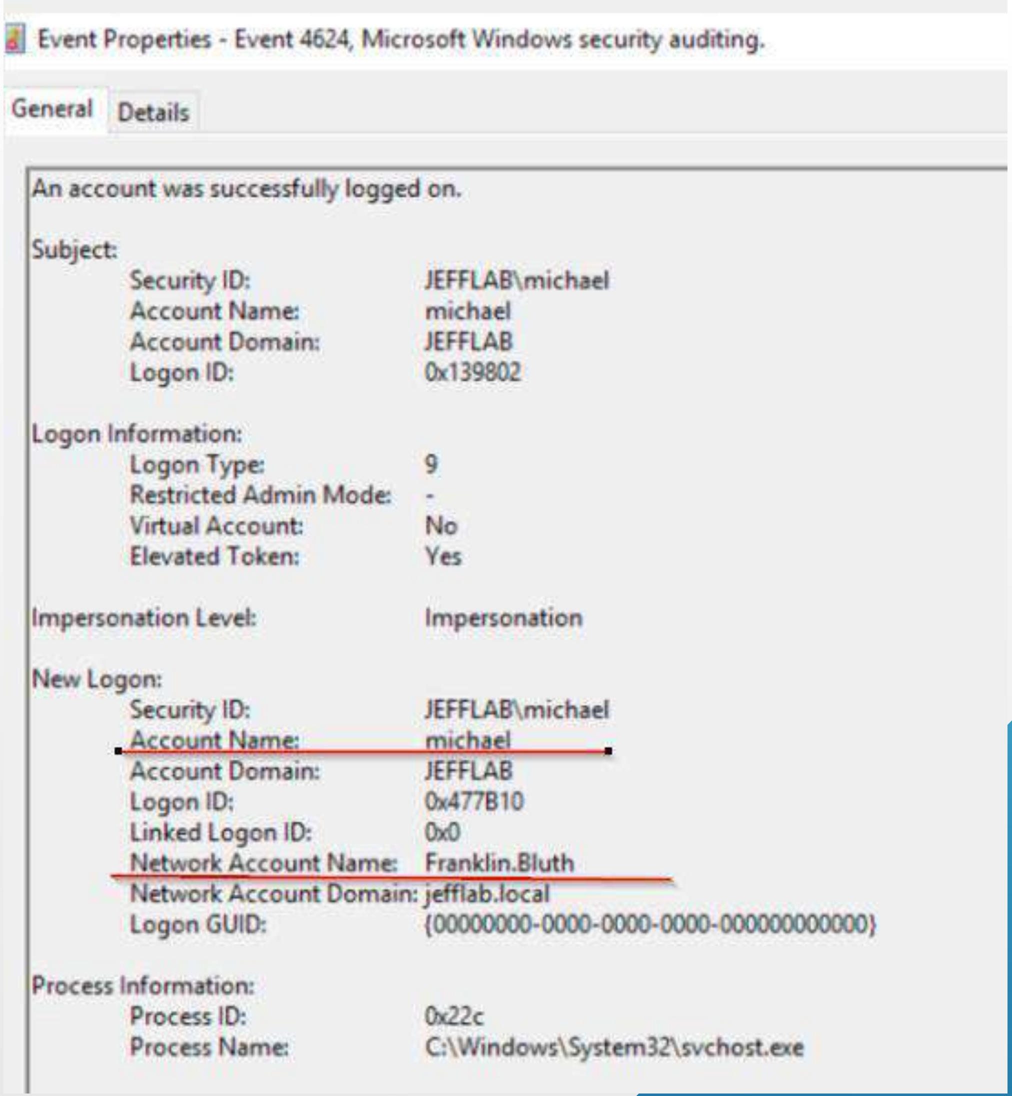


```
An account was successfully logged on.

Subject:
        Security ID:            S-1-5-21-1731862936-2585581443-184968265-100
1
        Account Name:           mantvydas
        Account Domain:         PC-MANTVYDAS
        Logon ID:               0xe082fe

Logon Type:                     9

New Logon:
        Security ID:            S-1-5-21-1731862936-2585581443-184968265-100
1
        Account Name:           mantvydas
        Account Domain:         PC-MANTVYDAS
        Logon ID:               0xfd815c
        Logon GUID:             {00000000-0000-0000-0000-000000000000}

Process Information:
        Process ID:             0x3f0
        Process Name:           C:\Windows\System32\svchost.exe

Network Information:
        Workstation Name:
        Source Network Address: ::1
        Source Port:            0

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

https://www.ired.team/offensive-security/credential-access-and-credential-dumping/network-vs-interactive-logons

Detection: PtH

Another example:



Event Properties - Event 4624, Microsoft Windows security auditing.

```
An account was successfully logged on.

Subject:
        Security ID:                JEFFLAB\michael
        Account Name:               michael
        Account Domain:             JEFFLAB
        Logon ID:                   0x139802

Logon Information:
        Logon Type:                 9
        Restricted Admin Mode:      -
        Virtual Account:            No
        Elevated Token:             Yes

Impersonation Level:                Impersonation

New Logon:
        Security ID:                JEFFLAB\michael
        Account Name:               michael
        Account Domain:             JEFFLAB
        Logon ID:                   0x477B10
        Linked Logon ID:            0x0
        Network Account Name:       Franklin.Bluth
        Network Account Domain:     jefflab.local
        Logon GUID:                 {00000000-0000-0000-0000-000000000000}

Process Information:
        Process ID:                 0x22c
        Process Name:               C:\Windows\System32\svchost.exe
```

https://stealthbits.com/blog/how-to-detect-pass-the-hash-attacks/

LOGON TYPES

10

Logon Type 10 – RemoteInteractive

When you access a computer through Terminal Services, Remote Desktop or Remote Assistance, Windows logs the logon attempt with logon type 10.

(Prior to XP, Windows 2000 doesn't use logon type 10 and Terminal Services logons are reported as logon type 2.)

We monitor Remote Interactive login to DC.

Detection: RDP over reverse SSH Tunnel

10

EventID 4624 with Logon Type =10

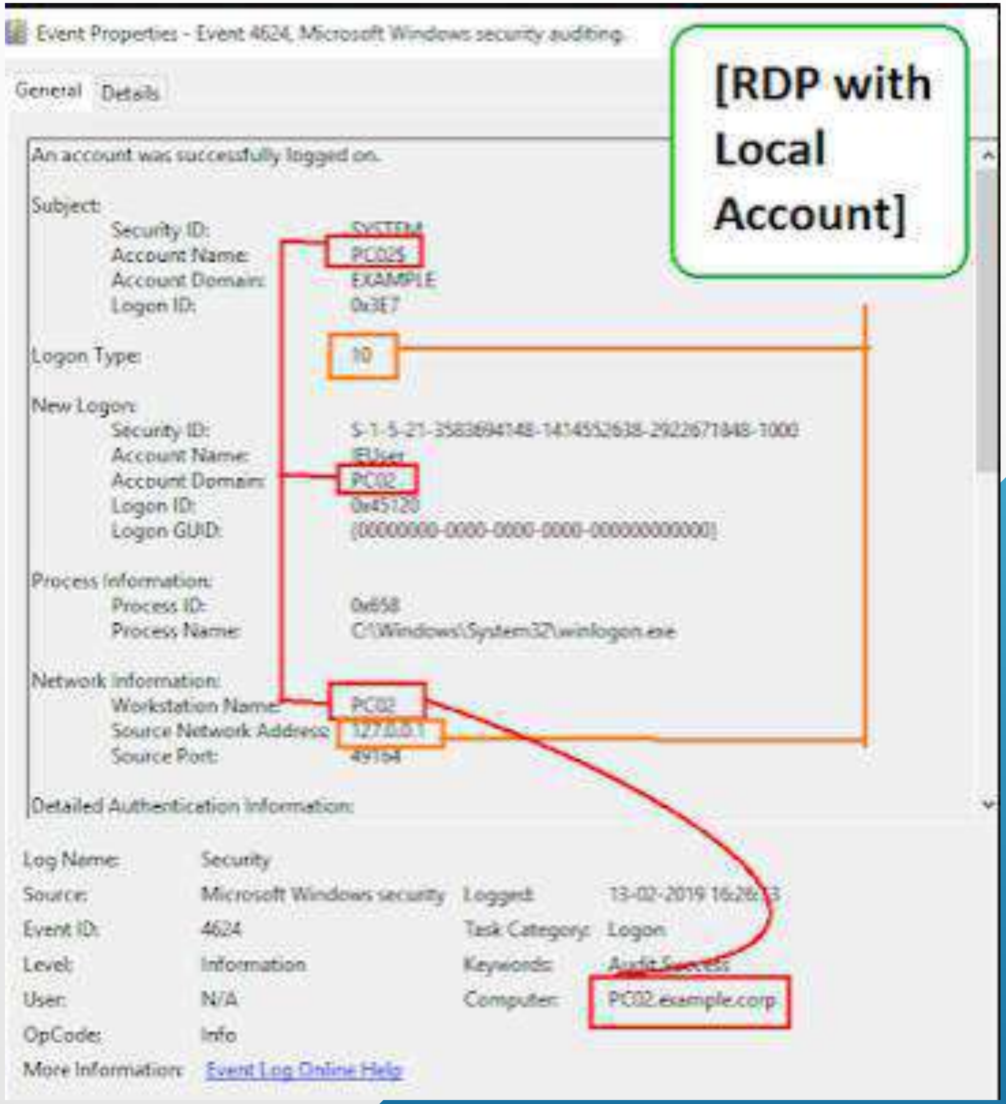
Source IP address = loopback address

Source Workstation Name = Account Domain=Subject-Account Name

(those indicators are very abnormal)

Command used:
plink.exe 10.0.2.17 -P 80 -C -R 127.0.0.1:12345::3389 -l test -pw test

https://blog.menasec.net/2019/02/



Event Properties - Event 4624, Microsoft Windows security auditing.
General
Details
[RDP with Local Account]

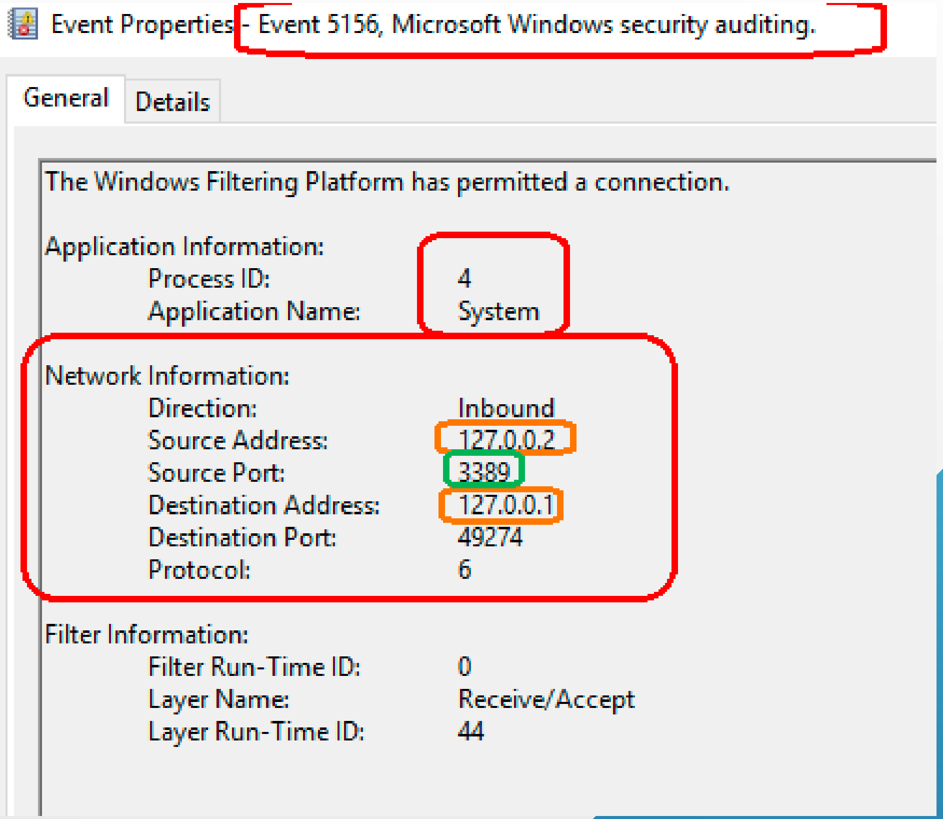
```
An account was successfully logged on.

Subject:
        Security ID:            SYSTEM
        Account Name:           PC02$
        Account Domain:         EXAMPLE
        Logon ID:               0x3E7

Logon Type:                     10

New Logon:
        Security ID:            S-1-5-21-3583694148-1414552638-2922671848-1000
        Account Name:           IEUser
        Account Domain:         PC02
        Logon ID:               0x45120
        Logon GUID:             {00000000-0000-0000-0000-000000000000}

Process Information:
        Process ID:             0x658
        Process Name:           C:\Windows\System32\winlogon.exe

Network Information:
        Workstation Name:       PC02
        Source Network Address: 127.0.0.1
        Source Port:            49164

Detailed Authentication Information:
```

```
Log Name:          Security
Source:            Microsoft Windows security   Logged:         13-02-2019 16:28:13
Event ID:          4624                         Task Category:  Logon
Level:             Information                  Keywords:       Audit Success
User:              N/A                          Computer:       PC02.example.corp
OpCode:            Info
More Information:  Event Log Online Help
```

Detection: RDP over reverse SSH Tunnel

If the attacker entered the remote IP manually in the command, check also event 5156, and you can see all loopback communications with port 3389.

EventID="3" Image="*\\svchost.exe" SourcePort="3389" (DestinationIp="127.*" OR DestinationIp="::1« - Network connection



Event Properties - Event 5156, Microsoft Windows security auditing.

```
The Windows Filtering Platform has permitted a connection.

Application Information:
        Process ID:                 4
        Application Name:           System

Network Information:
        Direction:                  Inbound
        Source Address:             127.0.0.2
        Source Port:                3389
        Destination Address:        127.0.0.1
        Destination Port:           49274
        Protocol:                   6

Filter Information:
        Filter Run-Time ID:         0
        Layer Name:                 Receive/Accept
        Layer Run-Time ID:          44
```

Command used:

```
plink.exe 10.0.2.17 -P 80 -C -R 127.0.0.1:12345:10.0.2.18:3389 -l test -pw test
```

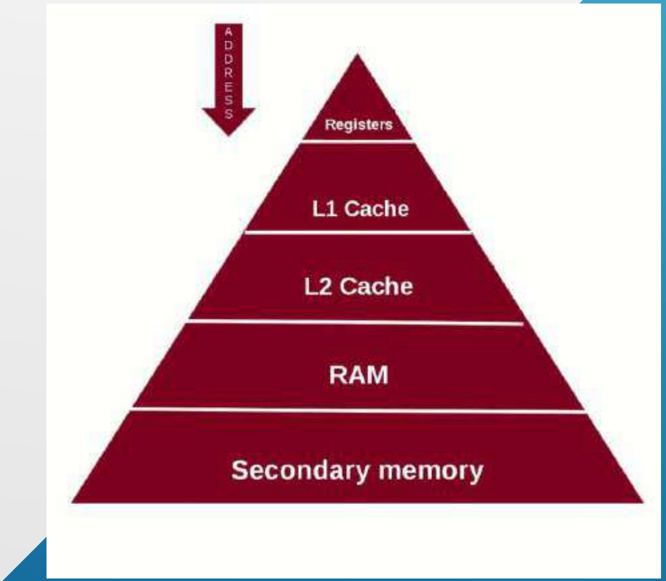
https://blog.menasec.net/2019/02/

LOGON TYPES

11

Logon Type 11 – **CachedInteractive**

Windows supports a feature called Cached Logons which facilitate mobile users.
When you are not connected to your organization’s network and attempt to logon to **your laptop** with a **domain account** there’s no domain controller available to the laptop with which to verify your identity.
To solve this problem, Windows caches a hash of the credentials of the last 10 interactive domain logons. Later when no domain controller is available, Windows uses these hashes to verify your identity when you attempt to logon with a domain account.



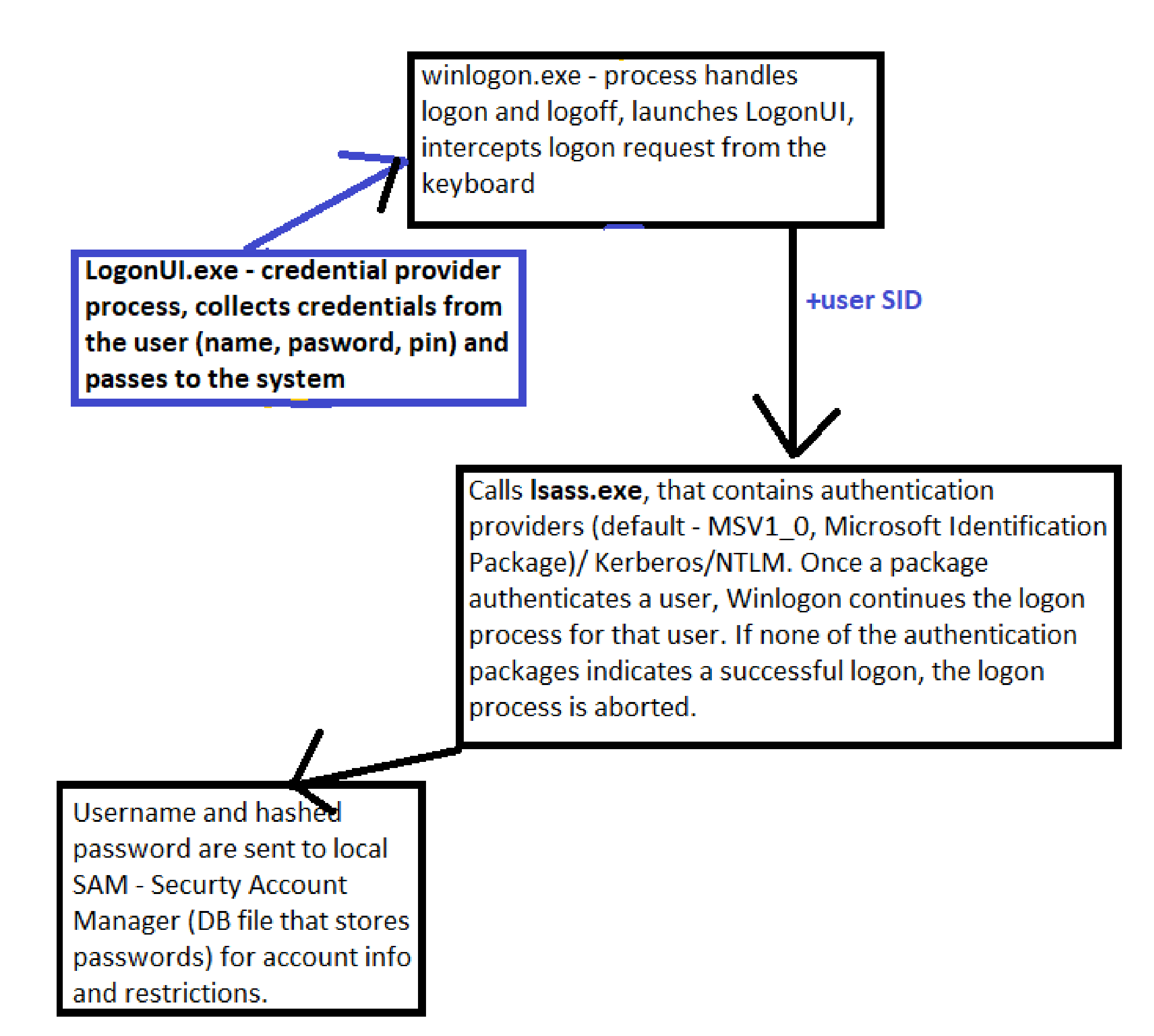
CyberSafe

What is failed login?

- ->Authentication packages are DLLs that perform authentication checks.

- MSV1_0
- KERBEROS
- NTLM

https://attack.mitre.org/techniques/T1547/002/



winlogon.exe - process handles logon and logoff, launches LogonUI, intercepts logon request from the keyboard

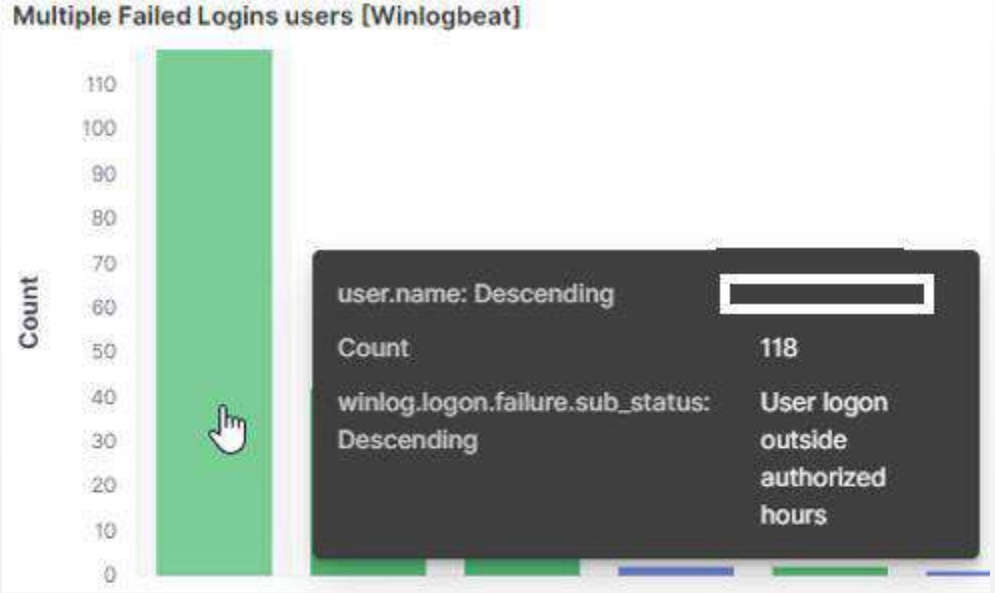
LogonUI.exe - credential provider process, collects credentials from the user (name, pasword, pin) and passes to the system

Calls **lsass.exe**, that contains authentication providers (default - MSV1_0, Microsoft Identification Package)/ Kerberos/NTLM. Once a package authenticates a user, Winlogon continues the logon process for that user. If none of the authentication packages indicates a successful logon, the logon process is aborted.

Username and hashed password are sent to local SAM - Securty Account Manager (DB file that stores passwords) for account info and restrictions.

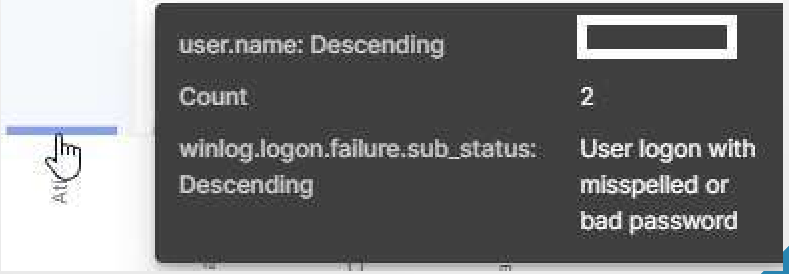
EXAMPLES

Example of SAM restrictions:

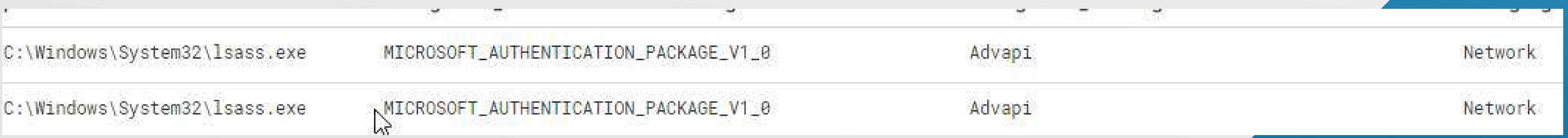


user.name: Descending	[redacted]
Count	118
winlog.logon.failure.sub_status: Descending	User logon outside authorized hours

Lsass Failed login – Bad password



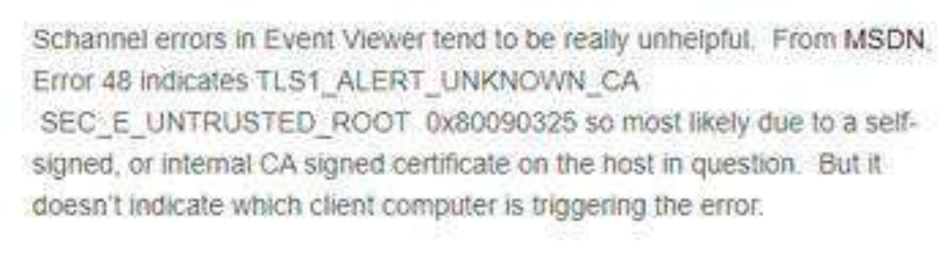
user.name: Descending	[redacted]
Count	2
winlog.logon.failure.sub_status: Descending	User logon with misspelled or bad password



C:\Windows\System32\lsass.exe	MICROSOFT_AUTHENTICATION_PACKAGE_V1_0	Advapi	Network
C:\Windows\System32\lsass.exe	MICROSOFT_AUTHENTICATION_PACKAGE_V1_0	Advapi	Network

EXAMPLE OF SCHANNEL FAILED LOGIN

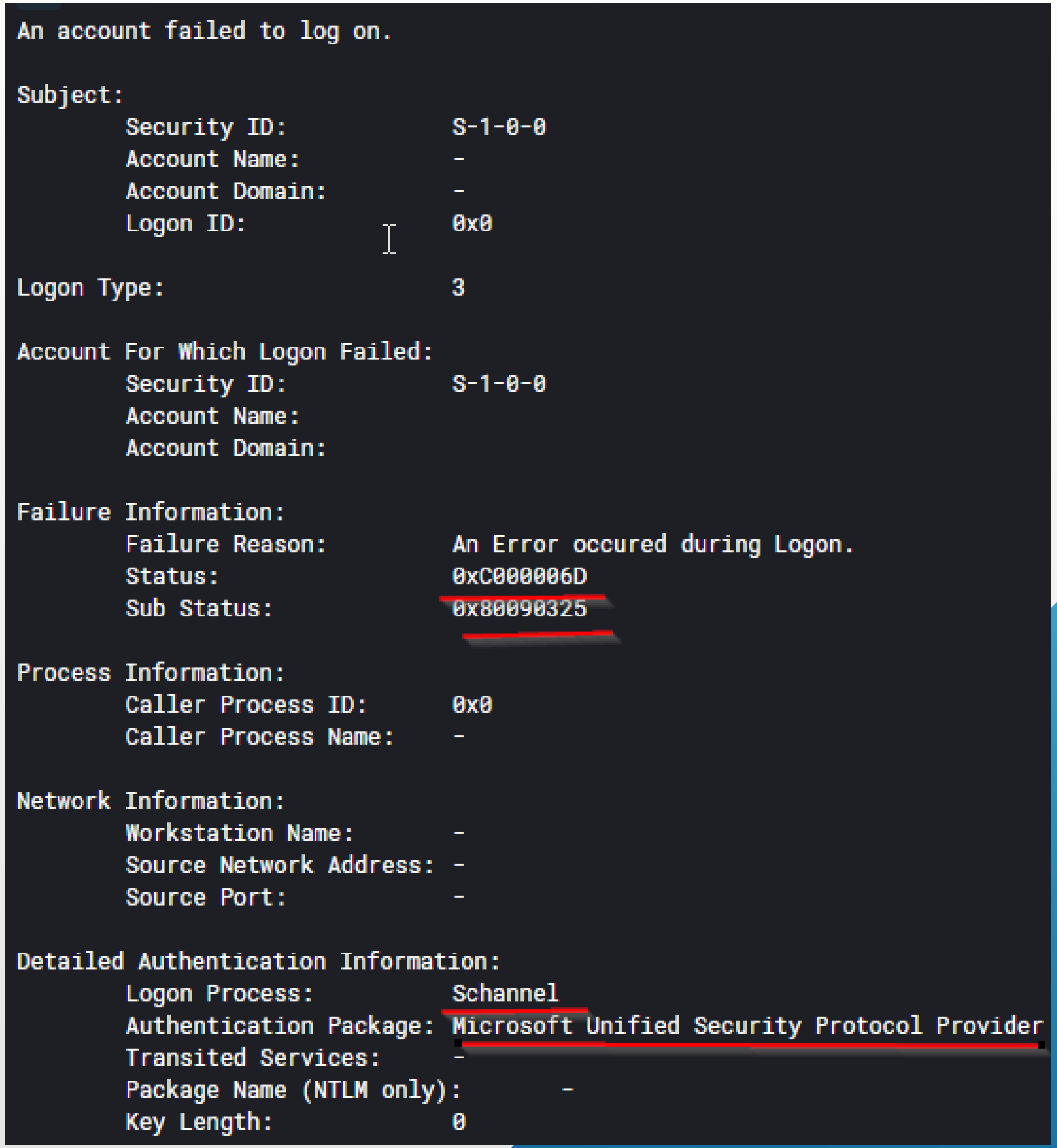
TLS1_ALERT_UNKNOWN_CA	SEC_E_UNTRUSTED_ROOT
48	0x80090325



Schannel errors in Event Viewer tend to be really unhelpful. From MSDN Error 48 indicates TLS1_ALERT_UNKNOWN_CA SEC_E_UNTRUSTED_ROOT 0x80090325 so most likely due to a self-signed, or internal CA signed certificate on the host in question. But it doesn't indicate which client computer is triggering the error.

It is an SSL issue and can be solved by adding internal CA cert to the client machine

https://ril3y.wordpress.com/2014/06/11/clearing-up-event-36887-schannel-the-following-fatal-alert-was-received-48/



```
An account failed to log on.

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

Logon Type:                     3

Account For Which Logon Failed:
        Security ID:            S-1-0-0
        Account Name:
        Account Domain:

Failure Information:
        Failure Reason:         An Error occured during Logon.
        Status:                 0xC000006D
        Sub Status:             0x80090325

Process Information:
        Caller Process ID:      0x0
        Caller Process Name:    -

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

Detailed Authentication Information:
        Logon Process:          Schannel
        Authentication Package: Microsoft Unified Security Protocol Provider
        Transited Services:     -
        Package Name (NTLM only):       -
        Key Length:             0
```

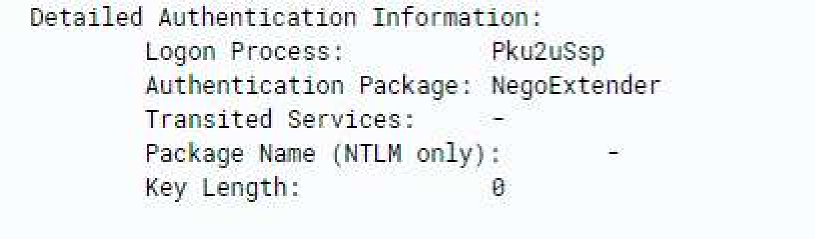
OTHER Aps: NegoExtender

NegoExtender AP - Negotiate Extensions SSP (Negoexts.dll)

PKU2U - Public Key Cryptography User-to-User, peer-2-peer

When computers are configured to accept authentication requests by using online IDs, Negoexts.dll calls the PKU2U SSP on the computer that is used to log on. The PKU2U SSP obtains a **local certificate** and exchanges the policy between the peer computers. When validated on the peer computer, the certificate within the metadata is sent to the logon peer for validation. It associates the user's certificate to a security token, and then the logon process completes.

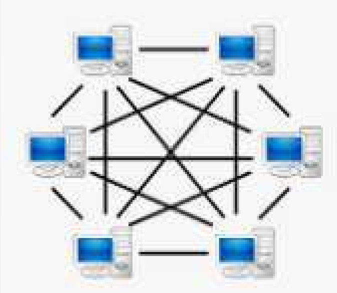
An Elevation of Privilege (EoP) vulnerability exists in PKU2U authentication. An attacker who successfully exploited the vulnerability, could run processes in an elevated context. To exploit the vulnerability, an attacker would first have to log on to the system. (CVE-2021-25195, Critical)



```
Detailed Authentication Information:
        Logon Process:          Pku2uSsp
        Authentication Package: NegoExtender
        Transited Services:     -
        Package Name (NTLM only):       -
        Key Length:             0
```

May be used in Hyper-V for CLI user login

To prevent online identities from authenticating to domain-joined systems:
Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> "Network security: Allow PKU2U authentication requests to this computer to use online identities" to "**Disabled**".



https://www.gov.il/BlobFolder/reports/microsoft_feb2021/he/MICROSOFTFEB21-CERT-IL-W-1277.pdf

OTHER Aps: WDigest

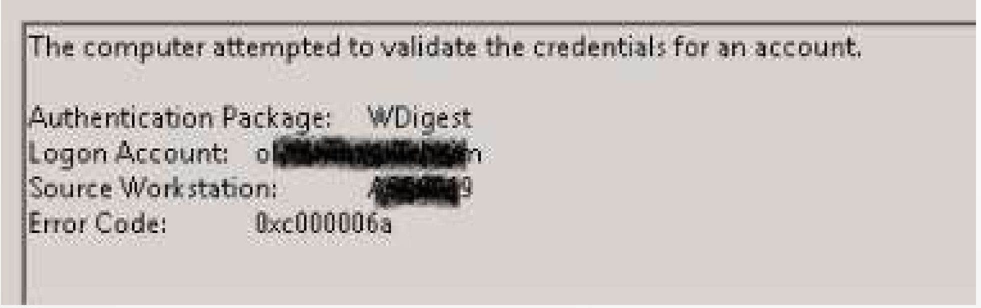
Rare SSP – not found in our clients' logs

WDigest Authentication is a challenge/response protocol that is used for LDAP and web-based authentication.

A client requests access, the authenticating server challenges the client, and the client responds to the challenge by encrypting its response with a key derived from the password. The encrypted response is compared to a stored response on the authenticating server to determine if the user has the correct password.

WDigest stores passwords in **clear-text**, in memory. If a malicious user has access to an endpoint and is able to run a tool like **Mimikatz**, not only would they get the hashes currently stored in memory, but they'd also be able to get the clear-text password for the accounts as well.

Microsoft released a security update that allows users to configure a setting in the registry that would prevent storing clear-text passwords in memory.



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

Authentication Package:    WDigest
Logon Account:   o[redacted]n
Source Workstation:            [redacted]9
Error Code:          0xc000006a
```

event ID **4624**
'Authentication Package**: WDigest**'.

https://adsecurity.org/?p=1760 – mimkatz dll SSP

Happy Hunting…