

 Details



Detecting Local Account Creation (T1136.001) with Atomic Red Team and Splunk

FIGURE 1: LOGICAL DIAGRAM

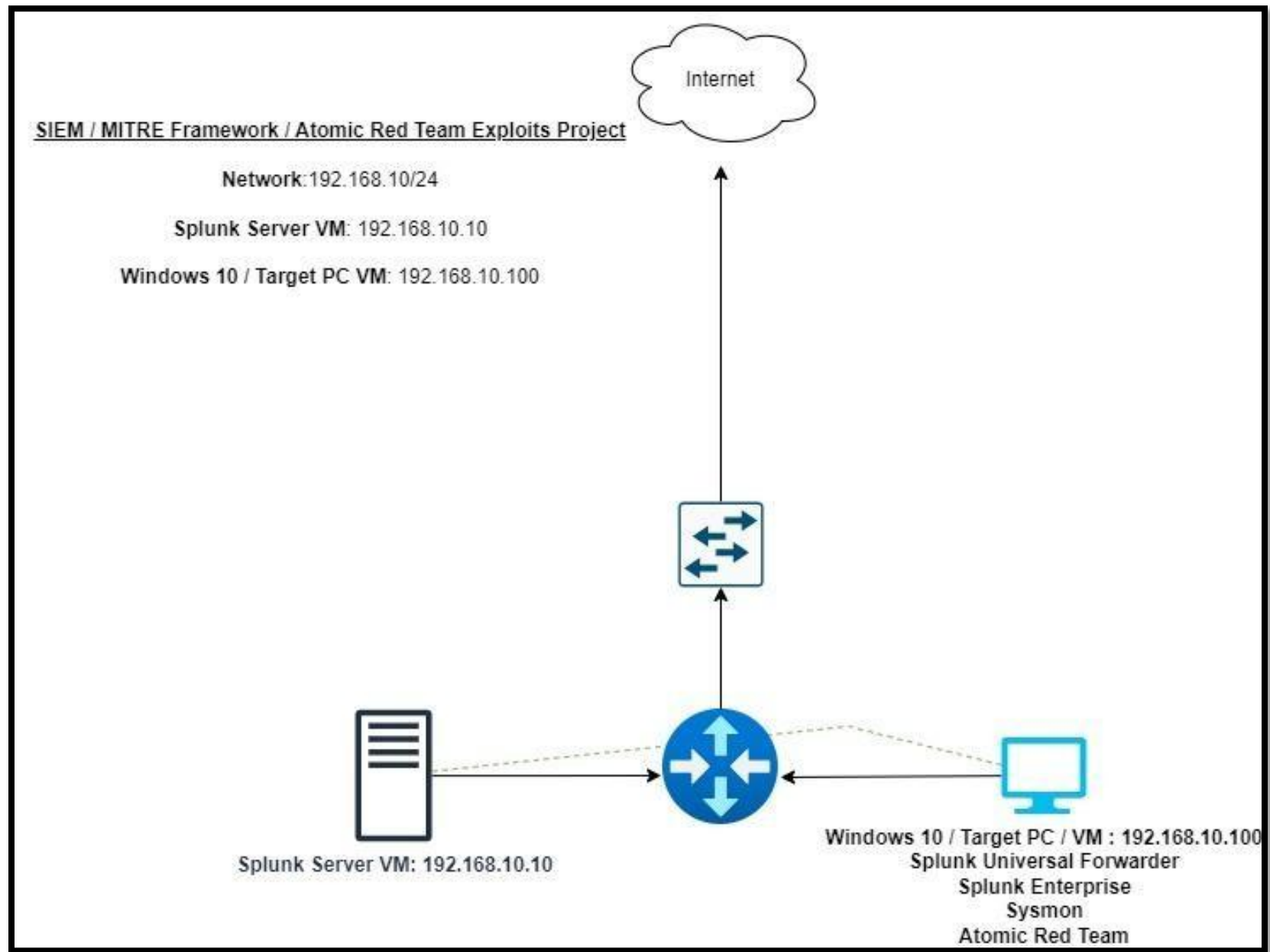


FIGURE 2: SYSTEM CONFIGURATIONS



Windows 10 / Target PC / VM : 192.168.10.100
Splunk Universal Forwarder
Splunk Enterprise
Sysmon
Atomic Red Team

- Installed Atomic Red Team on **TARGET-PC**
- Configured exclusions in Windows Virus & Threat Protection settings to the C: drive to prevent the security software from blocking or interfering with the deployment of simulated MITRE ATT&CK techniques
- Executed **MITRE ATT&CK ID: T1136.001** (Create Account - Local Account)
- Verified the creation of a new account by investigating the output of the **net user** and **net localgroup** Administrator commands.
- Captured telemetry data using **Splunk Enterprise**



Splunk Server VM: 192.168.10.10

- **Ubuntu Server** with Splunk installed and sending telemetry to **TARGET-PC**

FIGURE 3: CONFIGURED EXCLUSIONS IN WINDOWS VIRUS & THREAT PROTECTION SETTINGS



FIGURE 4: ATOMIC RED TEAM INSTALLATION ON TARGET PC

```
Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> powershell -exec bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> Install-Module -Name invoke-atomicredteam,powershell-yaml -Scope CurrentUser

NuGet provider is required to continue
PowerShellGet requires NuGet provider version '2.8.5.201' or newer to interact with NuGet-based repositories. The NuGet
provider must be available in 'C:\Program Files\PackageManagement\ProviderAssemblies' or 'C:\Users\TARGET
PC\AppData\Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet provider by running
'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet to install and import
the NuGet provider now?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): y

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'PSGallery'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"):
WARNING: User declined to install module (Invoke-AtomicRedTeam).
WARNING: User declined to install module (powershell-yaml).
PS C:\Windows\system32> Install-Module -Name invoke-atomicredteam,powershell-yaml -Scope CurrentUser

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'PSGallery'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): Y
PS C:\Windows\system32> Import-Module "C:\AtomicRedTeam\invoke-atomicredteam\Invoke-AtomicRedTeam.psd1" -Force
```


FIGURE 5: MITRE FRAMEWORK T1136.001 TACTIC & TECHNIQUE INFORMATION

MITRE | ATT&CK®
Matrices ▾
Tactics ▾
Techniques ▾
Defenses ▾
CTI ▾
Resources ▾
Benefactors
Blog
Search

ATT&CK®

[Get Started](#)
[Take a Tour](#)

[Contribute](#)
[Blog](#)

[FAQ](#)
[Random Page](#)

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world – by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

ATT&CK Matrix for Enterprise

layout: side ▾
show sub-techniques
hide sub-techniques

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	44 techniques	17 techniques	32 techniques	9 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (7)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (4)	Account Discovery (4)	Exploitation of Remote Services
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (11)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (7)	Build Image on Host	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Movement
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Debugger Evasion	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Services
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Host Software Binary	Direct Volume Access	Deploy Container	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removal Media
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media	Native API	Create Account (3)	Domain Account	Domain or Tenant Policy Modification (2)	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Local Account	Domain or Tenant Policy Modification (2)	Execution Guardrails (2)	Modify Authentication Process (9)	Container and Resource Discovery	
Search Open Websites/Domains (4)			Serverless Execution	Cloud Account	Exploitation for Defense Evasion	Exploitation for Defense Evasion	Device Driver Discovery		

- For this attack the Persistence tactic / Create Account/ Local Account T1136.001 technique is used.

[Home](#) > [Techniques](#) > [Enterprise](#) > [Create Account](#) > Local Account

Create Account: Local Account

Other sub-techniques of Create Account (3)

Adversaries may create a local account to maintain access to victim systems. Local accounts are those configured by an organization for use by users, remote support, services, or for administration on a single system or service.

For example, with a sufficient level of access, the Windows `net user /add` command can be used to create a local account. On macOS systems the `dscl -create` command can be used to create a local account. Local accounts may also be added to network devices, often via common [Network Device CLI](#) commands such as `username`, or to Kubernetes clusters using the `kubectl` utility.^{[1][2]}

Such accounts may be used to establish secondary credentialed access that do not require persistent remote access tools to be deployed on the system.

ID: T1136.001

Sub-technique of: [T1136](#)

① Tactic: [Persistence](#)

① Platforms: Containers, Linux, Network, Windows, macOS

Contributors: Austin Clark,
[@c2defense](#)

Version: 1.3

Created: 28 January 2020

Last Modified: 16 October 2023

[Version](#) [Permalink](#)

FIGURE 6: AVAILABLE EXECUTIONS WITHIN T1136.001 TECHNIQUE DISPLAYED IN POWERSHELL

```
PS C:\Windows\system32> Invoke-AtomicTest T1136.001 -ShowDetailsBrief
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

T1136.001-4 Create a new user in a command prompt 1
T1136.001-5 Create a new user in PowerShell 2
T1136.001-8 Create a new Windows admin user 3
T1136.001-9 Create a new Windows admin user via .NET 4
```

T1136.001 executions

JSO
JonSecOps

FIGURE 7: T1136.001 DEPLOYMENT & EXECUTIONS

```

PS C:\Windows\system32> Invoke-AtomicTest T1136.001
PathToAtomicFolder = C:\AtomicRedTeam\atomics

Executing test: T1136.001-4 Create a new user in a command prompt
The password does not meet the password policy requirements. Check the minimum password length, password complexity and password history requirements.
More help is available by typing NET HELPMSG 2245.
Exit code: 2
Done executing test: T1136.001-4 Create a new user in a command prompt
Executing test: T1136.001-5 Create a new user in PowerShell
Name           Enabled Description
-----
T1136.001_PowerShell True
Exit code: 0
Done executing test: T1136.001-5 Create a new user in PowerShell
Executing test: T1136.001-8 Create a new Windows admin user
The command completed successfully.
The command completed successfully.
Exit code: 0
Done executing test: T1136.001-8 Create a new Windows admin user
Executing test: T1136.001-9 Create a new Windows admin user via .NET
This script creates a new user, adds it to a local administrator group and then deletes the user.
User 'NewLocalUser' created successfully.
User 'NewLocalUser' added to the 'Administrators' group.
Newly Created User Info:
User name           NewLocalUser
Full Name           NewLocalUser
Comment
User's comment
Country/region code 000 (System Default)
Account active      Yes
Account expires     Never
Password last set   12/16/2024 3:42:52 PM
Password expires     Never
Password changeable 12/17/2024 3:42:52 PM
Password required    Yes
User may change password No
Workstations allowed All
Logon script
User profile
Home directory
Last logon          Never
Logon hours allowed All
Local Group Memberships
Global Group memberships *None
The command completed successfully.
User 'NewLocalUser' deleted successfully.
Exception calling "Add" with "3" argument(s): "The network path was not found.

```

Activate Windows
Go to Settings to activate Windows.

FIGURE 8: TARGET PC NET USER & NET LOCALGROUP INFORMATION

```
C:\Users\TARGET PC>net user
User accounts for \\TARGET5PC

-----
Administrator          DefaultAccount          Guest
T1136.001_Admin         T1136.001_PowerShell    TARGET PC
WDAGUtilityAccount
The command completed successfully.

C:\Users\TARGET PC>net user T1136.001 Admin
User name                T1136.001_Admin
Full Name
Comment
User's comment
Country/region code      000 (System Default)
Account active           Yes
Account expires          Never

Password last set        12/16/2024 3:42:54 PM
Password expires         1/27/2025 3:42:54 PM
Password changeable      12/17/2024 3:42:54 PM
Password required        Yes
User may change password Yes

Workstations allowed     All
Logon script
User profile
Home directory
Last logon               Never

Logon hours allowed      All

Local Group Memberships  *Administrators          *Users
Global Group memberships *None
The command completed successfully.
```

```
C:\Users\TARGET PC>net localgroup Administrators
Alias name     Administrators
Comment       Administrators have complete and unrestricted access to the computer/domain

Members

-----
Administrator
LAB\Domain Admins
1136.001_Admin
TARGET PC
The command completed successfully.
```



FIGURE 9: ATTACK ORDER

Attack Order

1. **Event ID 4798 - A user's local group membership was enumerated**
 - **Reconnaissance:** Attackers query group memberships to identify accounts with elevated privileges.
2. **Event ID 4724 - An attempt was made to reset an account's password**
 - **Initial Compromise or Privilege Escalation:** Attackers try to reset passwords to gain access to or control over accounts.
3. **Event ID 4738 - A user account was changed**
 - **Privilege Escalation or Persistence:** Attackers modify accounts, e.g., changing attributes or passwords to maintain control.
4. **Event ID 4722 - A user account was enabled**
 - **Persistence:** Attackers re-enable disabled accounts to exploit dormant or forgotten credentials.
5. **Event ID 4720 - A user account was created**
 - **Persistence:** Attackers create new accounts to maintain access without relying on existing credentials.
6. **Event ID 4726 - A user account was deleted**
 - **Cleanup:** Attackers may delete accounts to hide traces of their activity or disrupt operations.

FIGURE : SPLUNK TELEMETRY IN ATTACK ORDER

i	Time	Event
	8:42:53.000 PM	<p>LogName=Security EventCode=4798 EventType=0 ComputerName=TARGET5PC.LAB.local SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=4395 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user's local group membership was enumerated.</p> <p>Subject:</p> <p>Security ID: S-1-5-21-4034659041-4078518514-33229716-1001 Account Name: TARGET PC Account Domain: TARGET5PC Logon ID: 0x7ABCB2</p> <p>User:</p> <p>Security ID: S-1-5-21-4034659041-4078518514-33229716-1009 Account Name: NewLocalUser Account Domain: TARGET5PC</p> <p>Process Information:</p> <p>Process ID: 0xcd0 Process Name: C:\Windows\System32\net1.exe</p> <p>Collapse</p> <p>EventCode = 4798 host = TARGET5PC source = WinEventLog:Security sourcetype = WinEventLog:Security</p>

i	Time	Event
>	12/16/24 8:42:52.000 PM	12/16/2024 03:42:52 PM LogName=Security EventCode=4724 EventType=0 ComputerName=TARGET5PC.LAB.local SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=4389 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=An attempt was made to reset an account's password. Subject: Security ID: S-1-5-21-4034659041-4078518514-33229716-1001 Account Name: TARGET PC Account Domain: TARGET5PC Logon ID: 0x7ABCB2 Target Account: Security ID: S-1-5-21-4034659041-4078518514-33229716-1009 Account Name: NewLocalUser Account Domain: TARGET5PC Collapse EventCode = 4724 host = TARGET5PC source = WinEventLog:Security source type = WinEventLog:Security

Activate Windows

Go to Settings to activate Windows.

> 12/16/24 12/16/2024 03:42:52 PM
8:42:52.000 PM LogName=Security
EventCode=4738
EventType=0
ComputerName=TARGET5PC.LAB.local
SourceName=Microsoft Windows security auditing.
Type=Information
RecordNumber=4391
Keywords=Audit Success
TaskCategory=User Account Management
OpCode=Info
Message=A user account was changed.

Subject:

Security ID:	S-1-5-21-4034659041-4078518514-33229716-1001
Account Name:	TARGET PC
Account Domain:	TARGET5PC
Logon ID:	0x7ABCB2

Target Account:

Security ID:	S-1-5-21-4034659041-4078518514-33229716-1009
Account Name:	NewLocalUser
Account Domain:	TARGET5PC

Changed Attributes:

SAM Account Name:	NewLocalUser
Display Name:	NewLocalUser
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:	12/16/2024 3:42:52 PM
Account Expires:	<never>
Primary Group ID:	513

i	Time	Event
>	12/16/24 8:42:52.000 PM	<div>12/16/2024 03:42:52 PM LogName=Security EventCode=4722 EventType=0 ComputerName=TARGET5PC.LAB.local SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=4387 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user account was enabled. Subject: Security ID: S-1-5-21-4034659041-4078518514-33229716-1001 Account Name: TARGET PC Account Domain: TARGET5PC Logon ID: 0x7ABCB2 Target Account: Security ID: S-1-5-21-4034659041-4078518514-33229716-1009 Account Name: NewLocalUser Account Domain: TARGET5PC Collapse EventCode = 4722 host = TARGET5PC source = WinEventLog:Security sourcetype = WinEventLog:Security</div>

> 12/16/24 12/16/2024 03:42:52 PM
8:42:52.000 PM LogName=Security
EventCode=4720
EventType=0
ComputerName=TARGET5PC.LAB.local
SourceName=Microsoft Windows security auditing.
Type=Information
RecordNumber=4386
Keywords=Audit Success
TaskCategory=User Account Management
OpCode=Info
Message=A user account was created.

Subject:

Security ID:	S-1-5-21-4034659041-4078518514-33229716-1001
Account Name:	TARGET_PC
Account Domain:	TARGET5PC
Logon ID:	0x7ABC2

New Account:

Security ID:	S-1-5-21-4034659041-4078518514-33229716-1009
Account Name:	NewLocalUser
Account Domain:	TARGET5PC

Attributes:

SAM Account Name:	NewLocalUser
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

Activate Windows
Go to Settings

> 12/16/24 12/16/2024 03:42:53 PM
8:42:53.000 PM LogName=Security
EventCode=4726
EventType=0
ComputerName=TARGET5PC.LAB.local
SourceName=Microsoft Windows security auditing.
Type=Information
RecordNumber=4397
Keywords=Audit Success
TaskCategory=User Account Management
OpCode=Info
Message=A user account was deleted.

Subject:

Security ID:	S-1-5-21-4034659041-4078518514-33229716-1001
Account Name:	TARGET PC
Account Domain:	TARGET5PC
Logon ID:	0x7ABCB2

Target Account:

Security ID:	S-1-5-21-4034659041-4078518514-33229716-1009
Account Name:	NewLocalUser
Account Domain:	TARGET5PC

Additional Information:

Privileges -

Collapse

EventCode = 4726 | host = TARGET5PC | source = WinEventLog:Security | sourcetype = WinEventLog:Security

Activate Windows
Go to Settings to activate Windows