Windows Logons

1️⃣ Winlog Source & Channel

🔹 winlog.channel

```
external_table('Winlog')
| where WinlogChannel =="Security"
| take 10
```

📌 Logon events အများစုက Security channel ထဲမှာရှိတယ်

```
external_table('Winlog')
| where WinlogChannel =="Security"
| summarize count() by EventAction
| sort by count_
| render barchart
```

👉 Security channel ထဲမှာရှိတဲ့ action နဲ့အရေအတွက်ကြည့်ချင်တဲ့အခါ သုံးတယ်။

2️⃣ Important Logon Event Codes

EventCode	Action	Short Explanation
4624	Logon	Login **အောင်မြင်**
4625	Logon	Login **မအောင်မြင်**
4776	Credential Validation	Username / password စစ်ဆေး

🧠 Forensics Tip

- 4625 များ → brute force / password spraying
- 4624 + odd logon type → suspicious access

3️⃣ Logon Types (အရမ်းအရေးကြီး)

Type	Title	Meaning (Short)
0	System	System startup
2	Interactive	Local user login

Type	Title	Meaning (Short)
3	Network	Network login (SMB, share)
4	Batch	Scheduled / batch job
5	Service	Service account
7	Unlock	Screen unlock
8	NetworkCleartext	Cleartext credential usage
9	NewCredentials	RunAs / token cloning
10	RemoteInteractive	RDP / Terminal
11	CachedInteractive	Cached domain login
12	CachedRemoteInteractive	Cached RDP
13	CachedUnlock	Cached unlock

📌 **Detection Hint**

- LogonType **10** → RDP
- LogonType **3** → Lateral movement
- LogonType **8** → 🔥 High risk

4️⃣ Incident Response – Scoping

🔹 Scoping ဆိုတာဘာလဲ?

- Incident response ရဲ့
  👉 **Detection & Analysis phase** မှာလုပ်
- Compromised ဖြစ်နိုင်တဲ့
  - Systems
  - Accounts
  - Credentials
  - Vulnerabilities ကို

  တကယ့်ဖြစ်ရပ်များဟုတ်မဟုတ် အတည်ပြုရန်နှင့် ၎င်းတို့၏ အတိုင်းအတာနှင့် သက်ရောက်မှုကို နားလည်ရန် စုံစမ်းစစ်ဆေးသည်။

📌 **Fully scoped intrusion**
= Containment မလုပ်ခင်
အန္တရာယ်ရှိတာအားလုံး သိပြီးသား

> အဓိကအချက်က “ဒီ login က ဘယ် account အမျိုးအစားလဲ၊ ဘယ်နေရာမှာ authenticate လုပ်လဲ၊ အောင်မြင်ရင် ဘယ် system မှာ log ပေါ်လဲ” ဆိုတာကို ဆက်စပ်စဉ်းစားနိုင်ရပါမယ်။

5️⃣ Local Logons (SAM Based)

🔹 Local Account Authentication Flow

Windows machine တစ်လုံးချင်းစီမှာ **Security Account Manager (SAM)** ဆိုတဲ့ local database တစ်ခု ရှိပါတယ်။
ဒီ SAM ထဲမှာ local user accounts တွေ (ဥပမာ Administrator) ရဲ့ *credential information* ကို သိမ်းထားပါတယ်။
User တစ်ယောက်က local account နဲ့ login ဝင်တဲ့အခါ Windows ရဲ့ **Local Security Authority (LSA)** က domain controller ကို မမေးပါဘူး။ ကိုယ့်စက်ထဲက SAM နဲ့ပဲ username/password ကို စစ်ပါတယ်။
Credential မှန်ရင် login အောင်မြင်ပြီး user ကို local resources တွေကို access ပေးပါတယ်။
ဒါကြောင့် local logon ဆိုတာက "ဒီစက်တစ်လုံးထဲမှာပဲ ဖြစ်ပေါ်တဲ့ authentication လို့ နားလည်ရပါမယ်။

🔹 Built-in Accounts

- `Administrator` က local admin privilege အပြည့်ရှိပြီး၊
- `NT AUTHORITY\SYSTEM` ကတော့ local system အတွင်းမှာ အမြင့်ဆုံး privilege ရှိတဲ့ account ဖြစ်ပါတယ်။

📌 Local admin compromise
= Full control of machine

> SYSTEM account က user မဟုတ်ဘဲ OS နဲ့ services တွေအတွက် သုံးတဲ့ account ဖြစ်ပါတယ်။ အဲ့ဒီကြောင့် attacker တစ်ယောက်က local Administrator သို့မဟုတ် SYSTEM privilege ရခဲ့ပြီဆိုရင်၊ ဒီစက်တစ်လုံးကို အပြည့်အဝ ထိန်းချုပ်နိုင်ပြီ လို့ သတ်မှတ်လို့ရပါတယ်။ File system, registry, memory အားလုံးကို access လုပ်နိုင်ပြီး credential တွေကို dump လုပ်နိုင်တဲ့ အခြေအနေပါ။

6️⃣ Domain Logons (Active Directory)

🔹 Domain Authentication

Domain environment မှာ user account တွေက local SAM ထဲမှာ မရှိဘဲ **Active Directory (AD)** ထဲမှာ ရှိပါတယ်။ User တစ်ယောက်က domain account နဲ့ login ဝင်တဲ့အခါ LSA က local SAM ကို မကြည့်ဘဲ Domain Controller (DC) ကို ဆက်သွယ်ပြီး authentication လုပ်ပါတယ်။ DC က credential မှန်ကြောင်း အတည်ပြုပေးရင် login အောင်မြင်ပြီး logon event (4624) က user ဝင်ထားတဲ့ target computer ပေါ်မှာပဲ ပေါ်လာပါတယ်။ ဒါကြောင့် domain logon ဆိုတာက **"credential စစ်တာက DC မှာ၊ event ပေါ်တာက endpoint မှာ"** ဆိုတဲ့ အချက်ကို သေချာမှတ်ထားရပါမယ်။

✔️ Auth success →
Logon event **target computer** မှာပေါ်

7️⃣ Domain Logon Detection (KQL)

```
external_table('Winlog')
| where EventCode == 4624 and TargetDomainName == "SOLIDLABS"
| project Timestamp, HostName, EventCode, LogonType, TargetUserName,
TargetDomainName
```

🧠 Use Case

ဒီအချက်ကြောင့် SOC / DFIR အလုပ်လုပ်တဲ့အခါ domain user တွေရဲ့ activity ကို trace လုပ်ဖို့ Winlog ထဲက 4624 event တွေကို TargetDomainName နဲ့ filter လုပ်ပါတယ်။ ဥပမာ domain name က **SOLIDLABS** ဆိုရင် အဲ့ဒီ domain user တွေက ဘယ် `machine` တွေကို ဘယ်အချိန်မှာ `login` ဝင်ထား လဲ ဆိုတာကို အလွယ်တကူ မြင်နိုင်ပါတယ်။ ဒီလို analysis က lateral movement hunting မှာ အလွန် အသုံးဝင်ပါတယ်၊ attacker က domain credential တစ်ခုကိုယူပြီး machine တစ်လုံးမှ တစ်လုံးကို ရွှေ့ သွားတဲ့အခါ ဒီ logon footprint တွေ ချန်ထားလို့ပါ။

8️⃣ Domain Account Types

🔹 1. User Accounts

Domain ထဲမှာ account အမျိုးအစား နှစ်မျိုးရှိတာကိုလည်း နားလည်ထားရပါမယ်။

ပထမတစ်မျိုးက **user accounts** ဖြစ်ပြီး လူတွေသုံးတဲ့ `admin / standard users` တွေပါ။

ဒုတိယတစ်မျိုးက **computer accounts** ဖြစ်ပါတယ်။ Computer account တွေကို `<hostname>$` ဆို တဲ့ပုံစံနဲ့ AD ထဲမှာ သိမ်းထားပါတယ် (ဥပမာ WIN10-A51S9A8$)။ ဒီ account က *"ဒီ machine ကို AD မှာ ကိုယ်စားပြုတဲ့ identity"* ဖြစ်ပါတယ်။ Machine တစ်လုံးက domain resource ကို access လုပ်တဲ့ အခါ user account မဟုတ်ဘဲ သူ့ရဲ့ computer account ကို သုံးတာများပါတယ်။

🔹 2. Computer Accounts

- Format: `<hostname>$`
- Example: `WIN10-A51S9A8$`

📌 Computer account = machine identity in AD

9️⃣ SYSTEM Account = High Impact

🔹 NT AUTHORITY\SYSTEM

ဒီနေရာမှာ SYSTEM account ရဲ့ အန္တရာယ်ကို ဆက်စပ်စဉ်းစားရပါမယ်။ Local machine ပေါ်မှာ SYSTEM account က domain resource ကို access လုပ်တဲ့အခါ သူ့ရဲ့ `computer account (<hostname>$)` ကို အသုံးပြုပါတယ်။

ဒါကြောင့် attacker တစ်ယောက်က **SYSTEM privilege** ရခဲ့ပြီဆိုရင်၊ local machine ကို ထိန်းချုပ်နိုင်တာတင်မကဘဲ domain ထဲမှာလည်း ဒီ machine အဖြစ် acting လုပ်နိုင်ပါပြီ။ ဒီဟာက computer domain account compromise ဖြစ်ပြီး domain escalation လမ်းကြောင်းတစ်ခု ဖြစ်လာပါတယ်။

🔟 Attacker with SYSTEM / Admin Privileges

🔥 Potential Impact

- file system အားလုံးကို ဖတ်နိုင်၊
- registry နဲ့ memory ကို access လုပ်နိုင်၊
- cached user credentials တွေကို ထုတ်ယူနိုင်၊
- SAM database ထဲက password hashes တွေကို dump လုပ်နိုင်ပြီး
- domain computer account အဖြစ် အသုံးပြုနိုင်ပါတယ်။

> ဒါကြောင့် ဒီအဆင့်ရောက်သွားပြီဆိုရင် incident က workstation level မဟုတ်တော့ဘဲ domain level risk ဖြစ်သွားပါပြီ။

📌 **This = Domain escalation path**

1️⃣1️⃣ Defensive / IR Note (Very Important)

Incident ဖြစ်တဲ့ system ကို investigator က direct login ဝင်သွားမယ်ဆိုရင် ကိုယ့် account credential ကို memory/cache ထဲမှာ ထားသွားနိုင်ပြီး attacker အတွက် **နောက်ထပ် credential အသစ်တစ်ခု** ဖန်တီးပေးသလို ဖြစ်သွားနိုင်ပါတယ်။

✔️ Best Practice:

- ဒါကြောင့် IR မှာ minimal interaction, log-based investigation, safe procedures တွေကို အသုံးပြုရတာ အရေးကြီးပါတယ်။

> အကျဉ်းချုပ်ရရင် local logon နဲ့ domain logon တို့ရဲ့ခြားနားမှုကို နားလည်နိုင်ရင် attacker ရဲ့ privilege level၊ lateral movement အန္တရာယ်နဲ့ domain impact ကို log တွေကနေ မှန်မှန်ကန်ကန် ခန့်မှန်းနိုင်လာပါလိမ့်မယ်။

🧠 Quick Memory Map

- **4624** → Success
- **4625** → Fail
- **LogonType 10** → RDP
- **LogonType 3** → Network / lateral

- **SYSTEM compromise** → Domain risk
