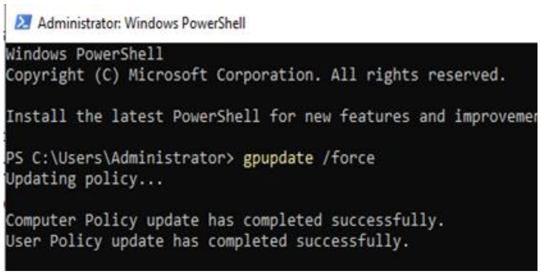
ACTIVE DIRECTORY RECON DETECTION VIA HONEY USER ACCOUNT (T1087)

🗄️ SECTION 1: LAB OVERVIEW

Field	**Value**
MITRE Technique	T1087 – Account Discovery
Environment	Kali Linux (192.168.40.140), Windows Server 2022 (Domain Controller), AD Domain: lab.local
Objective	Detect unauthorized AD enumeration by baiting attacker with a honey account
Author	Brayden Thompson
Date	June 30, 2025

🛠️ SECTION 2: SETUP SUMMARY

- Created svc_backup1 in new OU IT_Secrets
- User had no permissions and never logged in
- Enabled audit policies (4625, 4662, 4624, 4648, 4776)



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improveme

PS C:\Users\Administrator> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.
```

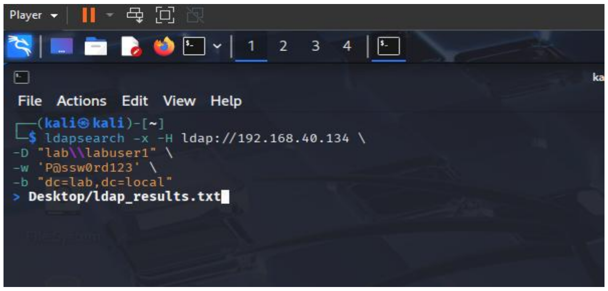
Figure 1: Forced Group policy Update

- Monitored logon failures and directory access to the honey user

🧪 SECTION 3: SIMULATED ATTACK

- Used authenticated bind with ldapsearch:

```
ldapsearch -x -H ldap://192.168.40.134 -D "lab\\labuser1" -w "Passw0rd123" -
b "dc=lab,dc=local"
```



```
┌──(kali㉿kali)-[~]
└─$ ldapsearch -x -H ldap://192.168.40.134 \
-D "lab\\labuser1" \
-w 'P@ssw0rd123' \
-b "dc=lab,dc=local"
> Desktop/ldap_results.txt
```

Figure 2: Kali Command for searching LDAP indexes

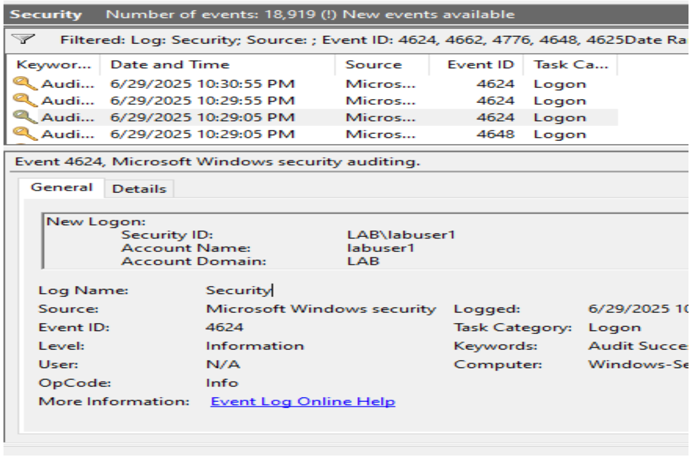
- Output redirected to Desktop/ldap_results.txt
- Triggered failed login to svc_backup1 from attacker IP

🔍 SECTION 4: DETECTION

- Event ID 4625 from attacker IP on honey user
- PowerShell used to extract logs:

```
Get-WinEvent -LogName Security | ? { $_.Message -like "*svc_backup1*" }
```

- Also went into Event Viewer > Windows Logs > Security and filtered the events to the last hour and set the event IDs to match what we were searching for.
- Captured Successful login onto labuser1 from the kali machine.



Security   Number of events: 18,919 (!) New events available

Filtered: Log: Security; Source: ; Event ID: 4624, 4662, 4776, 4648, 4625Date Ra

Keywor...	Date and Time	Source	Event ID	Task Ca...
Audi...	6/29/2025 10:30:55 PM	Micros...	4624	Logon
Audi...	6/29/2025 10:29:55 PM	Micros...	4624	Logon
Audi...	6/29/2025 10:29:05 PM	Micros...	4624	Logon
Audi...	6/29/2025 10:29:05 PM	Micros...	4648	Logon

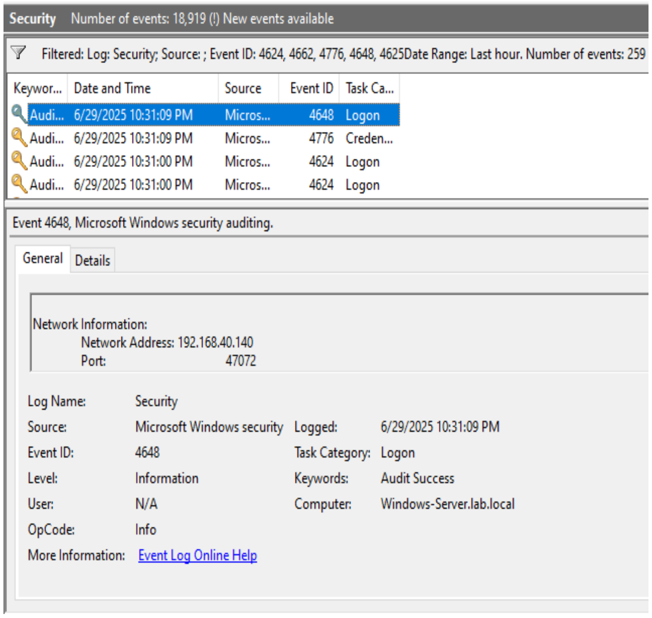
Event 4624, Microsoft Windows security auditing.

```
New Logon:
        Security ID:          LAB\labuser1
        Account Name:         labuser1
        Account Domain:       LAB
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	6/29/2025 1(
Event ID:	4624	Task Category:	Logon
Level:	Information	Keywords:	Audit Succe
User:	N/A	Computer:	Windows-Se
OpCode:	Info		
More Information:	Event Log Online Help		

Figure 3: labuser1 logon Detected

- Captured explicit credential use – Event ID 4648



Security Number of events: 18,919 (!) New events available

Filtered: Log: Security; Source: ; Event ID: 4624, 4662, 4776, 4648, 4625Date Range: Last hour. Number of events: 259

Keywor...	Date and Time	Source	Event ID	Task Ca...
Audi...	6/29/2025 10:31:09 PM	Micros...	4648	Logon
Audi...	6/29/2025 10:31:09 PM	Micros...	4776	Creden...
Audi...	6/29/2025 10:31:00 PM	Micros...	4624	Logon
Audi...	6/29/2025 10:31:00 PM	Micros...	4624	Logon

Event 4648, Microsoft Windows security auditing.

```
Network Information:
        Network Address: 192.168.40.140
        Port:            47072
```

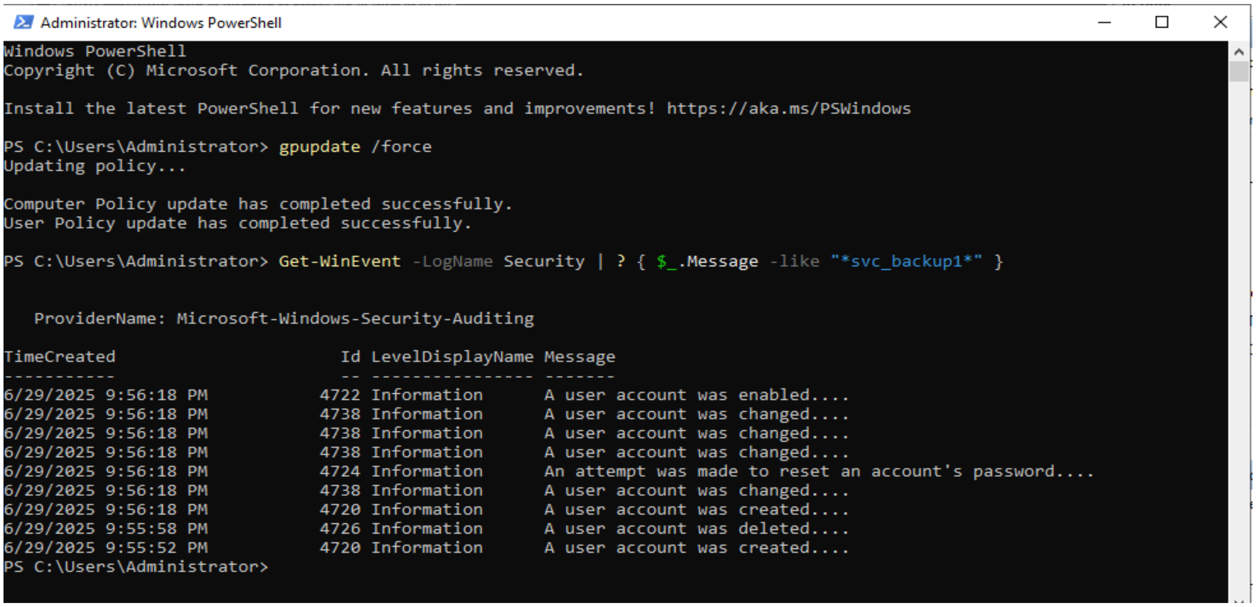
Log Name:	Security		
Source:	Microsoft Windows security	Logged:	6/29/2025 10:31:09 PM
Event ID:	4648	Task Category:	Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	Windows-Server.lab.local
OpCode:	Info		
More Information:	Event Log Online Help		

Figure 4: Explicit credential use caught on audit

- Captured NTLM credential validation – Event ID 4776

🧠 SECTION 5: OUTCOME + RECOMMENDATION

- **Detected** unauthorized AD recon
- Alert triggered on honey user probe



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

PS C:\Users\Administrator> Get-WinEvent -LogName Security | ? { $_.Message -like "*svc_backup1*" }


   ProviderName: Microsoft-Windows-Security-Auditing

TimeCreated                     Id LevelDisplayName Message
-----------                     -- ---------------- -------
6/29/2025 9:56:18 PM          4722 Information      A user account was enabled....
6/29/2025 9:56:18 PM          4738 Information      A user account was changed....
6/29/2025 9:56:18 PM          4738 Information      A user account was changed....
6/29/2025 9:56:18 PM          4738 Information      A user account was changed....
6/29/2025 9:56:18 PM          4724 Information      An attempt was made to reset an account's password....
6/29/2025 9:56:18 PM          4738 Information      A user account was changed....
6/29/2025 9:56:18 PM          4720 Information      A user account was created....
6/29/2025 9:55:58 PM          4726 Information      A user account was deleted....
6/29/2025 9:55:52 PM          4720 Information      A user account was created....
PS C:\Users\Administrator>
```

Figure 5: Manually Pulled Logs Via CLI

- Recommend deeper forensic pull of source IP + 30min log window
- Validate logon source (192.168.49.140) against asset inventory.
- Monitor for repeated queries against unused or hidden accounts.
- Recommend alerting on failed or successful bind attempts to honey accounts.