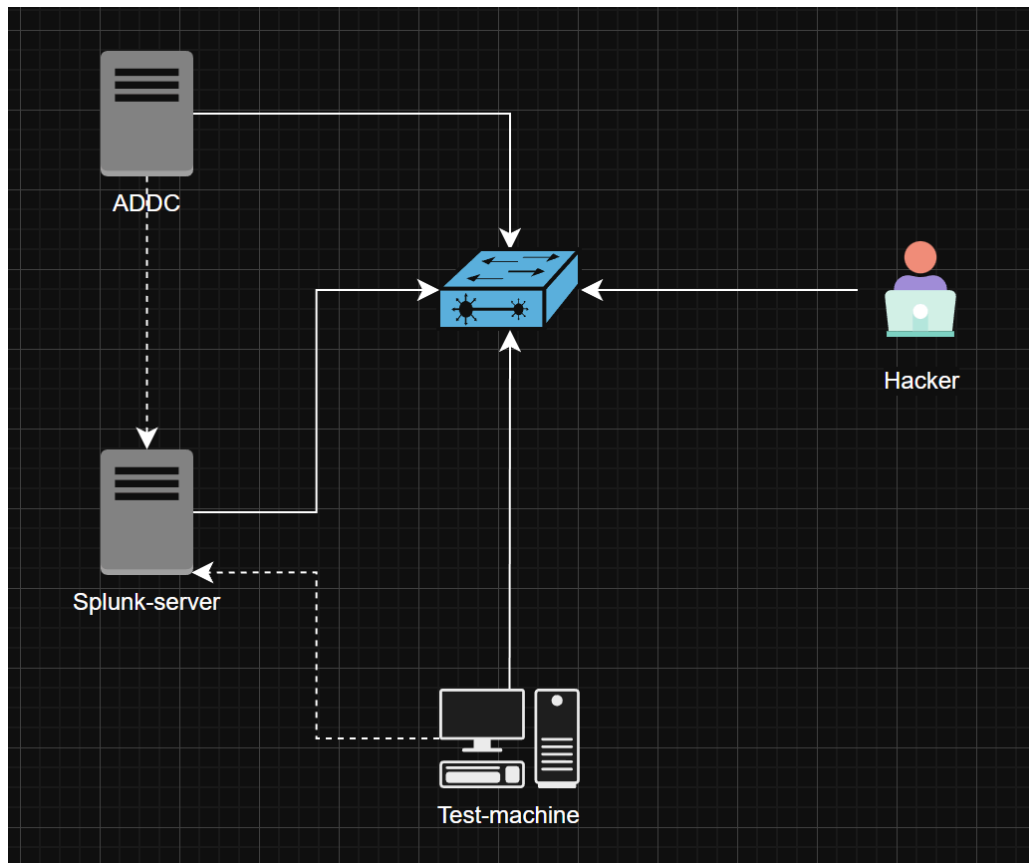


# Active Directory 001

## 1. Mô hình



## 2, Tiến hành triển khai

### 1. Cài đặt AD và thêm user

Computer name	ADDC01
Domain	ducbahpb.local
Windows Defender Firewall	Domain: Off
Remote management	Enabled
Remote Desktop	Disabled
NIC Teaming	Disabled
Ethernet0	192.168.8.7, IPv6 enabled

```

PS C:\Users\Administrator> Get-ADDomain

AllowedDNSSuffixes      : {}
ChildDomains             : {}
ComputersContainer       : CN=Computers,DC=ducbahpb,DC=local
DeletedObjectsContainer  : CN=Deleted Objects,DC=ducbahpb,DC=local
DistinguishedName        : DC=ducbahpb,DC=local
DNSRoot                  : ducbahpb.local
DomainControllersContainer : OU=Domain Controllers,DC=ducbahpb,DC=local
DomainMode               : Windows2016Domain
DomainSID                : S-1-5-21-4132880267-2153279017-2716968246
ForeignSecurityPrincipalsContainer : CN=ForeignSecurityPrincipals,DC=ducbahpb,DC=local
Forest                   : ducbahpb.local
InfrastructureMaster      : ADDC01.ducbahpb.local
LastLogonReplicationInterval : 
LinkedGroupPolicyObjects : {CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Polici
ies,CN=System,DC=ducbahpb,DC=local}
LostAndFoundContainer    : CN=LostAndFound,DC=ducbahpb,DC=local
ManagedBy               : 
Name                     : ducbahpb
NetBIOSName              : DUCBAHPB
ObjectClass               : domainDNS
ObjectGUID               : ef2cbadb-43b6-4d44-8a62-0540f6565c82
ParentDomain             : 
PDCEmulator              : ADDC01.ducbahpb.local
PublicKeyRequiredPasswordRolling : True
QuotasContainer          : CN=NTDS Quotas,DC=ducbahpb,DC=local
ReadOnlyReplicaDirectoryServers : {}
ReplicaDirectoryServers  : {ADDC01.ducbahpb.local}
RIDMaster                 : ADDC01.ducbahpb.local
SubordinateReferences    : {DC=ForestDnsZones,DC=ducbahpb,DC=local,
DC=DomainDnsZones,DC=ducbahpb,DC=local,
CN=Configuration,DC=ducbahpb,DC=local}
SystemsContainer         : CN=System,DC=ducbahpb,DC=local
UsersContainer           : CN=Users,DC=ducbahpb,DC=local

```

## 2. Join test-machine vào domain

## System

Processor: AMD Ryzen 7 H 255 w/ Radeon 780M Graphics 3.79 GHz (2 processors)  
Installed memory (RAM): 2.00 GB  
System type: 64-bit Operating System, x64-based processor  
Pen and Touch: No Pen or Touch Input is available for this Display











## Computer name, domain, and workgroup settings

Computer name: test-machine  
Full computer name: test-machine.ducbahpb.local  
Computer description:  
Domain: ducbahpb.local

### 3. Cài Sysmon và Splunk universal forwarder trên ADDC và test-machine test-machine:

	Special Administration Cons...	Allows admi...		Manual	Local System
	<u>SplunkForwarder</u>	SplunkForw...	Running	Automatic	Local System
	Spot Verifier	Verifies pote...		Manual (Trigg...	Local System
	SSDP Discovery	Discovers ne...		Disabled	Local Service
	State Repository Service	Provides req...	Running	Manual	Local System
	Still Image Acquisition Events	Launches ap...		Manual	Local System
	Storage Service	Provides ena...	Running	Manual (Trigg...	Local System
	Storage Tiers Management	Optimizes th...		Manual	Local System
	SysMain	Maintains a...	Running	Automatic	Local System
	<u>Sysmon</u>	System Mon...	Running	Automatic	Local System
	System Event Notification S...	Monitors sy...	Running	Automatic	Local System

## ADDC:

	<u>SplunkForwarder</u>	SplunkForw...	Running	Automatic	<u>Local System</u>
	Spot Verifier	Verifies pote...		Manual (Trigg...	Local System
	SSDP Discovery	Discovers ne...		Disabled	Local Service
	State Repository Service	Provides req...	Running	Manual	Local System
	Still Image Acquisition Events	Launches ap...		Manual	Local System
	Storage Service	Provides ena...	Running	Manual (Trigg...	Local System
	Storage Tiers Management	Optimizes th...		Manual	Local System
	SysMain	Maintains a...	Running	Automatic	Local System
	<u>Sysmon</u>	System Mon...	Running	Automatic	<u>Local System</u>
	System Event Notification S...	Monitors sy...	Running	Automatic	Local System

lưu ý: chạy ở Local System Account

4. thêm file inputs.conf vào C:\Program Files\SplunkUniversalForwarder\etc\system\local với nội dung như sau:

```
[WinEventLog://Application]
index = endpoint
disabled = false

[WinEventLog://Security]
index = endpoint
disabled = false

[WinEventLog://System]
index = endpoint
disabled = false

[WinEventLog://Microsoft-Windows-Sysmon/Operational]
index = endpoint
disabled = false
renderXml = true
source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
```

để Splunk thu thập các telemetry cần thiết bao gồm (Log ứng dụng, Log bảo mật, Log hệ thống, Log sysmon) từ test-machine và ADDC

5. thêm index và forwarding port trên splunk

endpoint	Edit	Delete	Disable	Events	search	11 MB	500 GB	48.5K	18 days ago	a few seconds ago	\$SPLUNK_DB/endpoint/db	–	✓ Active
----------	------	--------	---------	--------	--------	-------	--------	-------	-------------	-------------------	-------------------------	---	----------

---

**Configure receiving**

Set up this Splunk instance to receive data from forwarder(s).

Listen on this port \*

For example, 9997 will receive data on TCP port 9997.

## 2. Test:

1. trên máy kali thực hiện RDP brute force test-machine

```
hydra -l ba1 -P /home/ducbahpb/ad-project/password.txt 192.168.8.8 rd  
p
```

khi đó trên splunk sẽ hiện các log có event id: 4625 là failed logon

11/18/25 11/17/2025 10:46:12.690 AM  
LogName=Security  
EventCode=4625  
EventType=0  
ComputerName=test-machine.ducbahpb.local  
[Show all 61 lines](#)

Event Actions ▾

Type	<input checked="" type="checkbox"/> Field	Value	Actions
Selected	<input checked="" type="checkbox"/> EventCode ▾	4625	▾
	<input checked="" type="checkbox"/> host ▾	test-machine	▾
	<input checked="" type="checkbox"/> source ▾	WinEventLog:Security	▾
	<input checked="" type="checkbox"/> sourcetype ▾	WinEventLog	▾
Event	<input type="checkbox"/> Account_Domain ▾	-	▾

và nó hiện thị luôn cả IP máy hacker:

<input type="checkbox"/>	SourceName ▾	Microsoft Windows security auditing.	▾
<input type="checkbox"/>	Source_Network_Address ▾	192.168.8.250	▾
<input type="checkbox"/>	Source_Port ▾	0	▾
<input type="checkbox"/>	Status ▾	0xC000006D	▾
<input type="checkbox"/>	Sub_Status ▾	0xC000006A	▾
<input type="checkbox"/>	Subject_Account_Domain ▾	-	▾
<input type="checkbox"/>	Subject_Account_Name ▾	-	▾
<input type="checkbox"/>	Subject_Logon_ID ▾	0x0	▾
<input type="checkbox"/>	Subject_Security_ID ▾	S-1-0-0	▾
<input type="checkbox"/>	TaskCategory ▾	Logon	▾
<input type="checkbox"/>	Transited_Services ▾	-	▾
<input type="checkbox"/>	Type ▾	Information	▾
<input type="checkbox"/>	Workstation_Name ▾	kali	▾

## 2. kiểm tra hoạt động của splunk và splunk bằng Atomic Red Team

giả lập hành động một kẻ tấn công tạo ra một tài khoản người dùng local mới trên máy tính của bạn. `Invoke-AtomicTest T1136.001`

```

PS C:\Windows\system32> Invoke-AtomicTest T1136.001
PathToAtomicsFolder = 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        11/17/2025 5:56:19 AM
Password expires         Never
Password changeable      11/18/2025 5:56:19 AM
Password required        Yes
User may change password No
Workstations allowed     All
Logon script
User profile

```

i	Time	Event
>	11/17/25 8:56:19.625 PM	11/17/2025 05:56:19.625 AM ... 19 lines omitted ... Security ID: S-1-5-21-413940635-1318548777-3126359107-1003 Account Name: NewLocalUser Account Domain: TEST-MACHINE  <a href="#">Show all 26 lines</a> EventCode = 4726   host = test-machine   source = WinEventLog:Security   sourcetype = WinEventLog
>	11/17/25 8:56:19.596 PM	11/17/2025 05:56:19.596 AM ... 19 lines omitted ... Security ID: S-1-5-21-413940635-1318548777-3126359107-1003 Account Name: NewLocalUser Account Domain: TEST-MACHINE  <a href="#">Show all 27 lines</a> EventCode = 4798   host = test-machine   source = WinEventLog:Security   sourcetype = WinEventLog
>	11/17/25 8:56:19.586 PM	11/17/2025 05:56:19.586 AM ... 19 lines omitted ... Security ID: S-1-5-21-413940635-1318548777-3126359107-1003 Account Name: NewLocalUser Account Domain: TEST-MACHINE  <a href="#">Show all 27 lines</a> EventCode = 4798   host = test-machine   source = WinEventLog:Security   sourcetype = WinEventLog
>	11/17/25 8:56:19.578 PM	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' </Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime ation/><Execution ProcessID='2420' ThreadID='3808' /><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>te ntData><Data Name='RuleName'>technique_id=T1018,technique_name=Remote System Discovery</Data><Data Name='UtcTime'>2025- 000000600</Data><Data Name='ProcessId'>3248</Data><Data Name='Image'>C:\Windows\System32\net1.exe</Data><Data Name='Fi Net Command</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corpora ne'>C:\Windows\system32\net1 user NewLocalUser</Data><Data Name='CurrentDirectory'>C:\Users\Administrator.DUCBAHPB\AppData e='LogonGuid'>{cf50ab12-2714-691b-b3e8-0e0000000000}</Data><Data Name='LogonId'>0xee8b3</Data><Data Name='TerminalSessi 085E23DF67774ED89FD0215E1F144824F79F812B,MD5=63DD4523677E62A73A8A7494DB321EA2,SHA256=C687157FD58EAA51757CDA87D06C30953A <Data Name='ParentProcessGuid'>{cf50ab12-2983-691b-0f01-0000000000600}</Data><Data Name='ParentProcessId'>3432</Data><Da andLine'>"C:\Windows\system32\net.exe" user NewLocalUser</Data><Data Name='ParentUser'>DUCBAHPB\Administrator</Data></E host = test-machine   source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational   sourcetype = XmlWinEventLog:Microsoft-W
>	11/17/25 8:56:19.568 PM	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' </Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime ation/><Execution ProcessID='2420' ThreadID='3808' /><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>te ntData><Data Name='RuleName'>technique_id=T1018,technique_name=Remote System Discovery</Data><Data Name='UtcTime'>2025- 000000600</Data><Data Name='ProcessId'>3432</Data><Data Name='Image'>C:\Windows\System32\net.exe</Data><Data Name='Fil et Command</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corpora e'>C:\Windows\system32\net.exe" user NewLocalUser</Data><Data Name='CurrentDirectory'>C:\Users\Administrator.DUCBAHPB\ Host = test-machine   source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational   sourcetype = XmlWinEventLog:Microsoft-W

	8:56:19.283 PM	... 19 lines omitted ... Security ID: S-1-5-21-413940635-1318548777-3126359107-1003 Account Name: NewLocalUser Account Domain: TEST-MACHINE  <a href="#">Show all 27 lines</a> EventCode = 4798   host = test-machine   source = WinEventLog:Security   sourcetype = WinEventLog
>	11/17/25 8:56:19.279 PM	11/17/2025 05:56:19.279 AM ... 18 lines omitted ... Target Account: Security ID: S-1-5-21-413940635-1318548777-3126359107-1003 Account Name: NewLocalUser Account Domain: TEST-MACHINE  <a href="#">Show all 23 lines</a> EventCode = 4724   host = test-machine   source = WinEventLog:Security   sourcetype = WinEventLog
>	11/17/25 8:56:19.279 PM	... 21 lines omitted ... Account Name: NewLocalUser ... 2 lines omitted ... Changed Attributes: SAM Account Name: NewLocalUser Display Name: NewLocalUser User Principal Name: -  <a href="#">Show all 48 lines</a> EventCode = 4738   host = test-machine   source = WinEventLog:Security   sourcetype = WinEventLog
>	11/17/25 8:56:19.279 PM	11/17/2025 05:56:19.279 AM ... 18 lines omitted ... Target Account: Security ID: S-1-5-21-413940635-1318548777-3126359107-1003 Account Name: NewLocalUser Account Domain: TEST-MACHINE  <a href="#">Show all 23 lines</a> EventCode = 4722   host = test-machine   source = WinEventLog:Security   sourcetype = WinEventLog
>	11/17/25 8:56:19.270 PM	... 21 lines omitted ... Account Name: NewLocalUser ... 1 line omitted ...  Attributes: SAM Account Name: NewLocalUser Display Name: <value not set>  <a href="#">Show all 49 lines</a> EventCode = 4720   host = test-machine   source = WinEventLog:Security   sourcetype = WinEventLog

Splunk query: `index="ducbahpb" NewLocalUser`

4720: A user account was created

4722: A user account was enabled

4738: A user account was changed

4724: An attempt was made to reset an account's password

4798: A user's local group membership was enumerated

4726: A user account was deleted