A C T I V E D I R E C T O R Y L A B

Configuration Guide

Full Lab Architecture & Network Configuration

Scope

KALI · UBUNTU01 · CORPCL01 · CORPDC01 · ROOTDC · MFGDC01

Author

Rakib Nadir

Junior Penetration Tester · Offensive Security Mentor

sec.rakibnadir@gmail.com

March 2026

1. Lab Overview

This document covers the complete network and Active Directory configuration for a multi-hop penetration testing lab. The lab simulates a real enterprise environment with two separate AD forests, a Windows client, a Linux pivot server, and an attacker machine connected across four isolated network segments.

1.1 Architecture Summary

The attack chain flows from Kali through Ubuntu01 into the internal corporate network, escalating through the domain hierarchy until reaching the manufacturing forest via cross-forest trust.

> KALI → UBUNTU01 → CORPCL01 → CORPDC01 → ROOTDC → MFGDC01

1.2 Forest Structure

Forest 1: enterprise.dc (Primary Forest)

- Forest Root DC: ROOTDC — 172.16.0.10
- Child DC: CORPDC01 — corp.enterprise.dc — 172.16.0.30
- Windows Client: CORPCL01 — corp.enterprise.dc — 172.16.0.40

Forest 2: manufacturing.local (Secondary Forest)

- Forest Root DC: MFGDC01 — 10.20.0.20
- Trust: Bidirectional Forest Trust with enterprise.dc

1.3 Network Segments

Field	Value
NET-1 (External)	192.168.220.0/24 — KALI ↔ UBUNTU01
NET-2 (DMZ)	192.168.20.0/24 — UBUNTU01 ↔ CORPCL01
NET-3 (Corporate)	172.16.0.0/24 — CORPCL01 ↔ CORPDC01 ↔ ROOTDC
NET-4 (Manufacturing)	10.20.0.0/24 — ROOTDC ↔ MFGDC01

1.4 Full Node IP Table

Node	ETH0	ETH1	Domain/OS	Role
KALI	192.168.220.135	—	Kali Linux	Attacker
UBUNTU01	192.168.220.141	192.168.20.3	Ubuntu Server	Pivot #1
CORPCL01	192.168.20.2	172.16.0.40	corp.enterprise.dc	Pivot #2
CORPDC01	172.16.0.30	—	corp.enterprise.dc	Child DC
ROOTDC	172.16.0.10	10.20.0.10	enterprise.dc	Forest Root

Node	ETH0	ETH1	Domain/OS	Role
MFGDC01	10.20.0.20	—	manufacturing.local	Forest 2 Root

2. KALI — Attacker Machine

Kali Linux is the attacker machine. It can only reach UBUNTU01 on the external network segment. All attacks are launched from here.

2.1 Network Configuration

Field	Value
Interface	eth0
IP Address	192.168.220.135
Subnet Mask	255.255.255.0
Network	NET-1 (External)
Reachable	UBUNTU01 (192.168.220.141) only

2.2 Key Tooling

- Ligolo-ng — multi-hop tunnel proxy
- Impacket — AD attack suite
- BloodHound + SharpHound — AD enumeration
- Hashcat — offline password cracking
- Mimikatz / CrackMapExec — credential attacks
- Certipy — AD CS ESC1 exploitation

3. UBUNTU01 — Pivot #1

Ubuntu01 is the first pivot point and the entry point into the internal network. It has two NICs bridging the external network (KALI side) and the DMZ network (CORPCL01 side).

3.1 Network Configuration

ens37 — NET-1 (External, faces KALI)

Field	Value
IP Address	192.168.220.141

Field	Value
Subnet Mask	255.255.255.0
Gateway	192.168.220.2

ens33 — NET-2 (DMZ, faces CORPCL01)

Field	Value
IP Address	192.168.20.3
Subnet Mask	255.255.255.0
Gateway	(none)

3.2 Intentional Vulnerabilities

- Weak SSH credentials
- bash_history containing plaintext passwords
- Apache2 web server with exploitable vulnerability
- Ligolo-ng agent deployed for tunneling

3.3 IP Forwarding

Enable IP forwarding so UBUNTU01 can route traffic between NET-1 and NET-2:

```
echo 'net.ipv4.ip_forward=1' >> /etc/sysctl.conf
sysctl -p
```

4. CORPCL01 — Corporate Client (Pivot #2)

CORPCL01 is a Windows client joined to corp.enterprise.dc. It has two NICs — one facing UBUNTU01 on the DMZ network and one on the corporate network alongside CORPDC01 and ROOTDC.

4.1 System Information

Field	Value
OS	Windows 10 / Windows 11
Hostname	CORPCL01
Domain	corp.enterprise.dc
User	nadir (domain user)

4.2 Network Configuration

Ethernet1 — NET-2 (DMZ, faces UBUNTU01)

Field	Value
IP Address	192.168.20.2
Subnet Mask	255.255.255.0
Gateway	(none)
DNS	(none)

Ethernet0 — NET-3 (Corporate, faces CORPDC01 + ROOTDC)

Field	Value
IP Address	172.16.0.40
Subnet Mask	255.255.255.0
Gateway	172.16.0.1
DNS	172.16.0.30 (CORPDC01)

4.3 Domain Join

CORPCL01 is joined to corp.enterprise.dc using CORPDC01 as the DNS server (172.16.0.30). The domain join was performed via:

```
Add-Computer -DomainName "corp.enterprise.dc" -Credential (Get-Credential) -Restart
```

4.4 Intentional Vulnerabilities

- SMBv1 enabled
- WDigest authentication enabled (cleartext creds in LSASS)
- SYSVOL GPP cpassword
- Ligolo-ng agent for tunneling

5. CORPDC01 — Child Domain Controller

CORPDC01 is the Domain Controller for corp.enterprise.dc, a child domain of enterprise.dc. It sits entirely on the corporate network (NET-3) alongside ROOTDC and CORPCL01.

5.1 System Information

Field	Value
OS	Windows Server 2022
Hostname	CORPDC01

Field	Value
Domain	corp.enterprise.dc
Forest	enterprise.dc
NetBIOS Name	CORP
Functional Level	Windows Server 2016
DSRM Password	**********

5.2 Network Configuration

Ethernet1 — NET-3 (Corporate)

Field	Value
IP Address	172.16.0.30
Subnet Mask	255.255.255.0
Gateway	172.16.0.1
Preferred DNS	172.16.0.10 (ROOTDC)
Alternate DNS	172.16.0.30 (self)

> **NOTE:** CORPDC01 has a single NIC on NET-3. It can reach both ROOTDC (172.16.0.10) and CORPCL01 (172.16.0.40) directly on the same subnet.

5.3 Promotion

CORPDC01 was promoted as a child domain of enterprise.dc using the Active Directory Domain Services Configuration Wizard. Enterprise Admin credentials from ROOTDC were used to authorize the promotion.

5.4 Intentional Vulnerabilities

- AD CS ESC1 — misconfigured certificate template
- Kerberoastable SPN accounts
- MSSQL SA account with weak password
- IIS with default credentials

6. ROOTDC — Forest Root Domain Controller

ROOTDC is the Forest Root Domain Controller for enterprise.dc. It holds all five FSMO roles, acts as the trust anchor, and has a second NIC on NET-4 to communicate with MFGDC01 for the cross-forest trust.

6.1 System Information

Field	Value
OS	Windows Server 2022
Hostname	ROOTDC
Domain	enterprise.dc
Forest	enterprise.dc
NetBIOS Name	ENTERPRISE
Functional Level	Windows Server 2016
DSRM Password	**********
Admin Password	**********

6.2 Network Configuration

Ethernet0 — NET-3 (Corporate)

Field	Value
IP Address	172.16.0.10
Subnet Mask	255.255.255.0
Gateway	172.16.0.1
Preferred DNS	172.16.0.10 (self)

Ethernet1 — NET-4 (Manufacturing)

Field	Value
IP Address	10.20.0.10
Subnet Mask	255.255.255.0
Gateway	(none)
DNS	(none)

> **NOTE:** The second NIC on NET-4 is solely for cross-forest trust communication with MFGDC01. No gateway or DNS is needed on this interface.

6.3 Forest Promotion

ROOTDC was promoted as a new forest root using the Active Directory Domain Services Configuration Wizard via Server Manager.

6.4 Enterprise Admins — CORP Admin Addition

To allow CORP\Administrator to promote CORPDC01 as a child domain, it was temporarily added to Enterprise Admins on ROOTDC:

```
$corpAdmin = Get-ADUser -Identity "Administrator" -Server "172.16.0.30"
Add-ADGroupMember -Identity "Enterprise Admins" -Members $corpAdmin
```

7. MFGDC01 — Manufacturing Forest Root DC

MFGDC01 is the Forest Root Domain Controller for manufacturing.local — a completely separate forest from enterprise.dc. It connects to ROOTDC via a bidirectional cross-forest trust over NET-4.

7.1 System Information

Field	Value
OS	Windows Server 2022
Hostname	MFGDC01
Domain	manufacturing.local
Forest	manufacturing.local
NetBIOS Name	MANUFACTURING
Functional Level	Windows Server 2016
DSRM Password	**********

7.2 Network Configuration

Ethernet0 — NET-4 (Manufacturing)

Field	Value
IP Address	10.20.0.20
Subnet Mask	255.255.255.0
Gateway	10.20.0.1
Preferred DNS	10.20.0.20 (self)

7.3 Pre-Promotion Fix

AD CS (Certificate Authority) was pre-installed on the VM and conflicted with DC promotion. It was removed via Server Manager before proceeding with the promotion wizard.

7.4 Forest Promotion

MFGDC01 was promoted as a new forest root using the Active Directory Domain Services Configuration Wizard. Domain name: manufacturing.local, NetBIOS name: MANUFACTURING.

8. Cross-Forest Trust Configuration

A bidirectional Forest Trust connects enterprise.dc and manufacturing.local. This enables Kerberos authentication across both forests and allows cross-forest trust attacks during penetration testing.

8.1 Trust Details

Field	Value
Trust Type	Forest Trust
Direction	Bidirectional
Source Forest	enterprise.dc
Target Forest	manufacturing.local
Authentication	Forest-wide authentication
SID Filtering	Disabled (SIDFilteringQuarantined: False)
Forest Transitive	True

8.2 DNS Conditional Forwarders

On ROOTDC — Forward manufacturing.local to MFGDC01

DNS Manager → Conditional Forwarders → New Conditional Forwarder:

Field	Value
DNS Domain	manufacturing.local
Master Server IP	10.20.0.20
Replication	All DNS servers in this forest

On MFGDC01 — Forward enterprise.dc to ROOTDC

Field	Value
DNS Domain	enterprise.dc
Master Server IP	10.20.0.10
Replication	All DNS servers in this forest

8.3 DNS Verification

On ROOTDC:

```
Resolve-DnsName "manufacturing.local"
```

Expected result: 10.20.0.20

On MFGDC01:

```
Resolve-DnsName "enterprise.dc"
```

Expected result: 172.16.0.10

8.4 Trust Creation (GUI)

1. Active Directory Domains and Trusts → Right-click enterprise.dc → Properties → Trusts tab
2. Click New Trust → Trust Name: manufacturing.local
3. Trust Type: Forest Trust
4. Direction: Two-way
5. Sides: Both this domain and the specified domain
6. Enter MANUFACTURING\Administrator credentials
7. Outgoing + Incoming Auth: Forest-wide authentication
8. Confirm both sides → Finish

8.5 Trust Verification

```
Get-ADTrust -Filter * | Select Name, Direction, ForestTransitive, SIDFilteringQuarantined
```

✓ Trust is operational when Direction shows BiDirectional and ForestTransitive is True.

9. Attack Paths

9.1 Multi-Hop Attack Chain

Field	Value
Hop 1	KALI → UBUNTU01 via SSH Brute / CVE exploit
Hop 2	UBUNTU01 → CORPCL01 via SMBv1 / WDigest / SYSVOL GPP
Hop 3	CORPCL01 → CORPDC01 via Kerberoasting / AD CS ESC1
Hop 4	CORPDC01 → ROOTDC via ExtraSID / DCSync / Golden Ticket
Hop 5	ROOTDC → MFGDC01 via Cross-Forest Trust Attack

9.2 Pivot Tools

Field	Value
Ligolo-ng	Multi-hop tunnel proxy — deployed on UBUNTU01 and CORPCL01
Chisel	TCP tunnel — deployed on CORPDC01 for deep network access

10. Lab Credentials Reference

> **NOTE:** These credentials are intentionally weak for lab use only. Never use in production environments.

Field	Value
ROOTDC Administrator	**********
CORPDC01 Administrator	**********
CORPCL01 User (nadir)	**********
MFGDC01 Administrator	**********
ROOTDC DSRM	**********
CORPDC01 DSRM	**********
MFGDC01 DSRM	**********